Tempered

Airwall help
v3.2

Contents

Video Overview and Demos

Overviews and demos for the Tempered Airwall Solution.

Overviews	Demos
A five-minute overview of the Airwall Solution. https://www.youtube.com/embed/tSNZFps1LaI	Set up your Conductor https://www.youtube.com/embed/sLxbHtAlcN0
A longer overview and demos of how to set up zero trust with the Tempered Airwall Solution. https://www.youtube.com/embed/D49ojcswOTM	Add Airwall Gateways to your Conductor https://www.youtube.com/embed/5CZFc-jcdd4
	Integrating Nozomi with the Airwall Solution. https://www.youtube.com/embed/Ielzi6WwpLo

Connect to Airwall™

Connect your cellphone, mobile device, laptop, or server to an Airwall secure network to get access to the protected things you need to do your work. All it takes is installing the Airwall Agent or Server for your device, and then linking it to the Conductor that controls who can see those protected things on that Airwall secure network.

Before you can connect, on the device you will use to connect, you need to:

- Install an Airwall Agent or Server on your device (laptop, tablet, or cellphone)
- Create a profile for the network you want to connect to. If you're using **Airwall Invitations** or Activation codes, this profile is created for you.

If you are not configuring the profile with **Airwall Invitations** or Activation codes, you also need to have the Conductor administrator provision and manage your Airwall Agent or Server before you can connect.

Note: If you only have one profile, when you start the Airwall Agent or Server, it automatically connects with that profile.

Set up an Airwall Agent or Server

If you have received an email or activation code, see Link my Airwall Agent or Server to an Airwall secure network on page 14. If you need to install and configure manually, follow these instructions.

To connect to an Airwall secure network, you need to install the Airwall Agent or Server software on the laptop, mobile device, or server that you want to connect with, and then set up a link with the secure network. Check the Operating system requirements for Airwall Agents and Servers on page 7, and find installation instructions for the device you want to connect with under Install an Airwall Agent or Server on page 6.

Install an Airwall Agent or Server

To connect to anything that is protected by an Airwall secure network on your mobile phone or laptop, you need to install an Airwall Agent or Server.

If you have received an email or activation code, see Link my Airwall Agent or Server to an Airwall secure network on page 14. If you need to install and configure manually, follow these instructions to connect to an Airwall secure network. Check the Operating system requirements for Airwall Agents and Servers on page 7 to make sure your laptop or mobile device can run the software.

Install an Airwall Agent or Server

On the device you are using to connect, install the Airwall Agent or Server software. Here are the places you can find the software for your device:

- Open the link in your Airwall invitation.
- Go to the store for your device and search for Airwall.
- Download and run the installation file for your device from Latest firmware and software on page 514.

If you need additional help installing the software for your platform, see the specific instructions for your device.

Once you have installed the software, you need to set it up so it can connect to the Airwall secure network. The administrator for the secure network may have sent you an Airwall Invitation or Activation code, or you may want to set up your Airwall Agent or Server manually, and request to connect to the secure network.

- I have an Airwall Invitation on page 14
- I have an Activation Code on page 15
- I have a "Finish Setting up my account" email on page 15
- I want to request to connect on page 17

You can uninstall an Airwall Agent or Server using your device's normal uninstall process.

Operating system requirements for Airwall Agents and Servers

Operating system requirements for the Airwall Solution and Airwall Teams.

System Requirements

Please review the system requirements before installing to make sure your device can run the Airwall Agent or Server.

Microsoft Windows	The Windows Airwall Agent works on Microsoft Windows 7, 8.1, or 10, and runs on both Home and Professional versions. **Airwall only:** The Windows-based Airwall Server works on Microsoft Windows Server 2008R2, 2012R2, or 2016, or later.
Apple macOS	Works on 10.14 Mojave, or 10.15 Catalina, and later.
Apple iOS	Works on iOS 13 and later. Compatible with the iPhone and iPad.
Android	Works on 6.0 (Marshmallow) and later.
Linux	Works on Ubuntu 18.04, 20.04, and 22.04 (v3.1 and later), CentOS 8, and (Airwall only) Fedora 33.
Raspbian (Raspberry Pi)	Raspbian 9 (Stretch) or 10 (Buster)
RPi4/Ubuntu ARM64 (Raspberry Pi)	Raspbian 10 (Buster)

Apple (OSX and macOS): Install and configure an Airwall Agent

If you have received an email or activation code, see Link my Airwall Agent or Server to an Airwall secure network on page 14. If you need to install and configure manually, follow these instructions. You must be an administrator of the computer to install and configure the Airwall Agent.

Note: Download the macOS/OSX installation files from the Software Downloads and Release Notes on page 514 Software Downloads section of Airwall help.

Important: In v2.2 and earlier, you may be required to install a TAP device driver. In earlier versions, the TAP driver's certificate may display a developer other than Tempered. If this occurs, you can safely click **Allow** and continue with your installation.

Once the installation is complete, the application starts automatically.

To install and configure manually:

1. To install the Airwall Agent locate the files you downloaded, double-click on them to run the installer, and follow the prompts.
2. Left-click the Tempered icon in the macOS menu bar.
3. Select **Configure**.
4. On the **Airwall Configuration** page, do the following:
   a) Select the plus (+) to add a new profile.
   b) Under **Conductor**, enter the IP address or host name of your Conductor.
   c) Under **Port**, use the default port setting of *8096*, unless your Airwall secure network administrator has told you to use a different port.
   d) If you have an Activation code, under **Invitation**, enter the code. If you do not have a code, copy down or screenshot your **Device ID** and send to your administrator to activate your account.

   Note: Device ID, **Overlay Device IP** and **Overlay Netmask** are read-only and configurable from the Conductor.

   e) Select **Save**.

If you have used an Airwall Invitation or Activation code, once the Airwall Agent is recognized by the Conductor, you should be able to start connecting to protected resources. If you are connecting manually, send your Device ID to your administrator so they can activate your account.

Note: You may need to stop and restart the Airwall Agent to allow it to connect to the Conductor. Left-click the Tempered icon in the menu bar and select **Stop Airwall** to disconnect or **Start Airwall** to connect.

For information on using your macOS Airwall Agent, see Connect with an Apple (OSX and macOS) Airwall Agent on page 19.

Apple iOS: Install and configure an Airwall Agent

If you have received an email or activation code, see Link my Airwall Agent or Server to an Airwall secure network on page 14. If you need to install and configure manually, follow these instructions. You can get the Airwall Agent for iOS from Apple's App Store.

Note: If you received an invite, follow the instructions in the email to install and configure your Airwall Agent. The instructions below are for manual installation and configuration.

1. Install the Airwall Agent on your device from the Apple Store: https://itunes.apple.com/US/app/id1233852249.
2. Open the Apple iOS Airwall Agent.
3. From the menu, tap **Profiles**. Tap + to add a new profile.
4. Give the profile a name, and fill in the Conductor URL (and port, if provided to you).
5. If you have an Airwall Invite Code, enter it at the bottom.
6. Tap **ADD**.

If you have used an Airwall Invitation or Activation code, once the Airwall Agent is recognized by the Conductor, you should be able to start connecting to protected resources. If you are connecting manually, send your Device ID to your administrator so they can activate your account.

For information on using your Apple iOS Airwall Agent, see Connect with an iOS Airwall Agent on page 21.

Android: Install and configure an Airwall Agent

If you have received an email or activation code, see Link my Airwall Agent or Server to an Airwall secure network on page 14. If you need to install and configure manually, follow these instructions. You can get the Airwall

Agent for Android from the Google Play Store. Once installed, you configure a profile on the Airwall Agent to link to the Airwall secure network.

Note: If you receive an invite, follow the instructions in the email to install and configure your Airwall Agent. These instructions are for manual installation and configuration.

1. Install the Airwall Agent on your device from the Google Play store: https://play.google.com/store/apps/details?id=com.temperednetworks.hipclient
2. Open the Android Airwall Agent.
3. Add a new profile:
   - **v3.0 and later** – Scroll down to **Select Profile**, tap **MANAGE**, and then tap +.
   - **v2.2.12 and earlier** – From the menu, tap **Profiles**, and then tap +.
4. Give the profile a name, and fill in the Conductor URL (and port, if provided to you).
5. If you have an Airwall Invite Code, enter it.
6. Tap **ADD**.

If you have used an Airwall Invitation or Activation code, once the Airwall Agent is recognized by the Conductor, you should be able to start connecting to protected resources. If you are connecting manually, send your Device ID to your administrator so they can activate your account.

For information on using your Android Airwall Agent, see Connect with an Android Airwall Agent on page 22.

Linux: Install and configure an Airwall Server

If you have received an email or activation code, see Link my Airwall Agent or Server to an Airwall secure network on page 14. If you need to install and configure manually, follow these instructions. You can get the Airwall Server for your Ubuntu, Centos, or Fedora Linux server from the administrator for your Airwall secure network, or from Latest firmware and software on page 514. Once installed, you configure a profile on the Airwall Agent to link to the Airwall secure network.

Note:

- For pre-3.0 versions, replace `airsh` with `airctl`. See airctl Reference (pre-v3.0) on page 10.
- For pre-2.2.3 versions, see pre-2.2.3 help.

1. Install the Linux Airwall Server package for your version of Linux. If your secure network administrator has not provided you with a download, you can download the package you need from Latest firmware and software on page 514.
   - **For CentOS 7 or 8 or Fedora 3.3**: `sudo rpm -i <CentOS or Fedora install package>`
   - **For Ubuntu 16.04, 18.04, or 20.04**: `sudo dpkg -i <Ubuntu 16 or 18 package>`
2. Create a profile: `sudo airsh profile create name=<profile name> conductor=<conductor_url> [act=activation_code]`.

   You can optionally enter an Airwall Invitation activation code.
3. Make a profile the active one: `sudo airsh profile activate <profile name or number>`
4. Start the service: `sudo airsh service start`.

   Note: If the service is already running, enter `sudo airsh service restart` to stop and start the service.

If you have used an Airwall Invitation or Activation code, once the Airwall Server is recognized by the Conductor, you should be able to start connecting to protected resources on the Airwall secure network. If you are connecting manually, send your Device ID to your administrator so they can activate your account.

For information on getting your Device ID, or using your Linux Airwall Server, see Connect with a Linux Airwall Server on page 26. For more Airshell commands, see Linux Airwall Server Airshell commands on page 372.

Uninstall the Linux Airwall Server

Follow the instructions for your operating system to uninstall the Linux Airwall Server:

- Ubuntu:

  ```
  sudo apt-get purge airwall
  ```

- CentOS/Fedora:

  ```
  sudo yum remove airwall
  ```

To remove all files (including profiles):

```
sudo rm -r /opt/tnw
```

airctl Reference (pre-v3.0)

If you are using a Linux Airwall Server that is earlier than v3.0, here are the `airctl` commands available. You can see commands by typing `airctl reference`.

You use the `airctl` command line to see details on Linux or Raspberry Pi Airwall Agent or Server. On your Linux or Raspberry Pi device, open a terminal window, and type `airctl` or `sudo aircrl`, followed by the desired command.

`profile details <profile name> details=<profile-details>`	Show all or some of the details of an Airwall Agent or Server profile. Instead of entering a profile name, you can get details on the currently-active profile by entering `airctl profile details --active`.
`profile modify <profile name> [new_name=<string>] [conductor=<addr:port>] [network=<interface | auto>] [invitation=<invitation>] [log_level=<info | warn | error | debug | trace>] [sys=<sys-impl>] [activate] details=<profile-details>`	Modify a profile. For example, to change the log level to debug for a profile named myprofile, you would enter: `airctl profile modify myprofile log_level=debug`.
`profile activate <profile name> [sys=<sys-impl>] profile_name=<string>`	Set the specified profile to the active one.
`profile create <new profile name> [allow_rename=<boolean>] conductor=<addr:port> [network=<interface | auto>] [invitation=<invitation>] [sys=<sys-impl>] [activate] details=<profile-details> profile_name=<string>`	Create a profile. You can specify the Conductor URL and port, interface to use, Invitation code, and name. Add `activate` to set the new profile as the active profile.
`profile delete <profile name> <no additional result data>`	
`profile rename <profile name> new_name=<string> profile_name=<string>`	Rename a profile.
`service start [sys=<sys-impl>] <no additional result data>`	Start the Linux Airwall Server.
`service stop [sys=<sys-impl>] <no additional result data>`	Stop the Linux Airwall Server.
`service restart [sys=<sys-impl>] [full] <no additional result data>`	Restart the Linux Airwall Server.

`service status running=<bool> conductor=<bool> tunnel=<bool>`	Show status of your Linux Airwall Server.
`list interfaces _interfaces=<_interfaces>`	List network interfaces.
`list profiles _profiles=<profile-list> current_dir=<string> current_name=<string> root_dir=<string>`	List profiles.
`list versions hipapp_version=<string> hipctl_version=<string>`	Show the version of your Linux Airwall Server.
`list log <profile name> [max_lines=<integer>] [log_level=<info | warn | error | debug | trace>] _log=<_log> profile_name=<string>`	List log messages.
`support reset <profile name> support reset=<string>`	Reset a profile.
`support bundle output=<string>`	Create a support bundle.

Microsoft Windows or Windows Server: Install and configure an Airwall Agent or Server

If you have received an email or activation code, see Link my Airwall Agent or Server to an Airwall secure network on page 14. If you need to install and configure manually, follow these instructions. You can get the Airwall Agent or Server for Windows from the administrator of your Airwall secure network, or download the latest installation files from Latest firmware and software on page 514. Once installed, you configure a profile on the Airwall Agent or Server to link to the Airwall secure network.

Note: You can start and stop the Airwall Agent or Server service as needed. Keep in mind when an Airwall Agent or Server service is stopped, you cannot connect to anything on the protected network.

To install and configure the Windows Airwall Agent or Server:

1. Log into your Windows computer as an administrator.
2. Download and install the Windows Airwall Agent or Server from Latest firmware and software on page 514.

   Note: If you are asked to install the TAP-Windows Provider as part of the installation procedure, click **Install** when prompted.
3. Once the installation is complete, the Airwall Agent or Server starts automatically.
4. Right-click the Tempered icon in the Windows System Tray
5. Select **Configure**
6. In the **Configure** window, do the following:

   a) Enter the IP address or host name of your Conductor. The default port setting is *8096*. If you have an activation code, enter it here.

      Note: The **Device ID**, **Overlay Device IP**, and **Overlay Netmask** fields are read-only and configurable from the Conductor.

   b) Click **OK**.

If you have used an Airwall Invitation or Activation code, once the Airwall Agent or Server is recognized by the Conductor, you should be able to start connecting to protected resources. If you are connecting manually, send your Device ID to your administrator so they can activate your account.

For information on using your Windows Airwall Agent or Server, see Connect with a Windows Airwall Agent or Server on page 27.

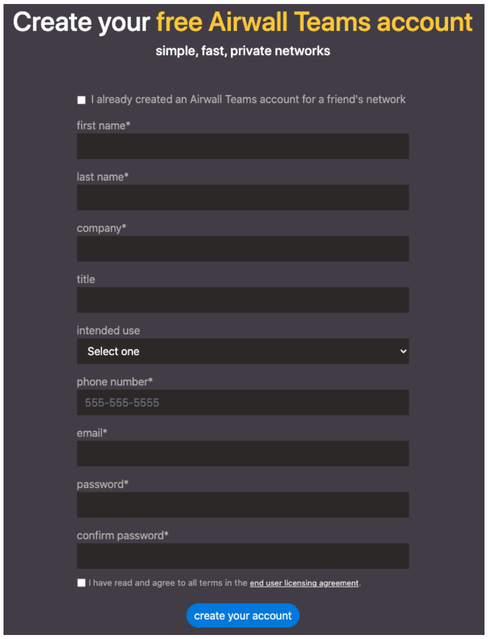
Note: You may need to stop and restart the Airwall Agent or Server to allow it to connect to the Conductor. Right-click the Tempered icon in the Windows System Tray and select **Stop** to suspend the service or **Start** to resume.

Raspbian and RPi4/Ubuntu ARM64 – Install the Airwall Server

To connect to Airwall Teams, install the Raspberry Pi Raspbian or RPi4/Ubuntu ARM64 Airwall Server on your device.

Before you begin, check the Operating system requirements for Airwall Agents and Servers on page 7 for your Raspberry Pi device.

1. On your Raspberry Pi, open the email you received and select **Click here to confirm this mail**.
2. Fill in the **Create Account** form: Enter your name and create an Airwall Teams account password.
3. Read and agree to the terms: Check **I have read and agree to all terms in the end user licensing agreement**, and click **Submit**.



Create your free Airwall Teams account

simple, fast, private networks

□ I already created an Airwall Teams account for a friend's network

first name*

last name*

company*

title

intended use

Select one

phone number*

555-555-5555

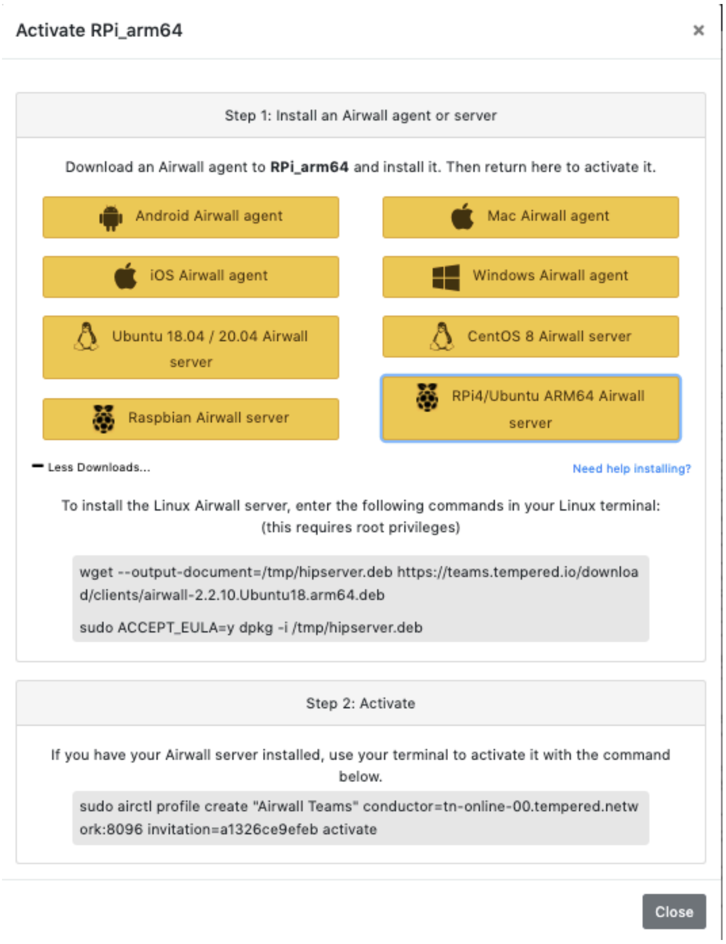
email*

password*

confirm password*

□ I have read and agree to all terms in the end user licensing agreement.

4. Under Step 1, click the link to download the installation file for your Raspberry Pi version. Click **More Downloads** if your installation type isn't shown.
5. Install the Airwall Server package for your version of Raspberry Pi. You can copy and paste the commands from the install page:



Step 1: Install an Airwall agent or server

Download an Airwall agent to **RPi_arm64** and install it. Then return here to activate it.

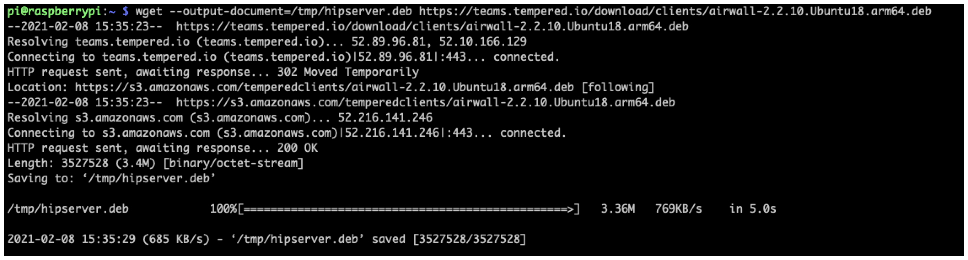
To install the Linux Airwall server, enter the following commands in your Linux terminal:
(this requires root privileges)

```
wget --output-document=/tmp/hipserver.deb https://teams.tempered.io/downloa
d/clients/airwall-2.2.10.Ubuntu18.arm64.deb
sudo ACCEPT_EULA=y dpkg -i /tmp/hipserver.deb
```

Step 2: Activate

If you have your Airwall server installed, use your terminal to activate it with the command below.

```
sudo airctl profile create "Airwall Teams" conductor=tn-online-00.tempered.netw
ork:8096 invitation=a1326ce9efeb activate
```



```
pi@raspberrypi:~ $ wget --output-document=/tmp/hipserver.deb https://teams.tempered.io/download/clients/airwall-2.2.10.Ubuntu18.arm64.deb
--2021-02-08 15:35:23--  https://teams.tempered.io/download/clients/airwall-2.2.10.Ubuntu18.arm64.deb
Resolving teams.tempered.io (teams.tempered.io)... 52.89.96.81, 52.10.166.129
Connecting to teams.tempered.io (teams.tempered.io)|52.89.96.81|:443... connected.
HTTP request sent, awaiting response... 302 Moved Temporarily
Location: https://s3.amazonaws.com/temperedclients/airwall-2.2.10.Ubuntu18.arm64.deb [following]
--2021-02-08 15:35:23--  https://s3.amazonaws.com/temperedclients/airwall-2.2.10.Ubuntu18.arm64.deb
Resolving s3.amazonaws.com (s3.amazonaws.com)... 52.216.141.246
Connecting to s3.amazonaws.com (s3.amazonaws.com)|52.216.141.246|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3527528 (3.4M) [binary/octet-stream]
Saving to: '/tmp/hipserver.deb'

/tmp/hipserver.deb           100%[=============================================>]   3.36M   769KB/s    in 5.0s

2021-02-08 15:35:29 (685 KB/s) - '/tmp/hipserver.deb' saved [3527528/3527528]
```

You can also manually install by entering:

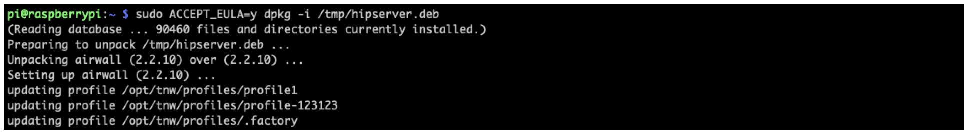
Raspbian:

```
wget --output-document=/tmp/airwall.deb https://teams.tempered.io/
download/clients/airwall_2.2.10.Raspbian9.armhf.deb
```

RPi4 Ubuntu ARM64:

```
wget --output-document=/tmp/airwall.deb https://teams.tempered.io/
download/clients/airwall-2.2.10.Ubuntu18.arm64.deb
```

6. Accept the EULA using sudo ACCEPT. Again, you can copy from the install page:

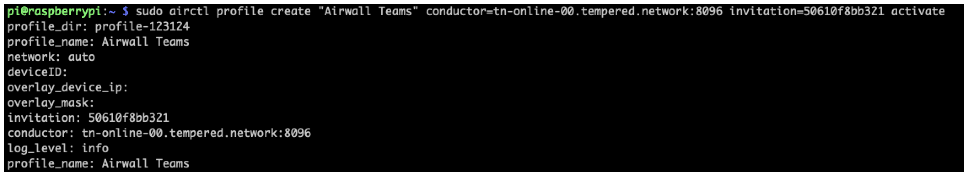


```
pi@raspberrypi:~ $ sudo ACCEPT_EULA=y dpkg -i /tmp/hipserver.deb
(Reading database ... 90460 files and directories currently installed.)
Preparing to unpack /tmp/hipserver.deb ...
Unpacking airwall (2.2.10) over (2.2.10) ...
Setting up airwall (2.2.10) ...
updating profile /opt/tnw/profiles/profile1
updating profile /opt/tnw/profiles/profile-123123
updating profile /opt/tnw/profiles/.factory
```

You can also manually enter the command:

```
sudo ACCEPT_EULA=y dpkg -i /tmp/airwall.deb
```

7. Create a profile and activate your connection by copying and pasting the activation command from the install page.



```
pi@raspberrypi:~ $ sudo airctl profile create "Airwall Teams" conductor=tn-online-00.tempered.network:8096 invitation=50610f8bb321 activate
profile_dir: profile-123124
profile_name: Airwall Teams
network: auto
deviceID:
overlay_device_ip:
overlay_mask:
invitation: 50610f8bb321
conductor: tn-online-00.tempered.network:8096
log_level: info
profile_name: Airwall Teams
```

You can also manually activate by entering:

```
sudo airctl profile create <profile name> conductor=<conductor>
 invitation=<invite code> activate
```

8. Start the service my entering:

```
airctl service start
```

Note: If the Airwall service is already running, it may not activate a new profile without first stopping and starting the service.

9. Return to the Airwall Teams website and click **Activate**. Copy the command under **Step 2: Activate**. You will use this command to activate the Airwall Server.
10. Paste the command into a terminal window, and press **Enter** to activate your Airwall Server.
11. Wait for the Airwall Server to activate. When complete, you will get a message that your Airwall Server has been activated.

Click **Look around** to close the activation window. Find your device in the device list on the left to verify you are connected. You can also check in a terminal by typing the following:

```
sudo airctl service status
```

In the output, look for the line `conductor=true`, which means you are connected to your Airwall Teams network.

Link my Airwall Agent or Server to an Airwall secure network

Once you have installed the Airwall Agent or Server software, you can link it to one or more Airwall secure networks.

Tip: For the best experience for you and the administrator for the secure network you are linking to, ask your Airwall administrator to send you an Airwall Invitation or **Activation Code**.

Choose the relevant section below based on how you are invited to an Airwall secure network.

I have an Airwall Invitation

Connect your Airwall Agent or Server to an Airwall secure network with an Airwall Invitation.

1. Install an Airwall Agent or Server on page 6.
2. After you have installed the software, open the Airwall invitation on the same device, and click **Activate**.
3. Open the Airwall Agent, and tap **Get Started**.
4. From the menu, tap **Profiles**.
5. Select the profile created when you activated your invitation, and slide the toggle to **On**. It may take a few minutes for your device to complete activation, and then it will show you are connected to the Conductor.

You can now turn on the Airwall Agent or Server profile when you need to access protected assets. See Connect to an Airwall secure network on page 19.

I have an Activation Code

Connect your Airwall Agent or Server to an Airwall secure network with an Activation code.

How to connect to an Airwall secure network when you have received an Activation code.

1. Install an Airwall Agent or Server on page 6.
2. To activate an Airwall Agent, see Set up my Airwall Agent Manually on page 18.

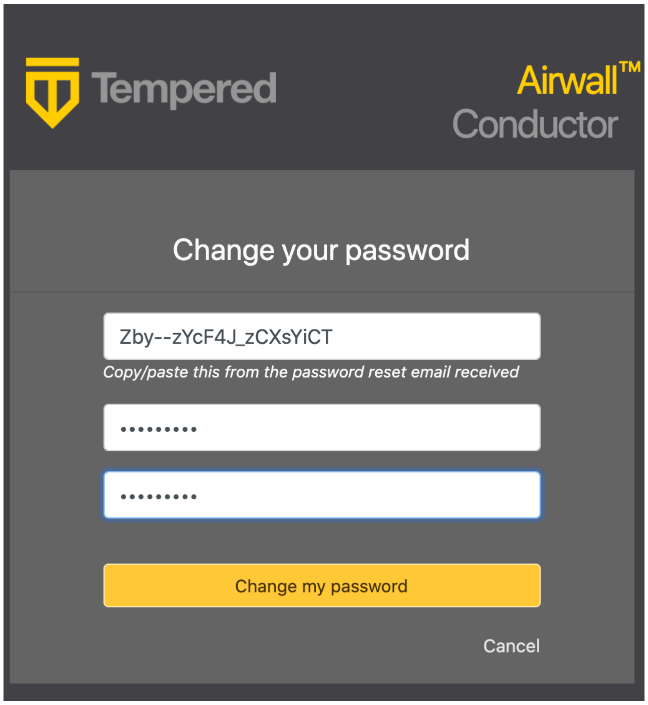
   To activate an Airwall Server, see Set up my Airwall Server Manually on page 18.

I have a "Finish Setting up my account" email

Connect your Airwall Agent or Server to an Airwall secure network from the "Finish setting up my account" email.

How to connect to an Airwall secure network when you received an email saying "Finish setting up your account."

1. Install an Airwall Agent or Server on page 6.
2. From the computer, cellphone, or tablet that you want to connect to this Airwall secure network, open the “Finish setting up your account” link in the email.
3. Enter and confirm a password, then click **Change my password**. If the token is not filled in, either click the link in the email that has the token, or copy the token from the email and paste in the top box.



Change your password

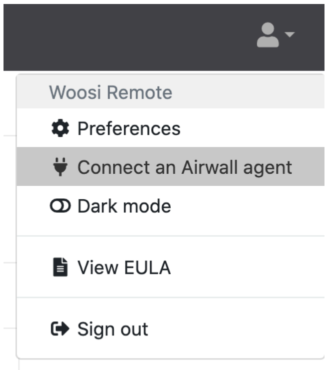
Zby--zYcF4J_zCXsYiCT

Copy/paste this from the password reset email received

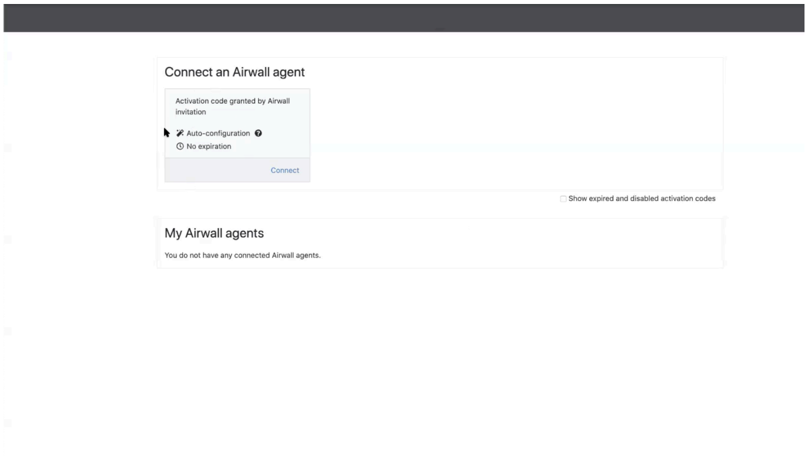
•••••••••

•••••••••

4. If you are not on the **Connect an Airwall Agent** page, click your profile icon in the upper right and select **Connect an Airwall Agent**.



5. On the **Connect an Airwall Agent** page, under **Activation code granted** box, click **Connect**.



Connect an Airwall agent

Activation code granted by Airwall invitation

Auto-configuration

No expiration

□ Show expired and disabled activation codes

My Airwall agents

You do not have any connected Airwall agents.

6. Follow the **Connect an Airwall Agent** steps to install the Airwall Agent or Server for your computer or mobile device.

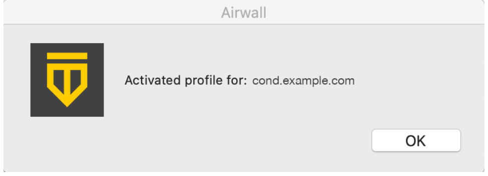
   If your computer or mobile device is not shown, open **More downloads** to find the correct version to install.

7. When the Airwall Agent or Server is installed, come back to the **Connect an Airwall Agent** page, and click **Activate**. You may need to give permission for the Airwall Agent or Server to make changes to your program.

   Activation creates a profile in your Airwall Agent or Server that you can use to access resources on the Airwall secure network. You can have multiple profiles if you need to connect to different secure networks. See Create or Edit Airwall Agent or Server Profiles on page 29.

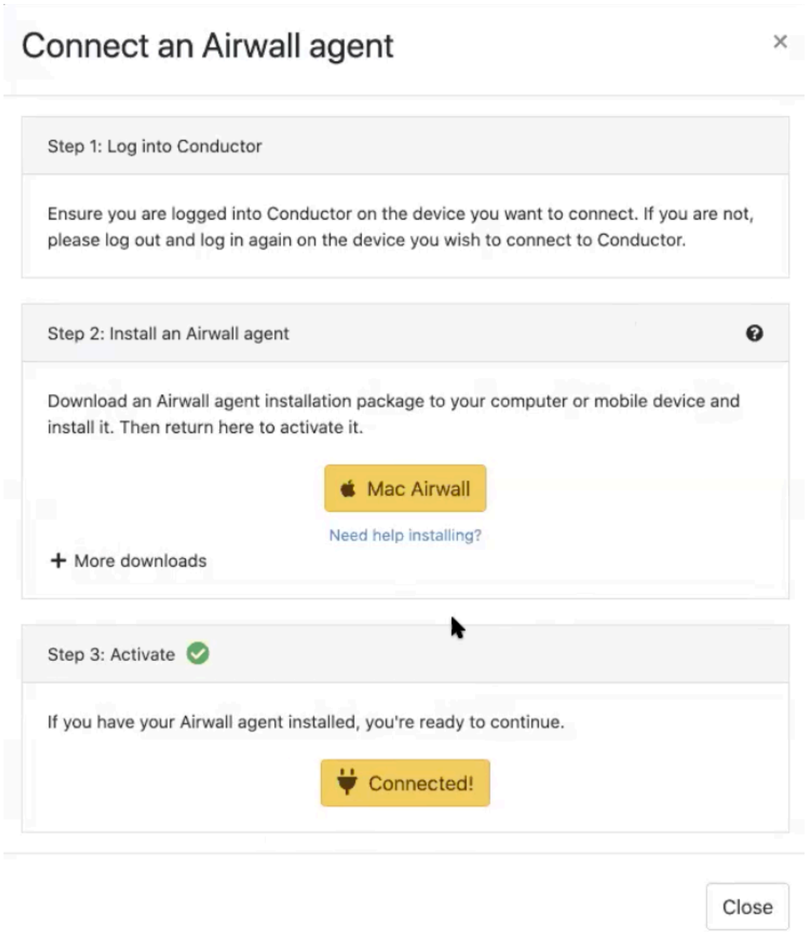
   Note: If you do not have an Activation code, you can select **Request a Connection** to send the Airwall secure network administrator a request to add you to the network.

8. When it's finished, you'll see an confirmation that your profile has been activated.



Airwall

Activated profile for: cond.example.com



Connect an Airwall agent

Step 1: Log into Conductor

Ensure you are logged into Conductor on the device you want to connect. If you are not, please log out and log in again on the device you wish to connect to Conductor.

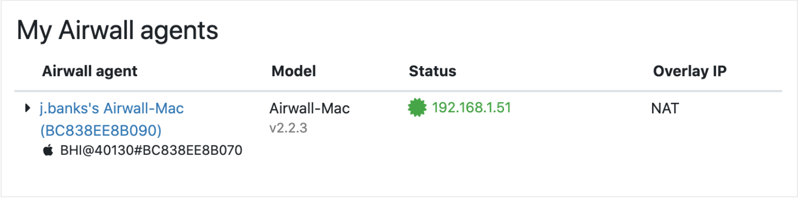
Step 2: Install an Airwall agent

Download an Airwall agent installation package to your computer or mobile device and install it. Then return here to activate it.

Step 3: Activate ✓

If you have your Airwall agent installed, you're ready to continue.

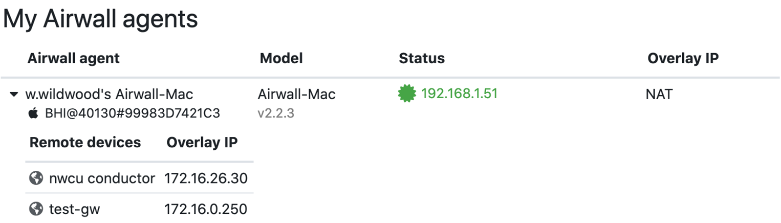
9. Select **Close** to close this page. The **Connect an Airwall Agent** page now shows your active Airwall Agents and Servers, and their status:



My Airwall agents

Airwall agent	Model	Status	Overlay IP
j.banks's Airwall-Mac (BC838EE8B090) BHI@40130#BC838EE8B070	Airwall-Mac v2.2.3	192.168.1.51	NAT

10. Click the arrow to the left of your Airwall Agent or Server to see what resources (Remote devices) you have access to:



My Airwall agents

Airwall agent	Model	Status	Overlay IP
w.wildwood's Airwall-Mac BHI@40130#99983D7421C3	Airwall-Mac v2.2.3	192.168.1.51	NAT

Remote devices	Overlay IP
nwcu conductor	172.16.26.30
test-gw	172.16.0.250

You can now use the Airwall Agent or Server to connect to these resources on the Airwall secure network. For how to start and stop your secure connection or change profiles, see Connect to an Airwall secure network on page 19.

I want to request to connect

Request to connect your Airwall Agent or Server to an Airwall secure network.

You can manually set up your Airwall Agent or Server by creating a profile and entering the Conductor address for the Airwall secure network. You can get the Conductor address from the administrator for the secure network. When you are finished setting up your profile, the first time you attempt to connect, the Airwall secure network administrator gets a request from you to allow you to connect and then configures the resources you have access to.

Set up my Airwall Agent Manually

1. Open the Airwall Agent, and tap Get Started.
2. From the menu, tap **Profiles**.
3. Tap the plus (+) sign.
4. Enter a name for your profile.
5. Enter the Conductor address (URL or IP address).
6. Tap **Add**.
7. On the main page of your Airwall Agent, select the new profile, and slide the toggle to open the connection.
8. If you have an Activation Code, enter it in the **Activation Code** or **Invitation** box.

   If you do not have an Activation Code, send your Conductor administrator your device ID (shown on the profile page) and request they provision your device. Leave the Airwall Agent profile on while your administrator finds and provisions your device.

If you have connected with an Activation code, you will be able to connect right away. If you have requested your device be provisioned, you will have access once the Conductor administrator provisions your device.

When your Airwall Agent shows you are connected to the Conductor, and you can reach assets in the Airwall secure network on your device. See Connect to an Airwall secure network on page 19.

You can now turn on the Airwall Agent profile when you need to access protected assets.

Set up my Airwall Server Manually

Set up a Windows Airwall Server manually

1. Open the Airwall Server, and from the menu, click **Configure**.
2. At the bottom of the left side, click the plus (+).
3. Enter your password to allow changes on your device.
4. Enter a name for the new profile.
5. Enter the Conductor URL or IP address provided by your Conductor administrator, and click **OK**.
6. On the main page of your Airwall Server, select the new profile.
7. Click the gear icon at the bottom of the profile list, and select **Make Active**.
8. Send your Conductor administrator your device ID (shown on the profile page) and request they provision your device. Leave the Airwall Server profile on while your administrator finds and provisions your device.

Set up a Linux Airwall Server manually

1. To create a new profile and activate with an Activation code, enter:

   ```
   sudo airctl profile create <profile_name> conductor=<conductor_url>
    invitation=<activation_code>
   ```

   For example:

   ```
   sudo airctl profile create MyProfile conductor=cond.example.com
    invitation=45k234k678k901k
   ```

2. To modify an existing profile and activate with an Activation code, enter:

   ```
   sudo airctl profile modify <profile_name> conductor=<conductor_url>
    invitation=<activation_code>
   ```

For example:

```
sudo airctl profile modify MyProfile conductor=cond.example.com
 invitation=45k234k678k901k
```

Once the Conductor administrator provisions your device, your Airwall Server shows you are connected to the Conductor, and you can reach assets in the Airwall secure network with your device.

You can now turn on the Airwall Server profile when you need to access protected assets. For more information, see Connect to an Airwall secure network on page 19.

Connect to an Airwall secure network

Once you have installed and linked your Airwall Agent or Server, you can then start and stop it at any time to connect and disconnect from the Airwall secure network.

Note:

- You can use your Airwall Agent or Server to connect to other Airwall secure networks. Just set up a new profile for each one you need to connect to. For information on how, see Create or Edit Airwall Agent or Server Profiles on page 29
- The Airwall Agent or Server does not disable the wired or wireless interfaces of your device. For example, if you are running an Airwall Agent, you can at the same time be connected to the Internet wirelessly and the corporate network via a wired connection.

Connect with an Apple (OSX and macOS) Airwall Agent

How to connect to an Airwall secure network with an OSX/macOS Airwall Agent.

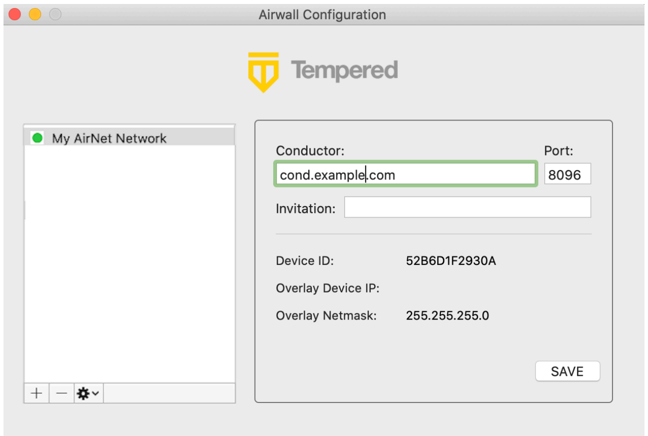
Connect to the Airwall secure network

In the macOS top bar, select the Tempered shield 🛡, and select **Start Airwall**.

Manage Profiles

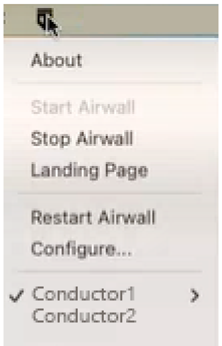
To manage your profiles, start the macOS Airwall Agent, click the Tempered shield 🛡, and then select **Configure** to open the Configure page.

- **To create a new profile**, From the menu, select **Configure**, and click the plus (+) + − .
- **To switch profiles**, If the profile you want has a solid green dot to the left, it is already the Active profile. If it does not, select the profile you want to use, select the gear or triple dot icon (depending on your version) below the profile list, and select **Make Active**. The Agent disconnects and then connects with the new profile. This can take a few minutes.



Conductor: cond.example.com
Port: 8096
Invitation:
Device ID: 52B6D1F2930A
Overlay Device IP:
Overlay Netmask: 255.255.255.0

Note: In v3.2.3 and later you can switch between Conductors from the drop down menu in the Tempered shield without opening the Configure page.

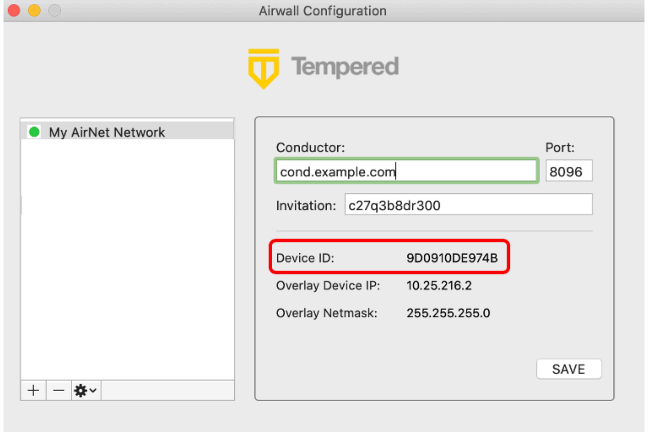


- **To edit an existing profile**, Select a profile to edit, edit the details on the right, then select **SAVE**.
- **To delete a profile**, Select it and below the list, click -.

Find your device ID

If you are still not connected, you may need to provide your device ID to the administrator for your Airwall secure network.

1. Open the macOS Airwall Agent.
2. In the macOS top bar, click the Tempered shield, and then select **Configure**.
3. Select the profile you are using to connect to the Airwall secure network.
4. Send your Airwall secure network administrator your **Device ID**.



Conductor: cond.example.com
Port: 8096
Invitation: c27q3b8dr300
Device ID: 9D0910DE974B
Overlay Device IP: 10.25.216.2
Overlay Netmask: 255.255.255.0

Check your Connection

There are two ways to check your connection:

- In the macOS top bar, look for the status dot next to the Tempered shield :
  - No dot or green dot: Connected to the active profile.
  - Dark grey dot: Service stopped.
  - Red dot: No connection.
  - Purple dot: In Disconnected mode (connected to resources but not the Conductor.) See Sync an Airwall Agent or Server in Disconnected Mode on page 29
- Select the shield icon and select **Configure** to see which profile is active on the **Airwall Configuration** page (shown by the green dot):

Disconnect from the Airwall secure network

In the macOS top bar, select the Tempered shield , and select **Stop Airwall**.

Connect with an iOS Airwall Agent

How to connect to an Airwall secure network with a iOS Airwall Agent.

Connect to the Airwall secure network

Open the iOS Airwall Agent, and under **Profile**, tap the slider to slide to the right to connect.

Manage Profiles

- **To create a new profile**, From the menu, tap **Profiles**. Tap + to add a new profile.
- **To switch profiles**, tap the **Profile** tab, tap the profile you want to switch to. If you are asked if you want to disconnect and switch to the profile selected, tap **Yes**.

  Note: If the profile you want is displayed, it is the Active profile.
- **To edit an existing profile**, From the menu, tap **Profiles**, tap **Edit**, and select a profile to edit.
- **To delete a profile**, touch the profile name, slide right to left and tap **Delete**.

Find your device ID

If you are still not connected, you may need to provide your device ID to the administrator for your Airwall secure network.

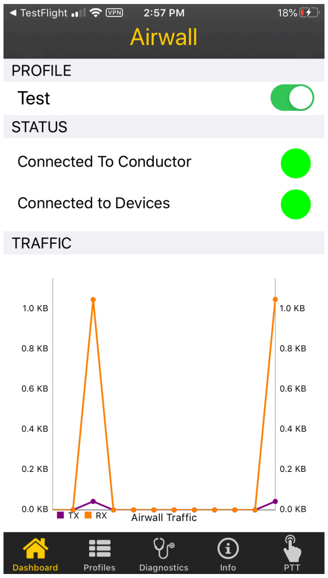
1. In the iOS Airwall Agent, switch to and connect the profile you want to use.
2. Tap the Info tab at the bottom of the page. Take note of the Device ID and send it to your Airwall secure network administrator.

Check your Connection

Open your iOS Airwall Agent. Check that:

- Under **Profile**, the correct profile is open, and that the slider is to the right and green.
- Under **Status**, both **Connected to Conductor** and **Connected to Devices** are solid green.

  This example shows that you are connected to the Conductor and Devices.



Airwall

PROFILE

Test

STATUS

Connected To Conductor ●

Connected to Devices ●

TRAFFIC

A **Grey dot** means no connection or not connected.

Disconnect from the Airwall secure network

Open the iOS Airwall Agent, and under **Profile**, tap the slider to slide to the left to disconnect.

Connect with an Android Airwall Agent

How to connect to an Airwall secure network with an Android Airwall Agent.

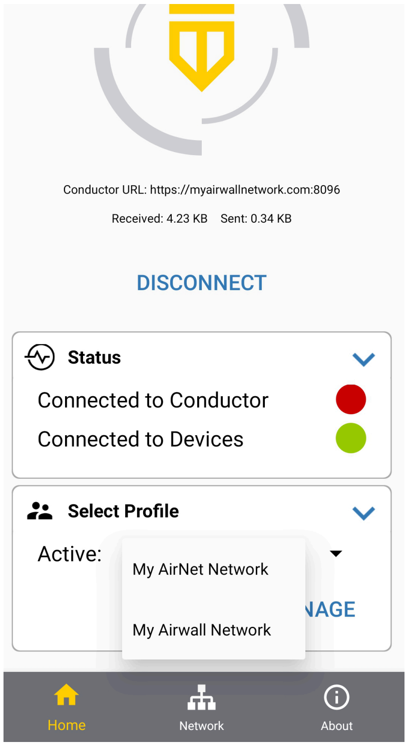
Connect to the Airwall secure network

- **v3.0 and later** – Tap **CONNECT**.
- **v2.2.12 and earlier** – Open the Android Airwall Agent, and under **Profile**, tap the slider to slide to the right to connect.

Manage Profiles

- **v3.0 and later** –
  - **To create a new profile** – Scroll down to **Select Profile**, tap **MANAGE**, and then tap +.
  - **To switch profiles** – Under **Select Profile**, tap the down arrow next to the active profile name, and select the profile you want to switch to.

    Note: If the profile you want is already displayed, it's already the Active profile.



Conductor URL: https://myairwallnetwork.com:8096

Received: 4.23 KB Sent: 0.34 KB

DISCONNECT

Status

Connected to Conductor ●

Connected to Devices ●

Select Profile

Active:

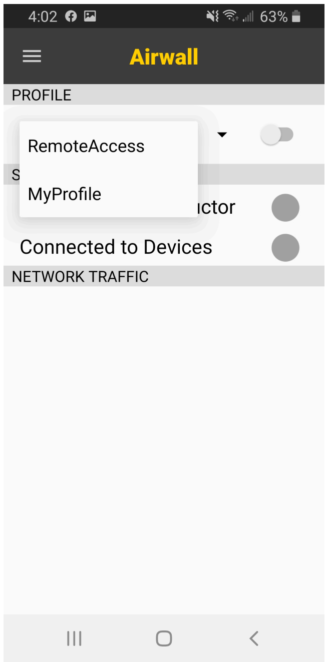
My AirNet Network

My Airwall Network

- **To edit an existing profile** – Scroll down to **Select Profile**, tap **MANAGE**, tap the three dots next to the profile you want to edit, and tap **Edit**. Or, tap and hold a profile to edit. Tap **Save** when done.
- **To delete a profile**– Scroll down to **Select Profile**, tap **MANAGE**, tap the three dots next to the profile you want to edit, and then tap **Delete**.

- **v2.2.12 and earlier** –
  - **To create a new profile** – From the menu, tap **Profiles**. Tap + to add a new profile. Enter the information needed and tap **Add**.
  - **To switch profiles** – Under **Profile**, tap the active profile name, and select the profile you want to switch to.

Note: If the profile you want is already displayed, it's the Active profile.



- **To edit an existing profile** – From the menu, tap **Profiles**. Tap and hold a profile to edit. Tap **Save** when done.
- **To delete a profile**– From the menu, tap **Profiles**. Tap and hold a profile to edit. At the bottom, tap **Delete**.

Find your device ID

If you're still not connected, you may need to provide your device ID to the administrator for your Airwall secure network.

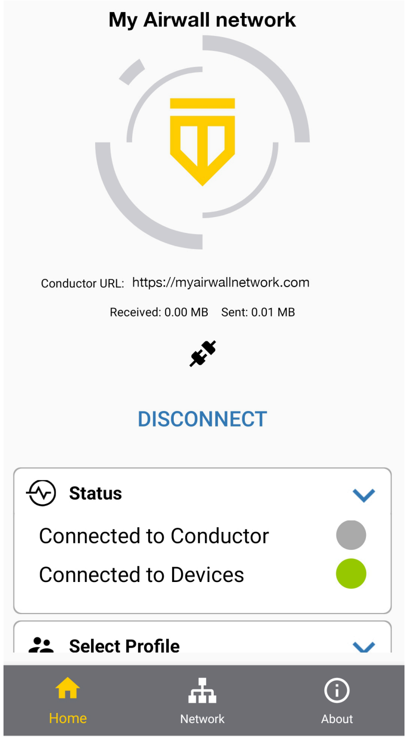
1. In the Android Airwall Agent, switch to and connect with the profile you want to use.
2. Find your device ID:
   - **v3.0 and later** – At the bottom, tap Network. Copy and give your Airwall secure network administrator the UID.
   - **v2.2.12 and earlier** – Tap the top left menu, and then tap **Info**. Find the Device ID to provide to your Airwall secure network administrator at the top of this page.

Check your Connection

Open your Android Airwall Agent. Check that:

- On v3.0 and later, check:
  - Under **Select Profile**, the correct profile is active.
  - Under **Status**, check that **Connected to Devices** shows connected (green).

Note: If your Airwall secure network administrator has your device set to Disconnected mode, your **Connected to Conductor** status shows as disconnected most of the time, but you will still have access to devices. See Sync an Airwall Agent or Server in Disconnected Mode on page 29.

- 

  My Airwall network

  Conductor URL: https://myairwallnetwork.com

  Received: 0.00 MB Sent: 0.01 MB

  DISCONNECT

  Status

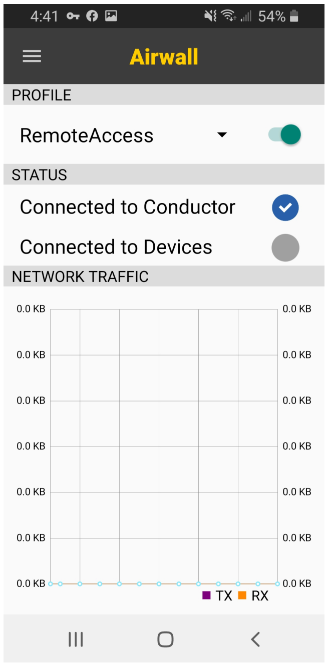
  Connected to Conductor ●

  Connected to Devices ●

  Select Profile

  - Tap **Networks**. The network details overlay view shows your connection to devices, and the underlay shows connection to Airwall Gateways that manage secure connections to the devices.
- On v2.2.12 and earlier, check:
  - Under **Profile**, the correct profile is active.
  - The slider next to the profile is to the right and green
  - Under **Status**, both **Connected to Conductor** and **Connected to Devices** are blue checks.

  This example shows that you're connected to the Conductor, but not yet connected to Devices.

  Airwall

  PROFILE

  RemoteAccess

  STATUS

  Connected to Conductor ✓

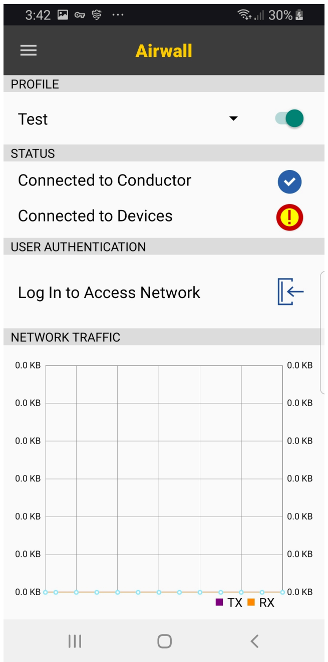
  Connected to Devices ●

  NETWORK TRAFFIC

-

In v2.2.12 and earlier, here are some other statuses you may see:

- **Red check**: You can reach the Conductor, but your administrator has not yet accepted your request to connect.
- **Grey dot**: No connection, or not connected.
- **Red exclamation point**: You need to log in. Tap the exclamation point, or under User Authentication, tap the Log in icon to log in.



3:42 30%

Airwall

PROFILE

Test

STATUS

Connected to Conductor ✓

Connected to Devices !

USER AUTHENTICATION

Log In to Access Network

NETWORK TRAFFIC

Disconnect from the Airwall secure network

- **v3.0 and later** – Open the Android Airwall Agent, and tap **DISCONNECT**.
- **v2.2.12 and earlier** – Open the Android Airwall Agent, and under **Profile**, tap the slider to slide to the left to disconnect.

Connect with a Linux Airwall Server

You manage your Linux Airwall Server profiles and connections on the command line using Airshell (`airsh`). You can currently substitute `airctl` for `airsh` in most of these commands, but `airctl` will be phased out in a future release.

In addition to the commands below, you can enter `sudo airsh help tree` to see available commands. Not all Airshell commands are supported on a Linux Airwall Server. See Linux Airwall Server Airshell commands on page 372.

Connect and Disconnect from the Airwall secure network

- To connect to the active profile, enter:

```
sudo airsh service start
```

- To disconnect, enter:

```
sudo airsh service stop
```

- If the service is already started, restart by entering:

```
sudo airsh service restart
```

Manage Profiles

- **To create a new profile**, run: `sudo airsh profile create name=<new profile name> conductor=<conductor_url> [act=<activation_code>]`
- **To switch profiles**, run: `sudo airsh profile activate <profile name or number>`
- **To edit an existing profile**, run: `sudo airsh profile modify <profile name or number> [name=<new_name>] [conductor=<conductor_url>] [act=<activation_code>] [log_level=<info | warn | error | debug | trace>]`
- **To delete a profile**, run: `sudo airsh profile delete <profile name or number>`

Find your device ID

If you are still not connected, you may need to provide your device ID to the administrator for your Airwall secure network. To get your device ID, enter:

```
sudo airsh profile list verbose <profile_name>
```

Check your Connection

To check your connection, enter:

```
sudo airsh status
```

Check your WiFi connection

To check your WiFi connection (when a WiFi NIC is available), enter:

```
sudo airsh status wifi
```

Follow the log to troubleshoot your Linux Airwall Server

To watch the log file, enter:

```
sudo airsh log follow
```

Connect with a Windows Airwall Agent or Server

How to connect to an Airwall secure network with a Windows Airwall Agent or Server.

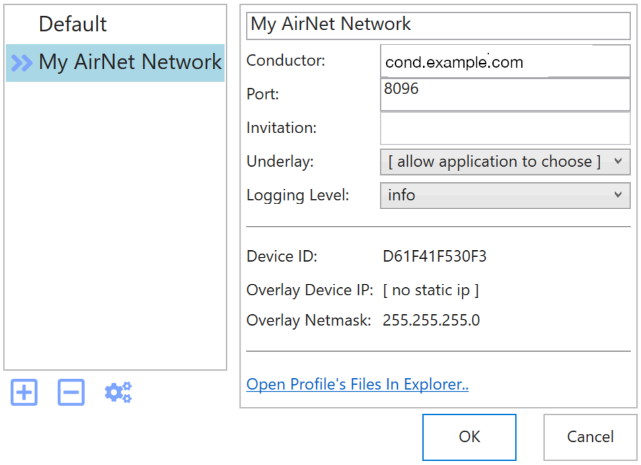
Connect to the Airwall secure network

Open the Airwall Agent or Server. If it does not connect automatically, on the Windows taskbar, right-click the Tempered icon, and select **Start**.

Manage Profiles

-
  - **To create a new profile**, from the Control Panel, click the gear ⚙, and click + to add a new profile.
  - **To edit an existing profile**, from the Control Panel, click the gear, and select a profile to edit it.
  - **To switch profiles**:

    1. From the Control Panel, click the gear. (You can also right-click the Airwall Agent icon, and select **Configure**.)
    2. On the **Configure** page, if the profile you want has the double arrows » to the left, it's already the Active profile. If it doesn't, select the profile you want to use.
    3. Click the gears icon ⚙ below the profile list, and choose **Make profile active**.
    4. Select **OK**. The Agent disconnects and then connects with the new profile. This can take a few minutes.
  - **To delete a profile**, select it and click -.



Default
My AirNet Network

My AirNet Network

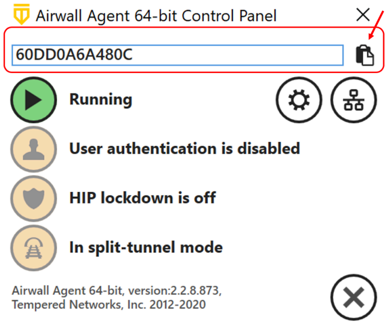
Conductor: cond.example.com
Port: 8096
Invitation:
Underlay: [allow application to choose]
Logging Level: info

Device ID: D61F41F530F3
Overlay Device IP: [no static ip]
Overlay Netmask: 255.255.255.0

Open Profile's Files In Explorer..

Find your device ID

If you are still not connected, you may need to provide your device ID to the administrator for your Airwall secure network. You can find and copy it from the top of the **Airwall Agent/Server Control panel**. Click the icon on the right to copy the device ID:



Airwall Agent 64-bit Control Panel

60DD0A6A480C

Running

User authentication is disabled

HIP lockdown is off

In split-tunnel mode

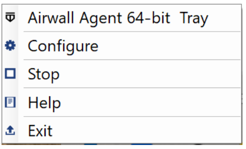
Airwall Agent 64-bit, version:2.2.8.873,
Tempered Networks, Inc. 2012-2020

Check your Connection

1. Open the Airwall Agent or Server.
2. At the top, you will see either **Stopped** or **Running**.
   a) If it is **Stopped**, the profile is still loading and connecting.
   b) If it is **Running**, the profile is running, but not necessarily connected.
3. When it says **Running**, just to the right, select the overlay icon 🖧.
4. Under **Conductor and Authentication**, check to see your connection status next to **Conductor**. If you are connected, it has a green dot and says **Connected**.
5. You can also see the resources this profile gives you access to under **Network Policies and Peer Devices**:
   a) To see the devices you have access to, open the **Overlays** tab.
   b) To see the **Airwalls** you have access to, open the **Underlay** tab.
6. To refresh the list, select **Ping opened network**.

Disconnect from the Airwall secure network

Right-click the Airwall Agent icon, and select **Stop**.



Create or Edit Airwall Agent or Server Profiles

How you configure your Airwall Agent or Server profile varies by which version you have installed.

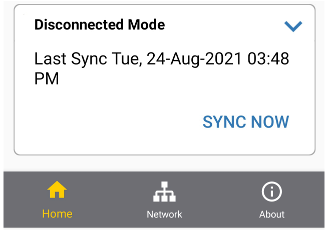
Go to Connect to an Airwall secure network on page 19 and select your platform to get information on creating and editing profiles, as well as connecting and disconnecting to an Airwall secure network using your Airwall Agent or Server.

Sync an Airwall Agent or Server in Disconnected Mode

If your Airwall secure network administrator has set your Airwall Agent or Server to Disconnected Mode, it will synchronize with the Conductor at regular intervals, and should not affect your connection to the resources you need to access on the Airwall secure network. If you are having issues, you can manually sync with the Conductor.

Sync Now for iOS, Android, macOS, and Windows Airwall Agents and Servers

- **For mobile Airwall Agents** – Open your mobile agent, and on the Home page, under **Disconnected Mode**, select **Sync Now**.

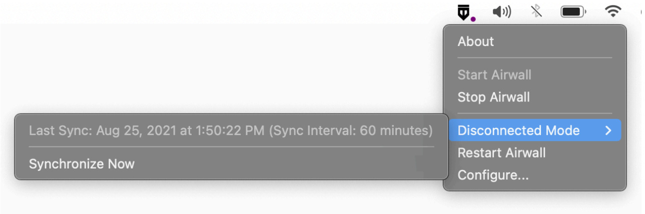


Disconnected Mode

Last Sync Tue, 24-Aug-2021 03:48 PM

Figure 1: iOS and Android Airwall Agent Sync Now

- **For desktop agents** – Open the Airwall Agent or Server menu by clicking the icon, hover over **Disconnected Mode** and select **Synchronize Now**.



Last Sync: Aug 25, 2021 at 1:50:22 PM (Sync Interval: 60 minutes)

Figure 2: macOS Sync Now

Note: If you do not have the Disconnected Mode pane on your home page, your Airwall Agent or Server is not in Disconnected mode. For assistance troubleshooting your connection, see I am having trouble connecting on page 31 or contact your Airwall secure network administrator.

Sync Now for Linux Airwall Servers

If you need to manually sync your Airwall Server with the Conductor, open Airshell and enter the `conductor sync` command:

1. Make sure the Linux Airwall Server is started:

```
sudo systemctl start airwall
```

2. Get into Airshell:

```
sudo airsh
```

3. Check your connection status:

   ```
   airsh>> status conductor
   ```

   you will see Disconnected mode is on and the interval it is set to automatically reconnect:

   ```
   Connection status:  Disconnected
   Disconnected mode:  on
   Reconnect interval (minutes): 60
   Airwall Device ID:  C9234588172
   ```

   Note: If Disconnected mode shows as `off`, your Airwall Server is not in Disconnected mode. For assistance troubleshooting your connection, see I am having trouble connecting on page 31 or contact your Airwall secure network administrator.

4. Manually sync with the Conductor:

   ```
   airsh>> conductor sync
   ```

Your Linux Airwall Server reconnects to the Conductor and updates any configuration or trust policy changes since the last sync, then disconnects again.

See also: Linux Airwall Server Airshell commands on page 372

Change My Conductor Preferences

Change your Conductor password, theme and other options from your Preferences page.

1. Log in to the Conductor with your existing password.
2. Select the profile icon 👤.

   Note: You can toggle Dark mode on or off.

3. Select **Preferences** to open your Preferences page.
4. Scroll down to change these settings (depending on your role and permissions):
   - **API access** – Select New token to get a new access token.
   - **Show progress on dashboard** – Toggle to show or hide the Dashboard Setup progress bar
   - **Default overlay networks to advanced view** – Toggle to switch between simplified and advanced view on the Overlay networks page.
5. Depending on your role and permissions, you can also change your contact details or Alert email trigger level. Select **Edit Settings**, make your changes, then select **Update Settings**.

Change my Conductor password

You may need to change the password you use to log in to the Conductor.

1. Log in to the Conductor with your existing password.
2. Select the profile icon 👤, and then select **Preferences**.
3. Under **Preferences**, click **Edit Settings**.
4. Scroll down to **Change your password**, and enter your current password. Then enter and confirm your new password, or click **Generate** to generate a password and copy it to the clipboard.
5. Select **Update Settings**.

Be sure to save your new password in a secure place.

I am having trouble connecting

Here's help for issues connecting to an Airwall secure network.

My agent or server is in disconnected mode

Normally, Disconnected mode will not affect your ability to access resources on the Airwall secure network. If you are having issues, you can manually sync with the Conductor. See Sync an Airwall Agent or Server in Disconnected Mode on page 29.

Cannot connect to a website even though I am authenticated.

If you cannot connect to a website you should be able to connect to, try:

- Making sure the web URL starts with https://.
- Check that you have access to the Internet. If you do not, your administrator may need to configure a DNS server on their end for you to access the Internet.
- If you have more than one profile, make sure the one that gives you access to that resource is active.

My Windows Airwall Agent will not connect when multiple interfaces are active

This issue can be caused by a Windows default that does not allow multiple simultaneous active network interfaces, and prefers ethernet over cellular or WiFi.

To bypass the default and have Windows keep multiple interfaces open, you edit the `fMinimizeConnections` registry value:

1. Hold the Windows Key down and press the R key.
2. In the **Run** dialog, type `regedit` and click **OK**.
3. Navigate to the following path in Registry Editor: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WcmSvc\
4. See if the `GroupPolicy` subkey exists.
    - If it exists, check that the `fMinimizeConnections` value is 0.
    - If it does not exist, create it: Highlight **WcmSvc**, right click on **WcmSvc**, and select **New**, then select **Key**. Name the new key `GroupPolicy`. Right-click `GroupPolicy` and select **New**, select **DWORD (32-bit)**, and then select **Create value**. Name the value `fMinimizeConnections` and click **OK**. Check that the value is 0 (for false).
5. Reboot and test to see if the connection works over all network interfaces.

Linux Airwall Server or macOS Airwall Agent interface selection

The Linux Airwall Server and macOS Airwall Agent implement an interface auto-selection method. When you first install the Airwall Agent or Server, Linux or macOS determines the default gateway of the host and uses the associated network interface.

Note: Auto-selection is per profile.

Troubleshooting

If your macOS Airwall Agent is reporting as *online*, but does not seem to be working, check that the correct network interface is selected in the profile. See Set your preferred network in the macOS Airwall Agent (HIPclient-OSX) on page 80.

From Tkee: Linux agent conforms to the Gateway link manager operational rules. airsh currently does not have the ability to select the preferred uplink. Conductor is the method for selecting interfaces by port group weights. Short on details, the Gateway documentation might serve as a basis. Ticket to fill this in CD-412.

Manage Airwall™

Monitor, Maintain, Provision, Control Access

The Conductor Dashboard

The Conductor Dashboard gives you a quick view into the health and state of your Airwall secure network, showing you activity and alerting across the entire network.

With the Dashboard, you can, depending on your permissions:

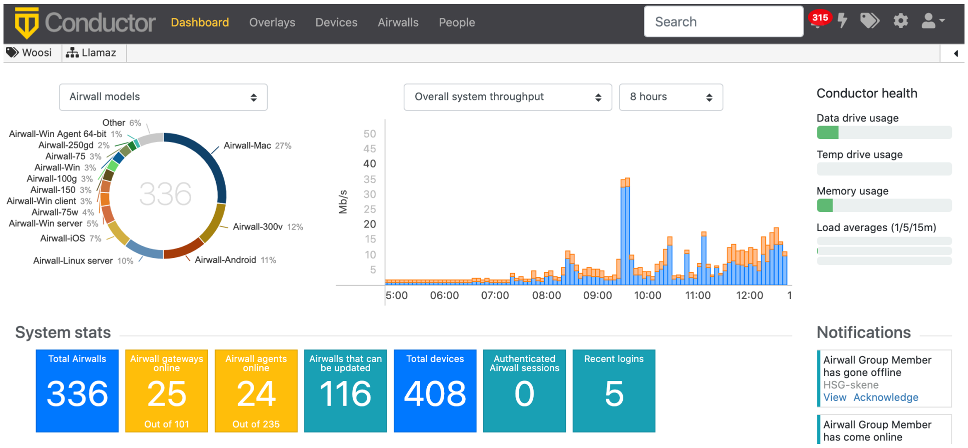
- See the state of the overlay networks that make up your Airwall secure network.
- See activity without needing management rights.
- Manage Airwall Edge Services and troubleshoot connection issues.
- Monitor the health of your network.
- See at a glance changes within the system.

View network status

See the models and versions of Airwall Edge Services, and the overall system throughput for up to the last 24 hours.

The System stats are tiles that show at a glance how many Airwall Gateways and Airwall Agents and Servers are online, how many can be updated, and other useful information.

Click a stat tile to show more details in the Navigation pane below. For example, click **Airwall agents online** to see a list of the Airwall Agents and Servers that are online below.



System stats

Total Airwalls	Airwall gateways online	Airwall agents online	Airwalls that can be updated	Total devices	Authenticated Airwall sessions	Recent logins
336	25 Out of 101	24 Out of 235	116	408	0	5

Notifications

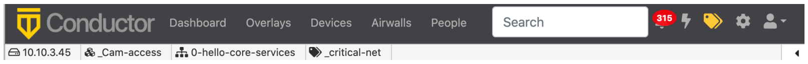
Airwall Group Member has gone offline
HSG-skene
View Acknowledge

Airwall Group Member has come online

Pin pages and Recently Viewed lists for quick access

Right under the menu bar, you will now find a pin bar, where you can pin up to 20 pages you visit frequently to quickly get back them. You can click the arrow on the right to see and pin **Recently viewed** items. On most pages, you can also click the pin icon to add the page to your pin bar. Click it again to remove the pin.

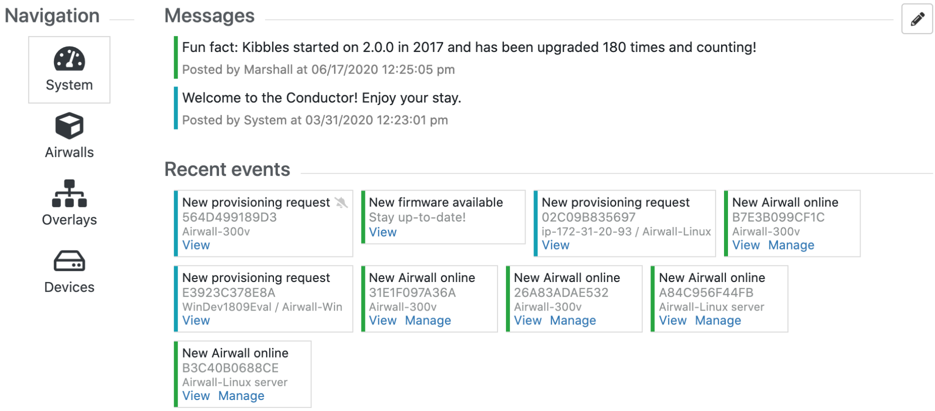
Note: To pin a device, open the device page, and then go to recently-viewed items to pin.



Navigation – System

The System navigation screen shows Messages from admins and firmware updates from Tempered, as well as recent events, such as provisioning requests and firmware updates. You can also see or create messages for other Conductor or network admins.

- To create a message, select the pencil icon. For more details, see Create or Manage Dashboard Messages on page 38.
- Under **Recent events**, select **View** on items to jump right to the page, or select **Manage** to manage and name without leaving the dashboard.



Messages

Fun fact: Kibbles started on 2.0.0 in 2017 and has been upgraded 180 times and counting!
Posted by Marshall at 06/17/2020 12:25:05 pm

Welcome to the Conductor! Enjoy your stay.
Posted by System at 03/31/2020 12:23:01 pm

Recent events

New provisioning request
564D499189D3
Airwall-300v
View

New firmware available
Stay up-to-date!
View

New provisioning request
02C09B835697
ip-172-31-20-93 / Airwall-Linux
View

New Airwall online
B7E3B099CF1C
Airwall-300v
View Manage

New provisioning request
E3923C378E8A
WinDev1809Eval / Airwall-Win
View

New Airwall online
31E1F097A36A
Airwall-300v
View Manage

New Airwall online
26A83ADAE532
Airwall-300v
View Manage

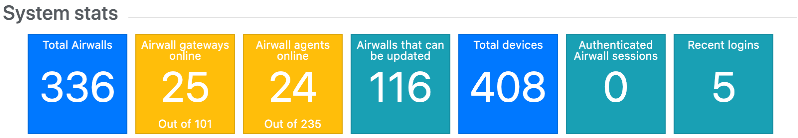
New Airwall online
A84C956F44FB
Airwall-Linux server
View Manage

New Airwall online
B3C40B0688CE
Airwall-Linux server
View Manage

Navigation – Airwalls

Here is what you can do on the **Airwalls** navigation page:

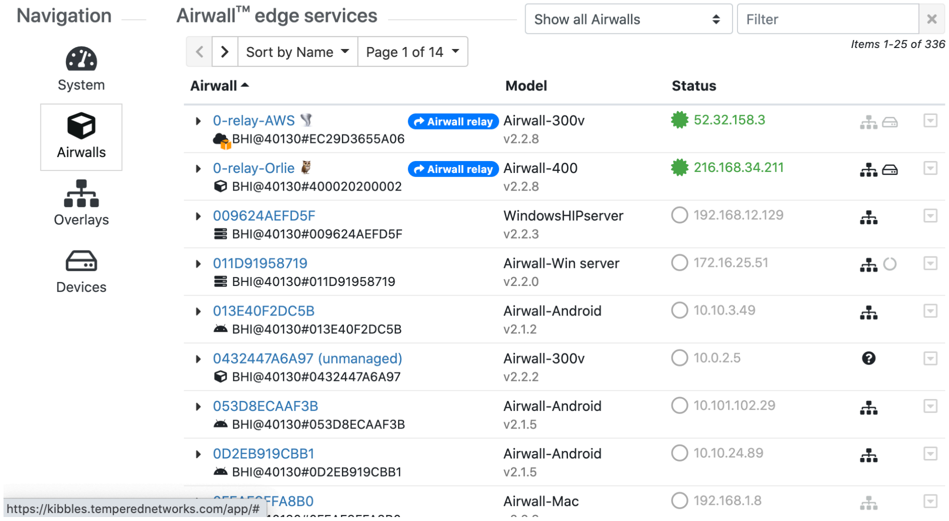
- Select an Airwall Edge Service name to open it.
- Click one of the Airwall **System stats** tiles to see the details.



System stats

Total Airwalls 336
Airwall gateways online 25 Out of 101
Airwall agents online 24 Out of 235
Airwalls that can be updated 116
Total devices 408
Authenticated Airwall sessions 0
Recent logins 5

- Filter which Airwall Edge Services you see:
  - In the **Show all Airwalls** box, select an Airwall status (such as offline or unmanaged) to view.
  - Type in the **Filter** box to filter on name or model, or other aspects of the Airwall Edge Services, like Tags.



Airwall™ edge services

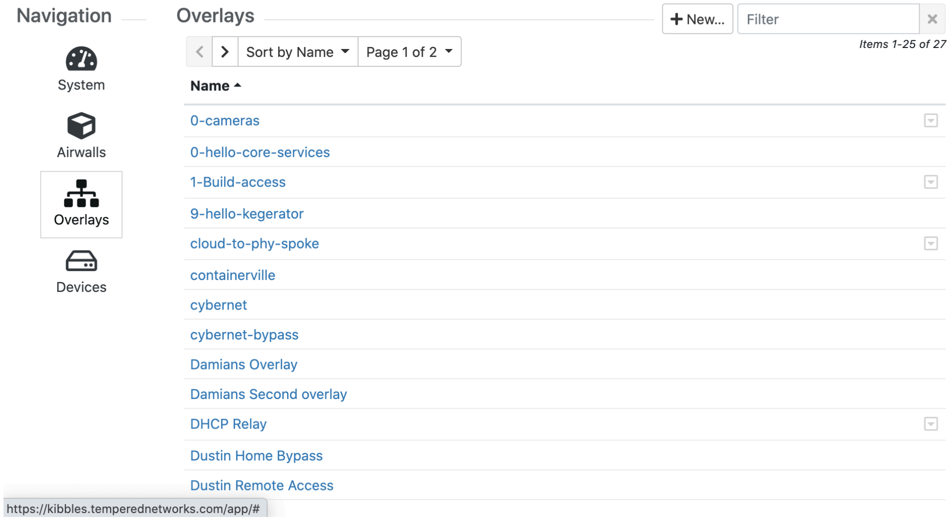
Items 1-25 of 336

Airwall ▴		Model	Status
0-relay-AWS BHI@40130#EC29D3655A06	Airwall relay	Airwall-300v v2.2.8	52.32.158.3
0-relay-Orlie BHI@40130#400020200002	Airwall relay	Airwall-400 v2.2.8	216.168.34.211
009624AEFD5F BHI@40130#009624AEFD5F		WindowsHIPserver v2.2.3	○ 192.168.12.129
011D91958719 BHI@40130#011D91958719		Airwall-Win server v2.2.0	○ 172.16.25.51
013E40F2DC5B BHI@40130#013E40F2DC5B		Airwall-Android v2.1.2	○ 10.10.3.49
0432447A6A97 (unmanaged) BHI@40130#0432447A6A97		Airwall-300v v2.2.2	○ 10.0.2.5
053D8ECAAF3B BHI@40130#053D8ECAAF3B		Airwall-Android v2.1.5	○ 10.101.102.29
0D2EB919CBB1 BHI@40130#0D2EB919CBB1		Airwall-Android v2.1.5	○ 10.10.24.89
FFA8B0		Airwall-Mac	○ 192.168.1.8

Navigation – Overlays

Here is what you can do on the Overlays navigation page:

- Select **New** to create a new Overlay. For more details, see Create an overlay network on page 418.
- Type in the **Filter** box to filter by **Name**.
- Select the drop-down menu to edit, tag, or disable the Overlay.
- Select an Overlay name to open it.



Overlays

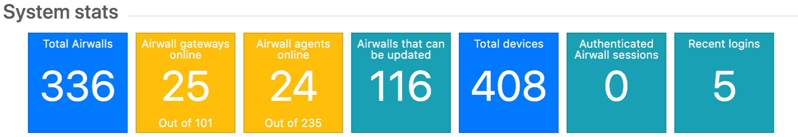
Items 1-25 of 27

Name ▴
0-cameras
0-hello-core-services
1-Build-access
9-hello-kegerator
cloud-to-phy-spoke
containerville
cybernet
cybernet-bypass
Damians Overlay
Damians Second overlay
DHCP Relay
Dustin Home Bypass
Dustin Remote Access

Navigation – Devices

Here's what you can do on the **Devices** navigation page:

- Select a device to go to that device.
- Click the **Total Devices System stats** tile to open the **Devices** navigation page.

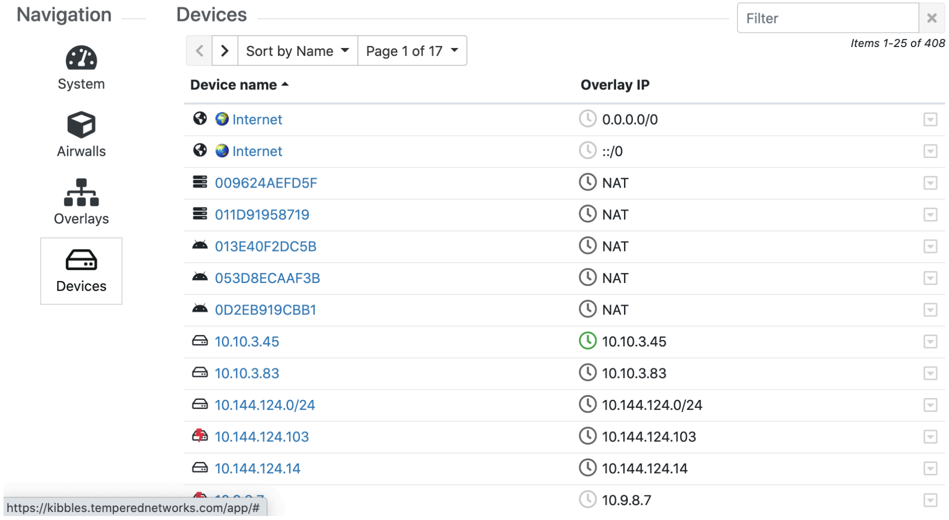


System stats

Total Airwalls	Airwall gateways online	Airwall agents online	Airwalls that can be updated	Total devices	Authenticated Airwall sessions	Recent logins
336	25 Out of 101	24 Out of 235	116	408	0	5

- Filter which **Devices** you see:

- Select the **Sort by** box to sort the devices.
- Type in the **Filter** box to filter by **Device name** or **Overlay IP**, among other things.

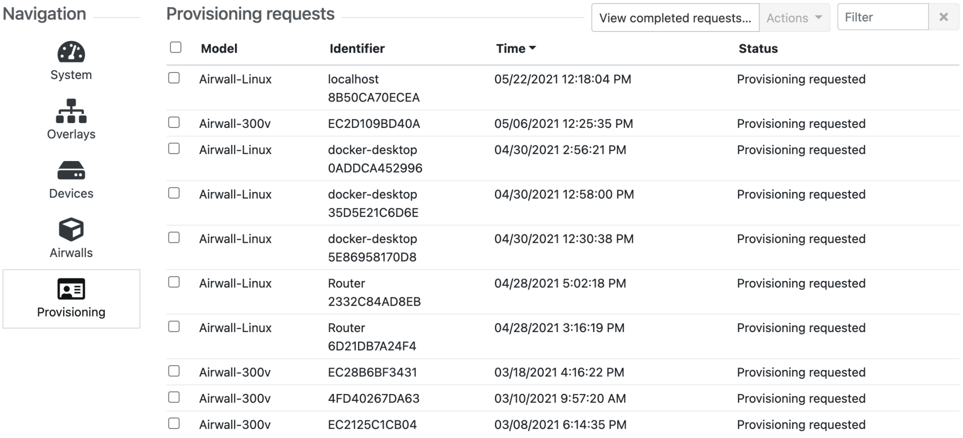


Device name ▴	Overlay IP
Internet	0.0.0.0/0
Internet	::/0
009624AEFD5F	NAT
011D91958719	NAT
013E40F2DC5B	NAT
053D8ECAAF3B	NAT
0D2EB919CBB1	NAT
10.10.3.45	10.10.3.45
10.10.3.83	10.10.3.83
10.144.124.0/24	10.144.124.0/24
10.144.124.103	10.144.124.103
10.144.124.14	10.144.124.14
	10.9.8.7

Navigation – Provisioning

The **Provisioning** page gives you a quick way to see what Airwall Edge Services need to be managed and quickly handle these provisioning requests. You can:

- Select one or more Airwall Edge Services and grant or deny the provisioning requests. Check next to the Airwall Edge Services, then from the **Actions** menu, select **Grant request** or **Deny request**.
- Filter which Airwall Edge Services you see:
  - Sort the Airwall Edge Services by any column by clicking on the column .
  - Type in the **Filter** box to filter by **Model** or **Identifier**, or other things.



☐	Model	Identifier	Time ▾	Status
☐	Airwall-Linux	localhost 8B50CA70ECEA	05/22/2021 12:18:04 PM	Provisioning requested
☐	Airwall-300v	EC2D109BD40A	05/06/2021 12:25:35 PM	Provisioning requested
☐	Airwall-Linux	docker-desktop 0ADDCA452996	04/30/2021 2:56:21 PM	Provisioning requested
☐	Airwall-Linux	docker-desktop 35D5E21C6D6E	04/30/2021 12:58:00 PM	Provisioning requested
☐	Airwall-Linux	docker-desktop 5E86958170D8	04/30/2021 12:30:38 PM	Provisioning requested
☐	Airwall-Linux	Router 2332C84AD8EB	04/28/2021 5:02:18 PM	Provisioning requested
☐	Airwall-Linux	Router 6D21DB7A24F4	04/28/2021 3:16:19 PM	Provisioning requested
☐	Airwall-300v	EC28B6BF3431	03/18/2021 4:16:22 PM	Provisioning requested
☐	Airwall-300v	4FD40267DA63	03/10/2021 9:57:20 AM	Provisioning requested
☐	Airwall-300v	EC2125C1CB04	03/08/2021 6:14:35 PM	Provisioning requested

Conductor Icon Reference

A reference for the icons you will see used in the Conductor.

Type	Icon	Meaning
Common		
	⟳	Refresh

	✎	Edit
	🗑	Delete
	📌, 📌	Click to Pin to top bar, Pinned to top bar. Click to unpin.
Dashboard		
	🌐	Bypass destination
	⏲	System
	📦	Airwalls
	🖧	Overlays
	🖴	Devices
People		
	👥	People group
	👤	Authenticated user
	🔌	Has an unused activation code. If grayed out, activation code has expired.
		People statuses
	🕒	Last 24 hrs
	🕒	Last week
	🕒	Longer than a week
	🕒	Never
Agents & Servers		
	🤖	Android Airwall Agent
	🍎	macOS or iOS Airwall Agent
	⊞	Windows Airwall Agent
	🗄	Airwall server
Overlays		
	⛓	Disable network communications disabled

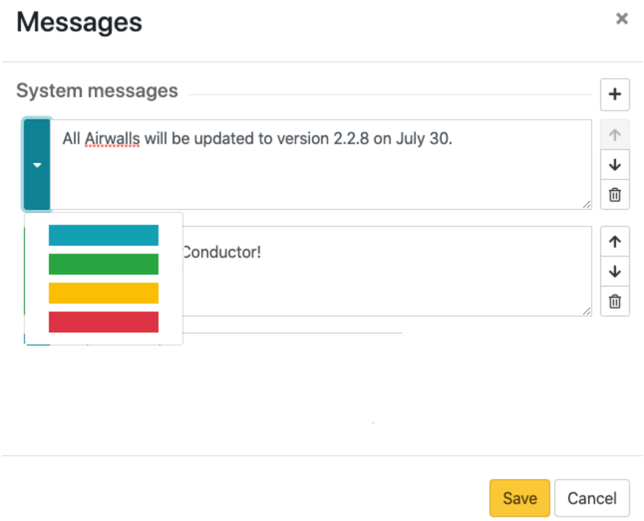
	🔗	Enable network communications
	🔓	Enable transparent mode
	🔒	Enable protected mode
	🕒 🕒 🕒	Device statuses (on Overlay page)
Airwalls		
	📦	Airwall
	☁	Cloud Airwall - the overlaid icon indicates which type. In this case, AWS (Amazon Web Services).
	📦	Airwall or Device group
	✹	Ethernet Airwall
	📶	Cellular Airwall
	🛜	Wifi Airwall
	❓	Unmanaged
	◌	Not authenticated
	○	Offline
	🚫	Revoked
		Icons superimposed on other icons to indicate which type of server, virtual, or cloud Airwall: Rackspace, VMware, Openstack, AWS, Azure, HyperV, Xen, Google, Alibaba Cloud
	🔒	Mac Lockdown
Devices and Device Groups		
	🖴	Device
	🖴	Discovered device (not yet accepted)
	📦	Device or Airwall group

	🎓	Smart device group
	🪄	Recompute disabled on this Smart Device Group, and there are devices that would be in this group. Click the action menu to recompute the devices added using the rules.
Alerts and monitoring	❓	Disabled on alert line
	⏹	Disabled on menu
	🔔	Alerts
	⚡	Event Monitors
	🏷	Tags
	⚙	Conductor Settings
	👤	User Profile
Settings		
	⬇	Download
	🛠	Install
	❗	Licensing Provisioning Request

Create or Manage Dashboard Messages

Create messages that appear on the Conductor Dashboard to notify other administrators about upcoming firmware updates or other events that other administrators need to know about.

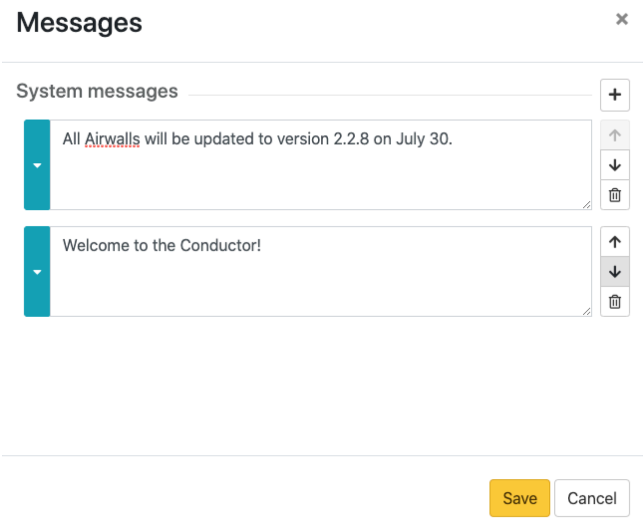
1. On the Conductor Dashboard, scroll down to the Navigation section, and open the System pane.
2. Select the pencil icon in the upper right of the pane to create or manage messages.
3. In Messages, to create a new message, select the + and write your message.
4. Select the color drop-down on the left to select the color of the message bar. Your organization can decide how to classify messages. Here is a starting point:
   - Blue: Informational messages
   - Green: Resolved or managed events
   - Yellow: Warnings about non-blocking system issues
   - Red: Blocking system issues, downtime, or outages



All Airwalls will be updated to version 2.2.8 on July 30.

Conductor!

5. Use the side arrows or trash can to reorder or remove existing messages. as needed. If you do not rearrange them, messages are displayed with the latest messages at the top.



All Airwalls will be updated to version 2.2.8 on July 30.

Welcome to the Conductor!

6. Select **Save**.

Change My Conductor Preferences

Change your Conductor password, theme and other options from your Preferences page.

1. Log in to the Conductor with your existing password.
2. Select the profile icon .

   Note: You can toggle Dark mode on or off.

3. Select **Preferences** to open your Preferences page.
4. Scroll down to change these settings (depending on your role and permissions):

   - **API access** – Select New token to get a new access token.
   - **Show progress on dashboard** – Toggle to show or hide the Dashboard Setup progress bar

- **Default overlay networks to advanced view** – Toggle to switch between simplified and advanced view on the Overlay networks page.

5. Depending on your role and permissions, you can also change your contact details or Alert email trigger level. Select **Edit Settings**, make your changes, then select **Update Settings**.

Change my Conductor password

You may need to change the password you use to log in to the Conductor.

1. Log in to the Conductor with your existing password.
2. Select the profile icon 👤, and then select **Preferences**.
3. Under **Preferences**, click **Edit Settings**.
4. Scroll down to **Change your password**, and enter your current password. Then enter and confirm your new password, or click **Generate** to generate a password and copy it to the clipboard.
5. Select **Update Settings**.

Be sure to save your new password in a secure place.

Show or Hide Conductor Setup progress

You can show or hide the Conductor Setup progress bar on the Dashboard in your user preferences.

1. Log in to the Conductor with your existing password.
2. Select the profile icon 👤, and then select **Preferences**.
3. Scroll down to **Show progress on dashboard**, and toggle it on or off.

For more information on the Conductor tutorials, see Get Started using Conductor Help and Tutorials on page 140.

Customize the Conductor

You can customize the Conductor login screen and emails sent from the Conductor for your business.

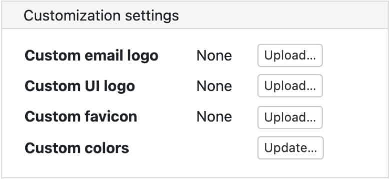
Here's what you can customize:

- **Conductor** login screen – Add your company logo, and change the background colors and favicon.
- **Conductor emails** – Add your company logo and change the text color. You can also customize the subject line and add a note from the administrator when sending Airwall Invitations.

Keep reading for more details and examples.

Customize the Conductor Login page

1. Go to **Settings** > **Customization settings**.

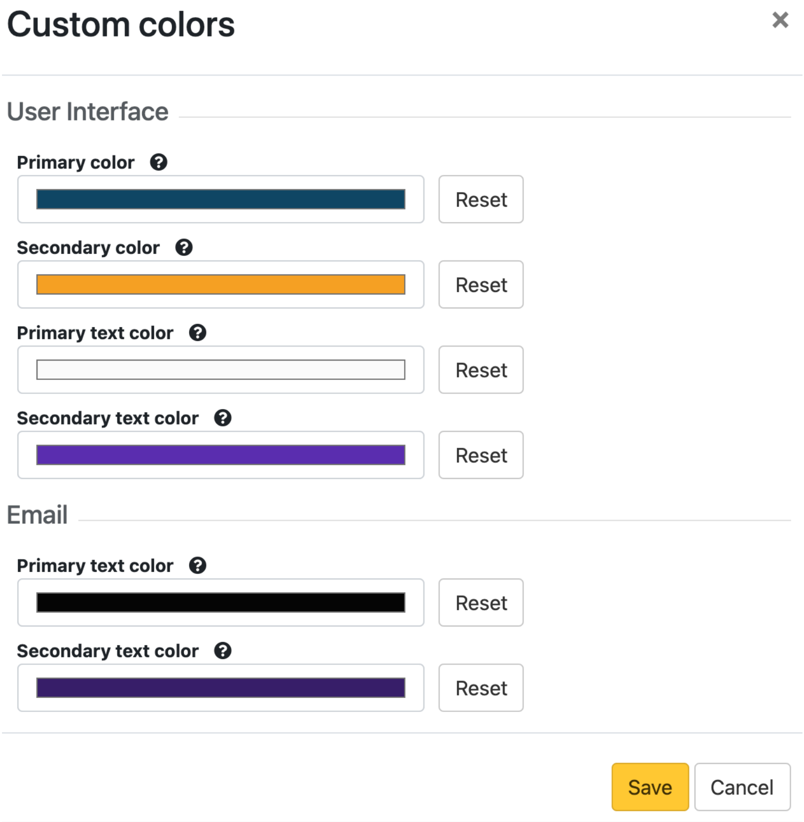


Customization settings

Custom email logo	None	Upload...
Custom UI logo	None	Upload...
Custom favicon	None	Upload...
Custom colors		Update...

2. Under **Custom UI logo**, select **Upload**, select **Choose File**, and choose the logo you'd like to appear on the login page, then select **Upload**.
3. Under **Custom favicon**, select **Upload**, select **Choose File**, and choose the favicon you'd like to appear on your web browser tab, and then select **Upload**.

4. Under **Custom colors**, select **Update**, and under User Interface, select the colors you'd like to use on the Conductor login page, and then select **Save**.



Custom colors

User Interface

Primary color

Secondary color

Primary text color

Secondary text color

Email

Primary text color

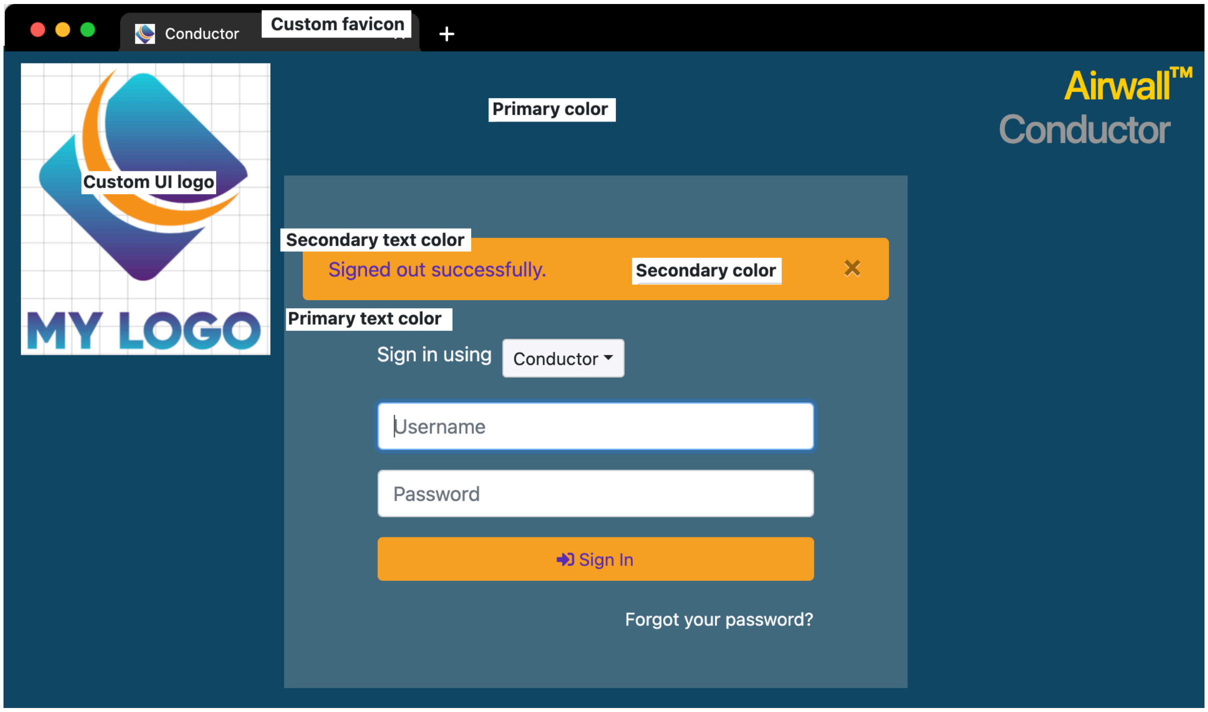
Secondary text color

5. Refresh your browser window to see the favicon change. Log out to see your login page changes.

Now the Conductor login page will use your customizations.

Example

Here is an example of what the Conductor login page looks like with a custom logo, favicon, and colors, showing how your selections will map to the page:



Customize Conductor emails

Customize the emails sent by the Conductor to reflect your company's branding.

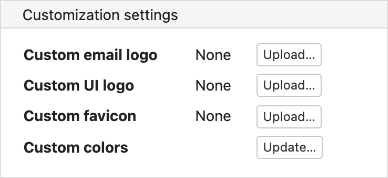
Before you Begin

Before you can customize the emails, you need to:

- Set up your email settings in the Conductor. To do this, see Configure Email Settings on page 238.
- Make sure the size of the logo and icon files you want to use are 10MB or less.

Customize emails

1. Go to **Settings** > **Customization settings**.



Customization settings

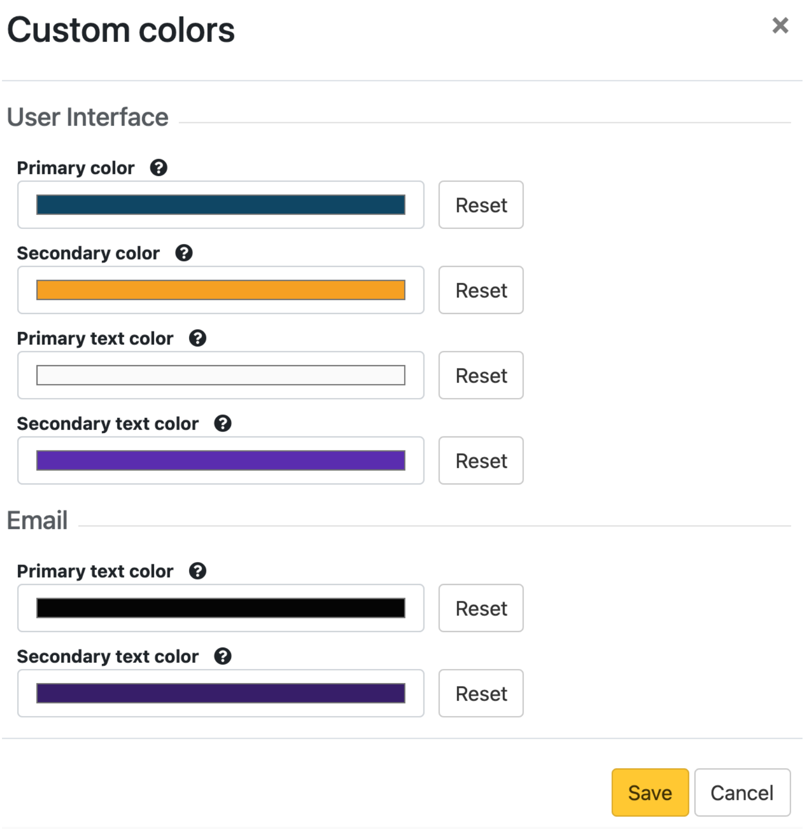
Custom email logo	None	Upload...
Custom UI logo	None	Upload...
Custom favicon	None	Upload...
Custom colors		Update...

Note: If you cannot see all of these options, make sure you've set up your email settings in the Conductor. See Configure Email Settings on page 238.

2. Next to **Custom email logo**, select **Upload**, select **Choose File**, and choose the logo you'd like to appear in emails from the Conductor, and then select **Upload**.

Tip: Allowed image types are .png, .jpg, .jpeg, and recommended sizes are, in pixels: 200x60, 400x120, 800x240, 1600x480.

3. Next to **Custom colors**, select **Update**, and under **Email**, select the primary and secondary text colors you'd like to use in emails from the Conductor, and then select **Save**.



Custom colors

User Interface

Primary color

Reset

Secondary color

Reset

Primary text color

Reset

Secondary text color

Reset

Email

Primary text color

Reset

Secondary text color

Reset

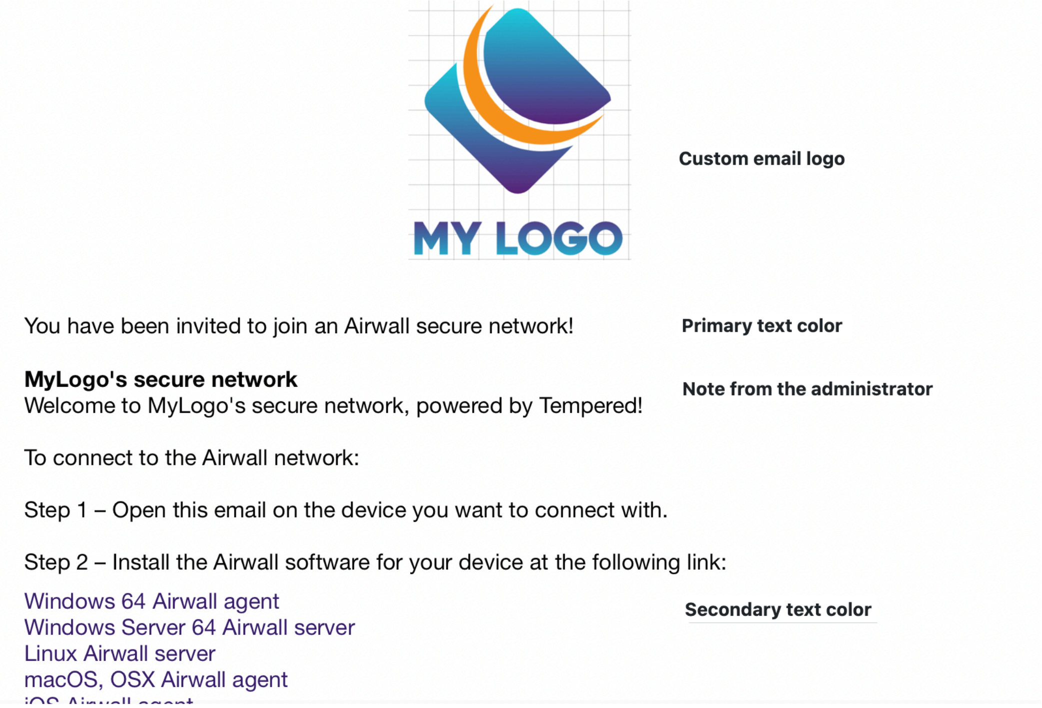
Save Cancel

4. When you create Airwall Invitations, you can also customize the subject of the email and add a note from the administrator to the top of the email. For more information, see Connect People's Devices with Airwall Invitations on page 64.

Now all emails you send from the Conductor will use your customizations.

Example

Here is an example of what emails from the Conductor look like with a custom logo and custom text colors, showing how your selections will map to the emails:



You have been invited to join an Airwall secure network!

MyLogo's secure network
Welcome to MyLogo's secure network, powered by Tempered!

To connect to the Airwall network:

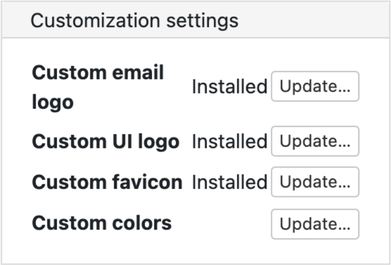
Step 1 – Open this email on the device you want to connect with.

Step 2 – Install the Airwall software for your device at the following link:

Windows 64 Airwall agent
Windows Server 64 Airwall server
Linux Airwall server
macOS, OSX Airwall agent
iOS Airwall agent

Remove Conductor customizations

1. Go to **Settings** > **Customization settings**.



Customization settings

Custom email logo	Installed	Update...
Custom UI logo	Installed	Update...
Custom favicon	Installed	Update...
Custom colors		Update...

2. **To reset logos and favicons** – Next to **Custom email logo**,**Custom UI logo**, and **Custom favicon**, select **Update**, and then select **Remove**.
3. **To reset colors** – Next to **Custom colors**, select **Update**, and then select **Reset** for any color you'd like to remove.
4. Refresh the browser window to see your changes.

Search in the Conductor

The Conductor supports searching by full text search or by expressions using the Conductor Query Language. Searching by expression is available in the search boxes on the **Overlays**, **Devices**, **Airwalls**, **People**, and **Dashboard** pages. Search results show in real time as you add search terms or expressions.

Supported versions	Search by expression is supported in v3.1.0 and later Conductors

- **To search by expression**: Select the gear icon , and click in the **Filter** box to see available query options and logical operators. This search method uses the Conductor Query Language. For more details, see Search by Expression with the Conductor Query Language on page 45.

- **To do a full text search**: Select the pencil icon and enter your search terms in the **Filter** box.

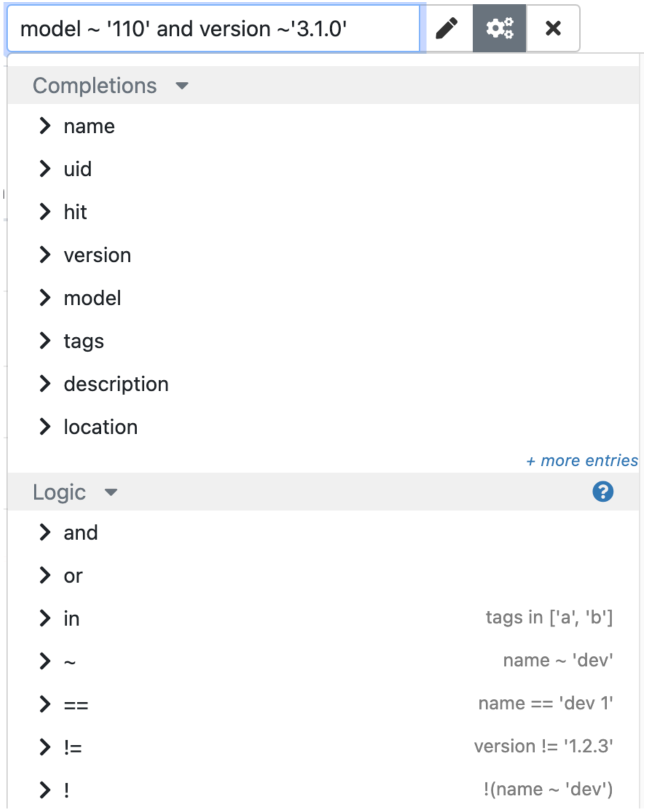
Tip: Both methods of searching work with the drop-down **Show all ...** filters. So if you select **Offline** under **Show all Airwalls**, your expression or full-text search only searches for Offline Airwall Edge Services.

Search by Expression with the Conductor Query Language

Supported versions	Search by expression is supported in v3.1.0 and later Conductors

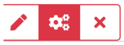
1. Select the gear icon .
2. Click in the **Filter** box to see available query options and logical operators for the page you're on.

   This help includes query options and states that you can search on under Completions, and logical operators under Logic. As you type, it filters on your entry to assist you in finding the syntax you're looking for.



model ~ '110' and version ~'3.1.0'

Note: If the expression is not supported, the gear icon turns red to assist you in correcting the syntax.



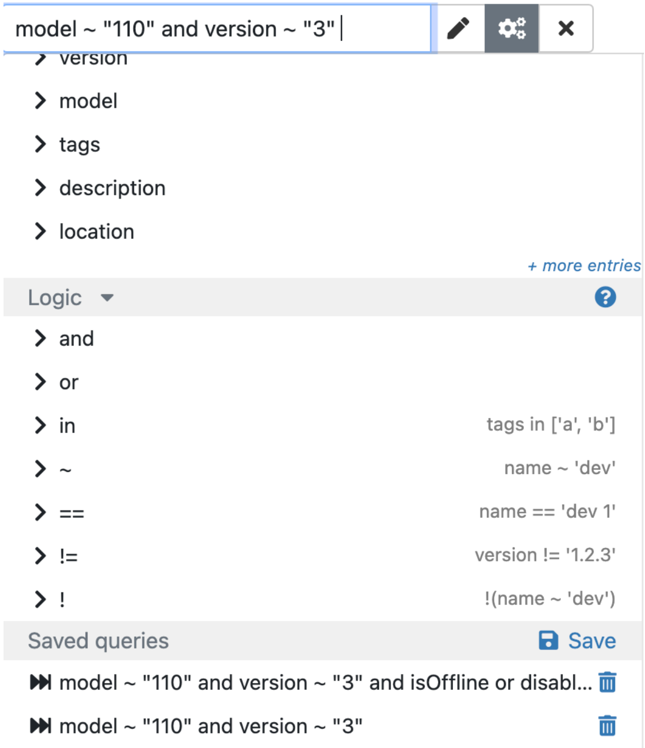
3. Add query options and logic operators to your query by selecting them from the drop down help, or type them into the **Filter** box. The query filters your results in real time as you enter expressions.

   Note: Enclose literal values in your queries in either double or single quotes. The usual Javascript escape rules apply. For example, use "\"" to match an inner double quote.

   For descriptions of the query options for the page you're on, see:

   - Overlays Query Options on page 48
   - Devices Query options on page 49
   - Airwalls Query Options on page 50
   - People Query Options on page 52

4. **Save a query** – You can also save queries and select them under **Saved queries** to search again. To save your query, enter a query and then scroll down in the drop down menu to **Saved queries**, and select **Save**.



model ~ "110" and version ~ "3"

model ~ "110" and version ~ "3" and isOffline or disabl...

model ~ "110" and version ~ "3"

Example

This query searches for Airwall Gateways that are cloud Airwall Gateways named “hello there”, or for any Airwall Gateways that are running version 3.1.0.

```
(isCloud and name == 'hello there') or version == '3.1.0'
```

Logical Operators

The supported logical operators you can use in an expression using the Conductor Query Language.

Logical Operator	Description	Examples
`and`	Finds everything that matches ***all*** expressions.	`model == ‘110g’ and version == ‘3.1.0’` Finds all 110g Airwall Gateways on v3.1.0
`or`	Finds everything that matches ***any*** expression.	`model == ‘110g’ or version == ‘3.1.0’` Finds all 110g Airwall Gateways and all Airwall Edge Services on v3.1.0

`in`	Finds everything that has any of the values in the list.	`tags in [‘a’, ‘c’]`
		Finds everything tagged a or c. Compare this with `tags == [‘a’, ‘c’]`, which returns items tagged with both and only these two tags.
		`'a' in tags`
		Finds everything tagged a, even if these items also have additional tags.
		`version in ["3.1.0", "3.0.2", "3.0.0"]`
		Finds everything on version 3.1.0, 3.0.2, or 3.0.0.

~ or `%`	Partial match of the value.	`name ~ ‘bldg4’` Finds all Airwall Edge Services with “bldg4” in the name.
`==`	Exact match of the value.	`name == ‘bldg4’` Finds only Airwall Edge Services named exactly ‘bldg4’.
`!=`	Not equal	`name != ‘bldg4’` Finds Airwall Edge Services that aren’t named ‘bldg4’.
`!`	Is not	`!isCloud` Matches everything that’s not a cloud Airwall Gateway.
`()`	Group expressions inside the parentheses.	`(model == ‘110g’ and version ~ ‘3.1.0’) or (model == ‘300v’ and version == ‘3.0.0’)`

Overlays Query Options

Query options for the **Overlays** page if you select to Search by Expression with the Conductor Query Language on page 45. Options include fields to search in and states that an overlay can be in.

Query option	Description	Example
`airwallCount`	How many Airwall Edge Services are in the overlay	`AirwallCount > 10` Finds overlays with more than 10 Airwall Edge Services in them
`airwallNames`	Names of the Airwall Edge Services in the overlay	`AirwallNames ~ 'bldg4'` Finds overlays that have Airwall Edge Services with 'bldg4' in their name.
`name`	Name of the overlay	
`description`	Description of the overlay	
`deviceCount`	How many devices are in the overlay	
`dnsServers`	List of DNS servers in the overlay	`dnsServers ~ '192.168.1.1'` Finds all overlays that have 192.168.1.1 set as a DNS server
`relayNames`	Names of relays in the overlay either used directly or through an Airwall group.	
`tags`	Tags (limited to tags that you have permission to see).	
`vlanTags`	The VLAN tags that are allowed in traffic in the overlay	
`vlanAllowTagged`	If tagged VLAN traffic is allowed in the overlay	
`vlandAllowUntagged`	If untagged VLAN traffic is allowed in the overlay	

Query state	Description	Example
`isDisabled`	Overlay is disabled	`isDisabled` Searches for overlays that are not enabled.
`isEnabled`	Overlay is enabled	`isEnabled` Searches for overlays that are enabled.

Query state	Description	Example
`hasManagedRelay`	Overlay has a managed relay configured	

Devices Query options

Query options for the **Devices** page if you select to Search by Expression with the Conductor Query Language on page 45. Options include fields to search in and states that devices can be in.

Query option	Searches in this field	Example
`airwallName`	Name of the Airwall Gateway managing this device	
`description`	Description	
`deviceGroupNames`	Device groups this device is in	
`deviceType`	Device type. Can be one of: 'Local device' 'Airwall agent device' 'Bypass destination'	`deviceType == 'Local device'`
`hostname`	Hostname	
`internalIP`	Overlay device IP	
`ip`	Overlay device IP (NAT). If not NAT'd, this is the same as internalIP.	
`mac`	Mac address	
`name`	Name	
`ouiName`	OUI name	See also Search for or Sort Devices by MAC Address OUI (Manufacturer) Name on page 115.
`tags`	Tags (limited to tags that you have permission to see).	
`uid`	UID of the device	

Query state	Description	Example
`canEdit`	You have permission to edit this device	
`hasRecentActivity`	Device was active during the latest interval set on the Airwall. You can set this interval on the Reporting tab of the Airwall. Defaults to 5 minutes.	

Query state	Description	Example
isAgentDevice	Device is an Airwall Agent or Server device	
`isBypassDestination`	Device is a bypass destination. Can be negated with !	`!isBypassDestination` Matches devices that are not bypass destinations
`isDisabled`	Device is disabled	
`isDiscovered`	Device has been discovered	
`isEnabled`	Device is enabled	
`isLocalDevice`	Device is a local device	
`isMacLockdown`	Device has Mac Lockdown set	
`isNetworkDevice`	Device is a network device	

`lastActivityAgoStatus`	Searches on activity status. Can be one of:
	`'none'`
	`'disabled'`
	`'stale'`
	`'recent'`	

Airwalls Query Options

Query options for the **Airwalls** page if you select to Search by Expression with the Conductor Query Language on page 45. Options include fields to search in and states that an Airwall Edge Service can be in.

Query option	Searches in this field	Example
`description`	Description	
`deviceCount`	The number of devices the Airwall Edge Service has.	
`hit`	Generated HIP HIT for the Airwall Edge Service	
`location`	Location	
`model`	Airwall Edge Service model	
`name`	Name	
`networkCount`	The number of overlay networks that the Airwall Edge Service is in.	
`notes`	Notes	
`tags`	Tags (limited to tags that you have permission to see).	
`uid`	UID of the Airwall Edge Service	
underlayIP	The primary published underlay IP address for an Airwall.	

Query option	Searches in this field	Example
underlayIPs	The full list of published underlay IP addresses for the Airwall.	
`version`	Firmware version	

Query state	Description	Example
`canEdit`	Airwall Edge Service is one you have permissions to edit.	
`hasDiscoveredDevices`	Airwall Edge Service has discovered devices through passive device discovery	
hasError	Airwall Edge Service is reporting one or more errors	`hasError` Finds all Airwalls reporting an error. **Note:** Any Airwalls with an error also have a notification bell with the number of errors on it.
`hasFirmwareUpdate`	Airwall Edge Service has a firmware update available on the Conductor	
`hasHotfix`	Airwall Edge Service has a hotfix update available on the Conductor	
`hasRemoteSession`	Airwall Edge Service currently has an active remote session	
`isAgent`	Airwall Edge Service is an Airwall Agent or Server	
`isBypassGateway`	Airwall Gateway is set to act as a bypass gateway	
`isCloud`	Airwall Edge Service is a cloud Airwall Gateway	
`isDisabled`	Airwall Edge Service is disabled	
`isDisconnected`	Airwall Edge Service is in disconnected mode	
`isGateway`	Airwall Edge Service is an Airwall Gateway	
`isHaPrimary`	Airwall Edge Service is a high-availability primary (active)	
`isHaSecondary`	Airwall Edge Service is a high-availability secondary (standby)	
`isManaged`	Airwall Edge Service is managed	
`isOffline`	Airwall Edge Service is Offline	
`isOnline`	Airwall Edge Service is Online	

Query state	Description	Example
`isRelay`	Airwall Edge Service is set up as an Airwall Relay	
`isRevoked`	Airwall Edge Service is revoked	
`isUnmanaged`	Airwall Edge Service is unmanaged	
`isUnsupportedVersion`	Airwall Edge Service is on a version not supported by your current Conductor	

People Query Options

Query options for the **People** page if you select to Search by Expression with the Conductor Query Language on page 45. Options include fields to search in and states that a person can be in.

Query option	Searches in this field	Example

`authProviderName`	Person is authenticating through the given provider. Can be one of:
	`‘local_accounts’`
	`‘openid_connect’`
	`‘ldap’`
		`authProviderName=='openid_connect’`
		Finds people who are authenticating through a third-party provider.

`description`	Search people's description.	
email	Search people's email	`email ~ ‘@tempered.io’` Searches for people with a tempered.io email address.
ip	Search by IP address	

Query option	Searches in this field	Example
name	Search by name	
permissionNames	Search the list of permissions that a person has in the Conductor. Can be any number of: • `permissions` – Person has permissions to edit permissions. • `system_config` – Person has permissions to edit system configuration. • `cloud` – Person has permissions to instantiate cloud Airwalls. • `firmware_conductor` – Person has permissions to update Conductor firmware. • `edit_unassociated_airwalls` – Person has permissions to provision and manage Airwalls that are not in an overlay. • `revoke_airwalls` – Person has permissions to revoke and delete or re-activate Airwalls. • `provision_airwalls` – Person has permissions to provision and manage Airwalls • `advanced_view` – Person has permissions to see the Advanced view in the Conductor. • `bypass_destinations` – Person has permissions to view and edit bypass destinations. • `airwall_groups_relay` – Person has permissions to view and edit Airwall groups and relay rules. • `send_invites` – Person has permissions to send **Airwall Invitations**.	`permissionNames ~ 'system_config'` Finds all people with permissions to edit the system configuration.
phone	Either phone field	

roleName	Person’s role in the Conductor. Can be one of:
	`‘System Administrator’`
	`‘Network Administrator’`
	`‘Read-Only System Administrator’`
	`‘Remote Access User’`
		`roleName ~ ‘Admin’`
		Searches for people who are any type of Conductor admin.

Query option	Searches in this field	Example
tags	Tags (limited to tags that you have permission to see).	
username	Username in the Conductor	

Query state	Description	Example
`hasApiAccess`	Person has access to the Conductor API	
`isActive`	Person is active	
`isInactive`	Person is not active	
`isNetworkAdmin`	Person is a network administrator in the Conductor	
`isReadonlyAdmin`	Person is a read-only administrator in the Conductor	
`isSystemAdmin`	Person is a system administrator in the Conductor	`!isAdmin` Finds people who are not system administrators.
`isRemote`	Person is a remote user in the Conductor	

Manage People

Manage Conductor admins and people connecting to your Airwall secure network with laptops and mobile devices.

Manage Conductor Admins

Create accounts and people groups in the Conductor to manage the administrators who access your Airwall Conductor and your overlay networks and devices.

Add a Person

Add a person and give them a role that determines what they can access on the Conductor and/or your Airwall secure network.

Note: If you are onboarding people using LDAP or a third-party authentication provider, people are imported as they log in. See Configure LDAP authentication on Conductor and Airwall Edge Services on page 257 and Configure LDAP to manage user roles on page 265, or Integrate Third-party Authentication with OpenID Connect on page 247.

1. Log in to the Conductor with a system administrator account and go to **People**.
2. On the **People** tab, select **New Person**.
3. Under **Status**, select whether to create this account as **Active** or **Inactive**. You can use this option to set up people's accounts prior to onboarding, or to deactivate a person's account as needed.
4. Under **User directory**, usually you leave it at **Local User List**, providing authentication through the Conductor. See note above if you are using LDAP or a third-party authentication provider.
5. Enter the person's information: **Username** and **Email** are required.
6. Under **Role**, select the Conductor role for the person.

For more information on:

- Conductor roles – See Understand People Roles and Permissions on page 58.
- Custom permissions for System and Network Administrators – See Customize Permissions for System and Network Administrators on page 56

7. (Optional) If you give the person an administrator role, select their initial **Alert email trigger level**.

   Note: Administrator roles can log in and change their alert level.

8. For password, you have two options:

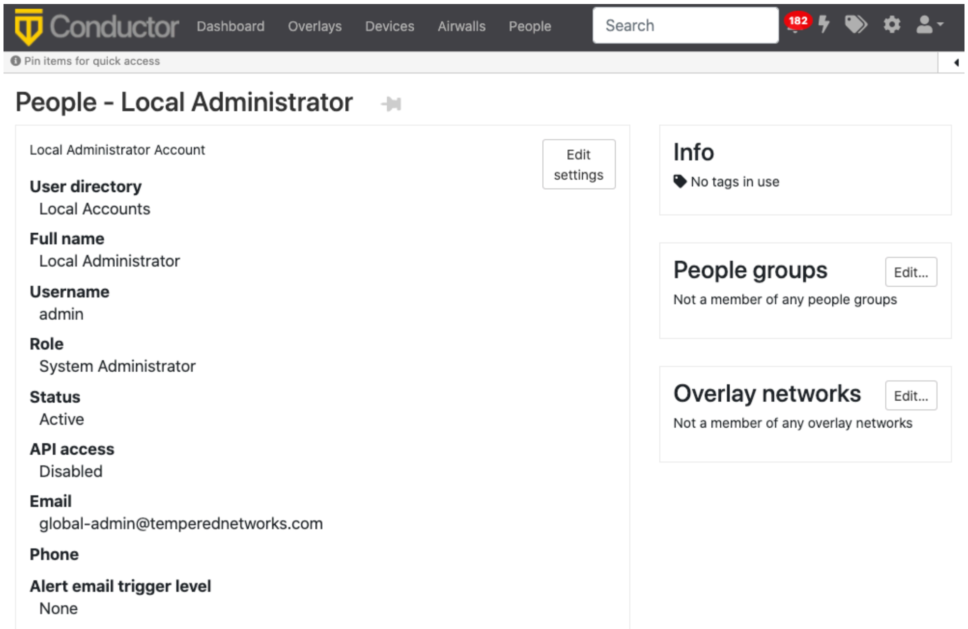
   - **User sets their own password** – Select **Send new user an email with a link to set their password** to let the user set their own password.
   - Or, **Set a password for the user** – Select **Set a password for the user to log in**. You can either enter a password, or select **Generate** to generate a password and copy it to your clipboard.

   Note: If you choose to set the password, you need to provide the username and password you created to the person.

9. Click **Create person**.

   Note: New accounts are active by default. A person can log in with the account after a few minutes. To create a user as inactive, or change their status to Inactive, under **Status**, select **Inactive**.

Once you've created the person's account, you can add them to **People groups** or Overlay networks.



People - Local Administrator

Local Administrator Account

User directory
Local Accounts

Full name
Local Administrator

Username
admin

Role
System Administrator

Status
Active

API access
Disabled

Email
global-admin@temperednetworks.com

Phone

Alert email trigger level
None

Info
No tags in use

People groups
Not a member of any people groups

Overlay networks
Not a member of any overlay networks

Related tasks

Set up a People Group on page 89
Set up a people group to make it easier to manage the people accessing your secure network.

Edit people who can access an overlay network on page 419
Overlay networks can only be modified by users who are editors of that network. After creating an overlay network, you may want to add additional editors, viewers, or users to your overlay network or edit their roles.

Change a Person's Account

Edit a person's account to change how they access the Conductor. You can edit settings such as whether the account is active or inactive, change passwords, change roles, and more.

1. Log in to the Conductor with a system administrator account and click **People**.

2. Select a person to open their page. You can sort or filter the list of people to find the person you're looking for.
3. Select **Edit Settings**.
4. Make the changes to the account.

   For more information on:

   - Conductor roles – See Understand People Roles and Permissions on page 58.
   - Custom permissions – See Customize Permissions for System and Network Administrators on page 56
5. Select **Update Settings**.

Customize Permissions for System and Network Administrators

You can fine-tune the permissions for System and Network administrators in your Airwall secure network.

System and Network administrators have a set of permissions by default in the Conductor. You can customize what these permissions are by default, and you can customize the permissions for individual system and network administrators.

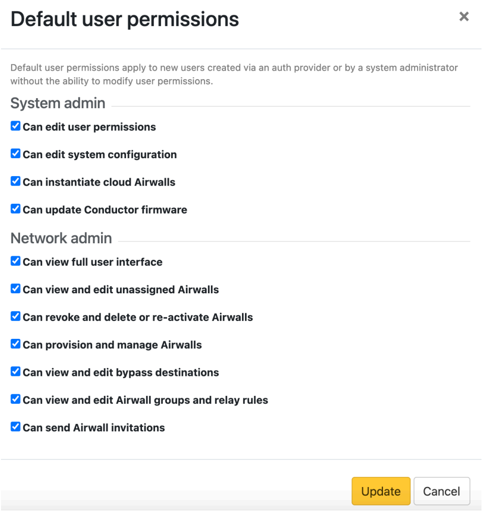
Supported Roles	System Administrators with **Can edit user permissions** enabled.

Customize Default Role Permissions

You can set the default permissions that are given to people who are newly assigned the system and network administrator roles in the Conductor.

Note: Default user permissions apply only to people currently being added to a role (both new users and users who are changing roles). It does not change the permissions of people already assigned that role. The defaults can be modified as a user is created if the person making the change has "Can edit user permissions" permission.

1. Go to **Settings** > **Authentication**.
2. Under **Default user permissions**, select **Edit Settings**.
3. Check the permissions you want new people to have by default when they are assigned these roles.



Default user permissions

Default user permissions apply to new users created via an auth provider or by a system administrator without the ability to modify user permissions.

System admin

☑ Can edit user permissions

☑ Can edit system configuration

☑ Can instantiate cloud Airwalls

☑ Can update Conductor firmware

Network admin

☑ Can view full user interface

☑ Can view and edit unassigned Airwalls

☑ Can revoke and delete or re-activate Airwalls

☑ Can provision and manage Airwalls

☑ Can view and edit bypass destinations

☑ Can view and edit Airwall groups and relay rules

☑ Can send Airwall invitations

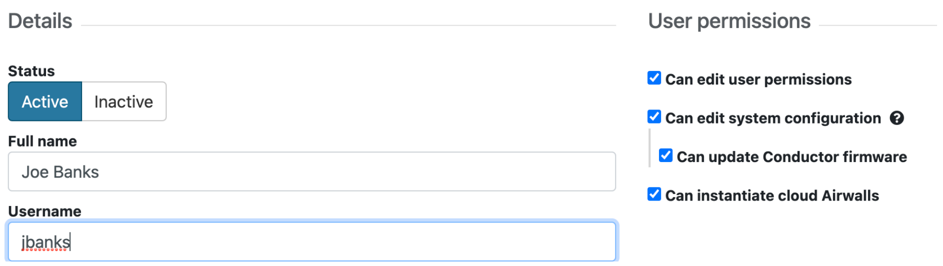
4. Select **Update** to save.

Customize Permissions for individual System and Network Administrators

If you are a system administrator with **Can edit user permissions** active, you can customize the permissions for system and network administrators.

1. Go to **People**, select a person to open their page, and then select **Edit Settings**.
2. Under **User permissions**, check or clear the permissions you want this person to have.

System Administrator customizable permissions



Details

Status

● Active ○ Inactive

Full name: Joe Banks

Username: jbanks

User permissions

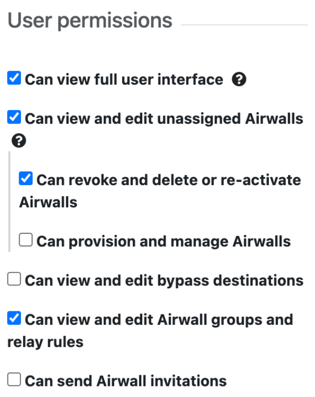
☑ Can edit user permissions

☑ Can edit system configuration

☑ Can update Conductor firmware

☑ Can instantiate cloud Airwalls

Network Administrator customizable permissions



User permissions

☑ Can view full user interface

☑ Can view and edit unassigned Airwalls

☑ Can revoke and delete or re-activate Airwalls

☐ Can provision and manage Airwalls

☐ Can view and edit bypass destinations

☑ Can view and edit Airwall groups and relay rules

☐ Can send Airwall invitations

For more information about these permissions, see Customizable Permissions Descriptions on page 57.

3. Select **Update Settings**.

Customizable Permissions Descriptions

These are the permissions that can be customized for people assigned the System or Network Administrator roles.

Permission	Description
For System Administrators:	
Can edit user permissions	Can edit Conductor default permissions and permissions for individual users, including assigning user roles and customizing their permissions. Can also create new overlay networks and assign them to a network admin to manage trust.
Can edit system configuration	Administrator can edit Conductor Settings, including High Availability (HA), email server, remote logging, authentication, or any other settings in **Settings** > **General**.
Can create and configure cloud features	Can create and configure cloud Airwall Gateways, and create an HA-paired Conductor in the cloud.
Can update Conductor firmware	This option is available if you have checked **Can edit system configuration**. Can update the Conductor software and Airwall Edge Service firmware from **Settings** > **Firmware updates**
For Network Administrators:	

Permission	Description
Can view full user interface	When clear, the user sees a simplified, easier-to-use view in the Conductor. For a description of the simplified view, see Set a Streamlined View for a Network Administrator on page 58.
Can view and edit unassigned Airwalls	Can view or edit any Airwall Edge Services that are not assigned to any overlay networks, including adding the devices in these Airwall Edge Services to any overlay networks they have permission to.
Can revoke and delete or re-activate Airwalls	Requires that **Can view and edit unassigned Airwall** is checked. Can revoke, delete, and re-activate Airwall Edge Services in their overlay networks, and can view and reactivate any revoked Airwall Edge Services .
Can provision and manage Airwalls	Requires that **Can view and edit unassigned Airwall** is checked. Can view and provision provisioning requests, and can manage unmanaged Airwall Edge Services.
Can view and edit bypass destinations	Can view and edit any bypass destinations.
Can view and edit Airwall groups and relay rules	Can view and edit Airwall groups and relay rules for Airwall Edge Services in their overlay networks.
Can send Airwall Invitations	Can send **Airwall Invitations** to invite users to connect to the Airwall secure network and gain access to the devices in their overlay networks.

Set a Streamlined View for a Network Administrator

When you set the permissions for a Network administrator, you can clear the **Can view full user interface** permission, which provides the Network administrator with a streamlined view that can simplify their workflow.

Network administrators using the streamlined view can manage their overlays, and the devices, Device groups, and Airwall Edge Services in them.

1. Go to **People**, and open the People page for the Network administrator.
2. Select **Edit Settings**.
3. Clear the **Can view full user interface** box.
4. **Update Settings**

The Network administrator now sees a streamlined view.

Note: You can also set the streamlined view as the default for all newly-assigned Network administrators. See Customize Permissions for System and Network Administrators on page 56.

To see what Network administrators with a limited view can see, see Manage Overlay Networks in Streamlined View on page 115.

Understand People Roles and Permissions

When you add a person to the Conductor, the person's role, and whether the person is a manager or member of an overlay, controls whether they have access to create, edit, or view overlay networks and their Airwall Edge Services and devices.

The Conductor supports the following people roles, with the following default permissions. You can also fine-tune permissions for System and Network Administrators. See Customize Permissions for System and Network Administrators on page 56:

- System Administrator - Designed for administrators who may need to perform all Conductor functions. By default, a system administrator can edit all Airwall Edge Services in the system and is a de facto editor of all Airwall Edge Services and overlay networks. Depending on granular user permissions, a system administrator can modify other users' permissions, edit system-level configuration (such as SMTP, Conductor HA pairing, remote syslog), create cloud Airwall Gateways, and upgrade the Conductor firmware.

- Network Administrator - Designed for administrators who need to manage and potentially modify existing overlay networks, Airwall Gateways and devices. Depending on granular user permissions, a network administrator can view and edit unassigned (not part of an overlay network) Airwall Edge Services, revoke and delete Airwall Edge Services, and provision and manage Airwall Edge Services. A network administrator cannot create new users or overlay networks or edit system configuration.
- Read-only System Administrator - Designed for administrators who need to monitor overlay networks, Airwall Gateways, and device information, but who do not have a need to modify configurations. A read-only system administrator can view all Airwall Edge Services in the system and is a de facto viewer of all overlay networks. A read-only system administrator can also run reports and perform diagnostic functions on the Conductor and Airwall Edge Services.
- Remote Access User - This role is for people who need access to an Airwall secure network through an Airwall Agent or Server. This user can only modify their account email and password. Remote access users can also view the remote access portal where they can see any activation codes assigned to them, a list of remote devices they have access to, and a list of the Airwall Edge Services assigned to them.

This table shows the default permissions. To customize these permissions, see Customize Permissions for System and Network Administrators on page 56

Task	System Administrator	Network Administrator	Read-only System Administrator	Remote Access User
Manage users	Create Modify Delete	Modify own email and password	View all users. Modify own email and password	Modify own email and password
Manage Conductor settings	Configure (with permissions)	Not available	View	Not available
Manage overlay networks	Create Modify Delete	View Modify	View	Not available
Manage Airwall Edge Services	Add Modify Delete	Add (with permissions) Modify Delete	View	Not available
Manage devices	Add Modify Delete	Add Modify Delete	View	Not available
Manage firmware updates	Download Update Publish	Update	Not available	Not available

See Also:

- To customize permissions, see Customize Permissions for System and Network Administrators on page 56
- For pre-3.0 roles, see Understand People Roles (v2.2.13 and earlier) on page 60

Understand People Roles (v2.2.13 and earlier)

When you add a person to the Conductor, the person's role, and whether the person is a manager or member of an overlay, controls whether they have access to create, view, or edit overlay networks and their Airwall Edge Services and devices.

The Conductor supports the following people roles:

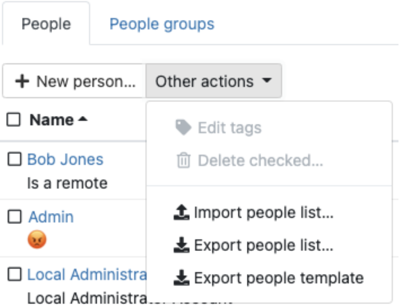
- System Administrator - Designed for administrators who need to perform all Conductor functions. A system administrator can edit all Airwall Edge Services in the system and is a de facto editor of all overlay networks. Depending on granular user permissions, a system administrator can modify other users' permissions, edit system-level configuration (such as SMTP, Conductor HA pairing, remote syslog), create cloud Airwall Gateways, and upgrade the Conductor firmware.
- Network Administrator - Designed for administrators who need to manage and potentially modify existing overlay networks, Airwall Gateways and devices. Depending on granular user permissions, a network administrator can view and edit unassigned (not part of an overlay network) Airwall Edge Services, revoke and delete Airwall Edge Services, and provision and manage Airwall Edge Services. A network administrator cannot create new users or overlay networks or edit system configuration.
- Read-only System Administrator - Designed for administrators who need to monitor overlay networks, Airwall Gateways, and device information, but who do not have a need to modify configurations. A read-only system administrator can view all Airwall Edge Services in the system and is a de facto viewer of all overlay networks. A read-only system administrator can also run reports and perform diagnostic functions on the Conductor and Airwall Edge Services.
- Remote Access User - This role is for people who need access to an Airwall secure network through an Airwall Agent or Server. This user can only modify their account email and password. Remote access users can also view the remote access portal where they can see any activation codes assigned to them, a list of remote devices they have access to, and a list of the Airwall Agents and Servers assigned to them.

Task	System Administrator	Network Administrator	Read-only System Administrator	Remote Access User
Manage users	Create Modify Delete	Not available	View	Modify own email and password
Manage Conductor settings	Configure	Not available	View	Not available
Manage overlay networks	Create Modify Delete	View Modify	View	List of Overlays they are in only
Manage Airwall Edge Services	Add Modify Delete	Add Modify Delete	View	Not available
Manage devices	Add Modify Delete	Add Modify Delete	View	Not available
Manage firmware updates	Download Update Publish	Update	Not available	Not available

Import people using a CSV file

Add many local users to the Conductor at one time by importing them in bulk. You export a .csv file as a template or with current users, edit it, and then import it back into the Conductor..

1. In the Conductor, go to the **People** page.
2. Under **People**, open **Other actions**.



3. Select **Export people list**, or **Export people template** and then confirm the export. You can use either to import people. The people list allows you to see and modify some options for people already in the Conductor.
4. Edit the .csv file that you downloaded to add people. See Import People .csv File Details on page 61 for an explanation of the columns. The minimum required columns are `username`, `role`, `name`, `email`, and `active`. Leave the password blank to send the person an email with a link to set their password. If you do include passwords, make sure they meet the password criteria. For information on setting password criteria, see Configure Authentication Options on page 242.

   Note: For existing people in the .csv file, you can also modify roles, permissions, and most other options. You cannot change passwords or remove people using the .csv.
5. Back on the **People** page, open **Other actions** again.
6. Select **Import people list**, select **Choose File**, and then select the file you edited and select **Upload**.
7. If validation fails, correct the file and try again.
8. Once the import passes validation, review the list of people being added, and select **Next** and then **Commit** to add them.

If you need to make any changes once the file is imported, you can edit the .csv and then re-import. Importing a file modifies the account for existing people (exceptions are you cannot change or remove passwords or remove people using import). After a person is added to the Conductor, you must manage passwords individually from each person's page.

Import People .csv File Details

The import people .csv has the following columns:

Column	Description	Example
username	*Required*. Enter a unique username. *Cannot update for existing users.*	joebanks
role	*Required*. Person's role in the Conductor. Must be one of: • system_admin • viewer • network_admin • remote_user	remote_user

Column	Description	Example
name	*Required*. Full name, with first name first.	Joe Banks
description	*Optional*. Description for the person.	Admin for Building 1
email	*Required*. A valid email for the person.	jbanks@tempered.io
phone1 and phone2 (both optional)	*Optional*. Phone number for the person.	+12065551212
active	*Required*. Add the person as an active user. Boolean TRUE or FALSE. In most cases, you want to have this as TRUE.	TRUE
password	*Optional*. If you want to set a password for the user, you can enter it here. If you have SMTP set up on your Conductor, you can leave it empty, the Conductor sends an email to the new user asking them to log in and set their password. *Cannot update for existing users.*	very_secure_P@assword
api_user	*Optional*. Add the person with rights to use the API. Boolean TRUE or FALSE. Only available for system_admin, network_admin, and viewer roles.	TRUE
email_alert_level	*Optional*. Enter the Conductor alerts this person should get in email. Must be one of: • none • info • warning • error	none
tags	*Optional*. Apply existing or new tags to people, in the format [“tag1”,“tag2”]. To make no changes, leave blank. To remove all tags, enter an empty array [ ]. See **Template Note**.	["fte", "engr"]
person_groups	*Optional*. Apply existing or a new set of people groups to people, in the format [“person group name 1”, “person group name 2”]. To make no changes, leave blank. To remove the person from all people groups, enter an empty array [ ]. See **Template Note**.	["building 2", "2nd floor"]

Template Note: The first row on the people_template.csv that you download has empty arrays for the tags and person_groups columns. These empty arrays will remove the tags and person_groups if you enter an existing person on that line.

When you import your .csv file, the Conductor validates the file and warns you of any detected issues. Edit the .csv to fix any issues and re-import. Once it validates, you can select Commit and the Conductor adds and updates the people on your list.

Remove people in bulk

You can delete users in bulk from the **People** page.

1. In the Conductor, go to the **People** page.
2. Select the people you want to delete.
3. Under **People**, open **Other actions**.
4. Select **Delete checked**.
5. Confirm the list of people to delete, and select **Delete**.

Restrict network access for Windows Airwall Agents and Servers users (Lockdown mode)

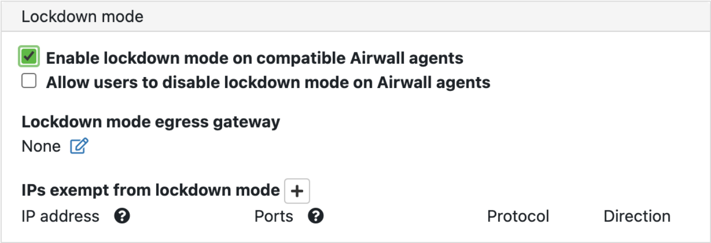
You can configure Windows Airwall Agents and Servers to run in Lockdown mode, which restricts access to network resources not explicitly allowed by Conductor trust policy.

Notes:

- This setting will be replaced when Windows Airwall Agents and Servers are updated and can use bypass settings.
- Lockdown mode is a global setting that applies to all Windows Airwall Agents and Servers on the Conductor.

To set up lockdown mode

1. Go to **Settings** > **Global Airwall agent settings**.
2. Select **Edit Settings**.
3. On the **Advanced** page, scroll to **Lockdown mode**.
4. Check **Enable lockdown mode on compatible Airwall agents**.



Lockdown mode

☑ Enable lockdown mode on compatible Airwall agents
☐ Allow users to disable lockdown mode on Airwall agents

Lockdown mode egress gateway
None

IPs exempt from lockdown mode +

IP address	Ports	Protocol	Direction

5. Select **Save**.

If you want to allow some level of access outside of the secure network, you have a few options:

- **Allow users to override Lockdown mode on their device** – Check **Allow users to disable lockdown mode on Airwall agents**. Users can then disable lockdown mode from their device. Select **Save**.
- **Provide Internet access** – Under **Lockdown mode egress gateway**, select an Airwall Gateway that has been configured as a bypass (egress) gateway. Select **Save**. Any traffic that is not allowed by trust policy is then sent to the bypass gateway and can reach the Internet.

Note:

- To set up a bypass gateway, you must configure an Airwall Gateway with an overlay port group that can route out to the Internet. In most cases, you must also set SNAT on that port group. For more details, see Configuring an Airwall Gateway as a bypass egress gateway on page 396.

- **Exempt specific resources from lockdown mode** - This option gives you the ability to allow access to certain resources without trust policy:

  1. Next to **IPs exempt from lockdown mode**, select the + (plus).
  2. For each exemption, specify an IP address, a protocol and direction, and, optionally, a port.
  3. Select **Save**.

  Once set, local traffic matching the IP and protocol is allowed.

Connect People's Devices to your Airwall secure network

How to connect cell phones, laptops, and servers to the resources people need access to behind your Airwall secure network.

People connect their devices to your secure network using Airwall software installed on their devices, called Airwall Agents and Servers. There are Airwall Agent or Server software applications for the most common device types.

The easiest way to get your users started is to Set up a People Group on page 89 and send people an Airwall Invitation or Activation code. You can also Connect People as Remote Access Users on page 74. Using these methods automates much of the process for both the people connection and for you, the Conductor administrator.

Here's how it works:

1. For people who need to connect their devices to your Airwall secure network, you send them **Airwall Invitations** or Activation Codes. You can send a single invitation or send in bulk, and can choose whether to invite by email or by downloading activation codes to distribute yourself.
2. For the people you've invited:
   - Via email **Airwall Invitations**, they open the invitation email and click the link.
   - Via activation codes, they open the link to go to the **Connect an Airwall Agent** activation page.
3. They download and install an Airwall Agent or Server onto their device.
4. Once the Airwall Agent or Server is installed, they click the link in the email or **Connect an Airwall Agent** page to activate their account.
5. Once a person activates their account, the Conductor automatically takes care of all the steps to provision, license, manage, and name the new Airwall Agents and Servers.

You can send **Airwall Invitations** or Activation codes in bulk to entire organizations, and manage the connections and what they have access to in the Conductor.

Help for your users to install the software and connect is here: Connect to Airwall on page 6.

If you choose not to use **Airwall Invitations** or Activation codes, the people connecting need to download and install the software, and then enter the Conductor address manually. You then need to review the provisioning requests, confirm device IDs with each person, and grant access to each person’s Airwall Agent or Server.

If you need to install the software from the Conductor, see Install Airwall Agents and Servers on people's laptops and devices on page 343.

Connect People’s Devices with Airwall Invitations

Airwall Invitations greatly simplify the steps required to add people’s mobile phones, tablets, and computers to your Airwall secure network.

Note: Another way to automate the process is using Activation Codes or adding people as Remote Access Users and adding them to a people group. See Connect People's Devices with Activation Codes on page 75, or Connect People as Remote Access Users on page 74 and Set up a People Group on page 89.

The Walkthrough – Send Expiring Guest Access Invitations on page 69 provides an example or how to set up **Airwall Invitations** that you can modify to meet your organization needs.

Send Airwall Invitations

You send **Airwall Invitations** to invite people to connect to your Airwall secure network. It can be as simple as sending the invitations to a list of email addresses. With a bit of preparation, though, you can also automatically set up device access and trust as people connect their devices.

Before you begin

If you are sending **Airwall Invitations** in email,

- Gather the list of emails you want to send the invitations to.
- Make sure your Conductor email has been set up. See Configure Email Settings on page 238.
- If you want to require authenticated sessions, Set up User Authentication on page 91.

*Send **Airwall Invitations***

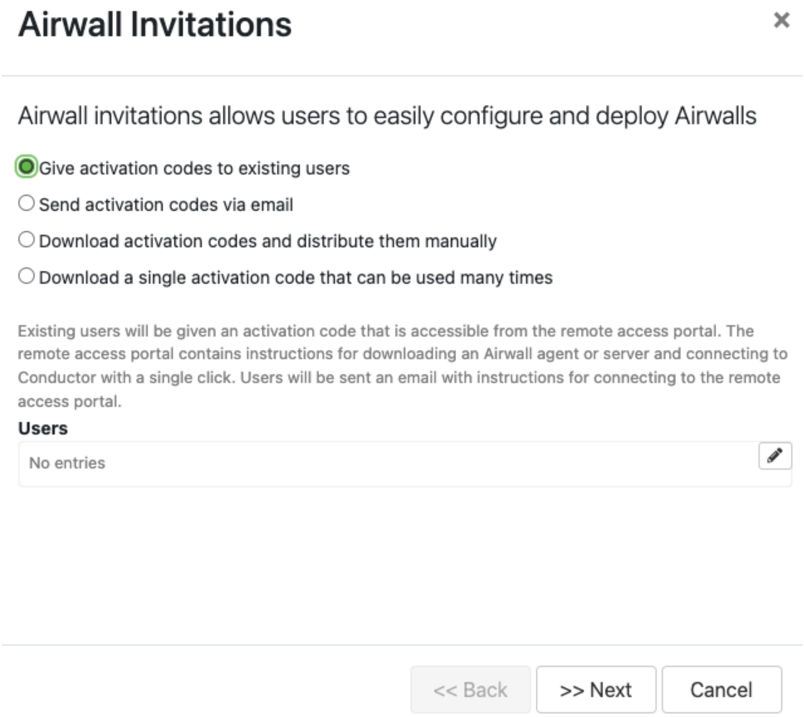
The possibilities include setting up which Overlay networks people belong to, what groups they're a part of, which Airwall Edge Services and devices they can access, and when a person's access to your Airwall secure network expires.

Before you begin

- Gather email lists for the types of people you need to grant access to
- (Optional) Group emails by people who need the same access permissions.
- (Optional) Create **Airwall groups** for the people you want to add. For example, you may want Employees and Contractors Airwall groups.
- (Optional) Create tags for the types of people and access.
- (Optional) Create Smart Device Groups to automatically add people to Device groups as they activate their Airwall Agents and Servers.

By doing a bit more planning and preparation in the optional steps above, you will save time in making sure people are able to access the resources they need. For a walkthrough showing how to set up invitations that automatically provide guests with access to your secure network for 4 hrs, see Walkthrough – Send Expiring Guest Access Invitations on page 69

1. Go to **Airwalls** > **Airwall Invitations**.
2. ***If you have already sent invitations***, you can open the drop down next to an invitation and select **Use as template** to send a similar invitation to more people. ***To create a new invitation***, select **New Airwall Invitations**.
3. In v3.0.0 and later, select how you want to invite people. Select each option to see a description.



Airwall Invitations

Airwall invitations allows users to easily configure and deploy Airwalls

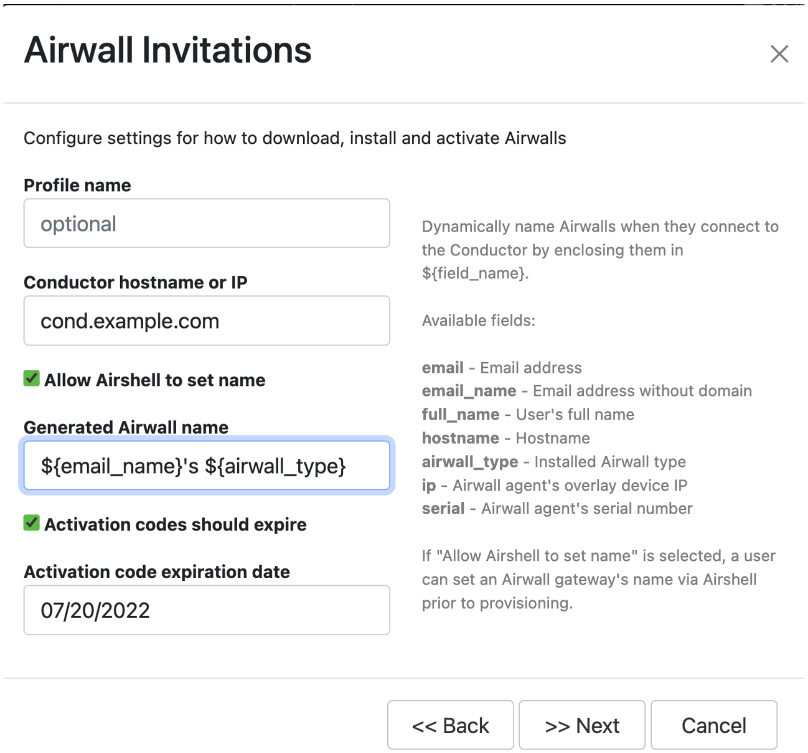
● Give activation codes to existing users
○ Send activation codes via email
○ Download activation codes and distribute them manually
○ Download a single activation code that can be used many times

Existing users will be given an activation code that is accessible from the remote access portal. The remote access portal contains instructions for downloading an Airwall agent or server and connecting to Conductor with a single click. Users will be sent an email with instructions for connecting to the remote access portal.

Users

No entries

4. After you select how to invite users, you will need to enter the options for that type. For example, select users if inviting current users, or enter the email addresses for the people you want to connect to your Airwall secure network.
5. Select **Next**.
6. Enter the options that are requested for your invitation type. Setting these options automates more of the process for the people trying to connect, as well as the administrator giving them access:
   a) **Profile name** – This is the name of the profile to create on the people's Airwall Agents and Servers.
   b) **Conductor hostname or IP** – Sets the Conductor they connect to.
   c) **Generated Airwall name** – Sets the name the Airwall Agent or Server has when the user activates it. The default value sets it to the email address followed by their Airwall Agent or Server type. See the help when you select this box to see other options for autogenerating names.
   d) **Activation codes should expire** – Check or clear this box, and if checked, set the **Activation code expiration date** – Sets the date the Airwall Invitation expires.



Airwall Invitations

Configure settings for how to download, install and activate Airwalls

Profile name

optional

Conductor hostname or IP

cond.example.com

☑ **Allow Airshell to set name**

Generated Airwall name

${email_name}'s ${airwall_type}

☑ **Activation codes should expire**

Activation code expiration date

07/20/2022

Dynamically name Airwalls when they connect to the Conductor by enclosing them in ${field_name}.

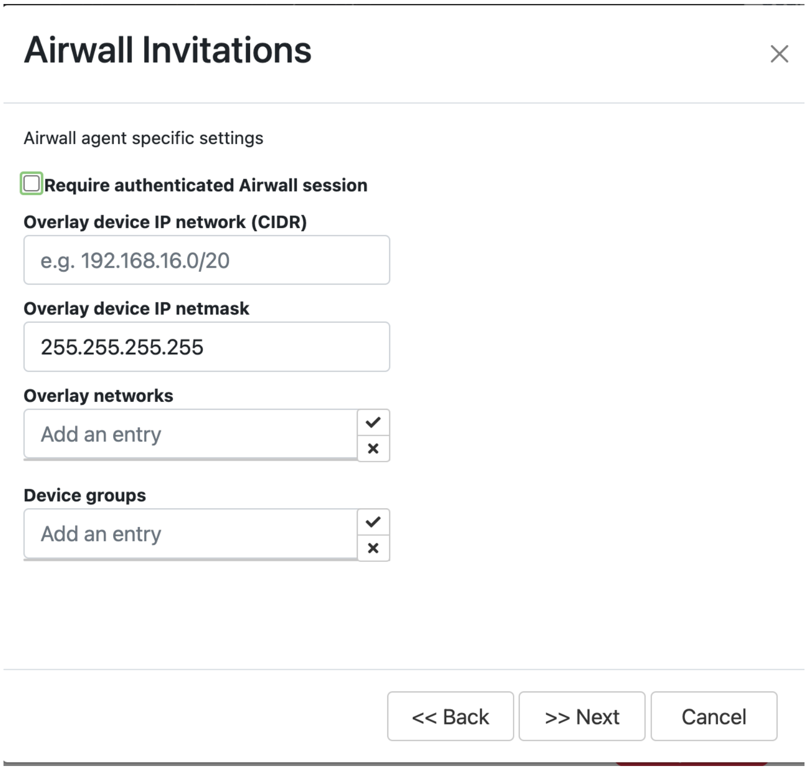
Available fields:

email - Email address
email_name - Email address without domain
full_name - User's full name
hostname - Hostname
airwall_type - Installed Airwall type
ip - Airwall agent's overlay device IP
serial - Airwall agent's serial number

If "Allow Airshell to set name" is selected, a user can set an Airwall gateway's name via Airshell prior to provisioning.

Note: pre-2.2.8 Conductors also have: **Install Package Location** – Enter a place accessible to your invitees where you've downloaded the Airwall Agent or Server software, or point to the latest version in Airwall help: https://webhelp.tempered.io/webhelp/content/topics/downloads_latest.html

7. Select **Next**.
8. Enter Airwall Agent or Server-specific settings to automate people's access as their devices connect:



Airwall Invitations

Airwall agent specific settings

□ **Require authenticated Airwall session**

Overlay device IP network (CIDR)

e.g. 192.168.16.0/20

Overlay device IP netmask

255.255.255.255

Overlay networks

Add an entry

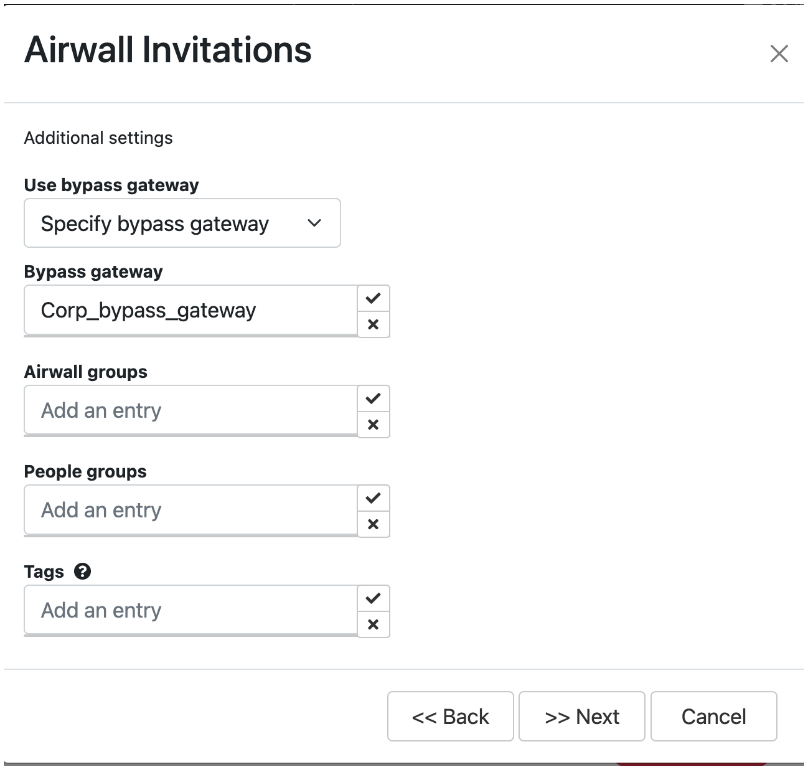
Device groups

Add an entry

- **Require authenticated Airwall session** – Check this option to require people accessing your Airwall secure network to authenticate.
- **Overlay device IP network (CIDR)** – (Optional) The network from which to assign IP addresses to devices as they connect.

  Note: If you use the same IP network in subsequent Invitations, the Conductor intelligently continues incrementing IP addresses. For instance, if you send out one Invitation starting at 192.168.1.15 with 10 emails and then another with the same IP with 10 emails, they all just get a free IP from the network as they come online.
- **Overlay device IP netmask** – Enter the netmask for the overlay device IP.
- **Overlay networks** – (Optional) The overlay networks to add people's devices to.
- **Device groups** – Select the **Device groups** to add devices to.

9. Enter any additional settings to automate people's access as their devices connect:



Airwall Invitations

Additional settings

Use bypass gateway: Specify bypass gateway

Bypass gateway: Corp_bypass_gateway

Airwall groups: Add an entry

People groups: Add an entry

Tags: Add an entry

- **Use bypass gateway** – If you want these users to use a specific bypass Airwall Gateway, select Specify bypass gateway, and then select the gateway you want them to use. You can also use the default bypass gateway set up in the Conductor, or not allow the use of a bypass gateway. For information on setting up bypass Airwall Gateways, see Backhaul Bypass on page 395 and Configuring an Airwall Gateway as a bypass egress gateway on page 396.
- **Bypass gateway** – Select the bypass Airwall Gateway you want users getting this Airwall Invitation to use.
- **Airwall groups** – Select **Airwall groups** to add Airwall Agents and Servers to. For example, you might assign these Airwall Agents and Servers to the Employee, Admin, or Vendor group.
- **People groups**– Select **People groups** to add users to.
- **Tags** – Create or assign tags to people's devices. For example, if you're using tags to create Smart Device Groups that add people's devices to the right overlays, enter these tags now. See Manage devices dynamically with Smart Device Groups on page 105.

10. **If you are generating Activation codes**, select **Generate** and skip the rest of these steps.
11. **If you are inviting existing users or sending emails**, select **Next**.

12. Double-check the email addresses and make any needed changes to the invitation email. To help the people receiving Activation codes to connect, point them to one of these help topics: I have an Airwall Invitation on page 14 or I have an Activation Code on page 15.
13. Select **Finish** to send the invitations.

Resend an Invitation

If you've sent an invitation and the person hasn't received it, or their invitation has expired before they activated it, you can resend it by using the original invitation as a template to create a new invitation. See Reuse an Invitation on page 69 to send a new invitation with a new expiration date.

Disable an Invitation

If you've sent an invitation and no longer want the person to be able to activate it, you can disable it.

1. In your Conductor, go to the **Airwalls** page.
2. Open the **Airwall Invitations** tab and find the invitation you want to disable.
3. Open the dropdown on the far right of the invitation row and select **Disable Invitation**.

Reuse an Invitation

If you have already created an invitation with the options needed for a new invitation, you can easily reuse it. Some of the information for the invitation will be already filled in.

1. In your Conductor, go to the **Airwalls** page.
2. Open the **Airwall Invitations** tab and find the invitation you want to disable.
3. Open the dropdown to the far right of the invitation row and select **Use as Template**.
4. Click through and fill in the information needed and click **Finish** to send.

Walkthrough – Send Expiring Guest Access Invitations

In this walkthrough, you set up and send **Airwall Invitations** that provide guests with 4 hours of access to your Airwall secure network, after which it automatically disables all communications.

One way you can use **Airwall Invitations** to group and configure people's devices as they accept the **Airwall Invitations** and connect to your Airwall secure network is to expire people's access to your secure network at a time you set.

Setting access that expires is useful when you have people, such as vendors or guests, that you want to give access to, but you want to enforce a time limit automatically.

You can modify this walkthrough to create your own rules for automatically configuring Airwall Agents and Servers using **Airwall Invitations**.

Walkthrough Overview

To create Airwall Invitations that expire, you need to:

1. **Create two Tags** – One to grant access and one to remove access. For example, if you're creating guest access, you might create tags of `Guest Access4hr` and `Guest Disabled`.
2. **Create two Smart Device Groups –**
   a) **Grant Access Group** – Create a rule that adds devices to the group if they have the `grant access` tag you created. For example, you might create a Smart Device Group called `Guest Access` and create a rule that adds devices tagged with `Guest Access4hr`.
   b) **Remove Access Group** – Create a rule that adds devices to the group if they have the `remove access` tag you created. For example, you might create a Smart Device Group called `Disabled Guests` with a rule to add devices tagged with `Guest Disabled`.
3. **Add the Grant Access group to the appropriate Overlays** – Add the Grant Access group to the Overlays that give the people's devices access to the resources they need.

Note: Do NOT assign the `Remove Access` Device Group to any Overlay Network. This Device Group is added as a negative to any other Smart Device Groups to prevent accidentally giving a guest access to resources they shouldn't have. Essentially, this Device Group is for guests whose access has expired.

4. **Hold or Revoke the `Remove Access` device group** – For people that have been moved to the `Remove Access` group, you can choose to:
   a) Hold – Allow the guests to stay until they require access again.
   b) Revoke –You can revoke the Airwall Agent or Server licenses for the people in the group, which returns the agent and server licenses back into the license pool.

   API Tip – You can revoke agents and servers in the API: Query for Airwall Agents with the “remove access" tag and revoke them if they no longer hold the grant access tag.
5. Add the “remove access" and grant access tags to the **Airwall Invitations** for the people you want to expire access

   API Tip – You can also set the tags and send **Airwall Invitations** in the API. The most recent API documentation is available in your Conductor. See Airwall API on page 508.

Step 1: Create Guest Access tags

The first step to do is create tags for visitors to your Airwall secure network. You need to create two tags, one for guests with 4 hr access, and one for guests whose access has expired.

To create a tag for guests with 4 hr access:

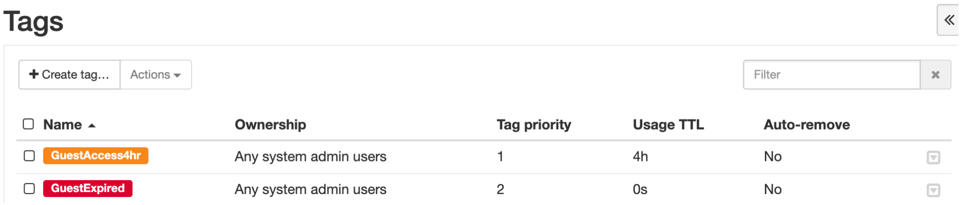
1. In your Conductor, open **Tags** in the upper right corner.
2. Select **Create tag** and name the tag `GuestAccess4hr`.

   Note: Make sure the tags you create are not being used elsewhere in the Conductor, as manually-added tags are also removed if they are the same as these conditional tags.
3. Under **Who can use this tag?**, set it to **Any Admin users**.
4. Under **Tag color scheme**, choose a color. This example uses orange.
5. Set **Tag priority** to **1**. This tag takes priority over the `Guest Expired` tag.
6. Set **Expire tag usage after this duration** to `4h`. If you want to customize the time period, supported units are: y, M, w, d, h, m, s (default) with no spaces. For example: 4h30m50s.
7. Click **Create**.

To create tag for guests whose access has expired:

1. On the **Tags** page, select **Create tag**, and name the tag `GuestExpired`.
2. Under **Who can use this tag?**, set it to **Any Admin users**.
3. Under **Tag background color** and **Tag text color**, choose colors, and check the example for the result. This example uses red.
4. Set **Tag priority** to **2**. This tag takes secondary priority to the `GuestAccess4hr` tag.
5. Leave **Expire tag usage after this duration** set to `0s` (this indicates the tag is permanent).
6. Click **Create**.

Your tags page now has these two tags. Notice that the **Expire tag usage after this duration** setting is shown under **Usage TTL**:



□ Name ▴	Ownership	Tag priority	Usage TTL	Auto-remove
□ GuestAccess4hr	Any system admin users	1	4h	No
□ GuestExpired	Any system admin users	2	0s	No

Step 2: Create Guest Access Smart device groups

Set up two Smart device groups that add people's devices as they connect.

Smart Device Groups are groups that are dynamically created and updated based on the rules you set up for the group. Along with tags, they allow you to automatically add devices people are connecting to groups based on what their Airwall Agent or Server has been tagged with.

You need to set up two groups that match your tags: one for guests with 4 hr access, and one for guests whose access has expired.

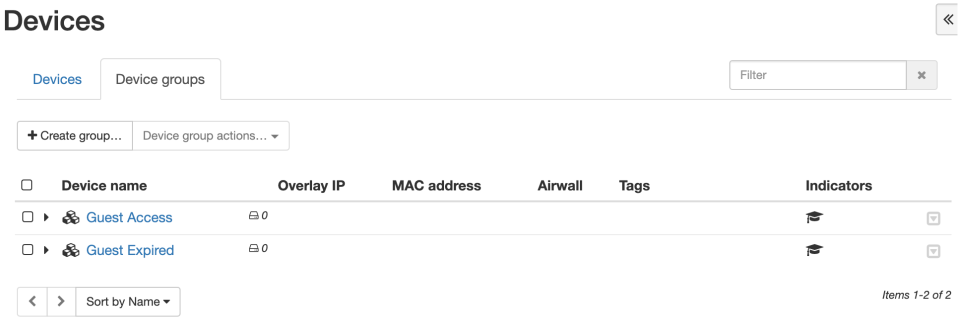
To create a Smart Device Group for guest 4 hr access:

1. In your Conductor, go to the **Devices** page.
2. Open the **Device groups** tab and select **Create group**.
3. On the **Device groups** page, name the group `Guest Access`.
4. On the `Guest Access` group page, under **Advanced properties**, check **Use rules to add devices**. This adds the **Rules** tab to the page.
5. Uncheck **Ignore auto-discovered devices until accepted**.
6. Open the **Rules** tab, click **Edit rules**, and then click **Add rule**.
7. In the **Rule Type** column, open the dropdown menu and select **Tag Match**. (Click the arrows to open the dropdown menu.)
8. In the **Arguments** column, select **Airwall**, and then right below the **Arguments** menu, click the edit icon ✎.
9. Choose the `GuestAccess4hr` tag, then click the check icon ✓ to set the tag.
10. Click **Create**.

To create a Smart Device Group for guests whose access has expired:

1. In your Conductor, go to the **Devices** page.
2. Open the **Device groups** tab and select **Create group**.
3. On the **Device groups** page, name the group `Guest Expired`.
4. Under **Advanced properties**, check **Use rules to add devices**. This adds the **Rules** tab to the page.
5. Uncheck **Ignore auto-discovered devices until accepted**.
6. Open the **Rules** tab, click **Edit rules**, and then click **Add rule**.
7. In the **Rule Type** column, and select **Tag Match**. (Click the arrows to open the dropdown menu.)
8. In the **Arguments** column, select **Airwall**, and then right below the **Arguments** menu, click the edit icon ✎.
9. Choose the `GuestExpired` tag, then click the check icon ✓ to set the tag.
10. Click **Create**.

You now have two Smart Device Groups (indicated by the 🎓 icon) for Guest Access:



Devices

□	Device name	Overlay IP	MAC address	Airwall	Tags	Indicators
□	Guest Access ⊟0					🎓
□	Guest Expired ⊟0					🎓

Step 3: Create an overlay for Guest Access

Creating a new overlay used for guest access gives you the most control over the resources guests have access to.

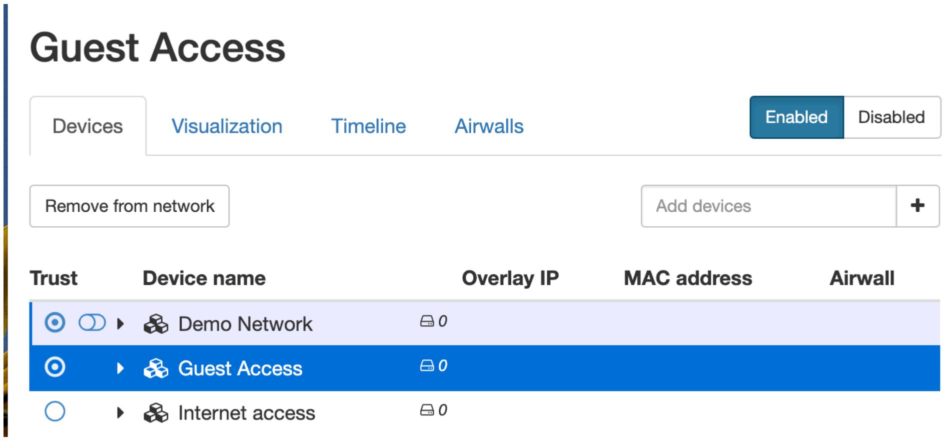
1. In your Conductor, go to the **Overlays** page.
2. Select **New overlay network**.
3. Under **Select Network Topology**, select **Manual** and click **Next**.

   For more information on other Network Topologies, see TBD.

4. On the **Create New Network** page, name the overlay `Guest Access`, and click **Finish**.
5. On the new `Guest Access` overlay page, by **Add devices**, click the plus sign (+).
6. Check the `Guest Access` group, and then also add the devices or device groups that you want guests to have access to and click **Add devices**.
7. Set trust between the `Guest Access` group and the devices you want them to have access to:
   a) In the **Trust** column, select the `Guest Access` radio button.
   b) Select the radio buttons for the devices guests can access.

   For more information on setting device trust, see Add and remove device trust on page 427.

In this example, the `Guest Access` group has access to the Demo Network but cannot access the Internet access group.



Trust	Device name	Overlay IP	MAC address	Airwall
◉	Demo Network	0		
◉	Guest Access	0		
○	Internet access	0		

You now have all of the pieces in place and are ready to send an invitation.

Step 4: Set up and send Airwall Invitations to guests

You can now create and send an invitation that automatically grants guest access to Airwall Agents and Servers connecting through that invitation.

1. In your Conductor, go to the **Airwalls** page.
2. Open the **Airwall Invitations** tab and click **Create Airwall Invitations**.
3. On the **Send Airwall Invitations** page, enter at least one email address for a guest, and click the Add icon ✓.
4. Click **Next**.
5. Add a name for the profile to create on the Guest's Airwall Agent or Server.
6. Under **Install package location**, enter a link for the Airwall Agent to install. You can link to the installation package for the type and version of Airwall Agents you want them to use, or link to the latest Airwall Software Downloads page here //webhelp.tempered.io/webhelp/content/topics/downloads_latest.html.
7. Check the **Conductor URL**. It should already be added by default.
8. Under **Activation code expiration date**, leave the default settings and click **Next**.

   Note: This is the expiration date for the invite only.
9. Under **Tags**, click the Edit icon ✎, and select the `Guest Access4hr` tag.
10. Click the **Add an entry** box to open the tag list again and choose `Guest Expired`. With both `Guest Access4hr` and `Guest Expired` tags in the list, click on the add icon ✓ .
11. Click **Next**.
12. Review, add, or edit the email addresses or the invitation.
13. To send the invitations, click **Finish**.

As people accept your invitations, they are automatically given access for 4 hrs, and then removed from all access. For more details on how it works, see How Expiring Access Works on page 73.

What to do next

With access being granted and revoked automatically, all that you need to do to give new guests access is send them an invitation using the invitation you just created as a template. What you can do now:

- **Manage your Guest Expired devices** – You will probably need to eventually manage your guest expired devices to free up licenses or give them additional access.
- **Reuse Guest Airwall Invitations** - You can also reuse the invitation you sent to quickly invite new guests. For more information, see Reuse Airwall Invitations.
- **Renew Guest Access** – You can renew guest access for an additional 4 hours by just retagging the person's device. For more information, see Renew Access for Guest Expired devices.

Manage Guest Expired devices

For your guests in the Guest Expired Device Group, you can:

- **Leave them alone** – Keep them in the GuestExpired group indefinitely (this holds the license for them).
- **Revoke access** – Airwall Agent or Server and return the license to your pool of available licenses. For more information, see Revoke Access for Guest Expired devices.
- **Renew access** – Tag them with the GuestAccess4hr tag again to give them 4 hours of access again. For more information, see Renew Access for Guest Expired devices.

Renew Access for Guest Expired devices

1. In your Conductor, go to the **Airwalls** page.
2. On the **Airwalls** tab, click the **Tags** column header to sort by Tags, and find the devices that are tagged with `GuestExpired`, but not `GuestAccess4hr`.
3. Check the box to select the Airwall you want to renew access for.
4. At the top of the page, select **Airwall actions**, and then **Edit Tags**.
5. Under **Add Tags to selected items**, click the box with **Add an entry**, select the `GuestAccess4hr` tag, and then click the check to add the tag.
6. Click **Update**. The access countdown begins again, giving the guest 4 more hours of access.

Revoke Access for Guest Expired devices

1. In your Conductor, go to the **Airwalls** page.
2. On the **Airwalls** tab, click the **Tags** column header to sort by Tags, and find the devices that are tagged with `GuestExpired`, but not `GuestAccess4hr`.
3. Check the box to select the Airwalls you want to revoke access for.
4. At the top of the page, select **Airwall actions**, and then **Revoke**.

To re-instate a revoked Airwall, check the **Display revoked Airwalls** box, check to select the revoked Airwall, select **Airwall actions**, and then **Re-activate**.

How Expiring Access Works

When people install Airwall Agents and Servers and accept **Airwall invitations** (clicking **Activate** in the email):

- Each person's Airwall Agent or Server is automatically added to both the `Guest Access` and the `Guest Expired` groups.
- Because the `Guest Access` tag takes priority, they are automatically added to the `Guest Access` Smart Device Group, and white listed to the devices or groups in your Guest Overlay for communication.
- The countdown for their 4 hr access starts.

When the 4 hrs is up, the `Guest Access` tag is automatically removed from the client, and the `Guest Expired` tag then takes priority and moves the Airwall Agent or Server to the `Guest Expired` smart device group, removing them from access to any overlay.

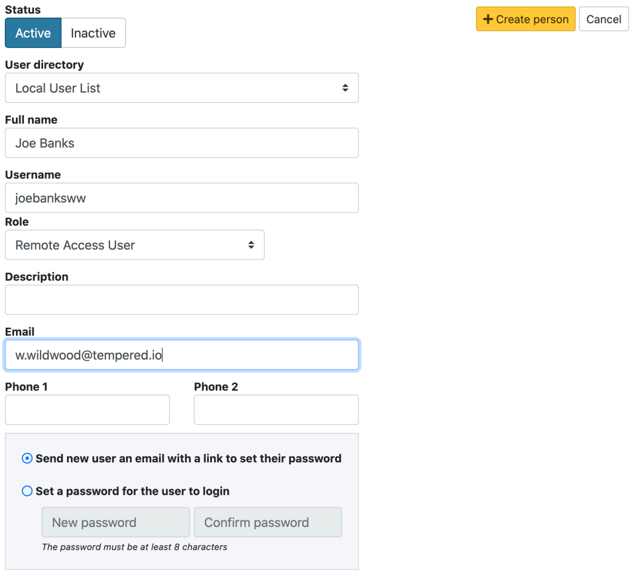
Connect People as Remote Access Users

You can create a remote access user to give a person access to your Airwall secure network using an Airwall Agent or Server. You can integrate with an LDAP user database, or add OpenID Connect authentication providers as shown in Integrate Third-party Authentication with OpenID Connect on page 247.

Set up remote access users to:

- Onboard users using membership in people groups (this gives them an activation code that they can click from the **Connect an Airwall agent** page)
- Authenticate a remote session on an Airwall Agent or Server
- Give users permission to view their connected Airwall Agent or Server status and see what remote devices they have access to (also via Connect an Airwall agent page)
- Enable and disable individual Airwall Agents and Servers authentication. For more information, see Walkthrough: Onboarding Users with User Authentication.

1. In Conductor, go to **People**, and select **New person**.
2. Fill in their details, and under **Role**, select `Remote Access User`.
3. At the bottom, choose whether to send the user a link to set their password, or create a password for them.



Status

Active | Inactive

User directory

Local User List

Full name

Joe Banks

Username

joebanksww

Role

Remote Access User

Description

Email

w.wildwood@tempered.io

Phone 1

Phone 2

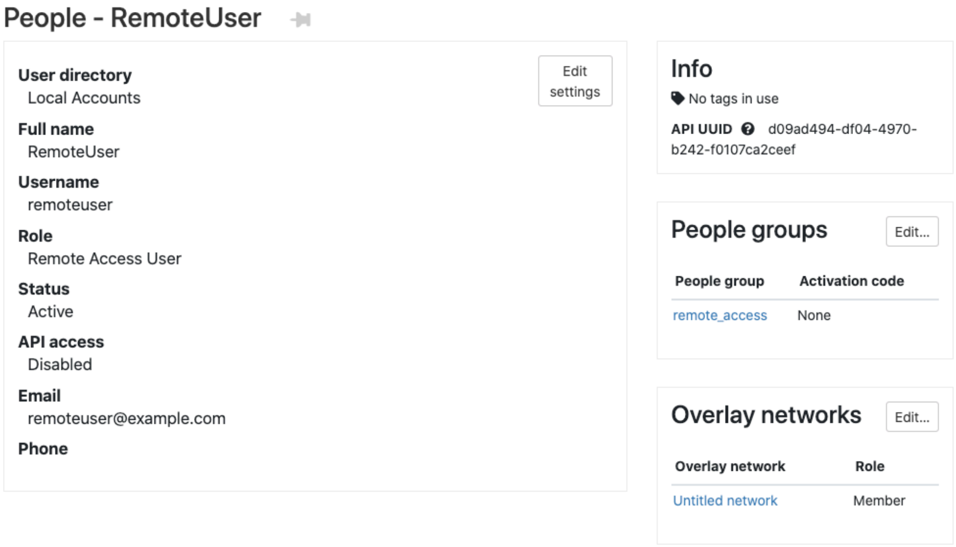
● Send new user an email with a link to set their password

○ Set a password for the user to login

New password | Confirm password

The password must be at least 8 characters

4. Select **Create person**.
5. **If you're onboarding users** – Add them to a user onboarding people group that provides them with an activation code. Then, once the user is logged in, they can download an Airwall Agent or Server, and activate their remote access. See Set up a People Group on page 89.
6. You can also add a person to an overlay from their **People** page.



People - RemoteUser

User directory
Local Accounts

Full name
RemoteUser

Username
remoteuser

Role
Remote Access User

Status
Active

API access
Disabled

Email
remoteuser@example.com

Phone

Info

No tags in use

API UUID d09ad494-df04-4970-b242-f0107ca2ceef

People groups

People group	Activation code
remote_access	None

Overlay networks

Overlay network	Role
Untitled network	Member

- **If you've sent the user a link to set their password**, they'll get an email with a link to set a password.
- **If you created a password for them**, you'll need to send them their password.
- To allow a remote access user to access your Airwall secure network with an Airwall Agent or Server, you'll have to send them an activation code, or an Airwall Invitation. See Connect People's Devices with Airwall Invitations on page 64 or Connect People's Devices with Activation Codes on page 75.

Connect People's Devices with Activation Codes

Connecting people's devices with Activation Codes is similar to using **Airwall Invitations**. The only difference is you distribute the Activation Code or Codes yourself rather than automatically sending emails.

You send Activation codes to invite people to connect to your Airwall secure network. It can be as simple as generating and distributing the Activation codes. With a bit of preparation, though, you can also automatically set up device access and trust as people connect their devices.

The possibilities include setting up which Overlay networks people belong to, what groups they're a part of, which Airwall Edge Services and devices they can access, and when a person's access to your Airwall secure network expires.

Before you begin

- Group people by the types of access permissions they need.
- (Optional) Create **Airwall groups** for the people you want to add. For example, you may want Employees and Contractors Airwall groups.
- (Optional) Create tags for the types of people and access.
- (Optional) Create Smart Device Groups to automatically add people to Device groups as they activate their Airwall Agents and Servers. See Manage devices dynamically with Smart Device Groups on page 105.

By doing a bit more planning and preparation in the optional steps above, you will save time in making sure people are able to access the resources they need.

1. Go to **Airwalls**, and open the **Airwall Invitations** tab.
2. ***If you have already created Activation Codes or Airwall Invitations with the details you need***, you can open the drop down next to an invitation and select **Use as Template** to send a similar invitation to more people. ***To create new Activation Codes***, select **New Airwall Invitations**, and select either **Download activation codes and distribute them manually** or **Download a single activation code that can be used many times**.
3. Enter the number of activation codes to generate, or how many times the single activation code can be used.
4. Select **Next**.
5. Enter the following options as needed. Setting these options automates more of the process for the people trying to connect:

- **Generated Airwall name** – Sets the name the Airwall Agent or Server has in the Conductor when the user activates it. The default value sets it to the Airwall Agent or Server type. See the help when you select this box to see other options for autogenerating names.
- **Activation codes should expire** – Check to have the activation codes expire
- **Activation code expiration date** – If you've checked the box above, sets the date the Airwall Invitation expires.

6. Select **Next**.
7. Enter additional settings to automate people's access as their devices connect:

- **Overlay device IP network (CIDR)** – (Optional) The network from which to assign IP addresses to devices as the connect.

  Note: If you use the same IP network in subsequent Invitations, IP addresses will keep incrementing. For instance, if you send out one Invitation starting at 192.168.1.15 with 10 emails and then another with the same IP with 10 emails they all just get a free IP from the network as they come online.
- **Overlay networks** – (Optional) The Overlay networks to add devices to.
- **Device groups** – Select the **Device groups** to add devices to.
- **Airwall groups** – Select **Airwall groups** to add devices to. For example, you might assign this group to the Employee, Admin, or Vendor group. Make sure this group has access to an Airwall Relay, if needed.
- **Tags** – Create or assign tags to people's devices. For example, if you're using tags to create Smart Device Groups that add people's devices to the right overlays, enter these tags now.

8. Select **Generate**.
9. Download or copy the Activation codes and distribute to the people you want to connect. To help your users receiving Activation codes to connect, point them to this help topic: I have an Activation Code on page 15.

To ensure people have access to the resources they need, add trust between their Airwall Agents and Servers and the resources they need to access on the overlays. And, if needed, add their devices to the Airwall Relay they'll use to access your Airwall secure network.

1. Add and remove device trust on page 427 on the Overlay between the device group for the people's Airwall Agents and the resources they need access to.
2. If needed, add the device group to any Relay rules they'll need to use to access resources. See Set Up an Airwall Relay on page 353.

Check Status of People Onboarding

You can check the status of people onboarding using Activation Codes or **Airwall Invitations** in the Conductor.

You can also run reports that show the overall status of your onboarding. See Run Network Activity Reports on page 116.

Check Activation Code Status

There are two ways to see the status of activation codes assigned to people from a People group:

On a person's detail page, look under **People** groups to see if they have unused activation codes from their People group membership.

On the **People** page, the far right column shows the following status icons. You can hover over the icons for additional details:

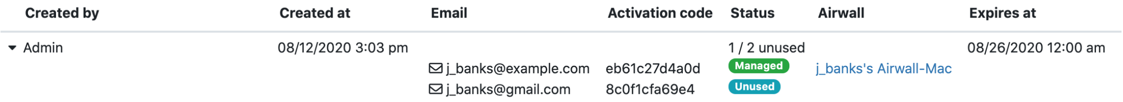
Icon	Meaning
👤	Authenticated user
🔌	Unused activation code
🔌	Expired activation code
🕒	Person logged in in the last 24 hours

Icon	Meaning
🕓	Person logged in last week
🕓	Person logged in more than a week ago
🕓	Person has never logged in

Check Airwall Invitations Status

You can check the status of **Airwall Invitations** you've sent on the Airwalls page, **Airwall Invitations** tab.

- Select the arrow to the right of the **Created by** column to expand the status of **Airwall Invitations** and Activation codes created by that administrator and see the email addresses invited to join your Airwall secure network.
- The **Status** column shows how many **Airwall Invitations** are used and unused, and when expanded, shows provisioned and unused activations by email address.
- When the invitation is expanded, the **Airwall** column shows the Airwall Agents and Servers activated for each activated email address.



Created by	Created at	Email	Activation code	Status	Airwall	Expires at
▾ Admin	08/12/2020 3:03 pm			1 / 2 unused		08/26/2020 12:00 am
		✉ j_banks@example.com	eb61c27d4a0d	Managed	j_banks's Airwall-Mac	
		✉ j_banks@gmail.com	8c0f1cfa69e4	Unused		

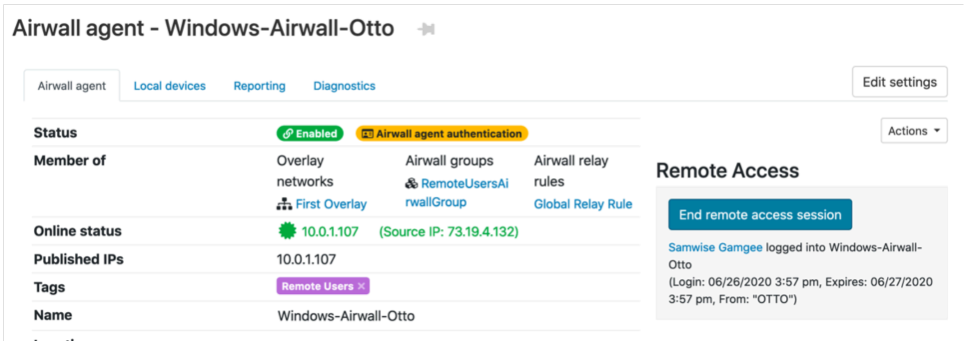
- The **Expires at** column shows how many **Airwall Invitations** are set to expire.

You can also select a **Filter by** tab at the top to filter by Unused, Managed, or Expired **Airwall Invitations**, or select **Refresh** to refresh the list..

Check Remote Sessions

You can check the status of Airwall Agent remote sessions in these ways:

- On the Conductor page for a specific Airwall Agent, look under Remote Access:



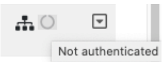
Airwall agent - Windows-Airwall-Otto

Status	Enabled Airwall agent authentication
Member of	Overlay networks First Overlay Airwall groups RemoteUsersAirwallGroup Airwall relay rules Global Relay Rule
Online status	10.0.1.107 (Source IP: 73.19.4.132)
Published IPs	10.0.1.107
Tags	Remote Users ×
Name	Windows-Airwall-Otto

Remote Access

Samwise Gamgee logged into Windows-Airwall-Otto (Login: 06/26/2020 3:57 pm, Expires: 06/27/2020 3:57 pm, From: "OTTO")

- The People page for a person shows details they are logged in.
- On the right side of the Airwall Edge Services list view, hover over the circle icon to see who's authenticated or Not authenticated. (Note that this icon only appears for Airwall Edge Services with authentication required.)



Here are some other icons that indicate status:

Icon	Meaning
🔌	Unused activation code
🔌	Expired activation code

Icon	Meaning
🕓	Person logged in last week
🕓	Person logged in more than a week ago
🕓	Person has never logged in

Install Airwall Agents and Servers

Select your device for detailed installation instructions.

Once you've installed an Airwall Agent or Server, see Connect to an Airwall secure network on page 19.

Microsoft Windows or Windows Server: Install and configure an Airwall Agent or Server

If you have received an email or activation code, see Link my Airwall Agent or Server to an Airwall secure network on page 14. If you need to install and configure manually, follow these instructions. You can get the Airwall Agent or Server for Windows from the administrator of your Airwall secure network, or download the latest installation files from Latest firmware and software on page 514. Once installed, you configure a profile on the Airwall Agent or Server to link to the Airwall secure network.

Note: You can start and stop the Airwall Agent or Server service as needed. Keep in mind when an Airwall Agent or Server service is stopped, you cannot connect to anything on the protected network.

To install and configure the Windows Airwall Agent or Server:

1. Log into your Windows computer as an administrator.
2. Download and install the Windows Airwall Agent or Server from Latest firmware and software on page 514.

   Note: If you are asked to install the TAP-Windows Provider as part of the installation procedure, click **Install** when prompted.
3. Once the installation is complete, the Airwall Agent or Server starts automatically.
4. Right-click the Tempered icon in the Windows System Tray
5. Select **Configure**
6. In the **Configure** window, do the following:
   a) Enter the IP address or host name of your Conductor. The default port setting is *8096*. If you have an activation code, enter it here.

      Note: The **Device ID**, **Overlay Device IP**, and **Overlay Netmask** fields are read-only and configurable from the Conductor.

   b) Click **OK**.

If you have used an Airwall Invitation or Activation code, once the Airwall Agent or Server is recognized by the Conductor, you should be able to start connecting to protected resources. If you are connecting manually, send your Device ID to your administrator so they can activate your account.

For information on using your Windows Airwall Agent or Server, see Connect with a Windows Airwall Agent or Server on page 27.

Note: You may need to stop and restart the Airwall Agent or Server to allow it to connect to the Conductor. Right-click the Tempered icon in the Windows System Tray and select **Stop** to suspend the service or **Start** to resume.

Unattended Windows installation of an Airwall Agent or Server

In v2.0 and above, you can install the Windows Airwall Agent or Server in unattended mode as an Administrator.

To do an unattended install of the Windows Airwall Agent or Server you use an .msi file. This method runs the regular installer in silent mode, allowing you to do a silent install through domain (GPO, SCCM).

Here's the recommended command to use to do the unattended install:

```
msiexec /i <msi_file> /l*v msi_out.log InvitationCode="<invite_code>"
 Conductor="<conductor_URL>"
```

For example:

```
msiexec /i AirwallAgent64-bit_UnattendedInstaller_2.2.11.333.msi /
l*v msi_out.log InvitationCode="575a52703294" Conductor="https://
my.conductor.com:8096"
```

Note: If you are not using DNS, you can replace the Conductor entry with its IP address. For example:

```
msiexec /i AirwallAgent64-bit_UnattendedInstaller_2.2.11.333.msi /
l*v msi_out.log InvitationCode="575a52703294"
 Conductor="https://192.168.56.2:8096"
```

Apple (OSX and macOS): Install and configure an Airwall Agent

If you have received an email or activation code, see Link my Airwall Agent or Server to an Airwall secure network on page 14. If you need to install and configure manually, follow these instructions. You must be an administrator of the computer to install and configure the Airwall Agent.

Note: Download the macOS/OSX installation files from the Software Downloads and Release Notes on page 514 Software Downloads section of Airwall help.

Important: In v2.2 and earlier, you may be required to install a TAP device driver. In earlier versions, the TAP driver's certificate may display a developer other than Tempered. If this occurs, you can safely click **Allow** and continue with your installation.

Once the installation is complete, the application starts automatically.

To install and configure manually:

1. To install the Airwall Agent locate the files you downloaded, double-click on them to run the installer, and follow the prompts.
2. Left-click the Tempered icon in the macOS menu bar.
3. Select **Configure**.
4. On the **Airwall Configuration** page, do the following:
    a) Select the plus (+) to add a new profile.
    b) Under **Conductor**, enter the IP address or host name of your Conductor.
    c) Under **Port**, use the default port setting of *8096*, unless your Airwall secure network administrator has told you to use a different port.
    d) If you have an Activation code, under **Invitation**, enter the code. If you do not have a code, copy down or screenshot your **Device ID** and send to your administrator to activate your account.

    Note: **Device ID**, **Overlay Device IP** and **Overlay Netmask** are read-only and configurable from the Conductor.

    e) Select **Save**.

If you have used an Airwall Invitation or Activation code, once the Airwall Agent is recognized by the Conductor, you should be able to start connecting to protected resources. If you are connecting manually, send your Device ID to your administrator so they can activate your account.

Note: You may need to stop and restart the Airwall Agent to allow it to connect to the Conductor. Left-click the Tempered icon in the menu bar and select **Stop Airwall** to disconnect or **Start Airwall** to connect.

For information on using your macOS Airwall Agent, see Connect with an Apple (OSX and macOS) Airwall Agent on page 19.

Perform an unattended macOS installation of an Airwall Agent

In v2.0 and above, you can perform a silent install on the Airwall Agent for macOS.

Note: This action requires administrator rights on the device.

To perform a silent install of the Mac client, from a terminal window, navigate to the location of the Airwall Agent installer package, and enter the command below:

```
sudo installer -pkg ./TemperedNetworksHIP.pkg -target /
```

Set your preferred network in the macOS Airwall Agent (HIPclient-OSX)

The macOS Airwall Agent (HIPclient-OSX) no longer uses the Network option, but instead automatically uses the network preferences on your macOS system settings.

Note: This action requires administrator rights on the device.

You can change the networks used by the agent by changing your macOS system settings.

Note: This setting is a system-wide setting, and affects network preferences for your entire mac system.

1. On your mac, click the WiFi icon, and select **Open Network Preferences**.
2. Under the list of available networks, click the gear icon, and select **Set Service Order**.
3. Drag the network options to set the network order you prefer, and then click **OK.**

2.2.3 macOS Airwall Agent Upgrade Instructions

If you have a previous version of the macOS/OSX Airwall Agent (formerly HIPclient) installed, follow these instructions to upgrade to 2.2.3:

Note: This action requires administrator rights on the device.

1. Check if you have this file on your Mac: /Applications/TemperedNetworksHIP.app. If not, you can upgrade as normal. If it is there, continue to step 2.
2. In your current Airwall Agent (HIPclient) menu, select **Configure**.
3. Note the Device ID and Conductor URL for each profile.
4. Go to the **About** menu, and select **Uninstall**.
5. Install the 2.2.3 macOS Airwall Agent.
6. Add a new profile for each of the Conductor URLs noted in Step 3. These new profiles will create new provisioning requests for each profile in the Conductor.
7. For the new profiles, a Conductor administrator needs to replace the old profiles with the new profiles. For more details, see Replace an Airwall Edge Service.

Apple iOS: Install and configure an Airwall Agent

If you have received an email or activation code, see Link my Airwall Agent or Server to an Airwall secure network on page 14. If you need to install and configure manually, follow these instructions. You can get the Airwall Agent for iOS from Apple's App Store.

Note: If you received an invite, follow the instructions in the email to install and configure your Airwall Agent. The instructions below are for manual installation and configuration.

1. Install the Airwall Agent on your device from the Apple Store: https://itunes.apple.com/US/app/id1233852249.
2. Open the Apple iOS Airwall Agent.
3. From the menu, tap **Profiles**. Tap + to add a new profile.
4. Give the profile a name, and fill in the Conductor URL (and port, if provided to you).
5. If you have an Airwall Invite Code, enter it at the bottom.
6. Tap **ADD**.

If you have used an Airwall Invitation or Activation code, once the Airwall Agent is recognized by the Conductor, you should be able to start connecting to protected resources. If you are connecting manually, send your Device ID to your administrator so they can activate your account.

For information on using your Apple iOS Airwall Agent, see Connect with an iOS Airwall Agent on page 21.

Android: Install and configure an Airwall Agent

If you have received an email or activation code, see Link my Airwall Agent or Server to an Airwall secure network on page 14. If you need to install and configure manually, follow these instructions. You can get the Airwall Agent for Android from the Google Play Store. Once installed, you configure a profile on the Airwall Agent to link to the Airwall secure network.

Note: If you receive an invite, follow the instructions in the email to install and configure your Airwall Agent. These instructions are for manual installation and configuration.

1. Install the Airwall Agent on your device from the Google Play store: https://play.google.com/store/apps/details?id=com.temperednetworks.hipclient
2. Open the Android Airwall Agent.
3. Add a new profile:
   - **v3.0 and later** – Scroll down to **Select Profile**, tap **MANAGE**, and then tap +.
   - **v2.2.12 and earlier** – From the menu, tap **Profiles**, and then tap +.
4. Give the profile a name, and fill in the Conductor URL (and port, if provided to you).
5. If you have an Airwall Invite Code, enter it.
6. Tap **ADD**.

If you have used an Airwall Invitation or Activation code, once the Airwall Agent is recognized by the Conductor, you should be able to start connecting to protected resources. If you are connecting manually, send your Device ID to your administrator so they can activate your account.

For information on using your Android Airwall Agent, see Connect with an Android Airwall Agent on page 22.

Linux: Install and configure an Airwall Server

If you have received an email or activation code, see Link my Airwall Agent or Server to an Airwall secure network on page 14. If you need to install and configure manually, follow these instructions. You can get the Airwall Server for your Ubuntu, Centos, or Fedora Linux server from the administrator for your Airwall secure network, or from Latest firmware and software on page 514. Once installed, you configure a profile on the Airwall Agent to link to the Airwall secure network.

Note:

- For pre-3.0 versions, replace `airsh` with `airctl`. See airctl Reference (pre-v3.0) on page 10.
- For pre-2.2.3 versions, see pre-2.2.3 help.

1. Install the Linux Airwall Server package for your version of Linux. If your secure network administrator has not provided you with a download, you can download the package you need from Latest firmware and software on page 514.
   - **For CentOS 7 or 8 or Fedora 3.3**: `sudo rpm -i <CentOS or Fedora install package>`
   - **For Ubuntu 16.04, 18.04, or 20.04**: `sudo dpkg -i <Ubuntu 16 or 18 package>`
2. Create a profile: `sudo airsh profile create name=<profile name> conductor=<conductor_url> [act=activation_code]`.

   You can optionally enter an Airwall Invitation activation code.
3. Make a profile the active one: `sudo airsh profile activate <profile name or number>`
4. Start the service: `sudo airsh service start`.

   Note: If the service is already running, enter `sudo airsh service restart` to stop and start the service.

If you have used an Airwall Invitation or Activation code, once the Airwall Server is recognized by the Conductor, you should be able to start connecting to protected resources on the Airwall secure network. If you are connecting manually, send your Device ID to your administrator so they can activate your account.

For information on getting your Device ID, or using your Linux Airwall Server, see Connect with a Linux Airwall Server on page 26. For more Airshell commands, see Linux Airwall Server Airshell commands on page 372.

Linux Airwall Server or macOS Airwall Agent interface selection

The Linux Airwall Server and macOS Airwall Agent implement an interface auto-selection method. When you first install the Airwall Agent or Server, Linux or macOS determines the default gateway of the host and uses the associated network interface.

Note: Auto-selection is per profile.

Troubleshooting

If your macOS Airwall Agent is reporting as *online*, but does not seem to be working, check that the correct network interface is selected in the profile. See Set your preferred network in the macOS Airwall Agent (HIPclient-OSX) on page 80.

From Tkee: Linux agent conforms to the Gateway link manager operational rules. airsh currently does not have the ability to select the preferred uplink. Conductor is the method for selecting interfaces by port group weights. Short on details, the Gateway documentation might serve as a basis. Ticket to fill this in CD-412.

Allow an Airwall Agent or Server to access your Airwall secure network

When a person configures an Airwall Agent or Server with your Conductor IP address or hostname, and are online with access to the **Conductor**, their Airwall Agent or Server will appear in the Conductor. How they appear depends on how they've connected:

- If they've activated their Airwall Agent or Server with an Airwall Invitation or Activation code, their Airwall Agent or Server is provisioned and configured as you specified when you set up the invitations or activation codes. You just need to license their Airwall Agent or Server and they will have access to the secure network.
- If the person is connecting manually, you get a provisioning request to allow the Airwall Agent or Server into your secure network. You need to provision and licensed the Airwall Agent or Server, and then add the person's device to the overlay networks and Add and remove device trust on page 427 for the resources they need access to.

  CAUTION: When you're accepting provisioning requests, make sure that you know who is connecting and they are authorized to access your network.

If you need to revoke an Airwall Agent or Server, you can also disable trust in one click. For more information, see Revoke and Reactivate an Airwall Edge Service on page 496. Open the **Visualization** tab on an overlay network to get a visual view of trust relationships.

Note: You can also automate Airwall Agent trust using the API. The most recent API documentation is available in your Conductor. See Airwall API on page 508.

Manage Airwall Agents through an MDM (Mobile Device Management) solution

If you are using an MDM solution to manage devices for your organization, you can push installation and configuration of Airwall Agents to your managed devices.

The Airwall Solution currently supports managed configuration for Android Airwall Agents.

When you manage Airwall Agents with an MDM, the MDM can:

- Install the Airwall Agents on your managed devices.
- Create Airwall Agent profiles for your Conductor.
- Automatically start the Airwall Agent, which then reads the profile and connects to the Conductor.

The Airwall Agent prevents users from making any changes to a managed profile.

You can also distribute Activation codes through the MDM, or as Airwall Agents connect, you can grant the provisioning requests and manage the devices in the Conductor.

Before you begin:

- **Add the Tempered Airwall Agent to your MDM solution** – Follow the instructions for your MDM to load the Airwall Agent managed configuration. The values you can enter should be Profile Name, Conductor url, Port number, and Invite code. If you need to select the value type, set it to `strings`. All values are mandatory except for the invite code.
- **(Optional) Generate Activation Codes and put into your MDM solution** – To automatically provision users, generate Activation codes for the Airwall Agents you want to manage. To generate Activation codes, see Connect People's Devices with Activation Codes on page 75. To add these to your MDM solution, see your MDM instructions.
- **(Optional) Set up Dynamic variables in your MDM** – If you want to use dynamic variables in your profile names, set them up in your MDM following the instructions for your MDM.

Configure the managed profile for your Airwall Agents

These instructions are a rough guide and may vary depending on your MDM solution. See your MDM help for more detailed instructions.

1. In your MDM, open up the managed configuration for the Airwall Agent.
2. Configure and save the following values for the Airwall Agent profile:
    - **Profile name** – Enter the profile name you want your Airwall Agent profiles to have. If supported by your MDM , you can use dynamic variables to create profiles unique for each user.
    - **Conductor URL** – Enter your Conductor URL or hostname.
    - **Conductor Port** – Set the port default to 8096.
    - **Activation code** – (Optional) If you have set these up and it is supported by your MDM, enter a dynamic variable to insert each user’s Activation code.
3. Save the profile, and save the configuration in your MDM.
4. Save and apply the managed configuration to managed devices following the instructions for your MDM solution.

You can change the profile information, except for the profile name, in the same way if you need to make changes to the managed profiles. If you change the profile name, the MDM creates a new profile on the Airwall Agents.

Automate the Airwall Agent or Server and Airwall Server using the API

Walkthrough - Onboard people to your Airwall secure network with User Authentication

How to set up global user/password authentication for Airwall Agents and Servers connecting to your Airwall secure network.

This walkthrough walks you through setting up authentication for all people connecting to your Airwall secure network.

Note: This walkthrough covers globally onboarding people with authentication. You can also turn on authentication for individual Airwall Agents and Servers.

Supported Versions	Conductor v2.2.10 and later. This walkthrough is based on v3.0, so some things may be slightly different on earlier versions.

The basic steps are:

1. Require User authentication globally.
2. Onboard people using People Groups.
3. Add people as Remote Access Users.

These steps are covered in more detail below.

Note: For pre-2.2.8 Airwall Agents and Servers only: There is an extra step to provide access at the end of this walkthrough.

Best Practice:

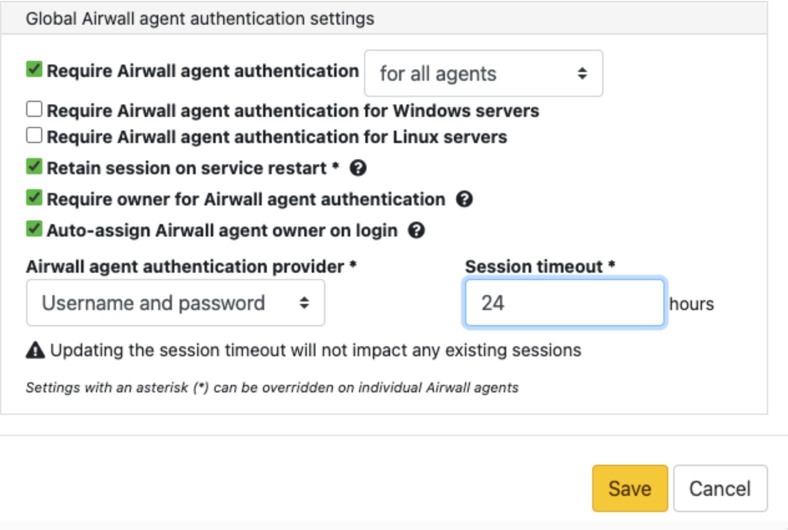
Finding the right balance between ease of use and security is an ongoing challenge.

This walkthrough shows how you can easily onboard and provide trust to a person, but you may choose to keep additional security checks in place, like granting the provisioning request based on the Device ID a person gives you.

A balanced option might include automatic onboarding, but only granting trust to a benign device that they can ping for communication verification and then provide final trust to secure environments once information has been verified verbally.

Step 1: Require user authentication globally

1. Go to **SettingsAuthentication**, and under **Settings**, select **Edit Settings** (in pre-v3.0, this is under **Global Airwall agent authentication settings**).
2. Check or set your authentication options:
   - Check **Require Airwall agent authentication** and select the option `for all agents`.
   - Under **Airwall agent authentication**, under **Airwall Agent Authentication Provider**, select `Username and password`, or an OpenID Connect (OIDC) third-party authentication provider, if you've set it up. See Integrate Third-party Authentication with OpenID Connect on page 247.
   - (Optional) You can also set a custom Session timeout or whether people need to log in when they restart their Airwall Agent



Global Airwall agent authentication settings

☑ **Require Airwall agent authentication** — for all agents

☐ **Require Airwall agent authentication for Windows servers**

☐ **Require Airwall agent authentication for Linux servers**

☑ **Retain session on service restart ***

☑ **Require owner for Airwall agent authentication**

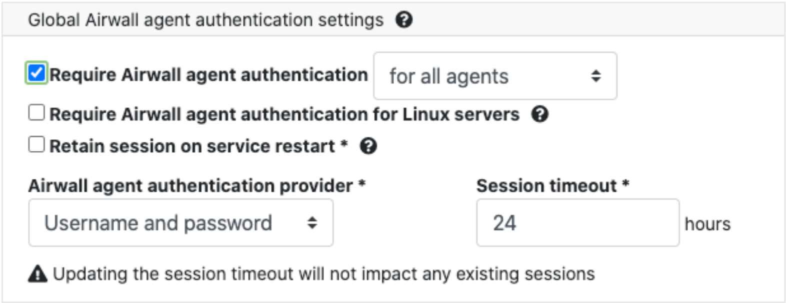
☑ **Auto-assign Airwall agent owner on login**

Airwall agent authentication provider *: Username and password

Session timeout *: 24 hours

⚠ Updating the session timeout will not impact any existing sessions

Settings with an asterisk (*) can be overridden on individual Airwall agents



Global Airwall agent authentication settings

☑ **Require Airwall agent authentication** — for all agents

☐ **Require Airwall agent authentication for Linux servers**

☐ **Retain session on service restart ***

Airwall agent authentication provider *: Username and password

Session timeout *: 24 hours

⚠ Updating the session timeout will not impact any existing sessions

For more information, see Configure Authentication Options on page 242. You can also require authentication per device on the Airwall Agent or Server page.

Step 2: Onboard People using People Groups

You may also want to Import people using a CSV file on page 61.

1. Set up a People Group on page 89, configuring the onboarding options you want to this People group to have. You can add people on the **People** tab, or add them to the group as you create users in the Conductor.

2. On the **User onboarding** tab:
    - Check **Provide an activation code for each member**.
    - Check **Send onboarding email to users** if you want to send emails automatically.
    - Pre-configure the **General**, **Airwall**, and **Groups** settings for users when they onboard. Setting these options allows members of the group to activate their connections. For more information, see Connect People's Devices with Activation Codes on page 75.

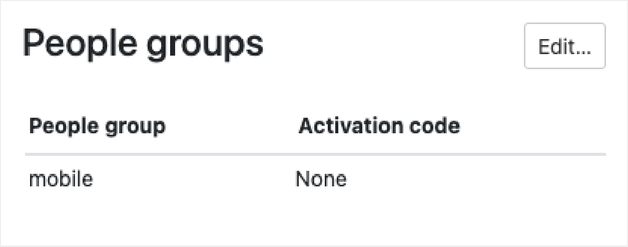
Note: If you want to configure which version of the Airwall Agent they download, you can set that on the Conductor **Settings** page under **Global Airwall agent settings**.

On the People Groups page, you will see your new group, and to the right, you will see the Activation Code icon 🔌 that indicates every person added to this group will receive an Activation Code. For more information, see Connect People’s Devices with Airwall Invitations on page 64 or Connect People's Devices with Activation Codes on page 75.

Step 3: Add Remote Access Users

1. Add the people you want to connect to the Conductor. For Remote Access Users, see Connect People as Remote Access Users on page 74.
2. As you save each user, from each person's **People** page, add users to the people onboarding group created in Step 2.

    a) Under **People groups**, select **Edit**.



People groups

People group	Activation code
mobile	None

    b) Select the onboarding People group created in Step 2.

3. The people are sent an onboarding email. If desired, you can send them custom instructions, or point them to one of these help topics: I have a "Finish Setting up my account" email on page 15 or I have an Activation Code on page 15.
   As people click the link in the email to set their password and log in to the Conductor, they'll be directed to the **Connect an Airwall Agent** page where they can install an Airwall Agent or Server and activate their connections.

What's Next

You can get a report on remote sessions from **Visibility** > **Reports**. For more information, see Run Network Activity Reports on page 116.

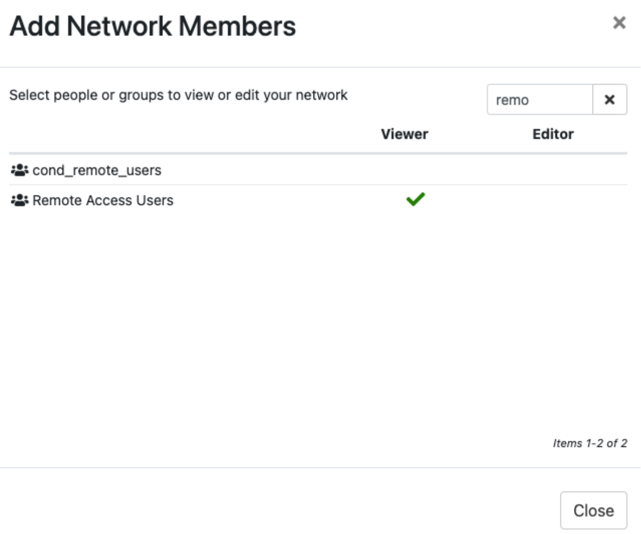
You can see who's remotely logged into your Airwall secure network. See Check Remote Sessions on page 77.

You can also see which users have used their Activation codes. See Check Status of People Onboarding on page 76.

For pre-2.2.8 Airwall Agents and Servers only) Give the People group access

If you are onboarding people using pre-2.2.8 Airwall Agents and Servers you need to give the People group access by adding them to Overlays and Relay Rules.

On the Overlay these people need to access, add the People group you created as a **Viewer** (or pre v3.0, as a **Member**).



Add Network Members

Select people or groups to view or edit your network

remo

	Viewer	Editor
cond_remote_users		
Remote Access Users	✓	

Items 1-2 of 2

Troubleshoot the Airwall Agent and Airwall Server

Follow the instructions below to resolve problems you may encounter using the software.

The Airwall Agent is not connected.

- Determine if the Conductor IP is configured. Follow the steps in the configuration section above.
- Verify that the Airwall Agent has not been given a certificate. Your administrator must grant a license in the Conductor. See the Conductor and Airwall Edge Service Administrator Guide for more information.

The Airwall Agent cannot contact a protected device

Configure the peer Airwall Gateway with an overlay network IP address and reestablish trust.

Customize People's Access to your Airwall secure network with People Groups

Using people groups, you can control what the people in the group can see and use on the Conductor, including cloud providers, Airwall Gateways, and Overlay networks and resources.

This control allows you to host several departments or customers on a single Conductor, where they have control over their own networks and access, but cannot see other networks or resources that are hosted on the Conductor.

Supported versions	• v3.1.0 Conductors • All Airwall Edge Services
Supported Roles	To set access with People groups, you must be a system administrator

You can give People groups access to Airwall Edge Services in two ways:

- Give members of the people group access directly by adding Airwall Edge Services to the Airwall permissions tab when creating or editing the people group.
- Set the people group as the permissions scope of a smart device group (SDG), so only devices from those Airwall Edge Services can be added to the SDG.

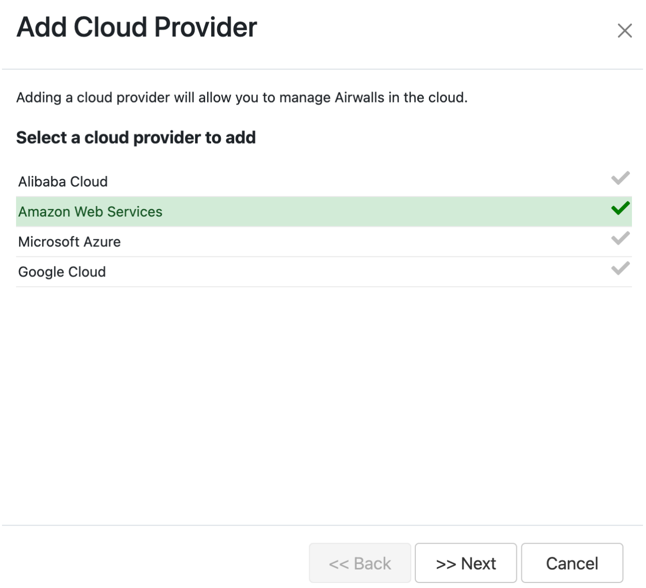
To support least-privileged access, you can set finer controls on what users have access to:

- Lock an Airwall Edge Service on page 94
- **Remove permissions to Relay rules** – This option can be important for privacy on a shared Conductor.
- **Limit the permissions scope for Smart device groups**

- Manage Tag Ownership on page 104 – In v3.1.0, tag ownership is more restrictive by default. If a system administrator creates a tag, then by default, only system administrators can see or use them. If a network administrator creates a tag, ownership defaults to only them or their people group, and system administrators.

Give Access to Cloud Providers with People Groups

1. In the Conductor, go to**People**, and open the**People groups** tab.
2. Open an existing people group, or select **New People Group** to create a new one.
3. Open the **Cloud providers** tab.
4. Select **Add Cloud provider**.
5. Select the cloud provider on which you'd like this people group to be able to create and manage Airwall Gateways on your Airwall secure network.
6. Select **Next**.



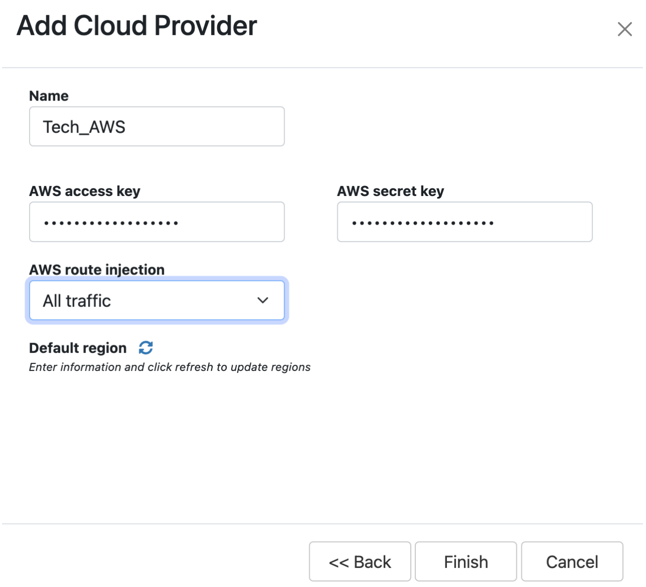
Add Cloud Provider

Adding a cloud provider will allow you to manage Airwalls in the cloud.

Select a cloud provider to add

Alibaba Cloud ✓
Amazon Web Services ✓
Microsoft Azure ✓
Google Cloud ✓

7. Enter a name and the credentials for the selected cloud provider.



Add Cloud Provider

Name
Tech_AWS

AWS access key
•••••••••••••••••••

AWS secret key
••••••••••••••••••••

AWS route injection
All traffic

Default region
Enter information and click refresh to update regions

8. Select the **Cloud route injection** option and **Default region** for this people group to use.

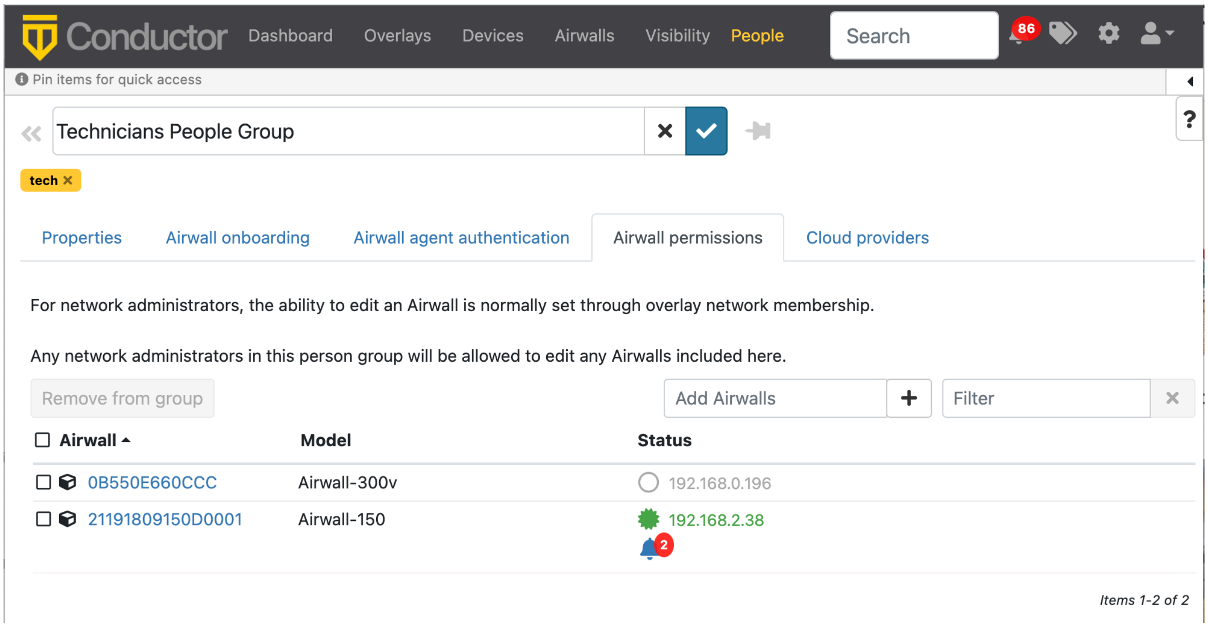
9. Select **Finish**.

The members of this people group can now manage and create Airwall Gateways on the added cloud provider.

Note: If you want to add additional cloud providers to this people group, repeat these steps for each cloud provider you want to give access to.

Give Access to Airwall Edge Services with People Groups

1. In the Conductor, go to**People**, and open the**People groups** tab.
2. Open an existing people group, or select **New People Group** to create a new one.
3. Open the **Airwall permissions** tab.
4. In the **Add Airwalls** box, enter a search term, or select the + to choose which Airwall Edge Services you want the members of this people group to have access to.



For network administrators, the ability to edit an Airwall is normally set through overlay network membership.

Any network administrators in this person group will be allowed to edit any Airwalls included here.

□ Airwall ▴	Model	Status
□ 0B550E660CCC	Airwall-300v	○ 192.168.0.196
□ 21191809150D0001	Airwall-150	192.168.2.38 2

Items 1-2 of 2

5. Select **Finish**.

Give Access to Overlay networks and Resources

You can give access to overlay networks and resources using people groups. When you give the people group the user role on an overlay network, the members of the group can use the overlay to add and remove devices and change trust, but they cannot edit the overlay network configuration and they do not gain permissions to edit the Airwall Edge Service in the overlay network. For more information, see Overlay network access roles on page 88.

1. Create a people group and add the people you want to be able to see an overlay network in the Conductor.
2. Create or open an ∫ network.
3. On the right, under **Network members**, select **Update**.
4. On the **Add network members** page, for the people or people group you want to give user access to, check the **Users** column.
5. Select **Close**.
   The selected people or people group now can add and remove device groups and change trust policy on the overlay network.

Overlay network access roles

There are several roles people can have on an overlay network. Refer to this table for what overlay permissions each role grants.

Overlay Permissions	Overlay Role		
	Viewer	User	Editor
View the overlay	X	X	X
Add and remove devices		X	X
Change trust policy between devices		X	X
Edit overlay network configuration			X
Edit Airwall Edge Services in the overlay network.			X

Set up a People Group

Set up a people group to make it easier to manage the people accessing your secure network.

Using a People Group, you can configure the User onboarding options, including Profile name, Conductor, and Airwall Gateways and resources these people have access to.

Note: If you are combining people groups with a third party authentication service such as LDAP or OIDC, you manage permissions in that service with group membership.

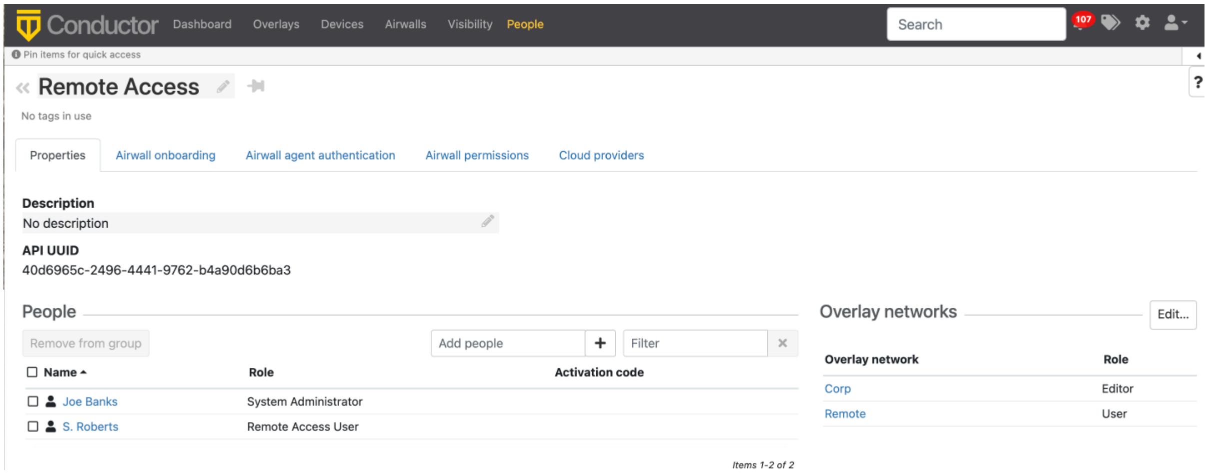
What you can do with People groups:

- **Manage trust** – You can assign trust dynamically to a people group using tags and a smart device group, or use the tag applied to Airwall Agents and Servers used by people in the group to easily find devices to add to a device group directly.
- **Onboard users** – You can use the **User onboarding** tab to send **Airwall Invitations** to people in the group and as they are added to the group. (You can also send invitations from the **Airwalls** page to the people currently in the people group).
- **Set Overlay network permissions** – Use the people to set overlay network editors and viewers.
- **Set groups to get alerts** – Send event monitor alerts to a people group.
- **Manage groups coming in from a third-party OIDC authentication provider** – Create people groups in the Conductor that exactly match the groups on your authentication provider to automatically add members of the group in the authentication provider to the group in the Conductor.

For more information on the types of users, see Understand People Roles and Permissions on page 58 or Understand People Roles (v2.2.13 and earlier) on page 60.

1. In Conductor, go to **People**>**People groups**.
2. Select **New People Group**.
3. Set a name for this people group and add a description or tags, if desired.

   Setting up a group for Third-party authentication: If you are managing people groups with a third-party authentication service, make sure the people group name matches your group on that service. Then, when you add people on that service, they are included in the people group when they log in.
4. Select **Create**.
5. ***If you are using a Third-party Authentication service, skip the rest of this procedure.*** On the **People groups** page, open the People group you just created.
6. Under **People**, select **Add people** and select the people you want to be a member of this group.



Remote Access

No tags in use

Properties | Airwall onboarding | Airwall agent authentication | Airwall permissions | Cloud providers

Description
No description

API UUID
40d6965c-2496-4441-9762-b4a90d6b6ba3

People

Remove from group | Add people + | Filter

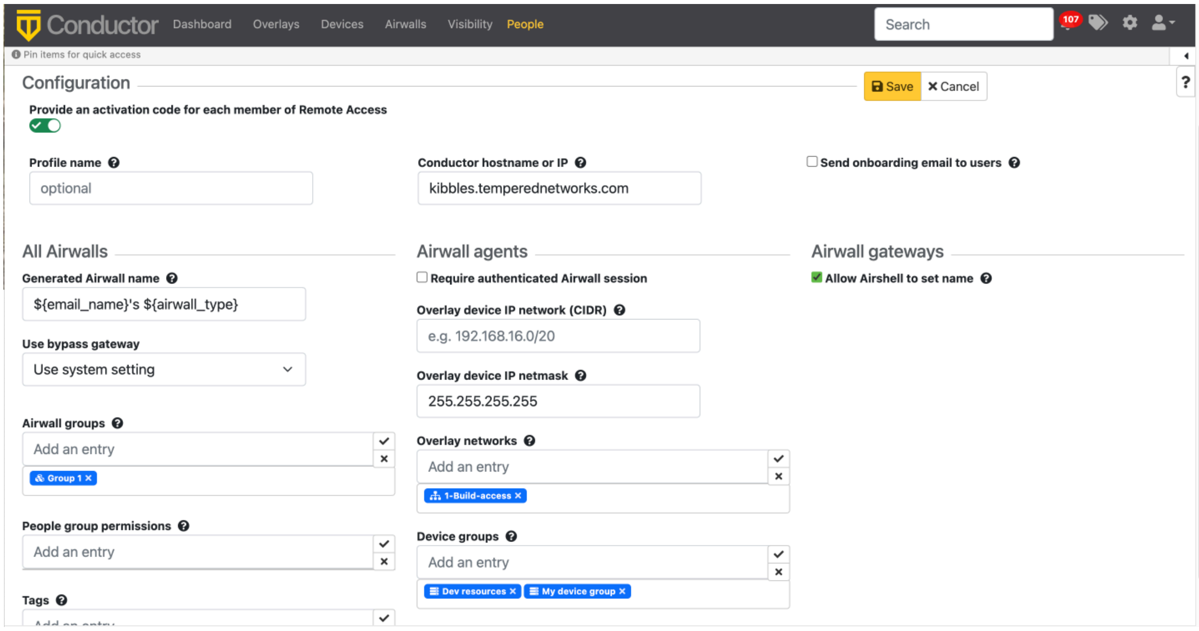
Name	Role	Activation code
□ Joe Banks	System Administrator	
□ S. Roberts	Remote Access User	

Items 1-2 of 2

Overlay networks — Edit...

Overlay network	Role
Corp	Editor
Remote	User

7. If you are using this group to onboard users, open the **Airwall onboarding** tab.
8. Next to **Configuration**, select the pencil icon ✎ to edit.
9. Check **Provide an activation code for each member of <groupname>**, and then set up how to onboard the users added to this group:



Configuration

Provide an activation code for each member of Remote Access ●

Profile name: optional

Conductor hostname or IP: kibbles.temperednetworks.com

□ Send onboarding email to users

All Airwalls

Generated Airwall name: ${email_name}'s ${airwall_type}

Use bypass gateway: Use system setting

Airwall groups: Add an entry — Group 1 ×

People group permissions: Add an entry

Tags: Add an entry

Airwall agents

□ Require authenticated Airwall session

Overlay device IP network (CIDR): e.g. 192.168.16.0/20

Overlay device IP netmask: 255.255.255.255

Overlay networks: Add an entry — 1-Build-access ×

Device groups: Add an entry — Dev resources × | My device group ×

Airwall gateways

☑ Allow Airshell to set name

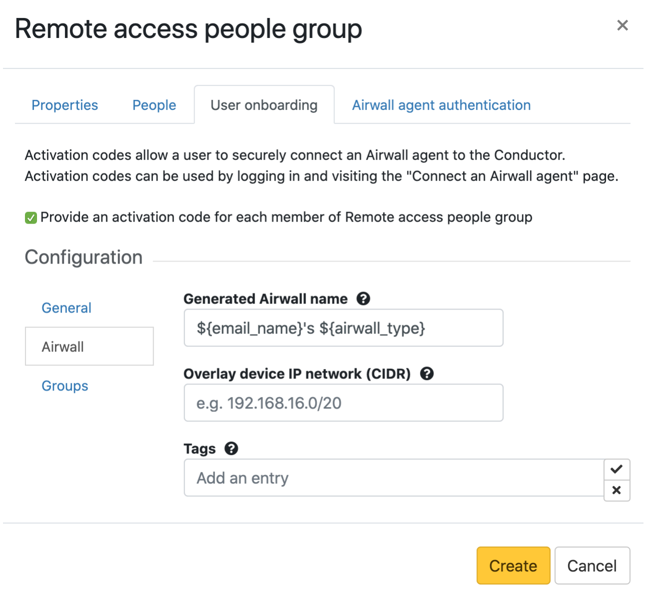
a) Under **Configuration**:

- **Profile name** – Set the name of the profile created on the Airwall Agent or Server for the user.
- **Conductor hostname or IP** – Enter the Conductor hostname or IP.
- **Send onboarding email to users** – Check to send new users of the group a notice that they have an activation code to connect.

b) Under **All Airwalls**:

- **Generated Airwall name** – Set the name to assign to the Airwall Agent or Server in the Conductor when the user activates it. The default value sets it to the Airwall Agent or Server type. See the help when you select this box to see other options for autogenerating names.
- **Use bypass gateway** – Select the bypass gateway you want this group to use.
- **Airwall groups** – Select the **Airwall groups** to add people's devices to. For example, you might assign this group to the Employee, Admin, or Vendor group.
- **People group permissions** – Automatically add Airwall Agents and Servers to these people groups when activated. This option gives members of the group editor rights to the Airwall.

- **Tags** – Create or assign tags to people's devices as they connect. For example, if you're using tags to create Smart Device Groups that add people's devices to the right overlays, enter these tags now.



Activation codes allow a user to securely connect an Airwall agent to the Conductor. Activation codes can be used by logging in and visiting the "Connect an Airwall agent" page.

☑ Provide an activation code for each member of Remote access people group

Configuration

Generated Airwall name: ${email_name}'s ${airwall_type}

Overlay device IP network (CIDR): e.g. 192.168.16.0/20

Tags: Add an entry

c) Under **Airwall agents**:

- **Require authenticated Airwall session** – Check to require an authenticated Airwall session to connect.
- Overlay **device IP network (CIDR)** – (Optional) Select the network from which to assign IP addresses to devices as the connect.

  Note: If you use the same IP network in subsequent Invitations, IP addresses will keep incrementing. For instance, if you send out one Invitation starting at 192.168.1.15 with 10 emails and then another with the same IP with 10 emails they all just get a free IP from the network as they come online.
- **Overlay device IP netmask** – Netmask in the form 255.255.255.0. Only applied if the Airwall Agent or Server has an overlay device IP assigned.
- Overlay **networks** – (Optional) The Overlay networks to add people's devices to.
- **Device groups** – Select the **Device groups** to add people's devices to.

d) Under Airwall Gateways, if you want to set the Airwall Edge Service's name using Airshell prior to provisioning, check **Allow Airshell to set name**.

10. **Control access** – If you want to grant or block access for this group at particular times, go to the **Airwall agent authentication** tab and set up Access windows for the group. For more details, see Set Times Authenticated Users can Access the Secure Network on page 92:
11. **Manage trust with tags** – If you want to manage trust for the people group using tags, go to the **Airwall agent authentication** tab and under **Authentication tags**, enter the tags you want to use to manage trust.

    Note: These tags are applied to the Airwall Agent or Server when people in this group log in to authenticate their session. Tags are removed when the remote session ends. Combined with smart device groups, you can use these tags to dynamically create trust.
12. **Manage Airwall permissions** – If you want to set what Airwall Edge Services this group has access to, go to the **Airwall permissions** tab, and add any you want them to have edit permissions to.
13. **Manage Cloud permissions** – If you want to give permissions to create cloud Airwall Gateways to this group, go to the **Cloud providers** tab, and add any cloud providers that you want them to have edit permissions to.

Set up User Authentication

How to set up user authentication for your Airwall secure network.

Here are the ways you can set up user authentication:

- Integrate Third-party Authentication with OpenID Connect on page 247
- Configure LDAP authentication on Conductor and Airwall Edge Services on page 257
- Use the local authentication in the Conductor

Related topics

- Walkthrough - Onboard people to your Airwall secure network with User Authentication on page 83
- Set Times Authenticated Users can Access the Secure Network on page 92

Set Times Authenticated Users can Access the Secure Network

Specify or restrict what days and times authenticated users can log in to access resources on your secure network by setting up Access Windows.

For example, you can use Access windows to:

- Allow one-time access for a vendor
- Restrict access to a resource except during defined maintenance windows.

Supported Versions	2.2.10 and later Conductor
Required Role	System and network administrators

Note: If a person is a member of multiple people groups with different Access windows, their session length will be either the longest available window, or the session length (which defaults to 24 hours), whichever is shorter. Multiple authentication tags will end according to the expiration you set (if any) for each Access window.

Related concepts

Manage devices dynamically with Smart Device Groups on page 105
Use Smart Device Groups to greatly simplify the creation and management of large groups of devices. Dynamically add devices to a group by defining rules to create a Smart Device Group. Rules can match criteria such as organizational hierarchy, geographic location, or network domain. When you create a Smart Device Group, any new devices that match the rules you defined are added to the group automatically.

Related tasks

Set up a People Group on page 89
Set up a people group to make it easier to manage the people accessing your secure network.

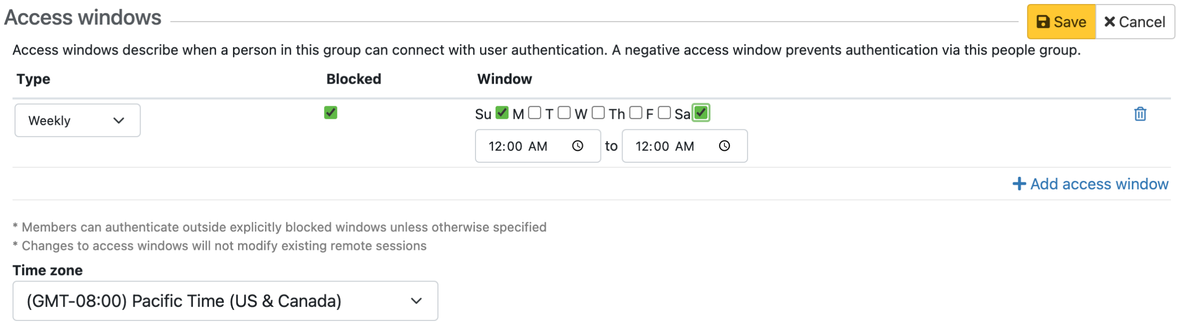
Set Access Windows (v3.1.0 and later)

1. Log in to the Conductor as a system or network administrator.
2. Create or open the people group for which you want to control access. (To create a group, see Set up a People Group on page 89.)
3. Open the **Airwall agent authentication** tab.
4. Select Edit ✎, then select **Add access window**.
5. For **Type**, select the type of window you want to create:
   - **Weekly** – Specify days of the week.
   - **Monthly** – Specify dates each month. For example, the 1st and 15th.
   - **Monthly day** – Specify a day each month. For example, the 2nd Tuesday of the month.
   - **Date range** – Specify a range of dates. You can use Date range to give someone one-time access to resources.
6. For **Blocked**, leave clear to allow access, or check to block access for the specified window.

   Note: If you set overlapping Allowed and Blocked Access windows for a People group, access will always be blocked during the overlapping times and removes authentication tags. However, if a person is in another People group that gives them access during that time, it does not block their access through the other People group's Access window.

7. Under **Window**, choose the options for your chosen Access window type.

   For example, for a Weekly Access window, you enter the days and time on those days to grant or block access. This Weekly Access window blocks access on the weekends:



Access windows describe when a person in this group can connect with user authentication. A negative access window prevents authentication via this people group.

Type	Blocked	Window
Weekly	☑	Su ☑ M □ T □ W □ Th □ F □ Sa ☑ 12:00 AM to 12:00 AM

* Members can authenticate outside explicitly blocked windows unless otherwise specified
* Changes to access windows will not modify existing remote sessions

Time zone
(GMT-08:00) Pacific Time (US & Canada)

8. Under **Time zone**, assign a Time zone for this People group's access windows. You can set different time zones for different People group's Access Windows.
9. To add more Access Windows for the group, select **Add access window** and repeat.
10. Select **Save**.
11. If you want to manage trust for this People group using tags, under **Authentication tags**, enter the tags you want to use to manage trust.

    Note: Make sure the tags you create are not being used elsewhere in the Conductor, as manually-added tags are also removed if they are the same as these conditional tags.

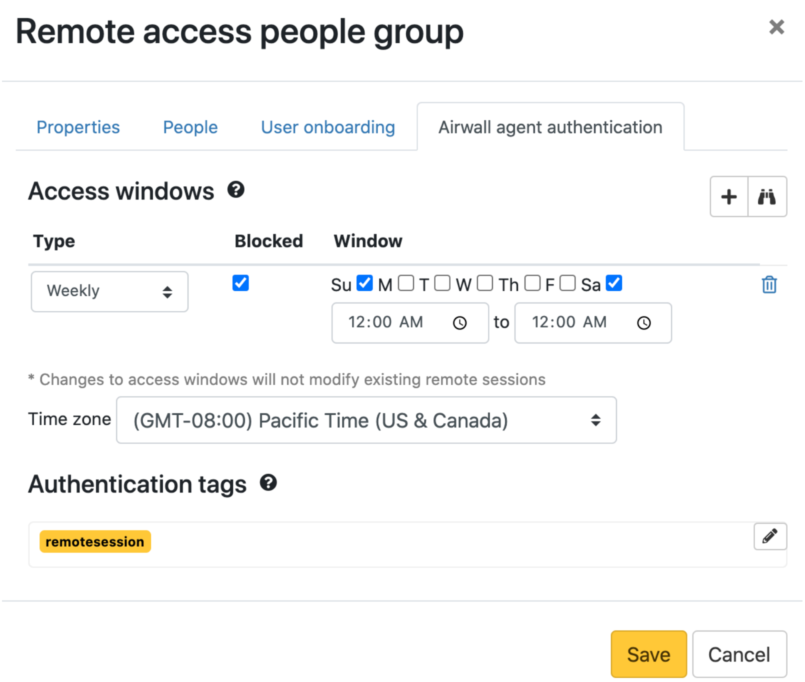
    Note: The Conductor adds the Authentication tags you've created for a people group to the person's Airwall Agent or Server when they authenticate, and removes the tags when they log out. You can see the authentication tags on a person's Airwall Agent or Server page under **Tags**. Combined with smart device groups, you can use these tags to dynamically create trust. See Manage devices dynamically with Smart Device Groups on page 105.

Set Access Windows (v3.0.3 and earlier)

1. Log in to the Conductor as a system or network administrator.
2. Create or open the people group for which you want to control access. (To create a group, see Set up a People Group on page 89.)
3. Open the **Airwall agent authentication** tab.
4. Select Edit , then select the plus sign (+) to add an Access window.
5. For **Blocked**, leave clear to allow access, or check to block access for the specified window.

   Note: If you set overlapping Allowed and Blocked Access windows for a People group, access will always be blocked during the overlapping times and removes authentication tags. However, if a person is in another People group that gives them access during that time, it does not block their access through the other People group's Access window.
6. For **Type**, select the type of window you want to create:
   - **Weekly** – Specify days of the week.
   - **Monthly** – Specify dates each month. For example, the 1st and 15th.
   - **Monthly day** – Specify a day each month. For example, the 2nd Tuesday of the month.
   - **Date range** – Specify a range of dates. You can use Date range to give someone one-time access to resources.
7. Under **Window**, choose the options for your chosen Access window type.

For example, for a Weekly Access window, you enter the days and time on those days to grant or block access. This Weekly Access window blocks access on the weekends:



Remote access people group

Access windows

Type	Blocked	Window
Weekly	☑	Su ☑ M ☐ T ☐ W ☐ Th ☐ F ☐ Sa ☑ 12:00 AM to 12:00 AM

* Changes to access windows will not modify existing remote sessions

Time zone (GMT-08:00) Pacific Time (US & Canada)

Authentication tags

remotesession

8. Select the plus sign (+) to add more Access Windows for the group. Select the binoculars to leave editing mode.
9. Under **Time zone**, assign a Time zone for this People group's access windows. You can set different time zones for different People group's Access Windows.
10. If you want to manage trust for this People group using tags, under **Authentication tags**, enter the tags you want to use to manage trust.

    Note: Make sure the tags you create are not being used elsewhere in the Conductor, as manually-added tags are also removed if they are the same as these conditional tags.

    Note: The Conductor adds the Authentication tags you've created for a people group to the person's Airwall Agent or Server when they authenticate, and removes the tags when they log out. You can see the authentication tags on a person's Airwall Agent or Server page under **Tags**. Combined with smart device groups, you can use these tags to dynamically create trust. See Manage devices dynamically with Smart Device Groups on page 105.
11. If you are creating a new People group, select **Create**. If you are editing an existing group, select **Save**.

Manage Devices and Airwall Edge Services

Set up tags, groups, and Smart Device Groups to help you manage the devices connected to your Airwall secure network.

Lock an Airwall Edge Service

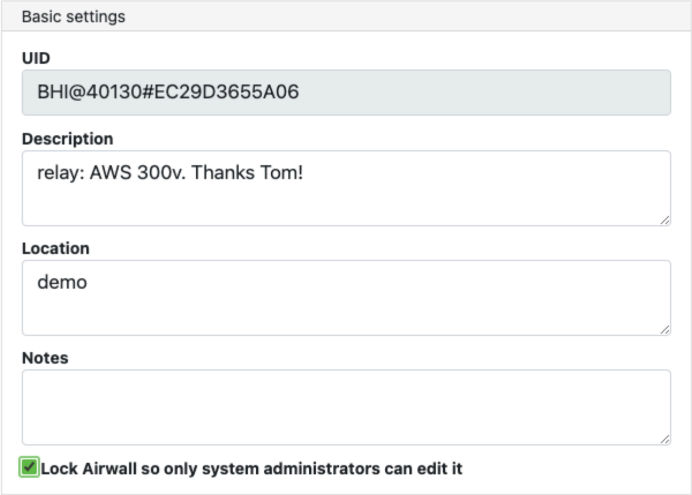
Lock an Airwall Edge Service so only system administrators can edit it.

Conductor users get editing permissions for Airwall Edge Services when they are an editor of an overlay network. If that overlay network contains a smart device group, the matching rules might pull additional Airwall Edge Services into the network. This might unexpectedly give network administrators editing permissions for those Airwall Edge Services.

You can lock an Airwall Edge Service so that only system administrators can edit it. This lock overrides all other permissions. This feature can be particularly useful on a Conductor shared by multiple groups of users where you do not want network administrators to gain elevated access to a shared resource.

Supported versions	- v3.1.0 Conductors - All Airwall Edge Services
Supported Roles	System administrators

1. In the Conductor, go to the Airwall Edge Service you want to lock.
2. Select **Edit Settings**.
3. Under **Basic settings**, check **Lock Airwall so only system administrators can edit it**.



Basic settings

UID: BHI@40130#EC29D3655A06

Description: relay: AWS 300v. Thanks Tom!

Location: demo

Notes:

☑ Lock Airwall so only system administrators can edit it

4. Select **Update Settings**.

The Airwall Edge Service can now only be edited by system administrators.

See Airwall Edge Service Information and Status

Supported Versions	2.2.8 and later

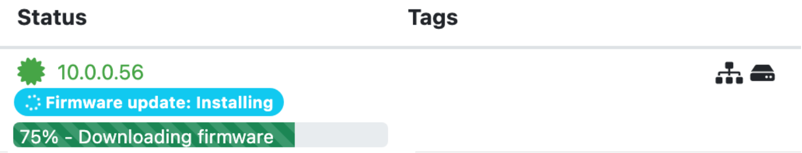
There are several ways to see information and status on the Airwall Edge Services connecting to your Airwall secure network.

All of the information and status for an Airwall Edge Service is shown when you select one to display its page. Some of that information is also available on the **Dashboard** and **Airwalls** page listings.

The following sections cover where to find some of the most commonly-needed information.

Airwall Status, Model, and Firmware

The **Status** column and field display information such as whether the Airwall Edge Service is Enabled (provisioned and managed), Unmanaged, or Revoked, and the progress of firmware updates.



Status	Tags
10.0.0.56 Firmware update: Installing 75% - Downloading firmware	

Note: Expanded status messages are available in Conductor v2.2.10 and later.

The **Model** column and **Model** and **Firmware** on an Airwall Edge Service page shows what kind of Airwall Edge Service it is and what version of the firmware it is currently running.

Most of the statuses are self-explanatory. For details, see Airwall Edge Service Statuses on page 97.

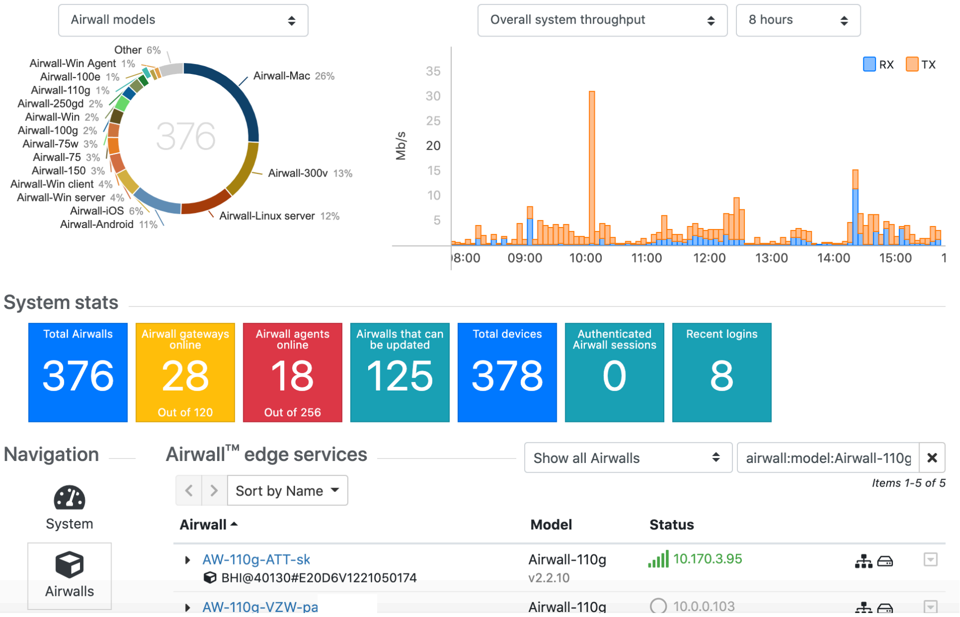
Where to See Status and Information

The following sections show different ways you can see status for one or multiple Airwall Edge Services.

On the Dashboard

The Conductor Dashboard has several ways to see what Airwall Edge Services are connecting, and what their status is.

- **The Airwall Donut Graph** – On both the Airwall models and Airwall versions graphs, click on a donut section to see what **Airwalls** are that model or have that version installed in the **Navigation Airwall edge services** section.



System stats

Total Airwalls	Airwall gateways online	Airwall agents online	Airwalls that can be updated	Total devices	Authenticated Airwall sessions	Recent logins
376	28 Out of 120	18 Out of 256	125	378	0	8

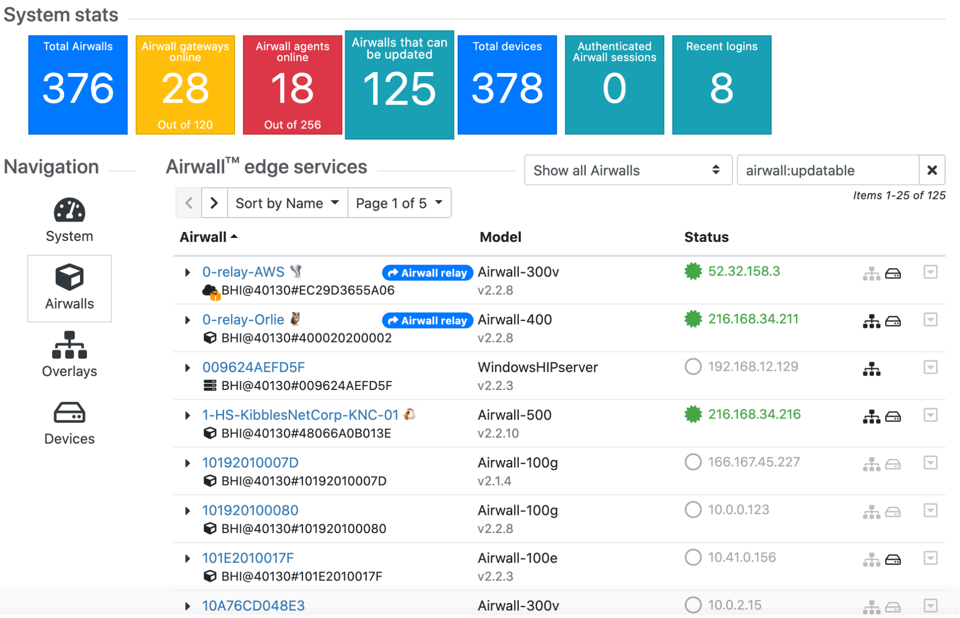
Navigation: System, Airwalls

Airwall™ edge services — Show all Airwalls — airwall:model:Airwall-110g ✕

Sort by Name — *Items 1-5 of 5*

Airwall ▲	Model	Status
AW-110g-ATT-sk BHI@40130#E20D6V1221050174	Airwall-110g v2.2.10	10.170.3.95
AW-110g-VZW-pa	Airwall-110g	○ 10.0.0.103

- **System stats** – Click on any stats tile to see more details **Navigation Airwall edge services** section.



System stats

Total Airwalls	Airwall gateways online	Airwall agents online	Airwalls that can be updated	Total devices	Authenticated Airwall sessions	Recent logins
376	28 Out of 120	18 Out of 256	125	378	0	8

Navigation: System, Airwalls, Overlays, Devices

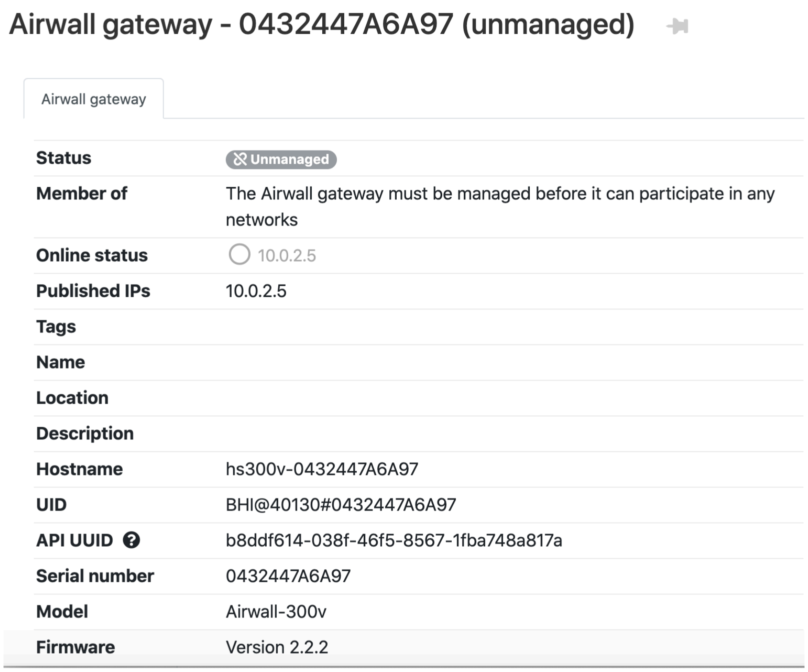
Airwall™ edge services — Show all Airwalls — airwall:updatable ✕

Sort by Name — Page 1 of 5 — *Items 1-25 of 125*

Airwall ▲	Model	Status
0-relay-AWS Airwall relay BHI@40130#EC29D3655A06	Airwall-300v v2.2.8	52.32.158.3
0-relay-Orlie Airwall relay BHI@40130#400020200002	Airwall-400 v2.2.8	216.168.34.211
009624AEFD5F BHI@40130#009624AEFD5F	WindowsHIPserver v2.2.3	○ 192.168.12.129
1-HS-KibblesNetCorp-KNC-01 BHI@40130#48066A0B013E	Airwall-500 v2.2.10	216.168.34.216
10192010007D BHI@40130#10192010007D	Airwall-100g v2.1.4	○ 166.167.45.227
101920100080 BHI@40130#101920100080	Airwall-100g v2.2.8	○ 10.0.0.123
101E2010017F BHI@40130#101E2010017F	Airwall-100e v2.2.3	○ 10.41.0.156
10A76CD048E3	Airwall-300v	○ 10.0.2.15

On an Airwall Edge Service page

Open an Airwall Edge Service to see more detailed status and information.



Airwall gateway - 0432447A6A97 (unmanaged)

Status	Unmanaged
Member of	The Airwall gateway must be managed before it can participate in any networks
Online status	○ 10.0.2.5
Published IPs	10.0.2.5
Tags	
Name	
Location	
Description	
Hostname	hs300v-0432447A6A97
UID	BHI@40130#0432447A6A97
API UUID	b8ddf614-038f-46f5-8567-1fba748a817a
Serial number	0432447A6A97
Model	Airwall-300v
Firmware	Version 2.2.2

Depending on what type of Airwall Edge Service you're looking at, you may have additional tabs on this page. For example, for Airwall Gateways, the tabs are:

- **Airwall gateway** – General information about the Airwall Gateway
- **Local devices** – Lists the devices protected by the Airwall Gateway.
- **Ports** – Port configuration, failover settings, and port mirroring configuration for the Airwall Gateway.
- **Diagnostics** – Diagnostic tools and reports for the Airwall Gateway.
- **Reporting** – Graphs, Health data, and Traffic and HIP tunnel stats for the Airwall Gateway.
- **Intrusion prevention** – Settings to help monitor and alert about intrusions into your network. These monitors can impact Conductor performance.
- **HA** – Where you set up high-availability Airwall Gateways. For more information, see Airwall Edge Service High Availability (HA) on page 399.
- **Airshell** – Gives you the ability to send Airshell commands to the Airwall Gateway remotely from the Airwall Conductor. For more information, see Run Airshell remotely from the Conductor on page 374.

Airwall Edge Service Statuses

Information on the statuses you might see for an Airwall Edge Service. Some of these statuses are not available in v2.2.8 and earlier.

Airwall Agent authentication	The person using this Airwall Agent to connect is required to use authentication.
Airwall Relay	This Airwall is running as an Airwall Relay.
Disabled	Policy configuration is disabled.
Disabled by group	The Airwall group has communication turned off.
Enabled	Policy configuration is enabled.
ha primary	High-availability active (primary) Airwall Gateway
ha secondary	High-availability standby (secondary) Airwall Gateway

Locked out	User authentication has been locked out due to too many authentication attempts.
Revoked	This Airwall has been revoked.
Transparent	Airwall Gateway is in transparent mode.
Unmanaged	Airwall has connected to the Conductor but is not managed yet. You must provision and manage before you can add it to overlays.

Manage Airwall Gateways remotely with Airshell

Use the Airshell command line to run diagnostic and configuration commands directly from the Conductor for online Airwall Gateways and for the Conductor.

Supported Roles	System and Network Administrators with **Allow Remote Airsh** permissions and **Edit** permissions for the Airwall Gateway.
Supported Versions	v3.1.0 Conductors and Airwall Gateways
Supported Airwall Edge Services	Online Airwall Gateways
Supported Airshell Commands	You can run most Airshell commands. Exceptions: shutdown, network configuration commands (commands that risk disconnecting the Airwall permanently from the Conductor). Enter `help` for a list of available commands.

1. For an Airwall Gateway, in the Conductor, open the page for an online Airwall Gateway, and then select the **Airshell** tab.

   For Conductor Airshell, go to **Settings** > **Airshell**.
2. Select **Open Remote Airshell**.
3. Enter the Airshell commands you need.
4. When done, enter `exit`, or just navigate to a different page.

Note: Airshell sessions automatically disconnect after 10 minutes of inactivity. To continue, select **Reconnect**.

Related concepts

Overlay network access roles on page 88
There are several roles people can have on an overlay network. Refer to this table for what overlay permissions each role grants.

Related tasks

Give Access to Cloud Providers with People Groups on page 87

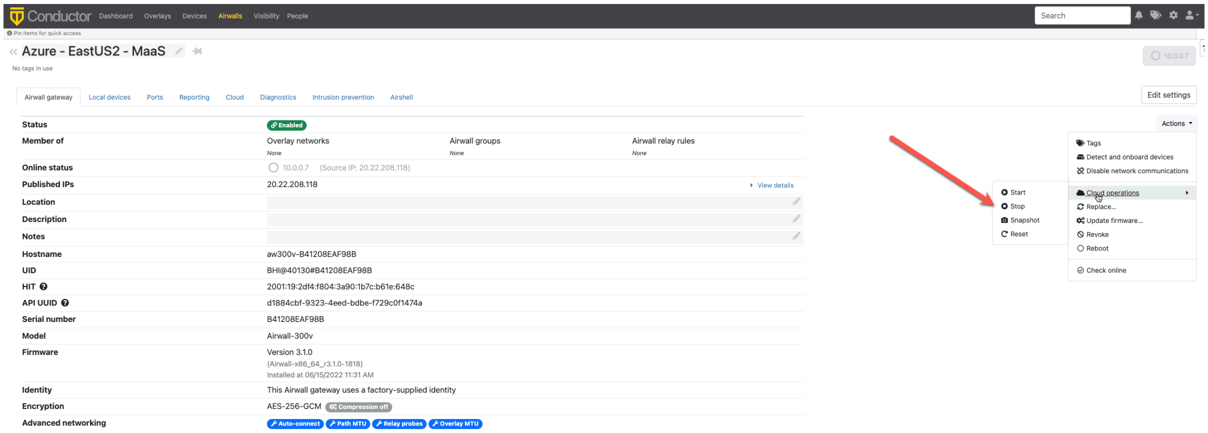
Give Access to Airwall Edge Services with People Groups on page 88

Give Access to Overlay networks and Resources on page 88

Manage Cloud Airwall Gateway Virtual Machines

You can do several management tasks for the virtual machines that host cloud Airwall Gateways from the Conductor.

1. Go to the page for a cloud Airwall Gateway.
2. On the **Airwall gateway** tab, open the **Actions** menu, and select **Cloud operations**.
3. Select the operation you want. These act on the virtual machine (VM) running the Airwall Gateway. You can Start and Stop the cloud virtual machine, take a Snapshot, or Reset it.



Azure - EastUS2 - MaaS

No tags in use

Status	Enabled		
Member of	Overlay networks None	Airwall groups None	Airwall relay rules None
Online status	10.0.0.7 (Source IP: 20.22.208.118)		
Published IPs	20.22.208.118		
Location			
Description			
Notes			
Hostname	aw300v-B41208EAF98B		
UID	BHI@40130#B41208EAF98B		
HIT	2001:19:2df4:f804:3a90:1b7c:b61e:648c		
API UUID	d1884cbf-9323-4eed-bdbe-f729c0f1474a		
Serial number	B41208EAF98B		
Model	Airwall-300v		
Firmware	Version 3.1.0 (Airwall-x86_64_r3.1.0-1818) Installed at 06/15/2022 11:31 AM		
Identity	This Airwall gateway uses a factory-supplied identity		
Encryption	AES-256-GCM Compression off		
Advanced networking	Auto-connect Path MTU Relay probes Overlay MTU		

- **Start** – Start the VM.
- **Stop** – Stop the VM.
- **Snapshot** – Creates a snapshot resource in the resource group where your VM is. To use it, you will need to create image resources from that snapshot, and then create a VM from that image.
- **Reset** – Restart the VM.

For more information, see the documentation for your cloud provider.

Disconnected Mode – Reduce Conductor traffic from Airwall Agents and Servers

Reduce the traffic from Airwall Agents and Servers connecting to your Conductor by setting up disconnected mode. In disconnected mode, Airwall Agents and Servers connect to your Conductor at intervals – between 10 minutes and 12 hours (720 minutes) – to get updates when people are not actively using the connection.

By reducing the traffic on your Conductor, disconnected mode allows you to improve performance and scalability of your Airwall secure network.

Note: People using Airwall Agents and Servers can manually sync to the Conductor when in Disconnected mode.

1. Open the page for the Airwall Agent or Server that you want to enable disconnected mode for.
2. Select **Edit Settings**.
3. Under **Advanced settings**, scroll down to the bottom and check **Enable disconnected mode**.
4. Enter the time interval for the Airwall Agent or Server to reconnect to the Conductor.
5. Select **Update Settings**.

The Airwall Agent or Server you set disconnected mode on now disconnects from the Conductor, and reconnects at the specified interval to get configuration and trust policy updates. While in disconnected mode, the Airwall Agents and Servers show in the Conductor as not connected, and if you hover over the online status, they show they are in Disconnected mode and when their next connection is scheduled.

Note: In Disconnected mode, an Airwall Agent or Server:

- Can still connect to resources on your Airwall secure network.
- Gets policy and firmware updates the next time they connect.
- Do not publish underlay IP updates or status (health data, traffic stats, port status).

Note: Certain changes (such as underlay IP changes) can cause a disconnected Airwall Agent or Server to not be able to reach resources on your Airwall secure network. If this happens, the person using the Airwall Agent or Server can get the changes and reestablish their connection by either selecting **Sync Now** on their Airwall Agent or using the `conductor sync` Airshell command on their Airwall Server. For more information on Airshell for the Linux Airwall Server, see Sync an Airwall Agent or Server in Disconnected Mode on page 29.

Manage and organize with Tags

Use tags to manage and organize your Airwall secure network. You can tag most things in the Conductor.

You can tag:

- Airwall Gateways and Airwall Gateway Groups
- Overlay Networks
- Devices and Device Groups
- People

You can use tags to:

- **Simplify user onboarding** with **Airwall Invitations** or **Activation codes**. See Connect People's Devices with Airwall Invitations on page 64.
- **Search and filter** throughout Conductor.
- **Automatically add devices to Smart Device Groups** by creating a rule matching a tag. See Use device groups and smart device groups on page 416.
- **Set a trigger for an Event Monitor**. See Monitor Activity with Events and Alerts on page 117.
- **Set network policies**, including temporary network policies like expiring access. For an example, see Walkthrough – Send Expiring Guest Access Invitations on page 69.
- **Revoke policy directly** from devices or Airwall Gateways without having to navigate to a network by deleting the tag that gives them access.
- Mark which assets are managed by which people.

You can tag items permanently, until you untag them, or set an expiration date, which untags an item after a period of time.

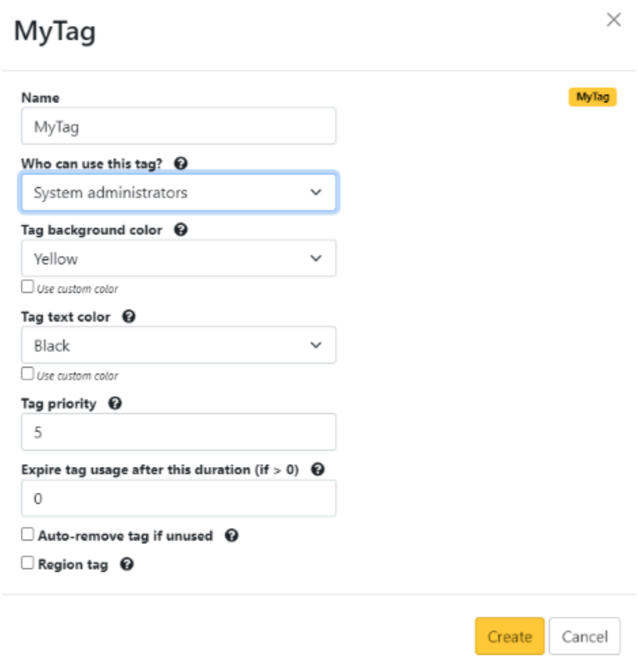
Note: When using tags that are added and removed dynamically (for example, with Smart Device Groups or Access Windows), make sure the tags you create are not being used elsewhere in the Conductor, as manually-added tags are also removed if they are the same as these conditional tags.

Create a Tag

To quickly create a tag, hover in an Tag column or box, and click the edit icon that appears. Enter a new tag, select the check mark or press `Enter` to add it, and then select **Save**.

To set advanced options on a tab, go to the Tags page:

1. In the upper right corner of the Conductor, select the Tag icon 🏷 to open the **Tags** page.
2. Select **New tag**.



Name: MyTag

Who can use this tag?: System administrators

Tag background color: Yellow

□ Use custom color

Tag text color: Black

□ Use custom color

Tag priority: 5

Expire tag usage after this duration (if > 0): 0

□ Auto-remove tag if unused

□ Region tag

3. Enter the following information:

    - **Name -** give your tag a name.
    - **Who can use this tag? -** select the permissions you want to set for the tag.
    - **Tag background color** and **Tag text color -** choose colors, and check the example for the result.
    - **Tag priority -** set the priority for the tag. Use this to set relative priorities for tags. The tag with the lowest number takes precedence over tags with higher numbers.
    - **Expire tag usage after this duration -** set an expiration duration, if needed. Leave it set to 0 to make the tag permanent..
    - **Auto-remove tag if unused -** check to remove the tag if it is not used.
    - **Region tag -** use to indicate a region. This tag is used to identify an select bypass Airwall.

    Note: Region feature available in Conductor v3.2.3 and later.

4. Select **Create**.

Related tasks

Edit Tags on page 101

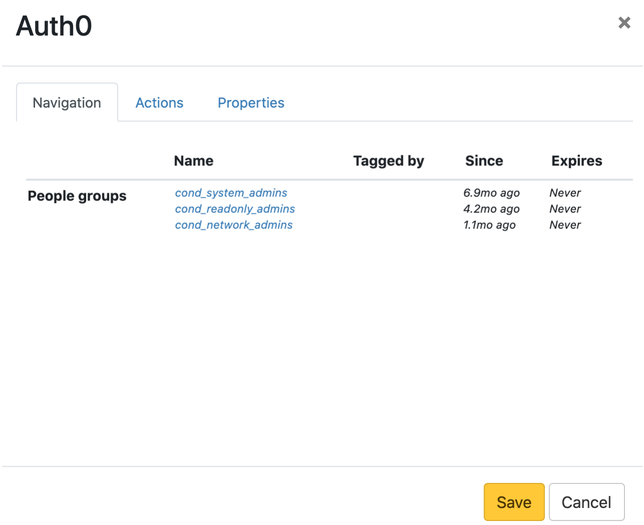
Delete Tags on page 103

Create or Manage Tags Inline on page 103

Edit Tags

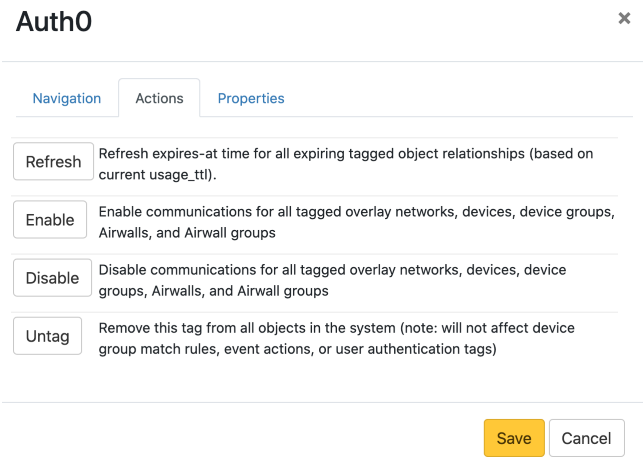
Note: You can only edit tags for items that you have permission to edit.

1. In the upper right corner of the Conductor, select the Tag icon 🏷 to open the **Tags** page.
2. Open tag you want to edit.
3. The **Navigation** tab shows everything tagged with this tag. You can click the Name of an item to open it.



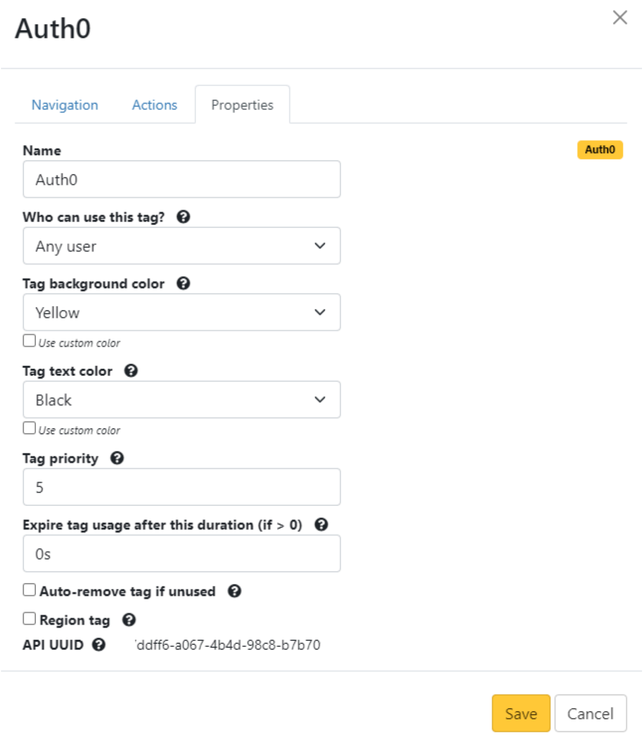
	Name	Tagged by	Since	Expires
People groups	*cond_system_admins*		*6.9mo ago*	*Never*
	cond_readonly_admins		*4.2mo ago*	*Never*
	cond_network_admins		*1.1mo ago*	*Never*

4. On the **Actions** tab, you can:
    - **Refresh** – **Refresh expiration time** for any expiring tagged items. You can check the expiration settings on the **Properties** tab.
    - **Enable** or **Disable** – **Enable or disable communications** for all tagged items. Select the confirmation message **Yes please...let's do this!** to continue, or select **Cancel** to cancel.
    - **Untag** – **Remove the tag** from all items, but not from rules, event actions, or user authentication.



Refresh	Refresh expires-at time for all expiring tagged object relationships (based on current usage_ttl).
Enable	Enable communications for all tagged overlay networks, devices, device groups, Airwalls, and Airwall groups
Disable	Disable communications for all tagged overlay networks, devices, device groups, Airwalls, and Airwall groups
Untag	Remove this tag from all objects in the system (note: will not affect device group match rules, event actions, or user authentication tags)

5. On the **Properties** tab, you can change any of the settings for the tab. For descriptions, see Create a Tag on page 100.



Name: Auth0

Who can use this tag? Any user

Tag background color: Yellow

□ Use custom color

Tag text color: Black

□ Use custom color

Tag priority: 5

Expire tag usage after this duration (if > 0): 0s

□ Auto-remove tag if unused

□ Region tag

API UUID 'ddff6-a067-4b4d-98c8-b7b70

6. Select **Save** if you want to save any changes to the tag.

Create or Manage Tags Inline

You can access tags from several places in the Conductor, both from the tables on the **Overlays**, **Devices**, **Airwalls**, or **People** pages, and on the page for a specific resource, such as an Airwall Gateway.

You can tag items permanently, until you untag them, or set an expiration date, which untags an item after a period of time.

1. Access the tag from one of these places:
   - Next to Tags on some pages.
   - By selecting **Edit Settings** on a page.
   - On any page with a table that has a **Tags** column.
2. Create or manage them inline:
   - **To add or create a tag** – Hover in the column and click the edit icon that appears. Type a new or existing tag, select the check mark or press Enter to add it, and then select **Save**.
   - **To remove a tag from a resource** – Click the **X** on the tag.
   - **To manage a tag** – Click the tag to open it, and edit on the **Actions** or **Properties** tabs for the tag. See Edit Tags on page 101.
   - **To navigate to a tagged resource** – Click the tag to open it, and select other items that have that tag to go there.

To delete a tag from the Conductor, see Delete Tags on page 103.

Delete Tags

You can delete tags individually, or delete several tags at once from the **Tags** page.

1. In the upper right corner of the Conductor, select the Tag icon 🏷 to open the **Tags** page.
2. Check the box next to one or more tags.
3. At the top of the page, open **Actions**, and select **Delete tags**.

Manage Tag Ownership

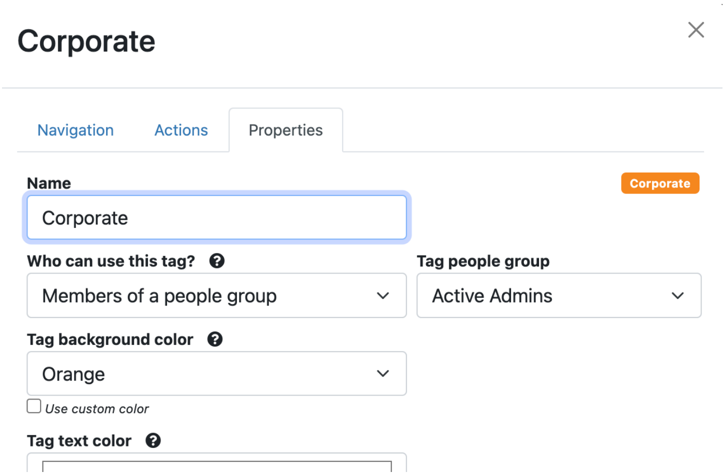
Manage who can see and edit tags.

With v3.1.0, the tag ownership rules have changed to be more restrictive by default. If a system administrator creates a tag, by default, only system administrators can see or use them. If a network administrator creates a tag, ownership defaults to only them or their people group, and system administrators. This change allows you to have department or customer-specific tags that only members of specific people groups can see and use.

Note: This change does not affect existing tags that will keep their existing ownership.

Supported versions	- v3.1.0 Conductors - All Airwall Edge Services
Supported Roles	To set tag permissions, you must be the owner of the tag, or a system administrator

1. In the upper right corner of the Conductor, select the Tag icon to open the**Tags** page.
2. Select a tag to manage, or create a new one by selecting **Create tag**.
3. On the tag's **Properties** tab, under **Who can use this tag**, select who you want to have access to this tag. You can select **Members of a people group**, and then under **Tag people group**, select the people group to give access to.



Corporate

Name: Corporate

Who can use this tag?: Members of a people group

Tag people group: Active Admins

Tag background color: Orange

□ *Use custom color*

Tag text color

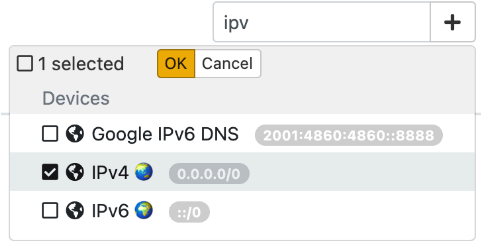
Create standard device groups

Put devices into device groups so you can manage them as a group. If you want to create a smart device group where devices are automatically added if they match rules, see Manage devices dynamically with Smart Device Groups on page 105.

v3.0 and later

To create device groups:

1. Go to **Devices** > **Device groups** and select **New group**.
2. Enter a unique name for the group and, optionally, a description and tags for the group.
3. Select **Create**. The page for your new device group opens.
4. In the **Add Devices** box, enter a string to search for, check the devices you want to add to the group, and select **OK**.



ipv +

☐ 1 selected OK Cancel

Devices

☐ Google IPv6 DNS 2001:4860:4860::8888

☑ IPv4 0.0.0.0/0

☐ IPv6 ::/0

Note: You can also select the + (plus sign) to filter and select devices, including sorting by devices or bypass destinations.

Before v3.0

To create device groups:

1. Go to **Devices** > **Device groups** and select **Create group**.
2. On the **Properties** tab, enter a unique name for the group and optionally, a description.

   Note: If *Automatically recompute* is not selected, the Conductor determines when recomputing a rule is required and displays the icon in the **Indicators** column of the device list. Manually recompute the group by selecting the drop-down arrow to the right of your device in the device list and select **Recompute group**.
3. Add any tags for this group.
4. On the **Devices** tab, check the box next to the devices you want to add to the group.

   Note: You can show all devices, show only members of the group, or show only non-members of the group, or filter the list of devices by entering text in the **Filter** field to quickly check the list or locate the devices you want to add.

   Note: In a standard device group, you add and remove members from this tab. In a Smart Device Group, this tab lists all devices added based on the Device match rules, and you cannot modify it directly.
5. Select **Create**.

Manage devices dynamically with Smart Device Groups

Use Smart Device Groups to greatly simplify the creation and management of large groups of devices. Dynamically add devices to a group by defining rules to create a Smart Device Group. Rules can match criteria such as organizational hierarchy, geographic location, or network domain. When you create a Smart Device Group, any new devices that match the rules you defined are added to the group automatically.

To find Smart Device Groups, go to **Devices** > **Device groups**. Look for the Smart Device Group icon (resembles an academic cap) 🎓.

To see an example, see Smart Device Group example on page 110.

Create a Smart Device Group

You create a device group and then give it an ordered list of Device Match Rules to determine which discovered devices to add to your device group. When the Conductor discovers a new device, it checks the rules for all Smart Device Groups. If the device matches all of the Device Match Rules successfully, the Conductor adds it to that group. Be sure to review the Best Practices for Smart Device Groups on page 113 for help on setting great rules.

v3.0 and later

Follow this section to add a smart device group in v3.0 and later.

1. To create a Smart Device group, create a device group, go to the **Match rules** tab, and enable **Use rules to add devices**. Enabling this shows the **Device match rules** section.
2. Next to **Device match rules**, select the edit icon ✎, and the next table row on the right, select **Add Rule**.
3. Set the rules you want to determine which devices are added to this group:

Order

Specify the order you want the rules run. You can receive very different results based on how you order your rules. For details, see Rule ordering on page 108.

Operator

Use an operator to determine the logic by which devices are added as members of the group. See Rule operators on page 109 for a list of operators.

Reverse (!)

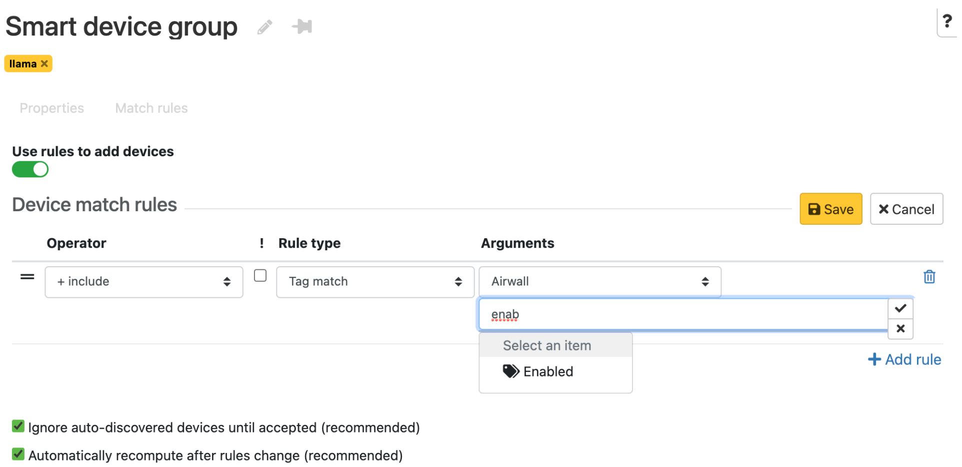
The reverse option reverses the result of the operator. The Smart Device Group example on page 110 contains a device match rule that uses the reverse option as an example.

Rule type

Select the information you want to use to determine what devices are added to a Smart Device Group. See Rule types on page 109 for a list of rule types.

Arguments

Select the arguments, or options, for the rule type you selected.



Smart device group

llama ×

Properties Match rules

Use rules to add devices

Device match rules Save ✕ Cancel

Operator	!	Rule type	Arguments
+ include	□	Tag match	Airwall

enab

Select an item

Enabled

+ Add rule

☑ Ignore auto-discovered devices until accepted (recommended)

☑ Automatically recompute after rules change (recommended)

4. To add additional rules, select **Add rule** again.

   To delete rules, next to the rule, click the delete icon 🗑 .

5. Under the rules table, check the rule options. It is best practice to keep both of these checked:

   - **Ignore auto-discovered devices until accepted** – Keep this box checked to only add discovered devices after they have been managed by a Conductor administrator.
   - **Automatically recompute after rules change** – Keep this box checked to recompute the device group whenever the rules are changed.

6. Set the Rule editor to a person with permissions to manage the devices in the Smart Device group.

Note: If one of your rules is adding and removing tags, make sure the tags you create are not being used elsewhere in the Conductor, since manually-added tags are also removed if they are the same as these conditional tags.

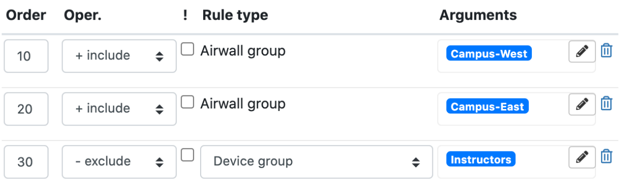
CAUTION: If you disable **Use rules to add devices** on an existing Smart Device Group and click **Save**, the Smart Device Group reverts to a standard device group and the Device match rules are deleted. Devices added by the rule retain membership in the group but now you must add and delete devices manually using the **Properties** tab.

CAUTION: If you enable **Use rules to add devices** on a regular device group, any existing devices will be removed from the device group.

Set Device Match Rules

The screenshot below illustrates how you might construct a typical set of device match rules. These rules:

- Add all Airwalls in the Campus-West Airwall group, then,
- Add all devices in the Campus-East Airwall group, then,
- Remove all devices that are in the Instructors device group.



Order	Oper.	!	Rule type	Arguments	
10	+ include	□	Airwall group	Campus-West	✎ 🗑
20	+ include	□	Airwall group	Campus-East	✎ 🗑
30	- exclude	□	Device group	Instructors	✎ 🗑

Note: If you change the order of these rules to exclude instructor devices first, it will exclude the Instructor device group first, then add Airwalls in the Campus-West and then Campus-East Airwall groups, which means instructor devices in those groups are added back in.

Before v3.0

Follow this section to create a Smart device group in earlier versions.

1. To create a Smart Device group, when creating a device group, on the **Rules** tab under **Use rules to add devices**, select **Enabled**. You can then create Device match rules.
2. Select the edit icon ✎ , and then select the plus sign (+).
3. Set the rules you want to determine which devices are added to this group (see descriptions in the v3.0 instructions).
4. To add additional rules, select the plus sign again.

   To delete rules, next to the rule, click the delete icon 🗑 .
5. Check the rule options as described in the v3.0 instructions.
6. Set the Rule editor to a person with permissions to manage the devices in the Smart Device group.

CAUTION: If you disable **Use rules to add devices** on an existing Smart Device Group and click **Save**, the Smart Device Group reverts to a standard device group and the Device match rules are deleted. Devices added by the rule retain membership in the group but now you must add and delete devices manually using the **Devices** tab.

Add rules to a Smart Device Group

To add rules to a Smart Device Group:

1. In the Conductor, go to **Devices>Device groups**.
2. Create and open a device group, or open an existing group from the list.
3. Go to **Match rules** (before 3.1.0, this is **Rules** in the device group dialog).
4. Select the edit icon ✎ to enter editing mode and then select **Add rule** (before 3.1.0, select **Edit rules**).
5. Enter device match rules to add devices to this device group:
   - **In 3.1.0 and later** – Enter the **Operator**, **!** (negate the rule) **Rule type**, and **Arguments**.
   - **Before 3.1.0** – Enter the **Order**, **Oper.**, **!**, **Rule Type**, and **Arguments**.

   For more information, see Rule ordering on page 108, Rule operators on page 109, and Rule types on page 109.
6. Select **Add rule** to continue adding rules.
7. If necessary, select match rules. For the highest security, leave both of these options checked:
   - Check **Ignore auto-discovered devices until accepted** to have the Smart Device Group not add any auto-discovered devices until they are managed by an administrator.

- Check **Automatically recompute after rules change** to have the Smart Device Group recompute the rules and rebuild the group after any rules are changed.

8. **In 3.1.0 and later** – Under Permissions scope, specify what permissions you want this Smart Device group to include:

- Check **All devices in the Conductor** to add any devices in the Conductor.
- Check **All devices on Airwalls in a people group's Airwall permission list** and select one or more people groups to add only devices from those people groups.
- Check **All devices a network admin can edit** and select one or more network admins to add only devices editable by those network admins.

9. When you are finished, save your rules:

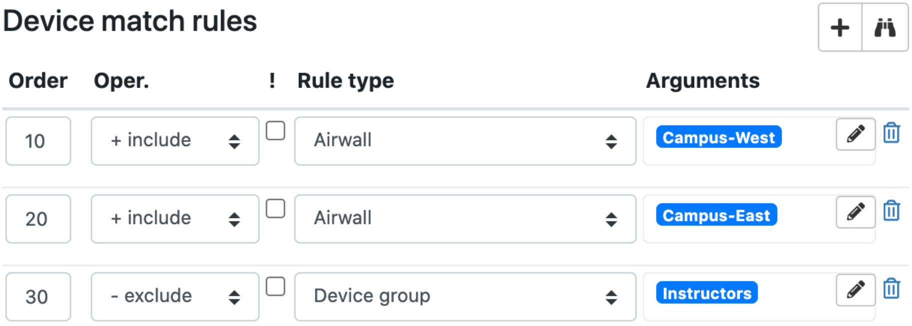
- **In 3.1.0 and later** – Select **Save**.
- **Before 3.1.0** – Select **View rules**, then **Save**.

Note: If any of the information is entered incorrectly, you will receive a validation error. Click **Edit rule** to return to editing mode.

Rule ordering

Device match rules are interpreted in order. You can get very different results based on how you order your rules.

This example illustrates how changing the order of rules can change which devices are added to the group.



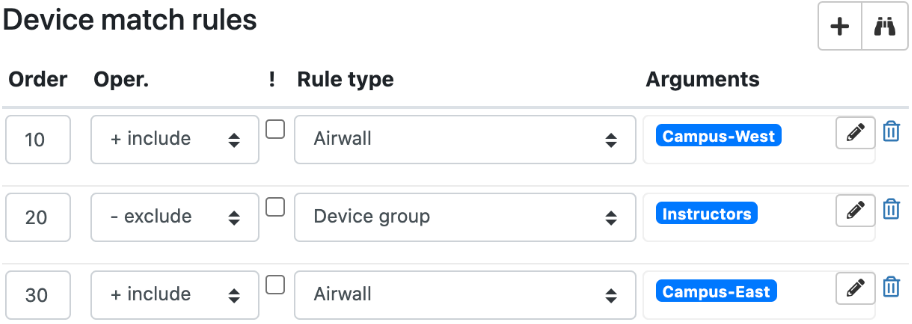
Device match rules

Order	Oper.	!	Rule type	Arguments
10	+ include	☐	Airwall	Campus-West
20	+ include	☐	Airwall	Campus-East
30	- exclude	☐	Device group	Instructors

The first rule adds all devices behind the **Campus - West** Airwall Gateway. The second rule adds any devices behind **Campus - East**. The third rule excludes all devices in the **Instructors** group, removing any Instructor Desktops from the group. This results in the following group membership:

- Classroom Desktop - 1st Floor Campus-West
- Classroom Desktop - 2nd Floor Campus-West
- Classroom Desktop - 3rd Floor Campus-West
- Classroom Desktop - 1st Floor Campus-East

If you reverse the second and third rule:



Device match rules

Order	Oper.	!	Rule type	Arguments
10	+ include	☐	Airwall	Campus-West
20	- exclude	☐	Device group	Instructors
30	+ include	☐	Airwall	Campus-East

You get different results. The second rule still removes Instructor Desktops in Campus-West, but it doesn't remove them from Campus-East, since that rule hasn't run yet. When the third rule runs, any Instructor devices in Campus-East are included:

- Classroom Desktop - 1st Floor Campus-West
- Classroom Desktop - 2nd Floor Campus-West
- Classroom Desktop - 3rd Floor Campus-West
- Classroom Desktop - 1st Floor Campus-East
- Instructor Desktop - 1st Floor Campus-East

Since rules are processed in order, make sure you enter rules in an order that produces the intended result.

Rule operators

The following operators are available while editing rules:

Operator	Description
+ *include*	Adds devices to the group that match this rule. **Example:** *include* CIDR *10.0.0.0/8* **Result:** Include any devices with an IP address between *10.0.0.0* and *10.255.255.255*.
~ *filter*	Filter the previous rule's results to only devices that match this rule as well. This operator is equivalent to *intersect* in set theory. **Example:** *include* Airwall *Campus-West* *filter* Range *10.0.0.100 10.0.0.106* **Result:** Include devices in the group that are behind the Airwall Gateway *Campus-West* **and** have an IP address between 10.0.0.100 and 10.0.0.106.
- *exclude*	Removes devices that match this rule from devices added to the group by previous rules. **Example:** *exclude* Device Group *Instructors* **Result:** Exclude any devices that belong to the *Instructors* group.

Rule types

Here are the rules types you can select for device match rules:

Rule Type	Arguments	Description
CIDR	1	Match devices with IP addresses in the specified CIDR (Classless Inter-Domain Routing) group.
Overlay device IP network	2	Match devices matching the IP address and netmask specified (use dotted decimal notation, for example, 10.6.10.40).
Overlay device IP range	2	Match devices with IP addresses in the range specified by the two IP addresses (use dotted decimal notation).
MAC Prefix	1	Match devices with the specified MAC address prefix. Enter an empty field to match devices without a MAC address.
Airwall	1	Match devices under the specified Airwall Edge Service.

Rule Type	Arguments	Description
Airwall Attribute	2	Match devices under any Airwall where the selected attribute matches the text you specify. The following attributes are available: Name Description Location Model Product Platform Capability Code Cloud Attributes Version Hotfix List
Airwall Group	1	Match devices in the specified A drop-down list of existing Airwall group.
Tag match	1	Match devices with the specified tag.
Tag search	2	Match the selected type of objects (Airwall, Airwall group, or Device, or any object) that contain the specified tag.
Device Group	1	A drop-down list of existing device groups.

Delete rules from a Smart Device Group

To delete a rule:

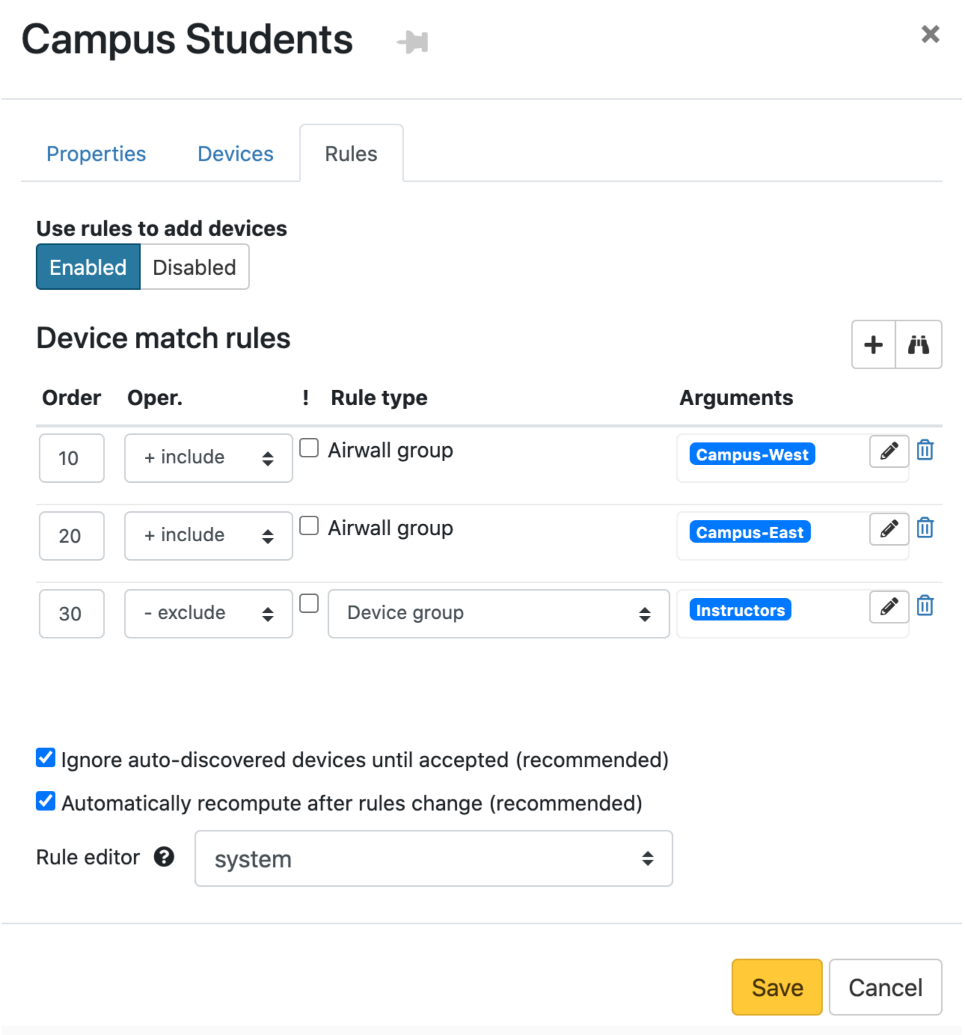
1. In the Conductor, go to **Devices** and then **Device groups**.
2. From the list, open a device group.
3. Go to **Match rules** (before 3.1.0, this is **Rules** in the device group dialog).
4. Select the edit icon ✎ to enter editing mode and then select **Add rule** (before 3.1.0, select **Edit rules**).
5. To the right of the rule you want to delete, click the trash icon.

   Important: There is no confirmation when deleting a rule. It is removed from the list immediately. If you delete a rule in error, click **Cancel** to revert to your last saved changes.

6. When you are finished, save your rules:
   - **In 3.1.0 and later** – Select **Save**.
   - **Before 3.1.0** – Select **View rules**, then **Save**.

Smart Device Group example

The example below illustrates how a Device Group Rule (DGR) is interpreted (the screenshot is from pre-v3.0 Conductor, but later versions work similarly):



Use rules to add devices

Enabled | Disabled

Device match rules

Order	Oper.	!	Rule type	Arguments
10	+ include	□	Airwall group	Campus-West
20	+ include	□	Airwall group	Campus-East
30	- exclude	□	Device group	Instructors

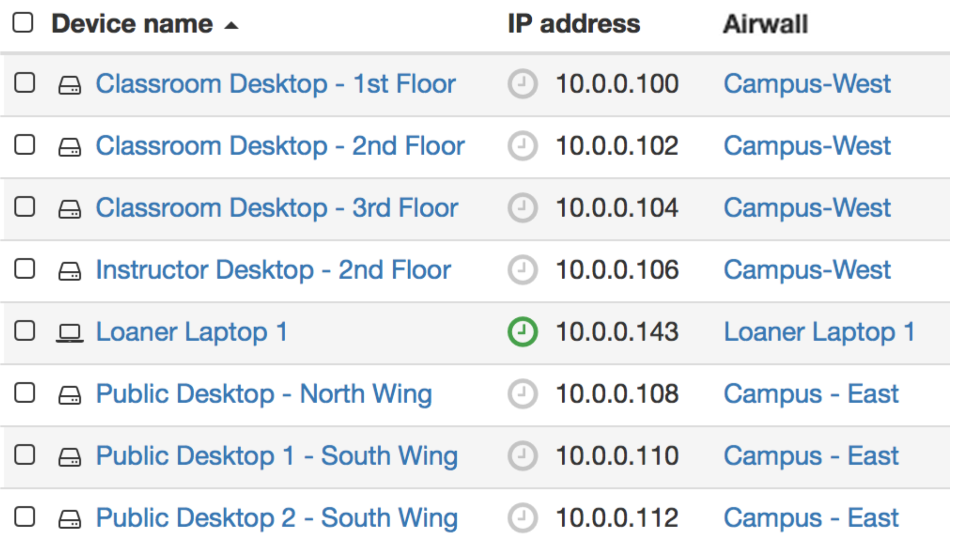
☑ Ignore auto-discovered devices until accepted (recommended)

☑ Automatically recompute after rules change (recommended)

Rule editor: system

There are two Airwall Gateways in this example, named **Campus - West** and **Campus - East**.

There are eight discovered devices, four behind the Airwall Gateway **Campus - West**, three behind the Airwall Gateway **Campus - East**, and one loaner laptop running an Airwall Agent.

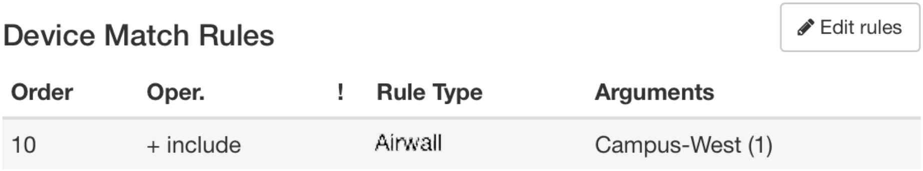


□ Device name ▲	IP address	Airwall
□ Classroom Desktop - 1st Floor	10.0.0.100	Campus-West
□ Classroom Desktop - 2nd Floor	10.0.0.102	Campus-West
□ Classroom Desktop - 3rd Floor	10.0.0.104	Campus-West
□ Instructor Desktop - 2nd Floor	10.0.0.106	Campus-West
□ Loaner Laptop 1	10.0.0.143	Loaner Laptop 1
□ Public Desktop - North Wing	10.0.0.108	Campus - East
□ Public Desktop 1 - South Wing	10.0.0.110	Campus - East
□ Public Desktop 2 - South Wing	10.0.0.112	Campus - East

In this example, the rules dynamically add devices to the group that are behind the **Campus - West** Airwall Gateway or devices with intermittent connections to the network, while excluding devices from **Campus - East** and devices belonging to the Instructor Devices group.

10 *include* Airwall Edge Service *Campus-West*

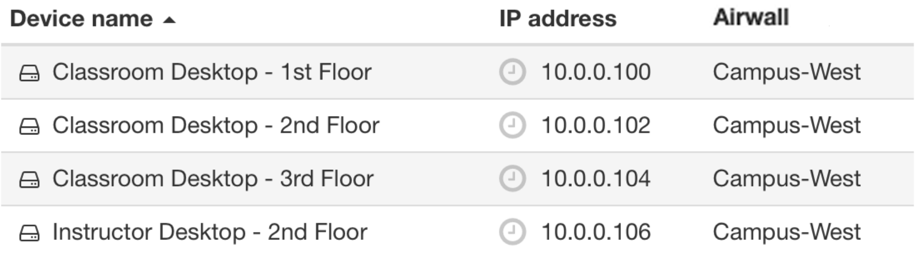
The first rule adds all devices behind the **Campus - West** Airwall Gateway by using the *include* operator, the *Airwall Edge Service* rule type, and the selection *Campus - West* argument.



Device Match Rules

Order	Oper.	!	Rule Type	Arguments
10	+ include		Airwall	Campus-West (1)

This rule matches the following devices:



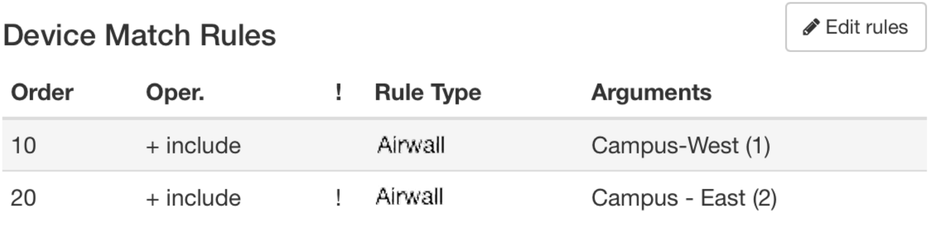
Device name ▲	IP address	Airwall
Classroom Desktop - 1st Floor	10.0.0.100	Campus-West
Classroom Desktop - 2nd Floor	10.0.0.102	Campus-West
Classroom Desktop - 3rd Floor	10.0.0.104	Campus-West
Instructor Desktop - 2nd Floor	10.0.0.106	Campus-West

Please note that there is one instructor device in the result, which is a member of the Instructor Devices group that we need to remove later.

20 *include [negate]* Airwall Edge Service *Campus-East*

The next rule adds any devices that are not behind the **Campus - East** Airwall Gateway by using the *include* operator, the negate option, *Airwall Edge Service* rule type, and the selection *Campus - East* argument. This captures any laptops running Airwall Agents that may intermittently require network access.

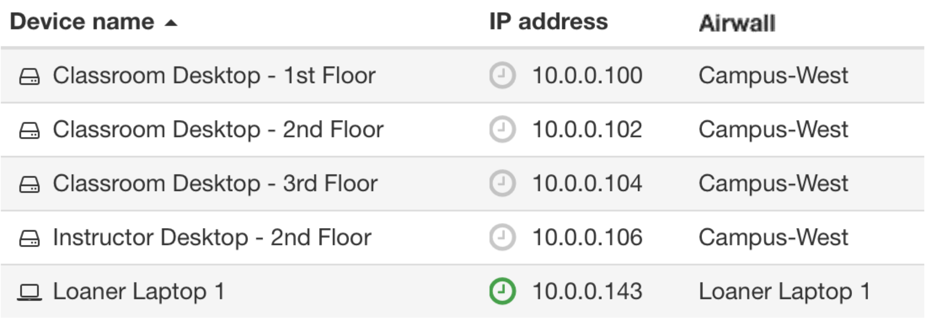
Note: In this example, you could remove the first rule and achieve the same result. It is included to illustrate the difference between the *include* operator plus the negate option and the *exclude* operator, later in this example.



Device Match Rules

Order	Oper.	!	Rule Type	Arguments
10	+ include		Airwall	Campus-West (1)
20	+ include	!	Airwall	Campus - East (2)

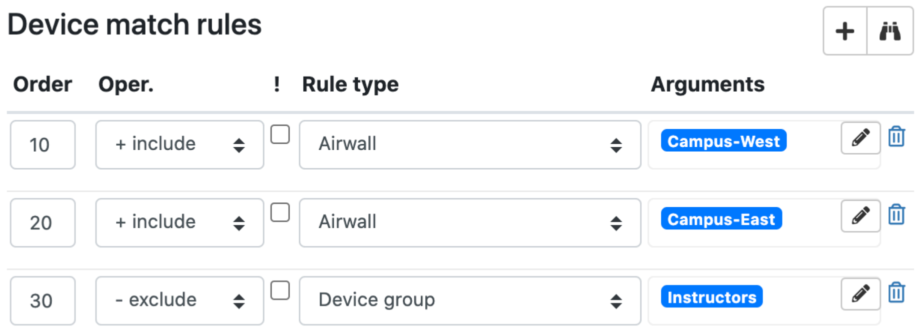
These two rules will add one additional device, *Loaner Laptop 1*, to the result:



Device name ▲	IP address	Airwall
Classroom Desktop - 1st Floor	10.0.0.100	Campus-West
Classroom Desktop - 2nd Floor	10.0.0.102	Campus-West
Classroom Desktop - 3rd Floor	10.0.0.104	Campus-West
Instructor Desktop - 2nd Floor	10.0.0.106	Campus-West
Loaner Laptop 1	10.0.0.143	Loaner Laptop 1

30 *exclude* Device Group *Instructor Devices*

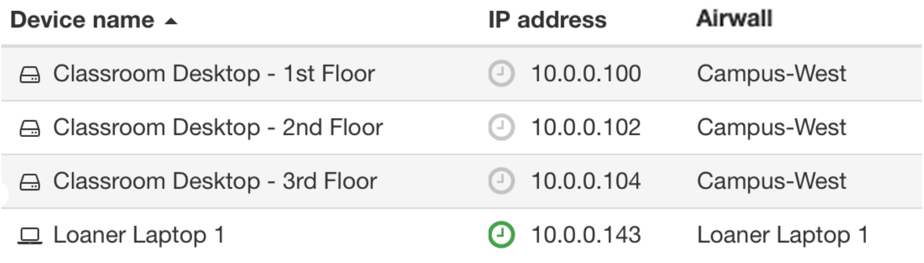
The third rule excludes all devices in the **Instructor Devices** group by using the *exclude* operator, *Device Group* rule type, and the selection *Instructor Devices* argument.



Device match rules

Order	Oper.	!	Rule type	Arguments
10	+ include	☐	Airwall	Campus-West
20	+ include	☐	Airwall	Campus-East
30	- exclude	☐	Device group	Instructors

This rule removes the device, *Instructor Desktop - 2nd Floor*, from the result:



Device name ▲	IP address	Airwall
Classroom Desktop - 1st Floor	10.0.0.100	Campus-West
Classroom Desktop - 2nd Floor	10.0.0.102	Campus-West
Classroom Desktop - 3rd Floor	10.0.0.104	Campus-West
Loaner Laptop 1	10.0.0.143	Loaner Laptop 1

As more devices are discovered and managed by the Conductor, either behind an Airwall Gateway or running an Airwall Agent, the following actions will be taken by the rule:

- A device added to the **Campus - West** Airwall Gateway will be added as a member
- A device added to the **Campus - East** Airwall Gateway will not be added as a member
- Any device running an Airwall Agent will be added as a member
- Any device added to the *Instructor Devices* group will not be added as a member

Delete a Smart Device Group

To delete a Smart Device Group:

1. Go to **Devices→ Device groups**
2. Select the drop-down to the right of the device group you want to delete, and click **Remove group**

Best Practices for Smart Device Groups

Create easy-to-use, effective Smart Device Groups by following these recommendations to ensure your rules are constructed properly.

Use Smart Device Groups only when necessary

Smart Device Groups are very powerful and can be instrumental in helping you to manage a large number of devices, but not every group should be a Smart Device Group. Generally, you should manage device group membership manually when:

- There are no complex patterns to match
- Devices are easily differentiated, such as cameras or Web servers
- You are creating denylists and allowlists

Create Smart Device Groups for frequently used matches

For ease of management, avoid repeating the same logic in multiple Smart Device Groups. It is best to create a Smart Device Group and reuse that group in other Smart Device Groups using the Device Group rule type. For example, if you capture devices from a particular set of Airwall Edge Services, consider creating a Smart Device Group for that purpose and including it in other Smart Device Groups that require it.

There are a few consideration you want to keep in mind when nesting device groups:

- If a device group changes membership, any Smart Device Groups that refer to it in a Smart Device Group's Device Match Rules will need to be recomputed.
- A Smart Device Group included in another Smart Device Group does not trigger the parent group to recompute unless it also is set to automatically recompute. For example, standard device group *DG-Seattle* is included in smart device group *DG-Washington*, which is not set to automatically recompute. *DG-Washington* is included in *DG-UnitedStates*, which is set to automatically recompute. If a device is added to *DG-Seattle*, neither Smart Device Group will recompute because *DG-Washington* is not set to autocompute and *DG-UnitedStates*, which is set will not detect any changes from *DG-Washington*.

Exclude what you do not require as soon as possible

If your Device Match rules create a large result set, consider excluding what you do not need as early as possible, starting with the largest sets first. For example **US Servers** *exclude* **West Coast Servers** *exclude* **Washington State Servers** is more efficient than **US Servers** *exclude* **Washington State Servers** *exclude* **West Coast Servers**.

Maintain exceptions separately

Keep it Smart: If there are exceptions (that is, a "denylist") of devices to exclude from a smart group, maintain a separate denylist device group containing these devices rather than abandoning the rules and manually removing the devices from the group. For example, when troubleshooting, or as bad actors emerge in the network, add them to the denylist device group, and then add a rule to the end of your device match rules to exclude that device group from all of your Smart device groups.

Negation is more costly on system performance

If you negate a rule type, the Conductor requires extra processing for every device in a device set. If you choose to use negation in your Device Match Rules (DMRs), consider creating a separate Smart Device Group that stores the result of the negation rule. You can then use this separate group in multiple Device Group Rules with increased system performance.

Use more efficient rule types if possible

To construct Smart Device Groups that run as efficiently as possible, whenever possible, use device match rules for device groups, Airwall Edge Services, and Airwall Gateway groups.

Disable unused rules

Remove or disable unused Smart Device Groups, or have auto-compute disabled until you plan on using them in the future. If left active, they will continually process their rules and may impact performance if changes occur that involve a large number of devices.

Create Airwall Edge Service groups

If you are managing a large number of Airwall Edge Services, you can create **Airwall groups** in the Conductor to simplify administrative tasks.

Once you have **Airwall groups**, you act on them in groups:

- Reboot
- Update firmware

- Install a hotfix
- Disable network communications
- Do Bulk Configuration of Airwall Edge Services on page 378 (you can also select individual Airwall Edge Services for bulk editing)

Note: You can only add Airwall Edge Services to a group if you have permissions to edit them.

To create an **Airwall groups**:

1. Go to **Airwalls**.
2. Check each Airwall Edge Service you want to add to the group.
3. In v2.2.8 and earlier, select **Create Group**.

   In v2.2.10 and later, select **Actions**, then **New group from selection**.
4. Enter a name, description, and tags, and if it is for an Airwall Relay, check **This group is an Airwall relay group**.
5. If you want the group to have network communication disabled when it is created, under **Network communications**, select **Disabled**.
6. Go to the **Airwalls** tab to add additional Airwall Edge Services.
7. Select **Create**.

See MAC address OUI (Manufacturer) Information for Devices

The MAC address OUI (organizationally unique identifier) column shows the manufacturer names for your devices, determined from their MAC address.

1. In the Conductor, go to the **Devices** page and **Devices** tab.
2. Look at the OUI column in the **Devices** list, or open a device page and the OUI is shown under **MAC address**.

If the manufacturer list seems to be out of date, see Update the MAC address (OUI) (Manufacturer) List on page 484.

Search for or Sort Devices by MAC Address OUI (Manufacturer) Name

You can search for devices by the MAC address OUI identifying the manufacturer name for asset management.

Note: If you are not seeing some manufacturers, you may need to Update the MAC address (OUI) (Manufacturer) List on page 484.

To search by manufacturer name

There are two ways to search by manufacturer name:

- **In the ConductorSearch box** at the top right, enter a manufacturer name. Select from the list of matching devices that appears to open that device page.
- **On the Devices page**, in the Filter box, enter a manufacturer name. The **Devices** list is filtered to devices from that manufacturer.

  Note: Search finds the manufacturer's name in any field, so if the manufacturer name appears in other areas, they will be included.

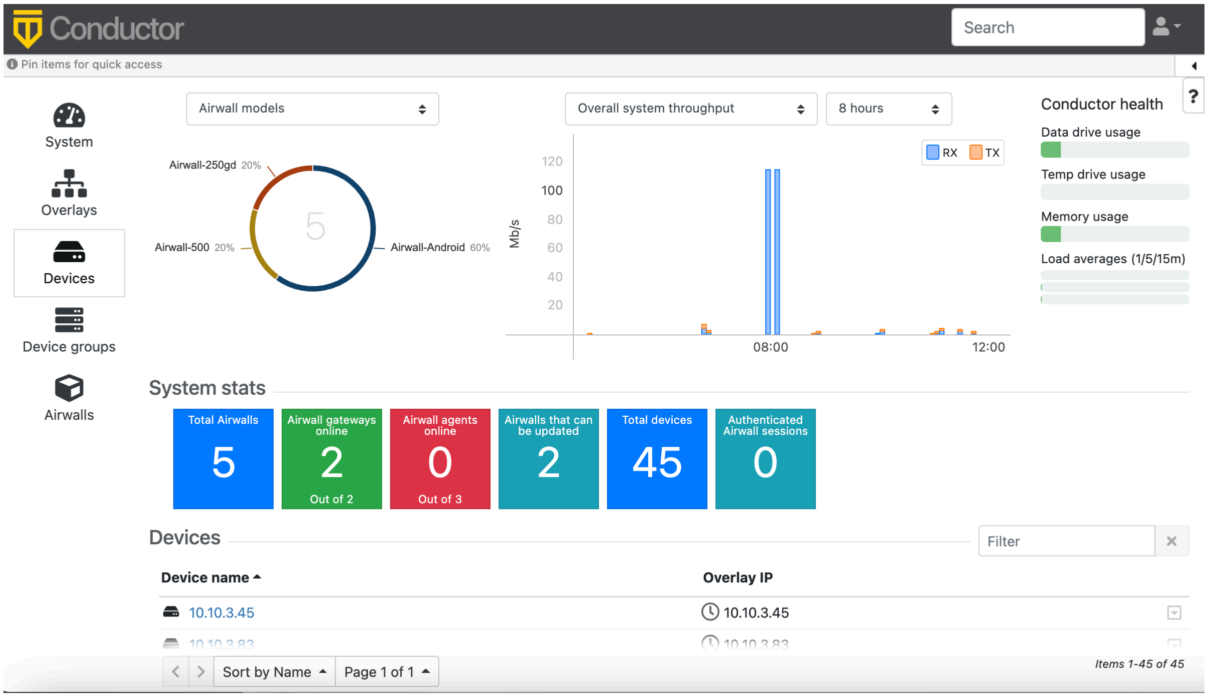
To sort by manufacturer name

On the **Devices** page, in the **Devices** list, click on the **OUI** column header to sort the list by manufacturer.

Manage Overlay Networks in Streamlined View

If you are a Network administrator using the streamlined view in the Conductor, the parts of the Conductor that you do not have access are hidden so you can more easily navigate and manage your overlay networks. You can more easily access your overlays and the devices, Device groups, and Airwall Edge Services in those overlays. Depending on your permissions, you may also be able to see unmanaged Airwall Edge Services.

Here's an example of the devices page in the streamlined view. Select a tile from the System stats to manage, or look below for a list you can click to go to a specific page:



Device name	Overlay IP
10.10.3.45	10.10.3.45
10.10.3.83	10.10.3.83

Note: To check your permissions, select your profile icon ( ) in the upper right, and selecting **Preferences**. You can see your permissions under **User permissions**. For permissions help, contact a Conductor System administrator.

Monitor Activity and Connections

Monitor activity and connections to your Airwall secure network with Conductor Event monitoring and alerting.

Roles	All Administrators for the overlays they have access to.

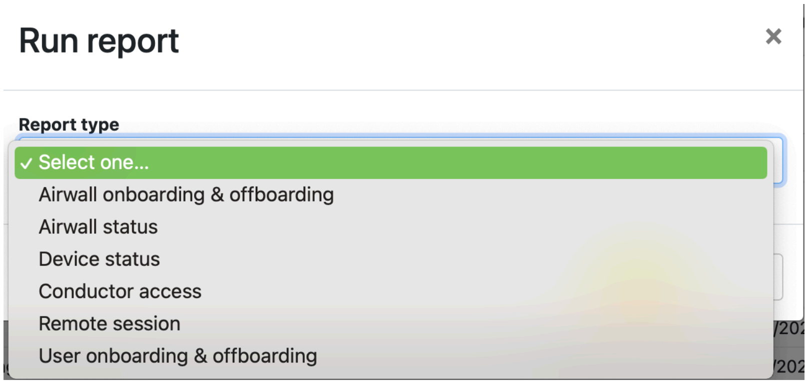
If you are looking to troubleshoot connectivity, see Connection Troubleshooting on page 484.

Run Network Activity Reports

Run reports on different types of activity on your Airwall secure network.

You can create reports for the following network activity:

- Onboarding and offboarding of Airwall Edge Services or users
- Status of Airwall Edge Services or devices
- Conductor local or remote access



Note: You can also check the status of an individual. See Check Status of People Onboarding on page 76.

1. To run a report, go to **Visibility** > **Reports**.
2. Select **Run Report**.
3. Select the type of report to run, and enter any options.
4. Select **Run**.

The report you selected runs and then opens the report results.

View, Download, or Delete a Report

To view, download, or delete a report:

1. Go to **Visibility** > **Reports**.
2. In the list of Reports, find the report you want, and open the menu (click the down arrow on the right).
3. Select **View**, **Download**, or **Delete**.

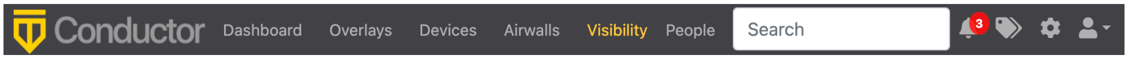
You can also download or delete a report when viewing it.

Monitor Activity with Events and Alerts

Use Events Monitors and Conductor-generated Alerts to create triggers to collect, analyze, and signal events that help you monitor activity and health of your Airwall secure network.

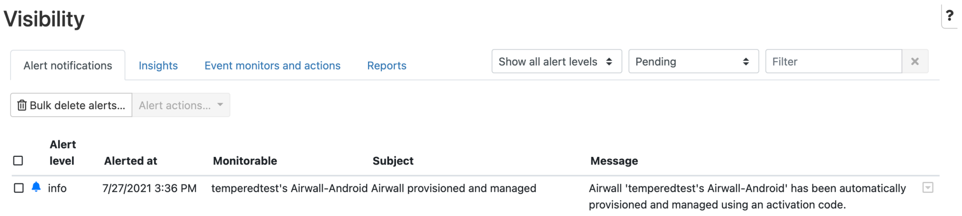
Roles	All Administrators. As a network administrator, you can view and manage event monitors and alerts for the overlays you manage.

To check or set Alerts and Event Monitors, open the **Visibility** page, or click the Bell icon (that indicates if you have alerts) in the upper right corner of the Conductor.



On the **Alert notifications** tab, you can view and take action on alerts.

On the **Event Monitors and actions** tab, you can create, edit, and view the event monitors you've created.



☐	Alert level	Alerted at	Monitorable	Subject	Message
☐	info	7/27/2021 3:36 PM	temperedtest's Airwall-Android	Airwall provisioned and managed	Airwall 'temperedtest's Airwall-Android' has been automatically provisioned and managed using an activation code.

See and Manage Alerts

You can see and manage the alerts for overlays you have permission to see at **Visibility**>**Alert notifications**.

The **Alert notifications** tab shows both the default alerts from the Conductor, as well as the alerts set as actions for triggers on the Event monitors and actions.

You can choose to view alerts, or acknowledge, delete, or both acknowledge and delete alerts.

- **Acknowledge** - When you acknowledge an alert, you acknowledge it for everyone who received that alert. You can add a comment if desired. Other administrators will see the alert has been acknowledged.
- **Delete** - When you delete an alert, you are only deleting for yourself. Other administrators will still see the alert.
- **Acknowledge and Delete** - Do both.

To set which alerts send you emails, see Set your Email Alert Level on page 118.

Manage Alerts from the Visibility page

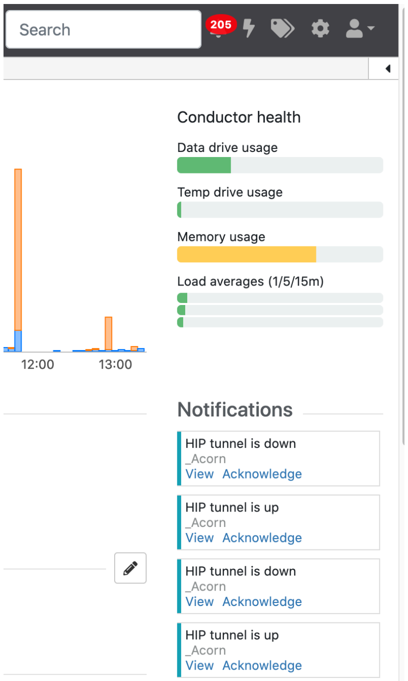
1. Click the Alerts icon 🔔 to open the **Alerts notifications** tab with a list of alerts.
2. Check the box next to one or more alerts, then at the top of the table, select **Alert actions**, and select how to handle the alert.

   Best Practice:

   - *Acknowledge* alerts to indicate that you have checked out the alert and done what is needed to handle it, so other administrators know they do not need to.
   - *Delete* alerts that are not ones you need to handle, or that you no longer need to see.
3. Alternately, you can select the drop down on any alert to view or manage the alert.

Manage Alerts from the Dashboard

1. On the Conductor **Dashboard**, you can see alerts under **Notifications** on the right sidebar under the **Conductor health** section.



Search

205

Conductor health

Data drive usage

Temp drive usage

Memory usage

Load averages (1/5/15m)

Notifications

HIP tunnel is down
_Acorn
View Acknowledge

HIP tunnel is up
_Acorn
View Acknowledge

HIP tunnel is down
_Acorn
View Acknowledge

HIP tunnel is up
_Acorn
View Acknowledge

2. You can select **View** or **Acknowledge** to manage the alert from the Dashboard.

Set your Email Alert Level

Typically, you change your alert level temporarily for support, or to get more insight into what may be happening on your network for troubleshooting. This setting controls the level (and therefore number) of alerts that trigger an email to you when it occurs. If you're a Conductor system administrator, you can also set the level for other Conductor admins.

The default level is None.

In your Conductor profile, you can choose what level of alert triggers an email being sent to you. You can also set the email address and subject prefix for the email.

1. Open the Profile menu in the upper right, and select **Preferences**, or go to the **People** page and select yourself, or, if you have permissions, select an existing person or Add a Person
2. Select **Edit Settings**.
3. Under **Alert email trigger level**, select the alert level to receive email notifications for: **Info** (everything), **Warning** (Warnings and errors), or **Error** (Errors only).
4. Select **Update Settings**

Create an Event Monitor

Create event monitors to help you manage and maintain the health of your Airwall secure network.

Best Practice: Set up Event Monitors to alert when an Airwall Edge Service goes offline.

Some types, models, and versions of Airwall Edge Services do not support all of the monitors. For example, Airwall Agents and Servers do not support remote monitors (ones that run on the Airwall Edge Service), but do support monitors that run on the Conductor.

Note: If you select a group to monitor that contains Airwall Edge Services that do not support the monitor, the monitor ignores the ones that do not support it, but will still trigger for the ones that do.

1. Go to **Visibility** > **Event monitors and actions**.
2. Select **New event monitor**.
3. Select a **Monitor type**:
   - Airwall online/offline
   - Airwall reboot (Remote)
   - Device discovered
   - Health data
   - HIP tunnel (Remote)
   - HTTP GET (Remote)
   - Intrusion prevention (Remote)
   - Link failover (Remote)
   - Ping devices (Remote)
   - Ping IP
   - Traffic stats
   - Viz device attribute
   - Viz event
4. Fill in the options for that type of event monitor, and then click **Create**.
5. On the **Actions** page, add actions that you'd like to happen for this monitor.

   Best Practice: To make sure you are notified about an event, at a minimum, create an **Alert** Action for the monitor and under **Admins to receive this alert**, add a people group for the Admins who should see the alert.
6. After adding each action, select **Create** to add it to the **Action** list.
7. When you're done adding actions, select **Finish**.

For information on permissions and alerts, see Set who sees Event Monitors on page 119.

Set who sees Event Monitors

Set who sees alerts and event monitors

Note: Make sure the people you are adding to an event monitor have permissions that allow them to see the alert. See Understand People Roles (v2.2.13 and earlier) on page 60.

You set who can see an event monitor when you create or edit it. The person or people group must also have permissions to the overlay the monitor is set for.

Best Practice: When you create an Alert Action for the monitor, under **Admins to receive this alert**, add a people group for the Admins in the overlay who should see the alert.

See Create an Event Monitor on page 119 for details.

Event Monitors and Alerts Reference

Descriptions of the Event Monitors and Alerts you can set in the Conductor.

See Also: Create an Event Monitor on page 119 and See and Manage Alerts on page 118.

Definitions

Monitorable objects:

System objects that can be monitored by a particular monitor. For example, an Airwall, Airwall group, device, device group, or **Visibility** (in beta) source.

Event types:

The reasons why a monitor is triggered. The “monitor triggered” event type matches for any reason the monitor was triggered. The “monitor resumed” event type only applies to some monitors. It matches when a monitor has left the state which caused it to trigger. For example, a device’s ping stopped responding, but then it started again.

Templated values:

Data results from a monitored event that can be used in the HTTP call monitor action.You can use these values when integrating monitors with external services. For example, you may want to make an HTTP call that integrates a health data monitor looking at CPU temperature for Airwall Gateways placed in the field. When the temperature exceeds the threshold, it can integrate with an external service to tell a technician which Airwall Gateway exceeded the threshold and what the temperature was. Available templated values are different for each monitor. The monitored_object.* templated value indicates that any field in the API response for that monitored object (be it Airwall or device) can be inserted into the template.

Event Monitors

Descriptions of the event monitors you can set in the Conductor to monitor your Airwall secure network

Airwall online / offline

Detects when an Airwall Edge Service connects to or disconnects from the Conductor. An Airwall can only receive configuration or policy changes while it is connected to the Conductor. This monitor is a proxy indicator for Airwall health but does not explicitly indicate that the Airwall is able to connect with its peers. For more details about Airwall to Airwall connectivity, see the HIP tunnel event monitor.

Monitorable objects:

Airwall Edge Services (Airwall Gateways, Relays, Servers, and Agents), Airwall Groups

Event types

Airwall online, Airwall offline, monitor triggered

Templated values:	monitored_object_id, monitored_object, monitored_object.*, initial_time, status

Airwall reboot

Detects when and why an Airwall Edge Service rebooted.

Monitorable objects:	Airwall Edge Services (Airwall Gateways, Relays, Servers, and Agents), Airwall Groups
Event types:	monitor triggered
Templated values:	monitored_object_id, monitored_object, monitored_object.*, initial_time, reason

Device discovered

Detects when a new device was discovered on an Airwall Gateway.

Monitorable objects:	Airwall Edge Services (Airwall Gateways, Relays, Servers, and Agents), Airwall Groups
Event types:	monitor triggered
Templated values:	monitored_object_id, monitored_object, monitored_object.*, initial_time, device_id, ip, mac

Health data

Monitors health data indicators (fields) such as free memory or CPU temperature. The monitor triggers an event if an expected threshold is exceeded or within a range. For example, you can choose to monitor when the number of active tunnels is >= 100. Not all indicators are supported by every Airwall Edge Service. To see if an indicator is supported for a given Airwall Edge Service, go to the page for the Airwall Edge Service, and check **Reporting** > **Health data**.

Health data indicators:	Memory free, CPU load, CPU temperature, active tunnels, relay sessions, resident memory for HIP, resident memory for the Conductor connection, average CPU frequency.
Monitorable objects:	Airwall Edge Services (Airwall Gateways, Relays, Servers, and Agents), Airwall Groups
Event types:	monitor triggered, monitor resumed
Templated values:	monitored_object_id, monitored_object, monitored_object.*, initial_time, value

HIP tunnel

Detects when a HIP tunnel between two Airwall Edge Services goes up or down. This monitor can be filtered by Airwall peer or the reason the tunnel went up or down.

Tunnel up / down reasons:	Peer opened tunnel, data transmitted, auto-connect, admin request, probe, peer closed tunnel, idle timeout, identity updated, shutdown, incomplete tunnel creation, relay revoked, HIP update packet timed out.

Monitorable objects:	Airwall Edge Services (Airwall Gateways, Relays, Servers, and Agents)
Event types:	tunnel up, tunnel down, monitor triggered
Templated values:	monitored_object_id, monitored_object, monitored_object.*, initial_time, status, remote_peer_id

HTTP GET

Makes HTTP GET requests to check the status of an HTTP server. The response code can be checked or a regex is used against the body of the response. Useful to ensure that the HTTP healthcheck is up.

Monitorable objects:	Airwall Edge Services (Airwall Gateways, Relays, Servers, and Agents)
Event types:	regex match failed, response code failed, monitor triggered, monitor resumed
Templated values:	monitored_object_id, monitored_object, monitored_object.*, initial_time, status, response_code, error

Intrusion prevention

Runs an intrusion prevention monitor on the Airwall Edge Service to monitor a selected port group and detect suspicious activity on the network. The monitor triggers events when the monitor matches traffic to the selected rule set. If the monitor detects multiple instances of suspicious activity in one reporting interval, they are batched together and sent as a single event to the Conductor. You can adjust the reporting frequency on the monitored Airwall Edge Service to increase or decrease the rate of reporting monitored events to the Conductor.

Monitorable objects:	Airwall Edge Services (Airwall Gateways, Relays, Servers, and Agents)
Event types:	info level event, warning level event, error level event, monitor triggered
Templated values:	monitored_object_id, monitored_object, monitored_object.*, initial_time

Link failover

Detects when an Airwall Edge Service has a link failover event.

Monitorable objects:	Airwall Edge Services (Airwall Gateways, Relays, Servers, and Agents), Airwall Groups
Event types:	monitor triggered
Templated values:	monitored_object_id, monitored_object, monitored_object.*, initial_time, old_link, new_link

Ping devices

Send a ping from Airwall Gateways to local devices. Detects when the ping fails or exceeds an indicated timeout.

Monitorable objects:	devices, device groups

Event types:	timed out, round-trip time exceeded, no route to IP, monitor triggered, monitor resumed
Templated values:	monitored_object_id, monitored_object, monitored_object.*, initial_time, status, rtt

Ping IP

Send a ping from an Airwall Gateway to the indicated IP address. Detects when the ping fails or exceeds an indicated timeout.

Monitorable objects:	Airwall Edge Services (Airwall Gateways, Relays, Servers, and Agents)
Event types:	timed out, round-trip time exceeded, no route to IP, monitor triggered, monitor resumed
Templated values:	monitored_object_id, monitored_object, monitored_object.*, initial_time, status, rtt

Traffic stats

Detects overlay or underlay traffic on an Airwall Edge Service – sent, received, or both. Monitor triggers based on thresholds set in the monitor.

Monitorable objects:	Airwall Edge Services (Airwall Gateways, Relays, Servers, and Agents), Airwall Groups
Event types:	monitor triggered, monitor resumed
Templated values:	monitored_object_id, monitored_object, monitored_object.*, initial_time, value

Event Actions

All event actions filter based on event types. For instance, you can choose to only get an alert for intrusion detection events you've set at the warning or error level.

Alert

Receive an alert in the Conductor or email.

Alert level:	Can be info, warning, or error. You can filter alerts based on level and have only certain alert levels sent out in email.
Show alert on dashboard:	Disable if this alert should not be shown on the dashboard
Admins to receive this alert:	By default, all system administrators receive the alert. Select specific people or people groups to restrict who receives the alert.

Enable/Disable

Enable or disable the monitorable. For example, can be used to automatically disable Airwall Edge Services that have triggered an error level intrusion detection.

Apply this action to something other than the monitored object:	Apply the operation to something else
Operation to perform:	Enable or disable
Target:	What to apply the operation to.

HTTP call

Make an HTTP call. Can use templated values from the monitor to customize the call. Can be used to integrate monitors with an external service.

URL / IP address:	Server to make HTTP call against.
Body:	HTTP body. Only applies to HTTP methods that can have a body.
HTTP method:	The HTTP method to use: GET, POST, PUT, PATCH, or DELETE.
SSL verification:	Verify the authenticity of the SSL cert for HTTPS requests.
Headers:	HTTP headers to include in requests. Headers are in the format 'Content-Type:application/json' (without quotation marks) and comma-separated to include more than one.

Reboot

Reboot the monitorable.

Apply this action to something other than the monitored object:	Apply the operation to something else
Target:	What to apply the operation to

Tag add/remove

Add or remove a tag or tags from the monitorable. May also be applied to system objects with a different tag.

Add:	Tags to add
Remove:	Tags to remove

Tag enable/disable

Enable and / or disable system objects with a tag. For example, all objects with the tag “tempered” can be enabled if this action is performed.

Enable:	Enable any system objects with these tags.
Disable:	Disable any system objects with these tags.

Monitor Connections to your Airwall secure network

The Conductor has several ways to monitor the people, Airwall Edge Services, and devices that are connecting to your Airwall secure network.

Monitor Connections from the Dashboard

The graphs and **System stats** tiles on the Conductor dashboard give you several quick views into the status of your Airwall secure network.

Note: Select a tile from **System Stats** to open up a more detailed view below under **Navigation**.

For more details, see The Conductor Dashboard on page 32.

Monitor and Manage Remote Sessions

1. In the Conductor, go to **People**.
2. Filter the people list, if desired.
3. In the **People** list, look at the clock icons at the end of the row. The clock icon shows by color the last time the person signed in, and you can hover over it to see the time and date they last signed in:

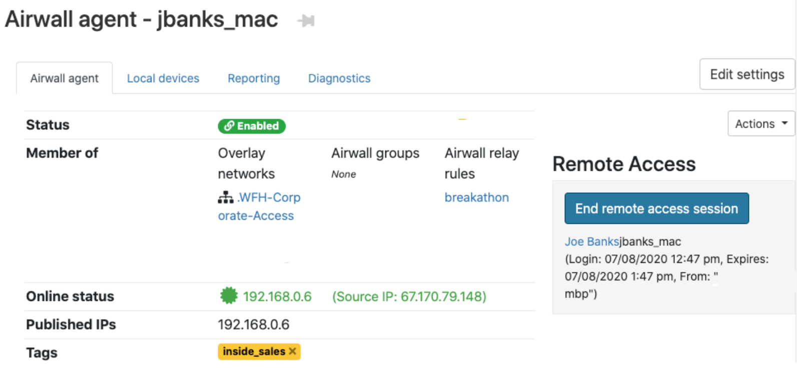
Icon	What it means
🕓	In the last 24 hrs
🕓	In the last week
🕓	More than a week ago
🕓	Never

Note: If you see a plug icon, it is an indicator of the state of user onboarding. See **Monitor User Onboarding** below for more details.

You can also open up the page for a person, and see their connected devices under People groups on the right. Click to open up any connected Airwall Agent or Server (that you have permissions to see), and review or end a remote access session.

- **To review the remote access session**, see the details in the **Remote Access** tile.
- **To end the remote access session**, select **End remote access session**.

Note: The Remote Access tile only appears when there is an active remote session.



Status	Enabled		
Member of	Overlay networks .WFH-Corporate-Access	Airwall groups *None*	Airwall relay rules breakathon
Online status	192.168.0.6 (Source IP: 67.170.79.148)		
Published IPs	192.168.0.6		
Tags	inside_sales ×		

Remote Access

Joe Banksjbanks_mac
(Login: 07/08/2020 12:47 pm, Expires: 07/08/2020 1:47 pm, From: " mbp")

Monitor User Onboarding Airwall Invitations and Activation Codes

Once you've sent out **Airwall Invitations** or started onboarding with Activation Codes, you can review which activations have been accepted, are still active, or have expired.

1. In the Conductor, go to **People**.

2. Filter the people list, if desired.
3. In the **People** list, look at the plug 🔌 icons at the end of the row. The plug icon indicates the person has been sent an activation codes or Airwall Invitation. Hover over the icon to see how many are active.:

Icon	What it means
🔌	If the plug is black, the person has unused, non-expired activation codes or invites available.
🔌	If the plug is grey, the person has used all of their activation codes or invites, or they've all expired.
No plug icon	This person has not received an activation code or invite.

Note: The clock icons are indicators of when a person last logged in. See **Monitor and Manage Remote Sessions** above for more details.

Monitor Device Status

1. In the Conductor, go to **Devices**.
2. Filter the device list, if desired.
3. In the **Device** list, look at the clock icons next to the **Overlay IP** column. The clock icon shows by color the last time the device was online. Hover over the icon to see the last time and date the device was active:

Icon	What it means
Dark Green 🕓	Currently online
🕓	Has been online in the past
🕓	Has never been online

For more information on the icons you might see in the Conductor and what they mean, see Conductor Icon Reference on page 35.

Visibility Insights

Update your Conductor and Airwall Edge Services

Update firmware and software, and maintain your Conductor and Airwall Edge Services.

You must be a System Administrator to apply firmware updates to the Conductor and Airwall Edge Services.

As an administrator, you deploy firmware updates to your Conductor and all Airwall Gateways from the Conductor, or you can manually update the firmware on individual Airwall Gateways using diagnostic mode.

Manage Versions of Airwall Agents and Servers

As an administrator of an Airwall secure network, you can manage which versions of software the Airwall Agents and Servers accessing your secure network use.

You do this by setting the version of Airwall Agents and Servers offered for people to install.

Important: This feature is deprecated in v3.1.1 and will be obsolete in v3.2.

To set versions of Airwall Agents and Servers offered:

1. Log in to the Conductor with a system administrator account.
2. Go to **Settings**, **Advanced**.
3. Under **Global Airwall Agent Settings**, select **Edit Settings**.
4. Under **Preferred Airwall agent version**, select the version you prefer.

The version you selected is now automatically provided to people when you onboard them using **Airwall Invitations**, Activation codes, or People Groups.

Update Conductor Firmware

How to update the firmware for an Airwall Conductor.

Roles	System Administrators

Firmware downloads

Important: Before you roll out a Conductor firmware update, create, download, and archive a Conductor database backup. See Create a Conductor database backup on page 479.

If your Conductor has access to Tempered's release repository on the Internet, the latest firmware downloads for your Conductor (and Airwall Edge Services) are automatically available on the Conductor **Settings** page. Otherwise, you can download the software from Latest firmware and software on page 514 and upload it to your Conductor.

Update non-HA Conductor firmware

CAUTION: When you are updating firmware, stay on the page (do not navigate away or log out). If something interrupts a Conductor firmware update (for example by a power outage), it may leave the Conductor in a corrupted state.

1. Log in to the Conductor using a system administrator account.
2. Go to **Settings** > **General Settings** > **Firmware Updates**, and find the version you want.

   Note: You can also download firmware from Latest firmware and software on page 514 and then upload it to the Conductor.
3. For the update you want, select **Download**. The Conductor downloads the update to your Conductor.

   Note: If you're uploading the firmware update, select **Upload Firmware**, select the Conductor firmware file you downloaded, and then select **Upload**. Wait on that page until the upload is complete.
4. When it completes, select **Install** to install the update.

Verify the firmware version under the **Configuration** section on the **Settings** page.

Update a Conductor HA pair

When upgrading a pair of HA Conductors, the sequence in which you perform the steps below between master and standby is critical:

1. Download, **but do not install**, the new firmware to the current **active** Conductor 1.
2. Install the new firmware on the **standby** Conductor 2 **first**. When it finishes the update, it reboots and becomes an active Conductor.
3. Install the new firmware on the now original active Conductor 1.
4. Last, demote the former standby Conductor 2 to the standby role

This table shows the sequence of the update.

Step	Conductor 1	Conductor 2
1	Active Download firmware to the current active Conductor 1	Standby
Result: *The HA pair synchronizes the firmware update so it is available on Conductor 2*		
2	Active	Standby Install the firmware update on Conductor 2
Result: *After the update, Conductor 2 reboots, and becomes active, so both Conductors are active. This prevents replication from happening while you complete the update of the HA pair.*		
3	Active Install the firmware update to Conductor 1.	Active
Result: *Both Conductors are updated and both are active.*		
4	Active	Active Return Conductor 2 to the standby role.
Result: *The HA pair is updated with no interruptions to service, and return to normal operation.*		
	Active	Standby

Detailed instructions to update an HA pair

1. Log in to the ***active*** Conductor 1 using a system administrator account.

   CAUTION: During the update process, stay connected to the Conductor, and do not navigate away from the UI. Uploads and updates may take several minutes to complete. If the Conductor firmware update is interrupted (for example by a power outage), it may leave the Conductor in a corrupted state.
2. Go to **Settings** > **General Settings** > **Firmware Updates**, open the version subtab, and find the Conductor update you want to install.
3. To the right of the update, select **Download**. Stay on the page while it downloads.
4. Log out of the active Conductor, and log in to the ***standby***.
5. Go to **Settings** > **General Settings** > **Firmware Updates**, and open the version subtab. The new firmware update has synced from the active Conductor and should be listed in the **Firmware Update** section.
6. On the ***standby*** Conductor, for the update you want, select **Install**. Stay on the page until the installation completes. After the update installs successfully, the standby Conductor reboots and becomes an active Conductor.
7. Log in to the ***original active*** Conductor 1, and go to **Settings** > **General Settings** > **Firmware Updates**.
8. Next to the update you want, again select **Install**. Stay on the page until the installation completes. After the update installs successfully, the Conductor 1 reboots.
9. Log back in to the ***original standby*** Conductor 2 and go to **Settings**. In the **Airwall Conductor high availability** section, select **Edit Settings** and then select **Demote to standby**.

Update Airwall Gateway firmware

Administrators can update the firmware for provisioned and managed Airwall Gateways directly from the Conductor. You cannot update Airwall Gateways in the factory reset state – you must provision and manage them first.

Roles	System Administrators – Download and update Network Administrators with permissions to the Airwall Gateways – Update

You can update firmware on individual Airwall Edge Services or apply updates to groups.

CAUTION: To prevent data loss and potential corruption, it is critical that Airwall Gateways remain powered on during the firmware update process. A loss of power during the firmware update process may leave the Airwall Gateway in a corrupted state.

Note: During the update process, Airwall Gateways go offline for a few minutes as they install the firmware update and then reboot. See the current state of any Airwall Gateway on the Airwall Edge Services page.

You can also manually updateAirwall Gateways not currently connected to a Conductor. For more information, refer to your model's Product Guide.

Download Airwall Edge Services firmware updates

In v2.2.8 and later, the Conductor Settings page shows a list of the Firmware updates available for your Airwall secure network, and makes it easy to download and install firmware updates.

Download firmware updates (v2.2.8 and later)

1. Log in to the Conductor with a system administrator account.
2. Go to **Settings** > **General Settings**.
3. Under **Firmware updates**, select **Check for Updates**. The Conductor displays the updates are available for your Airwall Edge Services.
4. If you have more than one version available, select the tab for the version you want.
5. Find the firmware updates you want to apply, and select **Download** to download each update. When they finish downloading, the **Download** links change to **Install**.
6. Select **Install** and check the boxes for the Airwall Edge Services to apply it to the next time they connect to your Airwall secure network.
7. Select **Apply** to start the installation.

You can also update a group of Airwall Edge Services. For more information, see Update firmware for a group of Airwall Edge Services on page 131.

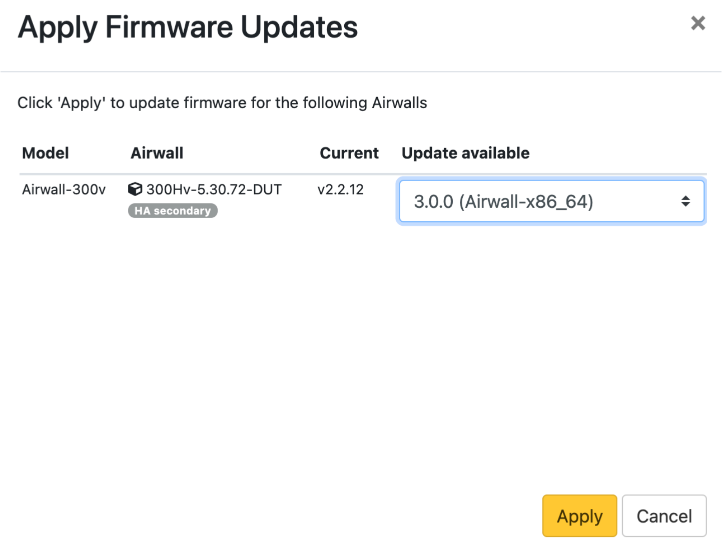
Download firmware updates (v2.2.5 and earlier)

1. Download the relevant Airwall Gateway firmware files for your Airwall Gateway models, and save them on the computer you use to access the Conductor.
2. Log in to the Conductor as a System Administrator.
3. Go to the **Settings** > **General Settings**, and click **Upload firmware**.
4. Select the Airwall Gateway firmware file and click **Upload**.

Update Airwall Gateway firmware

You can update the firmware for a single Airwall Gateway from the **Airwalls** page.

1. Go the **Airwalls** page.
2. For the Airwall Edge Service you want to update, open the **Actions** menu and select **Update Firmware**.
3. Select the version you want to install and then select **Apply**.



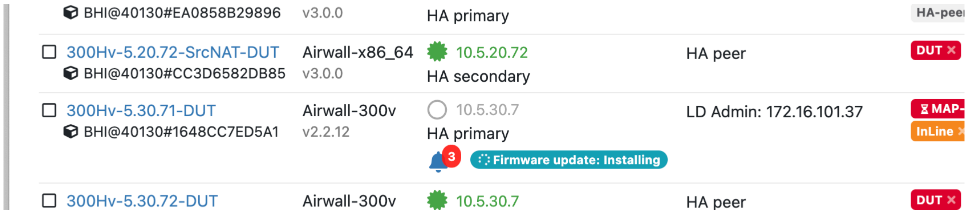
Apply Firmware Updates

Click 'Apply' to update firmware for the following Airwalls

Model	Airwall	Current	Update available
Airwall-300v	300Hv-5.30.72-DUT HA secondary	v2.2.12	3.0.0 (Airwall-x86_64)

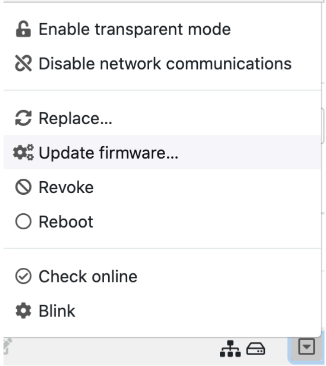
Note: If you are updating a virtual Airwall Gateway, and receive a message that the disk space is too low, see Expand the Disk Size for a virtual Airwall Gateway on page 311.

4. The installation process starts, and can take several minutes to complete.

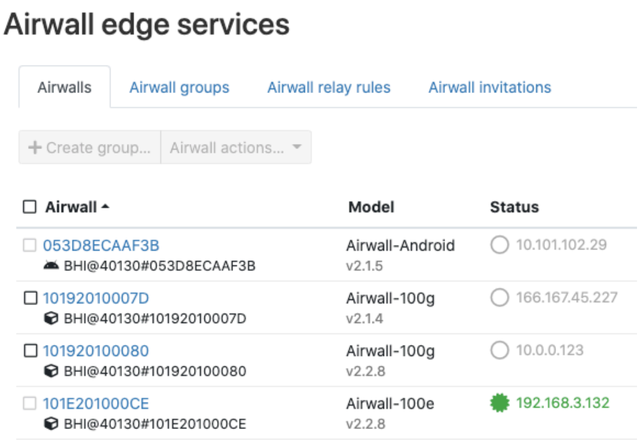


BHI@40130#EA0858B29896	v3.0.0	HA primary		HA-peer
☐ 300Hv-5.20.72-SrcNAT-DUT BHI@40130#CC3D6582DB85	Airwall-x86_64 v3.0.0	10.5.20.72 HA secondary	HA peer	DUT ×
☐ 300Hv-5.30.71-DUT BHI@40130#1648CC7ED5A1	Airwall-300v v2.2.12	○ 10.5.30.7 HA primary 3 Firmware update: Installing	LD Admin: 172.16.101.37	MAP- InLine
☐ 300Hv-5.30.72-DUT	Airwall-300v	10.5.30.7	HA peer	DUT ×

Note: The **Update firmware** option is only available if there is a current update available for that Airwall Gateway.



5. After the Airwall Gateway reboots, go to the **Airwalls** page, and verify that the new firmware version is displayed in the **Model** column.


Airwall edge services

□ Airwall ▴	Model	Status
□ 053D8ECAAF3B BHI@40130#053D8ECAAF3B	Airwall-Android v2.1.5	○ 10.101.102.29
□ 10192010007D BHI@40130#10192010007D	Airwall-100g v2.1.4	○ 166.167.45.227
□ 101920100080 BHI@40130#101920100080	Airwall-100g v2.2.8	○ 10.0.0.123
□ 101E201000CE BHI@40130#101E201000CE	Airwall-100e v2.2.8	● 192.168.3.132

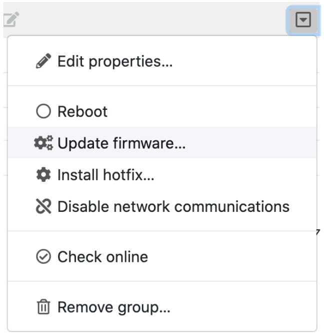
Update firmware for a group of Airwall Edge Services

There are two ways to update firmware for multiple Airwall Edge Services at a time. One is to update using Airwall groups, and the other is to update by firmware update package.

Roles	System Administrators Network Administrators with permissions to the Airwall Gateways and Overlays

Update by Airwall group

1. Log in to the Conductor as a system administrator.
2. Open the **Airwalls** page and select **Airwall groups**.
3. Find the group you want to update, and from the **Actions** menu, select **Update Firmware**. The firmware update process starts for all Airwall Edge Services in the group, and can take several minutes to complete and come back online.



4. Complete the above steps for each group that requires the firmware update.
5. Once complete, go to the **Airwalls** page, and verify that the new firmware version is displayed for each updated Airwall Edge Service.

Update by firmware update package

1. Log in as a system administrator to the Conductor.
2. Go to **Settings** > **General Settings**.
3. If you have more than one version available, under **Firmware updates**,select the tab for the version you want.
4. Find the firmware update you want to apply, and select **Download** to download the update.
5. When it is finished downloading, select **Install**.
6. On the **Apply Firmware Updates** page, check the box next to the Airwall Edge Services you want to update.

7. Select **Apply**. The firmware update process starts for all checked Airwall Edge Services, and can take several minutes to complete and come back online.

Replace an Airwall Gateway

An Airwall Gateway that is a member of one or more overlay networks can be replaced by an unassigned Airwall Gateway (that is, it is not a member of any overlay network).

Roles	System Administrators Network Administrators with permissions to the Airwall Gateways and Overlays

1. On the **Settings** page, go to **Licensing** tab and grant provisioning requests for the new Airwall Edge Service.
2. On the **Dashboard**, or the **Airwalls** page, find the Airwall Edge Service you want to replace.
3. Open the drop-down to the right of the Airwall Edge Service you want to replace and select **Replace**.
4. In the wizard, select the desired replacement Airwall Edge Service from the list of available replacements and click **Next**.

   Note: The wizard only lists unassigned Airwall Edge Services. If the replacement is still used in any overlay networks, you need to remove it from all overlay networks before you can select it as a replacement.
5. If you are replacing an Airwall Gateway, check if your replacement Airwall Gateway meets the requirements to transfer the port configuration:
   - Must be port-compatible with the Airwall Gateway it is replacing. Airwall Gateway are port compatible if they belong to the same model group (300x, 400x, etc.) and the replacement Airwall Gateway has at least as many ports as those in use on the Airwall Gateway being replaced.
   - Must not use any ports in underlay or HA port group configurations that are used in overlay port groups on the Airwall Gateway being replaced.
   - Must use the same number or fewer underlay port groups, and all ports used in those port groups are also used as underlay ports on the Airwall Gateway being replaced.
   - Must be online.
6. **Skip to the last step if:**
   - You are not replacing an Airwall Gateway
   - You do not want to replicate the port configuration.
   - Your replacement Airwall Gateway doesn't meet the requirements to replicate the port configuration.
7. **If your replacement Airwall Gateway meets the requirements listed above and you want to replicate the port configuration:**

   a) To transfer any static underlay IP configurations to the replacement, check **Transfer underlay IP addresses**.

   b) If the Airwall Edge Service being replaced uses a public IP, check **Transfer public IP addresses** to transfer it to the replacement.

   c) Initiate the port configuration transfer by selecting **Transfer port configuration**. The Conductor applies the new port configuration to the replacement Airwall Gateway.

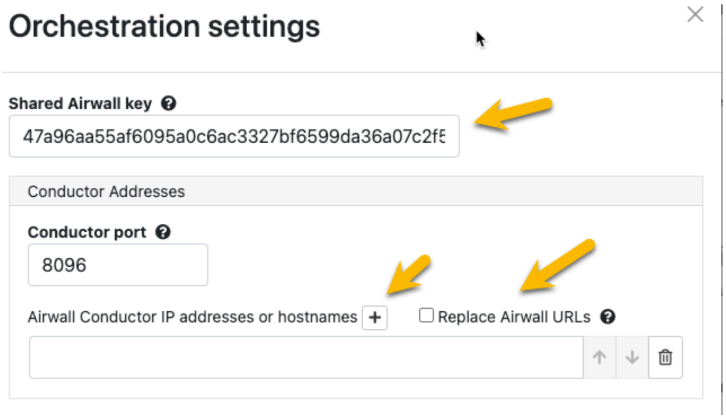
   d) When you see the confirmation that the transfer completed successfully, select **Next**.
8. Select **Finish** to complete the replacement.

When the replacement is complete, the new Airwall Edge Service is configured with the same overlay network membership, policy configurations, and user-specified information as the replaced Airwall Edge Service. A replacement Airwall Gateway will also have the same port configuration if it met the requirements and you chose to replicate them.

Move an Airwall Gateway to a Different Conductor

You can move an Airwall Gateway to a different Conductor by configuring the same Shared Airwall key between two Conductors.

1. On the old Conductor, in **Settings** > **Orchestration settings**, under **Conductor Addresses**, add the new Conductor as if it was another address or hostname for the old Conductor. The new Conductor's address should be the first one on the list.
2. Copy the old Conductor's **Shared Airwall key** from the box in the user interface.



Orchestration settings

Shared Airwall key

47a96aa55af6095a0c6ac3327bf6599da36a07c2f

Conductor Addresses

Conductor port

8096

Airwall Conductor IP addresses or hostnames

□ Replace Airwall URLs

3. In the new Conductor, in **Settings** > **Orchestration settings**, under **Shared Airwall key**, set the **Shared Airwall key** that was copied in the step above.
4. Reboot the Airwall Gateway from the user interface.
5. Leave the old Conductor on until all Airwall Gateways you want to move have connected to the new Conductor.

Note: As the moved Airwall Gateways connect to the new Conductor, they show up as unmanaged.

6. Shut off the old Conductor.

Back Up your Conductor and Airwall Edge Services

Back up your Conductor

Best practice is to back up your Conductor database on a regular basis.

1. In the Conductor, go to **Settings**, and open the **Diagnostics** tab.
2. Select **Download Database Backup**.

This backs up your Conductor database. To restore from a backup, see Restore your Conductor from a database backup on page 133.

Restore your Conductor from a database backup

If there are unexpected side effects or changes or updates to your Conductor, you can restore it from a database backup. A database backup restores everything except network configuration and SSL certificates. If you restore to the same Conductor, your network configuration and SSL certificates are maintained. If you restore to a different Conductor, it restores the database without changing the new Conductor's network and SSL configuration.

1. In the Conductor you want to restore, go to **Settings**, and open the **Diagnostics** tab.
2. Select **Restore Database Backup**.

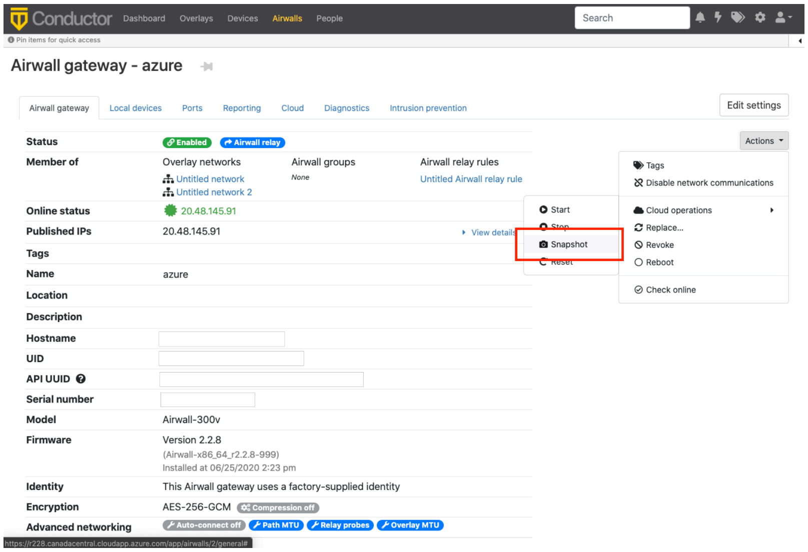
This restores your Conductor database. To back up your database, see Back up your Conductor on page 133.

Back up Azure Airwall Gateway 300v

You can back up your Azure Airwall Gateway by taking a snapshot in the Conductor.

1. Open the Airwall Gateway that you want to take a snapshot of.

2. On the **Actions** menu, open **Cloud Operations**, and select **Snapshot**.

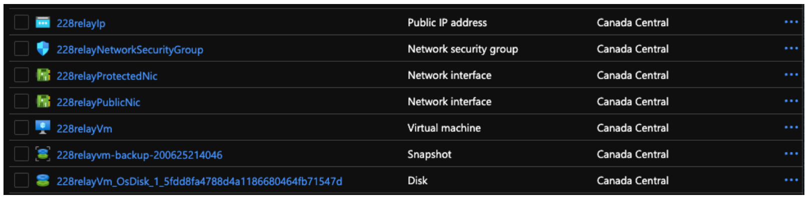


Airwall gateway - azure

Status	Enabled Airwall relay
Member of	Overlay networks: Untitled network, Untitled network 2 Airwall groups: None Airwall relay rules: Untitled Airwall relay rule
Online status	20.48.145.91
Published IPs	20.48.145.91
Tags	
Name	azure
Location	
Description	
Hostname	
UID	
API UUID	
Serial number	
Model	Airwall-300v
Firmware	Version 2.2.8 (Airwall-x86_64_r2.2.8-999) Installed at 06/25/2020 2:23 pm
Identity	This Airwall gateway uses a factory-supplied identity
Encryption	AES-256-GCM Compression off
Advanced networking	Auto-connect off Path MTU Relay probes Overlay MTU

https://r228.canadacentral.cloudapp.azure.com/app/airwalls/2/general#

The Conductor creates a Snapshot object in the same Azure resource group that your Airwall Gateway Virtual Machine is in.

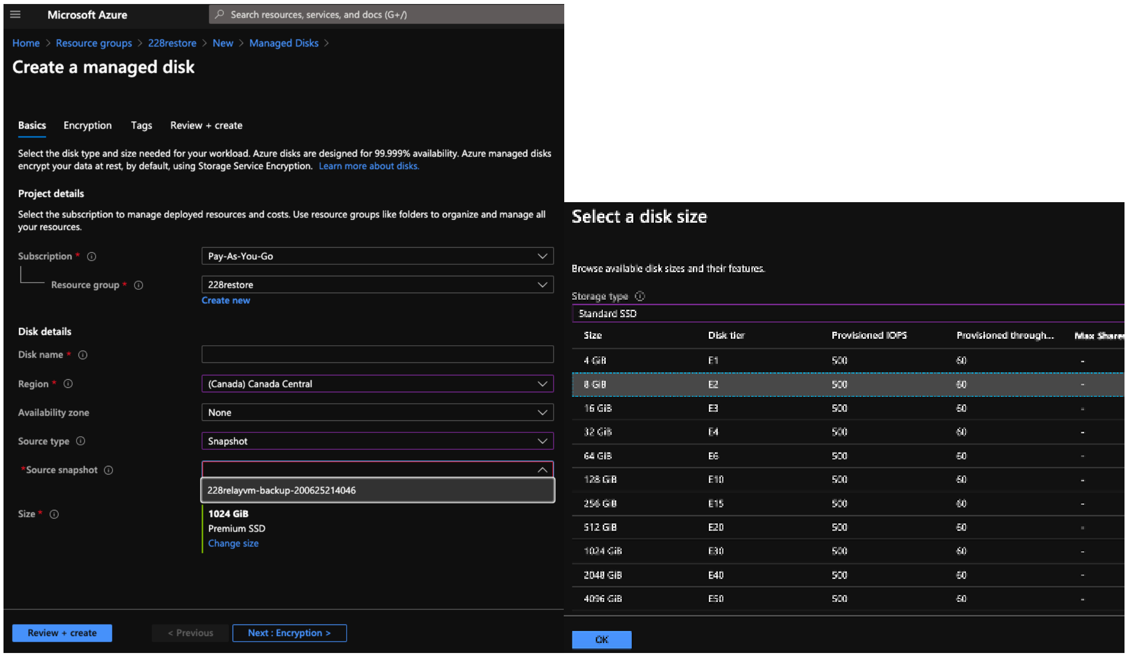


228relayIp	Public IP address	Canada Central
228relayNetworkSecurityGroup	Network security group	Canada Central
228relayProtectedNic	Network interface	Canada Central
228relayPublicNic	Network interface	Canada Central
228relayVm	Virtual machine	Canada Central
228relayvm-backup-200625214046	Snapshot	Canada Central
228relayVm_OsDisk_1_5fdd8fa4788d4a1186680464fb71547d	Disk	Canada Central

Restore an Azure Cloud Airwall Gateway

If you've backed up your Azure Cloud Airwall Gateway by creating a snapshot, this is how you restore it.

1. Create a new Azure resource group to store the restored Cloud Airwall Gateway.
2. In that resource group, create a **Managed disk object** that uses the Snapshot from your existing Airwall Gateway as the source.
3. Next to **Size**, select **Change size**, and change the **Storage type** and **Size** of the disk based on your requirements by selecting a disk size, and then selecting **Ok**.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Resource groups > 228restore > New > Managed Disks >
Basics
Encryption
Tags
Review + create
Review + create
< Previous
Next : Encryption >
OK

Create a managed disk

Select the disk type and size needed for your workload. Azure disks are designed for 99.999% availability. Azure managed disks encrypt your data at rest, by default, using Storage Service Encryption. Learn more about disks.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	Pay-As-You-Go
Resource group *	228restore Create new

Disk details

Disk name *	
Region *	(Canada) Canada Central
Availability zone	None
Source type	Snapshot
*Source snapshot	228relayvm-backup-200625214046
Size *	1024 GiB Premium SSD Change size

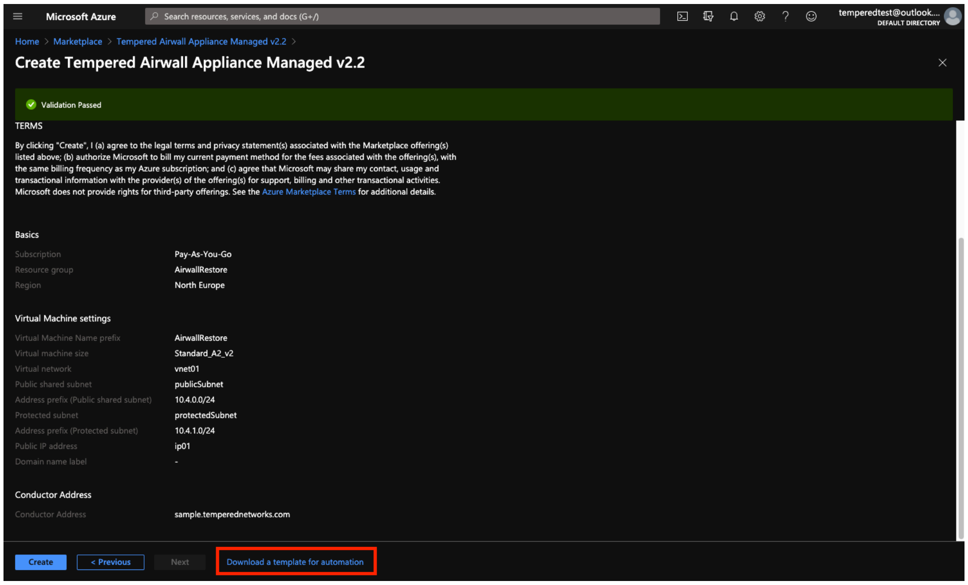
Select a disk size

Browse available disk sizes and their features.

Storage type: Standard SSD

Size	Disk tier	Provisioned IOPS	Provisioned through...	Max Share
4 GiB	E1	500	60	-
8 GiB	E2	500	60	-
16 GiB	E3	500	60	-
32 GiB	E4	500	60	-
64 GiB	E6	500	60	-
128 GiB	E10	500	60	-
256 GiB	E15	500	60	-
512 GiB	E20	500	60	-
1024 GiB	E30	500	60	-
2048 GiB	E40	500	60	-
4096 GiB	E50	500	60	-

4. Make sure the resource group and the managed disk are in the same region as the original Airwall Gateway.
5. From the Azure Marketplace, start creating a new Managed Airwall Gateway.
6. Select your new resource group as the destination and continue to fill out the form as you would a normal deployment.
7. Rather than finalizing the deployment, on the final screen, select **Download a Template for Automation** instead.


Microsoft Azure
Search resources, services, and docs (G+/)
temperedtest@outlook....
DEFAULT DIRECTORY
Home > Marketplace > Tempered Airwall Appliance Managed v2.2 >
Create
< Previous
Next
Download a template for automation

Create Tempered Airwall Appliance Managed v2.2

Validation Passed

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the Azure Marketplace Terms for additional details.

Basics

Subscription	Pay-As-You-Go
Resource group	AirwallRestore
Region	North Europe

Virtual Machine settings

Virtual Machine Name prefix	AirwallRestore
Virtual machine size	Standard_A2_v2
Virtual network	vnet01
Public shared subnet	publicSubnet
Address prefix (Public shared subnet)	10.4.0.0/24
Protected subnet	protectedSubnet
Address prefix (Protected subnet)	10.4.1.0/24
Public IP address	ip01
Domain name label	-

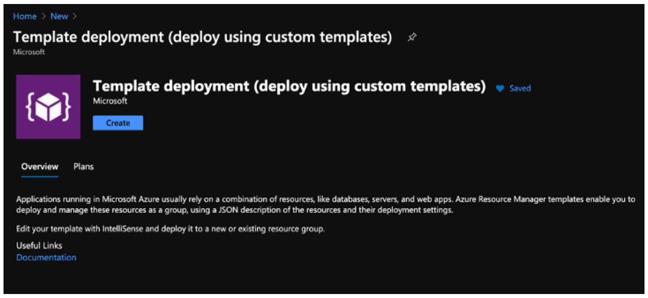
Conductor Address

Conductor Address	sample.temperednetworks.com

8. On the next screen, click the **Download** link in the upper left. You should get a .zip file with two .json files.
9. Unzip the files, and modify the template.json file as follows:
   a) Remove the `osProfile` properties portion of the template.
   b) Change the `storageProfile` properties to the following, filling the values for the managed disk created earlier

```
"storageProfile": {
  "osDisk": {
    "createOption": "attach",
    "osType": "Linux",
      "managedDisk": {
        "id": "/subscriptions/{subscription_id}/resourceGroups/
{resourcegroup_name}/providers/Microsoft.Compute/disks/
{managed_disk_name}"
      }
    }
},
```

10. Create a new Azure Template.

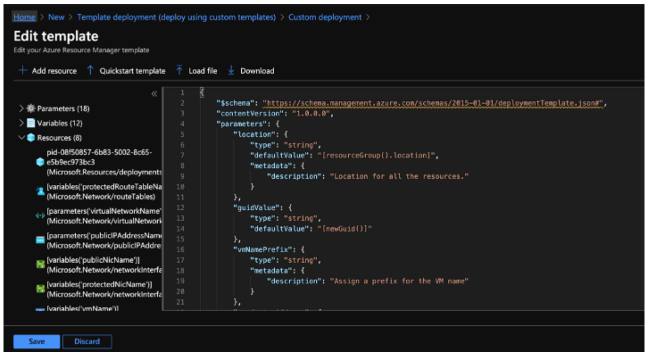

Home > New >
Template deployment (deploy using custom templates)
Microsoft
Template deployment (deploy using custom templates)
Saved
Microsoft
Create
Overview
Plans

Applications running in Microsoft Azure usually rely on a combination of resources, like databases, servers, and web apps. Azure Resource Manager templates enable you to deploy and manage these resources as a group, using a JSON description of the resources and their deployment settings.

Edit your template with IntelliSense and deploy it to a new or existing resource group.

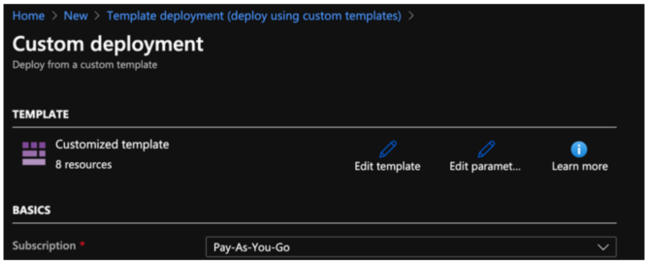
Useful Links
Documentation

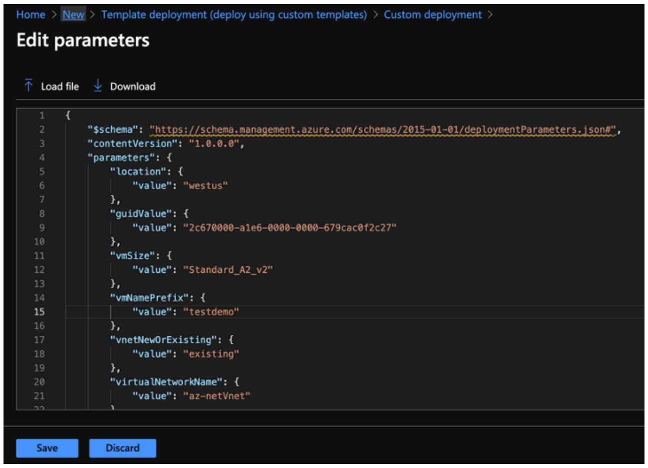
11. Select **Build your own template in the editor**, and copy the contents of template.json into the text field, and then select **Save**.


Home > New > Template deployment (deploy using custom templates) > Custom deployment >
Edit template
Edit your Azure Resource Manager template
Add resource
Quickstart template
Load file
Download
Parameters (18)
Variables (12)
Resources (8)
pid-08f50857-6b83-5002-8c65-e5b9ec973bc3 (Microsoft.Resources/deployments
[variables('protectedRouteTableNa (Microsoft.Network/routeTables)
[parameters('virtualNetworkName' (Microsoft.Network/virtualNetwork
[parameters('publicIPAddressNam (Microsoft.Network/publicIPAddre
[variables('publicNicName')] (Microsoft.Network/networkInterfa
[variables('protectedNicName')] (Microsoft.Network/networkInterfa
[variables('vmName')]
Save
Discard

```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "location": {
            "type": "string",
            "defaultValue": "[resourceGroup().location]",
            "metadata": {
                "description": "Location for all the resources."
            }
        },
        "guidValue": {
            "type": "string",
            "defaultValue": "[newGuid()]"
        },
        "vmNamePrefix": {
            "type": "string",
            "metadata": {
                "description": "Assign a prefix for the VM name"
            }
        },
```

12. Select the **Edit parameters** at the top of the form and paste the contents of parameters.json into the displayed field and select **Save**.

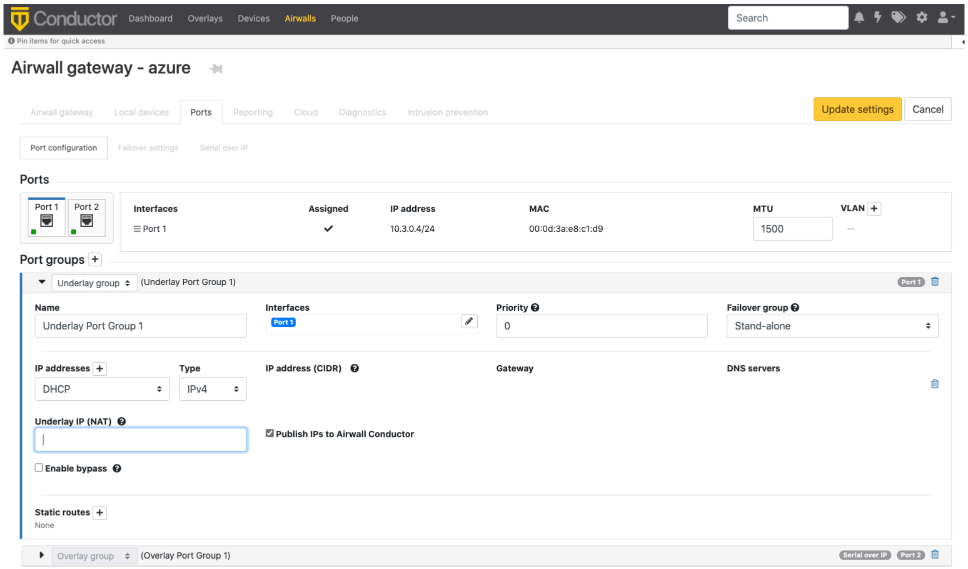



Home > New > Template deployment (deploy using custom templates) > Custom deployment >
Edit parameters
Load file
Download
Save
Discard

```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "location": {
            "value": "westus"
        },
        "guidValue": {
            "value": "2c670000-a1e6-0000-0000-679cac0f2c27"
        },
        "vmSize": {
            "value": "Standard_A2_v2"
        },
        "vmNamePrefix": {
            "value": "testdemo"
        },
        "vnetNewOrExisting": {
            "value": "existing"
        },
        "virtualNetworkName": {
            "value": "az-netVnet"
```

13. Finalize the deployment and wait for it to complete.

14. Once the restored Airwall Gateway is deployed and communicating with Conductor, open that Airwall Gateway in the Conductor, and on the **Ports** tab, update the **Underlay NAT IP** to match the new static IP object from the deployment.



Ports

Interfaces	Assigned	IP address	MAC	MTU	VLAN +
☰ Port 1	✓	10.3.0.4/24	00:0d:3a:e8:c1:d9	1500	--

Port groups +

Underlay group (Underlay Port Group 1) Port 1

Name: Underlay Port Group 1

Interfaces: Port 1

Priority: 0

Failover group: Stand-alone

IP addresses: DHCP

Type: IPv4

IP address (CIDR)

Gateway

DNS servers

Underlay IP (NAT):

☑ Publish IPs to Airwall Conductor

☐ Enable bypass

Static routes +
None

Overlay group (Overlay Port Group 1) Serial over IP Port 2

Conductor and Airwall Edge Service PCI Compliance

The Airwall Conductor and Airwall Edge Services are compliant with PCIDSS guidelines and Payment Card Industry (PCI) data security standards. The Airwall Solution provides secure transport of logs, firewall rules creation and reporting, retention of activity logs, and audit reporting of system configuration changes.

PCI Reporting is enabled by default. You can use it for both PCI compliance and for troubleshooting, as it records when a change was made, who made it, and what the change was.

Note: When PCI Reporting is enabled, PCI logs are kept for 90 days.

To access PCI data in the Conductor

PCI data settings are in the Conductor under **Settings** > **Advanced** > **Global Airwall settings**:

- **To enable or disable PCI reporting** – Select **Edit Settings**, and change the setting for **PCI Reporting support**.

- **To see PCI reports** – In the Global Airwall settings section, next to **PCI Reporting**, select **Downloads** to access the **PCI Report & References** download page.

PCI Compliance Reports

PCI Compliance Reports allow you to see when a change was made, who made it, and what the change was.

Note: When PCI Reporting is enabled, PCI logs are kept for 90 days.

For instructions on how to access these reports, see Conductor and Airwall Edge Service PCI Compliance on page 137.

You can download these reports from the **PCI Reports and References** page. You can cross-reference the reference ID in the User activity report with the IDs in each of the reference reports to get more details:

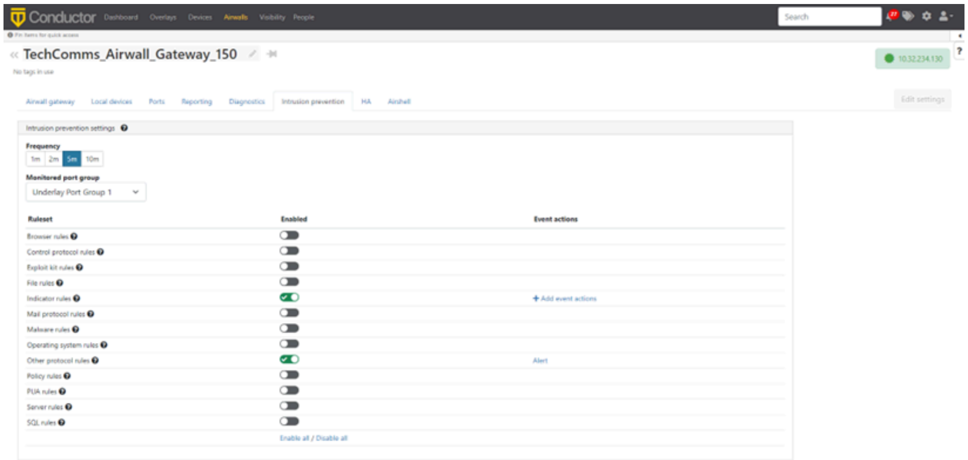
- **User activity report** – Contains when, what was changed, how it was changed (that is, modified, deleted, created, etc), and who changed it. Use the reference ID to look up more details in the reference reports. Includes log ins to the Conductor and authentication through an Airwall Agent or Server.
- **Policy reference** – Shows what policies are set, including the overlay the policy is in and the permissions between devices. Gives you a reference for what things on your network can connect with each other.
- **Device reference** – Details for changes on **Devices**.
- **Device group reference** – Details for changes on **Device groups**.
- **Airwall reference** – Details for changes on Airwall Edge Services.
- **Airwall group reference** – Details for changes on **Airwall groups**.
- **Overlay network reference** – Details for changes on Overlays.
- **Relay rule reference** – Details for changes on relay rules.
- **Tag reference** – Details for changes on tags.
- **User reference** – Details for changes on users.
- **People groups reference** – Details for changes on people groups.

Set Up Intrusion Prevention

Use intrusion prevention to monitor your network for malicious activity and take action to prevent it. Complete the following steps to enable intrusion prevention on an Airwall Gateway.

Note: Enabling intrusion prevention may reduce performance.

1. In the Conductor, go to **Airwalls** and select an Airwall Gateway.
2. Click **Intrusion prevention**.



Intrusion prevention settings

Frequency
1m | 2m | 5m | 10m

Monitored port group
Underlay Port Group 1

Ruleset	Enabled	Event actions
Browser rules	○	
Control protocol rules	○	
Exploit kit rules	○	
File rules	○	
Indicator rules	✓	+ Add event actions
Mail protocol rules	○	
Malware rules	○	
Operating system rules	○	
Other protocol rules	✓	Alert
Policy rules	○	
PUA rules	○	
Server rules	○	
SQL rules	○	
	Enable all / Disable all	

3. Select **Frequency** between 1 minute and 10 minutes. Frequency is the rate at which batches of intrusion events are sent to the Conductor.

   Note: If multiple intrusions of the same type occur in the time frame, they are sent as a single event.

4. Choose a **Monitored port group**.
5. Enable or disable the required **Ruleset(s)**:

   - **Browser rules**: This category contains detection for vulnerabilities present in products that have the "Gecko" engine (Firefox browser), Trident or Tasman engines (Internet Explorer browser), and the Webkit browser engine (Apple's Safari, Nokia, KDE, Webkit itself, etc.), along with rules for other engines and browser plugins.
   - **Control protocol rules**: This category is for rules that may indicate the presence of or vulnerabilities in SCADA, SNMP, and RPC protocol traffic.
   - **Exploit kit rules**: This category is specifically tailored to detect exploit kit activity (related "post-compromise" rules and rules relating to files that are dropped as result of visiting an exploit kit found in the indicator rules and files rules categories).
   - **File rules**: This category contains rules for vulnerabilities that are found inside of image files, Java files (.jar), multimedia files (mp3, movies, wmv), files related to the Microsoft Office suite (Excel, PowerPoint, Word, Visio, Access, Outlook, etc.).
   - **Indicator rules**: This category contains rules that look for traffic to be used for the detection of a positively compromised system or obfuscated content, and for markers of shellcode or indications of scanning in traffic.
   - **Mail protocol rules**: This category is for rules that may indicated the presence of or vulnerabilities in IMAP, NNTP, and POP traffic.
   - **Malware rules**: This category contains rules for the detection of traffic destined to known listening backdoor command channels, known malicious command and control activity for identified botnet traffic, tools that can be considered malicious in nature, and other potential malware traffic.
   - **Operating system rules**: This category contains rules that look for vulnerabilities in Linux, Solaris, Windows, Mobile, and other related rules.
   - **Other protocol rules**: This category is for rules that may indicated the presence of or vulnerabilities in ICMP, Telnet, TFTP, VOIP, and other protocol traffic not covered in the mail and control protocol categories.
   - **Policy rules**: This category contains rules that detect potential violations of policy for multimedia and social media, and rules that may indicate the presence of spam along with other rules that may violate the end-users corporate policy.
   - **PUA rules**: This category deals with Potentially Unwanted Applications (PUA) that deal with adware, spyware, p2p, toolbars installed on the client system, along with other PUAs.
   - **Server rules**: This category deals with vulnerabilities in or attacks against Apache Web Server, Microsoft IIS Web Server, Microsoft SQL Server, Oracle's MySQL Server, Oracle's DB Server, Samba's Servers, mail servers (Exchange, Courier), and other related rules.
   - **SQL rules**: This category contains rules that detect SQL injection or the presence of other vulnerabilities against SQL like servers.
6. When you enable a ruleset, select an **Action type**:

   - Alert
   - Enable / Disable
   - HTTP call
   - Reboot
   - Tag add / remove
   - Tag enable / disable

   Note: For more on Action type, see Event Actions on page 123

7. Fill in the required information and click **Create**.
8. Add another action or click **Finish**.

Deploy Airwall™

Successfully deploy and configure the Airwall solution and revolutionize security on your network. This deployment information assumes you are familiar with basic networking concepts and have a good working knowledge of your organization's hardware, software, and virtual products and services.

Get Started with the Airwall Solution

Tempered is on a mission to revolutionize security for a connected world. The Airwall Solution increases security, reduces complexity, and dynamically handles changes on your network, simplifying how you manage your network.

You can instantly provision and revoke networking and security services with minimal, if any, modification to your underlying network, applications, or infrastructure. Airwall helpThis guide contains information and instructions to help you deploy, manage, and troubleshoot your Airwall Solution.

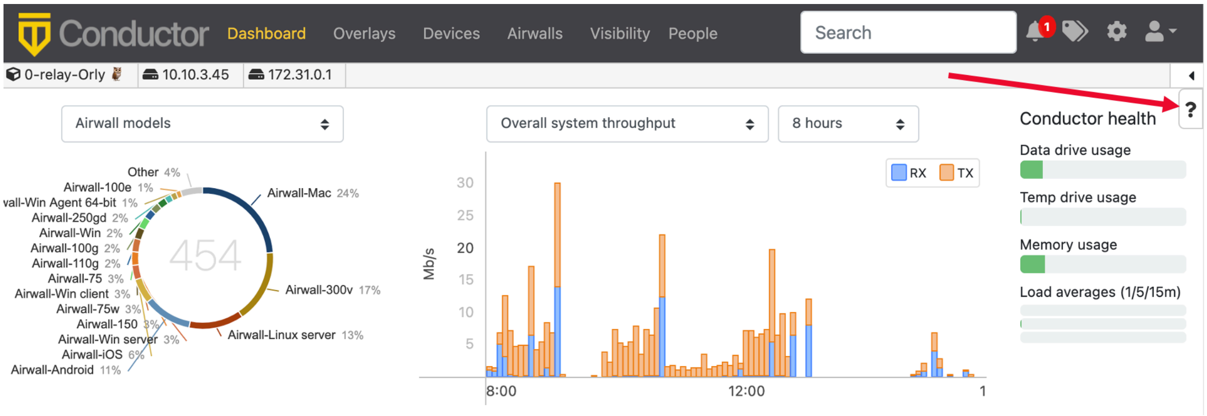
For a quick introduction to the Airwall Solution, check out Tempered's overview and demo Video Overview and Demos on page 6.

Get Started using Conductor Help and Tutorials

The Conductor contains several tutorials to help you set up and configure a new Conductor, as well as use and understand different features in the Conductor.

Open Airwall Help

Airwall Help is always available from the Conductor by going to the question mark in the upper right under the menu pane.



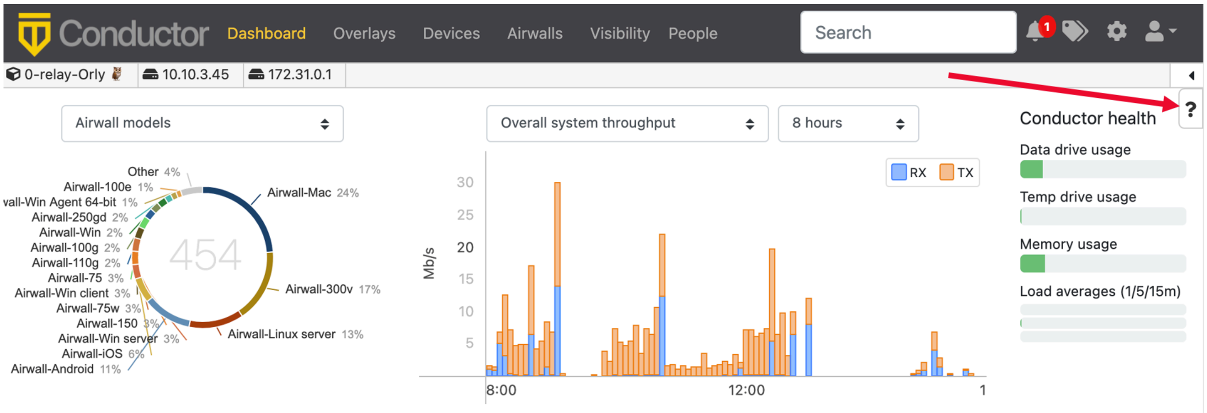
Use the Dashboard Setup Progress Bar

If you are a system administrator, when you first sign in to a newly-created Conductor, by default the Dashboard shows a Setup progress bar to walk you through configuring your Conductor. Select a step to get information and assistance completing that step, as well as see your progress or go back and change the configuration.

You can hide the Setup progress bar by clicking the hide icon . You can show it again from your user preferences. For help, see Show or Hide Conductor Setup progress on page 40.

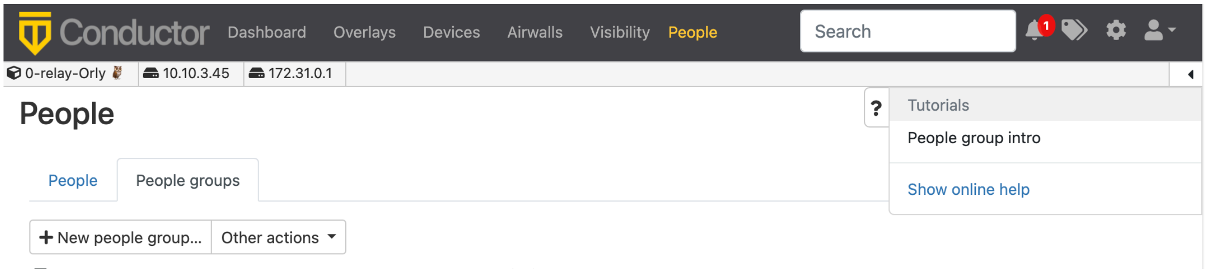
Start a Tutorial

When there is a tutorial available for the page you are on, you can access it under the Conductor help icon, or from the question mark on a page.

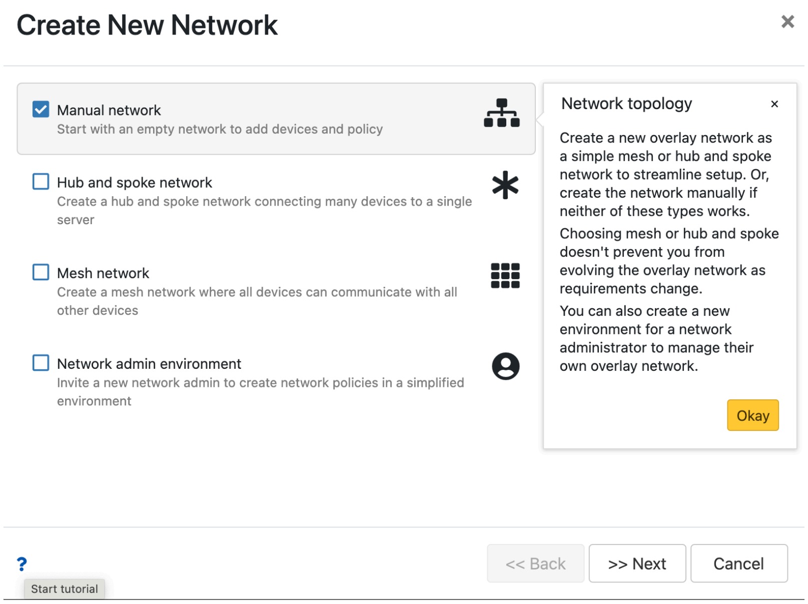


Examples

- **People groups tutorial** – To access the tutorial on people groups, go to the **People** page, select the **People groups** tab, and then click the question mark in the upper right to see the tutorials for the **People groups** tab:



- **Create a new network tutorial** – When creating a new overlay network, you can access the tutorial information by selecting the question mark icon in the lower left:



Create New Network

☑ Manual network
Start with an empty network to add devices and policy

☐ Hub and spoke network
Create a hub and spoke network connecting many devices to a single server

☐ Mesh network
Create a mesh network where all devices can communicate with all other devices

☐ Network admin environment
Invite a new network admin to create network policies in a simplified environment

Network topology

Create a new overlay network as a simple mesh or hub and spoke network to streamline setup. Or, create the network manually if neither of these types works.

Choosing mesh or hub and spoke doesn't prevent you from evolving the overlay network as requirements change.

You can also create a new environment for a network administrator to manage their own overlay network.

Stop a Tutorial

To stop a tutorial, just select the X in the upper right corner or select **Done**.

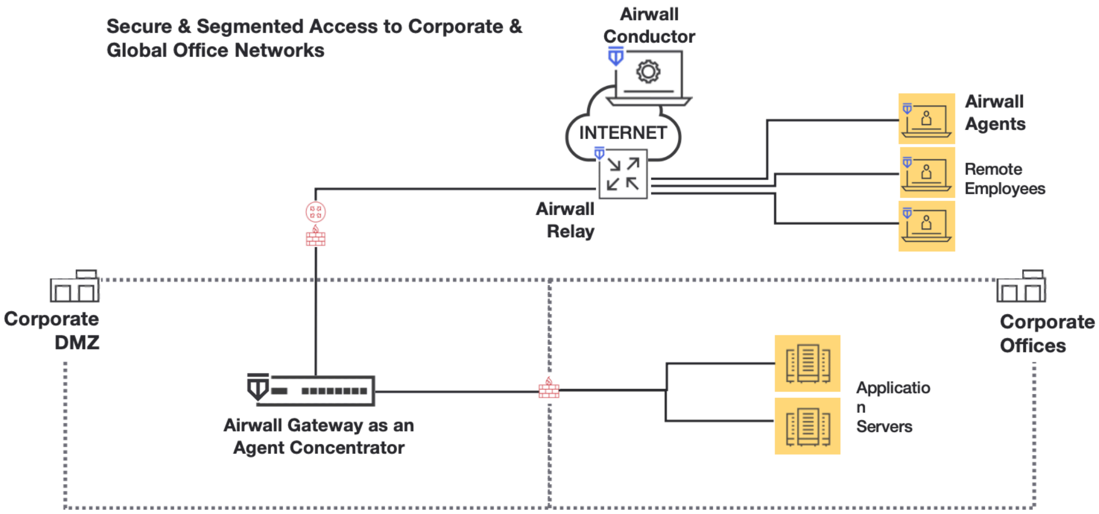
What makes up an Airwall secure network?

Get an overview of what goes into creating an Airwall secure network, a virtual air-gap solution that ensures your devices are completely invisible. You can secure and micro-segment network communication and remote access between devices at scale. The architecture also makes it possible to deploy and install an Airwall secure network over your existing network.

In an Airwall secure network, devices are assigned a cryptographic identity using Host Identity Protocol (HIP) as the sole criteria for network communications. By default, devices only communicate through the encrypted identity framework, which means devices don't even show up on a pen-test scan.

Rather than finding a metaphorical 'locked door,' there is no door to even knock on. From the perspective of a pen tester or bad actor, the network is essentially invisible.

Here is a simplified view of an Airwall secure network:



Airwall Agents, Servers, Gateways, and Relays, collectively Airwall Edge Services, are a collection of services that allow you to connect and protect all of your things. The Airwall Conductor provides an intuitive interface for you to manage your Airwall solution.

- Airwall Agent software protects and connects your employees mobile devices and laptops.
- Airwall Server software protects and connects your Windows and Linux servers.
- Airwall Gateways protect your devices - cameras, manufacturing, utility or hospital devices, and are available as hardware, cloud, and virtual appliances.
- Airwall Relays connect all of your things together, regardless of the way they are connecting. They route encrypted communications between all your 'things', without modifying the underlying network. Airwall Relays can be hardware, cloud, or virtual as well.
- The Airwall Conductor is an interface that allows you to set up and manage all of the above Airwall products and how they interact to create your Airwall secure network.
- Airwall Overlays create the connections and trust policies between these Airwall Edge Services. When you build an Overlay, you are connecting and establishing trust between two or more Airwall Edge Services.

More information on each of these is below.

Airwall Agents

Airwall Agents are software applications installed on devices (Windows, macOS, iOS, iPadOS, and Android) that enable zero-trust network access (ZTNA) from anywhere in the world. By default, all communications are encrypted end-to-end and multi-factor authenticated (MFA), enforcing a software-defined perimeter (SDP) at the distributed edge.

Easily integrate user authentication with device-based authentication, overcoming much of the complexity associated with extending directory services to include device-based trust. Explicitly allow or deny any device to securely connect to a network, and also easily segment access by defining resources that a device or group of devices can access. Devices do not have the session constraints and are not restricted by the number of concurrent client-to-resource encrypted sessions.

Airwall Servers

Airwall Servers support Windows Server and Linux, and behave much like Airwall Agents. They effectively make servers invisible and only allow communication with authenticated and authorized endpoints (ZTNA). Air-gap servers from unauthorized communication with a software-defined perimeter (SDP).

Airwall Gateways

Airwall Gateways protect ‘things’ downstream. They are deployed in front of devices or hosts that cannot protect themselves. Examples include legacy systems and machines, or when customers are unable to install an Airwall Agent or Server.

Physical Airwall Gateways, depending on the model, have built-in Ethernet, Wi-Fi, and Cellular (2G, 3G, 4G LTE modems), as well as Serial-over IP for the flexible link connectivity options. You can also deploy virtual and cloud Airwall Gateways.

Virtual Airwall Gateways use the 300v image and license. See Virtual Airwall Edge Services on page 147.

Airwall Relays

An Airwall Relay routes encrypted communications between all your ‘things’ across all of your networks. You can use them to reduce network complexity and enable complete connectivity between every endpoint. An Airwall Relay provides a private identity namespace that eliminates the need for public IP addresses and inbound firewall rules to connect devices.

Instead of Layer 3 rules, network addresses, or traditional routing protocols to securely connect and route privately addressed systems across networks, Airwall Relay relies on verifiable cryptographic identities to determine if a connection is allowed, and forwards only authenticated and encrypted traffic to authorized endpoints. You can deploy an Airwall Relay as a physical, virtual, or cloud device.

Airwall Conductor

The Conductor provides one centralized location for you to set up and manage Airwall products and create your Airwall secure network:

- Set up, provision, license, and manage all Airwall Edge Services.
- Manage the devices protected by Airwall Edge Services.
- Connect and set up trust relationship policies between the Airwall Edge Services with Overlays. You define the overlay network segments and systems that protected machines are allowed to access, as well as how they connect on the LAN, WAN, and public Internet.
- Monitor and troubleshoot your Airwall secure network.

The Conductor enforces visibility and access policy based on unchanging cryptographic machine identities, not network addresses that change and can be spoofed. It is not involved in the data that is exchanged between Airwall Edge Services and the devices they protect.

Airwall Overlays

When you build an Overlay, you are connecting and establishing trust between two or more Airwall Edge Services. Every endpoint in an Overlay knows the IP-layer state of its peers, and every peer maintains identity-based routing tables. This policy-based approach helps any edge service establish the most direct route to a resource within an Overlay.

The secured communications channels you create with an Overlay are encrypted HIP tunnels that allow trusted devices to communicate securely with each other across the network. These communication channels are controlled by the Airwall Edge Services deployed throughout the underlay and administered by the Conductor.

Underlay

This is your existing network. Airwall Edge Services (Gateways, Agents, and Servers) and the Conductor connect to the underlay over which you establish the Airwall secure network.

Airwall Gateway Hardware

Airwall Gateways provide cloaking, secure connectivity, identity-based routing, IP mobility, and micro, macro, as well as cross- boundary segmentation enforcement all within the military-grade encrypted fabric.

They enforce the Airwall Conductor provisioning, de-provisioning, and revocation of trust of any managed IP resource they protect. Airwall Gateways are currently available as hardware, virtual images for VMware ESXi and Microsoft Hyper-V, or cloud-based for Amazon Web Services, Microsoft Azure, and Google Cloud.

Airwall Gateway 75 Series

The Airwall Gateway 75 is designed for medical devices, point of sale systems, and others like building automation controls. It securely connects and protects those endpoints across all networks with little to no change to existing infrastructure. The 75's unique overlay technology rides on top of any network, even ones you do not control, eliminating the complexity, time, and cost associated with traditional networking and security methods. All protected endpoints are cloaked and segmented by the Airwall Gateway and all data encrypted so endpoints cannot be discovered or accessed by unauthorized devices, eliminating the network attack surface. The 75's plug and play design makes universal connectivity and segmentation simple, fast, and cost-effective.

Airwall Gateway 100 Series

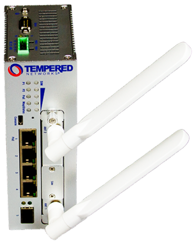
The Airwall Gateway 100 is a purpose-built industrial IoT edge gateway that makes connecting, collecting, and protecting IoT endpoints and data extremely secure and remarkably simple to deploy and manage. The 100 requires little to no change to existing infrastructure so you can rapidly join all SCADA, BACnet, and ICS endpoints to a private and segmented overlay network in minutes. The 100 eliminates the complexity associated with traditional network and security methods. All connected and protected devices are cloaked and can’t be discovered or reached by unauthorized devices, eliminating the network attack surface. The 100's plug and play design, ruggedized hardware, and optional cellular modem makes universal connectivity and segmentation across all networks simple, fast, and extremely cost-effective.

Airwall Gateway 110 Series

Introducing a complete refresh for the 100-series platform, with 4x the power, more ports, and future-proof for your industrial / OT networks. Unlike the AW-100, the 110 will run all monitors, handle up to 6 HD streams, has more storage and memory (thus less bugs and scalability problems in the field).

The Airwall Gateway 110 is a purpose-built industrial IoT edge gateway that makes connecting, collecting, and protecting IoT endpoints and data extremely secure and remarkably simple to deploy and manage. The 110 requires little to no change to existing infrastructure so you can rapidly join all SCADA, BACnet, and ICS endpoints to a private and segmented overlay network in minutes. The 110 eliminates the complexity associated with traditional network and security methods. All connected and protected devices are cloaked and cannot be discovered or reached by unauthorized devices, eliminating the network attack surface. The 110's plug and play design, ruggedized hardware, and optional cellular modem makes universal connectivity and segmentation across all networks simple, fast, and extremely cost-effective.

Airwall Gateway 150 Series



The Airwall Gateway 150 is a cost-effective and ruggedized Industrial IoT edge gateway that delivers peer-to-peer encrypted and segmented connectivity for machines anywhere in the world. It comes with PoE input, Serial-over-IP, and optional cellular module with seamless failover between wired and cellular networks for high availability. The 150 is often deployed as a bump-in-the-wire for machines that cannot protect themselves, while being easily managed with point-and-click policy configuration through the Conductor.

Airwall Gateway 250 Series

The Airwall Gateway 250 is a ruggedized industrial IoT edge gateway that makes connecting, collecting, and protecting ICS and SCADA systems and data extremely secure and remarkably simple to deploy and manage. The Ethernet and SFP port dense design with PoE, dual cell modems, and link management eliminates the cost, complexity, and availability limitations of deploying separate switches, VPNs, Firewalls, Cellular Routers, and APNs.

Deployment requires little to no change to existing infrastructure, so you can rapidly join all ICS and SCADA systems to a private and segmented overlay network in minutes. The 250's unique overlay technology rides on top of any network, even ones you don't control, eliminating the complexity associated with traditional networking and security methods. All protected endpoints are cloaked and segmented by the 250 with all data encrypted so endpoints can't be discovered or data accessed by unauthorized devices, eliminating the network attack surface. The 250's plug and play design makes universal connectivity and segmentation across all networks simple, fast, and extremely cost-effective.

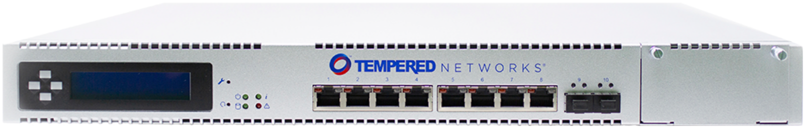
Airwall Gateway 400 Series

The Airwall Gateway 400 is a 1U rack mounted unified secure networking appliance. Designed to support mission-critical applications and servers throughout your organization, the 400 enables instant connectivity, cloaking, segmentation, mobility, and failover, as well as the ability to disconnect any physical or virtual resource behind it instantly. All communication from the 400 series is automatically AES 256 encrypted to any other Airwall Edge Service within the fabric and is not limited by the number of concurrent virtual trust segments that can be established.

It's the ideal choice for data center and enterprise network devices, machines or hosts that contain sensitive information, like financial servers, HR applications, 3rd party web services, or any systems with personally identifiable information (PII).

The 400 provides 8 Gigabit Ethernet ports and is configurable to meet SFP and 10G SFP+ requirements with the option to configure high availability (HA) for seamless failover between 400 Series appliances.

Airwall Gateway 500 Series



The Airwall Gateway 500 serves as a datacenter, campus, or plant services gateway that functions as either a hub or aggregation point and makes connecting, collecting, and protecting thousands of endpoints and data extremely secure and remarkably simple to deploy and manage.

The 500's high performance, port density, dual power, and optional FIPS and port expansion modules eliminate the cost, complexity, and ineffectiveness of managing VPNs, firewalls, VLANs, ACLs, and NAC for secure connectivity and segmentation across any network. The 500 serves as the network boundary and security perimeter for its protected endpoints. Its unique overlay technology rides on top of any network, even ones you do not control, eliminating the complexity associated with traditional network and security methods. All connected devices behind the 500 are cloaked and can't be discovered or reached by unauthorized devices, eliminating the network attack surface. The plug and play design makes universal connectivity and segmentation across all networks simple, fast, and extremely cost-effective.

Virtual Airwall Edge Services

The Airwall virtual Airwall Gateway is offered on multiple virtual platforms, including VMware ESXi and Microsoft Hyper-V, if you prefer a virtual form factor as a cost-effective data center implementation or a solution where a hardware-based Airwall Gateway may be impractical.

Airwall supports the following virtual platforms:

- Windows Server Hyper-V 2012 or later
- VMware ESXi version 5.0 or later

Virtual Airwall Gateways use the 300v image and license.

Cloud-Based Airwall Edge Services

Cloud Airwall Gateways are offered on multiple cloud platforms if you prefer a virtual cloud form factor as a cost-effective data center implementation or a solution where a hardware-based Airwall Gateway may be impractical.

Airwall supports the following virtual platforms:

- Alibaba Cloud – See Alibaba Cloud – Set up an Airwall Gateway on page 315.
- Amazon Web Services – See Amazon Web Services – Set up an Airwall Gateway on page 320.
- Microsoft Azure-- See Microsoft Azure – Set up an Airwall Gateway on page 324.
- Google Cloud – See Google Cloud (GCP) – Set up an Airwall Gateway on page 334.

Airwall Agents and Airwall Servers

Airwall Agents and Airwall Servers are designed to provide desktops, laptops, and servers with encrypted access from anywhere in the world, over any network. An Airwall Agent or Airwall Server protects the device on which it is installed.

Airwall Agents (Windows, macOS, iOS, and Android)

A Airwall Agent enables granular remote access to the network resources for employees, contractors, and vendors, without complex management of certificates, ACLs or IPSec tunnels.

Airwall Servers (Windows and Linux)

Serving as the network boundary and security perimeter for its protected workload, the Airwall Server can be deployed with little no changes to existing infrastructure and eliminates the complexity associated with traditionally separate network and security controls.

A workload protected by an Airwall Server can be cloaked and made undiscoverable by unauthorized systems. Server access is then restricted to only other authenticated and authorized Airwall Edge Services connecting from any network, significantly reducing the network attack surface.

Airwall Agents and Airwall Servers are a better alternative to virtual private networks

A virtual private network (VPN), while providing a host-to-network tunnel, lacks segmentation once authenticated and inside the network. In contrast, an Airwall Agent or Airwall Server allows secure access to mutually-authenticated and authorized machines only, making it easy to create private workgroups that are invisible and inaccessible to others, even from clients that may have valid user or application credentials. This allows devices to be logically segmented, connected, and protected in a manner that VPNs and firewalls cannot achieve.

Benefits

Universal Mobility: Instant Access and Revocation from Anywhere	Granting and revoking Airwall Agent access to individual resources on the network is simple and instant. The security context and ability to connect clients to

	specific resources never changes, regardless of where a user may be coming from – the LAN, WAN or Internet. The result is access from anywhere in the world, without the complexity and inflexibility of VPNs.
Airwall Invitations: Automate Rapid Deployment and Access	Automate user device access using **Airwall Invitations** to create secure and segmented access to individual resources, not entire networks. Provide email addresses, and as users download and add their machines, they'll have access to only the specific systems they're allowed and cannot see or access others, even if those systems reside on the same network. This significantly simplifies the time-consuming and complex process of getting people access to resources on the network.
Seamless and Transparent Multi-Factor Authentication (MFA)	Once the Airwall Agent is installed on a device, it now has an immutable and unique machine identity. Unlike port forwarding that enables arbitrary connections with no requirement for authentication, Airwall Agents are authenticated and authorized based on their trusted machine identity before a peer-to-peer encrypted connection is established and credentials used. User authentication can now be easily integrated with device-based authentication, overcoming much of the complexity associated with attempts to extend directory services to include device-based trust.
Private Workgroup Networks: Protect Intellectual Property and Sensitive Data	Our customers easily and quickly create overlay networks to isolate and control access to critical systems. For example, this includes controlling administrator access to network and security infrastructure to eliminate the threat of a hacker gaining access to those systems through a system's local management interface. Another example is creating private workgroups for DevOps, Executive, HR, and PCI teams to protect intellectual property and sensitive data from being breached by unauthorized machines with access to the same network.

What's New by Version

Find out what new features have been introduced in each version.

What's New in 3.3.0

This version of the Airwall Solution includes several usability and functionality improvements that can simplify and streamline the setup and diagnostics for an Airwall secure network.

Device group shows overlay networks

In the Conductor, the device groups page now shows overlay membership.

New and Improved Conductor Features

Learn more –

-
-

New and Updated Help

In addition to the content added for new features linked above, here's the new and updated content published since our last major release:

New –

- Set Up Intrusion Prevention on page 138
- Enable HIP on Conductor on page 274

Updated –

- Set up Microsoft Azure as a cloud provider on page 434
- Set up Google Cloud as a cloud provider on page 438
- Set up Amazon Web Services (AWS) as a cloud provider on page 433
- Manually deploy a Conductor on the Google Cloud Platform (GCP) on page 219
- Google Cloud (GCP) – Set up an Airwall Gateway on page 334
- Create an Event Monitor on page 119
- Local Bypass on page 394
- Backhaul Bypass on page 395
- Run the Conductor as an Airwall Relay on page 354
- Configure Airwall Relay rules on page 353

What's New in 3.2.4

This version of the Airwall Solution includes several usability and functionality improvements that can simplify and streamline the setup and diagnostics for an Airwall secure network.

Region Bypass

Use bypass regions to group and load-balance bypass gateways by region. A bypass region is configured by creating a region tag. Add the region tag (or tags) to one or more bypass egress gateways and to the Airwalls you want to use with the region bypass egress gateways. See Region bypass on page 397 and Create a Tag on page 100.

Airwall Agent Conductor toggle

You can now toggle between Conductors in the Airwall Agent (macOS) without opening Configure box, see Connect with an Apple (OSX and macOS) Airwall Agent on page 19.

Airwall AV3200g Installation Guide

There is now a specific installation guide for Airwall AV3200g, see Airwall Gateway AV3200g Hardware Installation Guide on page 281.

Airwall AV3033 Installation Guide

There is now a specific installation guide for Airwall AV3033, see Airwall Gateway AV3033 Hardware Installation Guide on page 284

New and Improved Conductor Features

Learn more –

-
-

New and Updated Help

In addition to the content added for new features linked above, here’s the new and updated content published since our last major release:

New –

- Region bypass on page 397
- Airwall Gateway AV3200g Hardware Installation Guide on page 281
- Airwall Gateway AV3033 Hardware Installation Guide on page 284

Updated –

- Airwall Gateway Hardware Installation Guide on page 276
- Airshell (airsh) Command Reference on page 362
- Create a Tag on page 100
- Add Interfaces to a Port on page 389

What's New in 3.1.0

This version of the Airwall Solution includes several usability and functionality improvements that can simplify and streamline the setup and diagnostics for an Airwall secure network.

Tutorial and Help Improvements

- **What's new Tutorial** – You can now see what’s new by running the **Dashboard** tutorial from the Conductor Dashboard.
- **Help links for a page** – In addition to tutorials, you can now access more specific Airwall help content for a page from the ? menu on most pages.
- **Video overviews and demos** – For video overviews and demos of the Airwall Solution, see Video Overview and Demos on page 6.

New tools to troubleshoot connectivity issues

The Conductor **Connectivity checker** does a full analysis of the connectivity between two devices in your Airwall secure network.

Learn more – Connectivity checker on page 486

Run Conductor as a Relay

For small- to moderate-sized Airwall secure networks, you can run your Conductor as a relay, rather than having a separate Airwall Relay. Since Airwall Edge Services must all be able to reach the Conductor, using it as an Airwall Relay simplifies your deployment. You must have both a Conductor and an Airwall Relay license to run your Conductor as a relay.

Learn more – Run the Conductor as an Airwall Relay on page 354

Control Access with People Groups

Using people groups, you can control what the people in the group can see and use on the Conductor, including cloud providers, Airwall Gateways, and Overlay networks and resources. You can also now see to which overlay networks the people group has permissions.

Learn more – Customize People's Access to your Airwall secure network with People Groups on page 86

Airwall Gateway High Availability (HA) Heartbeat options

You now have a choice on how the Airwall Gateway HA heartbeat functions. When setting up an Airwall Gateway HA pair, you can choose how to do the heartbeat between the two HA units. There are two options: LAN mode or routed mode.

Learn more – Configure High Availability Airwall Gateways (v2.2.8 and later) on page 399

Remote Airshell

For remote administration of Airwall Gateways, you can use Airshell to run diagnostic and configuration commands from the Conductor.

Learn more – Run Airshell remotely from the Conductor on page 374

Airshell Additions and Improvements

The following commands and functionality have been added to Airshell:

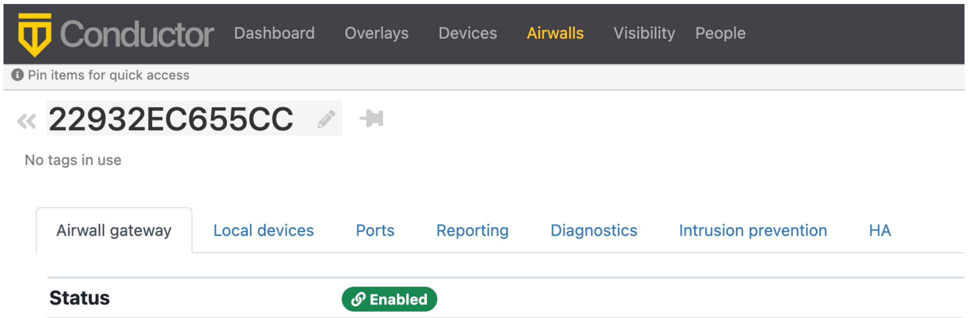
- `nmap` – (Network mapping support) Maps your network for discovery or security audits. **Learn more:** Do network discovery and security audits in Airshell (nmap) on page 377
- `table` – See the table command at Airshell (airsh) Command Reference on page 362.
- `conductor ping` – New `conductor ping` Airshell command for Airwall Gateways, Linux Airwall Servers, and macOS Airwall Agents checks name resolution and performs TLS connection attempt with every configured Conductor URI.
- `status dnscache` and `status dnscache flush` – For Airwall Gateways, dumps or flushes the DNS cache.
- `status threads` – Reports CPU and memory usage of threads of major services running on an Airwall secure network.
- `status` – Results now show information (revision hash and date) for the installed cellular firmware package.

Learn more – Airshell (airsh) Command Reference on page 362

Conductor and Airwall Edge Services Improvements

Navigation and Search

- **Back Navigation** – On most pages, you now have a link back to the original page. For example, from an Airwall Edge Service page, you can select the back icon « to get back to the list of Airwall Edge Services.



22932EC655CC

No tags in use

Status Enabled

- **Search by Expression** – The Conductor now supports an alternative to full text search, searching by expressions using the Conductor Query Language. Searching by expression is available in the search boxes on the **Overlays**, **Airwalls**, **Devices**, **People**, and **Dashboard** pages. **Learn more:** Search by Expression with the Conductor Query Language on page 45
- **Device quick filter** – The quick filter for devices is now also available on the **Dashboard Devices** list.

Overlay network graph

- **Multi-select** – Select more than one item on the network graph by holding down the meta key for your platform (`Ctrl` on Windows, or `cmd` on macOS) and clicking on multiple items. You can then use the context menu to create a device group or remove the items from the network.
- **Overlay Edit options** – The network graph also now has **Edit layout** and **Edit trust** options.
- **Create device group** – You can now create a device group by using multi-select to select devices, then right-click to create a device group.

- **Airwall model information** – When you hover over an Airwall Edge Service in the Airwall Edge Service network graph, the graph now shows the Airwall Edge Service model.

Learn more: Add and remove device trust on page 427

Set a preference for your overlay networks view

Go to **[your account]** > **Preferences** and scroll down to the bottom. Toggle the **Default overlay networks to advanced view** to show or hide the advanced view by default.

Learn more: Change My Conductor Preferences on page 30

Diagnostics and Monitoring Improvements

- **Email failure alerts** – When emails fail to send, the Conductor now shows alerts and records system events.
- **Summary for check secure tunnels** – There is now a summary for the **Check secure tunnels** Airwall Edge Service diagnostic tool indicating the number of remote Airwall Edge Services and the number of active tunnels.
- **Firmware Revision information** – In the Conductor, on an Airwall Edge Service page, revision information is shown on the main page below the Airwall Edge Service's firmware revision.
- **Ping peer Airwalls** – This diagnostic tool now indicates if traffic was conducted over a relay and which relay it used.
- **Airwall Relay diagnostics** – **Diagnostics** > **Airwall relay diagnostics** on an Airwall Relay now shows the IP addresses of the communicating Airwall Edge Services, as seen from the viewpoint of the relay.
- **HIP tunnel stats** – HIP tunnel stats now default to **On**, and are sent every 5 minutes for newly-connected Airwall Edge Services that support the feature. Go to **Airwall** > **Reporting** > **HIP tunnel stats** to see how much traffic you have over each tunnel.
- **HIP tunnel event monitors** – You can now configure a delay for actions on HIP tunnel event monitors, allowing you to reduce noise for transient events (for example, an Airwall Edge Service that goes offline briefly). There is also improved tracking and messaging around why a tunnel has closed. You can filter on the reasons a tunnel closed so that event actions are not performed for certain reasons. For example, you may not want to alert when a tunnel goes down due to an idle timeout (no traffic passed).
- **More fields for Templated values in Event monitor actions** - You can now use any data that is part of the monitored object by adding it as a templated value. For example, in the HTTP call action, you could use the Airwall Edge Service's name with "${monitored_object.name}", or get a device's overlay IP with "${monitored_object.overlay_device_ip}".
- **PCI user activities** – Now indicate if an action was performed via API.

Airwall Agents and Servers Improvements

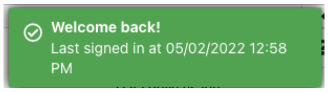
- **Linux** – The Linux Airwall Server now supports traceroute from the Conductor diagnostic page when installed and available. Looks for the presence of traceroute or tracepath. It also now remembers its state when you update the firmware, and return to that state after the update (either active or inactive).
- **Android** – The Android Airwall Agent now restarts when you update the app, or if you restart the device while the app service is running. You can also now ping devices on the **Network** page.

Deployment Improvements

- **Cloud accounts** – The Airwall Gateway detects the cloud `accountid` used during deployment and sends that provider-specific value to the Conductor.
- **Google Cloud** – There is now a standalone Airwall Gateway deployment for Google Cloud.
- **Device discovery** – The Conductor now shows the time a device was discovered.
- **Easier OpenID Connect integration troubleshooting** – It is now easier to troubleshoot integrating your Conductor with an OpenID Connect provider using Conductor Airshell and log following. **Learn more**: Integrate Third-party Authentication with OpenID Connect on page 247

Security and Privacy Updates

- **New overlay network role for Network Administrators** – The roles available for overlay permissions now are viewer, user, or manager. For more information, see Edit people who can access an overlay network on page 419.
- **New `conductor ping` airsh command** for Airwall Gateways, and macOS and Linux Airwall Agents and Servers – Checks name resolution and performs TLS connection attempt with every configured Conductor URI. **Learn more:** Diagnostic commands on page 366
- **Tag Ownership** – With v3.1.0, the tag ownership rules have changed to be more restrictive by default. If a system administrator creates a tag, by default, only system administrators can see or use them. If a network administrator creates a tag, ownership defaults to only them or their people group, and system administrators. This change allows you to have department or customer-specific tags that only members of specific people groups can see and use. **Learn more:** Manage Tag Ownership on page 104
- **Airwall Diagnostic permissions** – Diagnostics now require a network admin to have edit permissions on the Airwall Edge Service.
- **Lock Airwall Edge Services** – You can lock an Airwall Edge Service so only system administrators can edit it. **Learn more:** Lock an Airwall Edge Service on page 94
- **Login notifications** – The Conductor notifies admins the first time a user logs in, and the Conductor also shows a user's last log in when they log in, including through OpenID Connect Third-party integrations.



Welcome back!
Last signed in at 05/02/2022 12:58 PM

Onboarding Improvements

- **Delete Airwall Invitations** – You can now delete **Airwall Invitations**, both in the Conductor, and from the API.
- **Replace an Airwall Agent or Server** – You can now send an **Airwall Invitation** from a specific Airwall Agent or Server, and when the user activates the invitation, the Conductor automatically revokes and replaces the Airwall Agent or Server from which you sent the **Airwall Invitation**.
- **Device detection improvements** – The device detection workflow (and the related dialog) have been updated to streamline the onboarding process. The dialog now allows the user to detect devices and then, as they are detected, update their names and IP, apply an overlay IP NAT from a NAT pool and add them directly to an overlay.
- **Set an Airwall Gateway name using Airshell before provisioning** – You can now check the **Allow Airshell to set name** option when sending **Airwall Invitations**. When checked, you can use Airshell to set an Airwall Gateway's name before using the activation code to provision and manage it. If you use the invitation for other Airwall Edge Services, it is ignored.
- **New options for user onboarding** – When you onboard people using activation codes using either **Airwall Invitations** or People group user onboarding, you can now set up these new options:
  - User auth for remote sessions
  - Airwall Agent's or Server's overlay device IP netmask
  - Bypass Airwall Gateway

Logging Updates

- **Per-Airwall logging** – You can now configure remote syslog and overlay traffic logging per Airwall Edge Service. **Learn more:** Set overlay traffic logging for an Airwall Gateway on page 422.
- **Set global overlay traffic logging** – Tech Preview You can now set overlay traffic logging globally for your Airwall secure network on the page for an Airwall Gateway that supports it.
- **Log rate limiting** – The Conductor now rate limits log messages to 100 messages per second. You can examine rate limiting details using the Airshell command: `log status <hip|ebm2>`. **Learn more:** Status Commands on page 368.

Airwall Relay Updates

Message rate limiting – An Airwall Relay now rate-limits "Relay missing client address" messages to once every 15 minutes per client.

New and Improved Conductor Features

Learn more –

-
-

New and Updated Help

In addition to the content added for new features linked above, here's the new and updated content published since our last major release:

New –

- Move an Airwall Gateway to a Different Conductor on page 132
- Deploy a Conductor in Microsoft Hyper-V on page 231
- How to Update from Older Versions on page 515
- Airwall Agent or Server or Airwall Gateway using IPv6 has trouble connecting on page 489
- Event Monitors and Alerts Reference on page 120
- Auth0 Update does not affect OpenID Connect Integration on page 501
- U.S. Cellular Carrier Certifications on page 377
- 3G Sunset – Required Cellular Firmware Update for 110g on page 499
- Manage Airwall Edge Services from an Overlay on page 427
- Overlay Timelines on page 427
- Device page on page 417
- Set a Proxy Server on page 238
- Configure an authenticated Airwall Agent or Server session on page 384
- Knowledge Base (KB) Articles on page 778 - 90 KB articles are now available in Airwall Help

Updated –

- Step 1: Add Alibaba Cloud as a provider to your Conductor on page 315
- Microsoft Azure – Set up an Airwall Gateway on page 324 – Create Application
- Airshell (airsh) Command Reference on page 362
- Install a Custom CA Certificate Chain on page 239
- Put an Airwall Gateway into diagnostic mode on page 478
- Put the Conductor into diagnostic mode on page 477
- Backhaul Bypass on page 395
- Search in the Conductor on page 44
- Edit people who can access an overlay network on page 419
- See Airwall Edge Service Information and Status on page 95
- Security Notices on page 498

What's New in 3.0.0

This version of the Airwall Solution includes several usability and functionality improvements that can simplify and streamline the setup and administration of an Airwall secure network.

Add Trust Policy using Drag-and-drop

You can now add and remove trust between devices on an overlay visually, or through context menus on a graph. Changes to trust on the graph are reflected on the **Devices** tab.

Learn more – Add and remove device trust on page 427

Backhaul Bypass

You can designate an Airwall Gateway as a bypass egress and then point other Airwall Gateways at it so they can reach bypass destinations through the designated bypass egress Airwall Gateway.

Learn more – Backhaul Bypass on page 395

Bulk Editing of People and People Groups

You can add many local users to the Conductor at one time by importing them in bulk. You export a .csv file as a template or with current users, and then import to add people to the Conductor in one step.

Learn more –

- Import people using a CSV file on page 61
- Remove people in bulk on page 63

Customized Permissions for System and Network Administrators

You can fine tune permissions for system and network administrators, giving you finer control over permissions on your network.

Learn more – Customize Permissions for System and Network Administrators on page 56

Streamlined Conductor View for Network Administrators

One of the custom permissions you can set for Network administrators provides them with a streamlined view that can simplify their workflow. Network administrators using the streamlined view can manage their overlays, and the devices, **Device groups**, and Airwall Edge Services in them.

Learn more – Set a Streamlined View for a Network Administrator on page 58

Reports

You can now run reports on different types of network activity on your Airwall secure network, including:

- Onboarding and offboarding of Airwall Edge Services or people
- Status of Airwall Edge Services or devices
- Conductor local or remote access

Learn more – Run Network Activity Reports on page 116

Monitors and Alerts

This version includes the following additions:

- **CPU Frequency** – The Airwall health data monitors can now monitor CPU frequency.
- **Details for Intrusion prevention** – Intrusion prevention alerts now indicate which devices are the source or destination of the alert where possible.

Conductor Customization

You can customize the Conductor login screen and emails sent from the Conductor for your business. Here's what you can customize:

- **Conductor login screen** – Add your company logo, and change the background colors and favicon.
- **Conductor emails** – Add your company logo and change the text color. You can also customize the subject line and add a note from the administrator when sending Airwall Invitations.

Learn more –

- Customize the Conductor on page 40
- Customize the Conductor Login page on page 40
- Customize Conductor emails on page 42

Disconnected Mode

Reduce the traffic from Airwall Agents and Servers connecting to your Conductor by setting up Disconnected mode. In Disconnected mode, Airwall Agents and Servers connect to your Conductor at intervals – between 10 minutes and 12 hours (720 minutes) – to get updates when people are not actively using the connection.

By reducing the traffic on your Conductor, Disconnected mode allows you to improve performance and scalability of your Airwall secure network. In v3.0, Disconnected mode is supported by the v3.0 Android, Linux, and macOS Airwall Agents and Servers.

Learn more –

- Disconnected Mode – Reduce Conductor traffic from Airwall Agents and Servers on page 99
- Sync an Airwall Agent or Server in Disconnected Mode on page 29

Airwall Invitations

This version includes several enhancements to Airwall Invitations:

- When you're creating **People groups** with user onboarding enabled, you now have the option to send email to users when they get an activation code in the system. The email provides instructions on how to download an Airwall Agent and connect it to the Conductor.
- The email sent with Airwall Invitations has more options for customization. See **Conductor Customization** above.
- Airwall Invitations can now be used to give activation codes to existing users in addition to sending them to an email address or bulk downloading them. See the **Airwalls** > **New Airwall invitations**.
- The naming schema for Airwall Invitations can now include the hostname of the connecting Airwall Edge Service.
- You can now include the hostname of the connecting Airwall Edge Service when naming devices connecting using Airwall Invitations.

Learn more – Walkthrough - Onboard people to your Airwall secure network with User Authentication on page 83

Linux Airwall Server

This version includes these additions to the Linux Airwall Server:

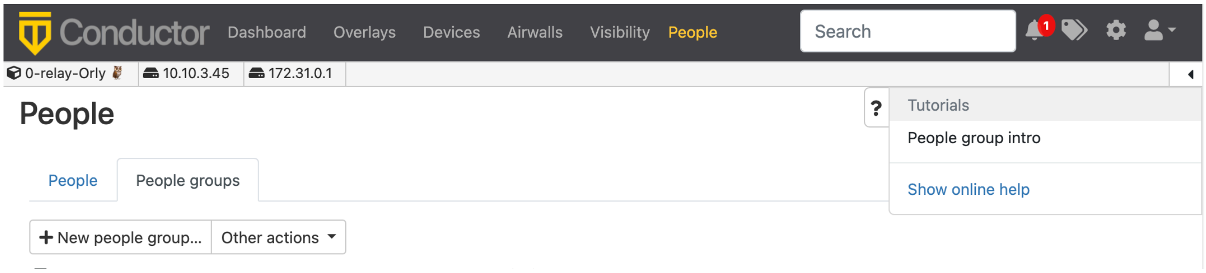
- **DockerHub deployment** – The Linux Airwall Server can now be deployed in a container from DockerHub using Ubuntu18 and CentOS8. For additional example Dockerfiles, contact Customer Success at Customer Success.
- **Supports Airshell** – The Linux Airwall Server now has the Airshell command-line utility. To start it, type `sudo airsh` (root user) or `sudo airwall -s`
- **Ping from port groups** – The ping function can now ping from the underlay or overlay port groups.
- **Firmware updates** – The Linux Airwall Server can now be updated from the Conductor.

Learn more –

- Connect with a Linux Airwall Server on page 26
- Linux Airwall Server Airshell commands on page 372

Conductor Tutorials and Help

The Conductor now contains several tutorials to help you set up and configure a new Conductor, as well as use and understand different features in the Conductor. You can also directly access Airwall help from the Conductor:



Learn more –

- Get Started using Conductor Help and Tutorials on page 140
- Show or Hide Conductor Setup progress on page 40

Licensing Updates

In v3.0, the following licenses have been changed:

- The Airwall Gateway 100V is no longer available
- You no longer need a separate license for port mirroring

Manage failover between underlay port groups

The Link Manager that Conductor uses to manage port failover groups has been improved. The following has been updated:

- You can now set port group link auto-repair globally per Airwall Gateway.
- You can now manage underlay links independently by traffic type.
- When you set up link failover groups, you can now require all pings to be successful if multiple ping destinations are assigned.

Learn more – Manage Failover between Underlay Port Groups on page 391

API Updates

The following updates and improvements have been made to the API:

- **Pagination** is turned on by default in 3.0 for all index endpoints, which may affect existing scripts. Enabling pagination helps scale Conductor capacity. If you need to preserve existing behavior, add a query parameter for `pagination=false` to any index API endpoints you are using.
- The API for **Airwall Invitations** now includes new invitation methods: email invites, download multiple activation codes, apply an invite to an existing person, or download a reusable invitation. The documentation has also been updated.
- **People reference** now includes `person_group_ids` and `overlay_network_ids`.
- **Person groups reference** now includes user onboarding configuration information.

Terraform Deployment Support

This version contains Terraform deployment support for Conductors, Airwall Gateways, and Linux Airwall Servers for all supported Cloud Providers. For example plans, please contact Customer Success at Customer Success.

New and Improved Conductor Features

Dashboard	The Dashboard now includes a **Provisioning** tab where you can see and manage all provisioning requests.
General	There is now infinite scrolling for lists on most pages, and streamlined inline editing, including direct editing of names and tags at the top on most pages.

Devices page	This page has been simplified, and provides more details on device conflicts to help you troubleshoot.
People page	Administrators can now view the Airwalls owned by a person from the person details page.
Settings	The Conductor Settings page has been streamlined and reorganized to make it easier to find the settings you want.
New Airwall Agent user authentication settings	New settings allow you to automate assigning an Airwall Agent owner: **Require owner for Airwall Agent authorization** and **Auto-assign Airwall agent owner on login**.
Replacing Airwalls	You now have the option to revoke, or both revoke and delete, a source Airwall Edge Service after replacing. Replaced Airwall Edge Services that are not deleted are named "<old name (Replaced by UID of replacement)>" to make them easier to find.
Diagnostic Tools on the Standby Conductor	You can now use diagnostic tools on a Standby Conductor.
Better CA certificate replacement and removal handling	When you replace your CA certificates, any Airwall Gateways with custom certs installed now check their cert against the new CA. If they cannot be verified, the cert is removed so the Airwall Gateway does not lose access to the Conductor. If the CA is removed entirely, all customer certs are also removed.

Learn more –

- The Conductor Dashboard on page 32
- Configure Authentication Options on page 242

New and Updated Help

In addition to the content added for new features linked above, here’s the new and updated content published since our last major release:

New –

- Expand the Disk Size for a virtual Airwall Gateway on page 311
- Airwall Gateway 75 Installation Guide (PDF)

Updated –

- Walkthrough - Onboard people to your Airwall secure network with User Authentication on page 83
- Configure Port Groups with Airshell on page 376
- Set up Conductor high availability on page 269
- Manage devices dynamically with Smart Device Groups on page 105
- Configuring a Conductor IP, Friendly URL, or Port on page 236
- Understand People Roles and Permissions on page 58
- Configure Conductor Remote Logging on page 273
- Enable DNS lookup for bypass destinations on page 398
- Monitor Activity and Connections on page 116
- Integrate Third-party Authentication with OpenID Connect on page 247
- Airwall Gateway Airshell Console Commands - airsh - New `conf model` command

What's New in 2.2.13

Here are the new features and enhancements in this version.

New and Improved Conductor Features

Port mirroring	Airwall Gateways configured with port mirroring now show mirrored status in list and status views. Port mirroring DEV-15399
OpenID Connect	OpenID Connect tokens are now included in the webapp log at the debug level to assist with integration.
User Preferences	The Conductor now remembers user page size settings across sessions, browsers, and computers.
Underlay Network view	This view now visually separates the different underlay IPs to show their ping statuses, RTT, and count as they are being pinged.
Device name now shown on Overlay and Device pages	If you set a name for a device in an Airwall Agent or Server, it is now shown on the **Overlays** and **Devices** pages in the Conductor.
CPU Graph Changes	Starting with 2.2.12, the CPU graph on an Airwall Gateway Reporting page now shows CPU percentage, not the previously-shown CPU load average. The CPU percentage graph shows the percentage of CPU capacity being used on the Airwall Gateway over time.

New and Updated Help

In addition to the content added for new features linked above, here's the new and updated content published since our last major release:

New –

- Diagrams for Port Mirroring
- Virtual Airwall Edge Services

Updated –

- How Airwall Licensing Works on page 191
- Set up a virtual Airwall Gateway in VMware ESX/ESXi on page 306
- Set up a virtual Airwall Gateway in Microsoft Hyper-V on page 308
- Alibaba Cloud – Set up an Airwall Gateway on page 315
- Amazon Web Services – Set up an Airwall Gateway on page 320
- Microsoft Azure – Set up an Airwall Gateway on page 324
- Google Cloud (GCP) – Set up an Airwall Gateway on page 334
- Airwall Gateway Airshell Console Commands - airsh - New `conf model` command
- Mirror Traffic to a Dedicated Port

What's New in 2.2.12

Here are the new features and enhancements in this version.

Licensing Changes

- Port mirroring now requires an add-on license for any Airwall Gateway acting as a Mirror Source

- Licensing page changes:
  - Licenses are now paginated as needed.
  - Vouchers are automatically consolidated

Airwall Servers for Raspbian and Ubuntu ARM64

You can now get an Airwall Server that runs on Raspbian or Ubuntu ARM. For installation information, see Raspbian and RPi4/Ubuntu ARM64 – Install the Airwall Server on page 12.

Platform End of Life for 100 Series Appliances

Tempered announces the End of Life schedule for the HIPswitch 100 series platforms. For more information and a schedule, see Platform end-of-life for Airwall Gateway/ HIPswitch 100 series on page 505.

New and Improved Conductor Features

Port mirroring	Airwall Gateways configured with port mirroring now show mirrored status in list and status views. Port mirroring DEV-15399
OpenID Connect	OpenID Connect tokens are now included in the webapp log at the debug level to assist with integration.
User Preferences	The Conductor now remembers user page size settings across sessions, browsers, and computers.
Underlay Network view	This view now visually separates the different underlay IPs to show their ping statuses, RTT, and count as they are being pinged.
Device name now shown on Overlay and Device pages	If you set a name for a device in an Airwall Agent or Server, it is now shown on the **Overlays** and **Devices** pages in the Conductor.
CPU Graph Changes	Starting with 2.2.12, the CPU graph on an Airwall Gateway Reporting page now shows CPU percentage, not the previously-shown CPU load average. The CPU percentage graph shows the percentage of CPU capacity being used on the Airwall Gateway over time.

New and Updated Help

In addition to the content added for new features linked above, here's the new and updated content published since our last major release:

New –

- Diagrams for Port Mirroring
- Virtual Airwall Edge Services

Updated –

- How Airwall Licensing Works on page 191
- Set up a virtual Airwall Gateway in VMware ESX/ESXi on page 306
- Set up a virtual Airwall Gateway in Microsoft Hyper-V on page 308
- Alibaba Cloud – Set up an Airwall Gateway on page 315
- Amazon Web Services – Set up an Airwall Gateway on page 320

- Microsoft Azure – Set up an Airwall Gateway on page 324
- Google Cloud (GCP) – Set up an Airwall Gateway on page 334
- Airwall Gateway Airshell Console Commands - airsh - New `conf model` command
- Mirror Traffic to a Dedicated Port

What's New in 2.2.11

Here are the new features and enhancements in this version.

Mirror network traffic for Packet Analyzers

You can now mirror network traffic to packet analyzer/visibility tools (like Nozomi or Wireshark) to see what's going on in your Airwall secure network.

See more: Mirror traffic from your Airwall Gateways to a packet analyzer tool on page 457

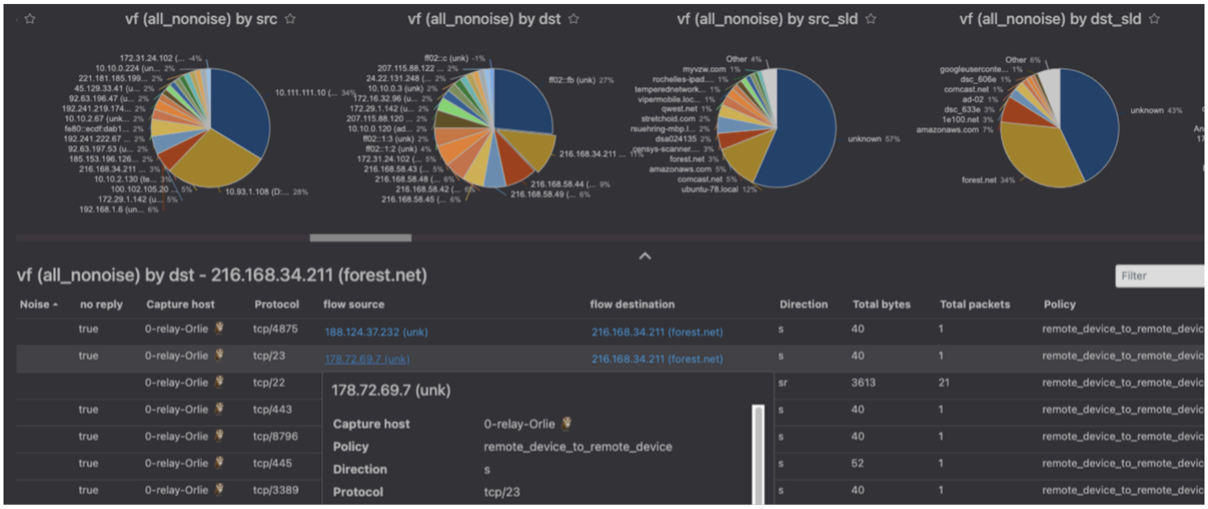
Assign Separate DNS Servers to Airwall Agents and Servers

If you need Airwall Agents and Servers to use different DNS servers, you can assign different DNS servers on an Overlay or individually for Airwall Agents and Servers that support it.

See more: Assign Separate DNS Servers to Airwall Agents and Servers on page 349

Preview - Airwall Visibility Connector

The Airwall Visibility Connector gives you a dynamic L4 view into the health and status of your Airwall secure network. You can explore many pre-computed reports in the Conductor, and can integrate other threat detection platforms. When configured, the Conductor continuously learns from these external systems, and can report or respond to threats as they are detected.



vf (all_nonoise) by dst - 216.168.34.211 (forest.net)

Noise ▴	no reply	Capture host	Protocol	flow source	flow destination	Direction	Total bytes	Total packets	Policy
	true	0-relay-Orlie	tcp/4875	188.124.37.232 (unk)	216.168.34.211 (forest.net)	s	40	1	remote_device_to_remote_devic
	true	0-relay-Orlie	tcp/23	178.72.69.7 (unk)	216.168.34.211 (forest.net)	s	40	1	remote_device_to_remote_devic
		0-relay-Orlie	tcp/22			sr	3613	21	remote_device_to_remote_devic
	true	0-relay-Orlie	tcp/443			s	40	1	remote_device_to_remote_devic
	true	0-relay-Orlie	tcp/8796			s	40	1	remote_device_to_remote_devic
	true	0-relay-Orlie	tcp/445			s	52	1	remote_device_to_remote_devic
	true	0-relay-Orlie	tcp/3389			s	40	1	remote_device_to_remote_devic

178.72.69.7 (unk)

Capture host	0-relay-Orlie
Policy	remote_device_to_remote_device
Direction	s
Protocol	tcp/23

Contact Customer Success at Customer Success if you would like to preview this feature. A future version will expose the full feature with appropriate documentation, training, and platform options.

Raspberry Pi Airwall Agent

You can now get an Airwall Agent that runs on Raspberry Pi. For information, see .

Platform End of Life for 100 Series Appliances

Tempered announces the End of Life schedule for the HIPswitch 100 series platforms. For more information and a schedule, see Platform end-of-life for Airwall Gateway/ HIPswitch 100 series on page 505.

New Knowledge Base and Support Site

Tempered has a new site for our product Knowledge Base articles and support. Update your links!

- New Link to open a Support ticket: https://www.tempered.io/support/supportReq.html

New and Improved Conductor Features

Update macOS Airwall Agents from the Conductor

In v2.2.11, the macOS Airwall Agent introduces the ability to update from a Conductor package. For those running v2.2.10, upgrade one last time manually, with:

```
sudo installer -pkg /path/to/
Airwall-Mac_2.2.11.xxxx.pkg -
target /
```

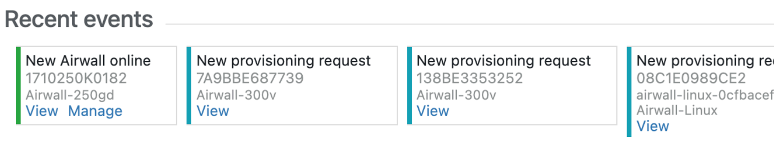
You can then update future versions from a Conductor update package.

DEV-14804

Clear Recent events on the Dashboard

On the Dashboard System navigation, you can clear all events by selecting the Dismiss events icon 🔕:

DEV-15157



Recent events

New Airwall online
1710250K0182
Airwall-250gd
View Manage

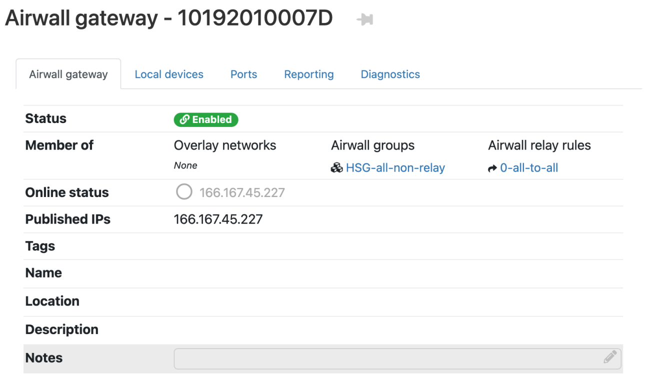
New provisioning request
7A9BBE687739
Airwall-300v
View

New provisioning request
138BE3353252
Airwall-300v
View

New provisioning re
08C1E0989CE2
airwall-linux-0cfbacef
Airwall-Linux
View

New Notes field on Airwall Edge Service pages

There is now a place where administrators can add notes on Airwall Edge Service pages: DEV-15111



Airwall gateway - 10192010007D

Status	Enabled		
Member of	Overlay networks None	Airwall groups HSG-all-non-relay	Airwall relay rules 0-all-to-all
Online status	○ 166.167.45.227		
Published IPs	166.167.45.227		
Tags			
Name			
Location			
Description			
Notes			

Conductor theme now follows you

Your Conductor theme is now saved across computers and browsers. DEV-15022

Failover groups improvement

Failover groups now start with an initial likely selection for underlay link failover configuration. DEV-14900

OpenID Connect improvement

OpenID Connect now supports Azure Active Directory (AD). DEV-14864

Conductor Certificate Expiration reminders

When a Conductor certificate is near expiration (1 month + 1 week), you get an event and a tag on the cert info that warns you of the upcoming expiration. On the day of

	expiration, you get an alert, event, and a tag telling you the certificate has expired. DEV-15160
Download a CSV with Licensing and Airwall Data	You can download all licensing and Airwall data in CSV format from **Settings** > **Licensing**. This data can be helpful in ensuring your Conductor vouchers are correctly renewed. DEV-14869
Access Windows Date Selection improvements	The way you choose dates for Access windows has been improved. DEV-14649
Airshell Improvements	You can now save your network configuration when doing a factory reset using the keep-networking option. See Airshell (airsh) Command Reference on page 362. DEV-14465
Alert Improvements	Intrusion prevention alerts now indicate which devices are the source or destination of the alert where possible. These alerts are in Conductor alerts and indicated by the ID in the event data from the API DEV-14502, and snort metadata will be included in the API. DEV-14490
Diagnostic Mode Improvements	• Diagnostic Report Addition – The Diagnostic report now includes policy-based routing rules and IPv6 routes. DEV-14720 • Return to Diag mode after a hotfix – When applying a hotfix that does not require reboot, when the hotfix is complete you get an option to return to Diag mode. DEV-14582
API Improvements	• API tracks when changes happened – The Conductor API now serializes when many resources were created and updated, and includes These changes make it easier to see when resources were added or have changed from the API. DEV-14962 • New API endpoints – New API endpoints show history of Airwall Edge Services being managed and revoked DEV-15113, and returns a list of devices that each device has policy to and what overlays the policies are in DEV-14717. • Date time/NTP settings – The API now allows updating of Date time/NTP settings. DEV-14716

New and Updated Help

In addition to the content added for new features linked above, here's the new and updated content published since our last major release:

New –

- Configure an Underlay Port Failover Group
- Best Practices for Underlay Port Failover Groups

Updated –

- Seamless Bypass

Introducing our new free offering – Airwall Teams

Airwall Teams allows you to build truly private system-to-system networks—that span public, private, cloud, and mobile networks using an intuitive graphical interface - just draw lines between devices you want to connect. Airwall Teams replaces and expands on our Airnet platform.

What's New in 2.2.10

Version 2.2.10 of our product includes many new features and enhancements.

What’s New

Access Windows for authenticated users

Specify or restrict what days and times authenticated users can log in to access resources on your secure network using Access Windows.

See more: Set Times Authenticated Users can Access the Secure Network on page 92

Automatic Relay Rules

Enable all connections in an overlay network to use a group of relays. This provides a less-granular, but simple way to manage relay rules.

See more: Set an Overlay to Automatically Manage Relay Rules on page 354

Airwall Gateway Custom Certificates

By default, Airwall Gateways come with a Tempered factory-installed certificate. You can now add your own custom CA certificate to use for Conductor communication.

See more: Add or Replace a Signed Certificate on an Airwall Gateway for Conductor Communication on page 384

Bulk Configuration of Airwall Gateways

Configure certain settings in bulk for Airwall Gateways or Airwall Gateway groups.

See more: Bulk Configuration of Airwall Edge Services on page 378

Enable DNS for Seamless Bypass

You can now enable DNS to use fully-qualified domain names (FQDN) for bypass destinations.

See more:

- Enable DNS lookup for bypass destinations on page 398
- Local Bypass on page 394

Setup Wizards for configuring Conductors and Airwall Gateways

2.2.10 has added two wizards to help you in deploying an Airwall secure network. The Conductor Deployment Wizard walks you through setting up, licensing, and provisioning a new Conductor, and the new Airshell (`airsh`) command `setup-ui` walks you through the most common Airwall Gateway setup options.

See more:

- Conductor Configuration Wizard Settings on page 197
- Configure an Airwall Gateway with the airsh Setup Wizard on page 274

Airwall Status Indicators

There are new ways to see information and status on the Airwall Edge Services connecting to your Airwall secure network

See more: See Airwall Edge Service Information and Status on page 95

Cloud Improvements

This release includes improvements that make it easier to deploy cloud Conductors and Airwall Gateways, and includes support for AWS GovCloud (see below):

- **ENA and SR-IOV support** – You can now deploy instances with enhanced networking configuration enabled with either ENA or SR-IOV, and see which machine types support or require ENA. Note that machine types marked as ENA may deploy as SR-IOV.
- **Disk IO has been improved** – Cloud deployments now include NVMe (memory) disk options.
- **Cloud HA deployment has been automated** – Simplified deployment for HA, eliminating many of the places where misconfiguration could happen.
- **New Azure cloud image names** – Image names now reflect their use, making it easier to choose the correct image.
- **Additional information as images are created** – More details are included in the status pane as the Conductor creates cloud images.
- **Can now choose resource groups** – You can now choose a new or existing resource group when you create cloud Airwall Gateways and Conductors.

  Note: If you choose an existing resource group, make sure no resource names in the existing resource group conflict with the new Airwall Gateway and Conductor deployment name that you are creating.
- **More information available in the Conductor** – New attributes are shown for cloud Airwall Gateways on the **Diagnostics** tab.

Preliminary IPv6 Support

If you have devices with IPv6 addresses, IPv6 is now supported for Airwall Gateways and Linux Airwall Servers. The control for source NAT is shared for both IPv4 and IPv6. Configurations sourcing NAT IPv4 but not IPv6 are not supported.

Airwall Gatewaysnow support static IPv6 addresses for both the underlay and overlay (some cellular carriers may not support it). You also need to assign a static IPv6 address to the Airwall Gateway.

Since IPv6 only supports routed configurations, you need to assign an IPv6 overlay address to the Airwall Gateway to use IPv6 overlay. L2/subnet extensions are not supported.

See more: Set up a secure IPv6 overlay on page 380

AWS GovCloud Support

Cloud Conductors and Airwall Gateways can be now be deployed in AWS GovCloud. Follow the instructions for deploying in AWS:

- Deploy a Conductor on Amazon Web Services (AWS) on page 205
- Set up Cloud Providers on page 433
- Deploy a cloud Airwall Server on page 355

Exponential Backoff

Added exponential backoff to the Airwall Gateway to/from Conductor management connection to comply with Verizon data retry requirements. This change means it could take up to 3 minutes to reconnect after an extended outage. *(DEV-14648)*

What's New in 2.2.8

Version 2.2.8 of our product includes many new features and enhancements.

What’s New

New Airwall Gateway Hardware – the Airwall-110

The Airwall-110 Series is a major upgrade for the 100-Series, with higher performance and global cellular connectivity – all in a smaller form factor that maximizes the v2.2.8 improvements. The Airwall-110 has more (4x) bandwidth performance and two serial ports, runs all Snort intrusion detection monitors, handles up to 6 HD video streams, and has more storage and memory (so it has higher capacity, quality, and scalability for production environments).

See more: Airwall Gateway 110 Series on page 144

New cellular modem support

Version 2.2.8 supports the upcoming North America and Global cellular expansion trays for our Airwall-150 appliance. These LTE Category 4 expansion modules come in two variants supporting North America and Rest of World. These expansion trays allow you to connect your Airwall 150 to more cellular carriers in more countries including the United States, Canada, Australia, New Zealand, Japan, the European Union, and other countries recognizing CE RED certificates.

Conductor Dashboard and Usability Improvements

The Conductor Dashboard has been improved to give you a broader look into the status of your Airwall secure network. New features include:

- Ability to pin pages you visit frequently
- See how many Airwall Edge Services are online, and how many authenticated users are logged in.
- Easily manage new provisioning requests
- See when new firmware and software is available, and easily update your network.
- Improved user onboarding workflow (see Improved User Management below)

See more:

- The Conductor Dashboard on page 32
- Create or Manage Dashboard Messages on page 38
- Conductor Icon Reference on page 35
- Monitor Connections to your Airwall secure network on page 124
- Download Airwall Edge Services firmware updates on page 129
- Update firmware for a group of Airwall Edge Services on page 131

Improved User Management and Remote Access User Features

Remote access user management has been expanded to scale for large organizations, with the Conductor doing most of the work that admins used to have to do to invite, onboard (especially installing and activating the Airwall Agents), orchestrate, and authenticate remote access users. Onboarded users can see what they can access through the overlay networks in Conductor, eliminating frequent support calls to Conductor admins for help getting server IP addresses.

See more:

Conductor Admin Topics

- Connect People's Devices to your Airwall secure network on page 64
- Connect People as Remote Access Users on page 74
- Connect People's Devices with Activation Codes on page 75
- Set up a People Group on page 89
- Manage Versions of Airwall Agents and Servers on page 126
- Provision Airwall Gateways using Activation Codes on page 193
- Walkthrough - Onboard people to your Airwall secure network with User Authentication on page 83

End user topics

- Change my Conductor password on page 30

- I have an Activation Code on page 15
- I want to request to connect on page 17
- I have a "Finish Setting up my account" email on page 15
- Create or Edit Airwall Agent or Server Profiles on page 29
- I am having trouble connecting on page 31

Enhanced Monitoring

You can now set monitor thresholds on health data and traffic stats to detect potential problems before they occur. We have redline stats for performance metrics of the Airwall Gateway, and for volumetric traffic stats.

Seamless Bypass (split tunnel)

Seamless bypass enables you to deploy without knowing all of the hosts to allow in an overlay policy. Seamless bypass replaces the need to create policy exceptions, and reduces the complexity, extra hardware, extra cabling, and reliance on configuration of your underlay infrastructure.

See more: Local Bypass on page 394

Alibaba Cloud Conductor and Airwall Gateways

You can now use Alibaba Cloud to deploy cloud Conductors and Airwall Gateways, and seamlessly connect cloud Conductors and Airwall Gateways with each other, as well as virtual and on-premises or physical environments. You can deploy an Airwall secure network on all of the major cloud providers.

See more:

- Deploy a Conductor on Alibaba Cloud on page 202
- Alibaba Cloud – Set up an Airwall Gateway on page 315

Routed Port Group Improvements

The ability to configure port groups can give you up to a 30% performance increase for common deployment cases using a single interface in the overlay port group (for example, cloud gateways, virtual gateways, and optionally on physical gateways). It is simpler to deploy and avoids multicast/broadcast chatter over the tunnel.

See more:

- Set up Port Groups on an Airwall Gateway on page 386
- Set up an Underlay Port Group on page 389
- Set up Overlay Port Groups on page 386

Custom signed Certificate Improvements

You can replace a signed certificate on the Conductor with the old certificate remaining active until the new certificate is activated.

See more: Add or Replace a Signed Certificate for the Conductor UI on page 239

Easier Deployment of High Availability Cloud Conductors

The Airwall Solution has automated the process of creating high availability Conductors in the cloud across different providers. You can now back up your Conductor and easily create an HA standby in the cloud using the Conductor's automated process and be guaranteed a successful cloud HA deployment.

See more: Automatically Create an Standby HA Conductor in the Cloud on page 265

Remote Airshell Access into Airwall Gateways

You can securely log in to the overlay IP address of an Airwall Gateway with key-based SSH, and run Airshell (airsh) commands remotely. Airsh has been enhanced to perform many of the functions of diagnostic mode. Remote access can help avoid in-person visits to perform diagnostics and troubleshooting. Status and statistics are available using airsh, which includes tab-completion and inline help.

See more:

- Set up Remote Access to Airshell via SSH on page 374
- Access an Airwall Gateway Remotely on page 375

Port configuration replication

You can now replicate the port configuration between two Airwall Gateways when setting up an Airwall Gateway HA pairing, or when replacing an Airwall Gateway.

See more:

- Configure High Availability Airwall Gateways (v2.2.8 and later) on page 399
- Replace an Airwall Gateway on page 132

Device Manufacturer (MAC address OUI) is now displayed

The **Devices** list now shows the manufacturer's name determined from the MAC address OUI (organizationally unique identifier), where available, in the **OUI** column. You can also now update the OUI list as needed.

See more:

- Update the MAC address (OUI) (Manufacturer) List on page 484
- See MAC address OUI (Manufacturer) Information for Devices on page 115
- Search for or Sort Devices by MAC Address OUI (Manufacturer) Name on page 115

Manage Airwall Agents through an MDM

Some MDM solutions now support managing Airwall Agents.

See more: Manage Airwall Agents through an MDM (Mobile Device Management) solution on page 82.

SD-WAN

An option was added to expose the Differentiated Services Code Point (DSCP) field of the inner IP header (plaintext) to the outer (encrypted) encapsulating header. This allows for classification of different types of network traffic for routing and prioritization purposes.

What's New in 2.2.5

Version 2.2.5 of our product includes many new features and enhancements.

What's New

Support for NAT Subnet Broadcasts	The Airwall Solution now supports NATing subnet broadcasts on the device network.
New Airwall help content	• Airwall Invitations • Renew Expired Licenses • Integrate Third-party Authentication with OpenID Connect • Set up an Airwall Gateway in Microsoft Azure
Updated Airwall help content	• Configure a DHCP relay on an Airwall Gateway

- Configure protected devices with DHCP
- Route encrypted connections with Airwall Relay
- Configure Airwall Relay rules
- Install Airwall Server on Linux

What's New in 2.2.3

Version 2.2.3 of our product includes many new features and enhancements.

Introducing Tempered Airwall

Tempered's fully encrypted, virtual air-gap network security solution is now called Airwall. Our product offerings are also changing to match our brand and make their functions clearer.

What’s New

OpenID Connect support for Airwall Clients

We have added OpenID Connect support for authenticating remote sessions on Android, iOS and macOS Airwall Agents (formerly Android, iOS, and OSx HIPclients). There is also now a global option to lock out clients that do not support user auth.

People groups as Overlay members/managers

People Groups are now able to be members of Overlay Networks as well as Managers of Overlay Networks. Now user permissions can be configured entirely in an authentication provider such as LDAP or OpenID Connect via people group membership.

Lockdown Mode

Lockdown Mode is now configurable from the Airwall Conductor for Airwall Agents (formerly HIPclients) that support this feature (currently supported by the Windows Airwall Agent).

Cloud Linux Airwall Servers

The Airwall Conductor can create and deploy Linux Airwall Servers directly in any cloud provider, such as Azure, AWS, or Google.

New Airwall Names

Here are translations from previous names to current terms for the Airwall Solution Airwall:

What it used to be		Airwall name
Conductor	->	Airwall Conductor
HIPservice	->	Airwall Edge Service
HIPswitch	->	Airwall Gateway
HIPclient	->	Airwall Agent
HIPserver	->	Airwall Server
HIPapp	->	Airwall Agent or Server
HIPrelay	->	Airwall Relay
hipsh	->	airsh
Tempered Networks	->	Tempered
Tempered Networks Technical Documentation		Airwall Help

You may see both old and new terms used in content and the Airwall Conductor as this transition is made.

Introducing Tempered Airwall

Tempered's fully encrypted, virtual air-gap network security solution is now called Airwall™ – a revolution in secure networking, making networks invisible. The products and parts that make up the Airwall are also changing to match and make their functions clearer.

New Airwall Names

Here are translations from previous names to current terms for the Airwall Solution Airwall:

What it used to be		Airwall name
Conductor	->	Airwall Conductor
HIPservice	->	Airwall Edge Service
HIPswitch	->	Airwall Gateway
HIPclient	->	Airwall Agent
HIPserver	->	Airwall Server
HIPapp	->	Airwall Agent or Server
HIPrelay	->	Airwall Relay
hipsh	->	airsh
Tempered Networks	->	Tempered
Tempered Networks Technical Documentation		Airwall Help

You may see both old and new terms used in content and the Airwall Conductor as this transition is made.

Technical Documentation

If you are missing the previous Tempered Networks Technical Documentation, it is still available. All of the content for *current versions* is included and being improved right here in the new Airwall Help. If you want still want to see the pre-Airwall help, click the link on the Airwall Help home page.

What's Not Changing

What's not changing is our mission to revolutionize security for a connected world. Airwall increases security, reduces complexity, and dynamically handles changes on your network.

What's New in 2.2

Version 2.2 of our product includes many new features and enhancements.

2.2.1 HIP tunnelMonitoring

New in this release is the ability to monitor HIP tunnel state changes directly. You can configure a monitor to watch the HIP tunnel to a particular remote Airwall Edge Service or to all trusted peer Airwall Edge Services. As with all monitors, you can create actions on events to alert, change policies, etc.

2.2.1 HIP tunnelstats graph

The tunnel stats introduced in 2.1.5 for Airwall Relays is now available for all Airwall Edge Services. You can see Tx and Rx bits between any pair of Airwall Gateways, allowing you to troubleshoot underlay and overlay connectivity issues.

2.2.1 OpenID Connect

Conductors now support OpenID Connect as an external authentication provider type. You can now use an Identity and Access Management tool such as Okta or OneLogin and integrate Single Sign-On (SSO) or Multi-Factor Authentication (MFA) support.

2.2.1 Multiple Underlay Networks

We now support active/standby multi-homed wired and wireless uplinks, even allowing communication between different ISPs. Multiple Underlay Networks give you more control over which link handles HIP tunnels and which link handles connection to the Conductor.

2.2.1 Multiple Overlay Networks

We now support isolation between port groups. Each overlay port group has its own overlay IP, static routes, and related network settings. Each overlay port group bridges its interfaces, but communication between port groups requires policy.

2.2.1 Port group Configuration

The **AirwallsPorts** user interface has been completely overhauled to enable the configuration of multiple underlay and overlay port groups. Several things that were configured in different places in 2.1.x are now consolidated in one location:

- Port group
- Port role
- Failover group settings
- Wi-Fi
- Cellular
- 802.1q VLAN tags
- Overlay IP/Netmask

Interfaces appear on the screen with live status information from the Airwall Edge Service. Also, all configurations are committed only after the Airwall Edge Services validates and successfully implements the changes, eliminating disagreement between what is configured in the Conductor and what is actually implemented in the Airwall Edge Service.

2.2.1 Network Objects

You can now use a CIDR (like 10.3.5.0/24) instead of a /32 for a device address. The term **Network Objects** simply refers to a device that uses a CIDR, and this device can be used wherever you would use any other device, like in device groups and overlay networks. Using network objects, you can allowlist an entire IP network in one click. This should make policy migration from Firewalls and Routers during new deployments much easier. Site-to-site VPN becomes trivial. More specific policies are still supported, so you can create wide policies to open general site-to-site traffic and still segment traffic to Airwall Edge Services.

Negative policies are also supported so you can allow networks or individual IP addresses (like a router) and then create exceptions using a negative policy (like a firewall).

This makes it much easier to manage Airwall Edge Services. Configurations become simpler, shorter, and easier to maintain. For cloud-based Airwall Edge Services, route injection is much simpler because routes are summarized.

2.2.1 User Auth (Windows, Mac, Android; iOS to release shortly)

MacOS and Android now support the user authentication feature introduced in 2.1.3 Windows clients and Airwall Servers. macOS will support this feature in a later release. This feature allows an admin to require client users to provide an additional factor of authentication, currently username and password, to access the overlay for a period of time. Since usernames and passwords are centrally managed, this mitigates concerns about stolen laptops or devices, giving an admin a centrally managed way to approve and deny overlay access.

2.2.1 New shell for Airwall Gateways (airsh)

New in this release is **Airwall shell** (airsh), a console that replaces the special login user accounts such as like *mapconfig*, *macinfo*, and *factory reset*. The Airwall shell provides tab-completion, inline help, and greatly expands your ability to deploy & configure an Airwall Edge Service directly without going into diagnostic mode.

2.2.1 Overlay Intrusion Prevention Monitor (snort)

Intrusion Prevention allows you to activate any number of pre-defined rule sets. Traffic on the overlay is inspected and if a rule matches, an event is created and sent to the Conductor. You can define event actions based on Snort events.

2.2.1 Airwall Gateway Latency improvements

On certain platforms with a single CPU core, the data plane latency has been reduced from 7ms to approximately 2ms. However, it is important to note that the reduction in latency can vary and depends on concurrency, packet sizes, and various other factors, but in general the latency through an Airwall Edge Service is reduced.

2.2.1 Airwall Relay Performance improvements

In version 2.2, we improved the speed of Airwall Relay traffic using XDP acceleration, allowing traffic to scale even more on your existing hardware.

2.2.1 Full tunnel Windows Airwall Agents and Airwall Servers

In prior releases, an Airwall Agent or Airwall Server needs policies to opt-in to the overlay network, the default being *split tunnel*. In version 2.2, an administrator can check a box on the Airwall Agent or Airwall Server in the Conductor to make the default *full tunnel and* capture all network traffic into the overlay, allowing for a few exceptions that may be in the underlay like DNS, AD, etc. Please note this is Windows only; macOS clients and Linux Airwall Servers will be available in a future release.

2.2.1 Multiple VLAN Tags per interface

We now support trunk ports, allowing you to have two or more VLANs configured on an interface. Each VLAN tag makes a new sub-interface. For example, VLAN tag 25 on eth0 creates a virtual interface named eth0.25. These interfaces can go into various port groups. East-West policies in the Conductor can be built between devices in different VLANs. Please note that you can still create bridges between VLANs as you did in version 2.1.x and earlier.

2.2.1 MAPv1 no longer supported

Conductor version 2.2 and beyond will no longer be able to manage Airwall Edge Services running 2.0 and earlier. Please note that this requires you to upgrade your Airwall Edge Services to version 2.0 or later your Conductor to version 2.2. Review the upgrade section at the beginning of this document for more information about the recommended upgrade process.

2.2.1 Dual-use port mode deprecated

Dual-use mode for interfaces is no longer available. Using multiple port groups and trunk ports, it is now much easier to implement split-tunnel with East-West policies. You can add the DNS, AD, and other servers as protected devices to an Airwall Edge Service and give them a separate overlay port group connected to the underlay network. In Conductor, you can then give your protected devices policy to the DNS, AD, etc., servers.

What's New in 2.1

Version 2.1 of our product includes many new features and enhancements.

2.1.6 Modbus TCP to RTU Gateway

We’ve enhanced our Serial over IP (SoIP) feature with a Modbus TCP to Modbus RTU gateway. After configuring Modbus via the HIPswitch SoIP settings in Conductor, the HIPswitch will accept Modbus TCP commands from servers, issue the commands to serially-connected Modbus RTU device(s), and return the responses via Modbus TCP back to the server. The HIPswitch accepts pipelined requests from the server(s). This provides optimal efficiency for Modbus traffic in terms of throughput, latency, and number of messages as compared to transparent Serial over IP.

2.1.6 DHCP Relay

HIPswitches can now relay DHCP requests to a central DHCP server as an alternative to your existing DHCP server. This allows additional deployment flexibility where extended DHCP options are needed, or an existing DHCP server integrates with other systems such as Active Directory and DNS.

Note: When moving devices from one HIPswitch to a different one, the central DHCP server may issue the same IP address to the device, which could result in policy or routing conflicts depending on your network.

2.1.6 Wireless Underlay Failsafe

The HIPswitch Link Manager, introduced in version 2.1.0, intelligently monitors the health of the underlay connection, detecting when there are no options for the HIPswitch to connect to Conductor or peer HIPswitches. Link Manager is now enhanced to reboot the HIPswitch which may restore the wireless connection to a healthy state. Occasionally, changes made in the wireless provider network will drop or hang a cellular or WiFi HIPswitch uplink in such a way that the modem cannot recover. Rebooting the HS will force the modem and cell tower or access point to renegotiate their connection; sometimes this restores a healthy connection. This behavior is on by default for wireless models, and can be disabled and configured per HIPswitch in the Conductor UI. You can configure the amount of time Link Manager waits to reboot the HIPswitch after first detecting underlay failure, and a minimum amount of time to wait between reboot attempts. By default, all wireless models enable this feature with a wait-to-reboot value of 10 minutes, and min-wait-between-reboots value of 30 minutes.

Note: See known issue DEV-9877 for additional information in reference to running a HIPswitch on the Microsoft Azure platform.

2.1.6 APAC Modem Support

The HIPswitch cellular expansion module SFF-MOD-MC7430 (PLF-0118-01) is now available for the HIPswitch 150, which includes the Sierra Wireless MC7430 modem for operation in Hong Kong, Macau, and Japan.

Note: Firmware release 2.1.6 is required to use this expansion module.

2.1.6 HIPswitch 250 Series Revision 2 Support

The HIPswitch 250 Revision 2 is now available and includes the following SKUs:

- HIPswitch 250e (PLF-0062-02)
- HIPswitch 250g (PLF-0066-02)
- HIPswitch 250gd (PLF-0111-02)

Revision 2 provides improved SFP compatibility, modem watchdog support, and improved modem carrier compatibility.

2.1.6 Wired Interface Support for Android

The HIPclient for Android now supports wired ethernet connectivity.

2.1.6 Tag integration with HIP invitations

You can now specify tags for HIP invitations, which apply to HIP services as they activate. This makes it easy to organize newly-activated HIP services and, when combined with smart device groups, automatically give them communications policy in overlay networks.

2.1.6 Longer HIPswitch UIDs

HIPswitches which are licensed with a 2.1.6 or higher firmware may generate a longer serial number portion of the UID (up to 20 characters), compared to the previous 12 characters. HIPswitches licensed from a previous release will not change their UID.

2.1.5 FIPS

Tempered Networks now offers FIPS 140-2, based on the HS-500 and Conductor-500 platforms. With FIPS, private keys are stored on the FIPS-certified HSM (hardware security module). The HSM performs all cryptographic operations. For this added key security, performance may be noticeably slower in terms of data plane throughput and firmware update processing. Redundant HA FIPS is not supported at this time.

2.1.5 Improved time management

NTP sync is now configurable from the Conductor. Various improvements have been made to ensure the Conductor and HIPswitch times remain closely synchronized, eliminating time-drift.

Note: We recommend pointing your HIP-enabled servers and clients to the same NTP Time source to ensure proper synchronization.

2.1.5 HIPswitch 75w Series

We now offer the HIPswitch 75 Series with a built-in WiFi module. Software version 2.1.5 does not currently provide WiFi LED status on the outside of the unit, but the WiFi uplink functions correctly. This will be addressed in a future release.

2.1.5 HIPswitch 150e Series

We now offer the HIPswitch 150e base platform, suitable for ICS and SCADA environments and includes 4x Gig-E and 1x SFP port, 1x micro-USB console port, and can be powered by PoE or external single- or dual-power supply. The HS-150 can sustain 75 Mb/s, and burst up to 100 Mb/s. This new platform supports field-upgradeable expansion modules.

2.1.5 HIPswitch 150 Series cellular module

This release supports a cellular expansion module suitable for North American cell carriers, which accepts 3FF Micro SIM cards. ATT, Verizon, T-Mobile, Rogers, and Telus have been field-tested at the time of this release.

2.1.5 HIPswitch 250 Series single- and dual-modem automated recovery

We added an internal watchdog monitor for cell carrier uplink connections. If a HIPswitch cannot connect to Conductor via any means, then occasionally (approx. once per day) it will perform a full reset, which may re-establish the carrier connection in certain environments. This will only occur when the HS-250 has no means of reaching the Conductor or peer HIPswitches.

2.1.5 HIPrelay bandwidth reporting

It is now possible to view the bandwidth of relayed connections between HIP Services in Conductor! An extra tab will appear in Conductor at HIPservice > Reporting > HIPrelay Stats for each HIPrelay. These statistics provide visibility into your network utilization with full-color, layered bandwidth graphs. They are also useful for troubleshooting underlay network relayed connection issues.

2.1.5 Service-specific CPU and memory reporting

For 2.1.5 and above, your HIP Services will report resource utilization more granularly, and you will be able to see this diagnostic information in **HIPswitch** > **Reporting** > **Graphs**.

2.1.5 Headless install for Windows HIPclient and HIPserver

You can now perform non-interactive installations of the Windows 7 HIPclient or HIPserver using Microsoft's System Center Configuration Manager (SCCM). Previous releases required manual acknowledgment by an administrator to complete the installation of an unsigned network tap (TAP) driver on Windows. We have patched the driver and obtained Microsoft certification, so this step is no longer necessary.

2.1.5 Tags public API

All basic tagging capabilities released in software version 2.1.4 are exposed in the public API. This includes the ability to index the tags, set or unset tags on taggable objects, such as devices, device groups, HIP Services, HIPservice groups, networks, and people. You can manage tags, retrieve various objects by tag, manage tag expirations, and perform other tag-based actions on several taggable objects at once. Advanced tag management, such as using tags in smart device group rules, or managing monitor event-actions that manipulate tags, will be added in a future release.

2.1.5 Custom CA alerts & public API

Though technically possible, it was difficult to use a non-Airwall CA at scale with your Conductor and Airwall Edge Services. Prior releases required you to manually copy/paste each CSR and cert from the Conductor GUI. Now you can automate the process using new public API calls. This enables a scriptable, scalable Conductor-centric workflow. Also, an admin alert is created in Conductor when custom CA certs are near expiration.

2.1.4 Airwall Agent for Android

With this release, the Airwall Agent is available for Android. Your Android devices can now natively connect to your Airwall overlay, giving them a trusted and verifiable connection wherever you are. Multiple profiles allow you to easily switch between different Airwall overlays as needed.

2.1.4 Improved Conductor UI Navigation

Several UI elements have been redone to improve navigation:

- Conductor settings are now accessed from the gear icon in the upper right corner of the UI.
- The logged in user profile, API docs, EULA, and sign-out are accessed from the user account icon in the upper right corner of the UI.
- Item names in many lists throughout the UI now actively link to properties pages and dialogs. This greatly simplifies navigation between related elements.

2.1.4 Tags

Tags provide flexible asset management in the Conductor. Devices, Device Groups, Airwall Gateways, Airwall Groups, Overlay Networks, and People can be tagged directly. The Tag information dialog allows you to **Navigate** directly to any tagged item, perform bulk **Actions** (Enable, Disable, or Untag tagged items), and edit **Properties**. Items can be tagged permanently or until you untag them. You can also set an expiration date, which will untag a component after a configurable period of time. You can create tags from the **Tags** page, access from the tag icon in the upper right corner of the UI.

You can also create tags inline while modifying an item's tag members by entering a new tag name and select colors for easy classification. Tags have been integrated into searching and filtering throughout Conductor.

Tags can be used in matching rules to greatly simplify Smart Device Groups. They can also be added to or removed from taggable items in Event Monitor Actions, which allows monitor results to affect overlay network policies. By using tags with these features, you can optimize your workflows. For example, you can create temporary network policies for specific devices, easily revoke policy directly from devices or HIPswitches without having to navigate to a network, and allow multiple admins to keep track of their assets in a single Conductor.

2.1.4 Relay Probes

An Airwall Gateway with this option selected periodically sends probe packets to all of its relays, and use the closest relay when initiating secure tunnels. This reduces the amount of network traffic used to build new tunnels, and allows auto-connect to be turned off. You can find this option in the **Advanced settings** section of a HIPswitch's settings page.

2.1.4 Conductor Diagnostics

Similar to diagnostics offered for Airwall Gateways, the Conductor now has a set of maintenance and diagnostic functions consolidated under the Diagnostics tab of the Settings page. These include Creation or Restoration of a DB Backup, downloading a Conductor support bundle, and viewing a Conductor diagnostic report. Network diagnostics allow you to generate a packet capture on the Conductor interface, ping, and traceroute.

2.1.3 The Airwall 75 Series

The Airwall 75, released with 2.1.3, is designed for medical devices, point of sale systems, and others like building automation controls. It securely connects and protects those endpoints across all networks with little to no change to existing infrastructure. The 75 plug and play design makes universal connectivity and segmentation simple, fast, and cost-effective.

2.1.3 Airwall Agent for Linux

With this release, the Airwall Agent is now available for Linux. Your Linux devices now can natively connect to your Airwall overlay, giving them a trusted and verifiable connection wherever you are. Multiple profiles allow you to easily switch between different Airwall overlays as needed.

2.1.3 New platform support for Microsoft Azure and Google Cloud

You can now create, manage, and retire Microsoft Azure and Google Cloud HIP Services directly from the Conductor UI.

2.1.3 Support for offline Conductor licensing

We have added support to allow Conductors without access to the public Internet to complete voucher and provisioning requests with our licensing and provisioning server. You can export a sync package, send it to Tempered Networks Support, and import a file containing your licenses back in to your Conductor from a drop-down on the **Settings** > **Licensing** tab.

2.1.3 New API token system and improved token management

We have updated the API to make tokens more secure. All API requests now require two headers:

- **X-API-Client-ID** is unique by user and can be found on your user preferences page
- **X-API-Token** is generated from your user preferences page. This token is secret, so if you lose it, you must generate a new one. Whenever you refresh your token, all previous tokens will be expired.

The client ID and a refreshed secret token may also be acquired via the API using basic authorization at `/api/v1/token/generate`. Please refer to the API documentation for details.

Note: The **X-Person-Email** and **X-Person-Token** headers are deprecated and no longer function.

2.1.3 New network creation wizard

New in this release is the ability to quickly create a hub-and-spoke or full mesh network using a simple, wizard-driven UI.

2.1.2 The HIPswitch 250 Series

The Airwall 250 Series is our newest hardware product and the industry's first identity-based industrial IoT gateway for Industrial Control Systems, OT, SCADA, and critical infrastructure. The Airwall 250 includes highly available uplinks over ethernet and up to two different cellular carriers, all actively monitored using fast failover and the ability to prioritize across both cellular and wired links. It also provides 8 x 1 Gbps and 4 x SFP (fiber or copper) with PoE, eliminating the need for ethernet switches and additional power sources. The HIPswitch 250 can also act as a HIPrelay, a feature introduced in version 2.0 of our software.

2.1.2 Airwall Agent for macOS and iOS

With this release, the Airwall Agent is now available for macOS and iOS. Your devices now can natively connect to your IDN overlay, giving them a trusted and verifiable connection wherever you are. Multiple profiles allow you to easily switch between different IDN overlays as needed. Additionally, integration with Airwall Relay gives you seamless and secure mobility for your computers running Apple's macOS and your devices running iOS.

2.1.2 Link Manager

Link Manager supports all cellular platforms, including our new Airwall 250 Series, providing uplink redundancy and intelligent monitoring for one wired and two cellular uplinks. Dynamic switching occurs based on which port provides the best performance. Default monitors can be customized with your own destinations.

2.1.2 Integration with AWS

You can now create, manage, and retire AWS Airwall Edge Services directly from the Conductor. After creating a template, you can easily create more HIP Services to function as HIPrelays or protect virtual machines in your VPCs.

2.1.2 HIP Invitations

Airwall Invitations, a new feature in 2.1, allows you to add mobile phones, tablets, and computers running a Airwall Agent or Airwall Server to your Airwall solution by sending the user an email containing an invitation. When the user accepts the invitation, the Conductor automatically takes care of all the steps to provision, license, manage, name, group, and create policy for the new Airwall Agent or Airwall Server without manual steps by the administrator. Airwall Invitations can be sent in bulk to entire organizations, and the Conductor will handle the rest.

2.1.2 Improved alerts and monitoring

In this release we added additional monitors, such as the **HTTP GET** monitor that allows you to parse web responses from devices in an overlay. Monitors have been expanded to support device groups and HIPservice groups. The event history graphs will now display frequently or recently triggered monitors.

2.1.2 Improved performance

We made significant performance improvements across the board for all platforms, with virtual Airwall Gateways and the Airwall 400 roughly doubling in performance.

Definitions of Key Terms

Before you get started, you may want to review our list of key terms and definitions you will find in our documentation relating to Tempered products and services.

Product, Technology and Service terms

Note: These terms are specific to Tempered products, technologies, or services and may have additional definitions or descriptions unique to Tempered.

HIP

Host Identity Protocol. The secure protocol that ties our products together.

IF-MAP/MAP/MAP2

Interface to Metadata Access Points. Airwall Edge Services use this client/server protocol to communicate with the Conductor, which provides authentication keys and communication policy to them.

Conductor

The physical, virtual, or cloud-based appliance that centrally manages all connected Airwall Edge Services and devices.

Airwall Edge Service

Any HIP-enabled hardware or software connected to the Conductor. A collective term for all Airwall Gateways, Airwall Agents, and Airwall Servers. Formerly known as HIPservices.

Airwall Gateway

A physical, virtual, or cloud-based appliance that provides overlay network connectivity to connected devices. Formerly known as HIPswitch.

Airwall Agent

Software program that allows people to connect to protected resources using their cell or laptop devices (available on Windows, macOS, iOS, and Android). Formerly known as HIPclient.

Airwall Server

Software program that allows people to connect to protected resources using their Windows or Linux Server. Formerly known as HIPserver.

Underlay

The Underlay is your existing Layer 2 networks, including the Internet if your Airwall Edge Services traverse it. Your Airwall Gateways and Conductor communicate with each other over this network.

Overlay

An Overlay is an Airwall secure network, where your devices and resources are protected by Airwall Gateways and accessed securely through Airwall Agents and Servers.

Terms related to our technology

Note: These terms are not specific to Tempered products, technologies, or services and have definitions or descriptions relating to networks and networking in general.

Microsegmentation

Compartmentalizing your network into isolated segments in which devices are only exposed to each other when they have a need to communicate.

Multihoming

Connecting a single device to multiple networks, physical and/or virtual.

Tunneling

Encapsulating network traffic in an encrypted connection between two points (e.g. a virtual private network).

Bump-in-the-Wire (BITW)

An antiquated term for a communications device introduced to a legacy system to enhance it. While we rarely use this terminology, it accurately describes our Airwall Gateway line of products, especially when used with legacy systems to enhance security.

Back-haul Interface (BHI)

An interface that carries traffic from a central network to the network's edge. Airwall Edge Services are considered a type of Back-haul Interface, carrying overlay traffic to and from protected devices.

IPsec

A secure network protocol stack for encrypting packets of data sent over an IPv4 network.

Encapsulating Security Payload (ESP)

An encryption protocol used by IPsec.

Legacy and deprecated terms

Note: Although no longer used, older white papers, web articles, and videos may use these terms. Internally, the product may refer to components using these terms as well, such as in log files, for example.

Asguard/Asguard Networks

Our previous company names. Sometimes you will see **ama**, which stands for **Asguard Management Appliance**, a previous internal name for the Conductor.

SimpleConnect

Previous term for the Conductor. Sometimes you will see **sc** as a prefix in log entries and exported files, meaning that they are related to the Conductor.

Endbox

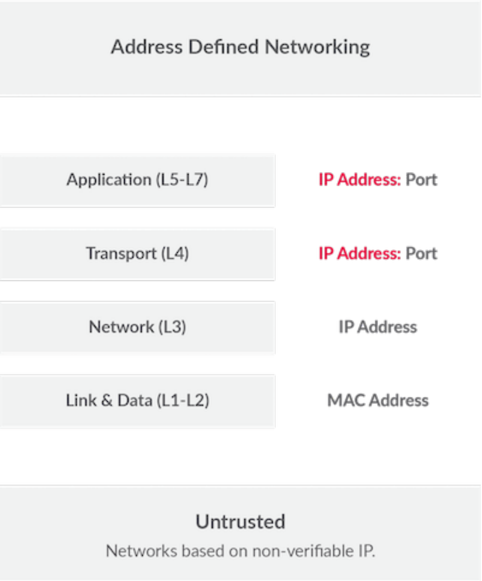
Previous term for an Airwall Edge Service. This term is still used internally, so you might see it in logs.

Host Identity Protocol (HIP)

HIP is an open standard that delivers a better approach to security, authentication, mobility, and resiliency for networks. The protocol has been under development for over 20 years in coordination with several Fortune 500 companies and standards bodies, before being officially approved in 2015 by the IETF. Tempered is the first company to commercially leverage the technology.

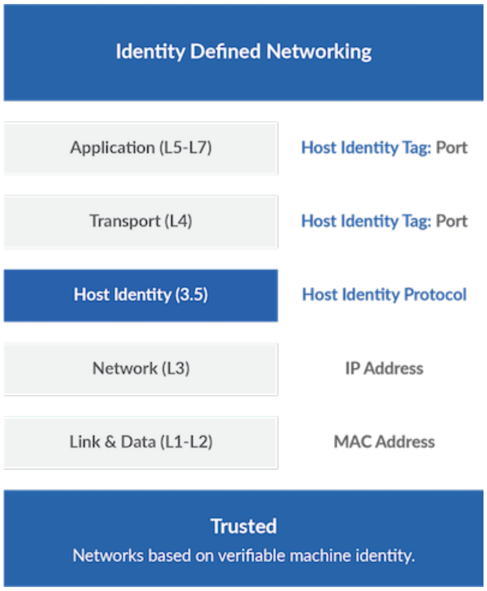
HIP separates the role of an IP address as both host identity and location within a network, such that hosts are instead identified using cryptographic identities in the form of public keys. We can then define device-to-device trust relationships based on the host identity instead of the IP address.

In a traditional networking model, referred to below as address-defined networking, routing is done via IP addresses. The upper layers of the standard networking framework, or stack, represent software that implements network services like encryption and connection management. The lower layers of the framework implement hardware-related functions like routing, addressing, and flow control.



In an identity-defined networking model, the HIP identity layer inserts itself in the stack between the network and transport layers. As a result, applications and transport protocols use a host identity tag instead of an IP address.

Each host is now identified on the network with a unique cryptographic identity, while the IP address is used only for location.



Identity Defined Networking

Application (L5-L7)	Host Identity Tag: Port
Transport (L4)	Host Identity Tag: Port
Host Identity (3.5)	Host Identity Protocol
Network (L3)	IP Address
Link & Data (L1-L2)	MAC Address

Trusted
Networks based on verifiable machine identity.

The Airwall Solution

The Airwall Solution makes your connected ‘things’ invisible. It eliminates network-based attacks, secures remote access at scale, and extends the life of existing infrastructure investments. It effectively reduces cyber risk and makes securing a corporate network less complex.

Airwall addresses the problems inherent in the existing solutions that tell you that you need more firewalls, VPNs, VLANs, ACLs, SSH keys, etc., but that you are never really secure.

The problems with TCP/IP

The root of the problems with the existing solutions lies within IP’s own shortcomings. TCP/IP was created with connectivity, not security, in mind. As the number of devices on a network increases, so too does the vulnerability to cyber attacks and the complexity of IP-based network security. The answer to these challenges is a trusted networking architecture model based on cryptographic identities.

Airwall offers a better way

The Airwall Solution is an infinitely better way to keep it all safe. It enables you to:

- Secure first, and connect later.
- Provide secure access and total invisibility at any scale, across any network.
- Secure your local datacenter and your global infrastructure with a solution that allows connections across both.
- Secure every endpoint in your network, with true micro-segmentation and secure remote access.

Make all of your things Invisible

Airwall allows only trusted and cryptographically-identified “things” to connect, creating a network that is more secure and flexible than the traditional TCP/IP model. The network just doesn't respond to any non-trusted sources, so all of your "things" are protected.

Easily deployed

The Airwall Solution enables you to easily deploy and extend a unified, trust-based, and encrypted network. Micro, macro, and cross-region segmentation, as well as global IP mobility are simple to set up. Deploying and maintaining intra-cloud (region to region), cloud-to-cloud, and cloud-to-data center cryptographic trust-based communications becomes simple, verifiable, and secure.

Airwall works on Existing Networks

Airwall requires little to no modification of the underlying network or security infrastructure. It provides a simple, policy-based configuration of devices or groups of devices that are explicitly trusted based on allowlisting. This trust, based on unique cryptographic identities, determines what systems or machines can initiate and establish communication before any data is exchanged.

The Airwall Solution is set up using the **Airwall Conductor**, an intuitive, visual, point-and-click management and orchestration engine. The Conductor easily manages a network, regardless of how many devices are part of it. Our Airwall Edge Services are software products delivered in different forms to support our commitment to securing any device, anywhere.

Built on the Host Identity Protocol (HIP)

The Tempered Airwall Solution uses **Host Identity Protocol (HIP)**, an open-standard network security protocol that provides provable host identities. This technology has been recognized by the **Internet Engineering Task Force (IETF)** as the next possible major improvement in IP architecture, making HIP a true paradigm shift in networking that solves the fundamental security flaws of TCP/IP. HIP was formally ratified by the IETF in 2015, capping 15 years of successful development and deployment in coordination with several major companies (Boeing, Verizon, Nokia) and standards bodies (Trusted Computing Group, IEEE 802).

Instead of using the flawed dual function of the IP address, HIP assigns identity with 2048-bit RSA public keys and assigns location with the original IP address. These identities are permanent, location-independent cryptographic identities that are connected to machines or networks, enabling security by default with verifiable authentication, authorization, and host-to-host encryption.

Within TCP/IP, there are two globally-deployed namespaces that allow the Airwall Solution to uniquely identify a host or service: IP addresses and DNS names. However, due to the fundamental flaws of TCP/IP, both namespaces are problematic for networks. HIP introduces a third option for namespaces: the **Host Identity Namespace (HIN)**. The HIN is compatible with the current namespaces, and provides global IP mobility and security policies based on unique cryptographic identities. It overcomes many of the fragile and costly challenges of traditional TCP/IP networking.

How to get support

You can often find answers to your questions in Airwall helpthe guide, or by logging in to your **Support** account and searching the knowledge base articles. If you still cannot find what you are looking for, you can contact support for help.

Note: You must have a current support contract with Tempered to open a support ticket.

There are several ways to contact support.

Open a case on the Tempered Support Web Portal

1. Go to https://www.tempered.io/support/supportReq.html.
2. Sign in using your support account log in.
3. Click + or **New**.
4. Fill in the name and contact information.
5. Provide the **Information to Include** listed below.
6. Attach the support bundle from the affected devices.
7. For network issues, attach a packet capture.

Contact Tempered Support via email

1. Send an email message to Customer Success.
2. Provide the **Information to Include** listed below.
3. Attach your support bundle to the email.
4. For network issues, attach a packet capture.

Information to Include

Provide the following information when you open a case with Tempered Support:

- A full description of the issue, including the following details:
  - The symptoms of the issue, including a brief description of all systems applicable to the configuration.
  - The approximate time the issue first occurred.
  - The number of times the issue has recurred.
  - Any error output provided by the system.
  - Steps to reproduce the issue.
  - Any changes you made to the system close to when the issue first occurred.
  - Any steps you've taken to resolve the issue.
  - Whether this is a new implementation.
  - How many data centers and devices are applicable to the configuration.
  - Which devices are affected by the issue.
- A description of the impact the issue is having on your site.
- Days and times you are available to work on the issue, and any alternative contacts that can work on the issue if you are not available.

Get a Support Bundle

The Support Bundle is the technical information about the device. To best answer support issues, Tempered Support needs the Support Bundle from the Conductor and Support Bundles from any Airwall Gateway, Airwall Agent, and/or Airwall Server that is part of the issue you are reporting. For more assistance, see Create a support bundle for a Conductor on page 481.

Get a Packet capture

If the issue involves the network, perform a packet capture while the issue is occurring. Provide this packet capture when you open the case. For more assistance, see Do a packet capture for an Airwall Gateway on page 482.

Copyrights

This source code and the methodology disclosed by it include proprietary and confidential information belonging to Tempered and its licensors ("Source Code"). The Source Code may not be copied, modified, or distributed without the prior express written permission of Tempered.

By using the Source Code, You agree to be bound by these terms and conditions of use. You acknowledge that this is only a limited, nonexclusive, non-transferable license. Tempered and its licensors remain the owners of all titles, rights, and interests in the Source Code. Further, use of the Source Code is governed by the terms and conditions of Your license agreement with Tempered regarding the Source Code, which license agreement is incorporated herein by reference.

Use of the Source Code is permitted to You only as a Partner of Tempered under written agreement and for no other purpose than the partnered work You are doing with Tempered. The Source Code may not be disclosed to or used by anyone other than Your employees or contractors working on Tempered product development projects. You may not disclose, assign, sublicense, lease, or in any other way transfer the Source Code to any third party without the prior express written consent of Tempered. Any product developed using the Source Code may be distributed, displayed, licensed, sold, or used in object code format only and as specified in a written license with Tempered permitting such distribution, display, license, sale or use.

Tempered has the right to terminate this License Agreement and Your right to use the Source Code upon any material breach of the License Agreement by You.

You agree to defend and indemnify Tempered and to hold Tempered harmless from all claims, losses,damages, complaints, or expenses connected with or resulting from Your business operations relating to use of the Source Code.

THE SOURCE CODE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESSOR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE WARRANTIES OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM,DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOURCE CODE OR THE USE OR OTHER DEALINGS IN THE SOURCE CODE.

Host Identity Protocol

Copyright © 2012-2022 Tempered, Inc. All Rights Reserved.

Tempered, Inc. ("Tempered"), hereby grants worldwide permission, free of charge and without a signed licensing agreement, for the duration of the copyright, to any person obtaining a copy of this software and associated documentation files ("The Software"), the right to deal in The Software without restriction, including, without limitation, the right to use, copy, modify, merge, publish, distribute,sublicense, and/or sell copies of The Software, to make, publish, distribute, and/or sell derivative works based on The Software, and to permit persons to whom The Software is furnished to do so, subject to the following conditions:

The above copyright notice and this Permission Notice shall be included in all copies or substantial portions of The Software and in all modifications and distributions of The Software, including derivative works based on The Software. Neither the names of Tempered nor the Authors, nor any of their trademarks or service marks, may be used to endorse products derived from The Software without the express prior permission of Tempered.

Except as expressly stated herein, nothing in this Permission Notice grants any license to Tempered's trademarks, service marks, copyrights, patents, trade secrets, or other intellectual property. No license is granted to the trademarks of Tempered even if such marks are included in The Software. Nothing in this Permission Notice shall be interpreted to prohibit Tempered from licensing under terms different from this Permission Notice any Original Work that Tempered otherwise would have a right to license.

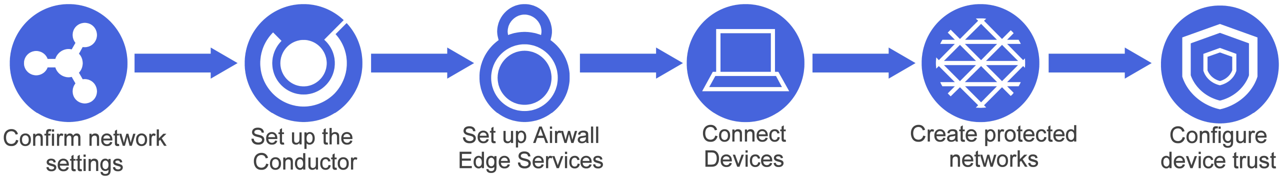
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM,DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. THE AUTHORS AND COPYRIGHT HOLDERS HAVE NO OBLIGATION UNDER THIS PERMISSION NOTICE TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS TO THE SOFTWARE.

Deploy an Airwall secure network

Deploy, Install, Configure, License

Building an Airwall Solution requires a minimum of three components: An Airwall Conductor and two or more Airwall Edge Services with devices attached behind them. You can manage these Airwall Edge Services and their attached devices from the Conductor dashboard. The Airwall Edge Services create a zero-trust virtual protected network. The Conductor acts as a centralized management dashboard for the network, pushing policy and trust information to the Airwall Edge Services. Every Airwall Edge Service within the protected network knows the network layer and state of its peers, and every peer maintains Identity-Based Routing (IDR) tables.

A typical deployment requires the following steps:



Note: If you are installing a physical Conductor or Airwall Edge Service, make sure you are familiar with your model, including the variety of power options and physical installation steps before you begin your deployment. Refer to the Platform or Install Guide included with your hardware.

Tip: For additional information about the Airwall Solution, see the What makes up an Airwall secure network? on page 141 in the Get Started with the Airwall Solution on page 140 section.

Tip: For additional information about the Airwall Solution, see **What makes up an Airwall Secure Network** in the **Get Started** section of our online documentation.

Deployment Checklist

A checklist for deploying the Airwall Solution

Also check out:

- A roadmap to topics to help you deploy: Deployment Roadmap on page 184
- The Airshell command setup-ui at Airshell (airsh) Command Reference on page 362
- Startup tutorials for the Conductor at Get Started using Conductor Help and Tutorials on page 140

A typical deployment requires the following steps:

1. Plan your deployment
2. Confirm your Network Settings on page 187
3. Deploy and Configure a Conductor on page 197
4. Deploy and Configure Airwall Edge Services on page 274
   a) Set up Airwall Gateways on page 274
   b) Connect People's Devices to your Airwall secure network on page 64
   c) Configure Airwall Edge Service Settings on page 359
   d) License a Conductor and Airwall Edge Services on page 191
5. Connect and Configure Devices on page 414
6. Create and Manage an Overlay (Protected) Network on page 418
7. Configure Device Trust on page 427

If you have special configuration needs, see Configure Advanced Airwall Edge Service Options on page 384 for different options on how to configure Airwall Edge Services.

Deployment Roadmap

A roadmap to the most helpful topics for getting the Airwall Solution up and running on your network.

Get Familiar with the Airwall Solution

This content helps you understand the components of the Airwall Solution and help you get started.

- What makes up an Airwall secure network? on page 141
- Definitions of Key Terms on page 177

Prepare to Deploy the Airwall Solution

Make sure your network is ready for deployment.

- Confirm your Network Settings on page 187
- Review the Software Downloads and Release Notes on page 514
- Create topics for Capacity Planning, etc?

Deploy and Configure your Conductor

If you run into issues, see Diagnostics and Troubleshooting on page 477 or Submit a support request.

Deploy a Conductor

The Conductor is what you use to orchestrate your zero-trust network, including the resources you are protecting and who can access them.

- Get Started using Conductor Help and Tutorials on page 140
- The Conductor Dashboard on page 32
- Conductor Icon Reference on page 35

- Deploy a Conductor on page 197
- 1. Deploy a Conductor in VMware ESX/ESXi on page 230
  2. Deploy a Conductor on Amazon Web Services (AWS) on page 205
  3. Deploy a Conductor on Microsoft Azure on page 211
  4. Manually deploy a Conductor on the Google Cloud Platform (GCP) on page 219
  5. Deploy a Physical Conductor on page 199

Log in and Configure the Conductor

- Log in and Configure the Conductor on page 201
- Best Practices for Conductor Configuration on page 235

Add Airwall Edge Service Licenses

Add Airwall Edge Service Licenses to the Conductor on page 192

License a Conductor and Airwall Edge Services

- License a Conductor and Airwall Edge Services on page 191
- **If you are deploying in an Isolated (dark) environment**, here's how to license your Conductor and Airwall Edge Services: License a Conductor and Airwall Edge Services in an Isolated Environment on page 196

Deploy and Configure Airwall Gateways

If you run into issues, see Diagnostics and Troubleshooting

Deploy and Configure Airwall Edge Services

Set up Airwall Gateways

Set up Physical Airwall Gateways

Set up a physical Airwall Gateways

- Set up 75-series hardware
- Set up 110-series hardware
- Set up 150-series Hardware
- Set up 250-series hardware
- Set up 500-series hardware (either Conductor or Airwall Gateway)
- Set up Advantech hardware - Latest Firmware and Software
- Other helpful topics:
  - Connect to the console port using Windows
  - Connect to the console port using Linux or macOS
  - Airwall Gateway Airshell console commands - airsh
  - Configure an Airwall Gateway with airsh Setup Wizard
  - Deploy Airwall Gateways using Activation Codes

Set up Virtual Airwall Gateways

If you run into issues, see Diagnostics and Troubleshooting

Set up virtual Airwall Gateways

- Set up a virtual Airwall Gateway in VMware ESX/ ESXi
- Set up a virtual Airwall Gateway in Microsoft Hyper-V
- COMING SOON- KVM?
- COMING SOON-VirtualBox?

Set up Cloud Airwall Gateways

If you run into issues, see Diagnostics and Troubleshooting

Set up cloud Airwall Gateways

- Set up an Amazon Web Services (AWS) Airwall gateway
- Set up a Microsoft Azure Airwall gateway
- Set up a Google Cloud Platform (GCP) Airwall gateway
- Alibaba Cloud – Set up an Airwall Gateway on page 315

Add the Devices you want to Protect

- Connect and Configure Devices on page 414
- Add devices to the Conductor on page 414
  - Use device discovery on page 414
    - Enable passive device discovery on page 414
    - Detect devices manually on page 414
  - Import devices using a .csv file on page 415
    - CSV Template
  - Add devices manually on page 416

Create and Configure your Protected Networks (Overlays) and Trust

To create a protected network in your Airwall Solution, you create an overlay (a secure network), add protected devices to it, and then set up the trust policy between devices and Airwall Edge Services (Airwall Gatewaysand Airwall Agents and Servers) on the protected network.

- Create and Manage an Overlay (Protected) Network
- Configure Airwall Relay rules
- Set an Overlay to Automatically Manage Relay Rules
- Set up device trust

Connect People’s Devices to yourAirwall secure network

For people to connect to your Airwall secure network and access resources, they need to install the Airwall Agent or Server software for their device and you’ll need to grant them access. The easiest way to do that is with Airwall Invitations.

Invite People to Join your Airwall secure network

Here are two ways to use Airwall Invitations to invite people and grant them access

- Send Airwall Invitations
- Walkthrough - Onboard people to your Airwall secure network with User Authentication

Manually Add People’s devices

You can also have users install and connect manually. They first install the Airwall Agent or Server on the computer or mobile device they are going to use to connect, and then request to connect to your network. An Airwall secure network administrator then grants these devices access, manages them, and then adds them to the overlays and sets up trust policy.

Install Airwall Agents and Servers

Point the people who you want to connect to these topics to install an Airwall Agent or Server:

- Operating system requirements for Airwall Agents and Servers on page 7
- Install an Airwall Agent or Server on page 6

Connect Airwall Agents and Servers to your Airwall secure network

Then point the people who have installed an Airwall Agent or Server to these topics to connect to your Conductor:

- Link my Airwall Agent or Server to an Airwall secure network on page 14
    - I have an Airwall invitation
    - I have an Activation code
    - I have an “Finish Setting up my account” email
    - I want to request to connect

Grant Access and Set Trust Policy for People's Devices

You can then grant the requests and set what resources the people connecting to your Airwall secure network can access.

- Allow an Airwall Agent or Server to access your Airwall secure network
- Configure Device Trust on page 427

Show or Hide Conductor Setup progress bar

You can show or hide the Conductor Setup progress bar on the Dashboard in your user preferences.

1. Log in to the Conductor with your existing password.
2. Select the profile icon 👤, and then select **Preferences**.
3. Scroll down to **Show progress on dashboard**, and toggle it on or off.

For more information on the Conductor tutorials, see Get Started using Conductor Help and Tutorials on page 140.

Confirm your Network Settings

Check that your network is set up to start deploying the Airwall Solution.

Your existing network is the underlay network, made up of your existing private networks and the Internet. It is any network that you connect an Airwall Edge Service to, and any network used to communicate between other Airwall Edge Services in your Airwall deployment. For Airwall to work correctly, all components must be able to communicate with each other from where they are installed.

The Conductor

The Conductor is the central management dashboard for all Airwall Edge Services. It tells the Airwall Edge Services how to contact one another and enforces policies on the protected network – allowing or preventing communication between devices. It also manages licensing and provides diagnostic tools.

Your Conductor can be either virtual or physical and can be configured in a high-availability (HA) pair. It passes no protected network traffic and does not communicate with the HIP protocol.

The Conductor must have at least two network interfaces. The recommended configuration is as follows:

Port 1	Connect to the Internet, either directly or with port forwarding.
Port 2	Connect to your Local Area Network (underlay)

For the Conductor to work, it must be able to listen on the following ports:

TCP 8096 (MAP)	This is the port in which Airwall Edge Services communicate with the Conductor.
TCP 443 (HTTPS)	This is the port in which the Conductor Management can be accessed.

Airwall Edge Services

An Airwall Edge Service carries out or facilitates the connectivity between two connecting devices.

An Airwall Gateway is a network appliance that allows Ethernet devices to be added to the protected network (Overlay). It connects to a Conductor via a Metadata Access Point (MAP) for policy and peer addresses, and it connects to peer Airwall Edge Services to establish secure tunnels between locations.

An Airwall Gateway can be either virtual or physical and can be configured in an HA pair. It passes traffic between devices over a HIP tunnel.

An Airwall Gateway must have at least two network interfaces. The recommended configuration is as follows:

Port 1	Connect to the Local Area Network (Underlay). Must be able to reach the Conductor and other Airwall Edge Services.
Port 2	Protected Device Network (Overlay). Must be able to reach the devices to add to the overlay.

It is possible to connect Ports 1 & 2 to the same network and provide existing device access to the Overlay, without isolating the protected devices inside of a separate network segment.

For the Airwall Gateway to work, it must have outbound connectivity on the following ports:

TCP 8096 (MAP)	Must have outbound connectivity to MAP to the Conductor.
UDP 10500 (HIP)	Must have outbound connectivity to HIP and to any other Airwall Edge Service it is a must to communicate with.

At least one Airwall Gateway on one end of a tunnel must also be able to listen on the following port:

UDP 10500 (HIP)	Must have outbound connectivity to HIP and to any other Airwall Edge Service it is a must to communicate with.

Alternately, if Airwall Edge Services cannot be configured to listen for incoming connections, you can employ an Airwall Relay to get around a network address translation (NAT).

Airwall Relays

An Airwall Relay is, typically, a virtual cloud-hosted appliance, running the Airwall Gateway 300v VM. It is able to listen for HIP traffic, allowing Airwall Gateways behind firewalls and routers to establish a tunnel between each other even when NATed.

For the Airwall Relay to work, it must have outbound connectivity on the following ports:

TCP 8096 (MAP)	Must have outbound connectivity to MAP to the Conductor.

UDP 10500 (HIP)	Must have outbound connectivity to HIP and to any other Airwall Edge Service it is a must to communicate with.

It must also be able to listen on the following port:

UDP 10500 (HIP)	This is the port, in which Airwall Edge Services communicate with the Conductor.

Airwall Relays are still considered a type of Airwall Edge Service, but they serve a special role. Any Airwall Gateway - physical or virtual - can be turned into an Airwall Relay. Once configured as an Airwall Relay, it is not advisable to add any devices to it, but instead use it exclusively to bridge Airwall Edge Services that are not able to listen for incoming connections.

Changing network ports

You can change the MAP and HIP ports from their defaults of 8096 and 10500 in the Conductor. This will change the settings for all Airwall Gateways connected to that Conductor.

These settings rarely need to be adjusted. When they are, it is either to get around some immutable firewall settings or to add extra security by using atypical ports.

Note: If you change the MAP port, you will need to manually reconfigure all Airwall Edge Services to point to the Conductor with the new port. This might involve traveling to remote sites and putting devices into diagnostic mode, so adjust this setting carefully.

If you change the Airwall Edge Service port, the change takes effect on all Airwall Edge Services connected to the Conductor, so make certain that they have the proper outbound connectivity and port forwarding configured before adjusting this setting.

To change the default ports:

1. In the Conductor, go to **Settings**.
2. Find the **Advanced** section near the bottom of the **Settings** page. Next to **Global HIPservice settings**, click **Edit Settings**.
3. Under **Port settings**, change the default ports, and click **Save**.

HIP and MAP Diagrams

Below are some diagrams illustrating successful and unsuccessful MAP and HIP configurations:

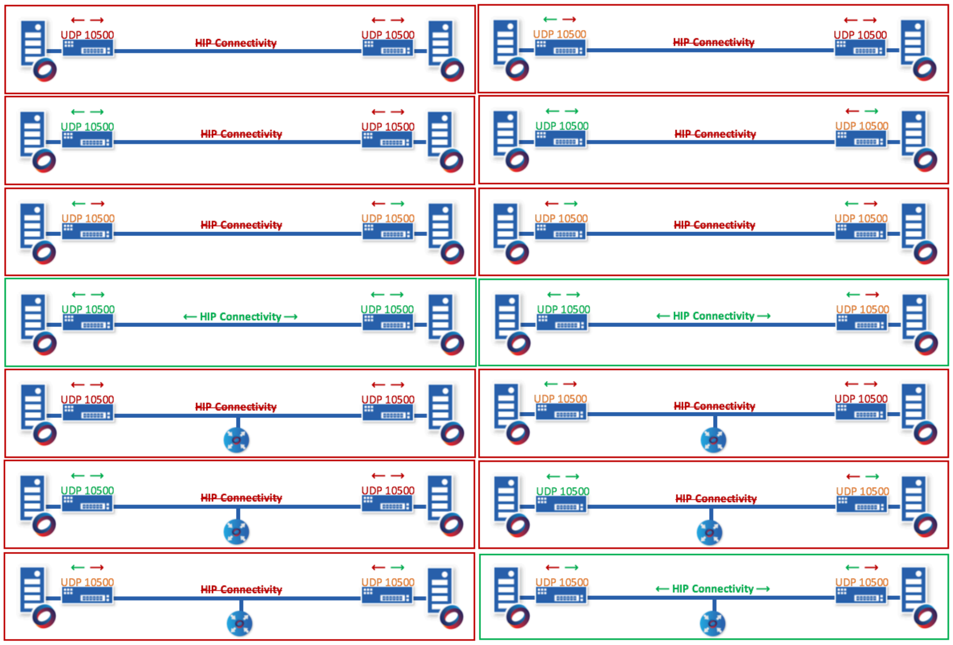
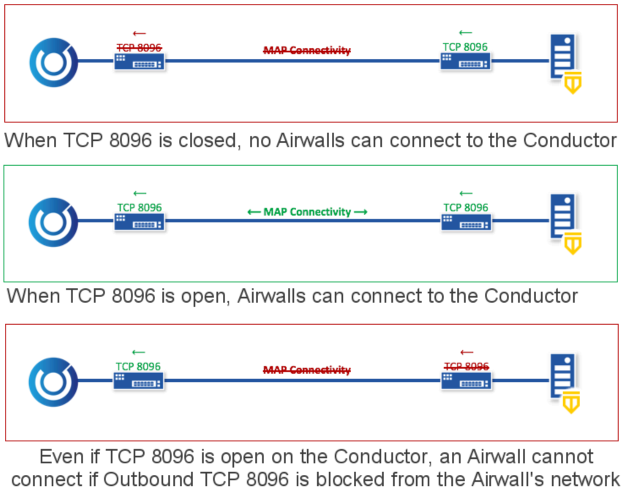


Figure 3: HIP configurations



When TCP 8096 is closed, no Airwalls can connect to the Conductor

When TCP 8096 is open, Airwalls can connect to the Conductor

Even if TCP 8096 is open on the Conductor, an Airwall cannot connect if Outbound TCP 8096 is blocked from the Airwall's network

Figure 4: MAP configurations

Check Your Underlay Settings

Check the following settings to confirm they are set for the new ports:

Firewalls

If a firewall is enabled between the Conductor and Airwall Edge Services in the solution, you must open the required firewall ports.

DHCP and DNS

If you prefer to configure your Conductor with a hostname or assign Airwall Edge Services IP addresses using DHCP, confirm that the underlay's DHCP and DNS settings are configured to support it.

Private Network Conductor

If the Conductor is located in a private network, either a firewall or router must provide a static public IP

	address so the Conductor can be reached by Airwall Edge Services outside the private network.
Private Network Airwall Gateway	If Airwall Edge Services located in a private network need to be accessed by Airwall Gateways outside the private network, a firewall or router must provide a static public IP address so the Airwall Edge Services can communicate.

License a Conductor and Airwall Edge Services

Everything you need to know about licensing your Conductor and Airwall Edge Services.

How Airwall Licensing Works

How licensing works in your Airwall Solution.

Tempered requires a license for each Conductor and Airwall Edge Service you have in use. Certain configurations also require add-on licenses, such as configuring an Airwall Gateway as an Airwall Relay.

When you purchase licenses, you receive a voucher code that allows you to apply your purchased licenses to a Conductor, or to Airwall Edge Services in a Conductor. The Conductor automatically consolidates licensing vouchers.

There is a significant difference between Conductor licenses and Airwall Edge Services licenses -- Conductor licenses are not transferrable, while Airwall Edge Service licenses are. More specifically:

- Conductor licenses ***cannot*** be reused or transferred once you've used it to license a Conductor.
- Airwall Edge Services licenses ***can*** be reused and are transferrable by type, and across Conductors. Some examples:
    - In a Conductor, you can delete a license from one Airwall Gateway-150 by revoking it and reassign the license to a different Airwall Gateway-150.
    - You ***cannot*** transfer a license from one type of Airwall Edge Service to another type.

You must have enough licenses available in your Conductor before you can provision Airwall Edge Services. For a list of the Airwall Edge Service licenses you have available, see the **Licensing** tab under Conductor **Settings**.

To purchase new or renew expired licenses, contact sales@tempered.io.

For how-to instructions on licensing and transferring licensing, see these topics:

- **License your Conductor,** see the **License and Provisioning** section in Deploy a Physical Conductor. Licensing and provisioning is the same for physical and virtual Conductors.
- License Airwall Edge Services, see Provision and License Airwall Edge Services on page 193.
- View your Licenses in Conductor, see View Licenses in Conductor on page 192.
- Transfer a License to Another Airwall Edge Service, see Transfer a license to another Airwall Edge Service on page 196.
- License an Isolated Conductor and Airwall Edge Services, see License a Conductor and Airwall Edge Services in an Isolated Environment on page 196.

License and Provision a Conductor (v2.2.8 and earlier)

To get a Conductor up and running, you need license and provision it. You need your licensing voucher to complete these steps.

Supported Versions	Conductor v2.2.8 and earlier

Note: For v2.2.10 and later, licensing and provisioning is included in the Initial Conductor configuration wizard. Start at Log in and Configure the Conductor on page 201.

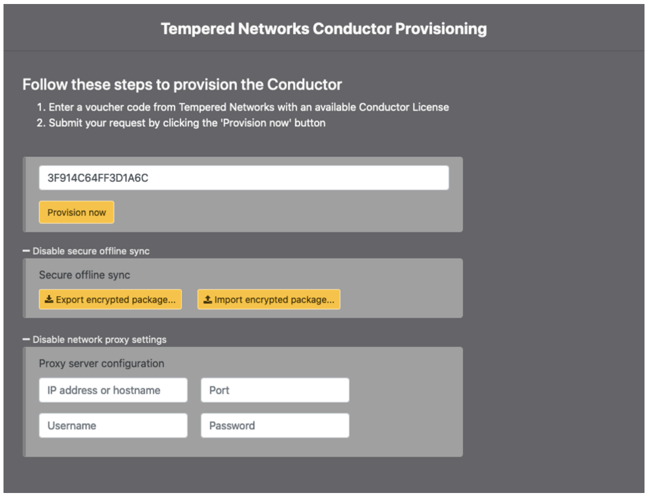
In v2.2.8 and earlier, you license the Conductor, and then Log in and Configure the Conductor on page 201.

1. If you have a physical Conductor, apply power to it, and connect a computer to Port 1 on the Conductor hardware using an Ethernet cable. Refer to your unit's Platform Guide for specific instructions.

2. In a web browser:

   - **Physical Conductor** – go to: `https://192.168.56.2`
   - **Cloud Conductor** – Click the link in your order email, or go to the public IP you set up when creating your Conductor.

   The Conductor **Provisioning** page opens so you can license your Conductor.



Tempered Networks Conductor Provisioning

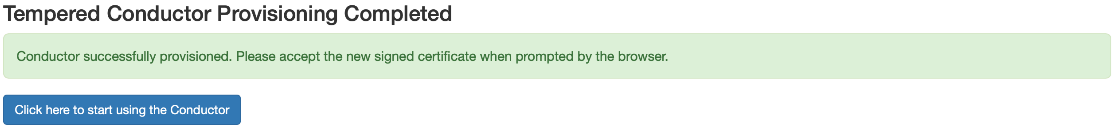
Follow these steps to provision the Conductor

1. Enter a voucher code from Tempered Networks with an available Conductor License
2. Submit your request by clicking the 'Provision now' button

3F914C64FF3D1A6C

Provision now
− Disable secure offline sync
Secure offline sync
Export encrypted package...
Import encrypted package...
− Disable network proxy settings
Proxy server configuration
IP address or hostname
Port
Username
Password

3. If you have a proxy server between your Conductor and the Tempered licensing server, under **Disable network proxy settings**, configure proxy server settings to allow your Conductor to reach the licensing server.
4. If you are licensing an isolated (dark) Conductor, you will use the **Disable secure offline sync** section. For more details, see License a Conductor and Airwall Edge Services in an Isolated Environment on page 196.
5. In the **Voucher code** box, enter the voucher code you received from Tempered.
6. Click **Provision now**. It takes a moment to finish applying the voucher. Once complete, you should see the following:



Tempered Conductor Provisioning Completed

Conductor successfully provisioned. Please accept the new signed certificate when prompted by the browser.

7. Select **Click here to start using the** Conductor.
8. Log in and Configure the Conductor on page 201.

Add Airwall Edge Service Licenses to the Conductor

The first step in licensing Airwall Edge Services is to add your licensing vouchers to the Conductor.

To add Airwall Edge Service licenses:

1. In Conductor, open **Settings**, and go to the **Licensing** tab.
2. Click **Enter Voucher**.
3. Type or paste your Voucher code, and click **Enter**. The licenses are added to your pool of licenses on the **Licensing** page.

Note: The Conductor automatically consolidates licensing vouchers.

View Licenses in Conductor

See what licenses you have available in the Conductor.

Note: Only Airwall Edge Service licenses are shown in the Conductor. Your Conductor license is not shown.

Note: The Conductor automatically consolidates licensing vouchers.

1. In Conductor, open **Settings**, and go to the **Licensing** tab.
2. Under **Licenses**, you can see the Airwall Edge Services licenses you have, and how many are in use.
3. Select a specific Airwall Edge Service license if you want to view your license count, type, and expiration date.

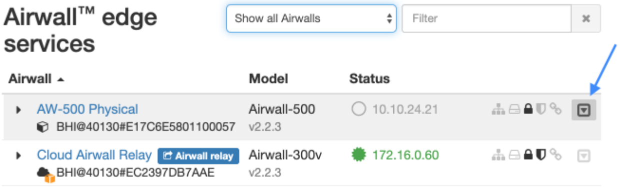
Provision and License Airwall Edge Services

How to provision and license Airwall Edge Services. You need to add Airwall Edge Services licenses to the Conductor before you can provision and license Airwall Edge Services.

1. In Conductor, open **Settings**, and go to the **Licensing** page.
2. If you have a license voucher, Add Airwall Edge Service Licenses to the Conductor on page 192. If you don't have a license voucher, contact sales@tempered.io to get one before continuing.
3. Install the Airwall Edge Services you want to license and connect them to the Conductor. For more information, see Deploy and Configure Airwall Edge Services on page 274 and Connect Airwall Gateways to the Conductor on page 292.
4. Under **Provisioning Requests**, select the check boxes for the Airwall Edge Services you want to provision, and under the **Actions** dropdown, click **Grant Request** to provision your Airwall Edge Services. They should reconnect to the Conductor and appear in your Airwall Edge Services list as unmanaged.

   Note: You can also grant provisioning requests from the **Provisioning** tab on the Dashboard.

5. On pre 2.2x Conductors, click **Sync**.
6. On the Conductor dashboard, click the **Show all Airwalls** box and filter the Airwall Edge Services by unmanaged.
7. In the row for the Airwall Edge Service you want to license, in the far right column, click the arrow to open the drop down menu, and select **Manage Airwalls**.



Airwall ▴	Model	Status
AW-500 Physical BHI@40130#E17C6E5801100057	Airwall-500 v2.2.3	○ 10.10.24.21
Cloud Airwall Relay Airwall relay BHI@40130#EC2397DB7AAE	Airwall-300v v2.2.3	● 172.16.0.60

Provision Airwall Gateways using Activation Codes

If you are deploying Airwall Gateways, you can use Activation codes to quickly set up and provision them using the console and `airsh`.

When you deploy Airwall Gateways using activation codes, they are automatically managed in the Conductor as they connect, and put into any **Airwall groups** you specified when creating the activation codes.

Note: Console access is required to input the activation code on Airwall Gateways. Some cloud providers do not provide console access to their servers (notably AWS), so you will need to provision them in a different way.

Before you begin

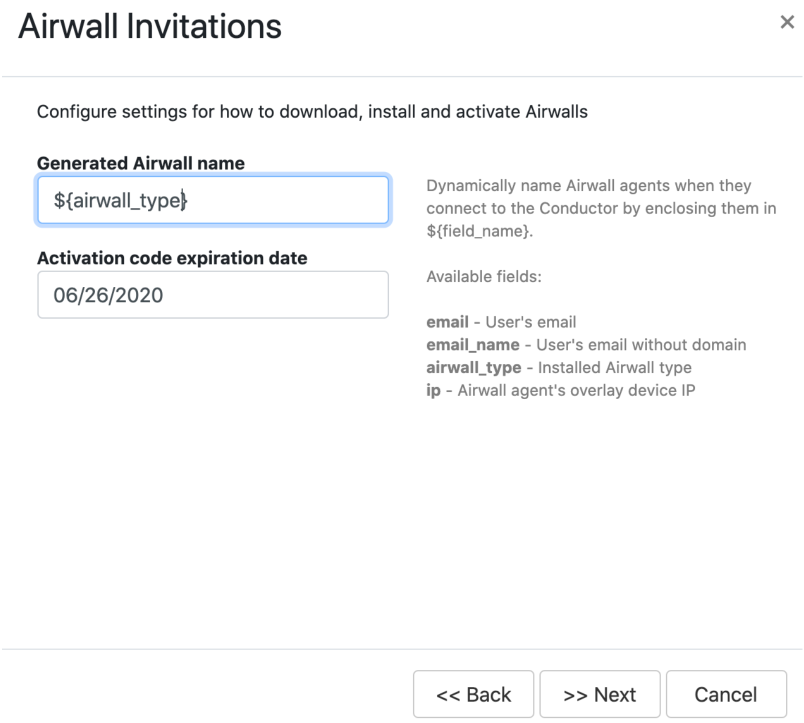
- Make sure the Airwall Gateways you are using can be accessed using the console. If you do not have console access, you need to deploy them in a different way. See License and Provision a Conductor (v2.2.8 and earlier) on page 191.
- Set up **Airwall groups** for the deployed Airwall Gateways.
- Set up any tags you'd like to use for the deployed Airwall Gateways.
- Determine how many Airwall Gateways you want to deploy, and how many are in each group. Go through this procedure for each group of Airwall Gateways.

To deploy Airwall Gateways using activation codes, you need to:

1. Create the activation codes
2. Use the console to apply the activation codes to the Airwall Gateways.
3. License the Airwall Gateways as described in License and Provision a Conductor (v2.2.8 and earlier) on page 191.

Create Activation Codes

1. In Conductor, go to **Airwalls**, and open **Airwall Invitations**.
2. Click **Create Airwall Invitations**.
3. On the **Airwall Invitations** page, select **Download activation codes and distribute them manually** , and enter how many Airwall Gateways are in this group. Click **Next**.
4. Select how the Airwall Gateways are named as they connect to the Conductor. Click in the **Generated Airwall name** box for help with how to dynamically create names.



Airwall Invitations

Configure settings for how to download, install and activate Airwalls

Generated Airwall name: ${airwall_type}

Activation code expiration date: 06/26/2020

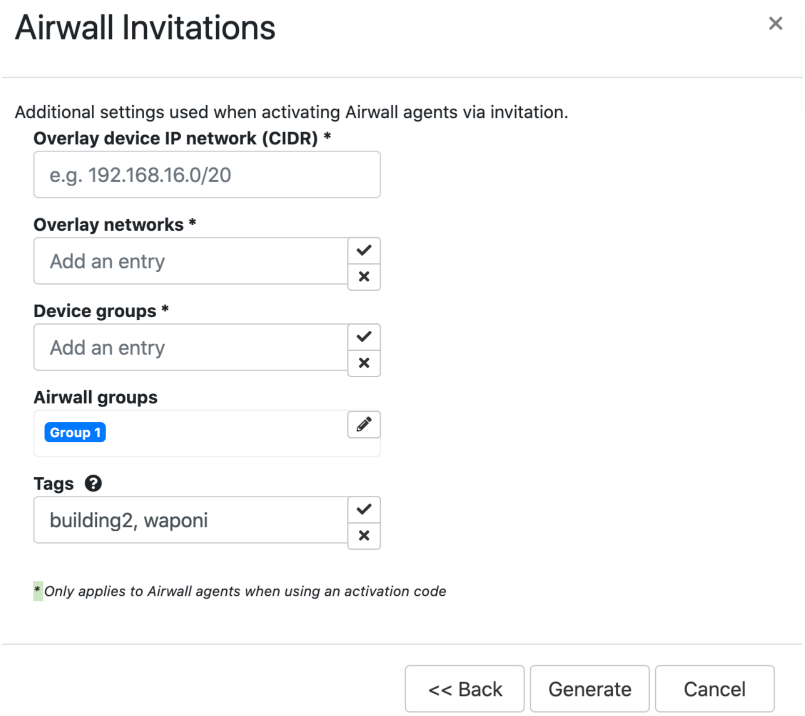
Dynamically name Airwall agents when they connect to the Conductor by enclosing them in ${field_name}.

Available fields:

email - User's email
email_name - User's email without domain
airwall_type - Installed Airwall type
ip - Airwall agent's overlay device IP

5. Change the **Activation code expiration date**, if needed, and select **Next**.
6. On the **Additional settings** page, select the Airwall groups and tags you want to apply to this group of Airwall Gateways.

   Note: You can skip the other options, as they are forAirwall Agents and Servers only.



Airwall Invitations

Additional settings used when activating Airwall agents via invitation.

Overlay device IP network (CIDR) *

e.g. 192.168.16.0/20

Overlay networks *

Add an entry

Device groups *

Add an entry

Airwall groups

Group 1

Tags

building2, waponi

* *Only applies to Airwall agents when using an activation code*

7. Click **Generate**.
8. Copy or download the activation codes. If you download the codes, the text file includes a summary of the options you've chosen for this group of activation codes.

```
Configuration

Profile name:
Conductor hostname or IP: cond.example.com
Generated Airwall name: ${airwall_type}-${ip}-group1
Activation code expiration date: 06/19/2020
Overlay device IP network (CIDR): undefined
Overlay networks:
Device groups:
Airwall groups: Group 1
Tags: building2, waponi

Activation codes

702d2fce3wee
8z130f85eed9
99508e9090qc
```

You're now ready to provision Airwall Gateways using these activation codes.

Deploy Airwall Gateways using Activation Codes

1. Plug in the Airwall Gateways you want to provision, and connect them to a network where they can reach the Conductor.
2. For physical Airwall Gateways, connect your laptop using the console port. For details, see Connecting to the console port on an Airwall Gateway on page 297. For console access on your cloud and virtual gateways, consult your cloud or virtual provider.
3. At the console, log in with name: `airsh`, and password: `airsh`
4. Use the `airsh activate` command, and enter your activation code when prompted.

5. To finish setting up the Airwall Gateway, use `airsh` to also add the Conductor URL and map port (if not using the standard port). See Airshell (airsh) Command Reference on page 362.
6. Repeat with any other Airwall Gateways you want to provision, using a different activation code for each one.

Once you've set the activation code and Conductor URL, the Airwall Gateways will automatically connect to the Conductor, and be provisioned and managed in the Conductor using the options you selected when creating the activation codes.

You can now license your Airwall Gateways. See the License section of Provision and License Airwall Edge Services on page 193.

Transfer a license to another Airwall Edge Service

You can transfer Airwall Edge Service licenses within the Conductor.

There are two ways to transfer a license from one Airwall Edge Service to another:

- **Replace** – Replacing an Airwall Edge Service transfers all of the settings from the replaced Airwall Edge Service along with the license. Follow the instructions in Replace an Airwall Gateway on page 132.
- **Revoke** – Revoking an Airwall Edge Service frees only the license for use, and does not transfer the settings.

Transfer a license by Revoking the Airwall Edge Service

1. Make sure the Airwall Edge Service you want to transfer the license to is installed and provisioned, but unmanaged (unlicensed).
2. Revoke the Airwall Edge Service you want to un-license. For details, see Revoke and Reactivate an Airwall Edge Service on page 496.
3. On the Conductor dashboard, filter the Airwall Edge Services by unmanaged.
4. Click the drop down on the Airwall Edge Service you want to license, and click **Manage Airwalls**.

Renew Expired Licenses

To renew Airwall Edge Service licenses:

1. Contact sales@tempered.io to renew your subscriptions.
2. Once you've received confirmation from Tempered that your subscription has been renewed, in Conductor, open **Settings**, and go to the **Licensing** tab.
3. On the right top, click **Full Sync** to update your vouchers.

Note: If Tempered provides new vouchers, see Add Airwall Edge Service Licenses to the Conductor on page 192.

License a Conductor and Airwall Edge Services in an Isolated Environment

To license a Conductor and Airwall Edge Services in an Isolated environment (also commonly called a dark or offline environment), you need to take a few additional steps.

To license an Isolated Conductor

1. On the Tempered Conductor Provisioning page, where it's asking for a voucher code, enter the voucher you received when you purchased the Conductor.
2. Click **Enable secure offline sync**.
3. Click **Export encrypted package**.
4. Save the exported package on the Conductor, and copy the package to a USB drive or other removeable device.
5. Mail the package to Customer Success for licensing.
6. When Customer Success sends you your encrypted licensing package, download it to a USB drive.
7. Click **Import encrypted package** (you may need to click **Enable secure offline sync** again to show the page), select the package you downloaded, and click **Import**.
8. After the package is opened and finished processing, your Conductor is licensed, and will move to the **Log In** page.

Follow the steps from starting at **Log In and Configure** in Deploy a Physical Conductor.

To provision and license Isolated Airwall Edge Services

1. In the licensed Isolated Conductor, open **Settings**, and go to the **Licensing** page.
2. If you have a license voucher, Add Airwall Edge Service Licenses to the Conductor on page 192. If you don't have a license voucher, contact sales@tempered.io to get one before continuing.
3. Under **Secure offline Conductor**, select **Enabled** to enable offline licensing.
4. Install the Airwall Edge Services you want to license and connect them to the Conductor. For more information, see Connect Airwall Gateways to the Conductor on page 292.
5. Under **Provisioning Requests**, select the check boxes for the Airwall Edge Services you want to provision, and under the **Actions** dropdown, click **Grant**.
6. Click **Export encrypted package**, and click **Save**.
7. Mail the package to Customer Success for licensing.
8. When Customer Success sends you your encrypted licensing package, download it.
9. In the Conductor, on the **Licensing** page, click **Import encrypted package**
10. Select the package you downloaded, and click **Import**.
11. After the package is opened and finished processing, your Airwall Edge Services are provisioned. They should reconnect to the Conductor and appear in your Airwall Edge Services list as unmanaged.
12. Click the drop down on the Airwall Edge Service you want to license, and click **Manage Airwalls**.

Deploy and Configure a Conductor

The Airwall Conductor helps you deploy, configure, administer, and update your Airwall Solution.

Deploy a Conductor

To set up a Conductor for the first time, you need to configure a few basic settings. After completing the following, you can connect the Conductor to your underlay.

Before you begin these steps

The Conductor manages policy for all distributed Airwall Edge Services, delivering simple control of the network. Confirm your existing network settings such as DHCP, DNS and firewalls to decide where your Airwall solution will exist within your environment. For more information, see Confirm your Network Settings on page 187.

Important: Do not connect any Airwall Edge Services or hardware until after the Conductor is configured.

Note: The Conductor uses a Tempered security certificate. This certificate is anchored to the Tempered Certificate Authority (CA). You may need to explicitly trust the certificate to connect to the user interface. If you would like to use your own certificate, see Install a Custom CA Certificate Chain on page 239.

Conductor Configuration Wizard Settings

Here are the settings you can configure in the Conductor Configuration Wizard.

For steps, see Log in and Configure the Conductor on page 201. For more settings see Best Practices for Conductor Configuration on page 235 and Configure a Conductor on page 235.

Supported Versions	v2.2.10 and later Conductor

Wizard page	Setting	Description
Define hostname settings	**Hostname** and **Domain name**	Enter a hostname and domain name to create a friendly URL for your Conductor. See Configuring a Conductor IP, Friendly URL, or Port on page 236.

Wizard page	Setting	Description
Configure network adapters	**Enable network adapter**	Set up the Network adapters to communicate with your existing network (the underlay). By default: • For physical and virtual Conductors, Network adapter 1 is configured with a static IP address of 192.168.56.2. • For cloud Conductors, the IP address should match the **Internal IP** or public IP of your Conductor instance. • Network adapter 2 is configured for DHCP IP addressing.
	Enable web access to Conductor	This setting enables or disables the web server (the Conductor UI) on the port. You have to have at least one enabled, unless they are both DHCP, then they both have to have it enabled.
	Network configuration	
	Static routes	Define static routes for each network interface if required for communication.
Apply network configuration	**Apply**	Confirm that the network settings are correct, then select **Apply**. If the network configuration has been changed, then you may need to manually navigate to the new location in your browser.
Create a second administrative account	Fill in the **Username** and other details for a second administrative account.	It is best practice to only use the 'admin' account for top-level administration. Creating user accounts for each person who will be administering the Conductor lets you see who is making changes in the system when you review log details.
Configure date and time settings	**Use NTP** and **NTP Servers**	Enable **Use NTP** and select the NTP servers to use to set the time. While you can set your system time manually, using NTP (Network Time Protocol) servers ensures your system time stays synchronized with Coordinated Universal Time (UTC). See Set the Conductor system time.
	Enter time manually	Check this box to set the time manually, and then enter the time, or select **Set from browser time** to use your browser's setting.

Wizard page	Setting	Description
Configure email settings		These email settings are used to send messages from the Conductor for Airwall invitations, alerts and password resets. If you do not set these up, you will not be able to send or receive email from the Conductor.
Provision Conductor	**Provision online** or **Provision offline**	Provision your Conductor online by accessing the Tempered licensing servers. You need to be able to access licensing.temperednetworks.com on the Internet. If you're provisioning a dark Conductor, the wizard will walk you through the process.
Provision Conductor online	**Voucher code**	Enter the voucher code you received when purchasing your Conductor license.
	Use proxy server	Enable and enter your proxy server information if you need to go through a proxy server to access the Conductor licensing server.
Provision Conductor offline		Follow the steps to license your isolated (or "dark") Conductor offline: **1.** Generate a secure licensing request. **2.** Send the licensing request to Tempered at Customer Success. **3.** Import the encrypted licensing package you receive from Customer Success. For more details, see License a Conductor and Airwall Edge Services in an Isolated Environment on page 196. If you get disconnected from the wizard during this step, it'll continue at the provisioning select screen. If that's the case, then select **Provision Offline** again and continue to the next step.

Note: When you start up your Conductor, you will have to proceed past the security warning (for example, in Firefox, click Advanced and then Accept risk). To avoid this warning, you can replace the Conductor-signed certificate with a custom certificate. See Install a Custom CA Certificate Chain on page 239.

Deploy a Physical Conductor

Tempered offers two physical Conductor models, the Conductor 400 Series and the Conductor 500 Series. Both are 1U rack-mount security appliances that facilitate private overlay networks between customer-provided equipment and devices.

Note: The hardware for an Conductor-500 and an Airwall Gateway-500 are similar. If your order contains both, check the bottom of the unit or the box for a sticker that marks Conductor hardware.

Note: For Conductor-500, use only Port 1 or Port 2. Do not connect anything to any of the other ports. For provisioning, and connection to the underlay network, connect to Port 1. For Diagnostics, connect to Port 2.

Familiarize yourself with your model's front panel layout, specifications, power requirements, and safety warnings before use. These can be found in your model's Platform Guide, included with your Conductor. If you are unable to locate your Platform Guide, you can download a PDF from the Documentation Downloads on page 810Documentation Downloads section of Airwall help.

License and Provision a Conductor (v2.2.8 and earlier)

To get a Conductor up and running, you need license and provision it. You need your licensing voucher to complete these steps.

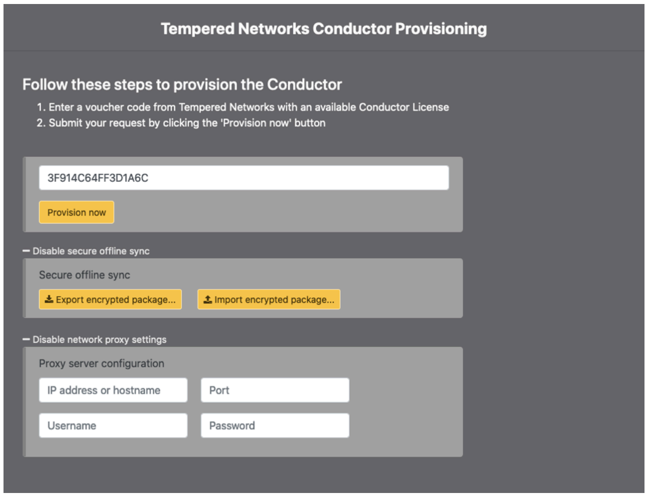
Supported Versions	Conductor v2.2.8 and earlier

Note: **For v2.2.10 and later**, licensing and provisioning is included in the Initial Conductor configuration wizard. Start at Log in and Configure the Conductor on page 201.

In v2.2.8 and earlier, you license the Conductor, and then Log in and Configure the Conductor on page 201.

1. If you have a physical Conductor, apply power to it, and connect a computer to Port 1 on the Conductor hardware using an Ethernet cable. Refer to your unit's Platform Guide for specific instructions.
2. In a web browser:
   - **Physical Conductor** – go to: `https://192.168.56.2`
   - **Cloud Conductor** – Click the link in your order email, or go to the public IP you set up when creating your Conductor.

   The Conductor **Provisioning** page opens so you can license your Conductor.



Tempered Networks Conductor Provisioning

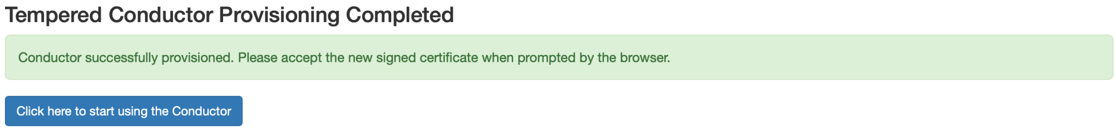
Follow these steps to provision the Conductor

1. Enter a voucher code from Tempered Networks with an available Conductor License
2. Submit your request by clicking the 'Provision now' button

3F914C64FF3D1A6C

Provision now
− Disable secure offline sync
Secure offline sync
Export encrypted package...
Import encrypted package...
− Disable network proxy settings
Proxy server configuration
IP address or hostname
Port
Username
Password

3. If you have a proxy server between your Conductor and the Tempered licensing server, under **Disable network proxy settings**, configure proxy server settings to allow your Conductor to reach the licensing server.
4. If you are licensing an isolated (dark) Conductor, you will use the **Disable secure offline sync** section. For more details, see License a Conductor and Airwall Edge Services in an Isolated Environment on page 196.
5. In the **Voucher code** box, enter the voucher code you received from Tempered.
6. Click **Provision now**. It takes a moment to finish applying the voucher. Once complete, you should see the following:



Tempered Conductor Provisioning Completed

Conductor successfully provisioned. Please accept the new signed certificate when prompted by the browser.

7. Select **Click here to start using the** Conductor.
8. Log in and Configure the Conductor on page 201.

Log in and Configure the Conductor

The first step in setting up a Conductor is to log in and configure it.

Before you begin

Before you begin, you will need the following:

- The IP or hostname of a cloud or virtual Conductor. Follow the link in your order email, or go to the public IP you set up when creating your Conductor.
- Your Conductor license voucher code.

Set up a v2.2.10 or later Conductor

When you first set up a Conductor, it walks you through the initial configuration steps, then licensing and provisioning. For descriptions of the settings, see Conductor Configuration Wizard Settings on page 197.

1. If you have a physical Conductor, apply power to it, and connect a computer to Port 1 on the Conductor hardware using an Ethernet cable. Refer to your unit's Platform Guide for specific instructions.
2. In a web browser:
   - **Physical Conductor** – Go to: `https://192.168.56.2`
   - **Cloud Conductor** – Follow the link in your order email, or go to the public IP you set up when creating your Conductor.
   - **Virtual Conductor** – Go to `https://192.168.56.2`, or the IP address for Network adapter 1 or 2 that you set up when deploying your virtual Conductor.

   Note: Depending on your browser, you may have to bypass the **Your connection is not private** warning to access your Conductor.
3. Enter the default username (admin) and the password from your Tempered Order Delivery email, from your cloud provider (Tnw-<*instance ID*>, or the default password (admin123), and select **Sign in**.
4. Change your password when prompted, and select **Update**.
5. You're now in the Conductor Configuration Wizard. Follow the wizard to configure essential settings on your Conductor, and then license and provision it.

After provisioning is complete, accept the new Conductor certificate. Now you can Add Airwall Edge Service Licenses to the Conductor on page 192.

Note: When you start up your Conductor, you will have to proceed past the security warning (for example, in Firefox, click **Advanced** and then **Accept risk**). To avoid this warning, you can replace the Conductor-signed certificate with a custom certificate. See Install a Custom CA Certificate Chain on page 239.

2.2.8 and earlier Conductor

With 2.2.8 and earlier, you need to License and Provision a Conductor (v2.2.8 and earlier) on page 191 first, then configure it.

1. In a browser window, enter the URL for your Conductor.
2. Enter the default username (admin) and the password from your Tempered Order Delivery email, from your cloud provider (usually Tnw-<*instance ID*>), or the default password (admin123), and select **Sign in**.
3. Change your password when prompted.
4. Select **Update**.

5. On the System Configuration dialog, you can leave all the fields as they are and select **Configure**. For recommended configuration, see Best Practices for Conductor Configuration on page 235.
6. Once configuration is finished, select **Return to settings**.

You should see the Conductor **Settings** page. You are now ready to connect Airwall Edge Services and devices, and create overlays.

Add Airwall Edge Service Licenses to the Conductor

The first step in licensing Airwall Edge Services is to add your licensing vouchers to the Conductor.

To add Airwall Edge Service licenses:

1. In Conductor, open **Settings**, and go to the **Licensing** tab.
2. Click **Enter Voucher**.
3. Type or paste your Voucher code, and click **Enter**. The licenses are added to your pool of licenses on the **Licensing** page.

Note: The Conductor automatically consolidates licensing vouchers.

Deploy a Conductor on a Cloud Platform

You can deploy a Tempered Conductor on several cloud platforms and manage physical, virtual, and cloud Airwall Edge Services and Airwall Agents.

Currently, you can deploy a Conductor on the following cloud platforms:

- Amazon Web Services (AWS)
- Microsoft Azure Cloud Platform
- Google Cloud Platform (GCP)
- Amazon Web Services (AWS)
- Microsoft Azure Cloud Platform (Azure)
- Google Cloud Platform (GCP)

There are several reasons you may choose to deploy your Conductor on a cloud platform:

- Conductor administrators can access a Conductor regardless of location.
- All three supported cloud platforms promise 99.9% up-time meaning that a Conductor will always be available and supported by each respective platform provider.
- Deploying a Conductor to the cloud reduces the risk associated with managing on-premises infrastructure, which can result in a significant cost savings over time.

If you decide to host your Conductor on a cloud platform, use the specific deployment instructions linked above for your chosen platform.

Deploy a Conductor on Alibaba Cloud

You can deploy an Airwall Conductor on Alibaba Cloud to manage physical, virtual, and cloud Airwall Edge Services, and Airwall Agents. Use the following steps to deploy a Conductor on Alibaba Cloud.

Supported Versions	Conductor 2.2.8 and later

Note: Click the print icon 🖶 at the top right of this topic to print or create a PDF.

Before you Begin

Before you begin, you need:

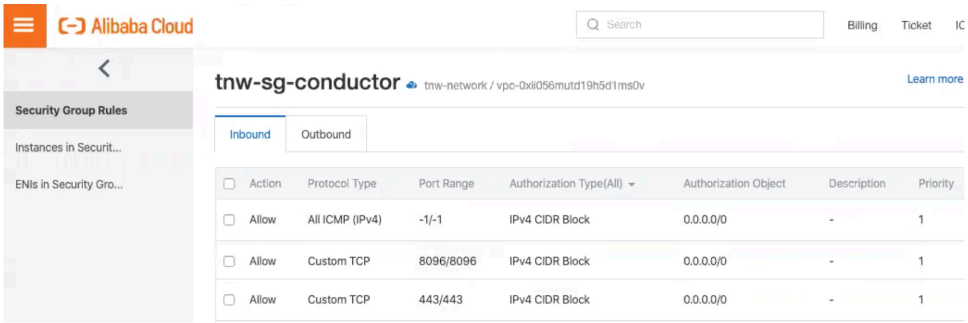
- Access to an Alibaba Cloud account. If you do not have an account, you can create one here.
- Billing information set up for your Alibaba Cloud account.
- A Conductor license voucher. You need to purchase a voucher to license and log in to your Conductor once you've deployed it on Alibaba Cloud.

Note: See Alibaba Cloud for details and up to date instructions.

Step 1: Set up a Security Group

Before you start setting up the Conductor, you need to set up a Security Group and Networks in Alibaba Cloud for the Conductor.

1. Follow the instructions on Alibaba Cloud to log in to your account.
2. In Alibaba Cloud, on the **Elastic Compute Service** side menu, go to **Networks and Security**, then **Security Groups**.
3. Create a new Security Group for your Conductor, and set up the following **Inbound Security Group Rules**:
   a) Allow ICMP IPv4 access. This allows the Conductor to check network communication and reachability (for example, ping).
   b) Allow TCP on port 8096. This is the port the Conductor uses to communicate.
   c) Allow TCP on 443/443. This opens up https:// for the Conductor's web interface and API calls.



tnw-sg-conductor tnw-network / vpc-0xii056mutd19h5d1ms0v

□	Action	Protocol Type	Port Range	Authorization Type(All)	Authorization Object	Description	Priority
□	Allow	All ICMP (IPv4)	-1/-1	IPv4 CIDR Block	0.0.0.0/0	-	1
□	Allow	Custom TCP	8096/8096	IPv4 CIDR Block	0.0.0.0/0	-	1
□	Allow	Custom TCP	443/443	IPv4 CIDR Block	0.0.0.0/0	-	1

Step 2: Set up Networks

1. In Alibaba Cloud, on the Elastic Compute Service side menu, go to **Networks and Security**, then **VPCs**.
2. Create a VPC for your Conductor.
3. Set up 2 subnets in that network, and select the datacenter and zone for them (these need to be the same as you choose for the Conductor in the next step):
   - public_network
   - private_network

Now you're ready to set up the Conductor.

Step 3: Set up a Conductor in Alibaba Cloud

Set General Settings

1. Search for **Tempered Airwall Conductor** in the Alibaba Cloud marketplace.
2. Select **Choose Your Plan**.
3. Select your **Billing method** and **Region**. Make sure you choose the same datacenter and zone as the subnets you set up earlier.
4. For **Instance Type**, select `ecs.g5.large`.
5. For **Image**, leave it on the default `Marketplace image`.
6. Under **Storage**, set:
   a) **System Disk** - Set to Ultra Disk with the minimum storage of 40 GiB.
   b) **Data Disk** – Add a second Enhanced SSD drive with 120 GiB for the database and log files.
7. Select **Next: Networking** at the bottom to continue.

Set Networking Settings

8. Under **Network Type**:
   a) **Type** - Choose `VPC`.

   b) **Select a VPC** - Select the VPC network you set up earlier
   c) **Select a VSwitch** – Select the public_network subnet you set up earlier.

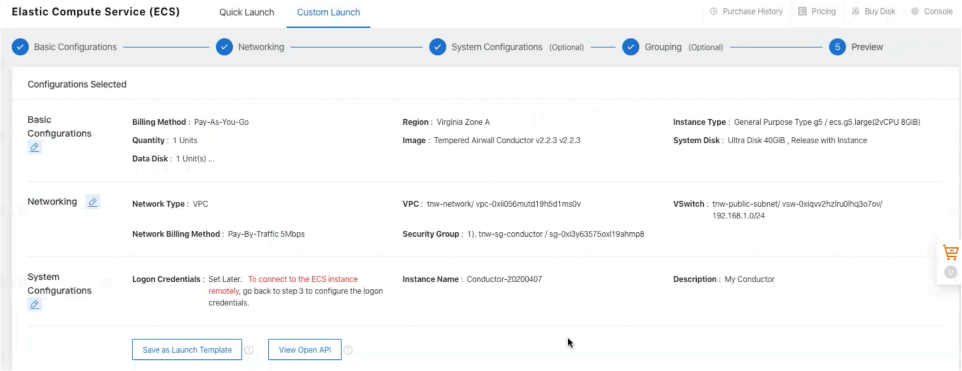
9. Under **Public IP Address**, check the **Assign Public IP Address** box.
10. Under **Bandwidth Billing**, select **Pay by Traffic**.
11. Under **Security Group**, select the security group you created earlier.
12. Leave the rest of the settings as the default, and select **Next: System Configurations**.

Set System Configurations

13. For **Logon Credentials**, select **Set Later**.
14. For **Instance Name**, set to `Conductor-<date>`. For example, `Conductor-20200501`.
15. (Optional) Fill in the **Description**, and set a **Hostname** if you have it set up.
16. Select **Next: Grouping**, then **Next: Preview**. (You do not need to set any Grouping settings.)

Preview your Settings and Create

17. On the **Preview** page, check your settings, check to accept the terms of service, and then select **Create Instance**.



Configurations Selected

Basic Configurations

Billing Method : Pay-As-You-Go
Quantity : 1 Units
Data Disk : 1 Unit(s) ...
Region : Virginia Zone A
Image : Tempered Airwall Conductor v2.2.3 v2.2.3
Instance Type : General Purpose Type g5 / ecs.g5.large(2vCPU 8GiB)
System Disk : Ultra Disk 40GiB , Release with Instance

Networking

Network Type : VPC
Network Billing Method : Pay-By-Traffic 5Mbps
VPC : tnw-network/ vpc-0xii056mutd19h5d1ms0v
Security Group : 1). tnw-sg-conductor / sg-0xi3y63575oxl19ahmp8
VSwitch : tnw-public-subnet/ vsw-0xiqvv2hzlru0lhq3o7ov/ 192.168.1.0/24

System Configurations

Logon Credentials : Set Later. To connect to the ECS instance remotely, go back to step 3 to configure the logon credentials.
Instance Name : Conductor-20200407
Description : My Conductor

   You get a confirmation that your instance has been created.

18. Click **Console** to go to your Conductor instance page, where you can see the status of the instance being created. Under IP address, note the IP of your Conductor.

Step 4: (Optional) Assign a permanent IP to your Conductor

If needed, you can assign a permanent IP address under Networks & Security, EIP. See the Alibaba Cloud help for instructions.

Verify, Configure, Provision, and License a Cloud Conductor

At this point the Conductor instance is running in your cloud provider.

To verify, paste your Conductor IP into a browser window. It should show you the Initial Conductor Configuration page. To log in, configure, and license your Conductor, see Log in and Configure the Conductor on page 201.

Note: In v2.2.8 and earlier, it shows the Provisioning page. See License and Provision a Conductor (v2.2.8 and earlier) on page 191.

It may take several minutes for the Conductor to become available after it starts, so if you attempt to access it and your browser appears to stop responding, please try again in a few minutes.

Here are the default passwords for cloud Conductors. You are prompted to change the password as soon as you log in:

- **Alibaba Cloud** – Tnw-<instanceID>
- **Amazon Web Services** – Tnw-<instanceID>
- **Microsoft Azure** – Tnw-<privateIpOfPublicNic>
- **Google Cloud** – Tnw-<instanceID>

Note: In Microsoft Azure, if you do not see a password on the Azure Outputs page next to **conductorPassword**, it is likely you are not using the Managed image.

Note: When running the Conductor for the first time, you may receive notifications indicating the connection is not private. Once you have finished configuring the Conductor, you can install a custom certificate on the Conductor that prevents these notifications in the future.

For more information, see:

- **Conductor v2.2.8 and earlier only** – License and Provision a Conductor (v2.2.8 and earlier) on page 191
- Log in and Configure the Conductor on page 201
- Add Airwall Edge Service Licenses to the Conductor on page 192
- Conductor Configuration Wizard Settings on page 197

Conductor v2.2.8 and earlier – Set Conductor System Time

After you've finished provisioning and licensing your v2.2.8 or earlier Alibaba Cloud Conductor, you may need to change the system time, as the default time zone may be out of sync with your current time. In v2.2.10 and later, you are prompted to set the system time during initial configuration.

1. In your Conductor, go to **Settings**.
2. Under System time, select **Edit Settings**.
3. Select **Set browser time**, and then select **Update**.

You can also enable NTP servers to set the system time. See **Set the Conductor system time** in Airwall help or your Airwall Deployment Guide.

You can also enable NTP servers to set the system time. See Set the Conductor system time on page 236.

Deploy a Conductor on Amazon Web Services (AWS)

You can deploy an Airwall Conductor on AWS and manage physical, virtual, and cloud Airwall Edge Services, and Airwall Agents. Use the following steps to deploy a Conductor on the AWS platform.

Note: Click the print icon 🖶 in the top right to print or download this topic.

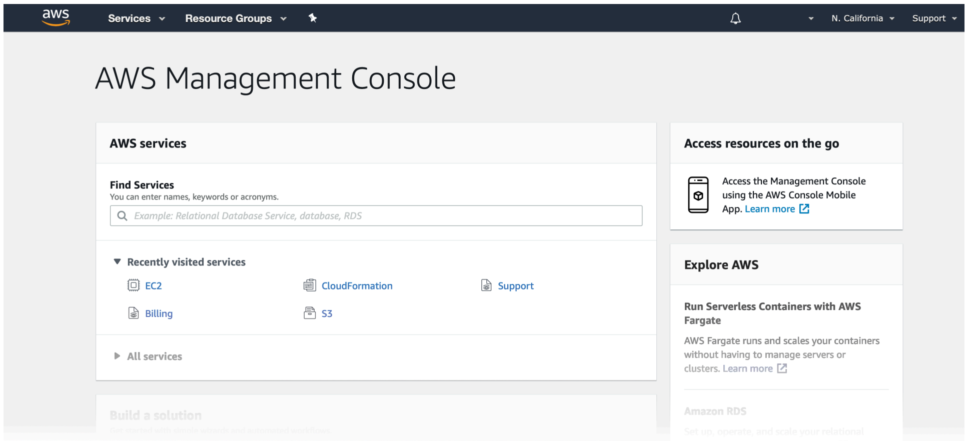
Prerequisites

To get started, you need to have:

- Access to a Amazon Web Services (AWS) account. If you do not have an account, you can create a free AWS Free Tier account and upgrade it to a full account later.
- Billing information set up on your AWS account. You cannot create a project until you are able to link your billing information to your newly created project.
- A Conductor license voucher if you want to start the Conductor and verify it is set up correctly. Fulfillment will provide this to you in an email after your purchase is complete.
- The Amazon Machine Image (AMI) ID that you received from Tempered Fulfillment when you purchased your AWS Conductor.

Log in to AWS

From a Web browser, navigate to https://console.aws.amazon.com/ and log in to your account to get to the AWS Management Console, pictured below:



You can enter names, keywords or acronyms.

Access the Management Console using the AWS Console Mobile App. Learn more

Run Serverless Containers with AWS Fargate

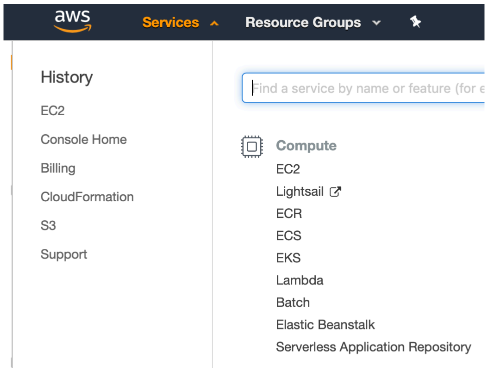
AWS Fargate runs and scales your containers without having to manage servers or clusters. Learn more

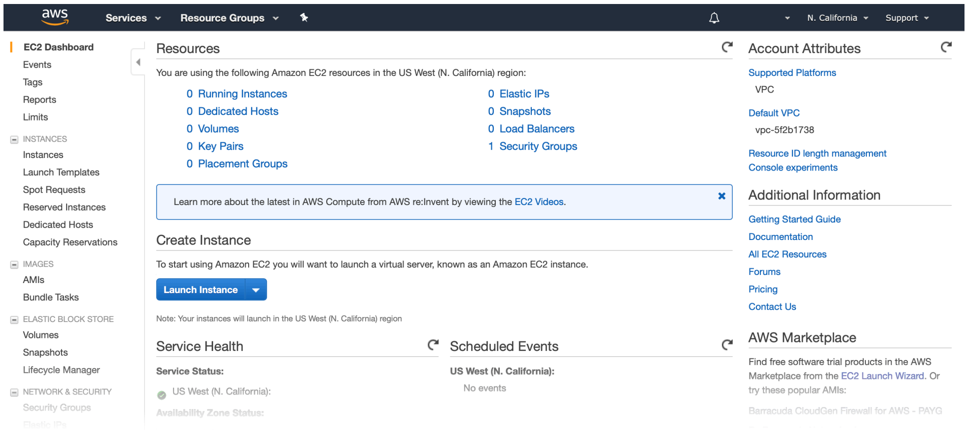
Create a Launch Instance

When you sign up for Amazon Web Services (AWS), your AWS account is automatically signed up for all services in AWS, including Amazon EC2. You add the Tempered Conductor as an EC2 instance, so make sure you have the AMI ID that you received from Tempered Fulfillment when you purchased your AWS Conductor.

To create an instance:

1. On the top bar of the **AWS Management Console**, select **Services** and then select **EC2** to access the **EC2 Dashboard**.





You are using the following Amazon EC2 resources in the US West (N. California) region:

0 Running Instances	0 Elastic IPs
0 Dedicated Hosts	0 Snapshots
0 Volumes	0 Load Balancers
0 Key Pairs	1 Security Groups
0 Placement Groups	

Learn more about the latest in AWS Compute from AWS re:Invent by viewing the EC2 Videos.

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

Note: Your instances will launch in the US West (N. California) region

Service Status:

US West (N. California):

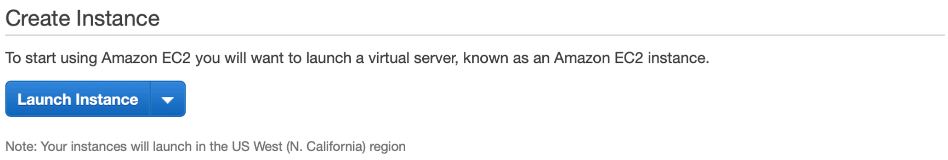
Availability Zone Status:

US West (N. California):

No events

Find free software trial products in the AWS Marketplace from the EC2 Launch Wizard. Or try these popular AMIs:

2. In the **Create Instance** section, click **Launch Instance**.



Create Instance

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

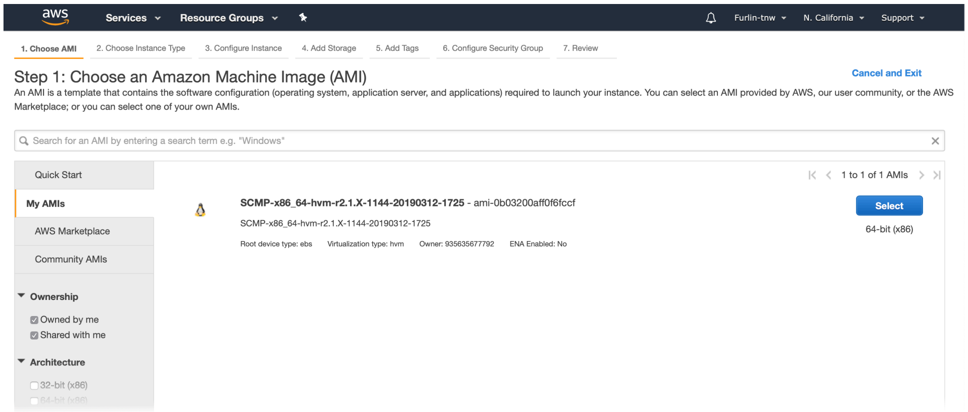
Note: Your instances will launch in the US West (N. California) region

3. Click **Launch Instance** to start the instance setup wizard.

Step 1: Choose an Amazon Machine Image (AMI)

The AMI is a custom template used to create a Conductor as a virtual machine in AWS. It contains the Conductor's root volume, permissions, and device mappings necessary to deploy the Conductor to your account.

1. On the **Choose AMI** tab, click **My AMIs** on the left.
2. Under **Ownership**, check the **Shared with me** box. You should see the Conductor image listed in the right pane.



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Search for an AMI by entering a search term e.g. "Windows"

SCMP-x86_64-hvm-r2.1.X-1144-20190312-1725 - ami-0b03200aff0f6fccf

SCMP-x86_64-hvm-r2.1.X-1144-20190312-1725

Root device type: ebs Virtualization type: hvm Owner: 935635677792 ENA Enabled: No

64-bit (x86)

Ownership

☑ Owned by me
☑ Shared with me

Architecture

☐ 32-bit (x86)
☐ 64-bit (x86)

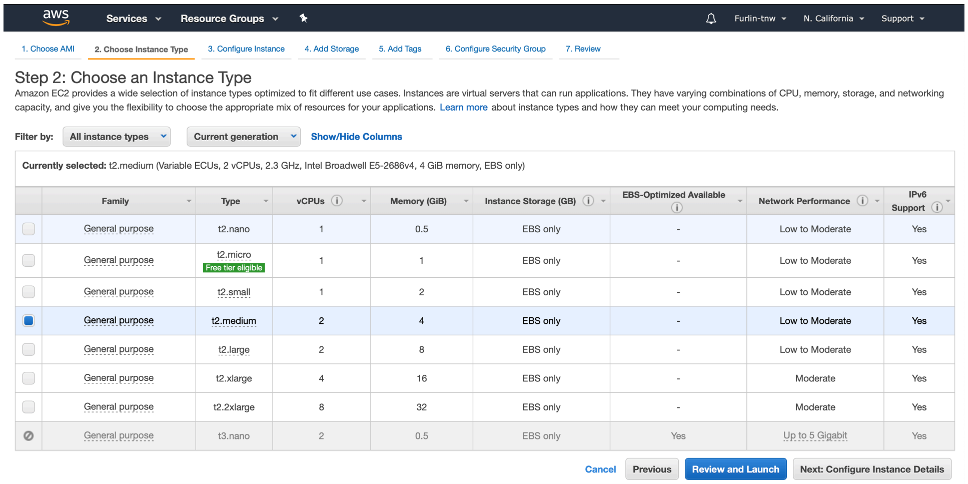
3. Click the **Select** button on the right to continue.

Step 2: Choose an Instance Type

The Amazon EC2 instance type identifies the combination of memory, networking capacity, CPU, and storage required by an application. For the Conductor we recommend a minimum machine type of **t2.medium**.

1. On the **Choose Instance Type** tab, select your desired instance type and click **Next: Configure Instance Details**.

> **Important:** DO NOT select the **Review and Launch** button, as this option will use the default settings for this instance type. You will need to make changes for the Conductor to operate correctly.



Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

Filter by: All instance types Current generation

Currently selected: t2.medium (Variable ECUs, 2 vCPUs, 2.3 GHz, Intel Broadwell E5-2686v4, 4 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
☐	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
☐	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
☐	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
☑	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
☐	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
☐	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
☐	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
⊘	General purpose	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes

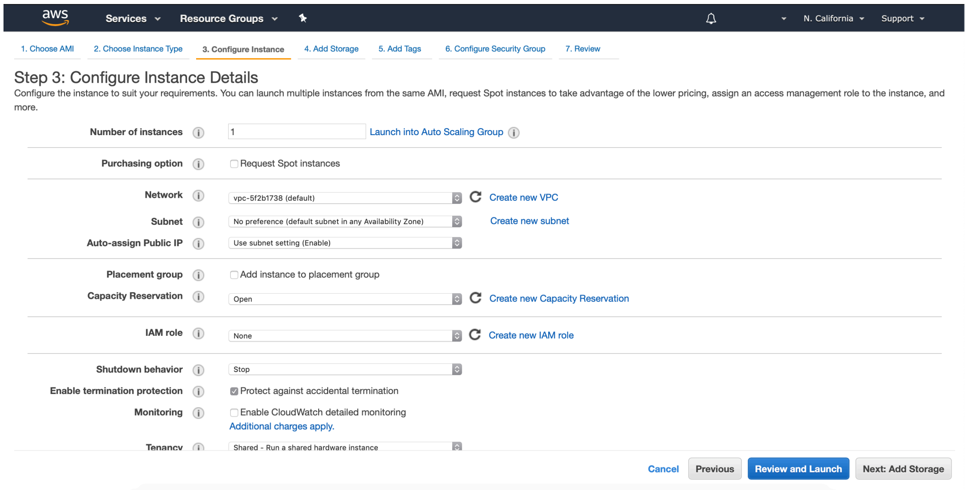
2. Click **Next: Configure Instance Details** to continue.

Step 3: Configure Instance Details

Your new instance requires that you to make a few changes to ensure the Conductor has access to resources needed for proper operation. Make the following changes as outlined below.

1. On the **Configure Instance** tab, do the following:
   a) Select your desired VPC from the **Network** drop-down.
   b) Select your region from the **Subnet** drop-down.
   c) Select **Enable termination protection** (recommended)

   You can leave all other settings as is.



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1
Purchasing option: □ Request Spot instances
Network: vpc-5f2b1738 (default)
Subnet: No preference (default subnet in any Availability Zone)
Auto-assign Public IP: Use subnet setting (Enable)
Placement group: □ Add instance to placement group
Capacity Reservation: Open
IAM role: None
Shutdown behavior: Stop
Enable termination protection: ☑ Protect against accidental termination
Monitoring: □ Enable CloudWatch detailed monitoring
Tenancy: Shared - Run a shared hardware instance

2. Click **Next: Add Storage** to continue.

Step 4: Add Storage

The Conductor AMI supplied by Tempered is relatively small in size. The configuration information and storage, however, requires a second hard disk, which you set up as part of the instructions below.

1. On the Add Storage tab, click **Add New Volume**.

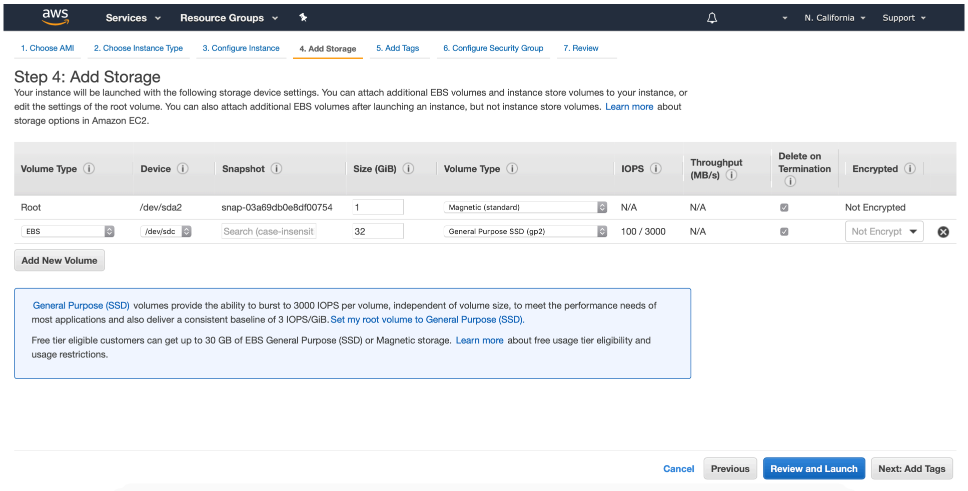
   Note: The volume must be a minimum of 32 GB. This size should be sufficient for normal operation; however, you can resize your volume later should you require additional space. See Modifying the Size, Performance, or Type of an EBS Volume in the AWS documentation for more information.

2. Change the following information on the new volume:
   a) Select **/dev/sdf** from the **Device** drop-down.

      Important: We recommend you use **/dev/sdf** for your second volume. Do not select **/dev/sdb, /dev/sdc, or /dev/sdd** as the Conductor will not function correctly. Other partitions may work but are not currently supported.

   b) Enter the value `32` in the **Size (GiB)** field.
   c) Check **Delete on Termination**.

   You can leave all other settings as is.



Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted	
Root	/dev/sda2	snap-03a69db0e8df00754	1	Magnetic (standard)	N/A	N/A	☑	Not Encrypted	
EBS	/dev/sdc	Search (case-insensit	32	General Purpose SSD (gp2)	100 / 3000	N/A	☑	Not Encrypt	⊗

General Purpose (SSD) volumes provide the ability to burst to 3000 IOPS per volume, independent of volume size, to meet the performance needs of most applications and also deliver a consistent baseline of 3 IOPS/GiB. Set my root volume to General Purpose (SSD).

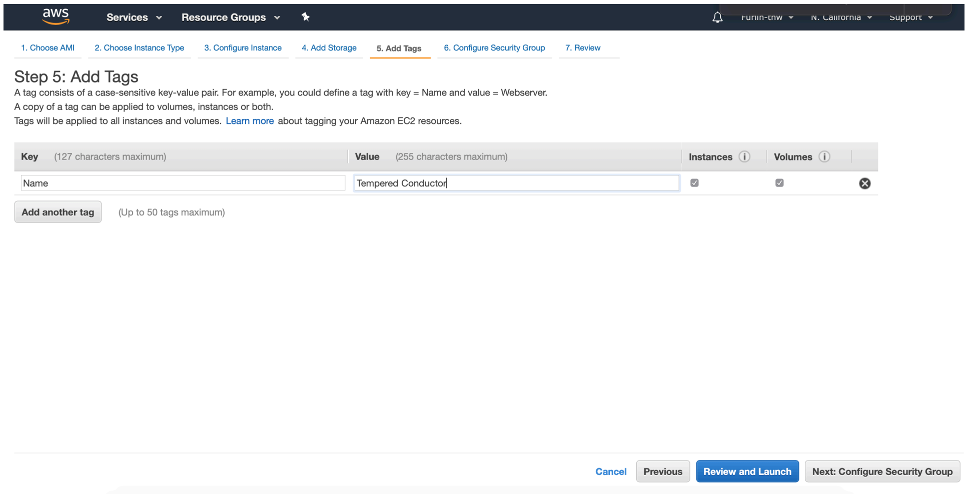
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

3. Click **Next: Add Tags** to continue.

Step 5: Add Tags

Tagging your Conductor instance can help you identify it if you have a large number of instances deployed to your account. While not required, we recommend you add a tag so you can find it quickly.

1. On the **Add Tags** tab, click **Add Tag** and enter the following:
   a) Enter **Name** in the **Key** column.
   b) Enter a name for your Conductor in the **Value** column.



Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key (127 characters maximum)	Value (255 characters maximum)	Instances	Volumes	
Name	Tempered Conductor	☑	☑	⊗

2. Click **Next: Configure Security Group** to continue.

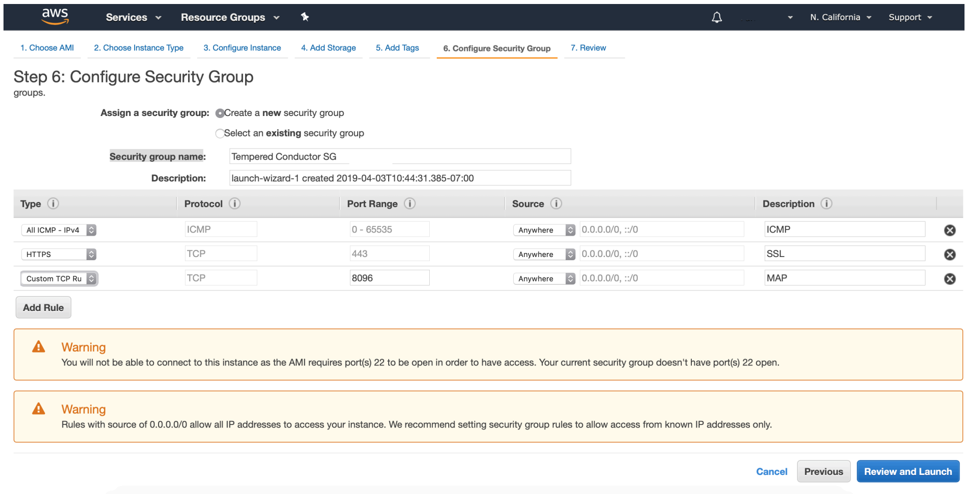
Step 6: Configure Security Group

Configuring a security group is synonymous with configuring firewall rules. You need to add three rules: ICMP to allow Airwall Edge Services to validate their link to the Conductor, HTTPS to allow for Conductor management, and a custom rule to allow Airwall Edge Services to communicate with the Conductor on port 8096.

1. In the **Assign a security group** section, select the **Create a new security group** radio button.
2. In the **Security group name** field, enter a name for your security group.
3. In the **Description** field, enter a description for your security group, or leave the default.
4. Add three rules to your security group:
   a) Click **Add Rule**, select **All ICMP – IPv4** from the **Type** drop-down, select **Anywhere** from the **Source** drop-down, and enter **ICMP** in the **Description** column.

b) Click **Add Rule**, select **HTTPS** from the **Type** drop-down, select **Anywhere** from the **Source** drop-down, and enter **SSL** in the **Description** column.

c) Click **Add Rule**, select **Custom TCP Rule** from the **Type** drop-down, enter **8096** in the **Port Range** column, select **Anywhere** from the **Source** drop-down, and enter **MAP** in the **Description** column.



Step 6: Configure Security Group

groups.

Assign a security group: ● Create a **new** security group

○ Select an **existing** security group

Security group name: Tempered Conductor SG

Description: launch-wizard-1 created 2019-04-03T10:44:31.385-07:00

Type	Protocol	Port Range	Source		Description
All ICMP - IPv4	ICMP	0 - 65535	Anywhere	0.0.0.0/0, ::/0	ICMP
HTTPS	TCP	443	Anywhere	0.0.0.0/0, ::/0	SSL
Custom TCP Ru	TCP	8096	Anywhere	0.0.0.0/0, ::/0	MAP

Warning
You will not be able to connect to this instance as the AMI requires port(s) 22 to be open in order to have access. Your current security group doesn't have port(s) 22 open.

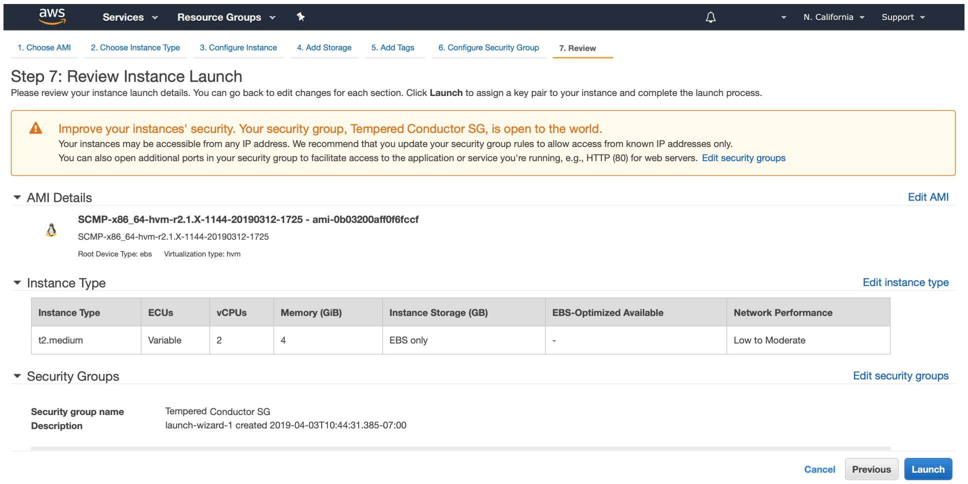
Warning
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

5. Click **Review and Launch** to continue.

Note: If you receive a **Boot from General Purpose (SSD)** dialog, select the **Continue with Magnetic as the boot volume for this instance** radio button and then click **Next**.

Step 7: Review

1. Review your setup information and if everything is correct, click **Launch**.



Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Improve your instances' security. Your security group, Tempered Conductor SG, is open to the world.
Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.
You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups

AMI Details — Edit AMI

SCMP-x86_64-hvm-r2.1.X-1144-20190312-1725 - ami-0b03200aff0f6fccf
SCMP-x86_64-hvm-r2.1.X-1144-20190312-1725
Root Device Type: ebs Virtualization type: hvm

Instance Type — Edit instance type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.medium	Variable	2	4	EBS only	-	Low to Moderate

Security Groups — Edit security groups

Security group name: Tempered Conductor SG
Description: launch-wizard-1 created 2019-04-03T10:44:31.385-07:00

2. In the **Select an existing key pair or create a new key pair** dialog, create a new key pair or enter one of your existing key pairs.

Note: This keypair is required to complete the wizard, but is never used since SSH is not enabled on Conductors.

3. Click **Launch Instance**.

Verify, Configure, Provision, and License a Cloud Conductor

At this point the Conductor instance is running in your cloud provider.

To verify, paste your Conductor IP into a browser window. It should show you the Initial Conductor Configuration page. To log in, configure, and license your Conductor, see Log in and Configure the Conductor on page 201.

Note: In v2.2.8 and earlier, it shows the Provisioning page. See License and Provision a Conductor (v2.2.8 and earlier) on page 191.

It may take several minutes for the Conductor to become available after it starts, so if you attempt to access it and your browser appears to stop responding, please try again in a few minutes.

Here are the default passwords for cloud Conductors. You are prompted to change the password as soon as you log in:

- **Alibaba Cloud** – Tnw-<instanceID>
- **Amazon Web Services** – Tnw-<instanceID>
- **Microsoft Azure** – Tnw-<privateIpOfPublicNic>
- **Google Cloud** – Tnw-<instanceID>

Note: In Microsoft Azure, if you do not see a password on the Azure Outputs page next to **conductorPassword**, it is likely you are not using the Managed image.

Note: When running the Conductor for the first time, you may receive notifications indicating the connection is not private. Once you have finished configuring the Conductor, you can install a custom certificate on the Conductor that prevents these notifications in the future.

For more information, see:

- **Conductor v2.2.8 and earlier only** – License and Provision a Conductor (v2.2.8 and earlier) on page 191
- Log in and Configure the Conductor on page 201
- Add Airwall Edge Service Licenses to the Conductor on page 192
- Conductor Configuration Wizard Settings on page 197

Additional Information

Once your Conductor is installed, you can configure and manage it as you would a physical Conductor. See Configure a Conductor on page 235. For additional help, you can accesssearch **Airwall help** by using the search bar at the top of the page or the navigation links to the left.

Deploy a Conductor on Microsoft Azure

You can deploy an Airwall Conductor on Azure and manage physical, virtual, and cloud Airwall Edge Services, and Airwall Agents. Use the following steps to deploy a Conductor on the Microsoft Azure platform.

Note: Click the print icon 🖶 in the top right to print or download this topic.

Prerequisites

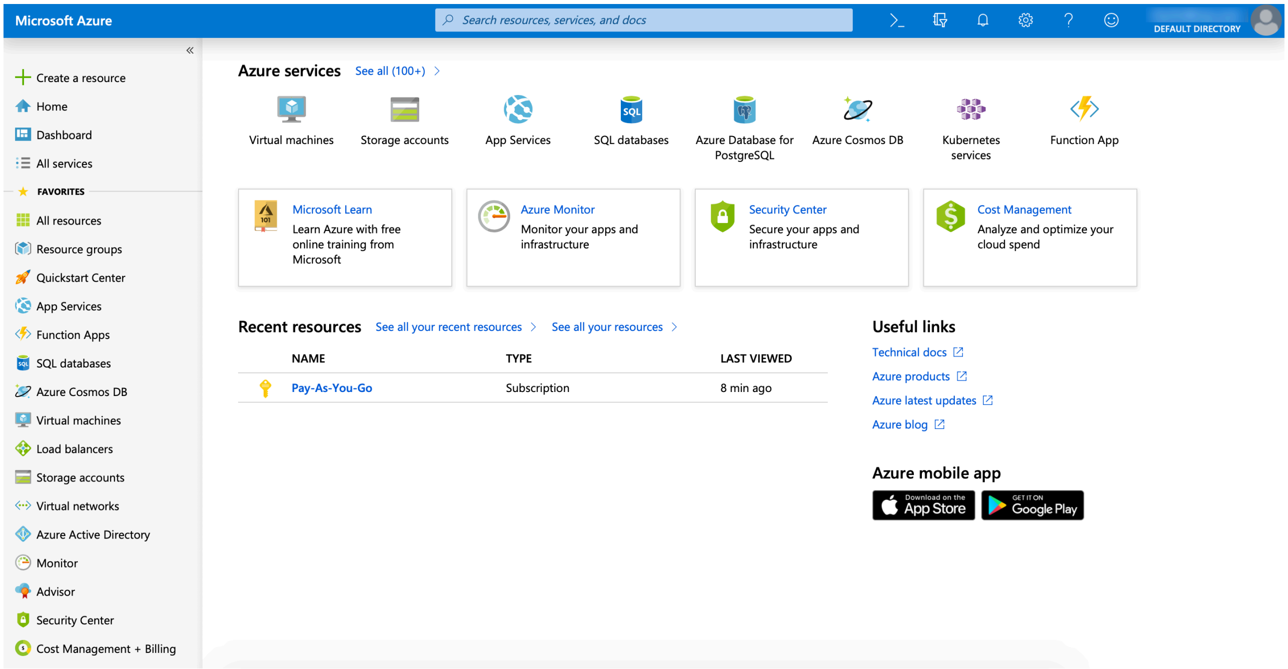
To get started, make sure you have access to your Azure account. If you do not have an account, you can create a free Microsoft Azure account and upgrade it to a full account later. If you have an existing Azure account, make sure your billing information is set up. You cannot create a project until you are able to link your billing information to your newly created project.

You need to purchase a Conductor license voucher for your Conductor to complete Step 3. After your purchase is complete, you get an email from Tempered Fulfillment with your voucher code.

Note: If you are familiar with how Azure organizes the components, you should be able to easily understand what is required and create them manually. However, this document does not cover a full manual deployment of a Conductor in Azure.

Step 1: Log in to Azure Cloud

From a Web browser, navigate to https://portal.azure.com and log in using your Azure credentials.



Microsoft Learn — Learn Azure with free online training from Microsoft

Azure Monitor — Monitor your apps and infrastructure

Security Center — Secure your apps and infrastructure

Cost Management — Analyze and optimize your cloud spend

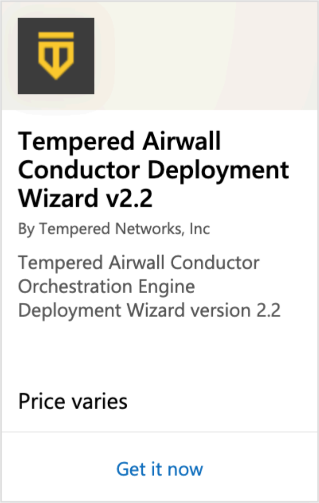
Recent resources — See all your recent resources — See all your resources

NAME	TYPE	LAST VIEWED
Pay-As-You-Go	Subscription	8 min ago

Step 2: Add a Conductor image

You add a Conductor image from the Azure marketplace to your project to create an instance.

1. In Azure, select **Create a Resource**, and search for `Tempered Conductor Deployment`.
2. Select **Tempered Airwall Conductor Deployment Wizard 2.2**, go to the **Plans** tab and check the version of the Conductor, and then select **Create**.



Tempered Airwall Conductor Deployment Wizard v2.2

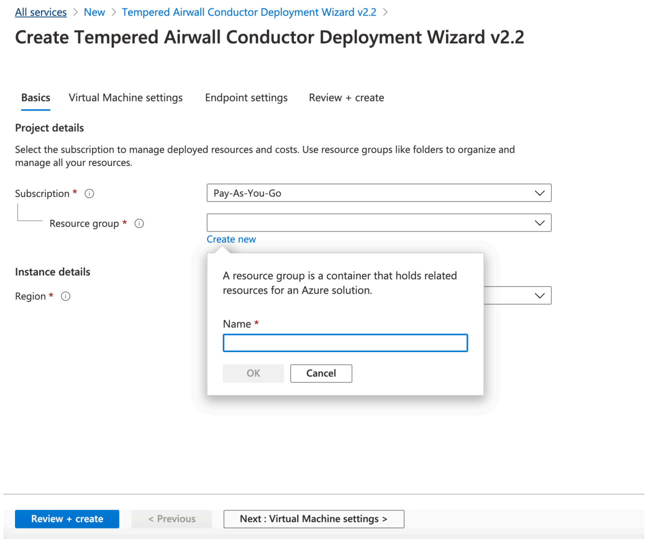
By Tempered Networks, Inc

Tempered Airwall Conductor Orchestration Engine Deployment Wizard version 2.2

Price varies

3. On the **Create Tempered Airwall Conductor Managed 2.2** page, **Basics** tab:

Subscription	Select your subscription model from the drop-down.
Resource group	Create a resource group for your virtual network. To do this click **Create New**, enter a new name, and click **OK**.
Region	Select the region for this instance.



All services > New > Tempered Airwall Conductor Deployment Wizard v2.2 >

Create Tempered Airwall Conductor Deployment Wizard v2.2

Basics | Virtual Machine settings | Endpoint settings | Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *: Pay-As-You-Go

Resource group *:

Create new

A resource group is a container that holds related resources for an Azure solution.

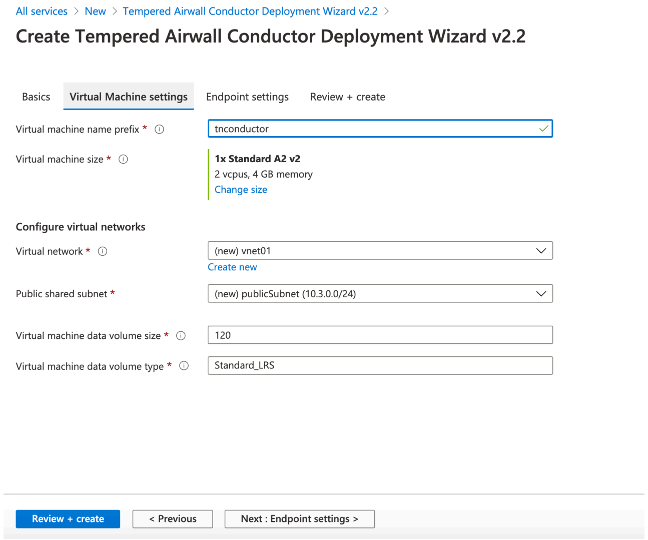
Name *

Instance details

Region *

4. Select **Next: Virtual Machine Settings**. On the **Virtual Machine settings** tab:

Virtual Machine name	Enter a prefix for the virtual machine.
Configure virtual networks	Select or create a Virtual network.
Public shared subnet	Select a public subnet from the virtual network you selected.



All services > New > Tempered Airwall Conductor Deployment Wizard v2.2 >

Create Tempered Airwall Conductor Deployment Wizard v2.2

Basics | Virtual Machine settings | Endpoint settings | Review + create

Virtual machine name prefix *: tnconductor

Virtual machine size *: 1x Standard A2 v2, 2 vcpus, 4 GB memory

Change size

Configure virtual networks

Virtual network *: (new) vnet01

Create new

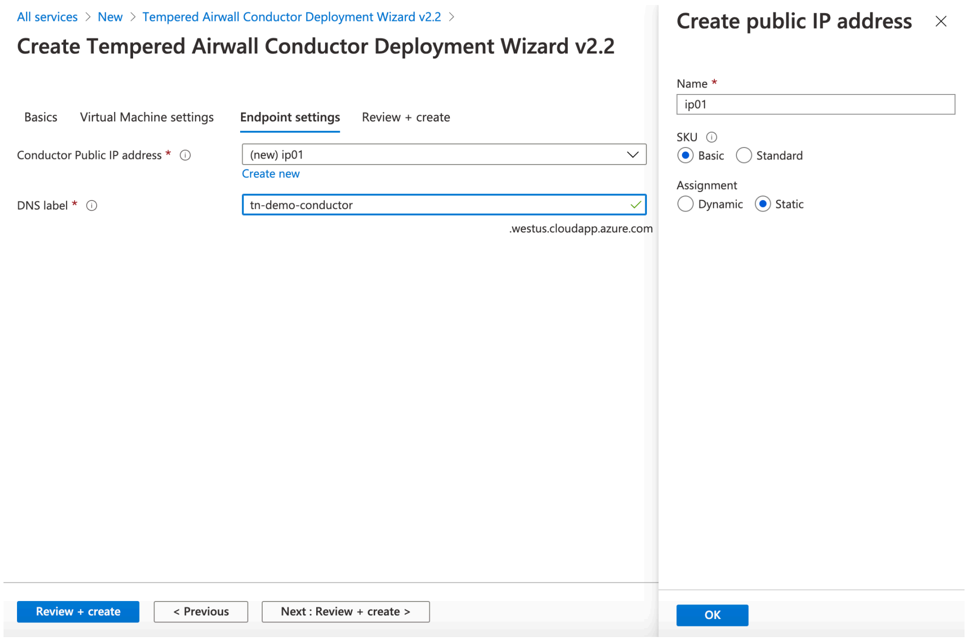
Public shared subnet *: (new) publicSubnet (10.3.0.0/24)

Virtual machine data volume size *: 120

Virtual machine data volume type *: Standard_LRS

5. Select **Next: Endpoint settings**. On the Endpoint Settings page:

Conductor Public IP address	Select **Create new**, then under **Create public IP address**, set **SKU** to **Basic** and **Assignment** to **Static**, and select **OK**.
DNS label	Enter a prefix for the DNS name. Check to make sure you get the green check, indicating the name is valid.



All services > New > Tempered Airwall Conductor Deployment Wizard v2.2 >

Create Tempered Airwall Conductor Deployment Wizard v2.2

Conductor Public IP address * ⓘ (new) ip01
Create new

DNS label * ⓘ tn-demo-conductor ✓
.westus.cloudapp.azure.com

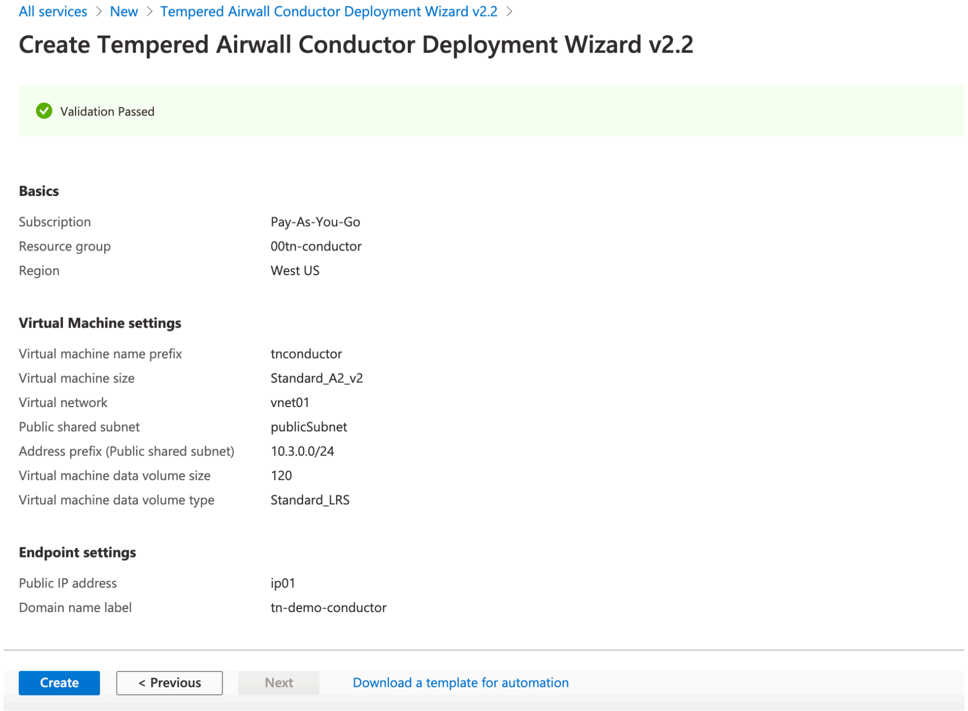
Create public IP address ×

Name *
ip01

SKU ⓘ
● Basic ○ Standard

Assignment
○ Dynamic ● Static

6. Select **Next: Review + create**.
7. Review your settings, and accept the Terms of Use, and then select **Create**. Azure starts deploying your image to the resource group you specified.



All services > New > Tempered Airwall Conductor Deployment Wizard v2.2 >

Create Tempered Airwall Conductor Deployment Wizard v2.2

✓ Validation Passed

Basics

Subscription	Pay-As-You-Go
Resource group	00tn-conductor
Region	West US

Virtual Machine settings

Virtual machine name prefix	tnconductor
Virtual machine size	Standard_A2_v2
Virtual network	vnet01
Public shared subnet	publicSubnet
Address prefix (Public shared subnet)	10.3.0.0/24
Virtual machine data volume size	120
Virtual machine data volume type	Standard_LRS

Endpoint settings

Public IP address	ip01
Domain name label	tn-demo-conductor

Step 3: Verify the install

At this point the Conductor instance is running in your cloud provider.

To verify, paste your Conductor IP into a browser window. It should show you the Initial Conductor Configuration page. To log in, configure, and license your Conductor, see Log in and Configure the Conductor on page 201.

Note: In v2.2.8 and earlier, it shows the Provisioning page. See License and Provision a Conductor (v2.2.8 and earlier) on page 191.

It may take several minutes for the Conductor to become available after it starts, so if you attempt to access it and your browser appears to stop responding, please try again in a few minutes.

Note: When running the Conductor for the first time, you may receive notifications indicating the connection is not private. Once you have finished configuring the Conductor, you can install a custom certificate on the Conductor that prevents these notifications in the future.

1. When Azure finishes deploying, it takes you to the Conductor instance. Leave this page up as you verify the install. Navigate to **Outputs**, and next to **publicIp**, select the copy icon to copy the public IP for your cloud Conductor.
2. Go to a web browser, enter in the IP you copied, and bypass the security warning.
3. Sign in to the Conductor:
   a) Go back to Azure Outputs page, and next to **conductorPassword**, click the copy icon to copy the Conductor password.

      Note: If you do not see a password on this page, it is likely you are not using the Managed image.

   b) Enter username: `admin`, and the password you copied. The default is `Tnw-<privateIpOfPublicNic>`.
   c) Change your password when prompted.
4. The Conductor starts the Initial Conductor Configuration wizard. To log in, configure, and license your Conductor, see Log in and Configure the Conductor on page 201.

   Note: In v2.2.8 and earlier, it shows the Provisioning page. See License and Provision a Conductor (v2.2.8 and earlier) on page 191.
5. When you've finished configuring, licensing, and provisioning your Conductor, you can sign in to start using or continuing configuring your Conductor.

For more information, see:

- License and Provision a Conductor (v2.2.8 and earlier) on page 191
- Log in and Configure the Conductor on page 201
- Add Airwall Edge Service Licenses to the Conductor on page 192
- Conductor Configuration Wizard Settings on page 197

Verify, Configure, Provision, and License a Cloud Conductor

At this point the Conductor instance is running in your cloud provider.

To verify, paste your Conductor IP into a browser window. It should show you the Initial Conductor Configuration page. To log in, configure, and license your Conductor, see Log in and Configure the Conductor on page 201.

Note: In v2.2.8 and earlier, it shows the Provisioning page. See License and Provision a Conductor (v2.2.8 and earlier) on page 191.

It may take several minutes for the Conductor to become available after it starts, so if you attempt to access it and your browser appears to stop responding, please try again in a few minutes.

Here are the default passwords for cloud Conductors. You are prompted to change the password as soon as you log in:

- **Alibaba Cloud** – Tnw-<instanceID>
- **Amazon Web Services** – Tnw-<instanceID>
- **Microsoft Azure** – Tnw-<privateIpOfPublicNic>
- **Google Cloud** – Tnw-<instanceID>

Note: In Microsoft Azure, if you do not see a password on the Azure Outputs page next to **conductorPassword**, it is likely you are not using the Managed image.

Note: When running the Conductor for the first time, you may receive notifications indicating the connection is not private. Once you have finished configuring the Conductor, you can install a custom certificate on the Conductor that prevents these notifications in the future.

For more information, see:

- **Conductor v2.2.8 and earlier only** – License and Provision a Conductor (v2.2.8 and earlier) on page 191
- Log in and Configure the Conductor on page 201
- Add Airwall Edge Service Licenses to the Conductor on page 192
- Conductor Configuration Wizard Settings on page 197

Additional Information

Once your Conductor is installed, you can configure and manage it as you would a physical Conductor. See Configure a Conductor on page 235. For additional help, you can accesssearch **Airwall help** by using the search bar at the top of the page or the navigation links to the left.

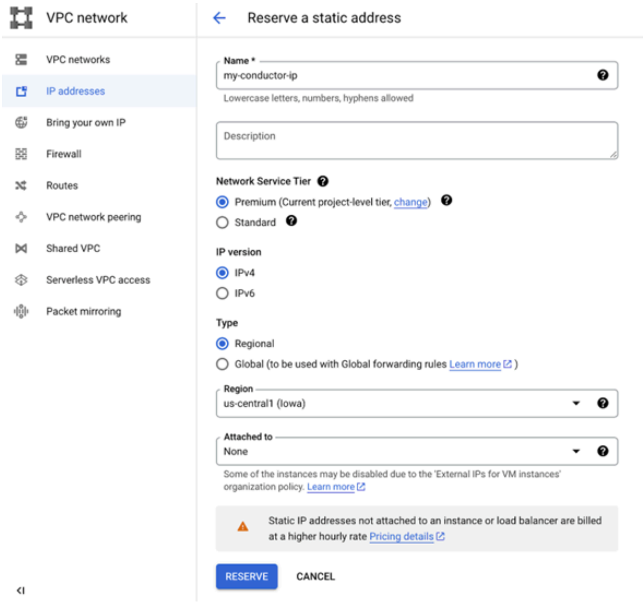
Deploy a Conductor on the Google Cloud Platform (GCP)

You can deploy an Airwall Conductor on GCP to manage physical, virtual, and cloud Airwall Edge Services, and Airwall Agents. Use the following steps to deploy a Conductor using the GCP marketplace. Alternatively, see Manually deploy a Conductor on the Google Cloud Platform (GCP) on page 219 if you require a special configuration.

Prerequisites

- A Google Cloud account with billing information set up. If you do not have an account, you can create a free Google Cloud account and upgrade it to a full account later.
- A Google Cloud project. Use an existing project, or see Create and configure a project on page 219.
- A Conductor license voucher to start the Conductor and verify it is set up correctly. Fulfillment provide this to you in an email once your purchase is complete.

1. Log on to Google Cloud Platform and click into your project.
2. Navigate to the External IP addresses page. Click **Reserve External Address**.
3. Specify the **Name** and selct the **Region** where your instance will be deployed. Click **Reserve**.



Reserve a static address

Name *
my-conductor-ip
Lowercase letters, numbers, hyphens allowed

Description

Network Service Tier
● Premium (Current project-level tier, change)
○ Standard

IP version
● IPv4
○ IPv6

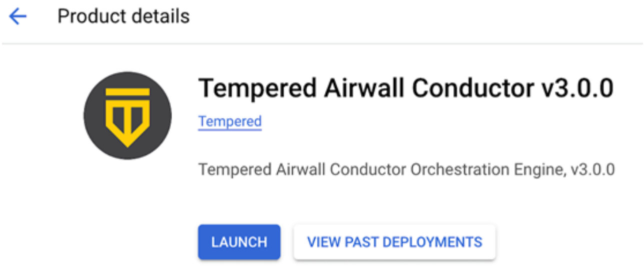
Type
● Regional
○ Global (to be used with Global forwarding rules Learn more)

Region
us-central1 (Iowa)

Attached to
None
Some of the instances may be disabled due to the 'External IPs for VM instances' organization policy. Learn more

Static IP addresses not attached to an instance or load balancer are billed at a higher hourly rate Pricing details

4. Navigate to the Tempered Airwall Conductor marketplace page. Alternatively, enter Tempered Airwall Conductor in the search bar.



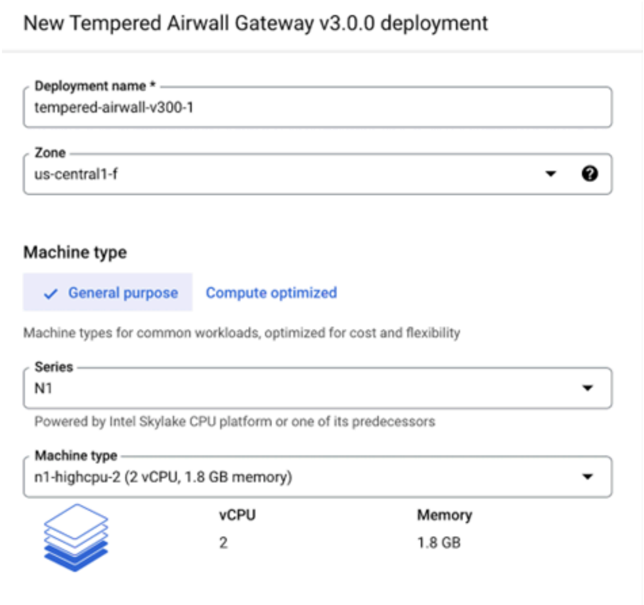
Product details

Tempered Airwall Conductor v3.0.0

Tempered

Tempered Airwall Conductor Orchestration Engine, v3.0.0

5. Click **Launch**. Sign in with your Google Cloud provider account details.
6. Specify the **Deployment name**. **Select Zone**, **Machine type**, **Data disk type**, and **Data disk size**.



New Tempered Airwall Gateway v3.0.0 deployment

Deployment name *: tempered-airwall-v300-1

Zone: us-central1-f

Machine type

✓ General purpose | Compute optimized

Machine types for common workloads, optimized for cost and flexibility

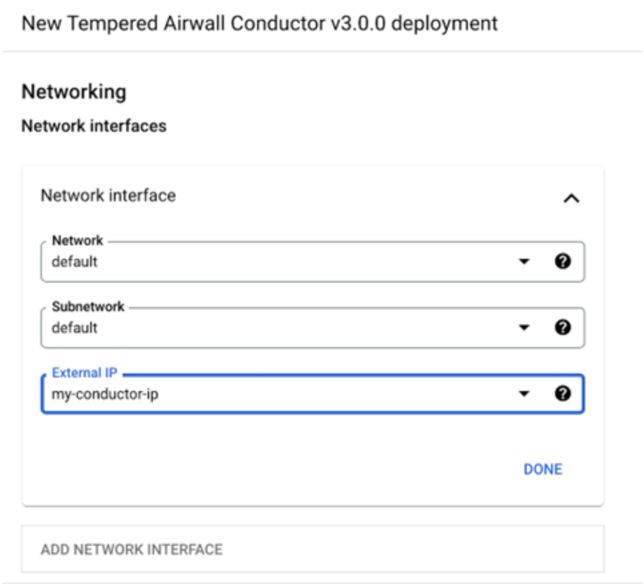
Series: N1

Powered by Intel Skylake CPU platform or one of its predecessors

Machine type: n1-highcpu-2 (2 vCPU, 1.8 GB memory)

vCPU	Memory
2	1.8 GB

7. Select **Network** and **Subnetwork** for your network interface. From the dropdown menu, select the External IP address that you created in step 3.



New Tempered Airwall Conductor v3.0.0 deployment

Networking

Network interfaces

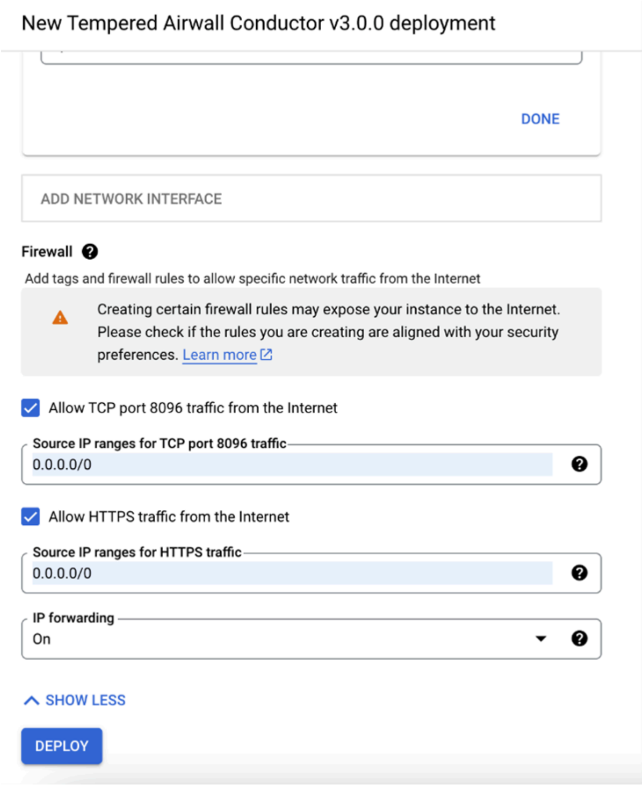
Network interface

Network: default

Subnetwork: default

External IP: my-conductor-ip

8. Specify the **Source IP ranges for TCP port 8096** and **HTTPS traffic**. Click **Deploy**.



New Tempered Airwall Conductor v3.0.0 deployment

Firewall

Add tags and firewall rules to allow specific network traffic from the Internet

Creating certain firewall rules may expose your instance to the Internet. Please check if the rules you are creating are aligned with your security preferences. Learn more

☑ Allow TCP port 8096 traffic from the Internet

Source IP ranges for TCP port 8096 traffic: 0.0.0.0/0

☑ Allow HTTPS traffic from the Internet

Source IP ranges for HTTPS traffic: 0.0.0.0/0

IP forwarding: On

Verify, Configure, Provision, and License a Cloud Conductor

At this point the Conductor instance is running in your cloud provider.

To verify, paste your Conductor IP into a browser window. It should show you the Initial Conductor Configuration page. To log in, configure, and license your Conductor, see Log in and Configure the Conductor on page 201.

Note: In v2.2.8 and earlier, it shows the Provisioning page. See License and Provision a Conductor (v2.2.8 and earlier) on page 191.

It may take several minutes for the Conductor to become available after it starts, so if you attempt to access it and your browser appears to stop responding, please try again in a few minutes.

Here are the default passwords for cloud Conductors. You are prompted to change the password as soon as you log in:

- **Alibaba Cloud** – Tnw-<instanceID>
- **Amazon Web Services** – Tnw-<instanceID>
- **Microsoft Azure** – Tnw-<privateIpOfPublicNic>
- **Google Cloud** – Tnw-<instanceID>

Note: In Microsoft Azure, if you do not see a password on the Azure Outputs page next to **conductorPassword**, it is likely you are not using the Managed image.

Note: When running the Conductor for the first time, you may receive notifications indicating the connection is not private. Once you have finished configuring the Conductor, you can install a custom certificate on the Conductor that prevents these notifications in the future.

For more information, see:

- **Conductor v2.2.8 and earlier only** – License and Provision a Conductor (v2.2.8 and earlier) on page 191
- Log in and Configure the Conductor on page 201
- Add Airwall Edge Service Licenses to the Conductor on page 192
- Conductor Configuration Wizard Settings on page 197

Additional Information

Once your Conductor is installed, you can configure and manage it as you would a physical Conductor. See Configure a Conductor on page 235. For additional help, you can accesssearch **Airwall help** by using the search bar at the top of the page or the navigation links to the left.

Manually deploy a Conductor on the Google Cloud Platform (GCP)

You can deploy an Airwall Conductor on GCP and manage physical, virtual, and cloud Airwall Edge Services, and Airwall Agents. Use the following steps to manually deploy on the Google Cloud platform. If you do not require any special configuration, see Deploy a Conductor on the Google Cloud Platform (GCP) with marketplace.

Prerequisites

To get started, make sure you have access to your Google Cloud account. If you do not have an account, you can create a free Google Cloud account and upgrade it to a full account later. If you have an existing Google Cloud account, make sure your billing information is set up. You cannot create a project until you are able to link your billing information to your newly created project.

Note: You should be familiar with using Google Cloud before attempting to deploy a Tempered Conductor or Airwall Gateway on the platform. To get started, we recommend you review the following content offered by Google:

- Google Cloud Platform Overview
- Google Cloud Storage
- Virtual Private Cloud
- Google Compute Engine Documentation

A Conductor license voucher is necessary at the end of this procedure if you want to start the Conductor and verify it is set up correctly. Fulfillment will provide this to you in an email after your purchase is complete.

Log in to Google Cloud

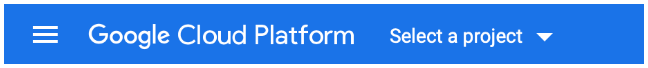
From a Web browser, navigate to https://console.cloud.google.com. You will see one of two pages, the **Getting Started** page if you have no projects or the **Home** page if you have existing projects.

Create and configure a project

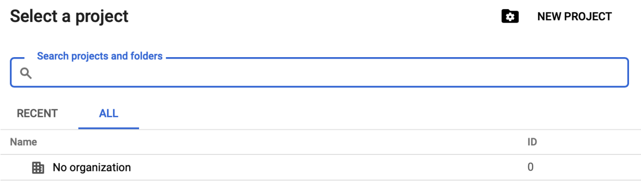
A Google Cloud project organizes all of your resources into a logical group for easier management. You will add the Tempered Conductor to a new or existing project, so you need to have a project created before you deploy the Conductor.

Note: If you are adding the Conductor to an existing project, you can skip step 2 and proceed directly to step 3 in this document.

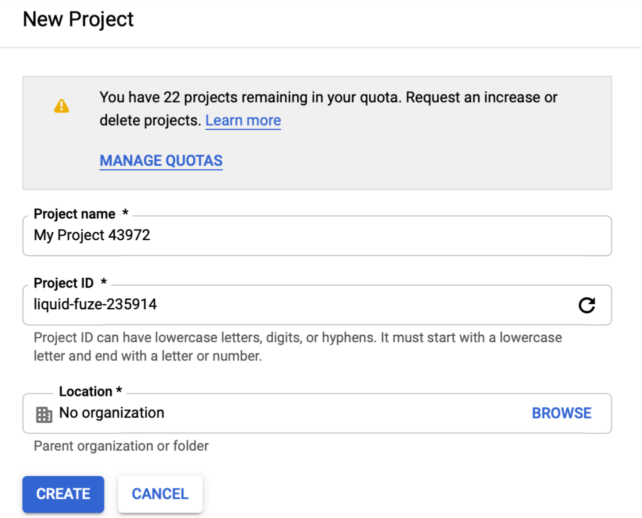
1. On the top bar of the Google Cloud page, click **Select a project**.



2. On the upper-right corner of the Select a project dialog, click **New Project**.



3. In the **Project Name** field, enter a name for your new project. By default, your new project is assigned a default ID, which you can change by clicking **Edit** to the right of the **Project ID** field.
4. Optional: If you want to add your project to an organization you have already created, select it in the **Location** field by clicking **Browse** to the right. For more information about organizations, see Quickstart Using Organizations in the Google Cloud documentation.



New Project

You have 22 projects remaining in your quota. Request an increase or delete projects. Learn more

MANAGE QUOTAS

Project name *
My Project 43972

Project ID *
liquid-fuze-235914

Project ID can have lowercase letters, digits, or hyphens. It must start with a lowercase letter and end with a letter or number.

Location *
No organization

Parent organization or folder

5. Once you are finished, click **Create**.

It will take a moment to set up your project. A notification window will indicate when the operation is complete. You can then select **Home** in the Google Cloud sidebar to access your dashboard.

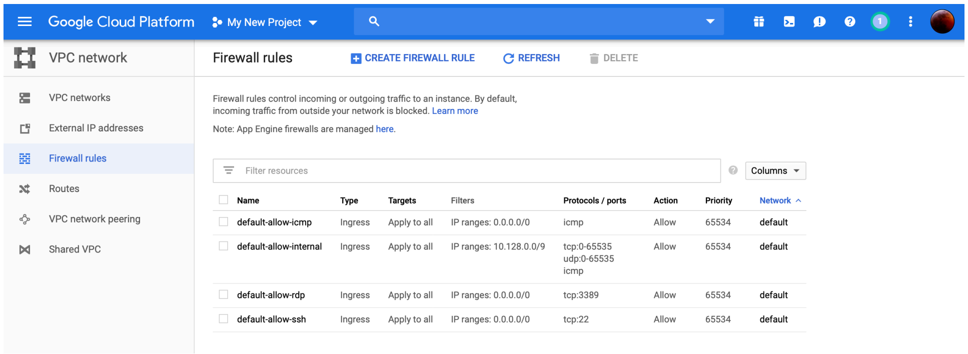
Set up firewall rules

GCP firewall rules will manage the traffic coming into your instance on a network. By default, you have a network with a default set of firewall rules for your region, and you will need to make a few changes to set up your environment so the Conductor can function correctly.

Note: This step assumes you are using the default network for your region. If you would like to create a separate virtual private cloud (VPC) network, please review the topic Virtual Private Cloud (VPC) Network Overview in the Google Cloud documentation.

To set up firewall rules:

1. In the Google Cloud sidebar, navigate to the **Networking** section, hover over **VPC network**, and select **Firewall rules**.

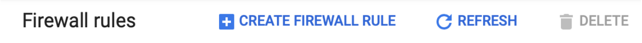


Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. Learn more

Note: App Engine firewalls are managed here.

Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network
default-allow-icmp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	icmp	Allow	65534	default
default-allow-internal	Ingress	Apply to all	IP ranges: 10.128.0.0/9	tcp:0-65535 udp:0-65535 icmp	Allow	65534	default
default-allow-rdp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:3389	Allow	65534	default
default-allow-ssh	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22	Allow	65534	default

2. Click **Create Firewall Rule**.



3. Fill in the **Create firewall rule** page with the following information:

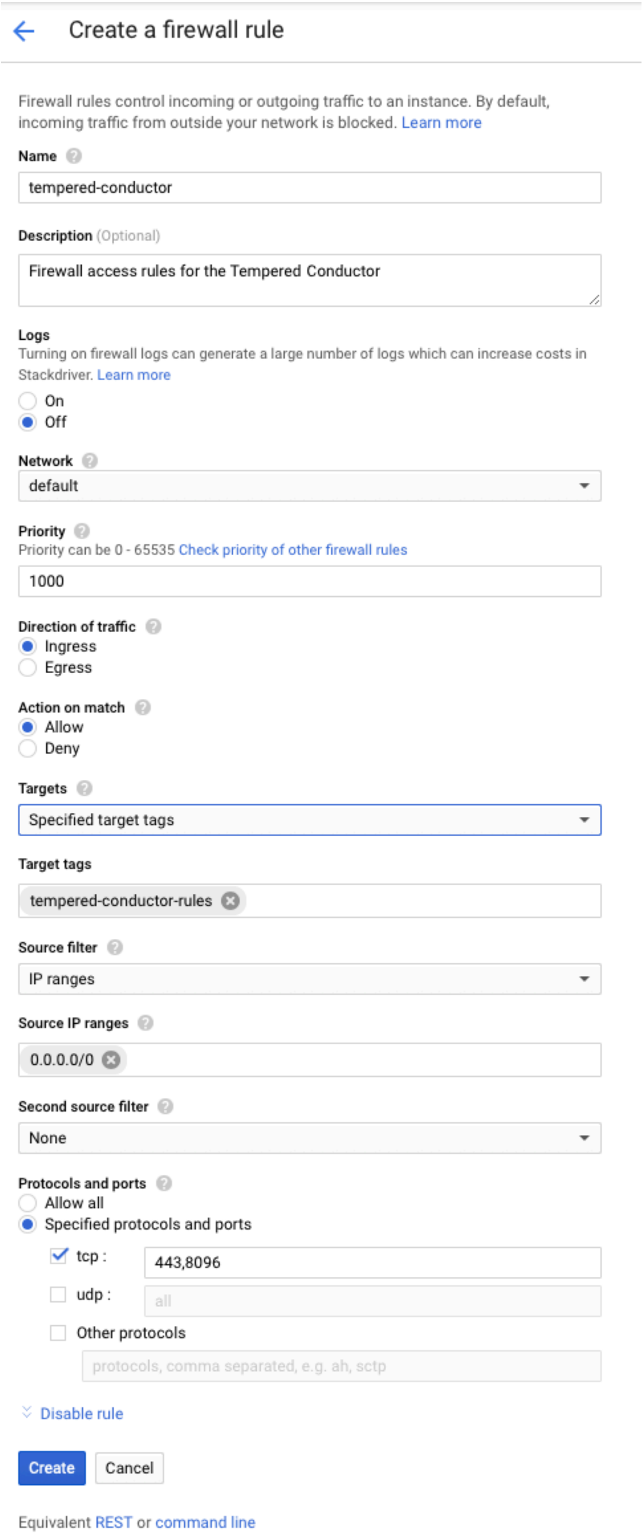
Name
You can use any name you choose, but it must be lowercase with no spaces.

Description
This can be anything you like. We recommend something descriptive such as **Firewall access rules for Tempered Conductor**.

Network	Select **default** from the drop-down unless you are using a different network.
Direction of traffic	Select the **Ingress** radio button.
Action on match	Select the **Allow** radio button.
Targets	Select Specific target tags from the drop-down.
Target tags	Enter **tempered-conductor-rules** **Note:** Remember this tag. You will need it later in this procedure.
Source filter	Select **IP ranges** from the drop-down.
Source IP ranges	Enter **0.0.0.0/0**.
Protocols and ports	Select the **Specified protocols and ports** radio button and enter **443,8096**. **Note:** Do not check the box next to **tcp** and then select the field to enter your ports – the box will revert to unchecked and disable both fields. Click only on the field to enter your ports.

Leave all other fields as is.

Your page should look similar to the image below:



← Create a firewall rule

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. Learn more

Name: tempered-conductor

Description (Optional): Firewall access rules for the Tempered Conductor

Logs
Turning on firewall logs can generate a large number of logs which can increase costs in Stackdriver. Learn more
○ On
● Off

Network: default

Priority
Priority can be 0 - 65535 Check priority of other firewall rules
1000

Direction of traffic
● Ingress
○ Egress

Action on match
● Allow
○ Deny

Targets: Specified target tags

Target tags: tempered-conductor-rules

Source filter: IP ranges

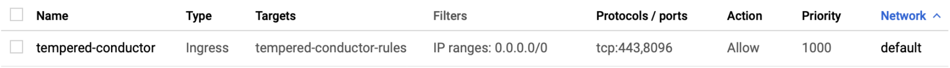
Source IP ranges: 0.0.0.0/0

Second source filter: None

Protocols and ports
○ Allow all
● Specified protocols and ports
☑ tcp : 443,8096
□ udp : all
□ Other protocols
protocols, comma separated, e.g. ah, sctp

Equivalent REST or command line

4. Click **Create**. It will take a moment to finish the operation. Once complete, you should see the following in your rules list:



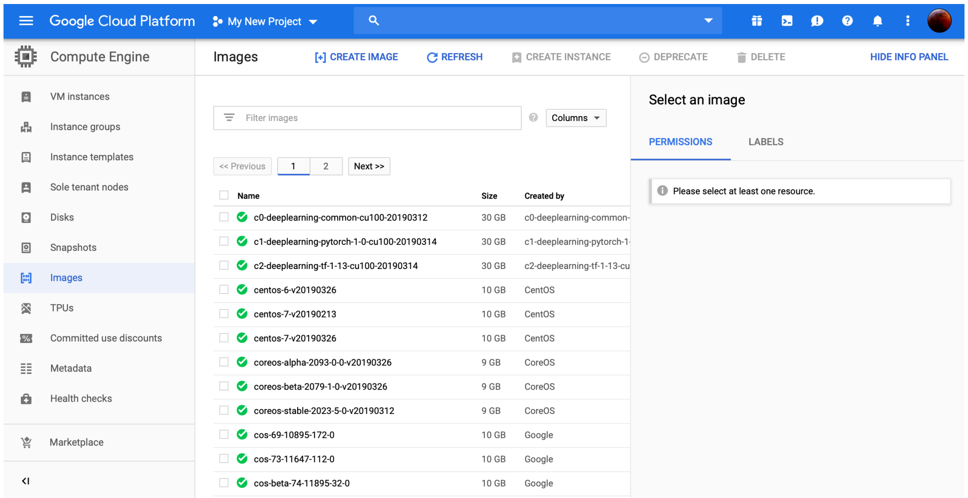
□	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network ^
□	tempered-conductor	Ingress	tempered-conductor-rules	IP ranges: 0.0.0.0/0	tcp:443,8096	Allow	1000	default

Add a Conductor Image

Add a Conductor image to create an instance in your Google Cloud project.

To add an image:

1. In the Google Cloud sidebar, navigate to the **Compute** section, hover over **Compute Engine**, and select **Images**.



Please select at least one resource.

Name	Size	Created by
c0-deeplearning-common-cu100-20190312	30 GB	c0-deeplearning-common-
c1-deeplearning-pytorch-1-0-cu100-20190314	30 GB	c1-deeplearning-pytorch-1-
c2-deeplearning-tf-1-13-cu100-20190314	30 GB	c2-deeplearning-tf-1-13-cu
centos-6-v20190326	10 GB	CentOS
centos-7-v20190213	10 GB	CentOS
centos-7-v20190326	10 GB	CentOS
coreos-alpha-2093-0-0-v20190326	9 GB	CoreOS
coreos-beta-2079-1-0-v20190326	9 GB	CoreOS
coreos-stable-2023-5-0-v20190312	9 GB	CoreOS
cos-69-10895-172-0	10 GB	Google
cos-73-11647-112-0	10 GB	Google
cos-beta-74-11895-32-0	10 GB	Google

2. Click **Create Image**.

Images
[+] CREATE IMAGE
REFRESH
CREATE INSTANCE
DEPRECATE
DELETE

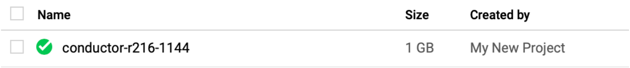
3. Fill in the **Create an image** page with the following information:

Name	Enter **conductor-r300-1721**.
Description	Enter Tempered Conductor **version 3.0.0**.
Source	Select **Cloud Storage file** from the drop-down.
Cloud Storage File	Enter **tempered-image-storage/conductor-r300-1721.tar.gz**.

You can leave all other fields as they are.

4. Click **Create**. It will take a moment to finish the operation.

Once complete, you should see the following in your images list:



Name	Size	Created by
conductor-r216-1144	1 GB	My New Project

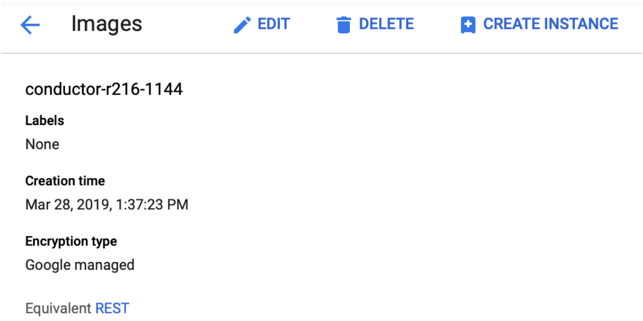
Note: If you have multiple projects, make sure the image is associated with your desired project, listed in the **Created by** column.

Create a Conductor Instance

The Conductor image can now be used to create a virtual machine instance. The image supplied by Tempered contains the Conductor and is relatively small in size. Configuration information and storage requires a second hard disk, which you will set up as part of the instructions below. This image must be a minimum of 120 GB.

To create a Conductor instance:

1. Select the image in the list by clicking on its name. You have several options available: Select **Create Instance**.



← Images   EDIT   DELETE   CREATE INSTANCE

conductor-r216-1144

Labels
None

Creation time
Mar 28, 2019, 1:37:23 PM

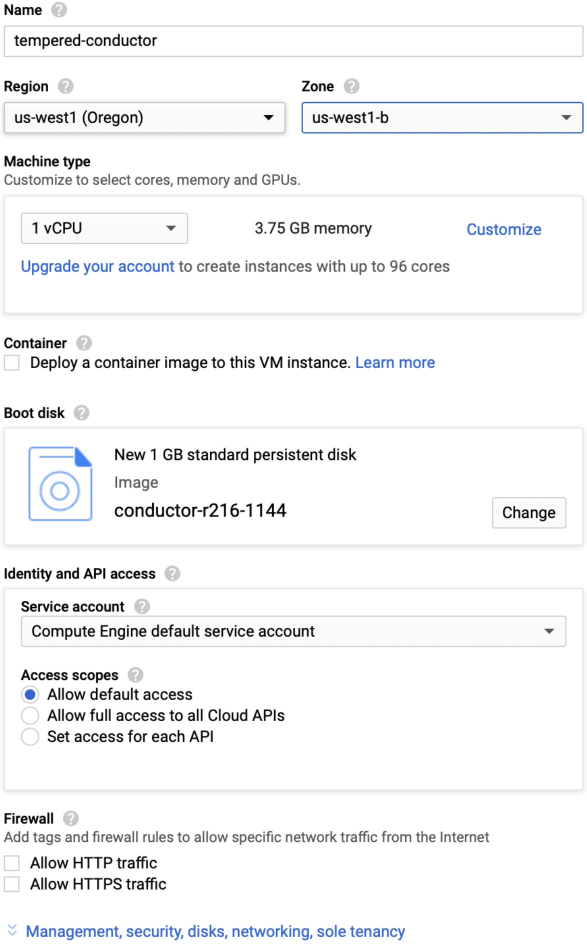
Encryption type
Google managed

Equivalent REST

2. Fill in the **Create an instance** page with the following information:

Name	Enter a name of your choice, but it must be lower case and without spaces.
Region	Select the region of your choice from the drop-down.
Zone	Select the zone of your choice from the drop-down.

You can leave all other fields as is.



Name
tempered-conductor

Region
us-west1 (Oregon)

Zone
us-west1-b

Machine type
Customize to select cores, memory and GPUs.

1 vCPU   3.75 GB memory   Customize

Upgrade your account to create instances with up to 96 cores

Container
□ Deploy a container image to this VM instance. Learn more

Boot disk
New 1 GB standard persistent disk
Image
conductor-r216-1144
Change

Identity and API access

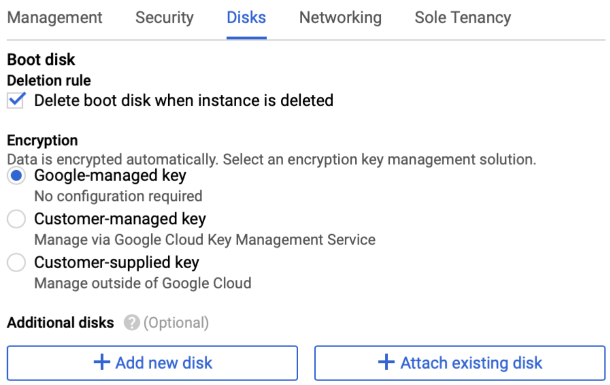
Service account
Compute Engine default service account

Access scopes
● Allow default access
○ Allow full access to all Cloud APIs
○ Set access for each API

Firewall
Add tags and firewall rules to allow specific network traffic from the Internet
□ Allow HTTP traffic
□ Allow HTTPS traffic

Management, security, disks, networking, sole tenancy

3. Click **Management, security, disks, networking, sole tenancy**.
4. On the **Disks** tab, leave all settings as is and click **+ Add new disk**.



Boot disk

Deletion rule

☑ Delete boot disk when instance is deleted

Encryption

Data is encrypted automatically. Select an encryption key management solution.

● Google-managed key
No configuration required

○ Customer-managed key
Manage via Google Cloud Key Management Service

○ Customer-supplied key
Manage outside of Google Cloud

Additional disks (Optional)

5. In the **New disk** dialog enter the following:

Name

You can leave this field as **disk 1**, otherwise enter a name of your choice.

Type

Select **Standard persistent disk** from the drop-down.

Source type

Select **Blank disk**.

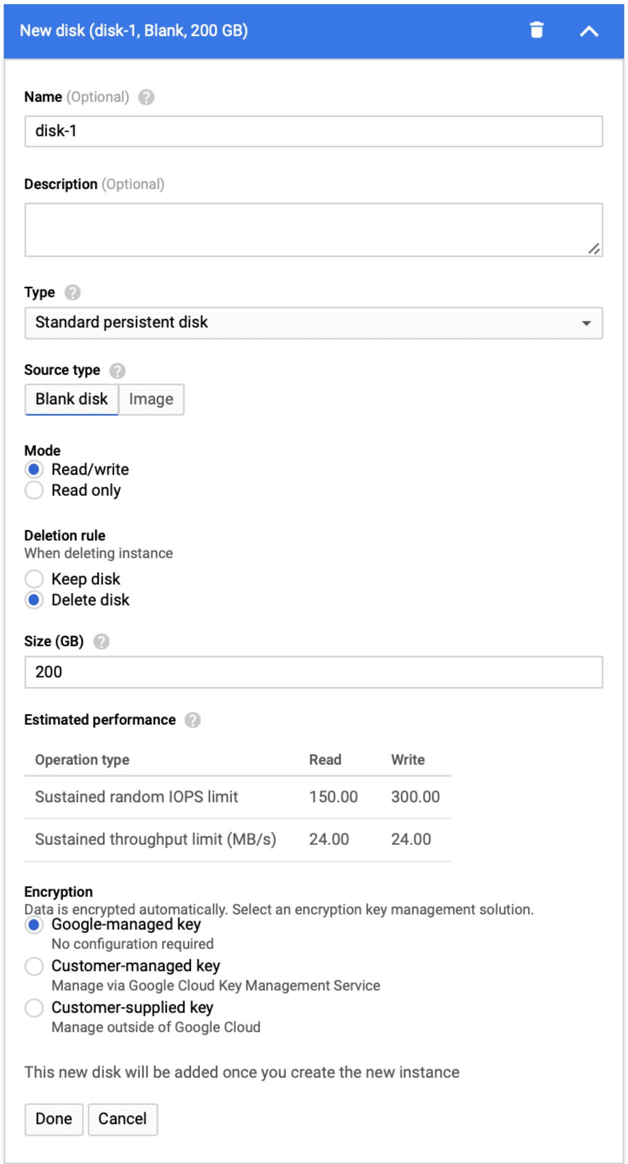
Deletion rule

Select the **Delete disk** radio button

Size (GB)

Enter the value **200**

You can leave all other settings as is.



New disk (disk-1, Blank, 200 GB)

Name (Optional)

disk-1

Description (Optional)

Type

Standard persistent disk

Source type

Blank disk | Image

Mode

● Read/write
○ Read only

Deletion rule

When deleting instance

○ Keep disk
● Delete disk

Size (GB)

200

Estimated performance

Operation type	Read	Write
Sustained random IOPS limit	150.00	300.00
Sustained throughput limit (MB/s)	24.00	24.00

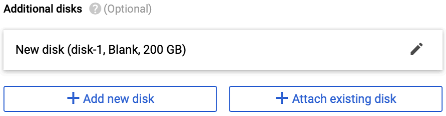
Encryption

Data is encrypted automatically. Select an encryption key management solution.

● Google-managed key
No configuration required
○ Customer-managed key
Manage via Google Cloud Key Management Service
○ Customer-supplied key
Manage outside of Google Cloud

This new disk will be added once you create the new instance

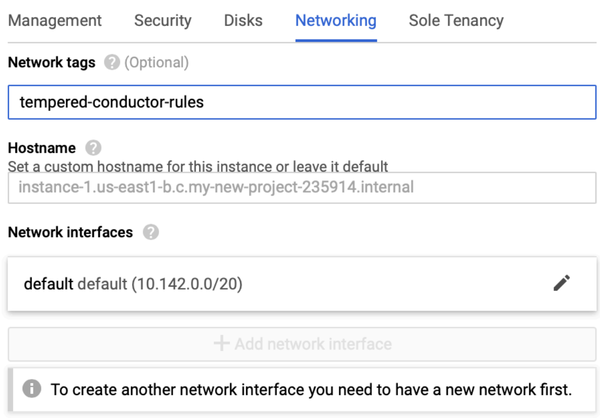
6. Click **Done**. The dialog will close, and you should see the following:



Additional disks (Optional)

New disk (disk-1, Blank, 200 GB)

7. Click the **Networking** tab to the right of the **Disk** tab and enter the tag name you created for your firewall rules in step 3.



Network tags (Optional)

tempered-conductor-rules

Hostname

Set a custom hostname for this instance or leave it default

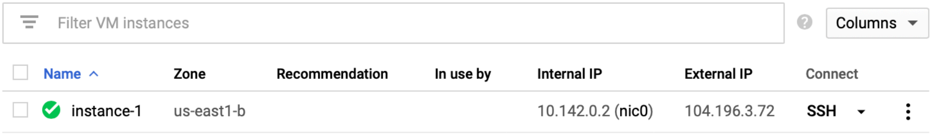
instance-1.us-east1-b.c.my-new-project-235914.internal

Network interfaces

default default (10.142.0.0/20)

To create another network interface you need to have a new network first.

8. Click **Create**. It will take a moment to finish the operation. Once complete, you should see the following:



	Name	Zone	Recommendation	In use by	Internal IP	External IP	Connect
□	✓ instance-1	us-east1-b			10.142.0.2 (nic0)	104.196.3.72	SSH

Note: The **External IP** for your instance is the address you will use to connect to the Conductor.

Verify, Configure, Provision, and License a Cloud Conductor

At this point the Conductor instance is running in your cloud provider.

To verify, paste your Conductor IP into a browser window. It should show you the Initial Conductor Configuration page. To log in, configure, and license your Conductor, see Log in and Configure the Conductor on page 201.

Note: In v2.2.8 and earlier, it shows the Provisioning page. See License and Provision a Conductor (v2.2.8 and earlier) on page 191.

It may take several minutes for the Conductor to become available after it starts, so if you attempt to access it and your browser appears to stop responding, please try again in a few minutes.

Here are the default passwords for cloud Conductors. You are prompted to change the password as soon as you log in:

- **Alibaba Cloud** – Tnw-<instanceID>
- **Amazon Web Services** – Tnw-<instanceID>
- **Microsoft Azure** – Tnw-<privateIpOfPublicNic>
- **Google Cloud** – Tnw-<instanceID>

Note: In Microsoft Azure, if you do not see a password on the Azure Outputs page next to **conductorPassword**, it is likely you are not using the Managed image.

Note: When running the Conductor for the first time, you may receive notifications indicating the connection is not private. Once you have finished configuring the Conductor, you can install a custom certificate on the Conductor that prevents these notifications in the future.

For more information, see:

- **Conductor v2.2.8 and earlier only** – License and Provision a Conductor (v2.2.8 and earlier) on page 191
- Log in and Configure the Conductor on page 201
- Add Airwall Edge Service Licenses to the Conductor on page 192
- Conductor Configuration Wizard Settings on page 197

Additional Information

Once your Conductor is installed, you can configure and manage it as you would a physical Conductor. See Configure a Conductor on page 235. For additional help, you can accesssearch **Airwall help** by using the search bar at the top of the page or the navigation links to the left.

Conductor for Google Cloud Platform Quick Start

To get started, make sure you have access to your Google Cloud account. If you do not have an account, you can create a free Google Cloud account and upgrade it to a full account later. If you have an existing Google Cloud account, make sure your billing information is set up. You cannot create a project until you are able to link your billing information to your newly created project.

A Conductor license voucher is necessary at the end of this procedure if you want to start the Conductor and verify it is set up correctly. Fulfillment will provide this to you in an email after your purchase is complete.

Log in to Google Cloud

From a Web browser, navigate to https://console.cloud.google.com. You will see one of two pages, the **Getting Started** page if you have no projects or the **Home** page if you have existing projects.

Step 2: Select the Tempered Conductor from the Marketplace

Select the Conductor in the Google Cloud Marketplace.

1. From your GCP Dashboard, select **Marketplace** on the left sidebar.
2. In the **Search** field at the top of the page, enter `tempered networks conductor` and press enter.
3. In the results list, locate and select **Tempered Networks Conductor v2.1**.

The product page opens where you can deploy the Conductor.

Step 3: Install the Conductor Image

1. On the product page, click **LAUNCH ON COMPUTE ENGINE**.
2. The Conductor deployment uses a template so most settings you can leave as is, however you may want to make the following changes:
   a) **Deployment name**: Enter a name for your Conductor.
   b) **Zone**: Select a zone from the drop-down. The zone determines what computing resources are available and where your data is stored and used.
   c) **Machine type**: Leave as is. Machine type determines the amount of memory, virtual cores, and persistent disk limits for the Conductor. The default settings are required for the Conductor to function correctly.
   d) **Data Disk**: Leave the **Data disk type** and **Data disk size in GB** fields as is.
   e) Networking: Leave the **Network**, **Subnetwork**, **External IP**, **Firewall**, and **IP forwarding** fields as is.

   Note: Some fields may be hidden based on your screen size. To view these fields, click **More** just above the **Deploy** button.
3. Click **Deploy**.

Step 4: Finalize the Deployment

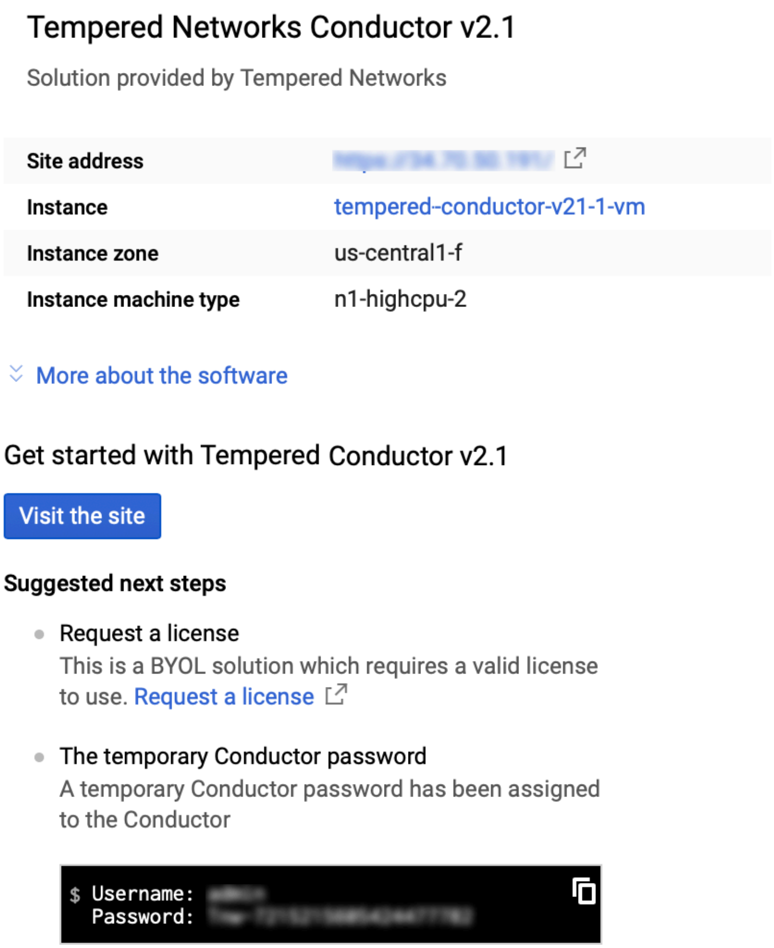
It will take a few moments for the process to complete. You can view the progress of your deployment by viewing the tree hierarchy of you components on the page.

Once complete, the message changes indicating your deployment is complete.

Step 5: Obtain your Conductor Address and Credentials

When your Conductor finishes installing, its information appears in the right pane of the page. You need three pieces of this information to log in to your Conductor for the first time: your Conductor site address, username, and temporary password.

Conductor site address	Copy from **Site address**, or click **Visit the site** to open it in your browser.
Username and password	Copy from the shaded box near the bottom.



Tempered Networks Conductor v2.1

Solution provided by Tempered Networks

Site address	[redacted]
Instance	tempered-conductor-v21-1-vm
Instance zone	us-central1-f
Instance machine type	n1-highcpu-2

More about the software

Get started with Tempered Conductor v2.1

Visit the site

Suggested next steps

- Request a license
  This is a BYOL solution which requires a valid license to use. Request a license
- The temporary Conductor password
  A temporary Conductor password has been assigned to the Conductor

```
$ Username: [redacted]
  Password: [redacted]
```

Step 6: Verify the install

At this point the Conductor instance is running in Google Cloud. You should verify it is installed correctly by logging in and licensing the Conductor. It may take several minutes for the Conductor to become available after it starts, so if you attempt to access it and your browser appears to stop responding, please try again in a few minutes.

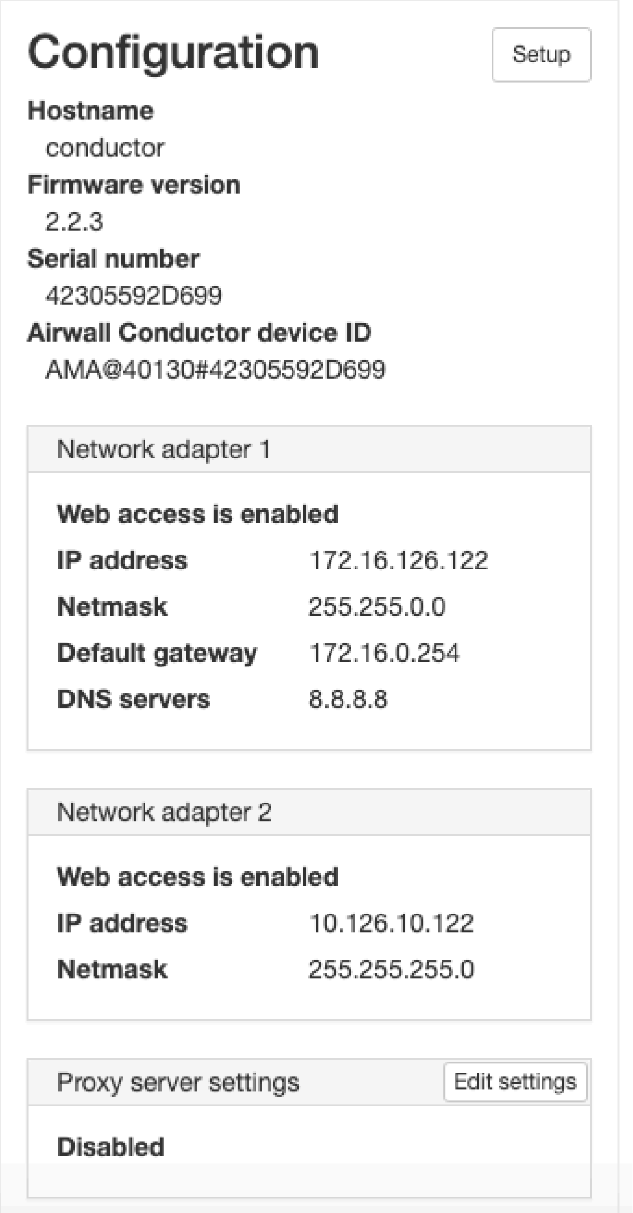
Note: When running the Conductor for the first time, you may receive notifications indicating the connection is not private. Once you have finished configuring the Conductor, you can install a customer certificate on the Conductor that preventd these notifications

To verify the install:

1. Point your web browser to the external IP address for your Conductor. Make sure you begin the address with *https://*.
2. An unlicensed Conductor will display the initial **Provisioning** page where you enter your license voucher.
3. Enter the voucher code you received from Tempered in the **Voucher code** field.
4. Click **Provision now**. It will take a moment to finish the operation. Once complete, you should see confirmation page.
5. Select **Click here to start using the** Conductor.
6. Enter the default username and password you received when you completed installation and click **Sign in**.
7. You will be prompted to enter a new password. Enter the default password in the **Current password** field and a new password of your choosing in the **New password** and **Confirm new password** fields.
8. Click **Update**.
9. On the System Configuration dialog, leave all the fields as is and click **Configure**.

10. It will take a moment to complete the operation. Once finished, click **Return to settings**.

You should see the Conductor **Settings** page. On the right side in the **Network adapter 1** section, the IP address should match the **Internal IP** of your instance in the GCP portal.



Configuration

Hostname
conductor

Firmware version
2.2.3

Serial number
42305592D699

Airwall Conductor device ID
AMA@40130#42305592D699

Network adapter 1

Web access is enabled

IP address	172.16.126.122
Netmask	255.255.0.0
Default gateway	172.16.0.254
DNS servers	8.8.8.8

Network adapter 2

Web access is enabled

IP address	10.126.10.122
Netmask	255.255.255.0

Proxy server settings

Disabled

Deploy a Conductor in VMware ESX/ESXi

Prerequisites

- An existing installation of VMware ESX/ESXi server version 6.5.0 and later
- A VMware open virtual appliance (OVA) for a Conductor or Airwall Gateway.

System Requirements

The following VMware ESX/ESXi server hardware is required:

Processor	• Minimum requirement of a single processor with hyper-threading support, VT-x technology, and 64-bit architecture.

- Optimum configuration is minimum 4 processing cores with hyper-threading support, VT-x technology, 64-bit architecture, and AES-NI enabled in the host's BIOS.

Virtual image

Below are the minimum configuration requirements available for a virtual Conductor or Airwall Gateway image:

Platform	Memory	Disk
Conductor	4GB	120GB*
Airwall Gateway	1GB	1GB*

* Already included in the default OVA package

To deploy a virtual Conductor

1. Deploy a new OVF template from within vSphere or vCenter. For most deployments, the default settings are sufficient.
2. Browse to the location of the downloaded OVA file.
3. Give the virtual machine a unique name and select its storage location.
4. Map the virtual machine's network interfaces with the correctly assigned port groups for the Conductor.
5. Disk provisioning can be set to **Thin Provisioned**
6. Verify the configuration, check **Power on after deployment**, and then click **Finish** to begin the update.

To configure the Conductor

An unlicensed, new VMware Conductor deploys with the default configuration.

- Network adapter 1 is configured with a static IP address of 192.168.56.2
- Network adapter 2 is configured for DHCP IP addressing

To determine the IP address assigned to network adapter 2, at the console, log in with name: `airsh`, and password: `airsh`, and then type `status`.

Run the Conductor web UI on either of the network adapters. To continue:

- **For a v2.2.10 and later Conductors**, see Log in and Configure the Conductor on page 201.
- **For v2.2.8 or earlier Conductors**, see License and Provision a Conductor (v2.2.8 and earlier) on page 191.

For more information, see:

- License and Provision a Conductor (v2.2.8 and earlier) on page 191
- Log in and Configure the Conductor on page 201
- Add Airwall Edge Service Licenses to the Conductor on page 192

Deploy a Conductor in Microsoft Hyper-V

The virtualization server role for Windows Server 2012 R2 or 2016 is called Hyper-V Manager. The following documentation show the steps to implement and manage a secure Conductor on Hyper-V.

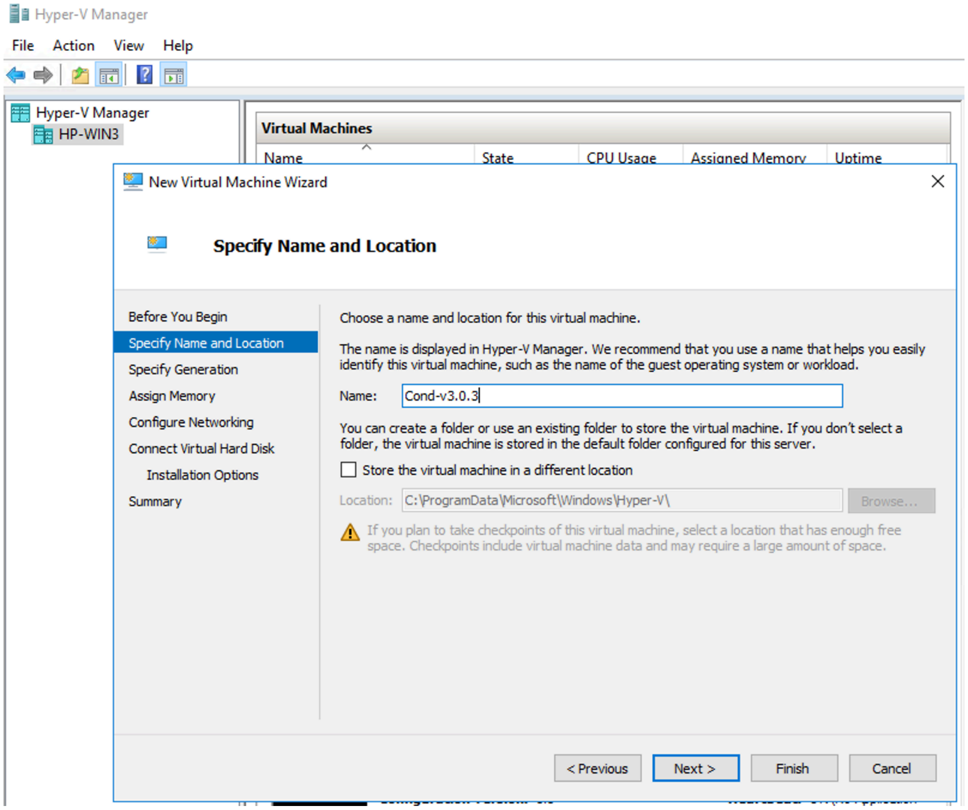
Prerequisites:

- An existing installation of Microsoft Hyper-V, v2012 or later.
- A Conductor virtual image (.vhdx). Request a Hyper-V Virtual Conductor .vhdx file from Customer Success.

Step 1: Create a new Conductor virtual machine

1. In Hyper-V Manager, under **Actions**, select **New** > **Virtual Machine**, and then select **Next**.

2. Give the Conductor a descriptive name (for example, Cond-v3.0.3), and select **Next**.



Specify Name and Location

Choose a name and location for this virtual machine.

The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name: Cond-v3.0.3

You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

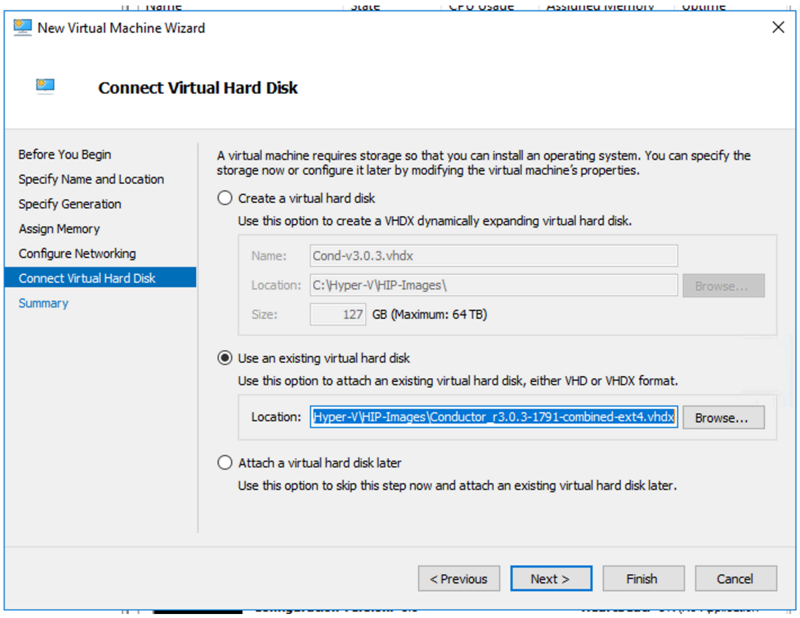
□ Store the virtual machine in a different location

Location: C:\ProgramData\Microsoft\Windows\Hyper-V\ Browse...

⚠ If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

3. Under **Specify Generation**, select **Generation 1**, and select **Next**.
4. Under **Assign Memory**:
   - **Startup Memory** – Enter no less than 8192 MB. Hardware Conductors ship with 8 GB or more.
   - **Use Dynamic Memory for this virtual machine** – Leave clear.

   Select **Next**.
5. Under **Configure Networking**, you will set that up later, so select **Next**.
6. Under **Connect Virtual Hard Disk**, select **Use an existing virtual hard disk** and then select **Browse**.



Connect Virtual Hard Disk

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

○ Create a virtual hard disk

Use this option to create a VHDX dynamically expanding virtual hard disk.

Name: Cond-v3.0.3.vhdx

Location: C:\Hyper-V\HIP-Images\ Browse...

Size: 127 GB (Maximum: 64 TB)

● Use an existing virtual hard disk

Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

Location: Hyper-V\HIP-Images\Conductor_r3.0.3-1791-combined-ext4.vhdx Browse...

○ Attach a virtual hard disk later

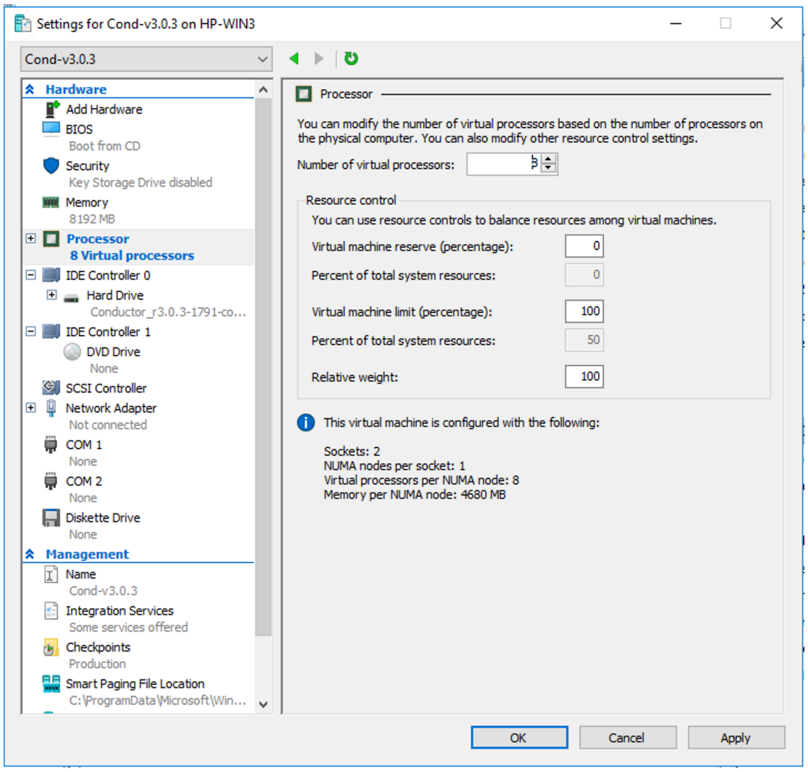
Use this option to skip this step now and attach an existing virtual hard disk later.

7. Go to and select the Conductor*.vhdx file you downloaded, and select **Open**.
8. Select **Next**, then **Finish**.

> **Important:** Do not start the virtual machine yet. You need to finish the configuration before you start it. If you already started it, you will need to delete the virtual machine and start over.

Step 2: Configure the Conductor virtual machine

1. With the new virtual machine selected, on the right, select **Settings**.
2. Open **Processor**, and under **Number of virtual processors**, select 8. Select **Apply**.



Settings for Cond-v3.0.3 on HP-WIN3

Cond-v3.0.3

Hardware
- Add Hardware
- BIOS
  Boot from CD
- Security
  Key Storage Drive disabled
- Memory
  8192 MB
- Processor
  8 Virtual processors
- IDE Controller 0
  - Hard Drive
    Conductor_r3.0.3-1791-co...
- IDE Controller 1
  - DVD Drive
    None
- SCSI Controller
- Network Adapter
  Not connected
- COM 1
  None
- COM 2
  None
- Diskette Drive
  None

Management
- Name
  Cond-v3.0.3
- Integration Services
  Some services offered
- Checkpoints
  Production
- Smart Paging File Location
  C:\ProgramData\Microsoft\Win...

Processor

You can modify the number of virtual processors based on the number of processors on the physical computer. You can also modify other resource control settings.

Number of virtual processors: 8

Resource control

You can use resource controls to balance resources among virtual machines.

Virtual machine reserve (percentage): 0

Percent of total system resources: 0

Virtual machine limit (percentage): 100

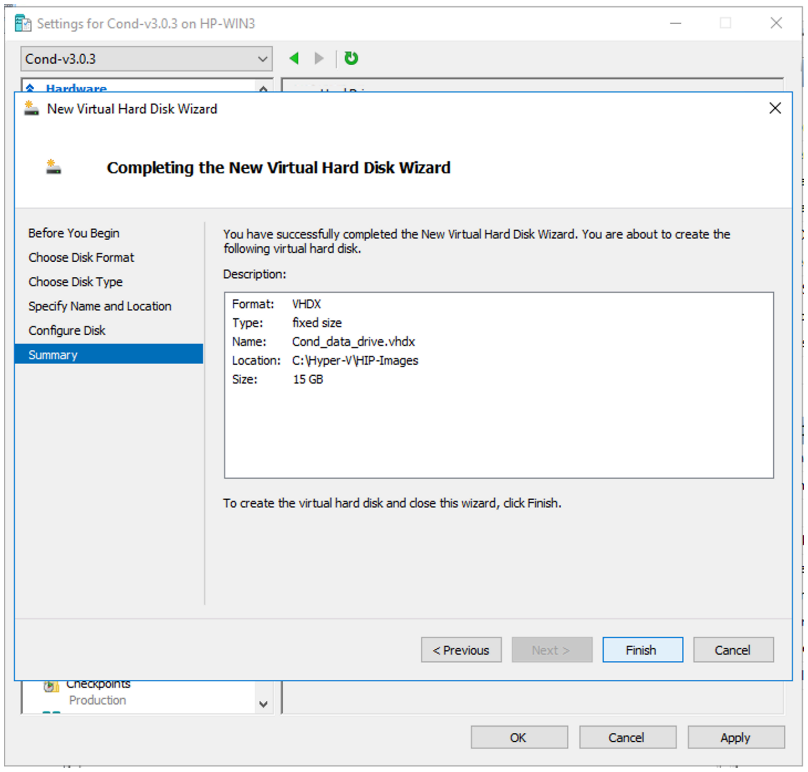
Percent of total system resources: 50

Relative weight: 100

This virtual machine is configured with the following:

Sockets: 2
NUMA nodes per socket: 1
Virtual processors per NUMA node: 8
Memory per NUMA node: 4680 MB

3. Open **IDE Controller 0**. Select **Hard Drive**, then **Add**. This is a second hard drive for the data partition.
4. **Configure a new Virtual hard disk for the data partition** – On the **Hard Drive** page, under **Virtual hard disk**, select **New** and configure the drive:
   - **Choose Disk Format** – Select **VHDX**. Select **Next**.
   - **Choose Disk Type** – Select **Fixed Size**. Select **Next**.
   - **Specify Name and Location** – Enter a descriptive name, and keep the default location. Select **Next**.
   - **Configure Disk** – Select **Create a new blank virtual hard disk** and for **Size**, enter 15 GB. Select **Next**.
   - **Summary** – Check your details, and select **Finish**.



Completing the New Virtual Hard Disk Wizard

You have successfully completed the New Virtual Hard Disk Wizard. You are about to create the following virtual hard disk.

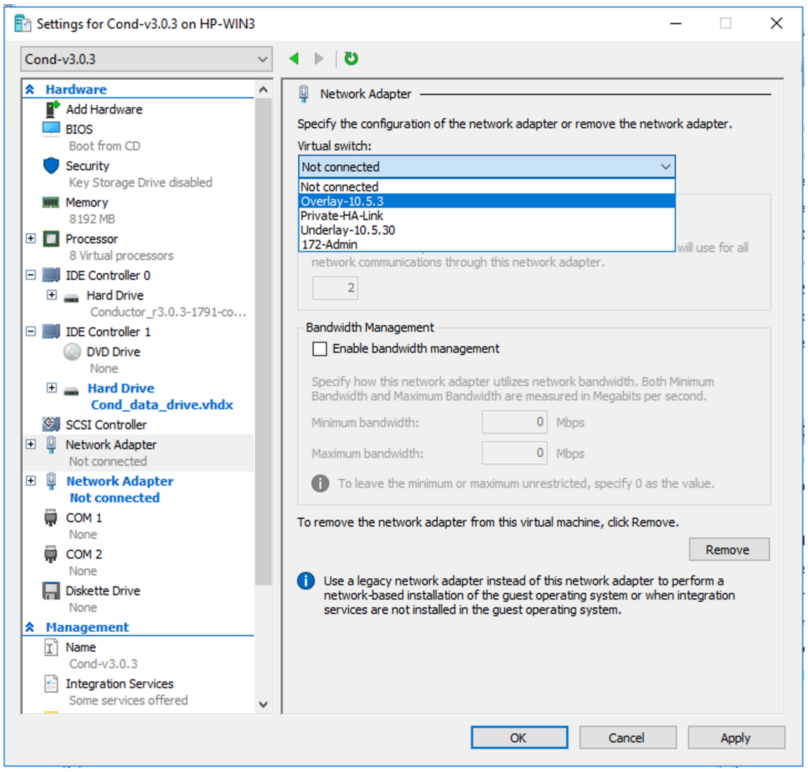
Description:

Format:	VHDX
Type:	fixed size
Name:	Cond_data_drive.vhdx
Location:	C:\Hyper-V\HIP-Images
Size:	15 GB

To create the virtual hard disk and close this wizard, click Finish.

5. **Wait while Hyper-V creates the new virtual hard disk**. This process can take up to 15 minutes.
6. **Add a second Network Adaptor** – Still under the new Conductor virtual machine **Settings**, at the top, select **Add Hardware**. Select **Network Adapter**, and then select **Add**.
7. **Attach Network Adapters** – Now you will assign the network adapters for your Conductor:

   a) Select the first Network Adapter, and under **Virtual switch**, attach it to your Administration network (or your underlay, if they are the same), and select **Apply** to save.



Specify the configuration of the network adapter or remove the network adapter.

Virtual switch: Not connected

...will use for all network communications through this network adapter.

2

Bandwidth Management

□ Enable bandwidth management

Specify how this network adapter utilizes network bandwidth. Both Minimum Bandwidth and Maximum Bandwidth are measured in Megabits per second.

Minimum bandwidth: 0 Mbps

Maximum bandwidth: 0 Mbps

To leave the minimum or maximum unrestricted, specify 0 as the value.

To remove the network adapter from this virtual machine, click Remove.

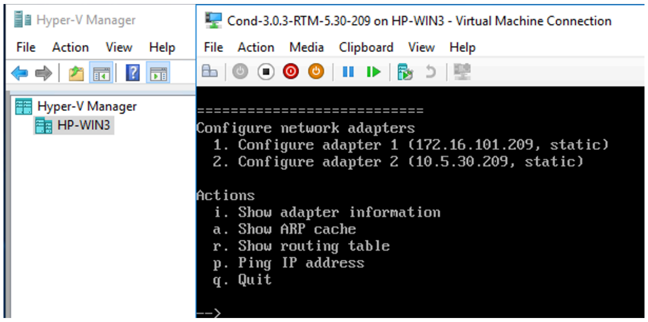
Use a legacy network adapter instead of this network adapter to perform a network-based installation of the guest operating system or when integration services are not installed in the guest operating system.

b) Configure the second Network Adapter, if needed, and select **Apply** to save.

8. Select **Ok** to exit the **Settings** page.

Step 3: Configure the Network Adapter on the Conductor Virtual Machine

1. In the Hyper-V Manager, select the Conductor virtual machine.
2. On the right, under **Actions**, select **Start**. It will take a few minutes for the Conductor virtual machine to initialize.
3. Select **Connect**, which opens a terminal window, and then type `airsh` to get into Airshell.
4. Type `conf network` and press `Enter`. If the system is still starting up, it will let you know. When it brings up the **Configure network adapters** menu, you can proceed.


Hyper-V Manager
File Action View Help
Hyper-V Manager
HP-WIN3
Cond-3.0.3-RTM-5.30-209 on HP-WIN3 - Virtual Machine Connection
File Action Media Clipboard View Help

```
==========================
Configure network adapters
  1. Configure adapter 1 (172.16.101.209, static)
  2. Configure adapter 2 (10.5.30.209, static)

Actions
  i. Show adapter information
  a. Show ARP cache
  r. Show routing table
  p. Ping IP address
  q. Quit
-->
```

5. Type 1 or 2 and follow the menu to configure adapter 1. You may want to set the IP to its actual address on the network. Set the following options, as needed:
   - **IP address** – Set to the IP for the Virtual Machine on the network.
   - **Netmask** – Set as needed.
   - **Default gateway** – Set as needed.
   - **DNS** – Set to your preferred DNS server, so the Conductor can access the Tempered Licensing Server.
6. Type `q` to quit to the main menu, then `s` to save your changes.
7. Type `q` again to quit to the main Airshell screen. You may need to type `reboot` to restart the Conductor.

Step 4: Configure the Conductor

An unlicensed, new Hyper-V Conductor deploys with a static IP address of 192.168.56.2 on Network adapter 1.

To determine the IP address assigned to network adapter 2, at the console, log in with name: `airsh`, and password: `airsh`, and then type `status`.

Run the Conductor web UI on either of the network adapters. To continue:

- **For a v2.2.10 and later Conductors**, see Log in and Configure the Conductor on page 201.
- **For v2.2.8 or earlier Conductors**, see License and Provision a Conductor (v2.2.8 and earlier) on page 191.

For more information, see:

- License and Provision a Conductor (v2.2.8 and earlier) on page 191
- Log in and Configure the Conductor on page 201
- Add Airwall Edge Service Licenses to the Conductor on page 192

Configure a Conductor

The **Settings** page contains many configurable options to help you customize Conductor behavior to support your environment.

When you finish deploying the Conductor in your environment, you may want configure additional settings. See Best Practices for Conductor Configuration on page 235.

Best Practices for Conductor Configuration

Here are some best practices for configuring your Conductor.

Conductor Initial Setup

Configure these settings when you're setting up your Conductor.

- **Use NTP servers to set System Time** – While you can set your system time manually, using NTP (Network Time Protocol) servers ensures your system time stays synchronized with Coordinated Univeral Time (UTC). See Set the Conductor system time on page 236.
- **Create a human-readable Conductor URL** – You can just keep your Conductor as an IP address, but giving it a human-readable name makes it easier for humans. See Configuring a Conductor IP, Friendly URL, or Port on page 236.
- **Create separate accounts for each person administering the Conductor** - Only use the 'admin' account for top-level administration. Creating user accounts for each person who will be administering the Conductor lets you see who is making changes in the system when you review log details. For how to create a user account, see Add a Person on page 54.
- **Configure email settings** - Configuring your email settings ensures your Conductor has an email address from which to send alerts Airwall and invitations. See Configure Email Settings on page 238.
- **Get and Set up a CA Certificate** - Setting up a CA Certificate will stop the warnings that your site is unsafe. See Install a Custom CA Certificate Chain on page 239.

Deploying Airwall Edge Services

- **Add a DNS SRV record pointing to your Conductor** – Adding this record allows easier deployment of physical Airwall Edge Services, as they can find and set the Conductor URL automatically once you connect them to your underlay network. See Connect an Airwall Gateway with a DNS SRV record on page 294.
- **Configure WiFi Settings** - When you configure WiFi settings on the Conductor, any Airwall Edge Services with WiFi capabilities can retrieve the WiFi settings once they connect to the Conductor. See Configure Wi-Fi Settings on page 241.

Managing Airwall Edge Services

- **Create Event Monitors** – Create monitors for events to help you manage the activity and health of your Airwall secure network. See Create an Event Monitor on page 119.

Set the Conductor system time

Set how your Conductor system time is determined.

1. Go to **Settings**, scroll down to **System Time** and click **Edit Settings**.
2. Under **Use NTP**, click **Enabled**.

   Note: You can manually set your system time, but it is a best practice to use an NTP (Network Time Protocol) server.

3. Under **NTP Servers**, enter at least one NTP server, such as *us.pool.ntp.org* or *time.google.com*.
4. Click **Update**.

Configuring a Conductor IP, Friendly URL, or Port

Set up the Conductor URL using the Conductor Configuration Wizard Settings on page 197. Use these instructions to edit the IP, URL, or Port if needed.

v3.0 and later

Friendly URLs cannot have spaces or special characters except - dash.

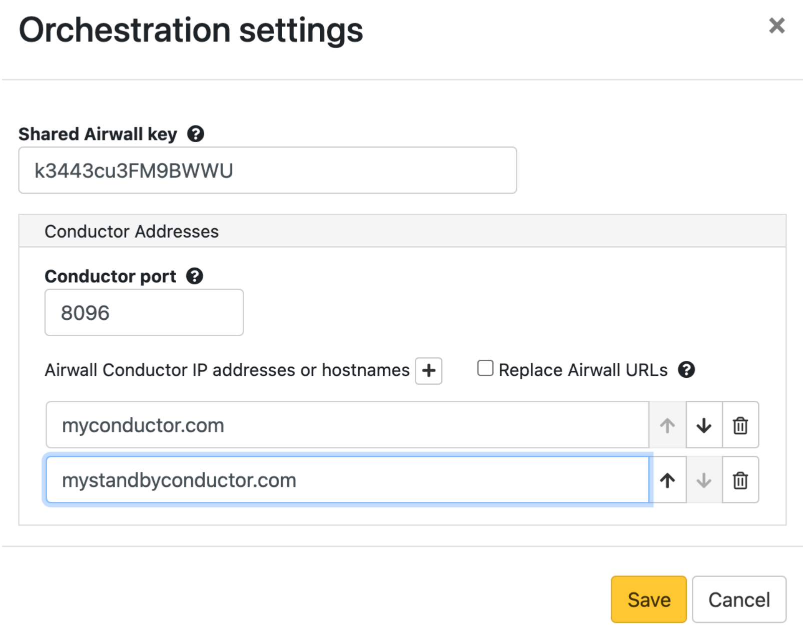
1. Go to **Settings**.
2. In **Orchestration Settings**, select **Edit Settings**.

   Note: The Shared Airwall key is assigned for your Conductor automatically. You do not need to change it unless you want to move an Airwall Gateway from one Conductor to another, see Move an Airwall Gateway to a Different Conductor on page 132.

3. Optional: If you need to change the Conductor port, you can do it here.

4. Beside **Airwall Conductor IP addresses or hostnames**, select the +, and enter an IP or friendly name for your Conductor.

   Note: Version 3.3.x and later also support https and wss URLs.



Orchestration settings

Shared Airwall key: k3443cu3FM9BWWU

Conductor Addresses

Conductor port: 8096

Airwall Conductor IP addresses or hostnames

□ Replace Airwall URLs

myconductor.com

mystandbyconductor.com

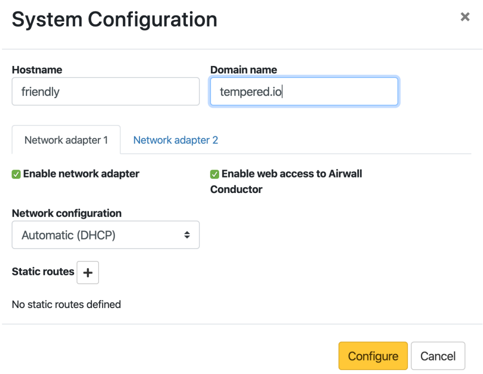
5. Select **Save**.

You can now use your friendly URL when connecting to the Conductor, and can provide it for others to connect manually, or using Airwall Invitations.

Before v3.0

Friendly URLs cannot have spaces or special characters except - dash.

1. Go to **Settings**.
2. In the **Configuration** section, click **Setup**.
3. Under **Hostname**, enter a friendly name for your Conductor.
4. Under **Domain name**, enter your domain. For example, the settings in the dialog below sets a friendly Conductor URL of friendly.tempered.io:



System Configuration

Hostname: friendly

Domain name: tempered.io

Network adapter 1 | Network adapter 2

☑ Enable network adapter

☑ Enable web access to Airwall Conductor

Network configuration: Automatic (DHCP)

Static routes

No static routes defined

5. Click **Configure**.

You can now use your friendly URL when connecting to the Conductor, and can provide it for others to connect manually, or using Airwall Invitations.

Configure Email Settings

If you are a member or manager of an Overlay network, you can set up the Conductor to send email notifications when specific events occur there. There are three steps involved: Add your email settings for the Conductor to send email, add emails to receive notifications, and turn on or off notifications.

v3.0 and later

1. Add email settings for the Conductor to set the email address the Conductor sends notifications from.
   a) Go to **Settings** > **Services** > **Email Server** and select **Edit Settings**.

      If you do not see it as a choice, select **Add service** and select **Email Server**.
   b) Make sure **Enable** is On (green with the bubble to the right).
   c) Enter the settings for the email you want Conductor notifications to come from.
   d) Under **Prefix for subject line**, enter a prefix for the Subject of the emails, if desired. For example, enter `Airwall Alerts`.
   e) Select **Configure**.
   f) Once email settings have been configured, go to **Settings** > **Services** > **Email Server** and then select **Send test email…** to verify that the settings are valid.
2. Add emails to receive notifications:
   a) In the Conductor, go to **People**.
   b) Select an existing person, or Add a Person on page 54.
   c) Under **Alert email trigger level**, select the alert level of notifications for that person to receive.
3. Add the person to the Overlays for which you want them to receive notifications:
   a) Go to **Overlays**, and create or select an Overlay.
   b) On the right, open the **People** tab, and select **Update**.
   c) For the person you want to add to the Overlay, click the column to make them a **Viewer** or **Editor** of the Overlay.
   d) Select **Close**.

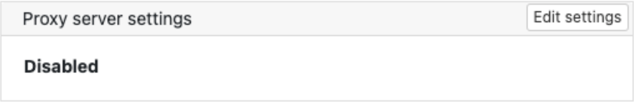
Before v3.0

1. Add email settings for the Conductor. This sets the email address the Conductor sends notifications from.
   a) Go to **Settings** > **Email Server** and click **Edit Settings**.
   b) Click **Enabled**.
   c) Enter the settings for the email you want Conductor notifications to come from.
   d) Under **Prefix for subject line**, enter a prefix for the Subject of the emails, if desired. For example, enter `Airwall Alerts`.
   e) Click **Save**.
   f) Once email settings have been configured, go to **Settings** > **Email Settings** and click **Send Test Email…** to verify that the settings are valid.
2. Add emails to receive notifications:
   a) In the Conductor, go to **People**.
   b) Select an existing person, or Add a Person on page 54.
   c) Under **Alert email trigger level**, select the alert level for that person to receive notifications.
3. Add the person to the Overlays that you want them to receive notifications for:
   a) Go to **Overlays**, and create or select an Overlay.
   b) On the right, under **People**, click **Update**.
   c) For the person you want to add to the Overlay, click the column to make them a **Member** or **Manager** of the Overlay.
   d) Click **Close**.

Set a Proxy Server

You may need to set a proxy server to allow the Conductor to reach the Tempered licensing server, update the OUI list, or to download firmware updates.

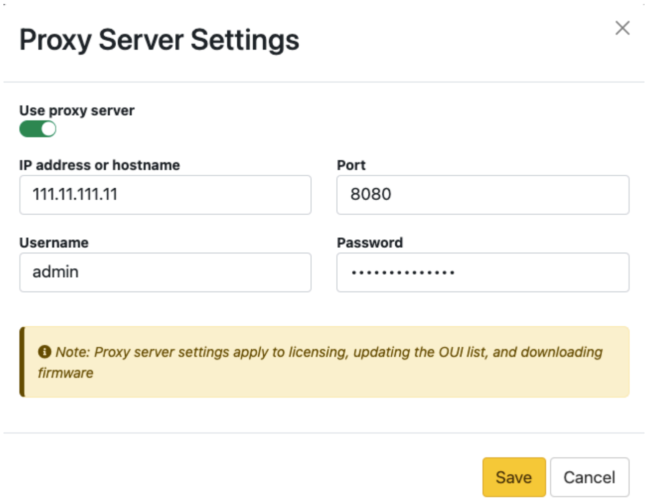
1. In Conductor **Settings**, scroll down to **Proxy server settings**, and select **Edit Settings**.



Proxy server settings

Disabled

2. Toggle **Use proxy server** to on, and then enter the IP address and Port name for your proxy server.



Proxy Server Settings

Use proxy server: on

IP address or hostname: 111.11.111.11

Port: 8080

Username: admin

Password: •••••••••••••••

Note: Proxy server settings apply to licensing, updating the OUI list, and downloading firmware

3. Enter the user name and password for your proxy server, if needed.
4. Select **Save**.

Configure Monitor and Alert Settings

Keep track of the health and activity on your Airwall secure network with monitors and alerts. For more information, see Monitor Activity with Events and Alerts on page 117.

Install a Custom CA Certificate Chain

You can install or replace a custom CA Certificate chain for the Conductor, which allows the Conductor to generate the CSRs you need to get signed certificates, and so the Conductor can verify the signed certificates you install. When you install custom certificates, they replace the default Tempered factory-installed certificate chain.

Before installing custom certificates on Conductor and Airwall Edge Services, you need to upload the intended certificate chain to Conductor. To install a custom certificate authority chain:

1. Log in to the Conductor with a System Administrator account.
2. Go to **Settings** > **General Settings** > **Certificates.**
3. To install certificates initially, select **Install CA certificates**.

   To replace certificates, select **Replace CA certificates** (supported in v2.2.8 and later)
4. Select **Choose File** and select a concatenated PEM file containing all of CA chain certificates (the full CA chain including the root). This is the certificate chain against which Conductor validates the signed Certificate Signing Request.
5. Select **Upload**.

The Conductor checks that the uploaded certificates validate the chain of trust and are not expired. You can now Add or Replace a Signed Certificate for the Conductor UI on page 239.

Add or Replace a Signed Certificate for the Conductor UI

Versions	v2.2.8 and later Conductors

By default, the Conductor comes with a Tempered factory-installed certificate. You can add your own custom certificate to prevent the “Your connection is not private” messages received on some browsers. A custom signed certificate is used by the Conductor for the SSL connection.

Important: For Conductors in HA environments, both Conductors must not be HA paired to upload and install custom certificates. Follow the steps for each Conductor. Once complete, HA pair the Conductors.

Note: When you are in the process of replacing a certificate, the Conductor uses the existing certificate until the replacement is complete.

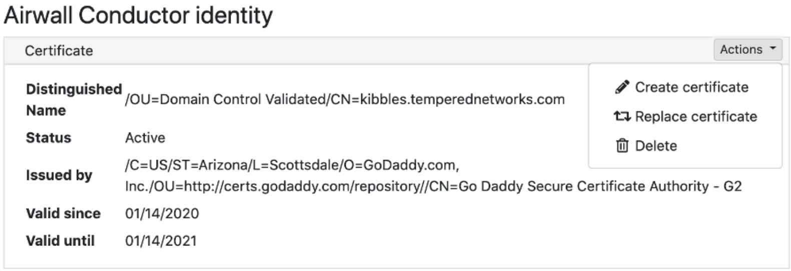
Before you Begin

Before you can upload or replace a signed certificate, you need to have a CA certificate chain installed so that the Conductor can verify the certificates. For more information, see Install a Custom CA Certificate Chain on page 239.

Step 1: Request and copy a CSR (Certificate Signing Request) for the Conductor

Once you've installed CA certificates (see Install a Custom CA Certificate Chain on page 239), you can generate a Certificate Signing Request (CSR) to create a certificate (for example, with a PKI Registration Authority):

1. In Conductor **Settings**, under **Airwall Conductor Identity**, click **Actions**, and then select **Create certificate** or **Replace certificate**.

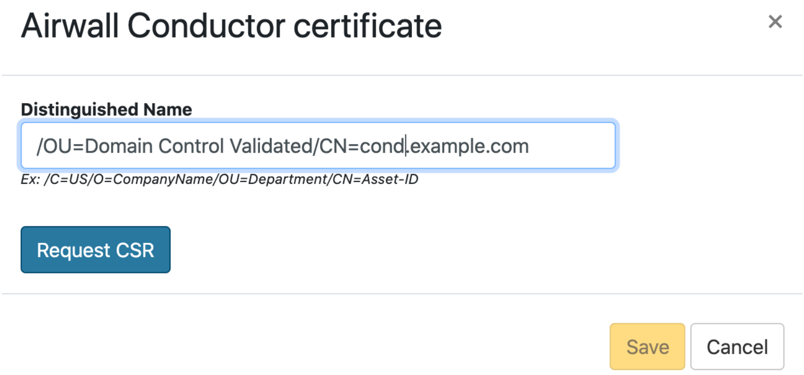


Airwall Conductor identity

Certificate

Distinguished Name	/OU=Domain Control Validated/CN=kibbles.temperednetworks.com
Status	Active
Issued by	/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certs.godaddy.com/repository//CN=Go Daddy Secure Certificate Authority - G2
Valid since	01/14/2020
Valid until	01/14/2021

2. Under **Distinguished Name**, enter the Identity (Distinguished Name) of the Conductor. If you're replacing a certificate, you can leave the Distinguished name the same. For example, `/C=US/O=Tempered/OU=Dev/CN=cond.example.com`



Airwall Conductor certificate

Distinguished Name: /OU=Domain Control Validated/CN=cond.example.com

Ex: /C=US/O=CompanyName/OU=Department/CN=Asset-ID

3. Under **CSR**, select either **Copy** or **Download** to generate and get the CSR you need to get a signed certificate. (In versions 2.2.5 and earlier, select and copy the CSR.)
4. Select **Save**.

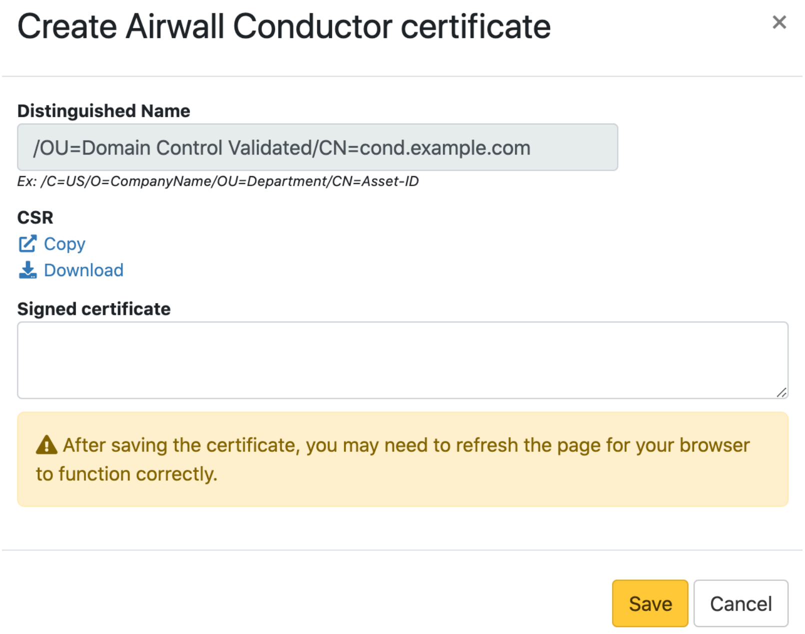
Getting a signed certificate

Use the CSR to request a new signed certificate. You can generate a new signed certificate using your organization's own process, or with a public PKI Registration Authority.

1. Submit the Certificate Signing Request (CSR) you copied or downloaded to your Enterprise PKI Registration Authority. They use it to create your certificates.
2. When you get the certificates, download or copy them.

Step 3: Upload the signed certificate to the Conductor

1. In Conductor **Settings**, under **General settings**, scroll down to **Airwall Conductor Identity**, and select **Edit**.
2. Under **Signed Certificate**, paste the custom-CA signed certificate to install the certificate on the Conductor.



Create Airwall Conductor certificate

Distinguished Name

/OU=Domain Control Validated/CN=cond.example.com

Ex: /C=US/O=CompanyName/OU=Department/CN=Asset-ID

CSR

Signed certificate

⚠ After saving the certificate, you may need to refresh the page for your browser to function correctly.

3. Select **Save**.
4. Refresh your browser window to apply the new certificate.

Configure Wi-Fi Settings

You can configure Wi-Fi settings for connectivity to the underlay in the Conductor. Once a Wi-Fi-enabled Airwall Gateway is assigned to an overlay network, it retrieves the Wi-Fi settings.

Airwall Gateways must first connect to the underlay with a wired connection to retrieve Wi-Fi settings. Once you've configured the Wi-Fi settings on the Airwall Gateway, it will switch to Wi-Fi whenever the wired underlay connection is unavailable. If you want an Airwall Gateway to only use the Wi-Fi configuration, just disconnect the underlay wired connection.

Note: You can configure Wi-Fi settings for an Airwall Gateway in the Conductor, or in diagnostic mode on the Airwall Gateway.

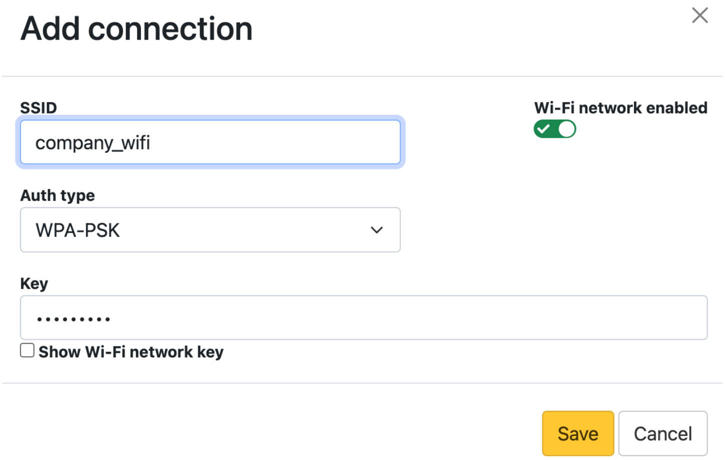
Note: You cannot configure EAP-TLS Wireless networks in conjunction with Customer Certificates.

Set up a Wi-Fi network

Wi-Fi networks you configure on the Conductor are available to all Airwall Edge Services that have Wi-Fi network interfaces. If you delete a Wi-Fi network, all configured Airwall Edge Services remove the Wi-Fi network from their configuration.

Note: Prior to defining an EAP-TLS connection, you must have a Customer CA Chain installed on the Conductor. Airwall Edge Services will not apply the EAP-TLS configuration until they have been provisioned with a Customer-signed PKI Certificate. EAP-TLS configurations use the Subject Common Name (CN) component of the Customer-signed Certificate Distinguished Name (DN) as the identity for the EAP-TLS transaction.

1. In the Conductor, go to **Settings** > **General Settings** and scroll down to **Wi-Fi Networks**.
2. Select **New connection**, and under **SSID**, enter the name of your Wi-Fi network. If needed, under **Auth type** select how your network authentication protocol and enter your Wi-Fi network key.



Add connection

SSID: company_wifi

Wi-Fi network enabled: ☑

Auth type: WPA-PSK

Key: •••••••••

□ Show Wi-Fi network key

3. Select **Save**.

Once you've set up the Wi-Fi network in the Conductor, you can Set the Wi-Fi network for an Airwall Gateway on page 383.

> **Note:** The Airwall Gateway automatically detects the wireless family and channel, and has two reverse-polarity SMA (RP-SMA) connectors for antenna connections used in diversity mode to improve wireless signal reception. If only a single antenna is used, connect the antenna to the main antenna connector.

Configure Authentication Options

Manage the settings for user login authentication, such as password requirements and lockout time.

To configure user account settings:

1. Log in to the Conductor with a system administrator account.
2. Go to **Settings** > **Authentication** > **Settings** > **Edit Settings**.
3. Configure **User authentication settings**:
   - **Default authentication provider** – Select the default authentication displayed when users log in.
   - **Login attempts before lockout** – Set the number of unsuccessful login attempts before lockout. Set to 0 to disable.
   - **Password expiration** – Set the number of days until password expires (default 180 days). Set to 0 to disable.
   - **Lockout time** – Set the amount of time to track unsuccessful login attempts (default 1 hour).
   - **API token expiration** – Set the number of days before API tokens expire. Set to 0 to disable.
   - **Show "Forgot Your Password?"** – Check to display a **Forgot your Password?** link that allows a user to reset their password (enabled by default).
4. Configure **Password requirements**:
   - **Minimum password length** – Enter the required minimum number of characters
   - **At least one number** – Check to require at least one number
   - **Upper and lowercase characters** – Check to require both upper- and lowercase letters
   - **At least one symbol** – Check to require at least one symbol
5. Configure **Session settings**:
   - **Conductor session expiration** – Set the number of hours before a Conductor session expires.
   - **Conductor session inactivity timeout** – Set the number of minutes before a Conductor session times out due to inactivity.
6. Configure **Global Airwall agent authentication settings**:
   - **Require Airwall agent authentication** – Check to require authentication, and select an option:

  - `for all agents` to require authentication, which may require some people to update their Airwall Agents)
  - `for supported agents` to allow older agents that do not support authentication to log in.
- **Require Airwall agent authentication for Linux servers** – Check to enforce authentication for Linux servers. Authentication is not required by default.
- **Retain session on service restart** – Check to allow an Airwall Agent to reconnect to a session after it restarts. By default, restarting ends the session.
- **Require owner for Airwall Agent authorization** – If checked, once an owner is set for an Airwall Agent, no other person will be able to log in from that Airwall Agent.
- **Auto-assign Airwall agent owner on login** – If checked, will assign the first person to log in with an Airwall Agent as the owner.
- **Airwall agent authentication provider** – Select `Username and password` to require Conductor username and password to log in, choose an authentication provider, or choose `All authentication providers` to allow the user to select how they log in.
- **Session timeout** – Set the number of hours before an Airwall Agent times out. Note that changing the session timeout does not affect current sessions.

7. Click **Save**.

Note: If you have email settings correctly configured in **Settings** > **Email Settings**, and you have a **Forgot your Password?** link on the Conductor login screen, all users can enter their username and click the link to send a password recovery email to the address associated with that username.

The password recovery email is sent from the address configured in Email settings, so if it is not set up, users will not be able to recover their passwords this way. If the password recovery email does not arrive within 5 minutes, check your spam folder and explicitly allow the address.

For instructions on setting up Conductor Email settings, see Configure Email Settings on page 238.

Configure user authentication for Airwall Agents and Airwall Servers

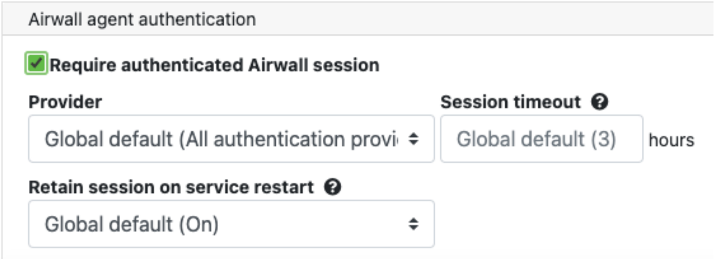
You can configure user authentication for Airwall Agents and the Windows Airwall Server by requiring a username or password before they can connect to an Overlay.

Note:

Linux servers don't support any form of user authentication.

Note: For user authentication compatibility and functionality, make sure your Conductor and all Airwall Agents and Airwall Servers are on the latest version (v3.0.3).

1. In the Conductor, on an Airwall Agent or Server configuration page, select **Edit Settings**, and check the **Require authenticated Airwall session**. Select **Update Settings**.



Airwall agent authentication

☑ Require authenticated Airwall session

Provider: Global default (All authentication provi

Session timeout: Global default (3) hours

Retain session on service restart: Global default (On)

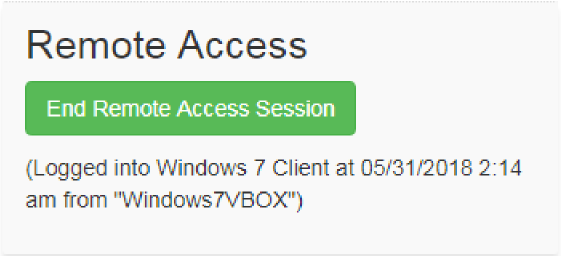
Note: If you do not see the **Edit Settings**, you do not have permissions to edit that Airwall Agent or Server.

2. Connect the Airwall Agent or Airwall Server to the Conductor.
3. Verify that:

- Logging in requires you enter Conductor or LDAP credentials.
- The Airwall Agent or Airwall Server has access to the Overlay.

4. You can monitor user connections from the information pages in the **People** tab in Conductor.

   You also have the ability to end the session on-demand as an administrator.



Remote Access

(Logged into Windows 7 Client at 05/31/2018 2:14 am from "Windows7VBOX")

See also:

- Integrate Third-party Authentication with OpenID Connect on page 247
- Configure LDAP authentication on Conductor and Airwall Edge Services on page 257
- Walkthrough - Onboard people to your Airwall secure network with User Authentication on page 83

Walkthrough - Onboard people to your Airwall secure network with User Authentication

How to set up global user/password authentication for Airwall Agents and Servers connecting to your Airwall secure network.

This walkthrough walks you through setting up authentication for all people connecting to your Airwall secure network.

Note: This walkthrough covers globally onboarding people with authentication. You can also turn on authentication for individual Airwall Agents and Servers.

Supported Versions	Conductor v2.2.10 and later. This walkthrough is based on v3.0, so some things may be slightly different on earlier versions.

The basic steps are:

1. Require User authentication globally.
2. Onboard people using People Groups.
3. Add people as Remote Access Users.

These steps are covered in more detail below.

Note: For pre-2.2.8 Airwall Agents and Servers only: There is an extra step to provide access at the end of this walkthrough.

Best Practice:

Finding the right balance between ease of use and security is an ongoing challenge.

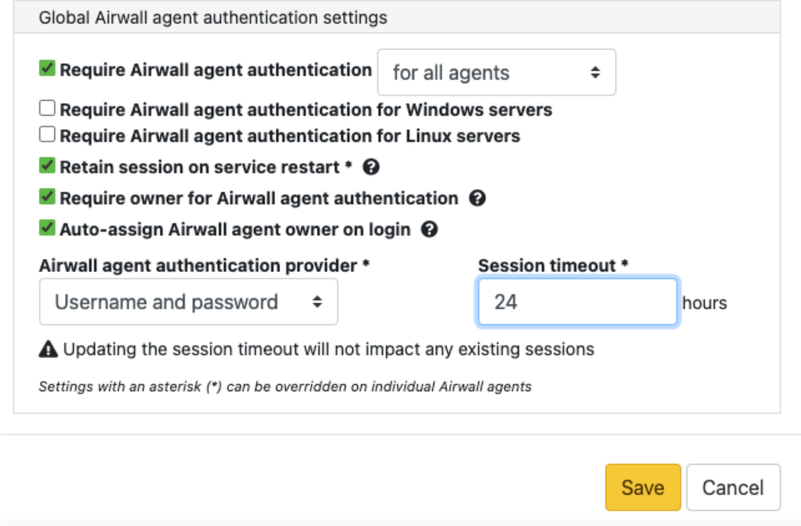
This walkthrough shows how you can easily onboard and provide trust to a person, but you may choose to keep additional security checks in place, like granting the provisioning request based on the Device ID a person gives you.

A balanced option might include automatic onboarding, but only granting trust to a benign device that they can ping for communication verification and then provide final trust to secure environments once information has been verified verbally.

Step 1: Require user authentication globally

1. Go to **SettingsAuthentication**, and under **Settings**, select **Edit Settings** (in pre-v3.0, this is under **Global Airwall agent authentication settings**).
2. Check or set your authentication options:
   - Check **Require Airwall agent authentication** and select the option `for all agents`.

- Under **Airwall agent authentication**, under **Airwall Agent Authentication Provider**, select `Username and password`, or an OpenID Connect (OIDC) third-party authentication provider, if you've set it up. See Integrate Third-party Authentication with OpenID Connect on page 247.
- (Optional) You can also set a custom Session timeout or whether people need to log in when they restart their Airwall Agent



Global Airwall agent authentication settings

☑ Require Airwall agent authentication [for all agents]

☐ Require Airwall agent authentication for Windows servers

☐ Require Airwall agent authentication for Linux servers

☑ Retain session on service restart *

☑ Require owner for Airwall agent authentication

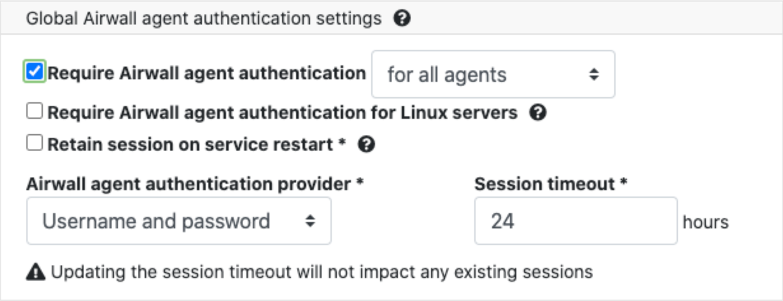
☑ Auto-assign Airwall agent owner on login

Airwall agent authentication provider *: Username and password

Session timeout *: 24 hours

⚠ Updating the session timeout will not impact any existing sessions

Settings with an asterisk (*) can be overridden on individual Airwall agents



Global Airwall agent authentication settings

☑ Require Airwall agent authentication [for all agents]

☐ Require Airwall agent authentication for Linux servers

☐ Retain session on service restart *

Airwall agent authentication provider *: Username and password

Session timeout *: 24 hours

⚠ Updating the session timeout will not impact any existing sessions

For more information, see Configure Authentication Options on page 242. You can also require authentication per device on the Airwall Agent or Server page.

Step 2: Onboard People using People Groups

You may also want to Import people using a CSV file on page 61.

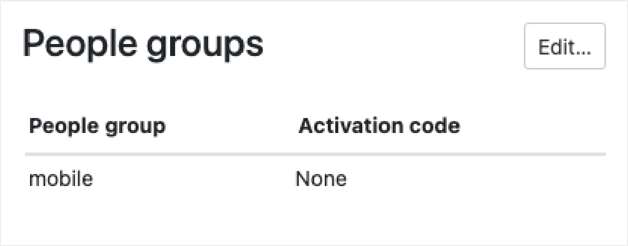
1. Set up a People Group on page 89, configuring the onboarding options you want to this People group to have. You can add people on the **People** tab, or add them to the group as you create users in the Conductor.
2. On the **User onboarding** tab:
   - Check **Provide an activation code for each member**.
   - Check **Send onboarding email to users** if you want to send emails automatically.
   - Pre-configure the **General**, **Airwall**, and **Groups** settings for users when they onboard. Setting these options allows members of the group to activate their connections. For more information, see Connect People's Devices with Activation Codes on page 75.

Note: If you want to configure which version of the Airwall Agent they download, you can set that on the Conductor **Settings** page under **Global Airwall agent settings**.

On the People Groups page, you will see your new group, and to the right, you will see the Activation Code icon 🔌 that indicates every person added to this group will receive an Activation Code. For more information, see Connect People’s Devices with Airwall Invitations on page 64 or Connect People's Devices with Activation Codes on page 75.

Step 3: Add Remote Access Users

1. Add the people you want to connect to the Conductor. For Remote Access Users, see Connect People as Remote Access Users on page 74.
2. As you save each user, from each person's **People** page, add users to the people onboarding group created in Step 2.
   a) Under **People groups**, select **Edit**.



People groups

People group	Activation code
mobile	None

   b) Select the onboarding People group created in Step 2.
3. The people are sent an onboarding email. If desired, you can send them custom instructions, or point them to one of these help topics: I have a "Finish Setting up my account" email on page 15 or I have an Activation Code on page 15.
   As people click the link in the email to set their password and log in to the Conductor, they'll be directed to the **Connect an Airwall Agent** page where they can install an Airwall Agent or Server and activate their connections.

What's Next

You can get a report on remote sessions from **Visibility** > **Reports**. For more information, see Run Network Activity Reports on page 116.

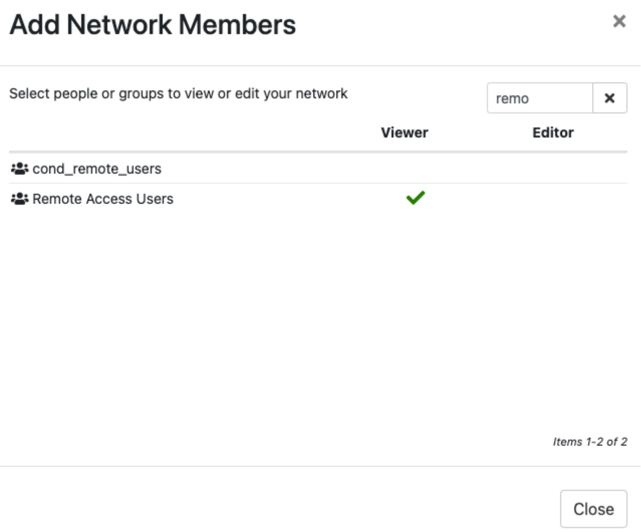
You can see who's remotely logged into your Airwall secure network. See Check Remote Sessions on page 77.

You can also see which users have used their Activation codes. See Check Status of People Onboarding on page 76.

For pre-2.2.8 Airwall Agents and Servers only) Give the People group access

If you are onboarding people using pre-2.2.8 Airwall Agents and Servers you need to give the People group access by adding them to Overlays and Relay Rules.

On the Overlay these people need to access, add the People group you created as a **Viewer** (or pre v3.0, as a **Member**).



Add Network Members

Select people or groups to view or edit your network

	Viewer	Editor
cond_remote_users		
Remote Access Users	✓	

Items 1-2 of 2

Integrate Third-party Authentication with OpenID Connect

You can integrate a third-party authentication provider with person authentication in the Conductor using OpenID Connect (OIDC). If your users are already configured for single sign-on (SSO) with a third party, or if you have a large number of users, this integration streamlines your user management.

Note: You can only configure one OpenID Connect provider on the Conductor at a time. If you need to support many OIDC authentication providers simultaneously, you can choose providers that support federated login so you can connect to one provider and have that provider connect to other providers to authenticate users.

Important: To use OpenID Connect on macOS or iOS Airwall Agents, you must have a public certificate on your Conductor.

User Roles

In the Airwall Conductor, you configure person roles in OIDC by including them in groups. The OIDC group names are pre-configured in the Conductor, so when you make a person a member of one of the OIDC groups in the OIDC provider, they are automatically given that role in the Conductor. For instance, you can declare that all members of the OIDC provider's cond_system_admins group are system administrators in the Conductor, and that members of the OIDC cond_remote_users group are remote-access users.

Multi-factor Authentication

If your OIDC provider supports a multi-factor authentication (MFA) protocols, you can use MFA on your provider to require MFA for logging into your Conductor or for Airwall Agent session authentication.

Integrate Authentication with the Conductor

To successfully integrate authentication, you must

1. Create and configure an application in your authentication provider.
2. Configure OIDC on the Conductor.
3. Set up Airwall Agents.
4. Verify third-party authentication is working on page 255

Since each provider is different, refer to the basics required here, and then the Provider-specific instructions that follow for integrating with some popular providers that support OIDC.

1. Create and configure an application in your authentication provider

Create and configure the application in your provider using the Provider-specific Instructions on page 249 before connecting it to the Airwall Conductor. Each provider's workflow is different, but here are the general steps:

1. Create an OpenID Connect application.
2. Configure it with the following information:

Field	Enter
Name	Whatever you want. For example, "Airwall Conductor"
Login Redirect URI	Your Conductor URI followed by `/user/auth/openid_connect/callback`. For example: `https://conductor.mycompany.com/user/auth/openid_connect/callback.` Note – If your Conductor is HA paired, add a second login redirect URI, with the same path added.
Logout Redirect URI	Your Conductor URI: https://conductor.mycompany.com

3. Depending on your provider, set the authentication method to **basic**, or indicate you are using an **authorization code** for authentication (not a refresh token).
4. Allow the **groups** claim for grant. The **groups** claim is what allows the Conductor to match a user's group with what role they are given. Because **groups** is not a default OIDC claim, it must be turned on in the provider. For more details, see the Provider-specific instructions.
5. Create four groups: `cond_system_admins`, `cond_readonly_admins`, `cond_network_admins`, and `cond_remote_users` to indicate the four different Conductor roles.
6. Add users to each group so they are assigned the correct role when logging into Conductor.
7. Give your users access to the application you created in your provider.
8. If you want to require MFA to log in, set it up in the OIDC provider. Generally MFA is associated with the app. Please consult your provider documentation for detailed instructions on setting up MFA.

2. Configure OIDC on the Airwall Conductor

1. Go to Conductor **Settings**.
2. Next to **Authentication**, select **Add provider**.
3. Select **OpenID Connect** and then select **Next**.
4. On the **Add Authentication Provider** page, under **General settings**, configure the Provider settings as follows (see the Provider-specific Instructions for help in finding this information):

For this Setting	Enter
Provider Name	Give your provider a descriptive name. This name appears as an option when logging into the Conductor.
Conductor host	Host of your Conductor. Must be in the format `https://conductor.mycompany.com` (no trailing slash)
OpenID Connect host	Must be in the format `https://hostname.com:{optional port}`
Issuer	Issuer provided by your OIDC provider. Sometimes this value is the same as the OpenID Connect host depending on the provider.
Client ID (sometimes called Identifier)	Token provided by your OIDC provider associated with the provider application
Secret	Secret token that goes with the Client ID

5. For **HA-paired Conductor host**, enter the Host of your HA Conductor (if applicable).
6. Configure the **Group** settings as follows, and then click **Next**:

For this Setting	Enter
Use groups to manage roles	Checked
System admin groups	Comma-separated list of groups from your provider that will give your user this role.
Read-only admin groups	Comma-separated list of groups from your provider that will give your user this role.
Network admin groups	Comma-separated list of groups from your provider that will give your user this role.
Remote-access user groups	Comma-separated list of groups from your provider that will give your user this role.

Note: If users are in groups that match more than one of the roles, they are given the highest level of access possible (system admin, read-only admin, network admin, then remote-access user).

7. Configure any Group filters you want, and click **Finish**.
8. If you have non-public DNS servers configured in the Conductor under **Global Airwall Agent/client settings**, your users won't be able to reach the public addresses on their devices that include the OpenID Connect providers. You may need to configure DNS servers on the Conductor to add your OpenID Connect provider's DNS server.
9. After changing OIDC configuration, you need to log out and log back in to the Conductor to restart it. When you log back in, you can now choose your third-party authentication provider.

3. Set up the Airwall Agents

Any Airwall Agents authenticating using your third-party provider also need to be set up:

1. Provision and License Airwall Edge Services on page 193 in the Conductor.
2. Go to the **Overlays** page, scroll down to **People**, and click **Update**, and add the Airwall Agent as a member.
3. Also check that:
   a) Airwall Agents are included in your Airwall Relay rules.
   b) Airwall Agent devices have been added to the appropriate Overlays, and you've set device trust on the Overlays as needed.

Your users should now be able to log in using the third-party authentication provider.

Require third-party authentication

You can also require users to authenticate using the third-party provider either individually or as a group (in 2.2.3 and later Conductors). On the agent's **Airwall Agent** tab, or on a **People Group Properties** tab:

- Check the **Require authenticated Airwall session** box.
- Under **Provider**, choose the third-party authentication provider you created.

Provider-specific Instructions

Here are specific instructions for a few of the common third-party authentication providers. Note your provider's documentation may be more up-to-date.

Okta - Create Application and Set Up Group Claims

Create an Application

1. In Okta, go to **Applications**.
2. Select **Add Application**.
3. Under **Create New Application**, select **Web**.
4. Set **Allowed grant type** to **Authorization code**.
5. Set the **OpenID Connect host** to the same value as the **Issuer** in Conductor. This value is found on the under **OpenID Connect ID Token** on the **Sign on** tab.
6. Note the Client ID and Secret that are in your application, on the **General** tab under **Client Credentials**.
7. Set up Groups Claim (see below).

Set up Groups Claim

To set up Okta to allow the groups claim in OpenID Connect, use the Classic UI.

1. In Okta Authentication, go to **Security**, and select **API**.
2. From the **Authorization Servers** tab, open the default API (or whatever API you are assigning to your application).
3. On the **Scopes** tab:
   a) Add a scope named `groups`.
   b) Uncheck **Set as Default**.
   c) Check **Include in Public Metadata**.

4. On the **Claims** tab:

   a) Add a claim named `groups`.

   b) Set **Include in token type** to **ID Token / Always**

   c) Set **Value type** to **Groups**

   d) Set a filter of **Matches regex** to `.*`. Alternatively, set a filter of **Starts with** and set to the prefix for your group names that you want to use in Conductor. For example, set **Starts with** to `cond_`.

   e) Set **Include in** to **Any scope**.

OneLogin - Create Application

1. In OneLogin, select **Add App,** and then choose **OpenID Connect (OIDC)**.
2. Set **Authentication method** to **basic**.
3. Add users to the roles you want. For example, to make them a system admin, add them to **cond_sysadmins**.

   Note: In OneLogin, roles are mapped to OIDC groups (groups mean something else), so add users to roles, not groups.

4. In your OneLogin application, on the **Parameters** tab, configure the roles-to-groups mapping. Edit the groups and modify the default on the **Roles** field to: **User roles, --No transform—**.
5. Note the information you'll need to configure the Conductor:

   a) **OpenID Connect host**: This is your OneLogin login URL, for example, `https://my-company.onelogin.com`.

   b) **Issuer**: On the **SSO** tab, select **OpenID Provider Configuration Information** for the **Issuer**.

   c) **Client ID and Secret**: These are both on the **SSO** tab.

Auth0 - Create Application

1. In Auth0, under **Applications**, select **Create Application**, and then **Regular Web Application**.
2. Skip the quick start.
3. On your new application's **Settings** page:

   a) Change **Application Properties** > **Token Endpoint Authentication Method** to **Basic**.

   b) In **Application URIs** > **Allowed Callback URLs**, add the login redirect URI. See the Login Redirect URI near the top of this page.

   c) In **Application URIs** > **Allowed Logout URLs**, add the logout redirect URI. See the Logout Redirect URI near the top of this page.

   Note: Auth0 does not currently support OpenID Connect Logout.

   d) Note the following information in Auth0 that you'll need to configure the Conductor:

   - **Basic Information** > **Domain**: On the Conductor, you enter this information as **Open Connect host** and **Issuer** (note that the https is required).
   - **Basic Information** > **Client ID** and **Client Secret**: On the Conductor, you enter this information as Client ID and Secret.

   e) When finished, select **Save Changes** at the bottom of the **Settings** page.

4. Add the rule required by Auth0 to set OIDC groups. (In Auth0, roles map to groups on the Conductor.)

   a) Under **Auth Pipeline** > **Rules**, select **Create Rule**.

   b) Select **Empty Rule**.

   c) Set the name to **Add groups to OIDC token**.

   d) Add this rule:

```
function (user, context, callback) {
    const namespace = 'https://<your issuer>';
    const assignedRoles = (context.authorization || {}).roles;
    let idTokenClaims = context.idToken || {};
    let accessTokenClaims = context.accessToken || {};

    idTokenClaims[`${namespace}/groups`] = assignedRoles;
    accessTokenClaims[`${namespace}/groups`] = assignedRoles;

    context.idToken = idTokenClaims;
    context.accessToken = accessTokenClaims;

    callback(null, user, context);
}
```

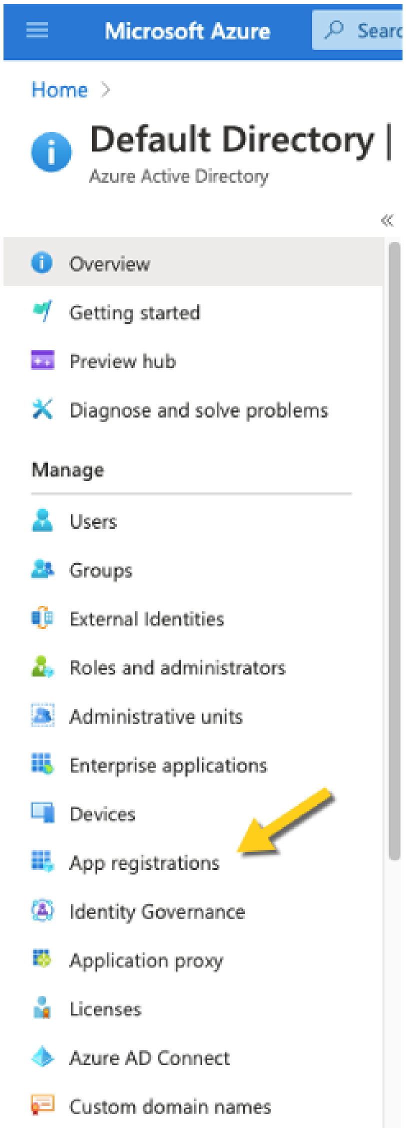
e) Change the namespace in the rule to be your Auth0 issuer. Example: `https://dev-abc123.auth0.com`

5. Following Auth0 instructions, add roles to users that give them the proper role in the Conductor.

Azure Active Directory - Create Application

Note that the Azure AD documentation may be more up-to-date and the settings in your Azure AD account may vary.

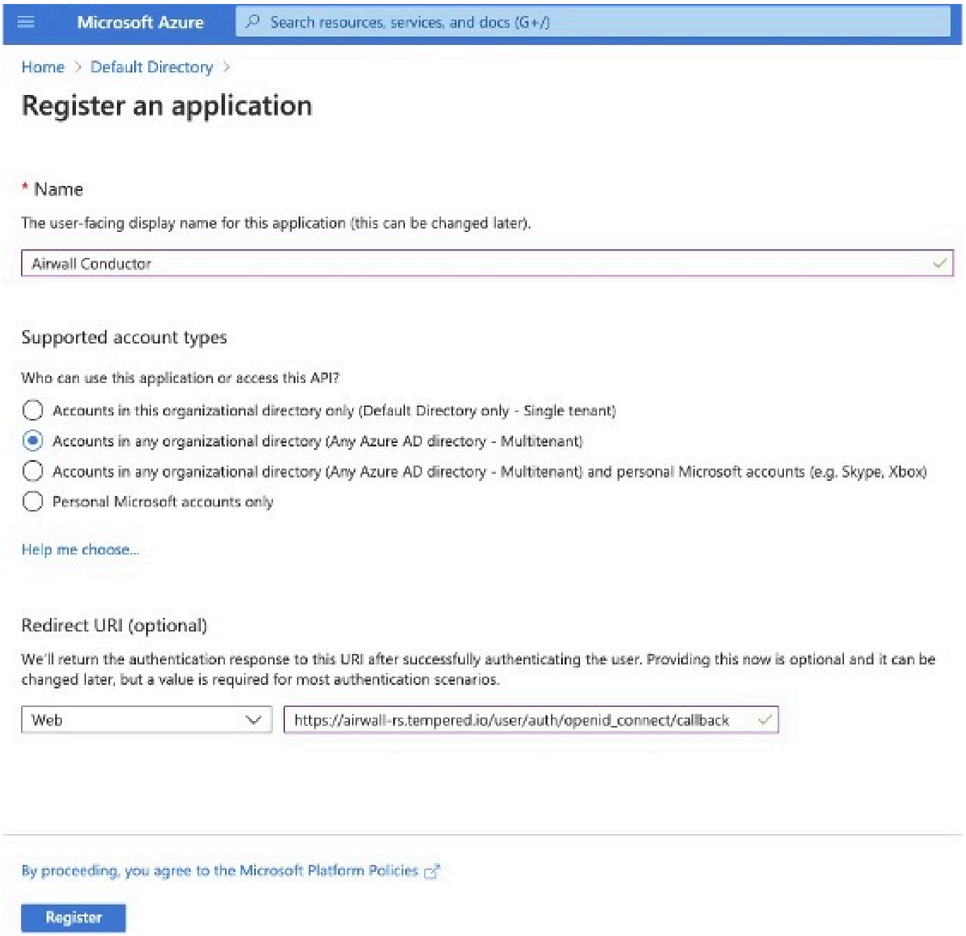
1. In Azure Active Directory (AD), select **App registrations**.



2. Select **New Registration**, and fill in the form as follows:

- **Name** – Enter a name for the Application (for example, "Airwall Conductor").

- **Supported account types** – Select **Accounts in any organizational directory (Any Azure AD directory – multitenant)**.
- **Redirect URI** – Select **Web**, and then enter the URL of your Conductor followed by `/user/auth/openid_connect/callback`:



Microsoft Azure

Search resources, services, and docs (G+/)

Home > Default Directory >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

Airwall Conductor ✓

Supported account types

Who can use this application or access this API?

○ Accounts in this organizational directory only (Default Directory only - Single tenant)

● Accounts in any organizational directory (Any Azure AD directory - Multitenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

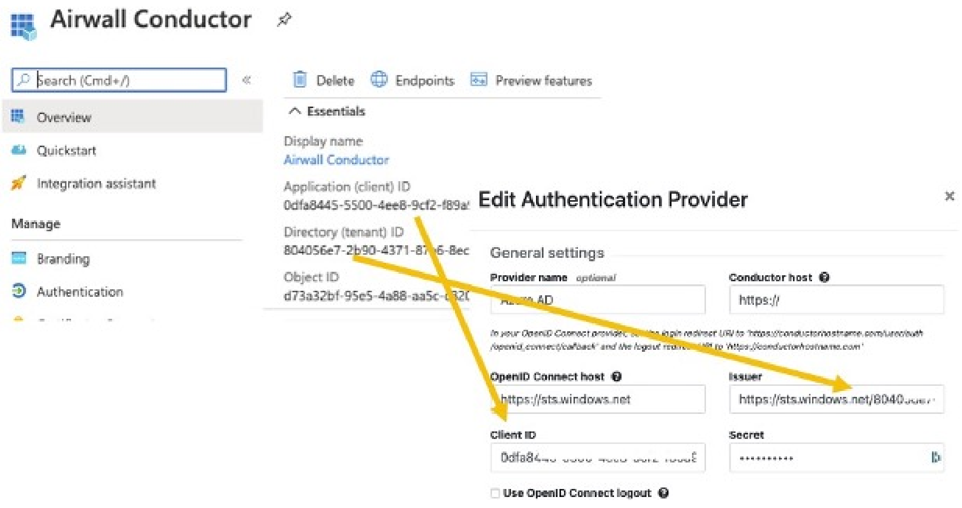
Web | https://airwall-rs.tempered.io/user/auth/openid_connect/callback ✓

By proceeding, you agree to the Microsoft Platform Policies

Register

3. Click **Register**. Take a note of the Application (client) ID and the Directory (tenant) ID provided by Azure AD.

   Once you've registered the Application, Azure AD provides a set of IDs that you configure in the Conductor when you set up Azure AD as an OIDC provider. Here is how they map to the Edit Authentication Provider options in the Conductor:



Airwall Conductor

Search (Cmd+/)

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Delete | Endpoints | Preview features

Essentials

Display name
Airwall Conductor

Application (client) ID
0dfa8445-5500-4ee8-9cf2-f89a

Directory (tenant) ID
804056e7-2b90-4371-87[illegible]6-8ec

Object ID
d73a32bf-95e5-4a88-aa5c-[illegible]

Edit Authentication Provider ×

General settings

Provider name *optional*: Azure AD

Conductor host: https://

In your OpenID Connect provider, [illegible] login redirect URI to 'https://conductorhostname.com/user/auth/openid_connect/callback' and the logout [illegible] URI to 'https://conductorhostname.com'

OpenID Connect host: https://sts.windows.net

Issuer: https://sts.windows.net/8040[illegible]

Client ID: 0dfa84[illegible]

Secret: ••••••••••

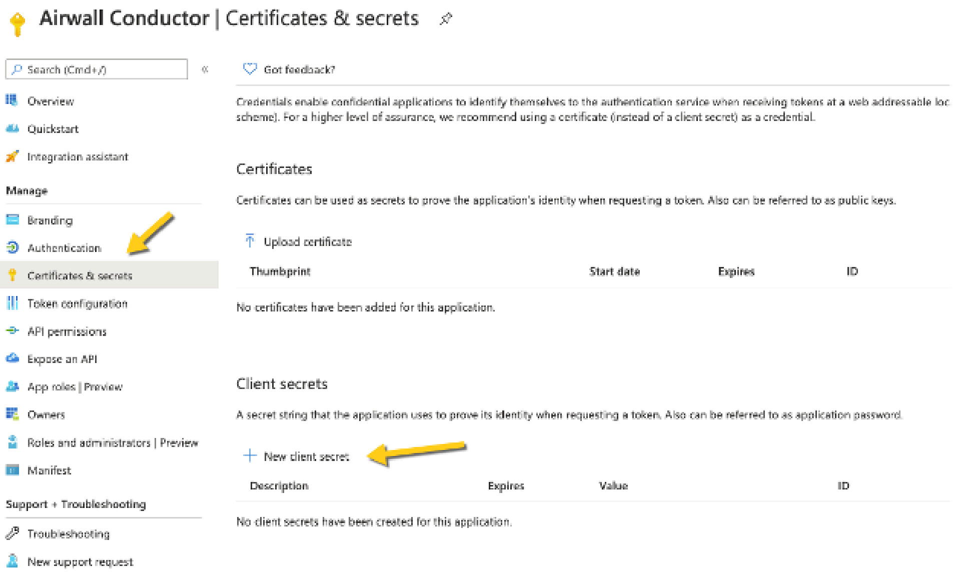
□ Use OpenID Connect logout

- Application (client) ID – Enter in the **Client ID** box.
- Directory (tenant) ID – Append this ID to `https://sts.windows.net/`and enter in the **Issuer** box .

4. In Azure AD, create a Client Secret:

a) Select **Certificates & secrets**.

b) Select **New client secret**.



Airwall Conductor | Certificates & secrets

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable loc scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires	ID

No certificates have been added for this application.

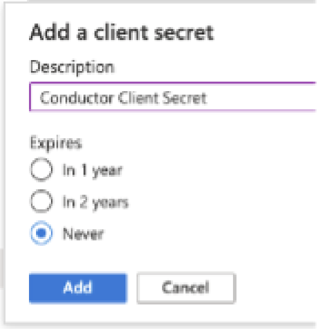
Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	ID

No client secrets have been created for this application.

c) Add a description, and select when the secret expires.



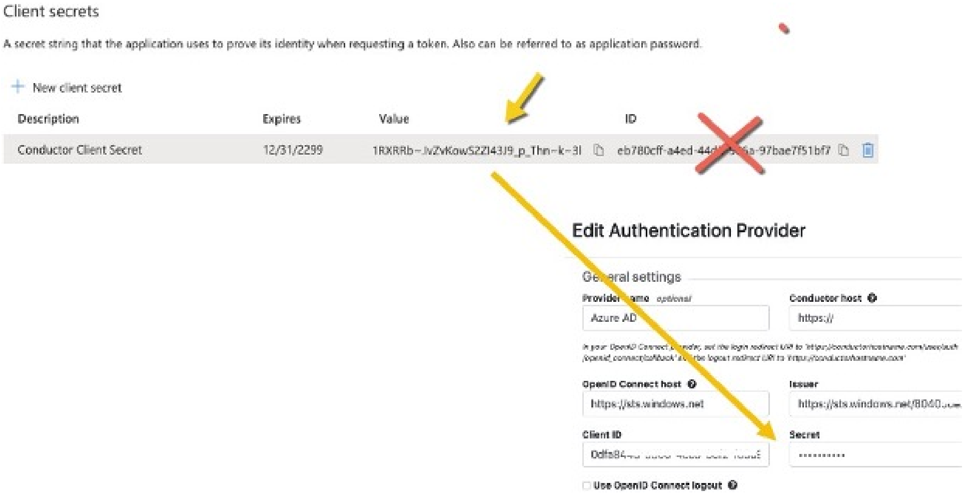
Add a client secret

Description: Conductor Client Secret

Expires
○ In 1 year
○ In 2 years
● Never

d) Select **Add**.

5. On the **Client secrets** page, copy the **Value** (not the ID). Enter the Value as the secret in the Conductor.



Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	ID
Conductor Client Secret	12/31/2299	1RXRRb~JvZvKowS2Zl43J9_p_Thn~k~3l	eb780cff-a4ed-44d[illegible]a-97bae7f51bf7

Edit Authentication Provider

General settings

Provider name *optional*: Azure AD

Conductor host: https://

In your OpenID Connect provider, set the login redirect URI to 'https://conductorhostname.com/users/auth/openid_connect/callback' and the logout redirect URI to 'https://conductorhostname.com'

OpenID Connect host: https://sts.windows.net

Issuer: https://sts.windows.net/8040...

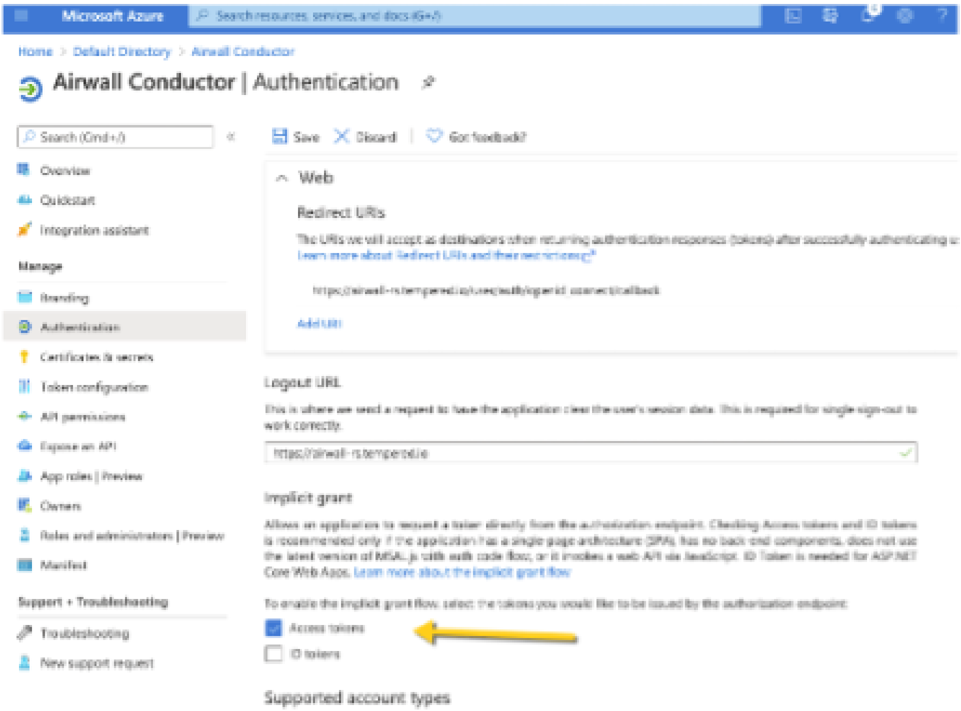
Client ID: 0dfa84[illegible]

Secret: ••••••••••

□ Use OpenID Connect logout

6. From the newly registered application in Azure AD, select **Authentication**.

7. Under **Implicit grant**, verify that **ID tokens** is checked.



Web

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating u

Learn more about Redirect URIs and their restrictions

https://airwall-rs.tempered.io/user/auth/openid_connect/callback

Logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

https://airwall-rs.tempered.io

Implicit grant

Allows an application to request a token directly from the authorization endpoint. Checking Access tokens and ID tokens is recommended only if the application has a single page architecture (SPA), has no back-end components, does not use the latest version of MSAL.js with auth code flow, or it invokes a web API via JavaScript. ID Token is needed for ASP.NET Core Web Apps. Learn more about the implicit grant flow

To enable the implicit grant flow, select the tokens you would like to be issued by the authorization endpoint:

☑ Access tokens

□ ID tokens

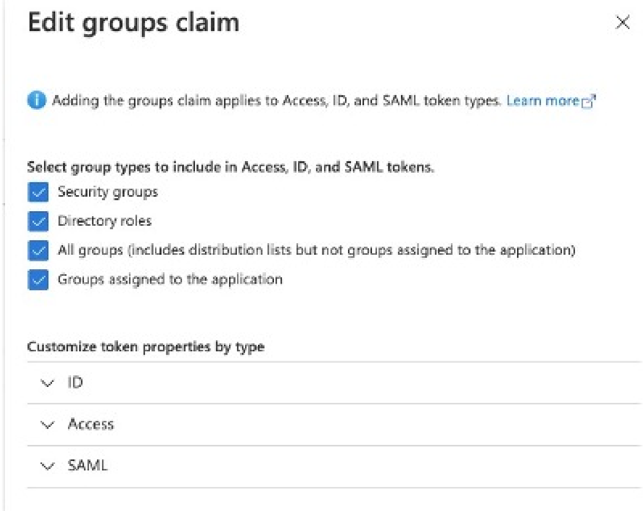
Supported account types

8. In the Azure AD application, set up the groups claim:

   a) From the menu on the left, select **Token configuration**.

   b) Select Add groups claim.

   c) Check all of the group types:



Adding the groups claim applies to Access, ID, and SAML token types.

Select group types to include in Access, ID, and SAML tokens.

☑ Security groups

☑ Directory roles

☑ All groups (includes distribution lists but not groups assigned to the application)

☑ Groups assigned to the application

Customize token properties by type

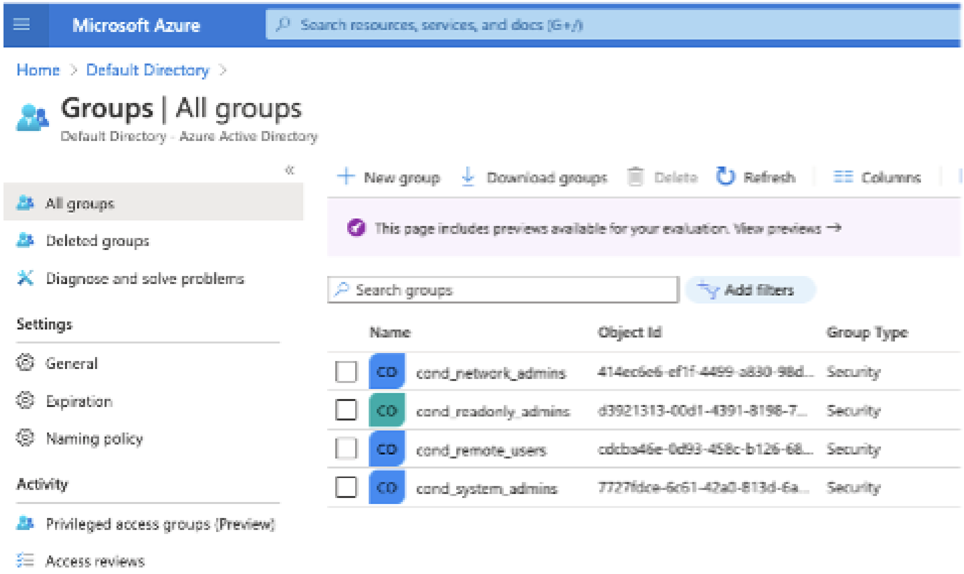
- ID
- Access
- SAML

   d) Under Customize token properties by type, expand and configure the properties as follows:

   - **ID** – Select **sAMAccountName**.
   - **Access** – Select **sAMAccountName**.
   - **SAML** – This is not used.

9. In Azure AD, create the groups you want to use for the Conductor. Here are some suggested groups:

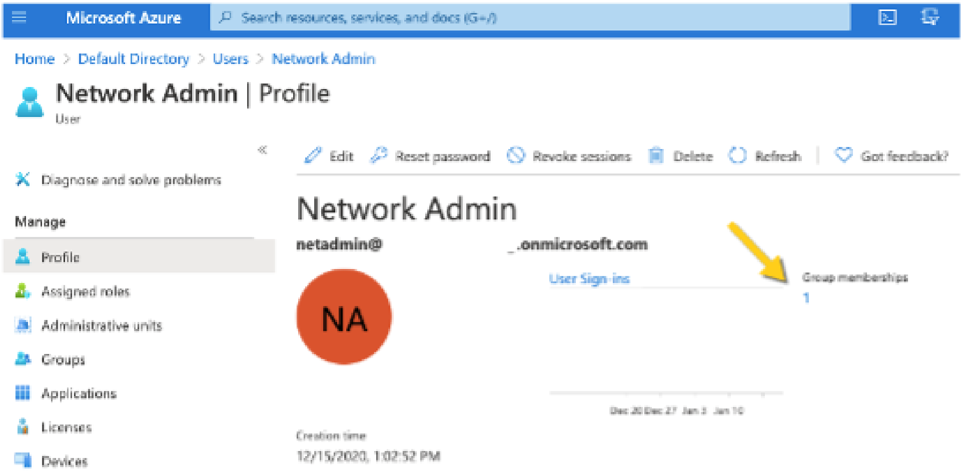
- cond_network_admins
- cond_readonly_admins
- cond_remote_users
- cond_system_admins



This page includes previews available for your evaluation. View previews →

	Name	Object Id	Group Type
□ CO	cond_network_admins	414ec6e6-ef1f-4499-a830-98d...	Security
□ CO	cond_readonly_admins	d3921313-00d1-4391-8198-7...	Security
□ CO	cond_remote_users	cdcba46e-0d93-458c-b126-68...	Security
□ CO	cond_system_admins	7727fdce-6c61-42a0-813d-6a...	Security

10. Add users to Azure AD, and assign them to the appropriate groups for Conductor access:



Network Admin

netadmin@ _.onmicrosoft.com

Creation time
12/15/2020, 1:02:52 PM

You are now ready to configure Azure AD as an OIDC provider in the Conductor as described in 2. Configure OIDC on the Airwall Conductor on page 248. For the mappings from Azure AD to the Conductor, see steps 3 to 7 above.

Verify third-party authentication is working

To verify your configuration:

1. Log out of the Conductor.
2. Open an incognito window and log in, choosing the provider name you chose in the Conductor.
3. Log in as a user you've set up with third-party provider. You should be able to log in to the Conductor using your third-party provider credentials.

To verify a client can connect:

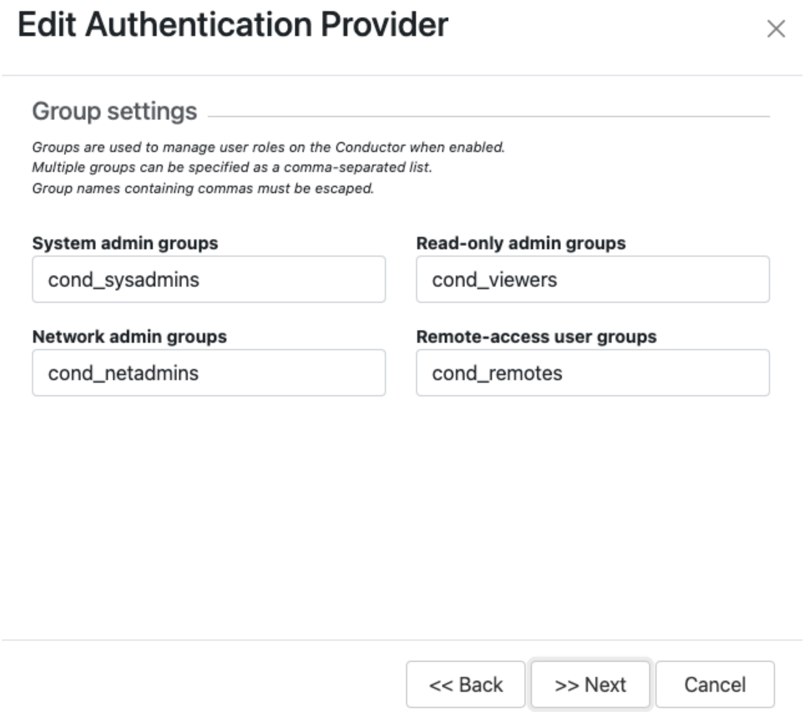
- After the client logs in using the third-party provider, ping the client.

Troubleshooting Third-party Authentication User Login

If user login is failing with "Could not find that username/password combination," usually the integration between the Conductor and OpenID Connect (OIDC) provider is working, but something about group membership is not correctly configured. Use these suggestions to troubleshoot what the issue is.

Check Conductor and OIDC provider group settings

1. On the Conductor, go to **Settings** > **General settings** > **Authentication** > **Your OIDC provider**.
2. Select **Actions** > **Edit**.
3. Select **Next**, and confirm that **Group settings** on the second page are filled out.



Edit Authentication Provider

Group settings

Groups are used to manage user roles on the Conductor when enabled.
Multiple groups can be specified as a comma-separated list.
Group names containing commas must be escaped.

System admin groups: cond_sysadmins

Read-only admin groups: cond_viewers

Network admin groups: cond_netadmins

Remote-access user groups: cond_remotes

4. In your OIDC provider, confirm that the groups you have chosen for each role have been created.
5. Confirm that the user that is trying to log in is a member of one of the groups that will give them a role on the Conductor. For example, if this user should be a Read-only admin then they should be in the “cond_viewers” group in the OIDC provider.

Follow the Log

If you've confirmed steps 1-3 are configured and are still having issues, follow the log to gain more information.

1. Under **Settings** > **General Settings** > **Other settings** > **Logging settings**, if you are logging at warn or error levels, change logging to at least info.
2. Go to **Settings** > **Airshell** > **Open remote Airshell**.
3. Enter the command: `log follow`. You should now see Conductor logs in the virtual terminal.
4. Have the user attempt to log in again with OIDC. If this is you, do not log out of the Airshell terminal – use a private browser window.
5. When the user completes login, there should be a log message for the user attempting to login such as

```
1Mar 11 20:57:34 kibbles SCMP[30051]: OpenID user
'google-oauth2|115620360600894761234' allowed groups: ["cond_netadmins"]
```

6. If the allowed groups is empty, the optional “groups” claim may not be correctly configured on the OIDC provider. Please refer to the specific documentation for your OIDC provider to allow the Conductor to receive the “groups” claim.
7. If there are allowed groups but none apply to a Conductor role are there three possible problems:
   a) The user is not a member of the group you expected
   b) The groups are being filtered by the OIDC provider. Please check your OIDC provider configuration.
   c) The groups are being filtered by the Conductor configuration. Check the configuration for your OIDC provider. The Conductor does attempt to prevent you from creating a filter that would invalidate groups assigned for roles.

Configure LDAP authentication on Conductor and Airwall Edge Services

You can use Active Directory and LDAP authentication with the Conductor to streamline user account management. When LDAP is configured, users can choose to log in with an LDAP account on the Conductor login page.

There are currently three different ways to authenticate with Conductor.

- With a Conductor account. These are local accounts that log directly into the device
- With LDAP authentication. This allows you to authenticate with any LDAP server, including Microsoft Active Directory services.
- With a third-party authentication provider that supports OpenID Connect. See Integrate Third-party Authentication with OpenID Connect on page 247.

To set up a LDAP authentication, you need to already have an LDAP server accessible to the Conductor.

Note: These instructions use Microsoft Active Directory, but other LDAP services also work.

There are four different roles in the Conductor:

- **System Administrator** – These users have full access to the Conductor and can adjust any settings. Note that to edit LDAP settings, you must be logged in locally to the Conductor, not through LDAP.
- **Read-only System Administrator** – These users have read access to the Conductor, but cannot make changes.
- **Network Administrator** – These users have access to and can adjust any overlay network they are a manager of. They do not have access to Conductor Settings.
- **Remote Access User** – These users can only see their own information, and can log in with their credentials if authentication is required for their Airwall Agent or Server.

For more detailed role information, see Understand People Roles and Permissions on page 58.

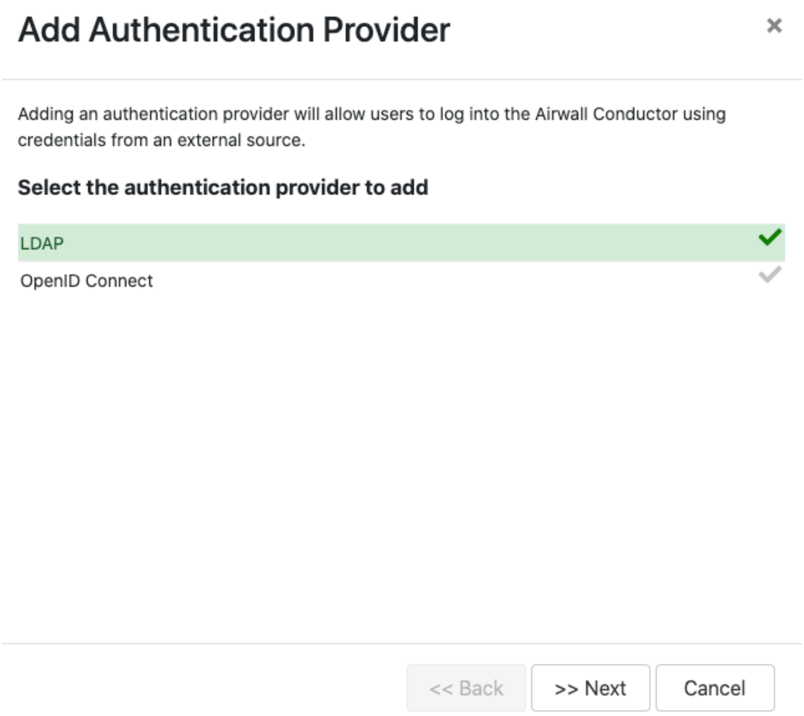
Step 1: Set up and configure your LDAP server

LDAP is not enabled in Active Directory by default, so you will have to turn it on. Once you have LDAP working and running, you can start.

Create a dedicated account with the necessary permissions to authenticate. In Active Directory, you could create a service account under the root "Users" OU, and make it a Domain Admin.

Step 2: Enter and verify your local Conductor admin account credentials, and select Authentication provider

1. Log into Conductor locally (not through LDAP) as a System Administrator. (Only local administrators have access to authentication provider settings.)
2. Open **Settings**, and next to **Authentication**, select **Add Provider**.
3. Select **LDAP** from the list of providers.



Add Authentication Provider

Adding an authentication provider will allow users to log into the Airwall Conductor using credentials from an external source.

Select the authentication provider to add

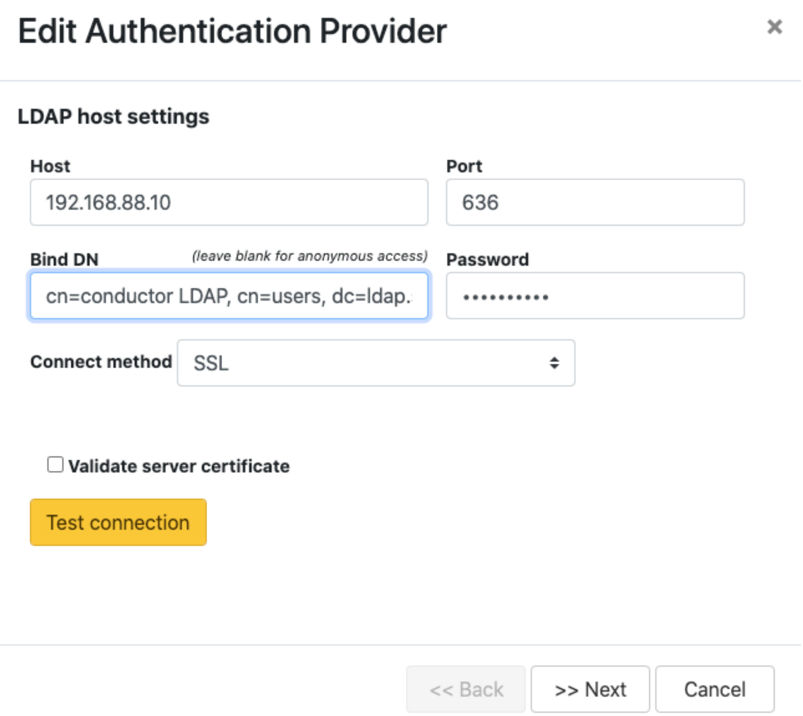
- LDAP ✓
- OpenID Connect ✓

Step 3: Enter your LDAP settings

You will need to know the following values:

- Host (Hostname or IP address)
- Port (636 is the default)
- If you are using a dedicated LDAP service account, the fully-distinguished path for the user account, and the password

Under **LDAP host settings**, enter the information for your LDAP host, and select **Next**. For more details on these settings, see LDAP host settings on page 263.



Edit Authentication Provider

LDAP host settings

Host: 192.168.88.10

Port: 636

Bind DN (leave blank for anonymous access): cn=conductor LDAP, cn=users, dc=ldap.

Password: ••••••••••

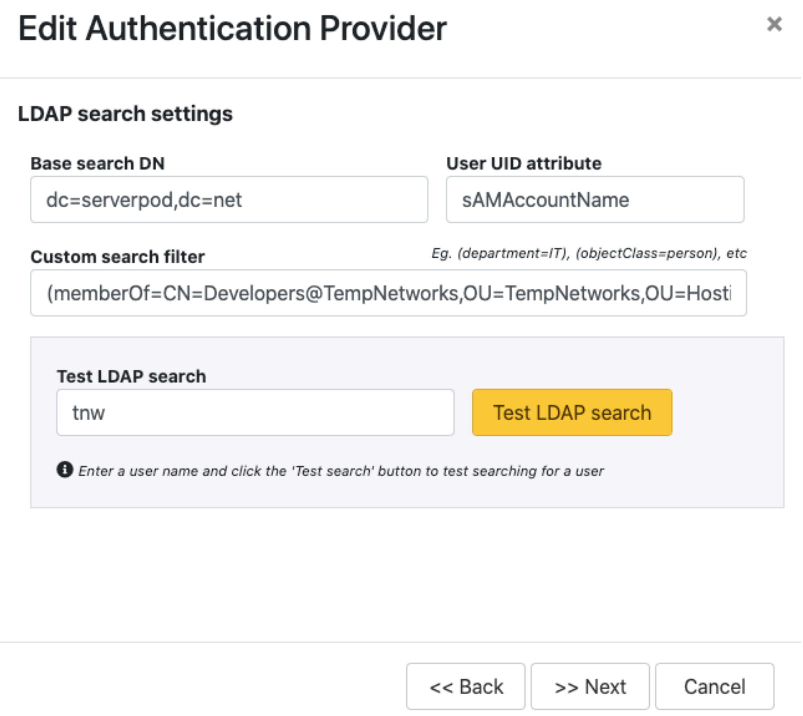
Connect method: SSL

□ Validate server certificate

Note: TLS LDAPS communication occurs over port TCP 636. LDAPS communication to a global catalog server occurs over TCP 3269. When connecting to ports 636 or 3269, SSL/TLS is negotiated before any LDAP traffic is exchanged.

Step 4: Configure Search Settings

This page can mostly be left as-is, unless you have special settings you wish to set. You can search for user accounts here to ensure that the Conductor can search the directory. Select **Next**. For more details on these settings, see LDAP search settings on page 264.



Edit Authentication Provider

LDAP search settings

Base search DN: dc=serverpod,dc=net

User UID attribute: sAMAccountName

Custom search filter (Eg. (department=IT), (objectClass=person), etc): (memberOf=CN=Developers@TempNetworks,OU=TempNetworks,OU=Hosti

Test LDAP search: tnw

Enter a user name and click the 'Test search' button to test searching for a user

You can test the search by entering a search term and selecting **Test LDAP search**.

Step 5: Configure Group Settings

The Conductor assigns LDAP users to one of the four account types above by making them a member of a security group.

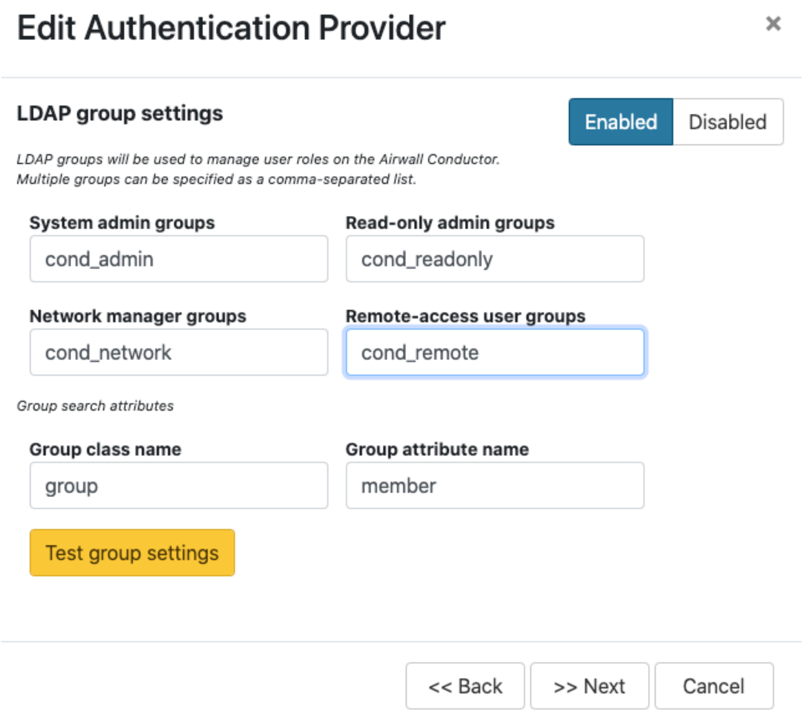
If you do not have appropriate groups already, create these groups in LDAP to link to Conductor roles (you can use different names – using cond_ makes it easier to see which roles are for the Conductor). By default, these groups place the users into the following roles:

- **cond_admin** – System Administrator
- **cond_readonly** – Read-only System Administrator
- **cond_network** – Network Administrator
- **cond_remote** – Remote Access User

Since users cannot have more than one role at a time, if they are members of multiple groups, they'll be assigned the role with the most permissions.

Remember to test the settings to ensure that Conductor can see all of the groups you reference on your LDAP server.

1. For **LDAP group settings**, enter the groups for the roles you want LDAP users to have, and **Group search attributes**, and select **Next**. For more details on these settings, see LDAP group settings on page 264.



Edit Authentication Provider

LDAP group settings

LDAP groups will be used to manage user roles on the Airwall Conductor. Multiple groups can be specified as a comma-separated list.

System admin groups: cond_admin

Read-only admin groups: cond_readonly

Network manager groups: cond_network

Remote-access user groups: cond_remote

Group search attributes

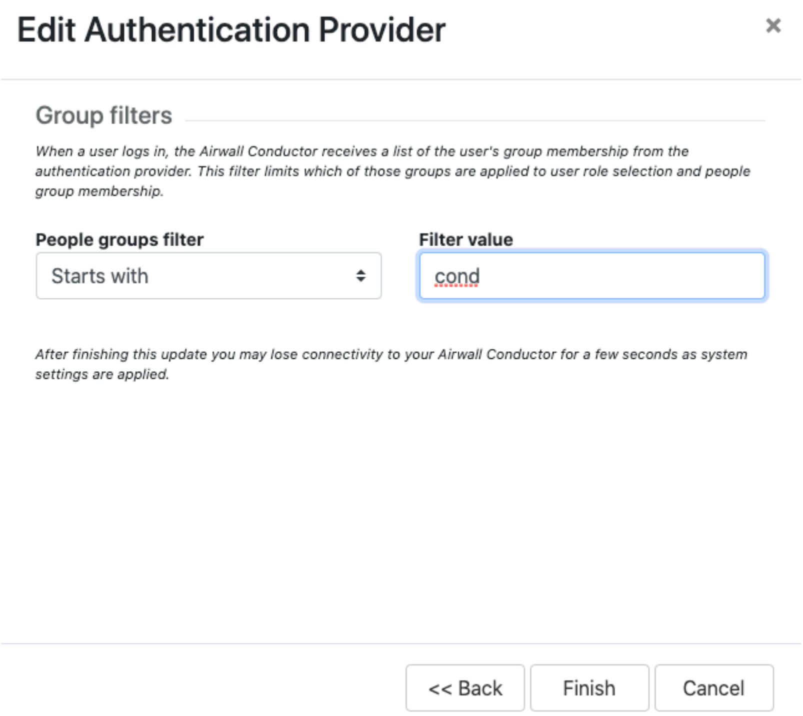
Group class name: group

Group attribute name: member

You can also add other security groups to the configuration, separated by commas.

Note: You can set up these groups on your LDAP server after setting up LDAP on the Conductor, but **Test group settings** will fail.

2. For **Group filters**, enter filters to specify which LDAP groups the Conductor sees. For example, if you've created the cond_ groups above, you may want to set the filter to **Starts with** with a value of `cond`.



Edit Authentication Provider

Group filters

When a user logs in, the Airwall Conductor receives a list of the user's group membership from the authentication provider. This filter limits which of those groups are applied to user role selection and people group membership.

People groups filter: Starts with

Filter value: cond

After finishing this update you may lose connectivity to your Airwall Conductor for a few seconds as system settings are applied.

3. Select **Finish**
   You may lose connection briefly as the new settings are applied.

Step 6: Configure user onboarding

Configure user onboarding for the people groups created above to give users access to overlay networks through Airwall Agents and Servers. Setting the groups up beforehand simplifies user onboarding.

1. In the Conductor, create **People groups** that match the LDAP groups you specified above (for example, cond-admin)
2. Specify user onboarding options as you create the groups. For details, see Set up a People Group on page 89.

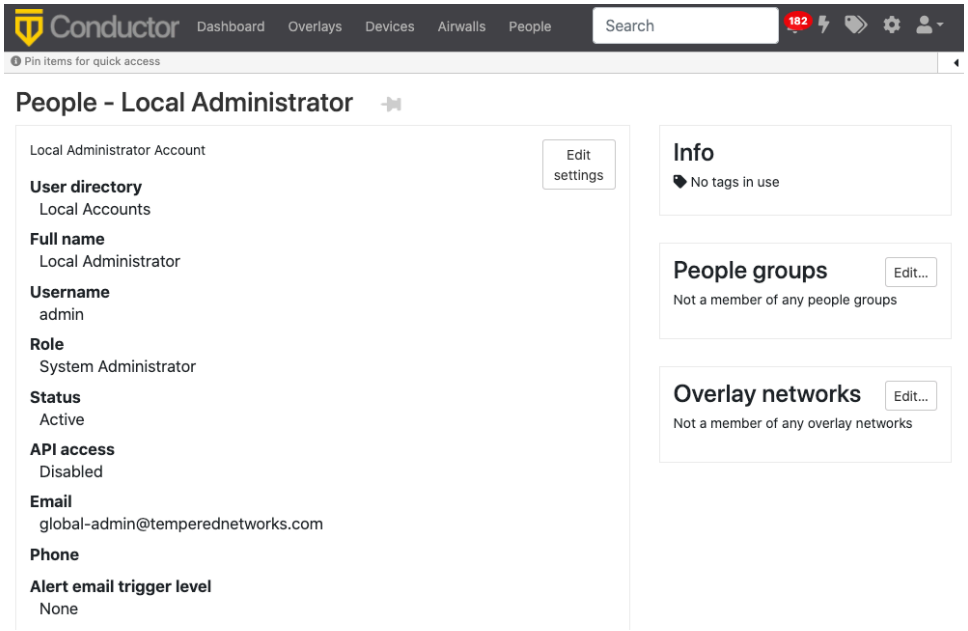
As users log in through LDAP, they are added to these **People groups** and given an activation code that activates the permissions and other options you specified for the **People groups**.

Step 7: Set up Conductor management access

You can also set up access for your Conductor system and network admins individually.

1. **Add administrators to Overlays** – Add administrators individually as members of Overlay networks to give them access to the resources they need. You can add them from their **People** page, or from an Overlay page:

   - **From the person's People page**, next to **Overlay networks**, select **Edit**. Add the person as a member or manager of Overlays.



People - Local Administrator

Local Administrator Account

User directory
Local Accounts

Full name
Local Administrator

Username
admin

Role
System Administrator

Status
Active

API access
Disabled

Email
global-admin@temperednetworks.com

Phone

Alert email trigger level
None

Info

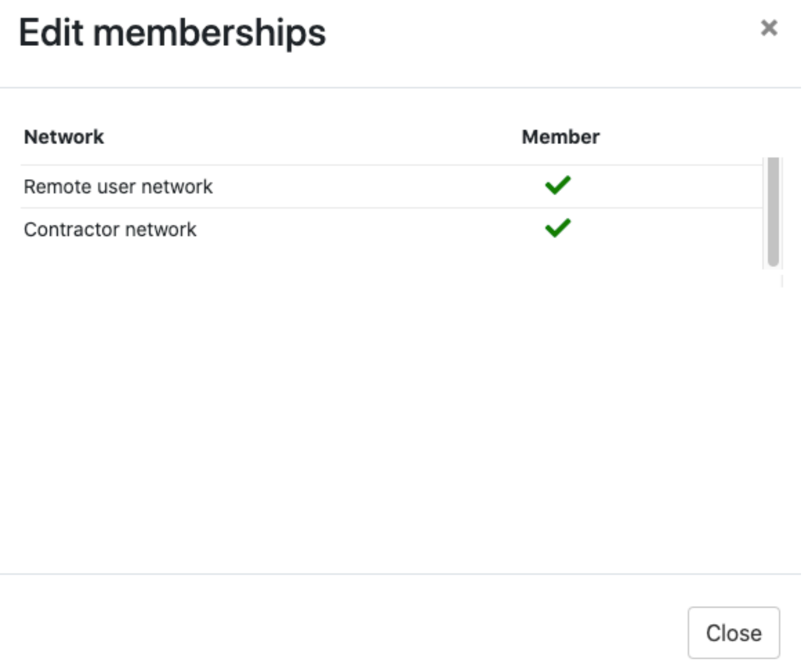
No tags in use

People groups

Not a member of any people groups

Overlay networks

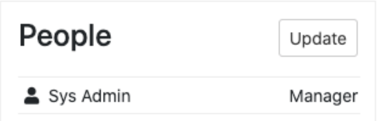
Not a member of any overlay networks



Edit memberships

Network	Member
Remote user network	✓
Contractor network	✓

- **From the Overlays page**, open the overlay, and under **People**, select **Update**. Add the administrators as members or managers of the overlay.



People

Sys Admin	Manager

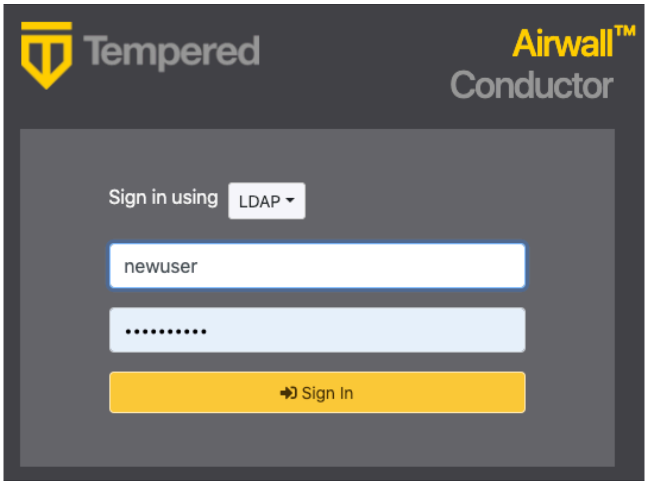
2. **Add administrators to People groups** – Similarly, you can add administrators to **People groups**, from their People page or add several administrators from the People group:

   - **From a person's People page** – Next to **People groups**, select **Edit** and select the **People groups** with the permissions they need.
   - **From a People group** – Open the **People group**, and on the **People** tab, select the people to add.

Step 8: Verify by logging in to the Conductor

Verify that LDAP is set up by logging in and checking permissions.

1. Log out from your local administrator account.
2. Next to **Sign in using**, select **LDAP**, and log into the Conductor with an LDAP account.



Sign in using: LDAP

newuser

••••••••••

3. Check that permissions are set correctly for that user.

See also: Configure user authentication for Airwall Agents and Airwall Servers on page 243.

LDAP host settings

LDAP host setting	Description
Host	The hostname or IP address of your Active Directory or server.
Port	• Select 389 for Plain or TLS - This option is only available for SSL or TLS connect methods, and is only enabled if you have uploaded CA certificates. • Select 636 for SSL. **Note:** TLS LDAPS communication occurs over port TCP 636. LDAPS communication to a global catalog server occurs over TCP 3269. When connecting to ports 636 or 3269, SSL/TLS is negotiated before any LDAP traffic is exchanged.
Bind DN	If you are using a dedicated LDAP service account, enter the fully-distinguished path for the user account, and then enter the password for the account in the next box. • CN=*User Full Name* • CN=*User OU* • DC=*Domain Component 1* • DC=*Domain Component 2* An example of a fully-distinguished path: `CN=ldapServceAccount,OU=ServiceAccounts,OU=Users,DC=mySecureCorpD` If you are using user accounts for LDAP Bind connection authentication and authorization, leave **Bind DN** and **Password** blank, providing anonymous access.
Password	Enter the password for the user account (specified in BindDN) used to connect to the LDAP service. Leave blank if **Bind DN** is blank.

LDAP host setting	Description
Connect method	• Plain - Do not use encryption to communicate with the LDAP server. **Not recommended.** • SSL - Use the SSL protocol to communicate with the LDAP server. • TLS - Use the TLS protocol to communicate with the LDAP server.
Validate server certificate	Select to validate the LDAP server's security certificate against the local CA certificate store.

LDAP search settings

LDAP search setting	Description
Base search DN	Enter the root of the tree in LDAP, underneath which your users and groups are defined.
User UID attribute	Enter the name of the attribute that contains the user's login name: • For Active Directory: *sAMAccountName* • For LDAP: *uid*
Custom search filter	Use to limit user search results, or to filter to only user entries in LDAP (filtering out non-user entries that are present in the user directory).
Test LDAP search	Enter a username and click **Test LDAP Search** to test your search settings. This test queries the LDAP directory for the given user using your current settings, and displays the number of records located, if any. **Best Practice:** Make sure this test is successful before continuing.

LDAP group settings

LDAP group setting	Description
System admin groups	Add the LDAP groups that contain members you want to have System Administrator access. Add only trusted groups to this setting.
Read-only admin groups	Add the LDAP groups that contain members you want to have read-only access. Add only trusted groups to this setting.
Network manager groups	Add the LDAP groups for members you want to have permissions to manage overlay networks. You can define which overlay networks they have access to by onboarding people using **People groups** before they log in, or individually after the user has logged in for the first time.
Remote access user groups	Add the LDAP groups for members you want to have remote access. You can define which overlay networks they have access to by onboarding people using **People groups** before they log in, or individually after the user has logged in for the first time.
Group class name	Enter the name of an objectClass that the group entry must contain in the LDAP directory, such as: • Active Directory: *group* • LDAP: *posixGroup*
Group attribute name	Enter the name of the attribute in the group entry that contains the list of users in that group: • Active Directory: *member* • LDAP: *memberUID*

LDAP group setting	Description
Test group settings	Select to test your group settings. **Best Practice:** Make sure this test is successful before continuing.

Configure LDAP to manage user roles

You can use Active Directory and LDAP authentication with the Conductor to streamline user account management. When LDAP is configured, users can choose to log in with an LDAP account on the Conductor login page. See Configure LDAP authentication on Conductor and Airwall Edge Services on page 257.

1. Log in to the Conductor with a System Administrator account and go to **Settings** > **Authentication** > **External authentication providers**.
2. Next to **LDAP**, and click **Next**.
3. Enter the LDAP host settings (see LDAP host settings on page 263), and click **Test Connection** to validate that your LDAP settings are valid, then click **Next**.
4. Enter the LDAP search settings (see LDAP search settings on page 264) and click **Test LDAP search** to validate that the your LDAP search is valid. Once the test confirms a valid LDAP search, click **Next**.
5. Determine whether you want to use LDAP groups to manage Conductor user roles:
   - To use LDAP groups: Enter the LDAP group settings (see LDAP group settings on page 264), and click **Test** to verify the group settings. Once the test confirms your group settings, click **Finish**.
   - No LDAP groups: If you do not want to use LDAP groups, simply click **Finish**.

Your LDAP configuration is now complete, and can be managed as needed in **Settings** > **Authentication**.

Note: TLS LDAPS communication occurs over port TCP 636. LDAPS communication to a global catalog server occurs over TCP 3269. When connecting to ports 636 or 3269, SSL/TLS is negotiated before any LDAP traffic is exchanged.

Optional Conductor Configuration

How to configure optional features on your Conductor.

Configure a Conductor for High Availability

Conductor High Availability (HA) provides hardware redundancy between two Conductors and requires a manual failover. When creating a Conductor HA pair, one Conductor is assigned as the active and the second is assigned as the standby. The active Conductor is used to manage Airwall Edge Services, overlay networks and communications policies.

As a system administrator, you can access a standby Conductor, but only limited functionality is available. In standby mode, the Conductor is kept in sync with the active Conductor, but has limited functionality as follows:

- Read-only database
- Conductor HA configuration changes
- System setup changes
- Firmware updates

Using failover

You need to manually initiate failover between the active and the standby Conductor. The manual failover can take several minutes to complete. During this time, the Airwall Edge Services and devices continue to operate in their current configurations, and overlay network communications are not interrupted.

Automatically Create an Standby HA Conductor in the Cloud

The Conductor has automated the process of setting up a High Availability (HA) Conductor in the cloud.

Once you’ve set up the cloud provider on your active/master Conductor, setting up and configuring a standby using the Conductor is simple and eliminates many of the mistakes that can happen when manually configuring a standby Conductor in the cloud.

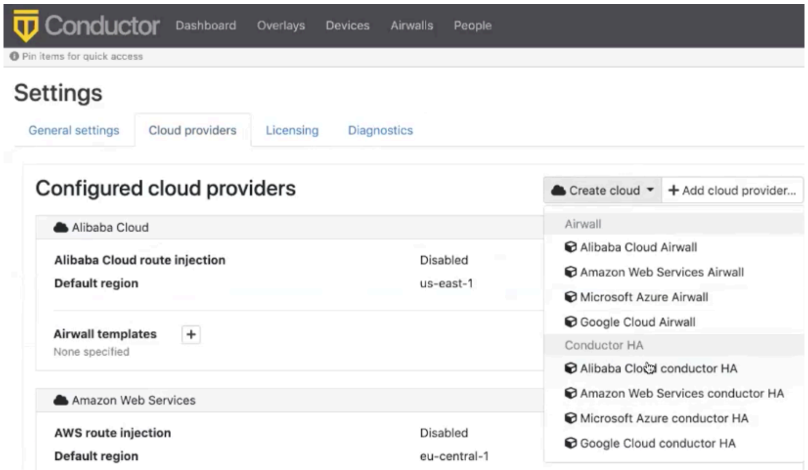
Before you begin

Before you can create a cloud standby Conductor automatically, you must:

- Have an account with a cloud provider
- Have your active/master Conductor set up in the same cloud provider
- Have a Conductor voucher for your new standby Conductor
- Set up a cloud provider in the Conductor. See Set up Cloud Providers on page 433.

To set up a Cloud HA Conductor

1. On the Conductor that you want to be active for the HA pair, go to the **Settings** page.
2. On the **Cloud providers** tab, select **Create cloud**.
3. Under **Conductor HA**, select the same cloud provider as your active Conductor.



Alibaba Cloud

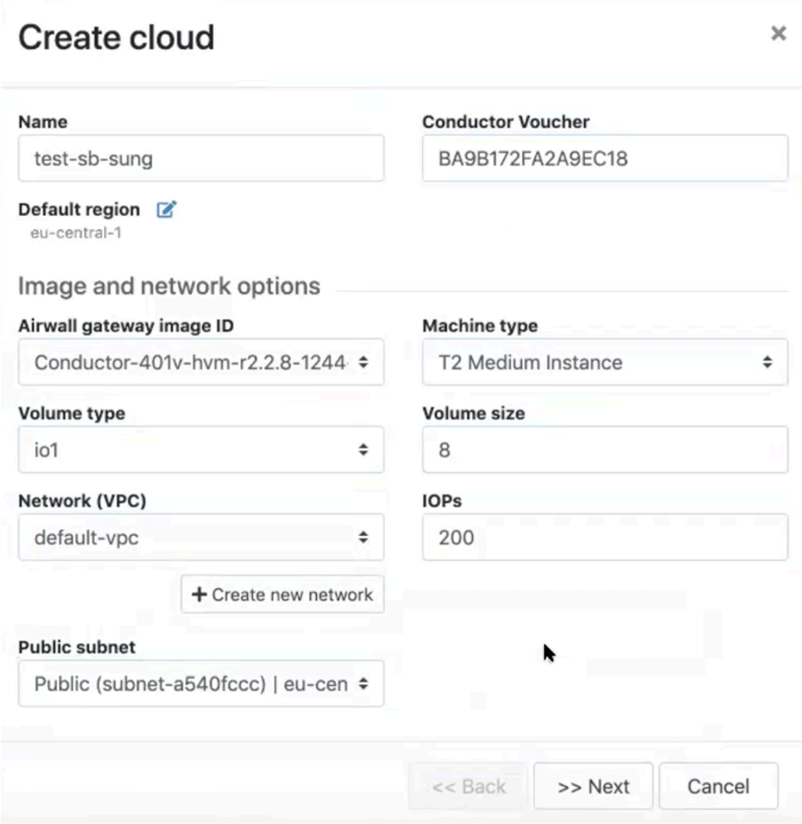
Alibaba Cloud route injection Disabled
Default region us-east-1

Airwall templates +
None specified

Amazon Web Services

AWS route injection Disabled
Default region eu-central-1

4. On the **Create cloud** page:
   a) **Name** – Enter a deployment name for your standby Conductor.
   b) **Conductor Voucher** – Add the Conductor voucher for your standby Conductor.
   c) **Default region** – Select your region from the cloud provider list.
5. Under **Image and network options**, select the cloud provider details for your new Conductor. Only Conductor images matching your active Conductor are displayed. Select the **Network (VPC)** to bring up the options for the public subnet from your cloud provider.



Create cloud

Name: test-sb-sung

Conductor Voucher: BA9B172FA2A9EC18

Default region: eu-central-1

Image and network options

Airwall gateway image ID: Conductor-401v-hvm-r2.2.8-1244

Machine type: T2 Medium Instance

Volume type: io1

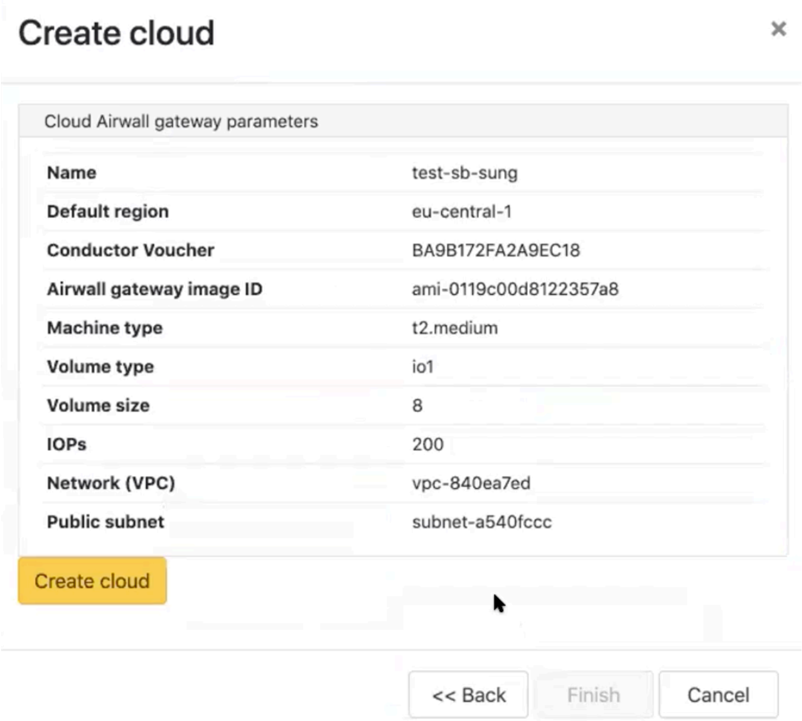
Volume size: 8

Network (VPC): default-vpc

IOPs: 200

Public subnet: Public (subnet-a540fccc) | eu-cen

6. Click **Next**
7. Check that the parameters are correct, and click **Create cloud**.

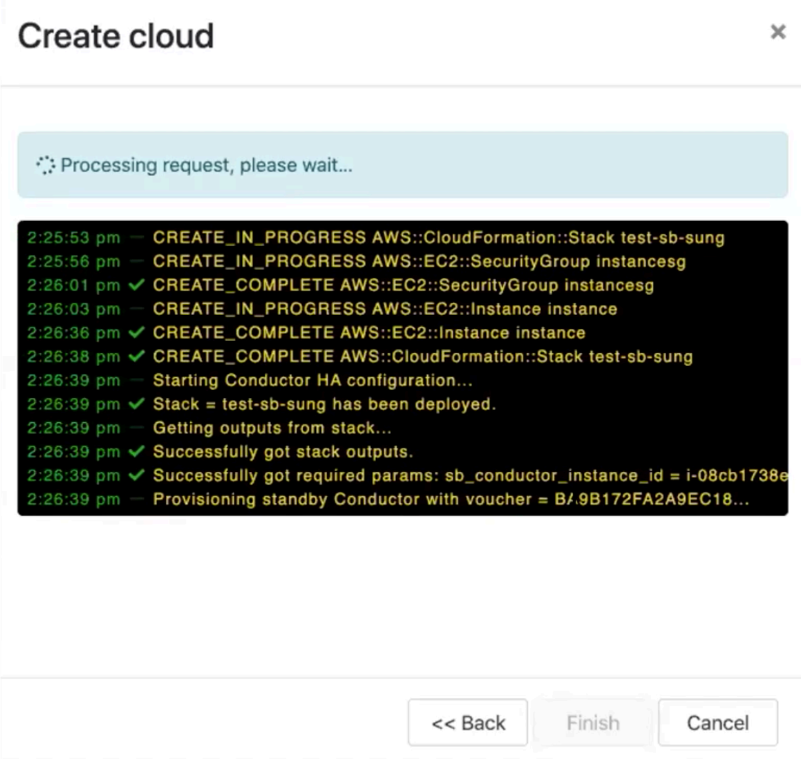


Create cloud

Cloud Airwall gateway parameters	
Name	test-sb-sung
Default region	eu-central-1
Conductor Voucher	BA9B172FA2A9EC18
Airwall gateway image ID	ami-0119c00d8122357a8
Machine type	t2.medium
Volume type	io1
Volume size	8
IOPs	200
Network (VPC)	vpc-840ea7ed
Public subnet	subnet-a540fccc

8. Wait for the active Conductor to create and provision a new Conductor, and then configure it automatically as a standby Conductor. The **Create cloud** HA Standby process adds port 5432 to the existing security group of the active Conductor (or creates it if it doesn't have one), and then sets Conductor HA settings to both active and

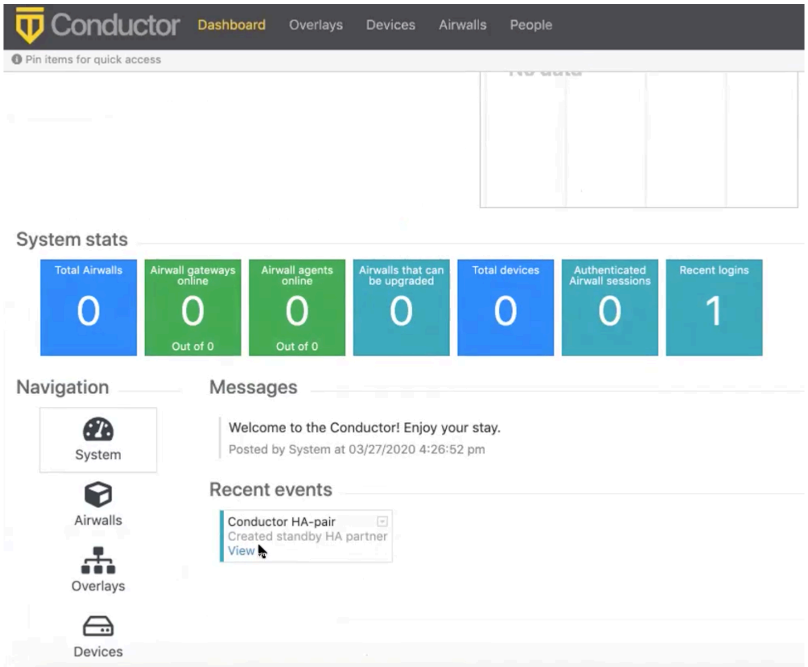
standby Conductors with the information from your current active Conductor. Depending on your cloud provider, this process can take up to 10 minutes.



Processing request, please wait...

```
2:25:53 pm — CREATE_IN_PROGRESS AWS::CloudFormation::Stack test-sb-sung
2:25:56 pm — CREATE_IN_PROGRESS AWS::EC2::SecurityGroup instancesg
2:26:01 pm ✓ CREATE_COMPLETE AWS::EC2::SecurityGroup instancesg
2:26:03 pm — CREATE_IN_PROGRESS AWS::EC2::Instance instance
2:26:36 pm ✓ CREATE_COMPLETE AWS::EC2::Instance instance
2:26:38 pm ✓ CREATE_COMPLETE AWS::CloudFormation::Stack test-sb-sung
2:26:39 pm — Starting Conductor HA configuration...
2:26:39 pm ✓ Stack = test-sb-sung has been deployed.
2:26:39 pm — Getting outputs from stack...
2:26:39 pm ✓ Successfully got stack outputs.
2:26:39 pm ✓ Successfully got required params: sb_conductor_instance_id = i-08cb1738e
2:26:39 pm — Provisioning standby Conductor with voucher = B/.9B172FA2A9EC18...
```

9. When it is done, select **Finish**.
10. As part of the provisioning process, you are logged out and will see a **Not connected to the Airwall Conductor** message. When this happens, log back into the active Conductor.
11. On the **Dashboard**, under **Recent Events**, you'll be able to see the HA Standby Conductor was created.



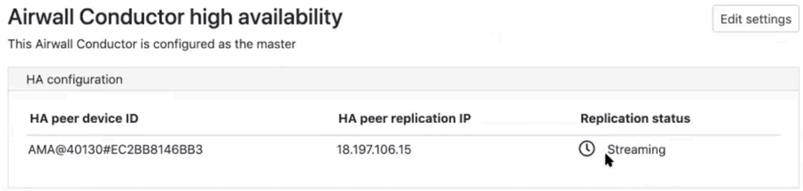
Welcome to the Conductor! Enjoy your stay.
Posted by System at 03/27/2020 4:26:52 pm

Conductor HA-pair
Created standby HA partner
View

Your standby HA Conductor is set up, provisioned, and configured.

Check the Status of your Standby Conductor

1. On your active Conductor, go to the **Settings** page.
2. Under **Airwall Conductor high availability**, you can see the status. It may say `Not streaming` until the cloud HA standby Conductor is fully set up on your cloud provider.



Airwall Conductor high availability

This Airwall Conductor is configured as the master

HA configuration

HA peer device ID	HA peer replication IP	Replication status
AMA@40130#EC2BB8146BB3	18.197.106.15	Streaming

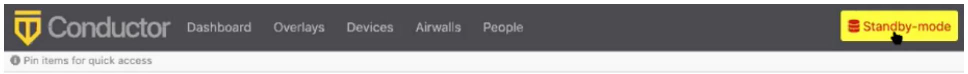
Once it says `Streaming`, your standby Conductor is ready and acting as a standby HA Conductor. You can also check on your cloud provider to see the new standby Conductor instance.

Log in to your Standby Conductor

Once your standby Conductor shows as `Streaming` on your active Conductor's **Settings** page, you can log in to the standby Conductor.

1. In your active Conductor, go to **Settings** and scroll down to **Airwall Conductor high availability**.
2. Copy the **HA peer replication IP** and enter it into a web browser.
3. Log in with the same user name and password as your active Conductor.

You won't need to configure anything. Everything is set up, provisioned, and configured as a standby HA Conductor. The standby Conductor shows **Standby-mode** in the title bar while acting as a standby.



Set up Conductor high availability

To configure Conductor High Availability (HA), you must first complete the initial setup for both Conductors.

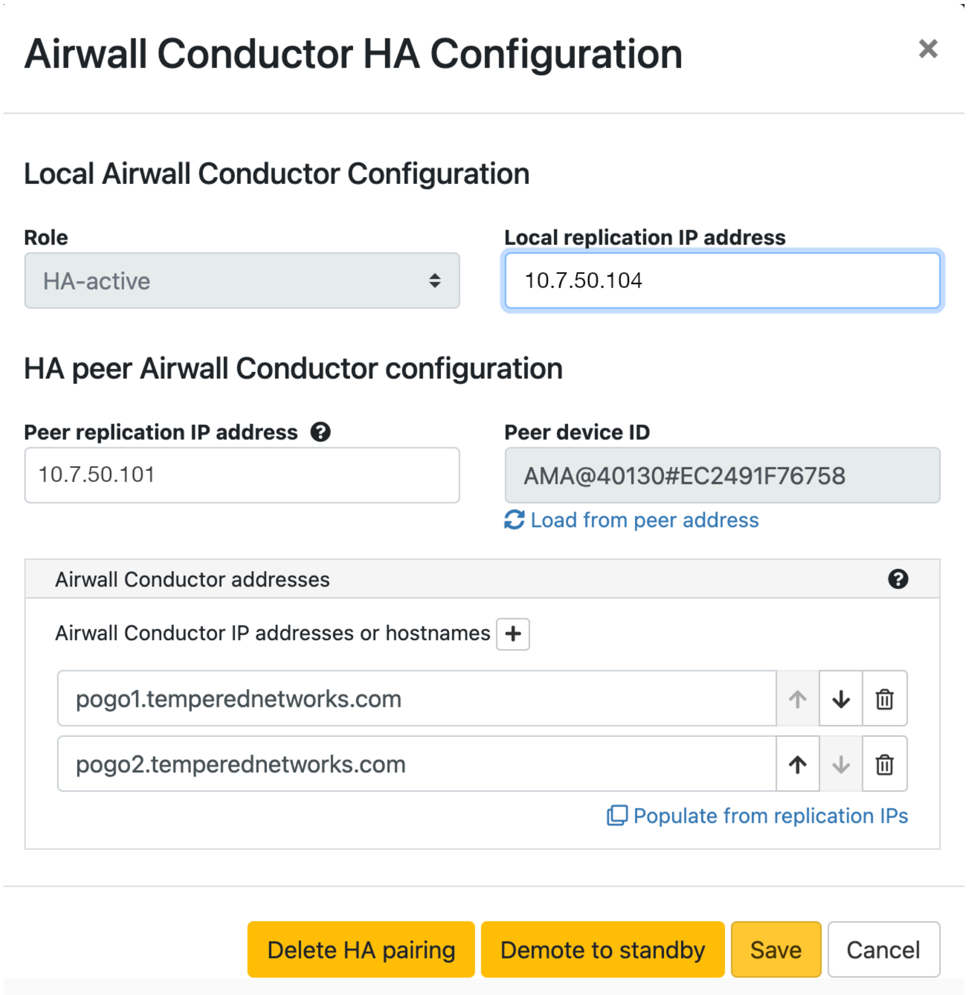
Configure the active Conductor

After you have completed initial setup on both Conductors, configure the active Conductor.

1. Log in to the Conductor you want to designate as the active.
2. In **Settings**, go to **Services** > **Conductor high availability**, and then select **Edit Settings**.

   Note: If you do not see it as a choice, select **Add service** and select **Conductor high availability**.
3. Select `HA-active` in the **Role** drop-down menu and fill in the fields as follows:
   - **Local replication IP address** - Enter the IP address of the network adapter on the master Conductor to use to replicate the data to the standby Conductor.
   - **Peer replication IP address** - Enter the IP address of the network adapter on the standby Conductor to use to stream the replication data with the master Conductor.
     - **Peer Device ID** - To automatically fill this field, select **Load from peer address**.

       In v2.2.13 and earlier – Enter the Device ID of the standby Conductor. To locate this ID, log in to the standby Conductor, go to the **Settings** tab, under **Configuration**, copy the **Conductor Device ID**, and paste it into this field on the master Conductor.
   - **Airwall Conductor addresses** – Enter the active and standby Conductor IPs or hostnames, or select **Populate from replication IPs**.



Airwall Conductor HA Configuration

Local Airwall Conductor Configuration

Role: HA-active

Local replication IP address: 10.7.50.104

HA peer Airwall Conductor configuration

Peer replication IP address: 10.7.50.101

Peer device ID: AMA@40130#EC2491F76758

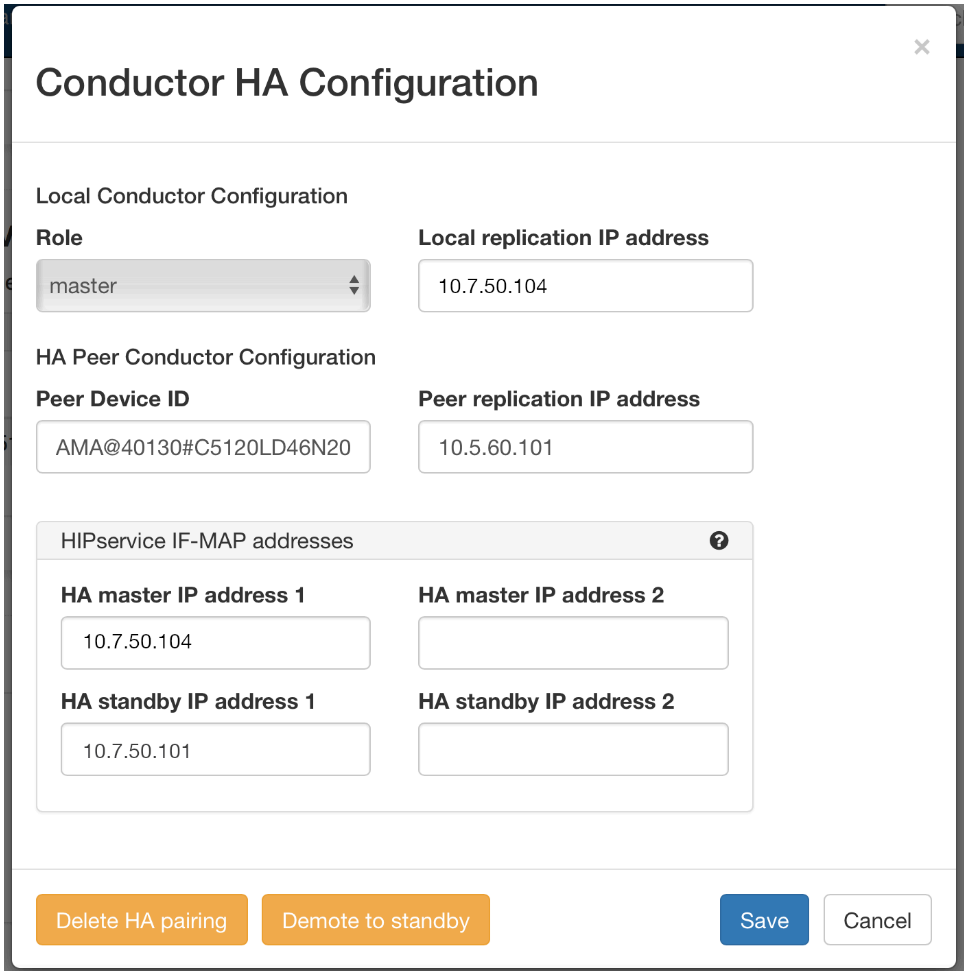
Airwall Conductor addresses

Airwall Conductor IP addresses or hostnames

pogo1.temperednetworks.com

pogo2.temperednetworks.com

- **For v2.2.13 and earlier:**
  - **HA master IP address 1** - Enter the IP address of the active Conductor network interface that Airwall Gateways use to connect to the active Conductor.
  - **HA master IP address 2** (Optional) - If the active Conductor is configured with two network interfaces enabled, enter the IP address of the second network interface of the active Conductor that Airwall Edge Services use to connect to active.
  - **HA standby IP address 1** - Enter the IP address of the standby Conductor network interface that Airwall Gateways should connect to if the active Conductor is unavailable.
  - **HA standby IP address 2** (Optional) - If the standby Conductor is configured with two network interfaces enabled, enter the IP address of the second network interface of the standby Conductor that Airwall Edge Services should connect to if the active Conductor is unavailable.



Conductor HA Configuration

Local Conductor Configuration

Role: master

Local replication IP address: 10.7.50.104

HA Peer Conductor Configuration

Peer Device ID: AMA@40130#C5120LD46N20

Peer replication IP address: 10.5.60.101

HIPservice IF-MAP addresses

HA master IP address 1: 10.7.50.104

HA master IP address 2:

HA standby IP address 1: 10.7.50.101

HA standby IP address 2:

4. Once configured, select **Save**. It may take several seconds to save the active configuration.

Configure the standby Conductor

Note: The standby Conductor inherits the configuration data of the active during the replication process, which erases any existing data on the standby during initial configuration.

Note: For HA pairing, you must have an open TCP port 5432 for Conductor HA communications. For a cloud Conductor, you need to open TCP port 5432 in the cloud provider security group. For a physical Conductor, you must open TCP port 5432 on your firewall.

Once an active Conductor is in place, you are ready to configure the standby.

1. Log in to the Conductor you will use as standby.
2. In **Settings** under **Conductor High Availability**, click **Edit Settings**.
3. Select `HA-standby` in the **Role** drop-down menu and fill in the fields described above for the active Conductor.

After you enter these configuration settings, the standby Conductor connects to the active and initializes data replication. The replication can take a significant amount of time, depending on the number of Airwall Edge Services in the active Conductor database and the network bandwidth available.

Note: After the setup is complete, you may have to re-authenticate.

Once the standby Conductor reboots, it returns you the **Settings** page where it now shows as running in standby mode.

Note: In **Settings** for both the active and standby Conductor, the **Conductor High Availability** section now displays a line indicating if the Conductor is active or standby, and the **Replication Status** displays `Streaming`.

High availability failover for the Conductor

If the master Conductor becomes unavailable, you can switch to the standby Conductor via a manual failover. Failover is performed on the standby Conductor, promoting it to become a master Conductor.

To initiate a failover:

1. Log in to the standby Conductor and go to **Settings**.
2. In the **Conductor High Availability** selection, click **Edit Settings**.
3. In **Conductor HA Configuration**, click **Promote to master** to promote the standby Conductor to the master.

It will take several seconds until the configuration is saved. Once complete, you are redirected to the **Settings** page. Standby mode no longer appears in the top menu and the Conductor's role changes to master in the **Conductor High Availability** section.

Airwall Gateways automatically reconnect to the new master Conductor over time as their connections to the failed Conductor time out. This process may take several minutes and does not affect the operations of the overlay networks.

High availability failback for the Conductor

After a failover has occurred, once the original Conductor becomes available again, or once a replacement is in place, you need to perform a failback to re-establish the high availability pairing.

If a replacement Conductor is required, follow the steps in Set up Conductor high availability to set up the replacement unit as the new standby Conductor.

Note: If the new Conductor will use different IP addresses than what the failed unit used, you need to re-configure the current active Conductor before proceeding with the failback.

If the original active Conductor can be brought back online without replacing, it can be easily switched to become the new standby. To do this,

1. Log in to the active Conductor,
2. In **Settings**, under **Conductor High Availability**, click **Edit Settings**.
3. In **Conductor HA Configuration**, click **Demote to standby** to transition the Conductor to become the standby.

This Conductor now connects to the active Conductor and initializes the data replication. The replication may take several minutes, depending on the number of Airwall Edge Services in the active Conductor database and the network bandwidth available.

Once you complete the setup, the standby Conductor reboots and you are directed to the Settings page.

Note: You may have to re-authenticate on the new standby Conductor once the setup is complete. If the configuration was successful, the Conductor displays standby-mode in the top menu bar.

Breaking a Conductor high availability pair

To break a Conductor HA pair. you first delete the HA configuration on the standby Conductor and then remove the HA configuration on the active Conductor.

To do this, go to **Settings** on the standby Conductor, and in the **Conductor High Availability** section, click **Edit Settings**. In **Conductor HA Configuration**, click **Delete HA pairing** to remove the HA configuration from the Conductor. The Conductors continue to operate, but failover between the two Conductors is no longer enabled.

Update HA-paired Conductors

Note: Conductor High Availability requires port TCP 443 to be open to validate its peer Conductor's version and to send firmware upgrades to the standby.

1. Upload the new Conductor firmware update package to the active Conductor.

   Note: The active Conductor sends the firmware update package to the standby Conductor.

2. Update the standby Conductor and wait for the update process to complete.

The standby Conductor is automatically promoted to the active role after the update.

3. Update the active Conductor and wait for the update process to complete.
4. Once both Conductors are updated, demote the designated standby Conductor back to the standby role from **Settings** > **High Availability**.

Configure Conductor Remote Logging

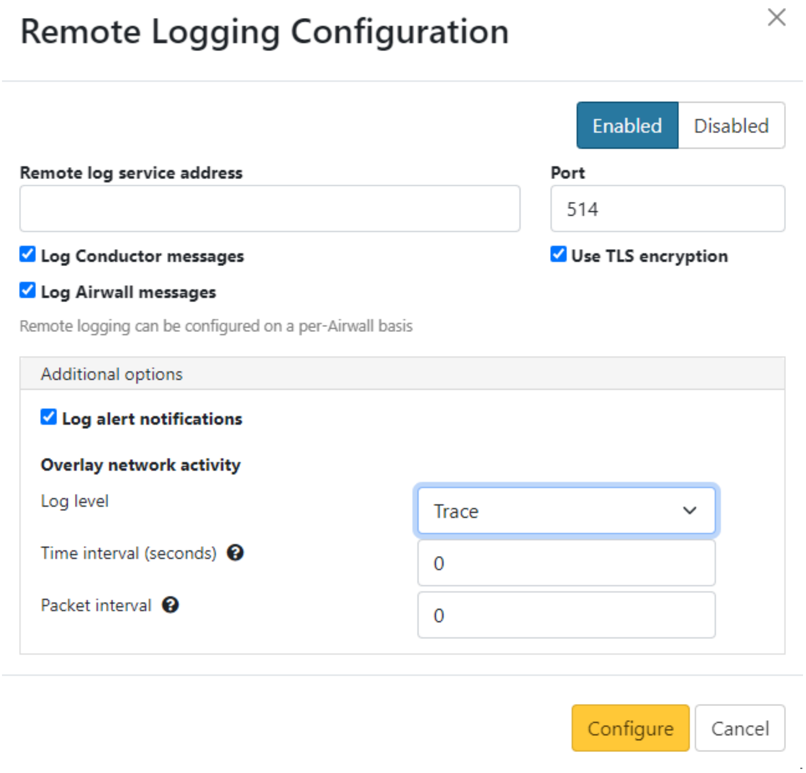
You can configure the Conductor to send system log messages to a centralized logging service. Your environment must have a syslog service available on the underlay.

Supported Roles	System Administrator

Note: You may need to coordinate with your underlay network administrator to determine the proper syslog service configuration for your environment.

1. Go to **Settings** > **Services** > **Remote logging** and select **Edit Settings**.

   If you do not see it as a choice, select **Add service** and select **Remote logging**.
2. Select **Enabled** or **Disabled** to turn remote logging on or off.
3. Set the address and port for your remote logging service:



Remote Logging Configuration

Enabled | Disabled

Remote log service address:

Port: 514

☑ Log Conductor messages

☑ Use TLS encryption

☑ Log Airwall messages

Remote logging can be configured on a per-Airwall basis

Additional options

☑ Log alert notifications

Overlay network activity

Log level: Trace

Time interval (seconds): 0

Packet interval: 0

4. Check whether to use TLS encryption (recommended unless your remote log service is on the same local network as the Conductor). If this box is clear, messages are sent over UDP, which is unencrypted and could introduce a security risk if you are sending the logs over unsecured networks.
5. Check whether to log Conductor and/or Airwall messages, or alerts.
6. Choose the Overlay network activity log level, time interval, and packet interval:

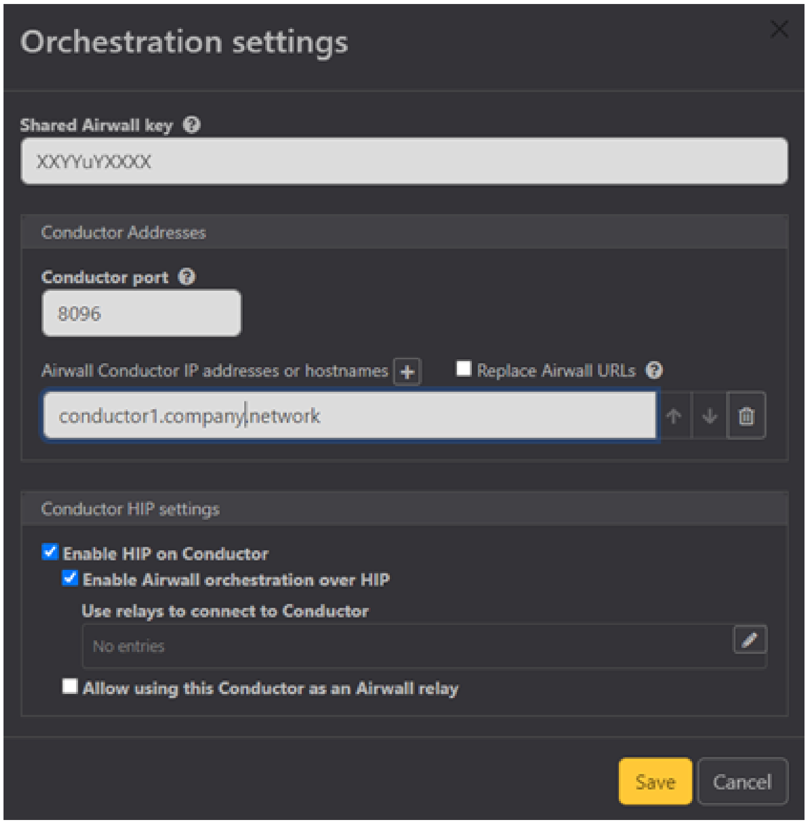
   - Log level: logs overlay network activity that equals or exceeds the log level of the Airwall. Options: Trace, Debug, Info, Warn, Error.
   - Time interval: number of seconds before logging additional device activity for a flow. 0 to disable.
   - Packet interval: number of packets before logging additional device activity for a flow. 0 to disable.
7. Select **Configure**.

Once the logging service is configured and enabled, the Conductor begins to duplicate system log messages and sends them to the configured logging service. Airwall Gateways also obtain the logging service configuration from the Conductor, and will start sending its messages to the logging service if you've configured it to log Airwall Edge Service messages.

Enable HIP on Conductor

To enable HIP on Conductor, complete the following steps:

1. Go to **Settings** > **Orchestration settings** > **Edit Settings**.



Orchestration settings

Shared Airwall key: XXYYuYXXXX

Conductor Addresses

Conductor port: 8096

Airwall Conductor IP addresses or hostnames: conductor1.company.network

□ Replace Airwall URLs

Conductor HIP settings

☑ Enable HIP on Conductor

☑ Enable Airwall orchestration over HIP

Use relays to connect to Conductor: No entries

□ Allow using this Conductor as an Airwall relay

2. Check **Enable HIP on Conductor**.
3. From the dropdown menu that appears, check **Enable Airwall orchestration over HIP** and choose a relay to connect to the Conductor.
4. Ensure that **Allow using this Conductor as an Airwall Relay** is unchecked. You cannot select a relay to use to connect to a Conductor and have the Conductor function as a relay at the same time.
5. Click **Save**.

Deploy and Configure Airwall Edge Services

Airwall Edge Services let you securely connect managed endpoints, such as laptops, PCs, tablets, and smartphones.

Set up Airwall Gateways

Set up physical, virtual, or cloud Airwall Gateways.

Configure an Airwall Gateway with the `airsh` Setup Wizard

Configure the most common Airwall Gateway setup options using the `airsh` Setup Wizard.

Supported Versions	2.2.10 and later Airwall Gateways
Supported on these Airwall Edge Services	All Airwall Gateways

Before you begin

Collect the following information to set up your Airwall Gateway:

- **Underlay network information** – The protocol (DHCP or static) and type (IPv4 or IPv6) of your underlay network, both wired and Wifi, if enabled. If you are using cell, also your APN (for both modems if you have 2).
- **Conductor address** – The IP address or hostname and port for the Airwall Conductor you want this Airwall Gateway to connect to.
- **Wifi information (if enabled)** – The authentication type, and SSID (network name) and key for your wireless network.
- **Cellular information (if included)** – Your active carrier, preferred access type (3G or 4G), pin code, authentication type (None, PAP, CHAP, PAP/CHAP), username and password (if applicable), IP connection type (default, IPv4, IPv6, IPv4/IPv6) and whether you want to enable or disable roaming.

Set up an Airwall Gateway with the `airsh` Setup Wizard

1. Connect a computer or Configure an Airwall Gateway with the airsh Setup Wizard on page 274 to access it remotely.
2. Log in to `airsh`. For information on how, see Airshell (airsh) Command Reference on page 362.
3. At the `airsh` prompt, enter:

   ```
   setup-ui
   ```

4. Fill in the information to set up your Airwall Gateway.
5. When you're finished, the status page shows the options you've selected and whether you are connected to your Wifi or cellular network. You may want to note your underlay IPs.

You can reboot to start using the Airwall Gateway, or go into Diagnostic mode to configure more options.

To troubleshoot connection issues, see Troubleshoot Initial Airwall Gateway connections on page 491.

Outside Antenna Guidance

Suggestions on outdoor/external cellular antennas to use with Airwall Gateways.

Outdoor/External Cellular Antenna Reference Guide	Download PDF

Set up physical Airwall Gateways

Before you begin installing your Airwall Gateway, ensure that you already have the Conductor installed and configured. After you are finished installing your Airwall Gateway, you can begin connecting devices.

A Tempered Airwall Gateway allows your organization to create an identity-based, secure and private global connected network. It creates a zero-trust Software Defined Perimeter (SDP), using the Airwall Gateway to establish the perimeter of your logical airgap. This perimeter can be deep in your network, closer to the data source, providing security for your IoT/ IIoT devices. It provides security for devices that can't protect themselves.

❗ **Important:** You should familiarize yourself with your model's front panel layout, specifications, power requirements, and safety warnings before use. Also, you should review the procedure for connecting your Airwall Gateway to your Conductor. This information can be found in your model's Platform Guide, included with your Airwall Gateway. If you are unable to locate your Platform Guide, you can download a PDF from the Documentation Downloads on page 810**Documentation Downloads** section of the **Documentation Center**.

To install and connect Airwall Gateways

To install Airwall Gateways and connect them to the Conductor, you must first apply power to the Airwall Gateway hardware. Once booted, you can configure an Airwall Gateway to connect to the Conductor in one of these ways:

- If your Airwall Gateway has a console port, connect a computer to the console port of the Airwall Gateway, and use airsh to configure the Conductor IP address or URL. See Connect to a physical Airwall Gateway or Conductor with a console port on page 293.

- Put the Airwall Gateway into diagnostic mode and manually configure the Conductor IP address or URL. See Connect an Airwall Gateway with Diag mode on page 292.
- Configure a DNS SRV record. This might require assistance from your network administrator. See Connect an Airwall Gateway with a DNS SRV record on page 294.
- Use a factory-configured Conductor URL. This requires assistance from Tempered. See Connect an Airwall Gateway by using a factory-configured URL on page 294

Airwall Gateway Hardware Installation Guide

This is a generic installation guide for all Airwall Gateway hardware appliances series: 75, 110, 150, 250, and 500. For more specific installation instructions, specifications, and panel layouts for your specific model, download the platform guide from Documentation Downloads on page 810.

Note: For Airwall Gateway Advantech models, see Airwall Gateway AV3200g Hardware Installation Guide on page 281 and Airwall Gateway AV3033 Hardware Installation Guide on page 284.

Follow this guide to set up basic network connectivity for an Airwall Gateway, and provision the gateway on the Airwall Conductor. The Conductor is the central configuration and management point for your Airwall secure network, and manages trust between devices and Airwall Gateways on your network. These instructions are based on Airwall Gateways and Conductor v2.2.8 and later.

Prerequisites

To bring the Airwall Gateway online, you need:

- the Conductor IP address or URL that the Airwall Gateway connects to
- network cables to connect the Airwall Gateway to your network, or a valid SIM card if you are only connecting via a cellular network
- a micro-USB cable to connect a computer to the Airwall Gateway

  Note: If your Airwall Gateway model does not have a micro-USB console port, use a network cable to connect to your computer's ethernet port. If your computer does not have ethernet port, use a RJ45-to-USB cable.

Unbox the Airwall Gateway

Unbox the Airwall Gateway and become familiar with the parts.

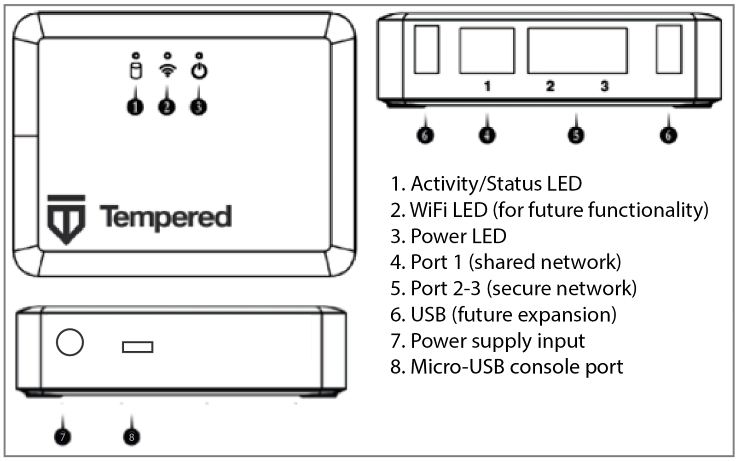
1. Open the box and carefully remove the Airwall Gateway.

   This picture shows an Airwall Gateway 75.

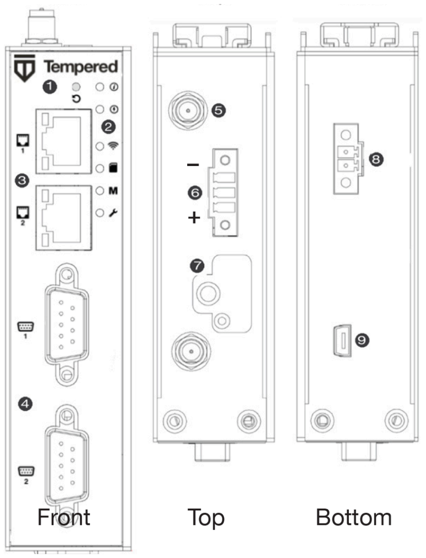
2. **Check out the platform guide/quick start guide that came with your Airwall Gateway to get familiar with the top and front panel of the Airwall Gateway.**

   Here are the panel layouts for the most common Airwall Gateways:

   - **75** –

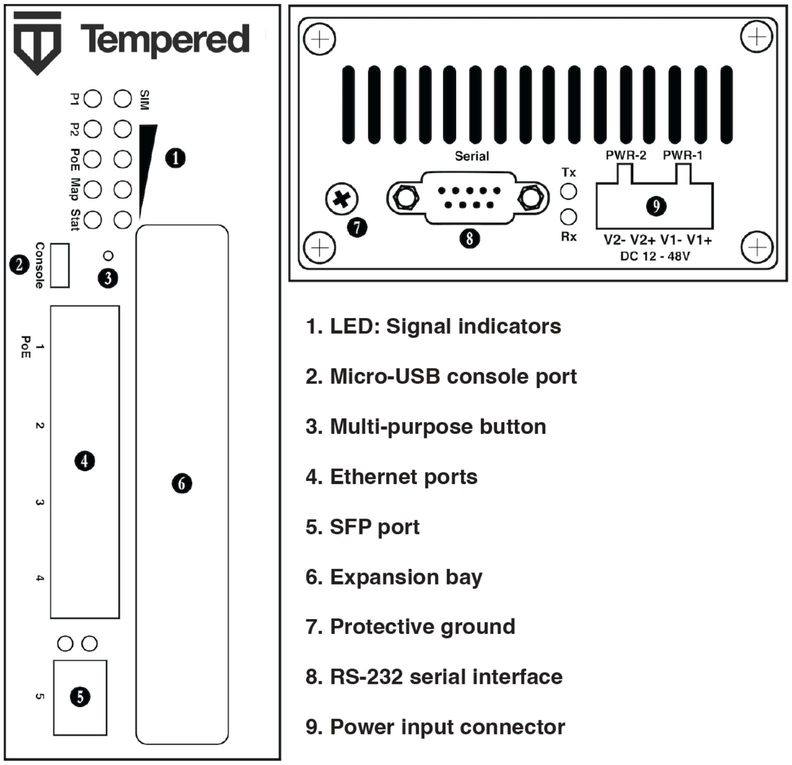

Tempered
1
2
3
1. Activity/Status LED
2. WiFi LED (for future functionality)
3. Power LED
4. Port 1 (shared network)
5. Port 2-3 (secure network)
6. USB (future expansion)
7. Power supply input
8. Micro-USB console port

   - **110** –



1. Multi-purpose button
2. LED - Signal indicators:
   - Status
   - Power
   - Cellular connection status
   - SIM card
   - MAP connection (Conductor)
   - Diagnostic mode
3. Ethernet ports
4. Serial ports
5. Antenna connectors
6. Power input connector
7. SIM card slot
8. Relay
9. Micro-USB console port

- **150** –



1. LED: Signal indicators

2. Micro-USB console port

3. Multi-purpose button

4. Ethernet ports

5. SFP port

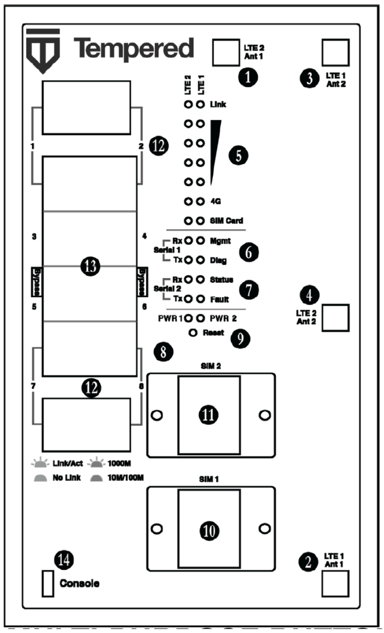
6. Expansion bay

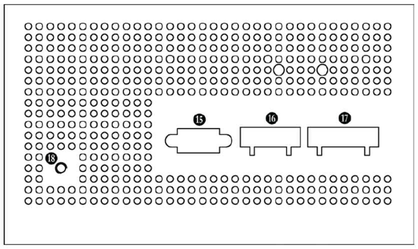
7. Protective ground

8. RS-232 serial interface

9. Power input connector

- **250** –

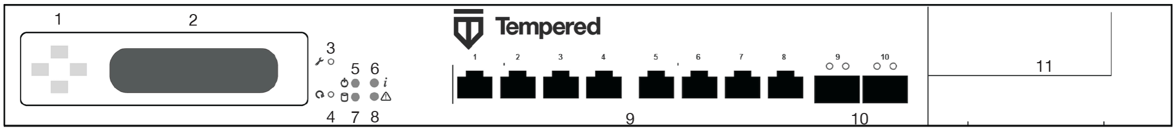




1. LTE 2, primary antenna connector (250g/250gd)
2. LTE 1, primary antenna connector (250g/250gd)
3. LTE 1, second antenna connector (250g/250gd)
4. LTE 2, second antenna connector (250g/250gd)
5. LED: Signal indicators, LTE modems 1 & 2
6. LED: Serial port 1 activity indicator
7. LED: Serial port 2 activity indicator
8. LED: Power input 1 & 2 indicators
9. Multi-purpose button
10. LTE modem 1 microSIM card slot (250g/250gd)
11. LTE modem 2 microSIM card slot (250g/250gd)
12. Ethernet, Combo RJ-45/SFP ports
13. Ethernet ports
14. Micro-USB console port
15. Serial interface, port 1
16. Serial interface, port 2
17. Power input connector
18. Ground (earthed)

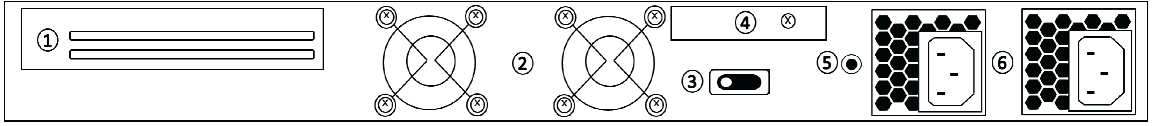
- **500** –

Front Panel Layout



1	Buttons for LCD display navigation	5	Power LED	9	8x RJ45 Ethernet ports
2	LCD display panel	6	Activity indicator LED	10	2x SFP ports
3	Diagnostic/Reset button	7	Status LED	11	1x Expansion bay
4	(non-functional)	8	Alert LED		(functional for the Airwall-500 only)

Back Panel Layout



1	Future expansion slots	3	Power switch	5	Silence Alarm button
2	Case exhaust fans	4	Case cover removal tab	6	Dual power supply (both required)

3. Check the specifications on the labels and platform guide included in the box to determine environments to which you can physically deploy the Airwall Gateway. Download the panel layouts and basic specifications for your Airwall Gateway from Documentation Downloads on page 810.

Connect the Airwall Gateway to the network and the Conductor

Connect the Airwall Gateway to your network.

You can connect and configure the Airwall Gateway in one of three ways:

- **Console Port connect** – Best option for Airwall Gateway series with a console port.
- **Diagnostic mode connect** – Best option for Airwall Gateway series without a console port.
- **Use a DHCP server** – Advanced option for adding a large number of Airwall Gateways, see Connecting Airwall Gateways using a DHCP server on page 287.

Note: Some Airwall Gateways have a micro-USB console port, others have a RJ45 console port, while some models have no defined console port. If your model has no console port, use Diagnostic mode to connect.

Console port connect

For provisioning, place the Airwall Gateway where it can reach the Conductor on your shared network. The fastest way to provision the Airwall Gateway is to connect a computer to the Airwall Gateway using the console port.

1. Locate the Airwall Gateway in an area that complies with the safe operating guidelines, and then plug it in with the supplied power cord.
2. Connect the Airwall Gateway to a network that has access to the Conductor (your company network or the Internet) using Port 1.
3. Connect your computer to the micro-USB console port on the Airwall Gateway.
4. Use a terminal (macOS or Linux) or terminal emulator such as PuTTY (Windows), to connect to the Airwall Gateway using baud rate 115200.
5. At the login prompt, log in using Airshell with name `airsh` and no password.

   Note: For more on Airshell command line options, see Airshell Command Line on page 360.

6. Check that the Airwall Gateway can reach the Conductor URL:

   ```
   ping <Conductor URL>
   ```

   For example:

   ```
   ping my-conductor.tempered.com
   ```

   When the ping is successful, continue.
7. Set the Conductor IP address or URL, and optionally, the port. For example, enter:

   ```
   conductor set my-conductor.tempered.com
   ```

   The Airwall Gateway is now recognized in the Conductor, showing up in the Provisioning tab, the Licensing tab, or on the Airwalls page as ready to manage. When the Airwall Gateway is connected to the Conductor, you can manage and configure it from there.
8. Connect the devices you want to protect to the Airwall Gateway on Port 2. See the platform guide that came with your Airwall Gateway for port locations.

Diagnostic mode connect

For provisioning, place theAirwall Gateways where it has network access to the Conductor through your company network or the Internet.

1. Locate the Airwall Gateway in an area that complies with the safe operating guidelines, and then plug it in with the supplied power cord.
2. Connect the Airwall Gateway to a network that has reachability to the Conductor (your company network or the Internet) using Port 1.
3. Connect your computer to Airwall Gateway's Port 2 with an ethernet cable.
4. For Airwall Gateway series:

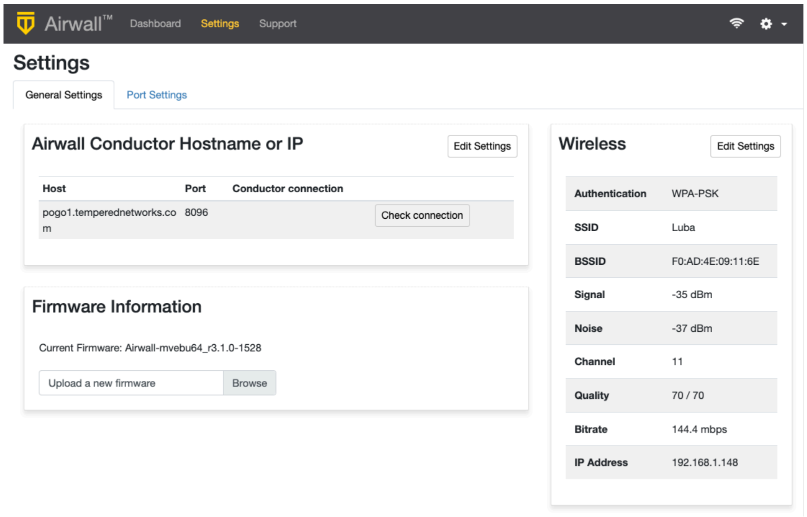
   - with a multi-purpose or reset button, press the button for 3 seconds to enter diagnostic mode. After three seconds, the status LED blinks to indicate the Airwall Gateway is in diagnostic mode.
   - without a multi-purpose or reset button, place into diagnostic mode by connecting a VGA monitor and a USB keyboard to port 2 of the Airwall Gateway, and entering the login prompt:

     - 2.2.3 and later: Enter `airsh` to enter the console, and then enter `diag`.

       Note: If you are asked for a password, enter default airsh, or the password you set.

     - Earlier than 2.2.3: Enter `diag`, then enter password `diag`.

   Once the Airwall Gateway is in diagnostic mode, Overlay network communications from the Airwall Gateway are disabled and the device network is reconfigured with a static IP address.
5. Open a web browser and go to `http://192.168.56.3` to access the Airwall Gateway diagnostic page.



Settings

Airwall Conductor Hostname or IP

Host	Port	Conductor connection
pogo1.temperednetworks.com	8096	

Firmware Information

Current Firmware: Airwall-mvebu64_r3.1.0-1528

Wireless

Authentication	WPA-PSK
SSID	Luba
BSSID	F0:AD:4E:09:11:6E
Signal	-35 dBm
Noise	-37 dBm
Channel	11
Quality	70 / 70
Bitrate	144.4 mbps
IP Address	192.168.1.148

6. Select Edit Settings and enter the Conductor URL. Select Update Settings.
7. Click Reboot to take the Airwall out of diagnostic mode.

   Important: After restarting, the Airwall Gateway may require up to three minutes to return to operating mode.

   The Airwall Gateway is now recognized in the Conductor, showing up in the Provisioning tab, the Licensing tab, or on the Airwalls page as ready to manage. When the Airwall Gateway is connected to the Conductor, you can manage and configure it from there.
8. Connect the devices you want to protect to the Airwall Gateway on port 2 and above.

License and Manage the Airwall Gateway in the Conductor

You need to Add Airwall Edge Service Licenses to the Conductor before you can provision and license Airwall Gateways. Airwall Edge Services include Airwall Gateways as well as Airwall Agents and Servers that allow people to connect their devices to your Airwall secure network.

To complete this step, a Conductor administrator must license and manage the Airwall Gateways. For instructions, see Provision and License Airwall Edge Services on page 193.

Once complete, Conductor administrators can configure the Airwall Gateways in the Conductor.

More Information

Status LED Blink Codes on page 480
Physical Airwall Gateways equipped with a Status LED use blink codes to indicate their status.

Airshell Common Commands on page 360
For Airwall Gateways that have a console port, you can deploy and configure the Airwall Gateway with the **Airshell** (airsh) command-line interface. You can deploy & configure an Airwall Gateway directly without going into diagnostic mode.

Terms and Definitions on page 812
Glossary of Airwall components.

Airwall Gateway AV3200g Hardware Installation Guide

This is an installation guide for the Airwall Gateway AV3200g hardware. The Airwall Gateway AV3200g is an Advantech ICR-3241 model router with pre-installed Airwall firmware.

Note: The Airwall Gateway AV3200g is a similar platform to the Airwall Gateway 110g.

Follow this guide to set up basic network connectivity for an Airwall Gateway AV3200g, and provision the gateway on the Airwall Conductor. The Conductor is the central configuration and management point for your Airwall secure network, and manages trust between devices and Airwall Gateways on your network. These instructions are based on Airwall Gateways and Conductor v2.2.8 and later.

Prerequisite

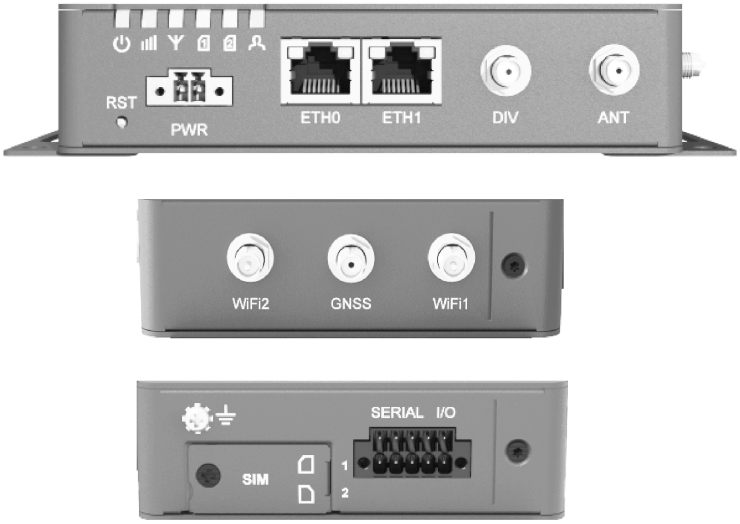
To bring the Airwall Gateway online, you need:

- the Conductor IP address or URL that the Airwall Gateway connects to
- a network cable to connect the Airwall Gateway to your network or a valid SIM card if you are only connecting via a cellular network
- a network cable to connect your computer to the Airwall Gateway

Unbox the Airwall Gateway AV3200g

The first step is to unbox the Airwall Gateway AV3200g and become familiar with the parts.

Open the box and carefully remove the Airwall Gateway.



RST	• 6 seconds: put the Airwall in Diagnostic mode • 8 seconds: restore the default factory configuration
PWR	Terminal block for the power supply
ETH0	Port 1: ethernet connection to the network
ETH1	Port 2: • During set up: connection for your laptop • After set up: connection for the device or devices you want to protect
SIM	Sim card for optional cellular connectivity. **Note:** Unscrew the cover to access SIM1. SIM2 is not supported.

Connect the Airwall Gateway AV3200g to the network and the Conductor

Complete the following steps to connect an Airwall Gateway AV3200g to your network.

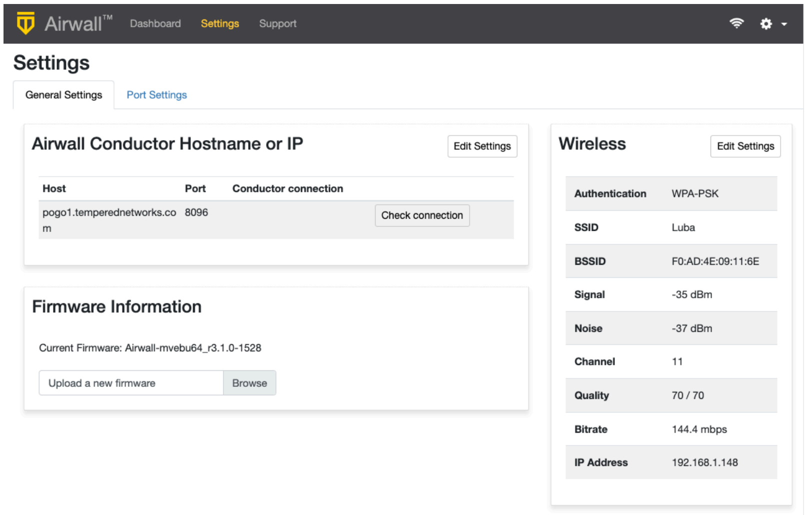
For provisioning, place the Airwall Gateway where it can reach the Conductor on your shared network.

Note: The Airwall assigns an IP address on the 192.168.56.0/24 network, so your computer connected to ETH1 must be set up for DHCP.

1. Locate the Airwall Gateway in an area that complies with the safe operating guidelines, and then plug it in with the supplied power cord.

2. Connect the Airwall Gateway to a network that has network access to the Conductor (your company network or the Internet) using the ETH0 port.
3. Connect a computer to the Airwall Gateway's ETH1 port and press the RST button for 6 seconds. After 6 seconds all the LED lights blink off. Release the button immediately. The status LED blinks to indicate the Airwall Gateway is in diagnostic mode.

   Important: Do not continue pressing the Multi-Purpose or Reset button after 7 seconds as this will reset the Airwall Gateway to factory settings.
4. When you see that you have an IP address on the 192.168.56.0/24 network subnet, verify that you can reach the Airwall by pinging 192.168.56.3 from your computer.
5. Open a web browser on your computer and go to http://192.168.56.3 to access the Airwall Gateway diagnostic page.



Settings

Airwall Conductor Hostname or IP

Host	Port	Conductor connection
pogo1.temperednetworks.com	8096	

Firmware Information

Current Firmware: Airwall-mvebu64_r3.1.0-1528

Wireless

Authentication	WPA-PSK
SSID	Luba
BSSID	F0:AD:4E:09:11:6E
Signal	-35 dBm
Noise	-37 dBm
Channel	11
Quality	70 / 70
Bitrate	144.4 mbps
IP Address	192.168.1.148

6. To edit the Conductor, select **Edit Settings**. Make your selections and select **Update Settings**.
7. In the upper right corner click **Reboot** to take the airwall out of diagnostic mode.

   Note: After restarting, the Airwall Gateway may require up to 3 minutes to return to operating mode.

   The Airwall Gateway should now be recognized in the Conductor, showing up on the Provisioning tab, the **Licensing** tab, or on the **Airwalls** page as ready to manage. Once the Airwall Gateway is connected to the Conductor, you can manage and configure it there.
8. Remove the cable from your computer and connect the devices you want to protect to the Airwall Gateway on the ETH1 port.

License and Manage the Airwall Gateway in the Conductor

You need to Add Airwall Edge Service Licenses to the Conductor before you can provision and license Airwall Gateways. Airwall Edge Services include Airwall Gateways as well as Airwall Agents and Servers that allow people to connect their devices to your Airwall secure network.

To complete this step, a Conductor administrator must license and manage the Airwall Gateways. For instructions, see Provision and License Airwall Edge Services on page 193.

Once complete, Conductor administrators can configure the Airwall Gateways in the Conductor.

More Information

Status LED Blink Codes on page 480
Physical Airwall Gateways equipped with a Status LED use blink codes to indicate their status.

Airshell Common Commands on page 360

For Airwall Gateways that have a console port, you can deploy and configure the Airwall Gateway with the **Airshell** (airsh) command-line interface. You can deploy & configure an Airwall Gateway directly without going into diagnostic mode.

Terms and Definitions on page 812
Glossary of Airwall components.

Airwall Gateway AV3033 Hardware Installation Guide

This is the installation guide for the Airwall Gateway AV3033 hardware appliance. The Airwall Gateway AV3033 is an Advantech FWA3033 internet security platform with pre-installed Airwall firmware.

Note: The Airwall AV3033 is a similar platform to the Airwall Gateway 500.

Follow this guide to set up basic network connectivity for an Airwall Gateway, and provision the gateway on the Airwall Conductor. The Conductor is the central configuration and management point for your Airwall secure network, and manages trust between devices and Airwall Gateways on your network. These instructions are based on Airwall Gateways and Conductor v2.2.8 and later.

Prerequisite

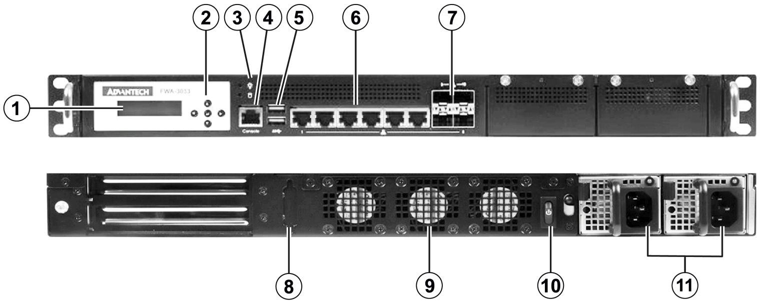
To bring the Airwall Gateway online, you need:

- the Conductor IP address or URL that the Airwall Gateway will connect to
- a network cable to connect the Airwall Gateway to your network
- a network cable to connect your computer to the Airwall Gateway

Unbox the Airwall Gateway AV3033

Unbox the Airwall Gateway AV3033 and become familiar with the parts.

Open the box and carefully remove the Airwall Gateway.



1	LCD screen
2	Keypad
3	Power LED
4	RJ45 console port
5	2 USB ports
6	6 RJ45 ethernet ports
7	4 SFP ports
8	DVI port
9	Fans
10	Power button
11	Dual power supply

Connecting the Airwall Gateway AV3033 to the network and the Conductor

Complete the following steps to connect an Airwall Gateway AV3033 to your network to your Conductor. You can connect through the console port (command line) or through diagnostic mode (UI).

Console port connect

Complete the following steps to connect an Airwall Gateway AV3033 to your network to your Conductor using the console port.

For provisioning, place the Airwall Gateway where it can reach the Conductor on your shared network.

1. Locate the Airwall Gateway in an area that complies with the safe operating guidelines, and then plug it in with the supplied power cord.
2. Connect the Airwall Gateway to a network that has access to the Conductor (your company network or the Internet) using Port 1.
3. Connect a computer to the Airwall Gateway's console port.

   Note: If your computer does not have an RJ45 port, you can use an RJ45-to-USB cable.
4. Use a terminal (macOS or Linux) or terminal emulator (Windows), to connect to the Airwall Gateway using baud rate 115200.
5. At the login prompt, log in with: name: `airsh` and no password.
6. Check that the Airwall Gateway can reach the Conductor URL:

   ```
   ping <Conductor URL>
   ```

   For example:

   ```
   ping my-conductor.tempered.com
   ```

   Once the ping is successful, continue.
7. Set the Conductor IP address or URL and, optionally, the port. For example, enter:`conductor set my-conductor.tempered.com`

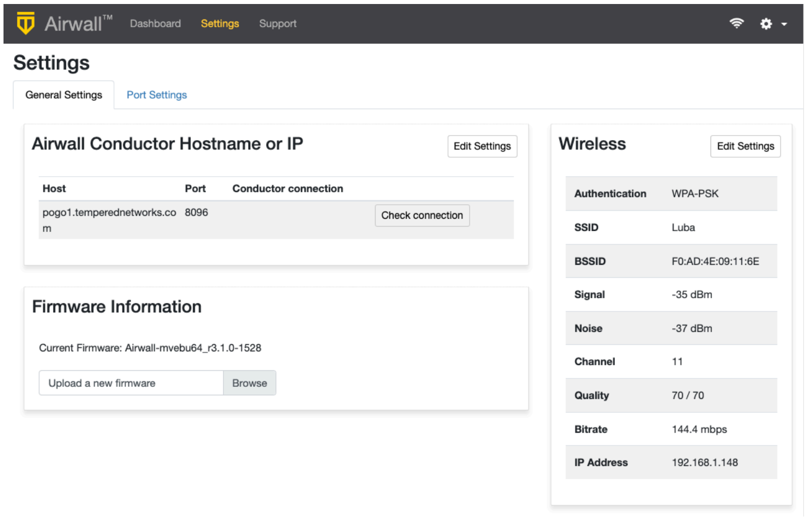
   The Airwall Gateway should now be recognized in the Conductor, showing up on the **Licensing** tab, or on the **Airwalls** page as ready to manage. Once the Airwall Gateway is connected to the Conductor, you can manage and configure it there. For more Airshell command line options, see Airshell Command Line.
8. Remove the cable from your computer and connect the devices you want to protect to the Airwall Gateway on the RJ45 or SFP ethernet ports.

Diagnostic mode connect

Complete the following steps to connect an Airwall Gateway AV3033 to your network to your Conductor using diagnostic mode.

Complete the following steps to connect an Airwall Gateway AV3033 to your network through diagnostic mode. Once in diagnostic mode, the Airwall issues an IP address from the 192.168.56.0/24 network to your computer connected to RJ45 Port 2. Your computer must be set up for DHCP.

1. Locate the Airwall Gateway in an area that complies with the safe operating guidelines, and then plug it in with the supplied power cord.
2. Connect the Airwall Gateway to a network that has access to the Conductor (your company network or the Internet) using RJ45 Port 1.
3. Connect your computer to the Airwall Gateway's console port with a serial interface. Then connect your computer to the Airwall Gateway's Port 2 with an ethernet cable.
4. Use the Airwall Gateway AV3033 LCD screen and buttons to enter diagnostic mode. The Airwall issues the IP address 192.168.56.3 to your computer to access diagnostic mode.
5. When you see that you have an IP address on the 192.168.56.0/24 network subnet, verify that you can reach the Airwall by pinging 192.168.56.3.
6. Open a web browser and go to http://192.168.56.3 to access the Airwall Gateway diagnostic page.



Settings

General Settings | Port Settings

Airwall Conductor Hostname or IP — Edit Settings

Host	Port	Conductor connection
pogo1.temperednetworks.com	8096	Check connection

Firmware Information

Current Firmware: Airwall-mvebu64_r3.1.0-1528

Upload a new firmware | Browse

Wireless — Edit Settings

Authentication	WPA-PSK
SSID	Luba
BSSID	F0:AD:4E:09:11:6E
Signal	-35 dBm
Noise	-37 dBm
Channel	11
Quality	70 / 70
Bitrate	144.4 mbps
IP Address	192.168.1.148

7. Click **Settings** > **Edit Settings** and enter the Conductor URL. Click **Save**.
8. In the upper right cornder click **Reboot**.

   Note: After restarting, the Airwall Gateway may require up to 3 minutes to return to operating mode.

   The Airwall Gateway should now be recognized in the Conductor, showing up on the **Licensing** tab, or on the **Airwalls** page as ready to manage. Once the Airwall Gateway is connected to the Conductor, you can manage and configure it there. For more Airshell command line options, see Airshell Command Line.
9. Remove the cable from your computer and connect the devices you want to protect to the Airwall Gateway on the RJ45 or SFP ethernet ports.

License and Manage the Airwall Gateway in the Conductor

You need to Add Airwall Edge Service Licenses to the Conductor before you can provision and license Airwall Gateways. Airwall Edge Services include Airwall Gateways as well as Airwall Agents and Servers that allow people to connect their devices to your Airwall secure network.

To complete this step, a Conductor administrator must license and manage the Airwall Gateways. For instructions, see Provision and License Airwall Edge Services on page 193.

Once complete, Conductor administrators can configure the Airwall Gateways in the Conductor.

More Information

Status LED Blink Codes on page 480
Physical Airwall Gateways equipped with a Status LED use blink codes to indicate their status.

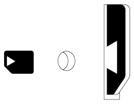
Airshell Common Commands on page 360
For Airwall Gateways that have a console port, you can deploy and configure the Airwall Gateway with the **Airshell** (airsh) command-line interface. You can deploy & configure an Airwall Gateway directly without going into diagnostic mode.

Terms and Definitions on page 812
Glossary of Airwall components.

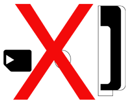
Insert the SIM card in a 110

Insert the SIM card with the angled corner up, as shown in the first picture.

Correct:



Incorrect:



Connecting Airwall Gateways using a DHCP server

Use the DHCP server advanced connection method when connecting a large number of Airwall Gateways at once.

For provisioning, place the Airwall Gateway on a network where it can reach the Conductor on your shared network, or on the Internet. Once you set up DHCP on your network, you can skip steps 2 and 3 when setting up any additional Airwall Gateway.

1. **Plug in the Airwall Gateway** – Locate the Airwall Gateway in an area that complies with the safe operating guidelines, and then plug it in or apply power.
2. **Check DHCP** – Ensure there is a DHCP server and a DNS resolver or DNS server for the local domain that is accessible on the shared network.
3. **Create a DNS SRV record** – On the DNS server, check that there is (or have a network administrator add) a SRV record pointing to the Conductor URL:

   ```
   _service._proto.name TTL class SRV priority weight port target
   ```

   For example, if your shared network domain is me.com and the Conductor hostname is cond-01, then the SRV record should be:

   ```
   _ifmap._tcp.example.com. 3600 IN SRV 10 0 8096 cond-01.me.com
   ```

   *Use the TTL, priority and weight for your DNS environment. Port 8096 is the default, but you can change it in the Conductor and set it to an alternate port.
4. **Connect to your network** – Connect the Airwall Gateway to a network shared with the Conductor using Port 1 (your company network or the Internet). The DHCP server assigns an IP address, netmask, and a default gateway to the Airwall Gateway. The Airwall Gateway then does an DNS lookup and configures itself using the Conductor address.
5. **Ping the Conductor URL** – Check that you can reach the Conductor by pinging it. Enter:

   ```
   ping my-conductor.tempered.com
   ```
6. **Connect to devices** – Connect the devices you want to protect to the Airwall Gateway on Port 2.

The Airwall Gateway should now be recognized in the Conductor, showing up on the **Provisioning** tab, the **Licensing** tab, or on the **Airwalls** page as ready to manage. Once the Airwall Gateway is connected to the Conductor, you can manage and configure it there (including serial ports).

Set up 75-series hardware

The Airwall Conductor is the central configuration and management point for all Airwall Edge Services. The fastest method to configure and connect your Airwall Gateway to the Conductor is from the console port.

1. Connect the Airwall Gateway to a network shared with the Conductor.
2. Connect a computer to the 75-series Airwall using the micro USB console port located on the back.
3. Using a terminal (macOS, Linux) or terminal emulator (Windows), connect to the Airwall using baud rate 115200.
4. At the login prompt, log in with name: airsh, no password. (For v2.2.3 and earlier, the password is airsh).
5. Use `conductor set` to set the Conductor IP address or URL and port (optional), or remove a Conductor URL. For example: `conductor set my-conductor.tempered`.
6. Turn the power off and back on again.

The Airwall Gateway should now be recognized in the Conductor.

For alternate methods provisioning the Airwall including automatically adding Airwall Gateways as they connect to the network, go to Connect Airwall Gateways to the Conductor on page 292.

Set up 110-series hardware

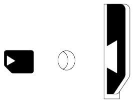
Download PDF

The Airwall 110 platforms are small form factor industrial security appliances that facilitate private overlay networks between customer-provided equipment and devices. This document contains important operating information, specifications, and installation instructions.

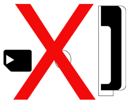
SIM Card Orientation

Insert the SIM card with the angled corner up and to the front, as shown in the first picture.

Correct:



Incorrect: Angled edge is inside the slot



Multi-Purpose Button

Also called the Reset button, the multi-purpose button provides two different functions, depending on how long it is pressed and held.

Press Length	Instructions	Function
Short Press	Press for 5 seconds and release. The Status LED will blink steadily.	Places the Airwall Gateway in Diagnostic mode.
Long Press	Press for at least 8 seconds and release. The Status LED will blink in a 2 flash, 1 flash pattern.	Resets the Airwall Gateway to factory defaults.

Note: To exit diagnostic mode, select **Reboot** in the Diagnostic mode interface, or turn the Airwall Gateway off and back on again.

Troubleshooting

If an Airwall Gateway is online, you can use the Conductor to download a packet capture file, a diagnostic report, or a support bundle for troubleshooting. Log in to the Conductor with a system administrator or network administrator account, then go to the Airwall Gateway's **Diagnostics** page: Select **Airwalls**, choose the one you want from the list, then click **Diagnostics**.

Start a packet capture to troubleshoot networking issues:

1. On the Airwall Gateway's **Diagnostics** page, begin a packet capture by clicking **Start Packet Capture**.
2. Stop the packet capture by clicking **Stop Packet Capture**.

You receive a download link once the Conductor has finished creating the packet capture .pcap file. View the .pcap file using any packet-capture and proto- col-analysis tool, such as Wireshark.

Create a diagnostic report to check Airwall Gateway health:

1. On the Airwall Gateway's **Diagnostics** page, you can put it into diagnostic mode and download a diagnostics report. If the Airwall Gateway's is offline, you can put it in **Diagnostics** mode to download the report.
2. Create your report by clicking **Request a diagnostic report**.

You receive a download link once the Conductor has finished creating the report .txt file. Review the diagnostic report for a high-level look at the overall health of the Airwall Gateway.

Create a support bundle for Tempered Support:

A support bundle .pkg file is an encrypted archive that facilitates technical support by Tempered.

1. On the Airwall Gateway's **Diagnostics** page, you can put it into diagnostic mode and download a support bundle. If the Airwall Gateway is offline, you can put it in **Diagnostics** mode to download the support bundle.
2. Create a support bundle by clicking **Request a support bundle**.
3. When the support bundle .pkg file is ready, download the file and send it as an email attachment to Customer Success

Fault Relay

This device also has a normally-open relay contact that is connected when the device is fully functional and has underlay connectivity. The relay disconnects when communication via this device is not possible. Connect your custom circuitry bearing in mind the following maximum ratings:

- Voltage: 220 VDC /240 VAC, Max current2.0A

Specifications

Airwall 110 Series	
Ethernet Ports	2 x 10/100 Mbps RJ-45 ports, auto MDI/MDIX
Console Port	1 x micro USB
Controls	1 x multi-purpose button (actuated with pin)
Indicators	1x Power 1x Status 1x Map / Conductor 1x Diagnostic mode 1x Cellular Link (110g) 1x SIM card (110g)
Relay	Voltage: 220V DC/250V AC, Max current 2.0A
DC Power Input	DC 9-48V, 0.55A-0.1A Over-voltage protection Reverse-polarity protection
Storage Temp range	-45° to 85° C (-49° to 185° F)
Operating Temp range	-40° to 70° C (-40° to 158° F)
Operating humidity	5% to 95% (non-condensing)

Airwall 110 Series	
Dimensions	31mm W x 100mm D x 125mm H 1.22in W x 3.94in D x 4.92in H
Mounting	DIN-rail, desk-mount
Weight	290g (10.23 oz)

Serial Interfaces	
Protocols	RS-232, RS-485, RS-422
Connector	2 x DE-9M

Cellular Connectivity (110g)	
SIM card	1x micro (3FF) Push-Push SIM card slot
3G	DC-HSDPA Category 24. 42mbps DL max HSUPA Category 5. 5.76Mbps UL max 24dBm+1dB/-3dB maximum transmit power
4G	LTE Category 4: 1.4 – 20MHz bandwidth FDD 150mbps DL, 50mbps UL max TDD 130mbps DL, 30mbps UL max 23dBm±2dB maximum transmit power
3G bands	WCDMA B1, B2, B4, B5, B6, B8, B19
4G LTE FDD bands	B1, B2, B3, B4, B5, B7, B8, B12, B13, B18, B19, B20, B25, B26, B28
4G LTE TDD bands	B38, B39, B40, B41

Regulatory approvals	
Global	IECEE CB Scheme safety
European Union	LVD, EMCD, RoHS, REACH, WEEE RED (110g)
United States	FCC Part 15B Class A, cULus, FCC Radio
Canada	ICES-03 Class A, cULus, ISED/IC Radio
Japan	VCCI, JATE (110g), TELEC (110g)
Australia	ACMA TLN 2015, RLN 2014, EMR LN 2014 (110g) ACMA EMC LN 2017 (110e, 110g)
New Zealand	Radio Standards Notice 2020 (110g) EMC Standards Notice 2019

Maximum approved antenna gain (dBi, peak)

Band	Uplink Freq (MHz)	USA	Canada	Japan
LTE B12	699 – 716	8.70	7.76	N/A
LTE B28	703 – 748	N/A	N/A	3.00
LTE B13	777 – 787	9.16	8.09	N/A

Band	Uplink Freq (MHz)	USA	Canada	Japan
LTE B5, B19, B20, B26, B18, WCDMA VI	814 – 849	9.36	8.25	3.00
LTE B8	880 – 915	N/A	N/A	3.00
LTE B3, B4	1710 – 1785	5.00	5.00	3.00
LTE B2, B25, B39	1850 – 1920	8.00	8.00	N/A
LTE B1	1920 – 1980	N/A	N/A	3.00
LTE B7, B38, B41	2496 – 2690	8.00	8.00	3.00

Notice:

Hereby, Tempered Networks, Inc declares that the radio equipment type Airwall 110g is in compliance with the Directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address:https://repo.tempered.io/DoC/110.

The Airwall-110e and Airwall-110g can be used in all EU Member States.

This device complies with Industry Canada’s license-exempt RSSs. Operation is subject to the following two conditions: (1) This device may not cause interference; and (2) This device must accept any interference, including interference that may cause undesired operation of the device.

Radiation Exposure:

This equipment complies with FCC and ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20cm between the radiator and your body and must not be co-located or operating in conjunction with any other antenna or transmitter.

If this device is installed with an antenna other than the type included with it, you must select an antenna and cabling system that respects the maximum antenna gain listed in the tables. If your selected antenna does not meet these criteria, you may void your legal authority to operate this equipment.

Parts List

WALL-HW-110e	**Power Supply:**
WALL-HW-110g	ACC-HW-110-PSU-25W
included with above:	**AC Power cables:**
• USB A to micro USB cable Micro SIM card slot door • 2x Antennas-ACC-HW-ANT-LTE-5 (ACC-HW-ANT-LTE-3 in Japan) • 1x 3 pin power connector 1x 2 pin relay connector DIN rail mounting kit	ACC-HW-PWR-C13-NA, (North America) ACC-HW-PWR-C13-JP, (Japan) ACC-HW-PWR-C13-AU, (Australia / New Zealand) ACC-HW-PWR-C13-UK, (UK, Singapore, Malaysia)

Safety and Warnings

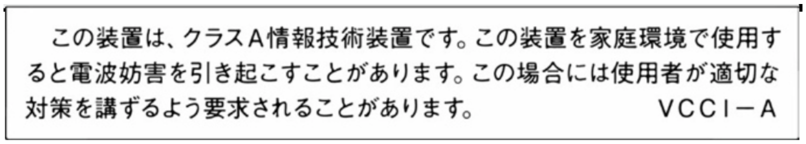
⚠ **DANGER: Elevated Operating Ambient**: If installed in a closed environment, make sure the operating ambient temperature is compatible with the maximum ambient temperature specified by the manufacturer.

⚠ **DANGER: Reduced Air Flow**: Make sure the amount of air flow required for safe operation of the equipment is not compromised during installation.

⚠ **DANGER: Mechanical Loading**: Make sure the mounting of the equipment is not in a hazardous condition due to uneven mechanical loading.

DANGER: Circuit Overloading: Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on over-current protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.



この装置は、クラスA情報技術装置です。この装置を家庭環境で使用す
ると電波妨害を引き起こすことがあります。この場合には使用者が適切な
対策を講ずるよう要求されることがあります。　VCCI－A

Set up 150 Series Hardware

Set up 250 Series Hardware

Set up 500 Series Hardware

Note: The hardware for an Conductor-500 and an Airwall Gateway-500 are similar. If your order contains both, check the bottom of the unit or the box for a sticker that marks Conductor hardware.

Connect Airwall Gateways to the Conductor

Set up and manage Airwall Gateways from the Conductor. Before you begin, ensure that you already have the Conductor set up. You can connect the devices that you want to protect to the Airwall Gateway after it is set up.

Note: Please refer to the Airwall Gateway Platform Guide that shipped with your model for additional information and physical port locations.

Once the Airwall Gateway is configured to connect to the Conductor, connect the Airwall Gateway to the underlay on Port 1, or the designated underlay port for your model.

After fully configuring an Airwall Gateway, you can view basic configuration information by navigating to the **Airwalls** tab and selecting an Airwall Gateway. The following information about the Airwall Gateway is available:

- Overlay networks it belongs to
- IP address
- UID (unique ID)
- serial number
- model
- firmware revision
- user authentication (disabled by default)
- encryption (AES-256 (default), AES-128, AES-256 with compression)

Connect an Airwall Gateway with Diag mode

You can manually point an Airwall Gateway to the Conductor URL, depending on your model.

Note: For additional information about manually configuring a URL, see the Platform Guide for your Airwall Gateway model.

1. Connect Port 1 of your Airwall Gateway to a network with access to your Conductor.
2. Configure a computer to use DHCP to obtain an IP address and netmask.
3. Connect the computer to port 2 of the Airwall Gateway.

4. Power up the Airwall Gateway.
5. Place the Airwall Gateway in Diagnostic mode. Use the display screen, if present, or follow the instructions in the Platform Guide for your model. The status LED will display a fast, steady blink pattern in Diagnostic mode.
6. In your web browser, navigate to http://192.168.56.3 to connect to the Diagnostic mode user interface. It may take a minute for the computer to connect.
7. In **General Settings**, select **Edit Settings**.
8. On the **Edit Airwall Conductor Hostname or IP Setting** page, click the Plus (+) sign.
9. In the **Host** box, enter your Conductor URL or IP address.
10. Click **Submit**.
11. Click **Check** to check your connection to the Conductor.
    If you get a "Connection failed" message, it doesn't necessarily mean the connection has failed. If it's yellow, it means unprovisioned, and unlicensed, therefore unable to connect to the Conductor.

    Tip: Ping the Conductor IP from the Airwall Gateway to make sure it can reach the Conductor.
12. Reboot the Airwall Gateway. Click **Settings** (gear) icon in the top-right corner of the window, and then click **Reboot**.

    Note: You can also reboot turning theAirwall Gateway off and back on.

    When the Airwall Gateway comes back online, it contacts the Conductor to request provisioning. To continue, see Provision and License Airwall Edge Services on page 193.

You can now:

- Provision and License Airwall Edge Services on page 193.
- Connect the devices you want to protect to the Airwall Gateway. See your platform guide for which port to connect devices to (typically Port 2). For information on adding devices in the Conductor, see Connect and Configure Devices on page 414

Connect to a physical Airwall Gateway or Conductor with a console port

If your physical Airwall Gateway or Conductor is equipped with a console port (or your cloud or virtual provider allows console access), you can configure the Conductor URL and other options using a computer connected to the console port using `airsh` commands.

Note: For additional information about manually configuring a URL, see the Platform Guide for your Airwall Gateway model.

Note: For more information about the commands available for `airsh`, see Airshell (airsh) Command Reference on page 362.

Note: If you've Set up Remote Access to Airshell via SSH on page 374, you can also Access an Airwall Gateway Remotely on page 375.

1. **Connect to your network** – Connect Port 1 of your Airwall Gateway to a network with access to your Conductor.
2. **Connect a computer to the Airwall Gateway console port** – Plug in using the micro USB console port. Check your platform guide for the location of your console port, or see Connecting to the console port on an Airwall Gateway on page 297.
    a) Using a terminal (macOS, Linux) or terminal emulator (Windows), connect to the Airwall Gateway using baud rate 115200.
3. **Log in to the Console:**
    - v2.2.8 and later: log in with name: `airsh`, and no password
    - v2.2.5 and earlier: log in with name: `airsh`, and password: `airsh`.
4. **Set the Conductor address** - Set the Conductor IP address or URL (and port, if needed (optional)). For example:

```
conductor set my-conductor.tempered.com
```

Tip: Ping the Conductor IP from the Airwall Gateway to make sure it can reach the Conductor.

When the Airwall Gateway comes back online, it contacts the Conductor to request provisioning.

You can now:

- Provision and License Airwall Edge Services on page 193.
- Connect the devices you want to protect to the Airwall Gateway. See your platform guide for which port to connect devices to (typically Port 2). For information on adding devices in the Conductor, see Connect and Configure Devices on page 414

Starting with v2.2.8, the Airshell console login has no default password. If you are concerned about securing physical access to Airshell, set a password by entering `conf password` and following the prompts to set and confirm a new password. Keep this password in a secure location, as it cannot be recovered. This password is only for airsh physical console access and is not used when you access airsh remotely.

CAUTION: If this password is lost, you will need to do a factory reset to clear the password.

Connect an Airwall Gateway with a DNS SRV record

You can connect an Airwall Gateway to the Conductor by using a DNS SRV record.

Note: For specific information, see the Platform Guide for your Airwall Gateway model.

1. **Check DHCP** – Ensure there is a DHCP server and a DNS resolver or DNS server for the local domain accessible from the shared network.
2. **Create a DNS SRV record** – On the DNS server, add a SRV record pointing to the Conductor URL:

   ```
   _service._proto.name TTL class SRV priority weight port target
   ```

   For example, if your shared network domain is `example.com` and the Conductor hostname is `cond-01`, then the SRV record should be:

   ```
   _ifmap._tcp.example.com. 3600 IN SRV 10 0 8096 cond-01.example.com
   ```

   Note: Use the TTL, priority and weight for your DNS environment. Port 8096 is the default, but you can change it in the Conductor and set it to an alternate port.
3. **Connect to your network** – Connect Port 1 of your Airwall Gateway to a network with access to your Conductor. The DHCP server assigns an IP address, netmask, and a default gateway to the Airwall Gateway. The Airwall Gateway then does a DNS lookup and configures itself using the Conductor address.

You can now:

- Provision and License Airwall Edge Services on page 193.
- Connect the devices you want to protect to the Airwall Gateway. See your platform guide for which port to connect devices to (typically Port 2). For information on adding devices in the Conductor, see Connect and Configure Devices on page 414

Connect an Airwall Gateway by using a factory-configured URL

Tempered can pre-configure the Conductor URL for each Airwall Gateway. Airwall Gateways configured with DNS require the user to configure the DNS service to resolve the correct IP address for the Conductor hostname based on the factory-configured URL.

1. Ensure domain name service is configured for your underlay.
2. Apply power to the Airwall Gateway hardware.
3. Connect the Airwall Gateway to your underlay via Port 1 or your underlay port.

You can now:

- Provision and License Airwall Edge Services on page 193.
- Connect the devices you want to protect to the Airwall Gateway. See your platform guide for which port to connect devices to (typically Port 2). For information on adding devices in the Conductor, see Connect and Configure Devices on page 414

Check if an Airwall Gateway or Airwall Agent is online

Once an Airwall Edge Service is connected to the Conductor and licensed, you can validate that it is online.

To determine if an Airwall Gateway or Airwall Agent or Server is online:

1. In the Conductor, click **Airwalls** and select the drop-down to the right of the desired Airwall Edge Service.
2. Click **Check online**
   If the Airwall Gateway is online, it temporarily displays offline in place of the IP address, then its IP address is displayed in green. If the Airwall Gateway is in fact offline, offline remains in place of the IP address.

Modbus-RTU and Modbus-TCP on an Airwall Edge Service

The Modbus protocol enables data transmission between devices using a serial interface.

Modbus-TCP applies to: 2.1.6 and higher

Beginning with v2.1.6, we have added Modbus support, making it possible to communicate over Internet or Intranet.

The following Airwall Gateways/HIPswitches support Modbus:

- Airwall Gateway-100s (RS-232)
- Airwall Gateway-150 (RS-232)
- Airwall Gateway-250e/g/d (RS-232 & RS-485)
- Airwall Gateway-300 (RS-232)

Modbus-RTU

The Modbus protocol is essentially a technique of enabling data transmission between devices using a serial interface. Our serial-enabled Airwall Gateways have been able to encapsulate Modbus-RTU (Remote Terminal Unit) over a serial line since firmware 1.x.

With v2.1.6, we have enhanced our Serial over IP (SoIP) feature with Modbus-TCP (Transmission Control Protocol) support making it possible to communicate over Internet or Intranet.

After configuring Modbus via the Airwall Gateway SoIP settings in Conductor, the Airwall Gateway accepts Modbus-TCP commands from servers, issues the commands to serially-connected Modbus RTU devices, and returns the responses via Modbus TCP back to the server. This configuration provides optimal efficiency for Modbus traffic in terms of throughput, latency, and number of messages as compared to transparent Serial over IP.

Modbus-TCP

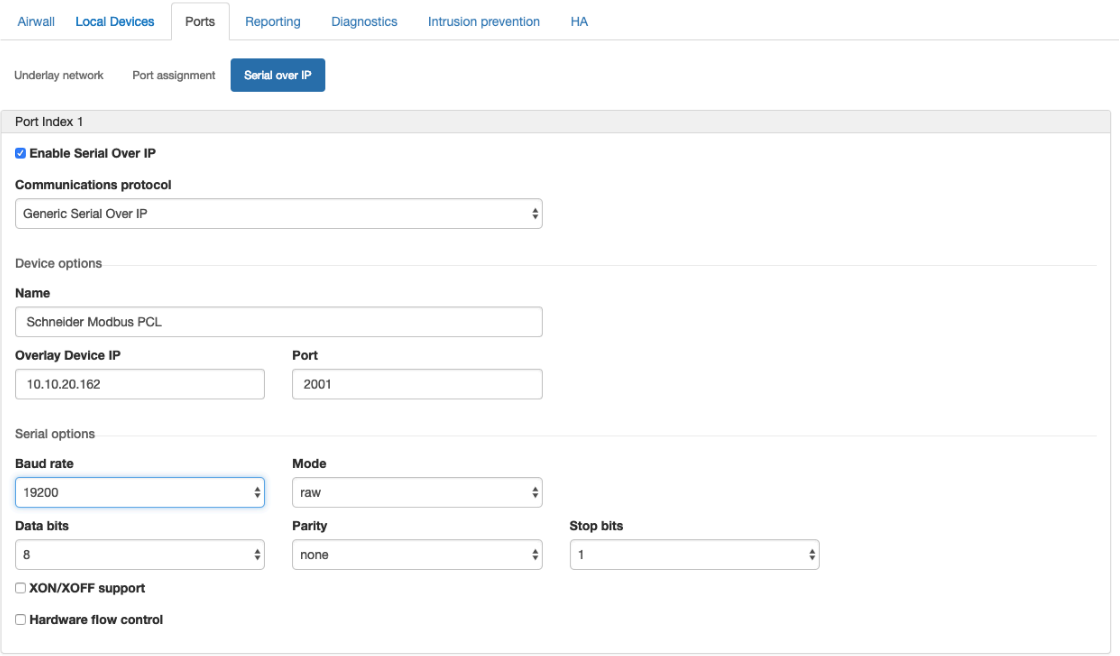
Modbus-TCP is a frame-aware Modbus-RTU encapsulation that is compatible with modern Modbus/SCADA systems. Unlike SoIP, Modbus-TCP processes each Modbus frame as a separate packet, and transfers the burden of error correction to the TCP protocol.

Configure Modbus-RTU

Use Modbus-RTU to enable data transmission between devices using the Airwall Gateway serial interface.

1. Connect an RS-232 Modbus Program Logic Controller (PLC) to your Airwall Gateway using a DB9-to-DB9 or DB9-to-RJ45 cable.

   Note: RS-485 is supported by the Airwall Gateway/HIPswitch-250, but others will require an adapter.
2. Go to **Airwalls>Airwalls>Ports>Serial over IP**
3. Click **Edit Settings**, and then configure SoIP using the **Generic Serial Over IP** communications protocol.



Port Index 1

☑ Enable Serial Over IP

Communications protocol: Generic Serial Over IP

Device options

Name: Schneider Modbus PCL

Overlay Device IP: 10.10.20.162

Port: 2001

Serial options

Baud rate: 19200

Mode: raw

Data bits: 8

Parity: none

Stop bits: 1

□ XON/XOFF support

□ Hardware flow control

4. Add the SoIP device to an overlay and create policy.

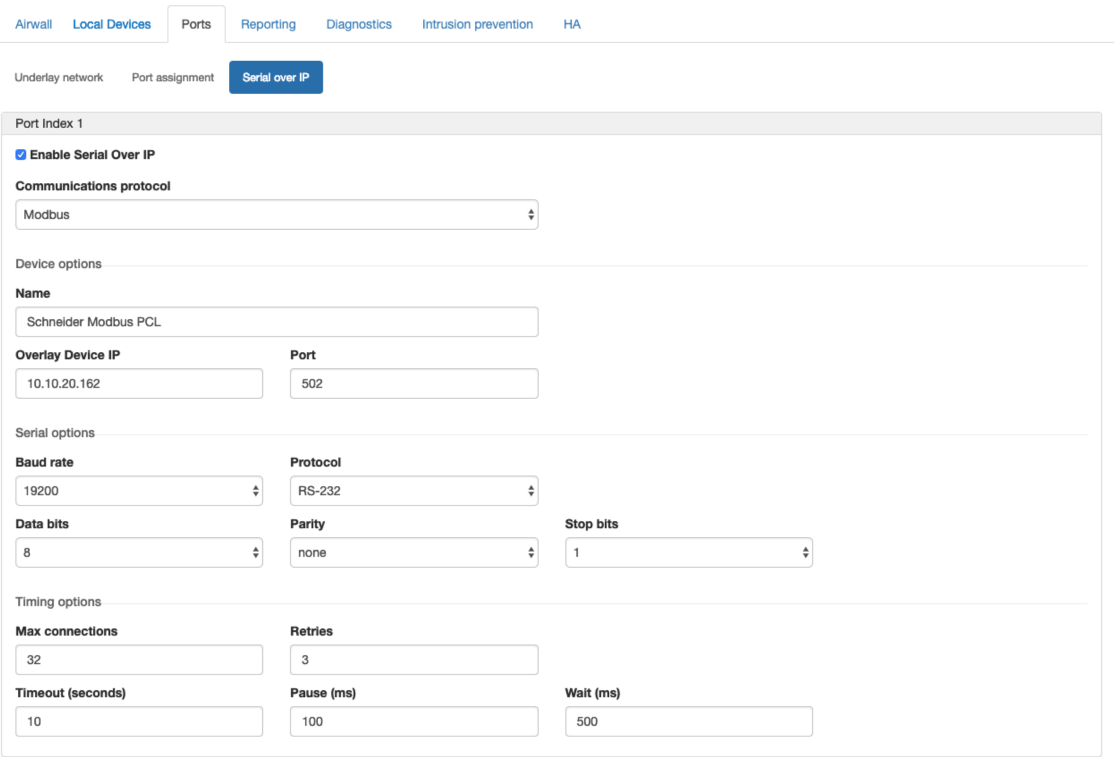
   For information, see Add devices or device groups to an overlay network on page 419.
5. Using Modbus Polling software, such as FieldTalk's ModPoll, test the configuration using a command such as the following: `modpoll -m rtu -r 1 -c 125 -1 -p 4001 10.10.20.162`

Set Modbus-TCP

Use Modbus-TCP now available in firmware 2.1.6 to enable data transmission between devices using the Airwall Gateway serial interface.

1. Connect an RS-232 Modbus Program Logic Controller (PLC) to your Airwall Gateway using a DB9-to-DB9 or DB9-to-RJ45 cable.

   Note: RS-485 is supported by the HIPswitch-250, but others will require an adapter.
2. Go to **Airwalls>Airwalls>Ports>Serial over IP**
3. Click **Edit Settings**, and then configure SoIP using the **Modbus** communications protocol.



Port Index 1

☑ Enable Serial Over IP

Communications protocol: Modbus

Device options

Name: Schneider Modbus PCL

Overlay Device IP: 10.10.20.162

Port: 502

Serial options

Baud rate: 19200

Protocol: RS-232

Data bits: 8

Parity: none

Stop bits: 1

Timing options

Max connections: 32

Retries: 3

Timeout (seconds): 10

Pause (ms): 100

Wait (ms): 500

4. Add Modbus-TCP device to the Overlay and create policy

   For more information, see Add devices or device groups to an overlay network on page 419.
5. Using Modbus Polling software, such as FieldTalk's ModPoll, test the configuration using a command such as the following: `modpoll -m tcp -r 1 -c 125 -1 10.10.20.162`

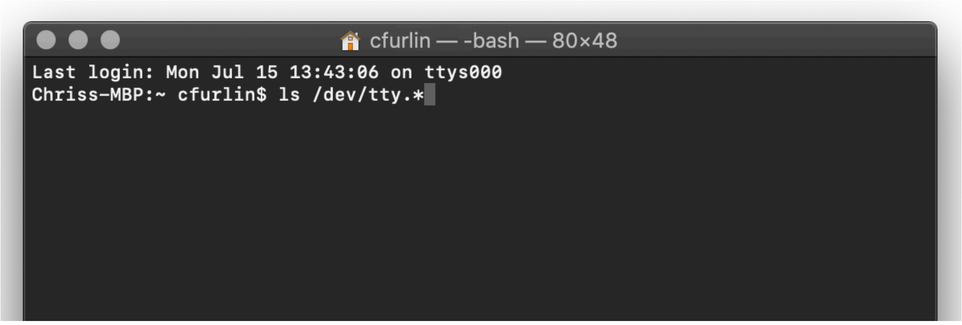
Connecting to the console port on an Airwall Gateway

Airwall Gateways with a console port allow you to connect a computer using a cable with a microUSB male connector on one end, and a connector supported by your computer on the other, commonly USB. Once you have connected the Airwall Gateway to your computer and applied power to the device, you can use one of the procedures below to access the Airwall Gateway's configuration options, depending on your computer's operating system.

Connect to the console port using Linux or macOS

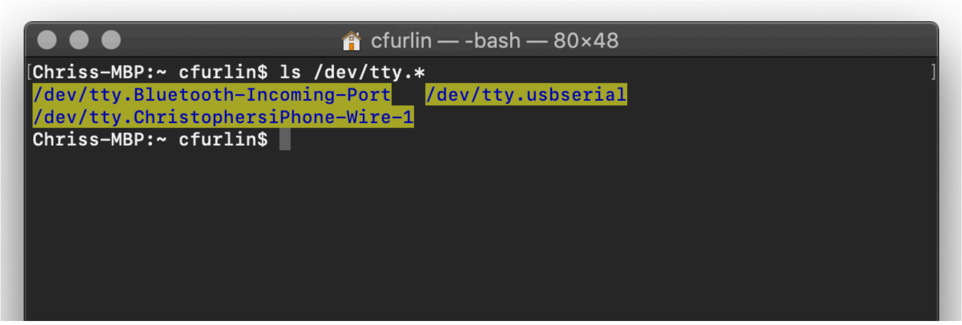
In a Terminal window, do the following:

1. Find the serial interface name. You can look in the dev folder for a tty* file, or use `|grep tty` and press `Enter` to obtain the name of the serial interface.



```
Last login: Mon Jul 15 13:43:06 on ttys000
Chriss-MBP:~ cfurlin$ ls /dev/tty.*
```

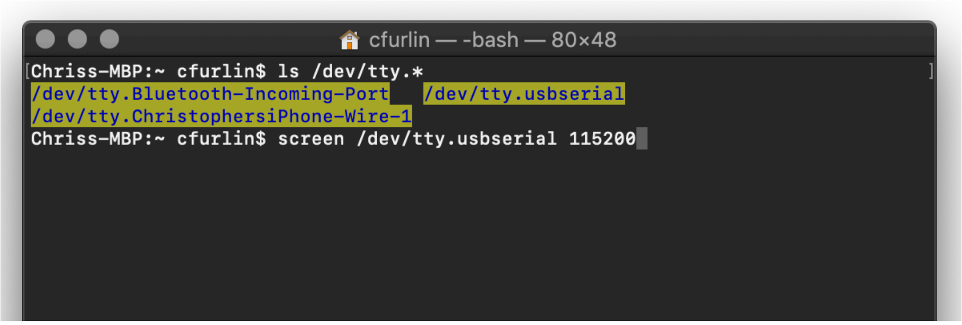
2. Locate the interface in the list. In the example below, the interface is `/dev/tty/usbserial`.



```
Chriss-MBP:~ cfurlin$ ls /dev/tty.*
/dev/tty.Bluetooth-Incoming-Port    /dev/tty.usbserial
/dev/tty.ChristophersiPhone-Wire-1
Chriss-MBP:~ cfurlin$
```

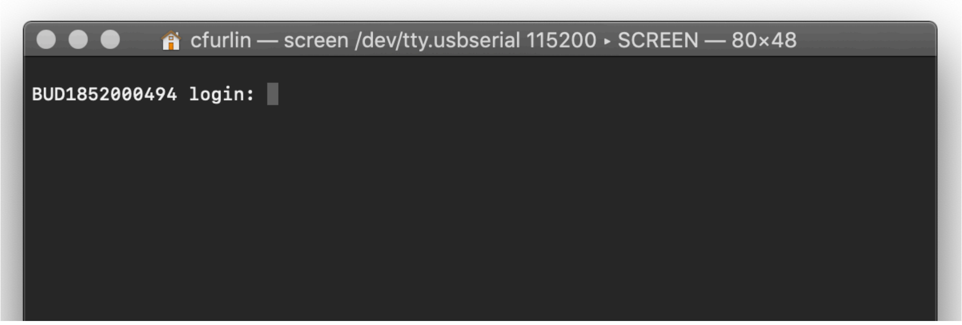
Note: If you have multiple serial devices attached to your computer, using the command with the Airwall Gateway disconnected and then reconnected may help you determine which interface belongs to the Airwall Gateway.

3. Use a TTY terminal app to enter the serial interface and name and baud rate. For example, enter `screen`, the serial interface name, and the baud rate `115200`. Press `Enter`.



```
Chriss-MBP:~ cfurlin$ ls /dev/tty.*
/dev/tty.Bluetooth-Incoming-Port    /dev/tty.usbserial
/dev/tty.ChristophersiPhone-Wire-1
Chriss-MBP:~ cfurlin$ screen /dev/tty.usbserial 115200
```

4. Press `Enter` again. You may have to do this several times until the login prompt appears.



```
BUD1852000494 login:
```

5. Log in with username: `airsh` and password `airsh`.
6. You can now use `airsh` commands to configure or run diagnostics. The two most commonly used commands are `diag`, which places the Airwall Gateway in diagnostic mode and `conductor set`, which tells the Airwall Gateway where to find the Conductor.

   For a list of commands, see Airshell (airsh) Command Reference on page 362.

Connect to the console port using Windows

You can connect to an Airwall Gateway equipped with a console port to configure or run diagnostics using `airsh`.

Note: If you're using an Airwall Gateway running a version earlier than 2.2.3, replace `airsh` with `hipsh` in the instructions below.

1. **Connect a computer to the Airwall Gateway** – Plug a computer in using the micro USB console port. For the location of the console port, see the platform guide for your hardware.
2. **Connect to the Airwall Gateway** - Using a terminal emulator, connect to the Airwall Gateway using baud rate 115200.
3. **Log in to `airsh`** - At the login prompt, log in with: name: `airsh`, password: `airsh`.

You can now run `airsh` commands to configure or run diagnostics on the Airwall Gateway. Examples:

- `diag` - Enter `diag` to put the Airwall Gateway into Diagnostics mode.
- `conductor set` - Set the Conductor URL:

  ```
  conductor set <conductor IP address or URL>
  ```

  For example,

  ```
  conductor set my-conductor.tempered.com
  ```

For more information, see Airshell (airsh) Command Reference on page 362.

Airwall Gateway Platform Guides

Download the latest platform guide for your Airwall Gateway.

Platform Guide	**PDF Download Link**
Airwall Gateway 75	English
Airwall Gateway 110-series	English French
Airwall Gateway 500-series	English Japanese

110-series Hardware Platform Guide

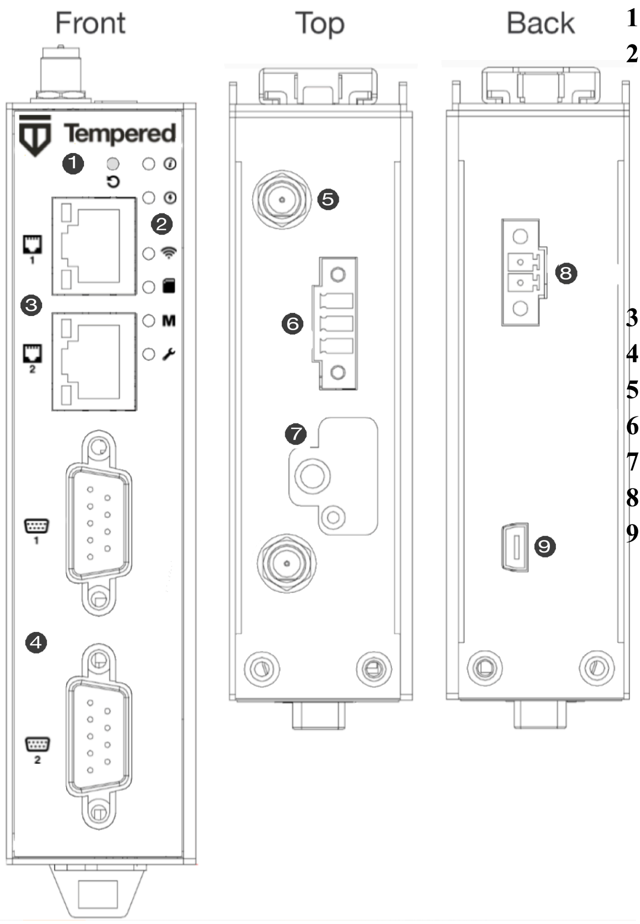
Download PDF

The Airwall 110 platforms are small form factor industrial security appliances that facilitate private overlay networks between customer-provided equipment and devices. This document contains important operating information, specifications, and installation instructions.

Models

Part Number	Model	Cellular	Eth Ports	Serial Ports
PLF-0138-01	Airwall 110e	No	2	2
PLF-0140-01	Airwall 110g	Yes	2	2

Panel Layouts



1. Multi-purpose button
2. LED - Signal indicators:
   - Status
   - Power
   - Cellular connection status
   - SIM card
   - MAP connection (Conductor)
   - Diagnostic mode
3. Ethernet ports
4. Serial ports
5. Antenna connectors
6. Power input connector
7. SIM card slot
8. Relay
9. Micro-USB console port

Quick Start

1. **Plug in the Airwall Gateway** – Locate in an area that complies with its safe operating guidelines, and then plug it in or apply power.
2. **Connect to your network** - Using Port 1, connect the Airwall Gateway to a network where it can reach the Conductor.
3. **Provide the Conductor address -** There are three ways to configure the Conductor address on the 110-series Airwall Gateways:
   - Connect an Airwall Gateway with Diag mode on page 292
   - Connect to a physical Airwall Gateway or Conductor with a console port on page 293
   - Connect an Airwall Gateway with a DNS SRV record on page 294
4. **Test your connection to the Conductor** – Check in **Diagnostics** mode, under Airwall Conductor, if the Conductor shows as Reachable, or using the console port, ping the conductor from the Airwall Gateway:

```
ping my-conductor.tempered.com
```

5. **Connect to devices** – Connect the devices you want to protect to the Airwall Gateway on Port 2.

Status LED Codes

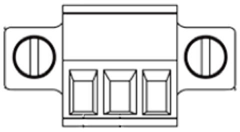
State	LED Pattern	State	LED Pattern
Normal Operation	On Steady	No Conductor Connection	**O O O O = = O O = =**

State	LED Pattern	State	LED Pattern
Conductor Blink	**O O** = =	System Error	**O O O O** = = **O O O** = =
Missing Identity	**O O O** = = **O** = =	Secure Network Error	**O O O O** = = =
Factory Reset	**O O** = = **O** = =	No Shared Network	**O O O O** = = **O** = =
Diagnostic Mode	**O** = **O** = (fast blink)	Firmware Download	**O O O** = = **O O** = =
		Firmware Update	**O O O** = = =
Key: **O** is on, = is off			

Wiring

Power Inputs

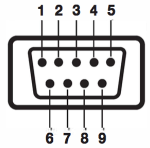
This device supports one power supply. The connector for PWR 1 is located on the terminal block on the top of the unit.



Step 1: Insert the negative DC into the V- terminal and the positive DC into the V+ terminal.

Step 2: To keep the DC wires from pulling loose, use a small flat-blade screwdriver to tighten the wire-damp screws in the front of the terminal block connector.

Serial Connector

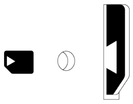


Pin #	RS-232	RS-422	RS-485
1		TX-	Data-
2	RxD	TX+	Data+
3	TxD	RX+	
4		RX-	
5	GND	GND	GND
6			
7	RTS		
8	CTS		
9			

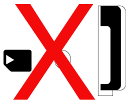
SIM Card Orientation

Insert the SIM card with the angled corner up, as shown in the first picture.

Correct:



Incorrect:



Multi-Purpose Button

Also called the Reset button, the multi-purpose button provides two different functions, depending on how long it is pressed and held.

Press Length	Instructions	Function
Short Press	Press for 5 seconds and release. The Status LED will blink steadily.	Places the Airwall Gateway in Diagnostic mode.
Long Press	Press for at least 8 seconds and release. The Status LED will blink in a 2 flash, 1 flash pattern.	Resets the Airwall Gateway to factory defaults.

Note: To exit diagnostic mode, select **Reboot** in the Diagnostic mode interface, or turn the Airwall Gateway off and back on again.

Troubleshooting

If an Airwall Gateway is online, you can use the Conductor to download a packet capture file, a diagnostic report, or a support bundle for troubleshooting. Log in to the Conductor with a system administrator or network administrator account, then go to the Airwall Gateway's **Diagnostics** page: Select **Airwalls**, choose the one you want from the list, then click **Diagnostics**.

Start a packet capture to troubleshoot networking issues:

1. On the Airwall Gateway's **Diagnostics** page, begin a packet capture by clicking **Start Packet Capture**.
2. Stop the packet capture by clicking **Stop Packet Capture**.

You receive a download link once the Conductor has finished creating the packet capture .pcap file. View the .pcap file using any packet-capture and proto- col-analysis tool, such as Wireshark.

Create a diagnostic report to check Airwall Gateway health:

1. On the Airwall Gateway's **Diagnostics** page, you can put it into diagnostic mode and download a diagnostics report. If the Airwall Gateway's is offline, you can put it in **Diagnostics** mode to download the report.
2. Create your report by clicking **Request a diagnostic report**.

You receive a download link once the Conductor has finished creating the report .txt file. Review the diagnostic report for a high-level look at the overall health of the Airwall Gateway.

Create a support bundle for Tempered Support:

A support bundle .pkg file is an encrypted archive that facilitates technical support by Tempered.

1. On the Airwall Gateway's **Diagnostics** page, you can put it into diagnostic mode and download a support bundle. If the Airwall Gateway is offline, you can put it in **Diagnostics** mode to download the support bundle.
2. Create a support bundle by clicking **Request a support bundle**.

3. When the support bundle .pkg file is ready, download the file and send it as an email attachment to Customer Success

Fault Relay

This device also has a normally-open relay contact that is connected when the device is fully functional and has underlay connectivity. The relay disconnects when communication via this device is not possible. Connect your custom circuitry bearing in mind the following maximum ratings:

- Voltage: 220 VDC /240 VAC, Max current2.0A

Specifications

Airwall 110 Series	
Ethernet Ports	2 x 10/100 Mbps RJ-45 ports, auto MDI/MDIX
Console Port	1 x micro USB
Controls	1 x multi-purpose button (actuated with pin)
Indicators	1x Power 1x Status 1x Map / Conductor 1x Diagnostic mode 1x Cellular Link (110g) 1x SIM card (110g)
Relay	Voltage: 220V DC/250V AC, Max current 2.0A
DC Power Input	DC 9-48V, 0.55A-0.1A Over-voltage protection Reverse-polarity protection
Storage Temp range	-45° to 85° C (-49° to 185° F)
Operating Temp range	-40° to 70° C (-40° to 158° F)
Operating humidity	5% to 95% (non-condensing)
Dimensions	31mm W x 100mm D x 125mm H 1.22in W x 3.94in D x 4.92in H
Mounting	DIN-rail, desk-mount
Weight	290g (10.23 oz)

Serial Interfaces	
Protocols	RS-232, RS-485, RS-422

Serial Interfaces	
Connector	2 x DE-9M

Cellular Connectivity (110g)	
SIM card	1x micro (3FF) Push-Push SIM card slot
3G	DC-HSDPA Category 24. 42mbps DL max HSUPA Category 5. 5.76Mbps UL max 24dBm+1dB/-3dB maximum transmit power
4G	LTE Category 4: 1.4 – 20MHz bandwidth FDD 150mbps DL, 50mbps UL max TDD 130mbps DL, 30mbps UL max 23dBm±2dB maximum transmit power
3G bands	WCDMA B1, B2, B4, B5, B6, B8, B19
4G LTE FDD bands	B1, B2, B3, B4, B5, B7, B8, B12, B13, B18, B19, B20, B25, B26, B28
4G LTE TDD bands	B38, B39, B40, B41

Regulatory approvals	
Global	IECEE CB Scheme safety
European Union	LVD, EMCD, RoHS, REACH, WEEE RED (110g)
United States	FCC Part 15B Class A, cULus, FCC Radio
Canada	ICES-03 Class A, cULus, ISED/IC Radio
Japan	VCCI, JATE (110g), TELEC (110g)
Australia	ACMA TLN 2015, RLN 2014, EMR LN 2014 (110g) ACMA EMC LN 2017 (110e, 110g)
New Zealand	Radio Standards Notice 2020 (110g) EMC Standards Notice 2019

Maximum approved antenna gain (dBi, peak)

Band	**Uplink Freq (MHz)**	**USA**	**Canada**	**Japan**
LTE B12	699 – 716	8.70	7.76	N/A
LTE B28	703 – 748	N/A	N/A	3.00
LTE B13	777 – 787	9.16	8.09	N/A
LTE B5, B19, B20, B26, B18, WCDMA VI	814 – 849	9.36	8.25	3.00
LTE B8	880 – 915	N/A	N/A	3.00
LTE B3, B4	1710 – 1785	5.00	5.00	3.00
LTE B2, B25, B39	1850 – 1920	8.00	8.00	N/A
LTE B1	1920 – 1980	N/A	N/A	3.00
LTE B7, B38, B41	2496 – 2690	8.00	8.00	3.00

Notice:

Hereby, Tempered Networks, Inc declares that the radio equipment type Airwall 110g is in compliance with the Directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address:https://repo.tempered.io/DoC/110.

The Airwall-110e and Airwall-110g can be used in all EU Member States.

This device complies with Industry Canada's license-exempt RSSs. Operation is subject to the following two conditions: (1) This device may not cause interference; and (2) This device must accept any interference, including interference that may cause undesired operation of the device.

Radiation Exposure:

This equipment complies with FCC and ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20cm between the radiator and your body and must not be co-located or operating in conjunction with any other antenna or transmitter.

If this device is installed with an antenna other than the type included with it, you must select an antenna and cabling system that respects the maximum antenna gain listed in the tables. If your selected antenna does not meet these criteria, you may void your legal authority to operate this equipment.

Parts List

WALL-HW-110e	**Power Supply:**
WALL-HW-110g	ACC-HW-110-PSU-25W
included with above:	**AC Power cables:**
• USB A to micro USB cable Micro SIM card slot door • 2x Antennas-ACC-HW-ANT-LTE-5 (ACC-HW-ANT-LTE-3 in Japan) • 1x 3 pin power connector 1x 2 pin relay connector DIN rail mounting kit	ACC-HW-PWR-C13-NA, (North America) ACC-HW-PWR-C13-JP, (Japan) ACC-HW-PWR-C13-AU, (Australia / New Zealand) ACC-HW-PWR-C13-UK, (UK, Singapore, Malaysia)

Safety and Warnings

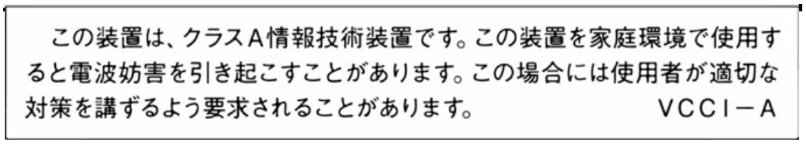
⚠ **DANGER: Elevated Operating Ambient**: If installed in a closed environment, make sure the operating ambient temperature is compatible with the maximum ambient temperature specified by the manufacturer.

⚠ **DANGER: Reduced Air Flow**: Make sure the amount of air flow required for safe operation of the equipment is not compromised during installation.

⚠ **DANGER: Mechanical Loading**: Make sure the mounting of the equipment is not in a hazardous condition due to uneven mechanical loading.

⚠ **DANGER: Circuit Overloading**: Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on over-current protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.



この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。　VCCI－A

Set up virtual Airwall Gateways

Set up a virtual Airwall Gateway in VMware ESX/ESXi

This section contains instructions to install a virtual Airwall Gateway on the ESXi/ESX (VMware) platform.

Prerequisites

Required licenses	An Airwall 300v license for each virtual Airwall Gateway you are setting up.

You will also need:

- An existing installation of VMware ESX/ESXi server version 6.5.0 and later
- An Airwall Gateway OVA
- The Conductor you are connecting to configured and available

System Requirements

The following VMware ESX/ESXi server hardware is required:

Processor

- Minimum requirement of a single processor with hyper-threading support, VT-x technology, and 64-bit architecture.
- Optimum configuration is minimum 4 processing cores with hyper-threading support, VT-x technology, 64-bit architecture, and AES-NI enabled in the host's BIOS.

Virtual image

Below are the minimum configuration requirements available for a virtual Conductor or Airwall Gateway image:

Platform	Memory	Disk
Conductor	4GB	120GB*
Airwall Gateway	1GB	1GB*

* Already included in the default OVA package

Port Group Configuration

By default, a virtual Airwall Gateway OVA image comes with two network interfaces.

Attach each interface to its own port group:

- Port 1 functions as the underlay network
- Port 2 functions as the overlay network

The virtual Airwall Gateway is expandable up to 6 ports. You can configure one port for HA heartbeats with the HA role.

Security configuration

VMware port groups have default security settings inherited from their parent virtual switch. The following port group security settings should be changed to **Accept**:

Note: These changes only need to be made on the port group associated with the overlay device network port group.

- Promiscuous Mode
  - Allows virtual interface adapters connected to this port group to see all Ethernet frames passed on the virtual switch that are allowed under the VLAN policy for the port group.
- Forged Transmits
  - Allows virtual machines to send frames with a MAC Address that is different from the one specified on the virtual interface.

VLAN configuration

- Set **VLAN type** to **VLAN**
- Set a **VLAN ID** unique to this Airwall Gateway overlay device network and protected device

Note: Because virtual Airwall Gateway port groups function as logical groups and not independent network groups, you must set a unique VLAN for each port group attached to an Airwall Gateway.

To deploy the virtual image

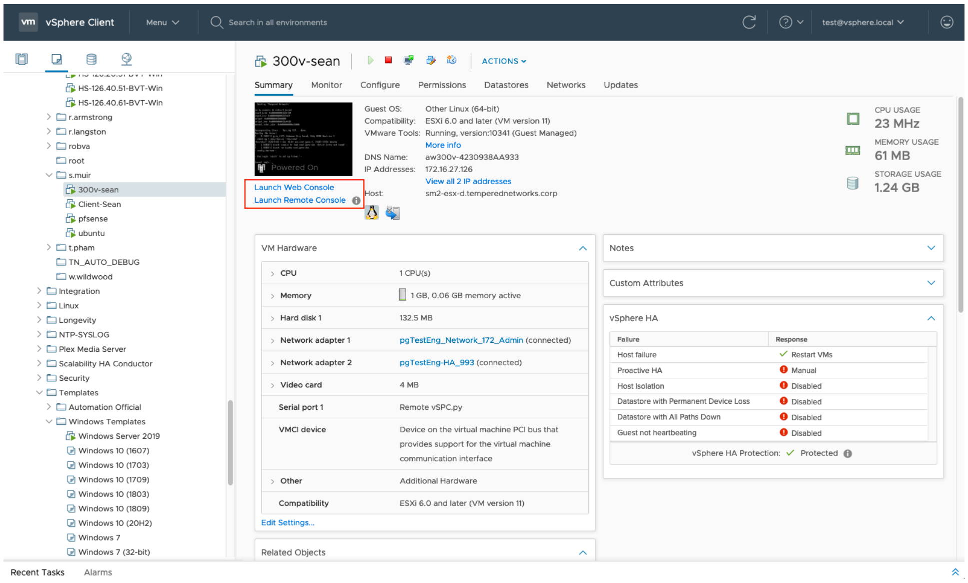
Please check your VMware documentation for the most recent instructions.

1. Download the Airwall x86_64 OVA (ESXi) file from Latest firmware and software on page 514.
2. Deploy a new OVF template from within ESXi using the downloaded OVA file. For most deployments, you can keep the default settings.
3. Give the virtual machine a unique name and select its storage location.
4. Map the virtual machine's network interfaces with the correctly assigned port groups for the Airwall Gateway.
5. Set **Disk provisioning** to **Thin Provisioned**.
6. Verify your configuration, check **Power on after deployment**, and then select **Finish** to begin the update.

Configure a running Airwall Gateway in VMware ESX/ESXi

Once the Airwall Gateway virtual image is successfully running, you can configure the unit to connect to Conductor. The underlay network interface (port 1) defaults to a DHCP-configured interface.

1. In the vSphere ESXi client, select one of the console links:



300v-sean

Guest OS: Other Linux (64-bit)
Compatibility: ESXi 6.0 and later (VM version 11)
VMware Tools: Running, version:10341 (Guest Managed)
More info
DNS Name: aw300v-4230938AA933
IP Addresses: 172.16.27.126
View all 2 IP addresses
Host: sm2-esx-d.temperednetworks.corp

CPU USAGE 23 MHz
MEMORY USAGE 61 MB
STORAGE USAGE 1.24 GB

VM Hardware

CPU	1 CPU(s)
Memory	1 GB, 0.06 GB memory active
Hard disk 1	132.5 MB
Network adapter 1	pgTestEng_Network_172_Admin (connected)
Network adapter 2	pgTestEng-HA_993 (connected)
Video card	4 MB
Serial port 1	Remote vSPC.py
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 6.0 and later (VM version 11)

vSphere HA

Failure	Response
Host failure	✓ Restart VMs
Proactive HA	! Manual
Host Isolation	! Disabled
Datastore with Permanent Device Loss	! Disabled
Datastore with All Paths Down	! Disabled
Guest not heartbeating	! Disabled

vSphere HA Protection: ✓ Protected

Launch Web Console opens in a new tab in the browser. **Launch Remote Console** opens in a desktop app that you may need to install.

2. On the Airwall Gateway, log in to Airshell with name: `airsh`, and no password (2.2.8 and later).
3. You can either determine the IP address for port 1, or manually set it:
   - **To determine the IP address assigned to port 1**, at the Airshell prompt, enter `status network`:

     ```
     airsh> status network
     ```

   - **To manually set the IP address for port 1**, from the console prompt, enter **conf network** and select 1 to configure the IP. For more help, see Configure Port Groups with Airshell on page 376:

     ```
     airsh> conf network
     ```

4. Configure the Conductor using `conductor set` followed by the address and port. For example:

   ```
   airsh> conductor set my-conductor.tempered
   ```

Set up a virtual Airwall Gateway in Microsoft Hyper-V

The virtualization server role for Windows Server 2012 R2 is called Hyper-V Manager. The following documentation show the steps to implement and manage a secure Airwall Gateway and overlay network on Hyper-V network.

Required Licenses

An Airwall 300v license for each virtual Airwall Gateway you are setting up.

Prerequisites

- An existing installation of Microsoft Hyper-V, v2012 or later
- An Airwall Gateway .vhdx file. Download the .vhdx file from Latest firmware and software on page 514.
- The Conductor you are connecting to configured and available.

Install the Airwall Gateway in Hyper-V

1. Open a Hyper-V Manager Console from within your Windows Machine.
   - **Hyper-V Manager in Windows Server 2012 or Windows Server 2012 R2:**
     a. In the lower left-corner, select the **Windows** icon.
     b. Search for `Hyper-V Manager` and open it.
   - **All other versions:**
     a. Right-click in the lower left-hand corner and select **Run**. Type `virtmgmt.msc` to open the Hyper-V Manager snap-in.
2. Go to the **Actions** pane and select **New** > **Virtual Machine** to create a virtual machine for your Airwall Gateway.

   Note: A wizard takes you through the steps to create a **New Virtual Machine**.

3. Select **Specify Name and Location** and give your Airwall Gateway a **Name**.
4. Leave **Store the virtual machine in a different location** unchecked and click **Next**.
5. For **Specify Generation**, select `Generation 1`, and select **Next**.
6. Set the **Startup memory** to *at least* 1 gigabyte of ram (1024).

   Note: Consider how much memory you want to assign your virtual machine, as this is the machine that both contains your data and runs the operating system.

7. Do not check the **Use Dynamic Memory** box. Select **Next**.
8. In **Configure Networking**, from the **Connection** drop-down, select **Not Connected**. You add this connection later.

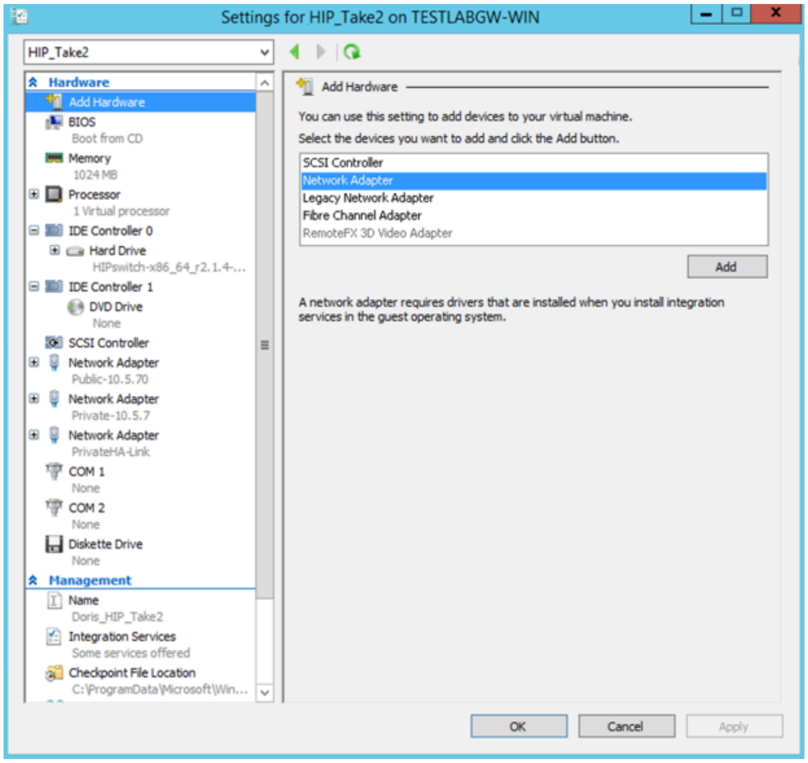
9. Select **Next**.
10. Under **Connect Virtual Hard Disk**, select **Use Existing virtual hard disk**, browse to the location where you saved the *vhdx* file downloaded from Tempered. Select it and click **OK**.
11. Click **Next** to complete the set up and view the **Summary** page. You are now ready to add your network adapters.

Important: Do not start the machine until you set up the hardware using the procedure below.

Add Network Adapters

Once you are finished installing the Airwall Gateway software, you are ready to add the network adapters to the machine that will serve as your Airwall Gateway.

1. From the **Virtual Machines** list, find your Airwall Gateway machine and select **Action** > **Settings**.
2. Add a minimum of two **Network Adapters**. To set the first network adapter, select **Add Hardware** > **Network Adapter** and click **Add**.


Settings for HIP_Take2 on TESTLABGW-WIN

HIP_Take2

Add Hardware

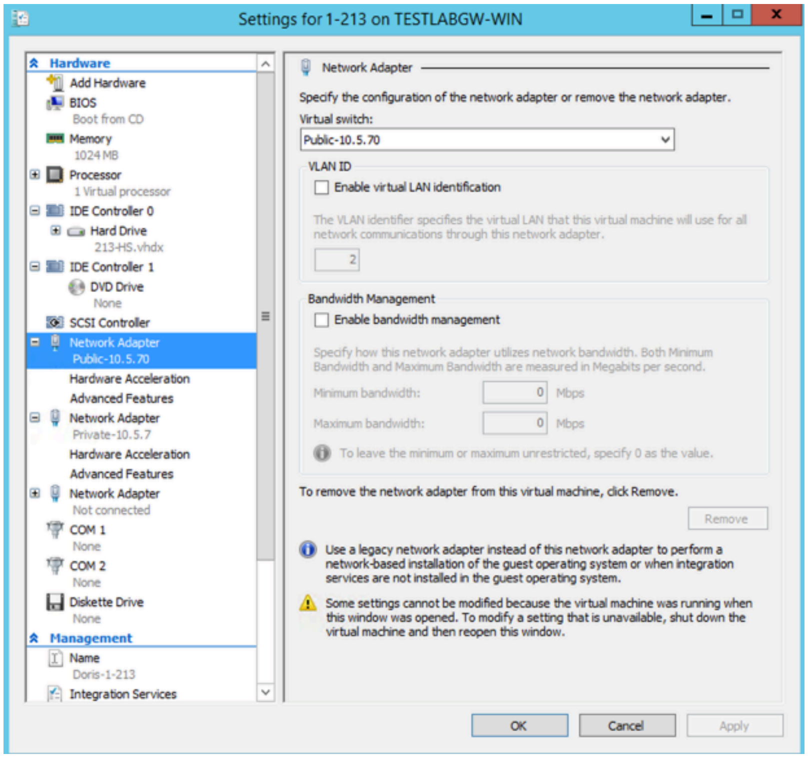
You can use this setting to add devices to your virtual machine.

Select the devices you want to add and click the Add button.

SCSI Controller
Network Adapter
Legacy Network Adapter
Fibre Channel Adapter
RemoteFX 3D Video Adapter

A network adapter requires drivers that are installed when you install integration services in the guest operating system.

3. Configure the first adapter to connect to your underlay. Leave the **VLAN ID** and **Bandwidth Management** options unchecked and click **OK**.



Specify the configuration of the network adapter or remove the network adapter.

Virtual switch: Public-10.5.70

VLAN ID

□ Enable virtual LAN identification

The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.

2

Bandwidth Management

□ Enable bandwidth management

Specify how this network adapter utilizes network bandwidth. Both Minimum Bandwidth and Maximum Bandwidth are measured in Megabits per second.

Minimum bandwidth: 0 Mbps

Maximum bandwidth: 0 Mbps

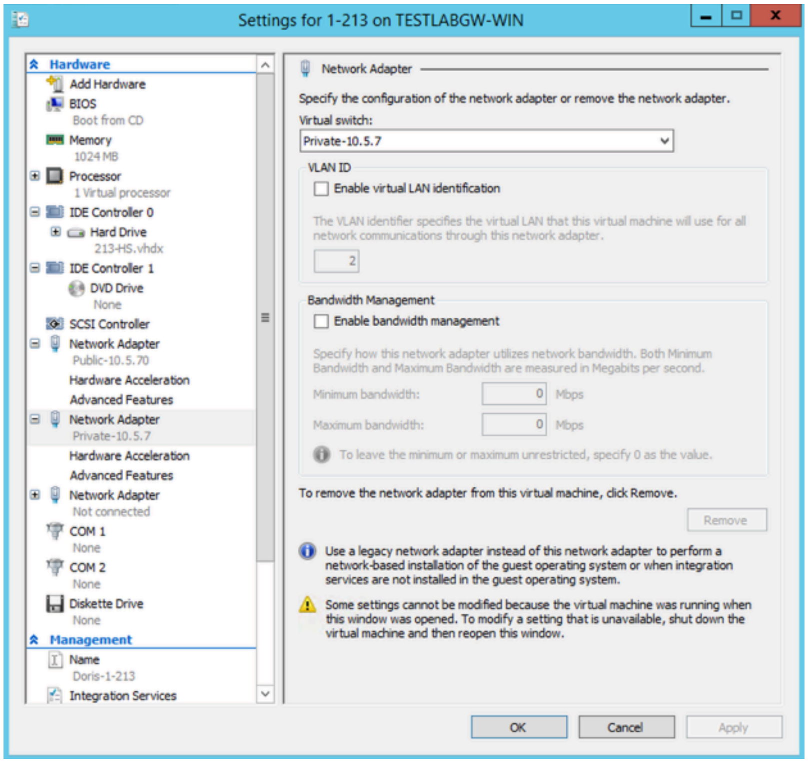
To leave the minimum or maximum unrestricted, specify 0 as the value.

To remove the network adapter from this virtual machine, click Remove.

Use a legacy network adapter instead of this network adapter to perform a network-based installation of the guest operating system or when integration services are not installed in the guest operating system.

Some settings cannot be modified because the virtual machine was running when this window was opened. To modify a setting that is unavailable, shut down the virtual machine and then reopen this window.

4. Return to **Add Hardware** and configure the second private adapter to connect to your overlay. Leave the **VLAN ID** and **Bandwidth Management** options unchecked and click **OK**.



Specify the configuration of the network adapter or remove the network adapter.

Virtual switch: Private-10.5.7

VLAN ID

□ Enable virtual LAN identification

The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.

2

Bandwidth Management

□ Enable bandwidth management

Specify how this network adapter utilizes network bandwidth. Both Minimum Bandwidth and Maximum Bandwidth are measured in Megabits per second.

Minimum bandwidth: 0 Mbps

Maximum bandwidth: 0 Mbps

To leave the minimum or maximum unrestricted, specify 0 as the value.

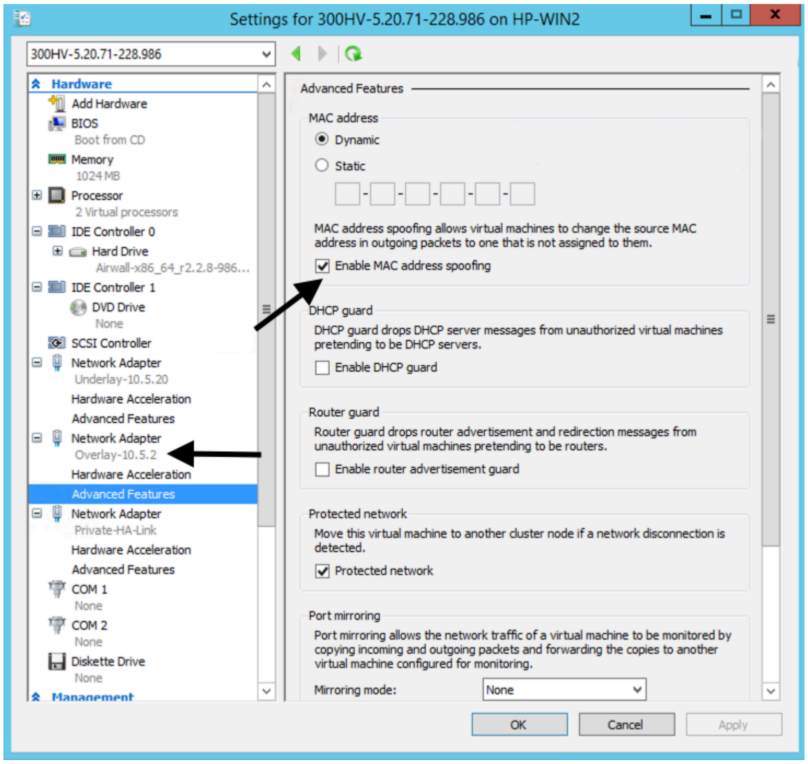
To remove the network adapter from this virtual machine, click Remove.

Use a legacy network adapter instead of this network adapter to perform a network-based installation of the guest operating system or when integration services are not installed in the guest operating system.

Some settings cannot be modified because the virtual machine was running when this window was opened. To modify a setting that is unavailable, shut down the virtual machine and then reopen this window.

Note: You can have up to two private isolated links. If you are using HA, you can create another adapter and set it to private. For more information on HA, see Airwall Edge Service High Availability (HA) on page 399.

5. Click the plus (next to the overlay Network Adapter, and select **Advanced Features**, and check **Enable MAC address spoofing**.



Settings for 300HV-5.20.71-228.986 on HP-WIN2

300HV-5.20.71-228.986

- Hardware
  - Add Hardware
  - BIOS
    Boot from CD
  - Memory
    1024 MB
  - Processor
    2 Virtual processors
  - IDE Controller 0
    - Hard Drive
      Airwall-x86_64_r2.2.8-986...
  - IDE Controller 1
    - DVD Drive
      None
  - SCSI Controller
  - Network Adapter
    Underlay-10.5.20
    - Hardware Acceleration
    - Advanced Features
  - Network Adapter
    Overlay-10.5.2
    - Hardware Acceleration
    - Advanced Features
  - Network Adapter
    Private-HA-Link
    - Hardware Acceleration
    - Advanced Features
  - COM 1
    None
  - COM 2
    None
  - Diskette Drive
    None
- Management

Advanced Features

MAC address

● Dynamic

○ Static

MAC address spoofing allows virtual machines to change the source MAC address in outgoing packets to one that is not assigned to them.

☑ Enable MAC address spoofing

DHCP guard

DHCP guard drops DHCP server messages from unauthorized virtual machines pretending to be DHCP servers.

□ Enable DHCP guard

Router guard

Router guard drops router advertisement and redirection messages from unauthorized virtual machines pretending to be routers.

□ Enable router advertisement guard

Protected network

Move this virtual machine to another cluster node if a network disconnection is detected.

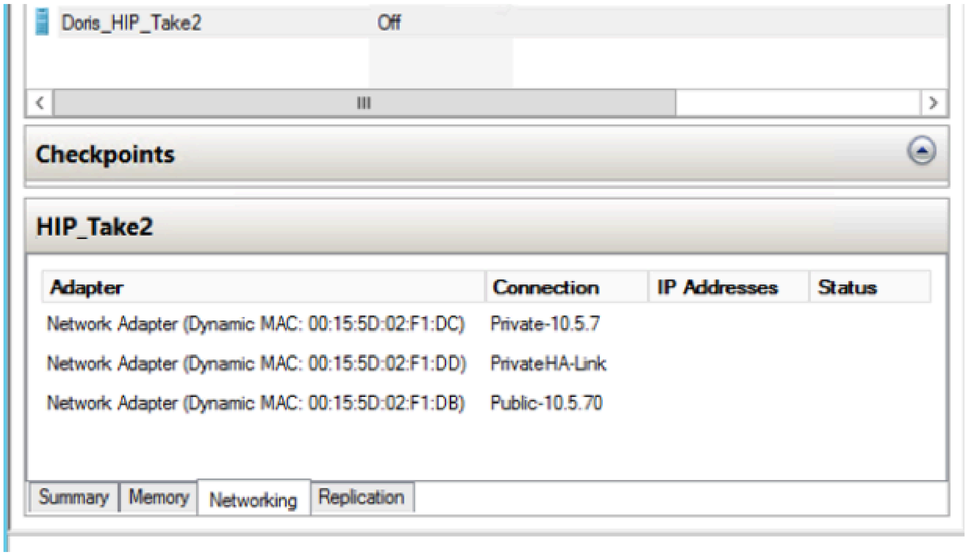
☑ Protected network

Port mirroring

Port mirroring allows the network traffic of a virtual machine to be monitored by copying incoming and outgoing packets and forwarding the copies to another virtual machine configured for monitoring.

Mirroring mode: None

6. Select the Airwall Gateway machine and open the **Networking** tab to review your settings. Your settings should be similar to this example:



Doris_HIP_Take2 Off

Checkpoints

HIP_Take2

Adapter	Connection	IP Addresses	Status
Network Adapter (Dynamic MAC: 00:15:5D:02:F1:DC)	Private-10.5.7		
Network Adapter (Dynamic MAC: 00:15:5D:02:F1:DD)	PrivateHA-Link		
Network Adapter (Dynamic MAC: 00:15:5D:02:F1:DB)	Public-10.5.70		

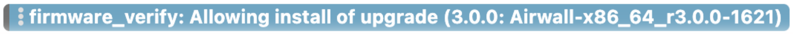
Configure the virtual Airwall Gateway

Connect your virtual Airwall Gateway to your Conductor and configure it.

1. In Hyper-V, select your virtual Airwall Gateway and then select **Action** > **Connect**.
2. Log in to Airshell.
3. Configure the Conductor and other settings. For more information, see Configure an Airwall Gateway with the airsh Setup Wizard on page 274.

Expand the Disk Size for a virtual Airwall Gateway

The v3.0 firmware for Airwall Gateways may require more disk space than you currently have allocated on your virtual machines. If so, you get an error message Under **Health data** > **Reporting** about the disk being too small when you try to update it:



firmware_verify: Allowing install of upgrade (3.0.0: Airwall-x86_64_r3.0.0-1621)

Important: If you are updating paired High Availability (HA) Airwall Gateways, expand and update the active first, then the standby.

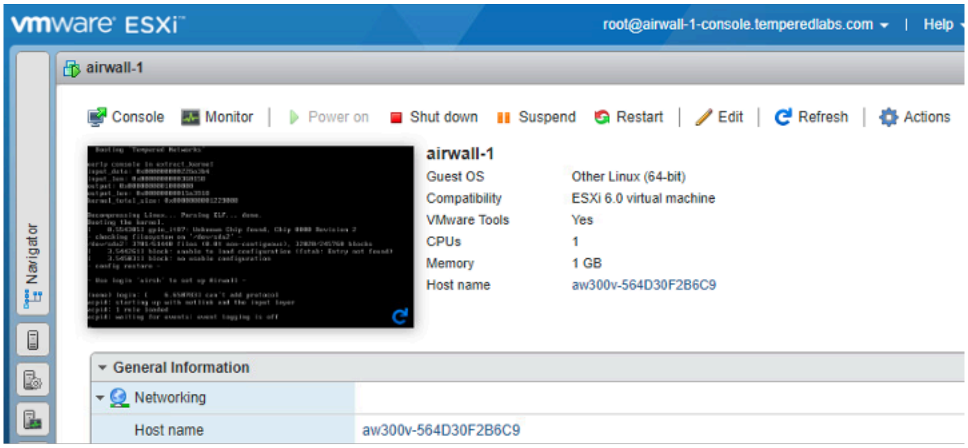
Before you begin

If you have checkpoints for the virtual machines you're expanding, you first need to either delete the checkpoints or clone the virtual machine. For more details on how, see the documentation for your virtual machine software.

Walkthrough – VMware ESXi

This walkthrough shows how to expand the disk size for a VMware ESXi virtual machine running an Airwall Gateway 300v on the VMware ESXi tool. For more details or updated instructions, see your virtual machine software instructions.

1. Open the VMware ESXi Tool, and select the virtual machine that hosts the Airwall Gateway you want to expand.
2. Select **Shut down** to shut down the virtual machine.

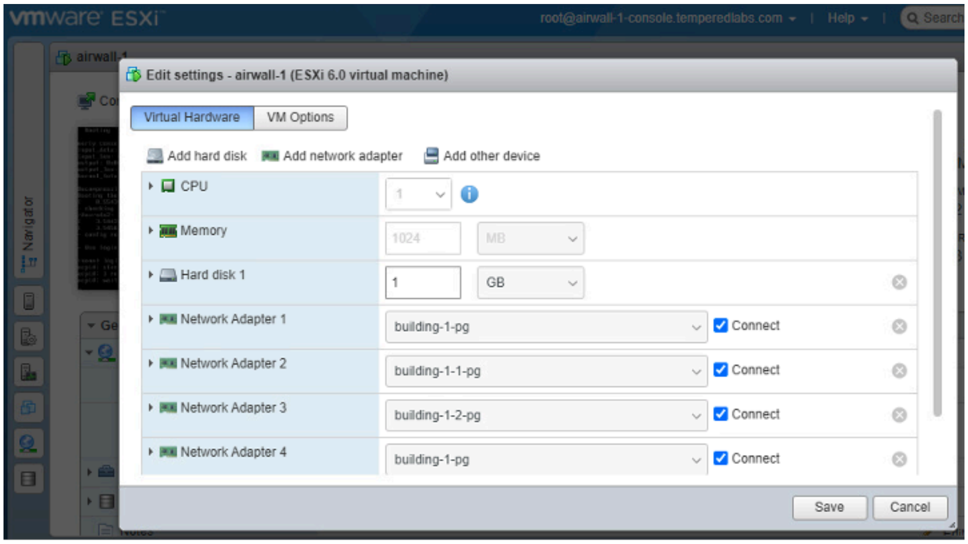


airwall-1

Guest OS	Other Linux (64-bit)
Compatibility	ESXi 6.0 virtual machine
VMware Tools	Yes
CPUs	1
Memory	1 GB
Host name	aw300v-564D30F2B6C9

Host name aw300v-564D30F2B6C9

3. Select Edit.
4. Next to **Hard disk 1**, change the size to 1 GB, and select **Save**.



CPU	1	
Memory	1024 MB	
Hard disk 1	1 GB	
Network Adapter 1	building-1-pg	☑ Connect
Network Adapter 2	building-1-1-pg	☑ Connect
Network Adapter 3	building-1-2-pg	☑ Connect
Network Adapter 4	building-1-pg	☑ Connect

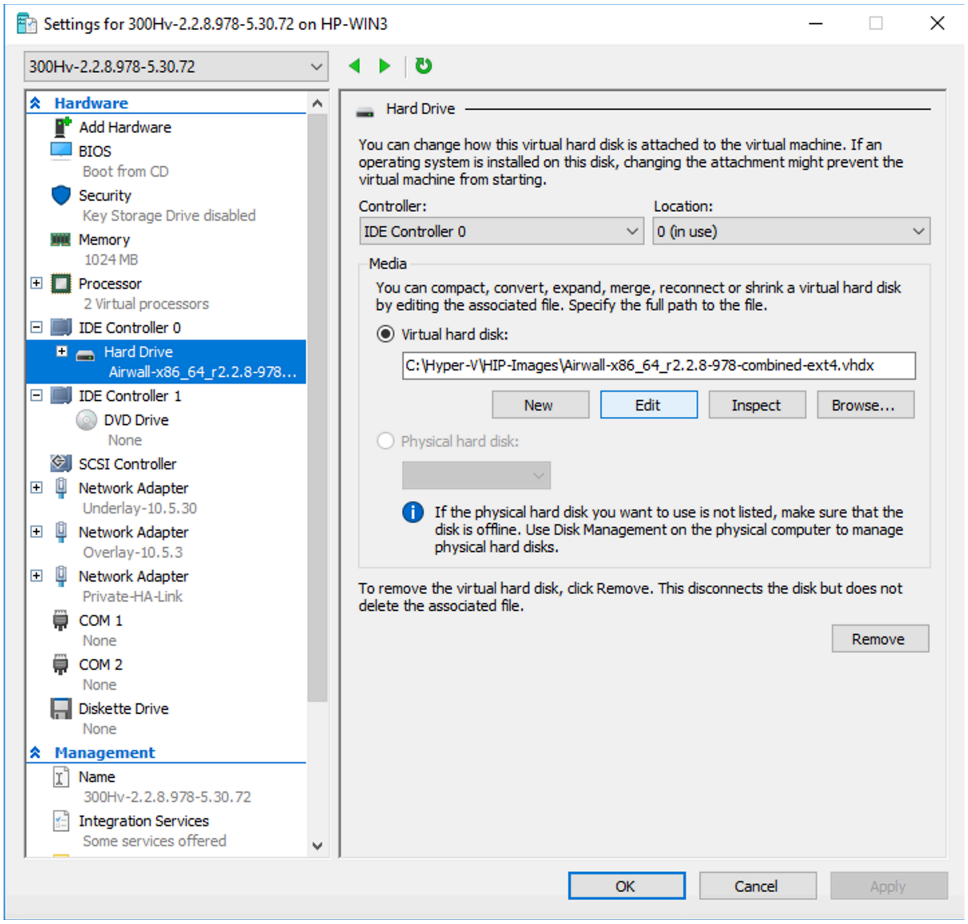
5. Back on the main page, select **Power on** to restart the virtual machine.

You should now be able to update the firmware for the Airwall Gateway. For help updating firmware, see Update Airwall Gateway firmware on page 128.

Walkthrough on Hyper-V

This walkthrough shows how to expand the disk size for a Hyper-V virtual machine running an Airwall Gateway 300v on the Hyper-V Manager v10. For more details or updated instructions, see your virtual machine software instructions.

1. Open the Hyper-V Manager, and select the virtual machine that hosts the Airwall Gateway you want to expand.
2. Check that the virtual machine has no checkpoints. If it does, delete them or clone the machine to continue.
3. Under the actions for the virtual machine, select **Turn Off**, and confirm.
4. Select **Settings**.
5. Under **Hardware** on the left, select **Hard Drive**.
6. On the right, under **Media**, select **Edit**.



Settings for 300Hv-2.2.8.978-5.30.72 on HP-WIN3

300Hv-2.2.8.978-5.30.72

Hardware
- Add Hardware
- BIOS: Boot from CD
- Security: Key Storage Drive disabled
- Memory: 1024 MB
- Processor: 2 Virtual processors
- IDE Controller 0
  - Hard Drive: Airwall-x86_64_r2.2.8-978...
- IDE Controller 1
  - DVD Drive: None
- SCSI Controller
- Network Adapter: Underlay-10.5.30
- Network Adapter: Overlay-10.5.3
- Network Adapter: Private-HA-Link
- COM 1: None
- COM 2: None
- Diskette Drive: None

Management
- Name: 300Hv-2.2.8.978-5.30.72
- Integration Services: Some services offered

Hard Drive

You can change how this virtual hard disk is attached to the virtual machine. If an operating system is installed on this disk, changing the attachment might prevent the virtual machine from starting.

Controller: IDE Controller 0

Location: 0 (in use)

Media

You can compact, convert, expand, merge, reconnect or shrink a virtual hard disk by editing the associated file. Specify the full path to the file.

● Virtual hard disk:

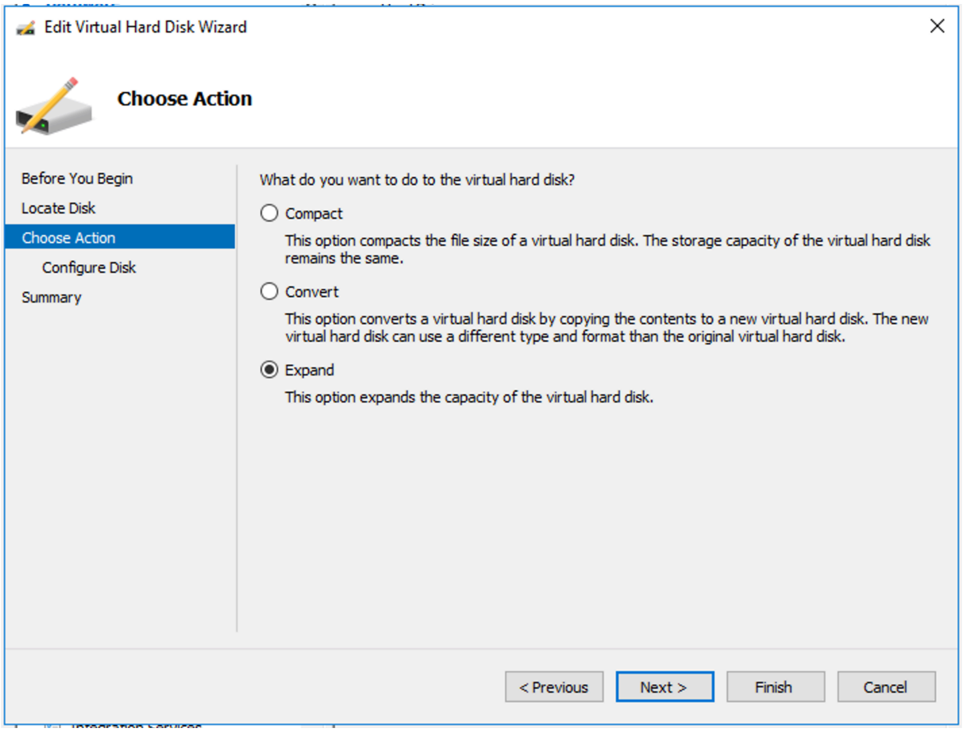
C:\Hyper-V\HIP-Images\Airwall-x86_64_r2.2.8-978-combined-ext4.vhdx

○ Physical hard disk:

If the physical hard disk you want to use is not listed, make sure that the disk is offline. Use Disk Management on the physical computer to manage physical hard disks.

To remove the virtual hard disk, click Remove. This disconnects the disk but does not delete the associated file.

7. On the **Locate Virtual Hard Disk** page, the correct one should already be selected. Select **Next**.
8. On the **Choose Action** page, select **Expand**, and then select **Next**.



What do you want to do to the virtual hard disk?

○ Compact

This option compacts the file size of a virtual hard disk. The storage capacity of the virtual hard disk remains the same.

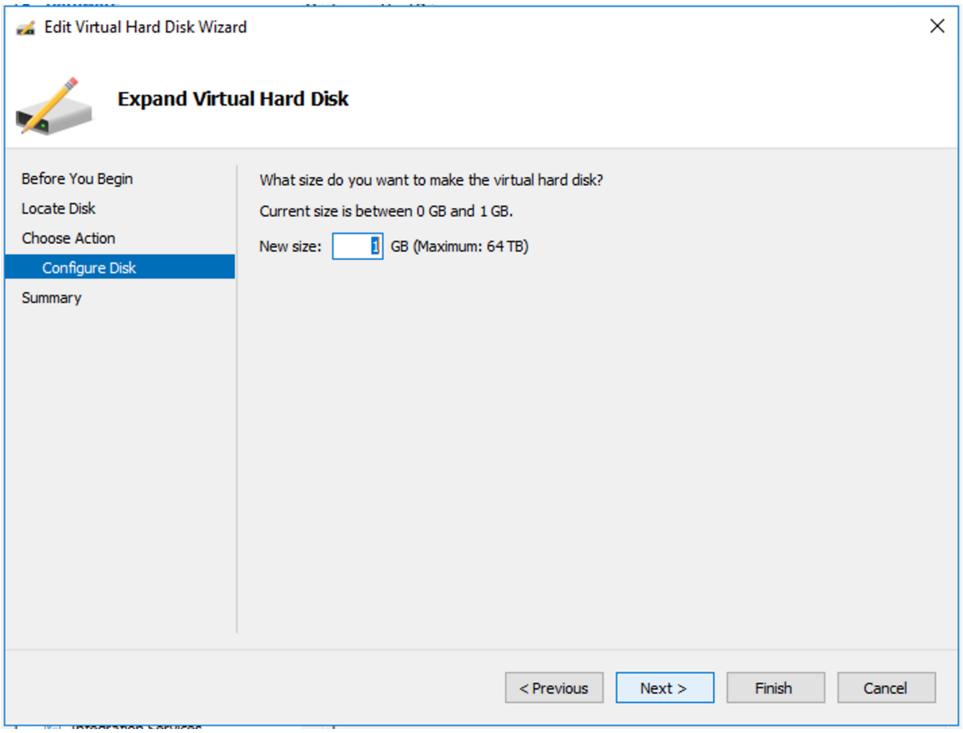
○ Convert

This option converts a virtual hard disk by copying the contents to a new virtual hard disk. The new virtual hard disk can use a different type and format than the original virtual hard disk.

● Expand

This option expands the capacity of the virtual hard disk.

9. On the **Expand Virtual Hard Disk** page, select `1 GB`, and select **Finish**.



What size do you want to make the virtual hard disk?

Current size is between 0 GB and 1 GB.

New size: 1 GB (Maximum: 64 TB)

10. Back on the main page, restart the virtual machine by selecting **Start** from the lower right menu.

You should now be able to update the firmware for the Airwall Gateway. For help updating firmware, see Update Airwall Gateway firmware on page 128.

Set up cloud Airwall Gateways

A cloud-based Airwall Gateway provides host-to-host peering between Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), or Alibaba Cloud, and on-premises assets and simplifies the process of managing them.

While you can set up cloud-based Airwall Gateways directly in your cloud platform, the Conductor provides an easy to use user interface for deploying Airwall Gateways in the cloud. Use the links below to view the instructions for each supported platform.

This content assumes you have a good working knowledge of your network and the services you are deploying on. For example, if you plan to deploy an Airwall Gateway in a cloud environment, such as Amazon Web Services (AWS), you should be familiar with the basics of AWS.

Related tasks

Manage Cloud Airwall Gateway Virtual Machines on page 98
You can do several management tasks for the virtual machines that host cloud Airwall Gateways from the Conductor.

Alibaba Cloud – Set up an Airwall Gateway
Once you've set up the Conductor to create Airwall Gateways on Alibaba Cloud, it's easy to create additional Airwall Gateways.

Prerequisites

Required licenses	An Airwall 300v license for each virtual Airwall Gateway you are setting up.
Supported versions	Conductor v2.2.8 and later

To deploy a cloud Airwall Gateway on Alibaba Cloud, you need the following:

- An Alibaba Cloud account, and your access and secret keys.
- The address and port of your Conductor.
- One or more Airwall Gateway image files (from the Alibaba Cloud marketplace, or from Tempered Fulfillment uploaded to the Alibaba Cloud console).

Deploy an Airwall Gateway on Alibaba Cloud

Here's how to deploy an Airwall Gateway to your Alibaba Cloud account:

- Step 1: Add Alibaba Cloud as a provider to your Conductor on page 315
- Step 2: Create an Airwall Gateway template on Alibaba Cloud on page 317
- Step 3: Deploy Airwall Gateways on Alibaba Cloud on page 318
- Step 4: (Optional) Change your Elastic IP Bandwidth Setting on page 320

Step 1: Add Alibaba Cloud as a provider to your Conductor
Set up Alibaba Cloud as a cloud provider in your Conductor to make deploying cloud Airwall Gateways and High-availability standby Conductor easier.

To add Alibaba Cloud as a provider, you need to:

- Get Alibaba Cloud Access Key credentials
- Set up Alibaba Cloud as a cloud provider in the Conductor

Get Alibaba Cloud Access Key credentials

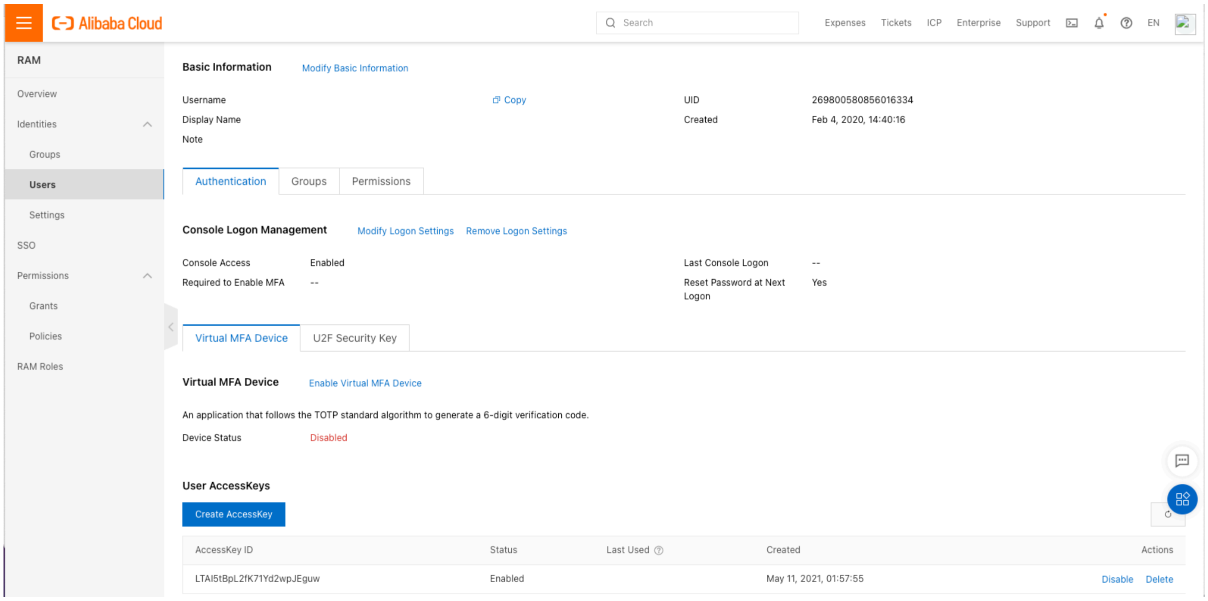
Alibaba Cloud accounts and RAM users have identities. Alibaba Cloud services use credentials for authentication.

For example, Alibaba Cloud services use passwords for authentication when you log on to a console. In this case, your email and password are the credentials.

Alibaba Cloud uses AccessKey pairs for authentication when you make API calls. An AccessKey pair consists of an AccessKey ID and an AccessKey secret. For the most up-to-date instructions, see Alibaba Cloud API overview - Alibaba Cloud API overview| Alibaba Cloud Documentation Center

1. Create or go to your Alibaba Cloud RAM account. For details, see Create a RAM user - Getting Started| Alibaba Cloud Documentation Center, or the most recent content from Alibaba Cloud.
2. To get your Alibaba Cloud AccessKey pair, in Alibaba Cloud go to the RAM console.

3. Under **Users**, scroll down to **User AccessKeys**. Create a new Access Key by selecting **Create AccessKey**.



Basic Information Modify Basic Information

Username	Copy	UID	269800580856016334
Display Name		Created	Feb 4, 2020, 14:40:16
Note			

Console Logon Management Modify Logon Settings Remove Logon Settings

Console Access	Enabled	Last Console Logon	--
Required to Enable MFA	--	Reset Password at Next Logon	Yes

Virtual MFA Device Enable Virtual MFA Device

An application that follows the TOTP standard algorithm to generate a 6-digit verification code.

Device Status Disabled

User AccessKeys

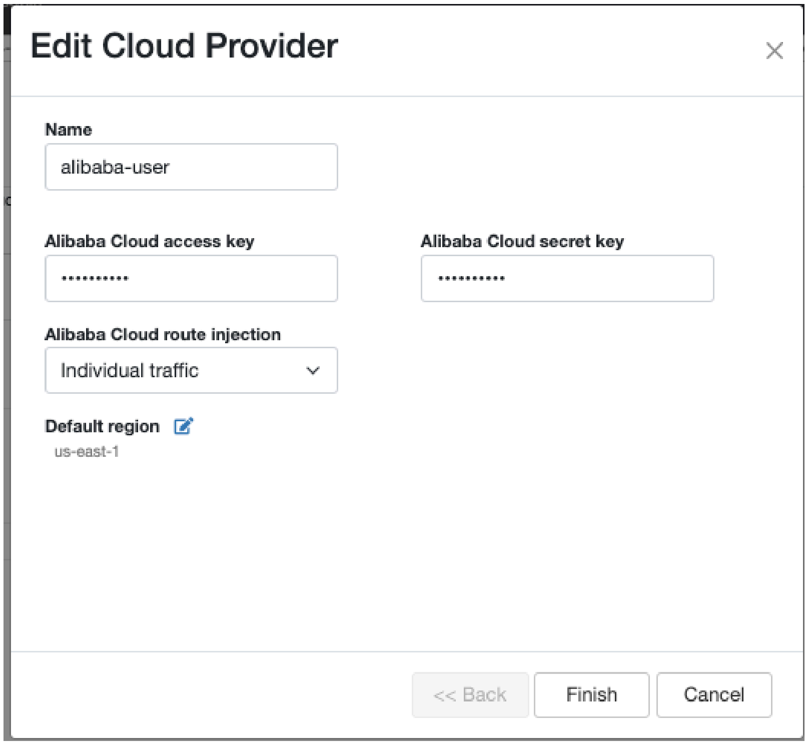
AccessKey ID	Status	Last Used	Created	Actions
LTAI5tBpL2fK71Yd2wpJEguw	Enabled		May 11, 2021, 01:57:55	Disable Delete

4. Note down your AccessKey ID and secret.

Once you have your ID and secret, you'll use them in the next step to add Alibaba Cloud as a cloud provider in the Conductor.

Set up Alibaba Cloud as a cloud provider

1. In the Conductor, select the gear icon in the upper-right to access the **Settings** page.
2. Select the **Cloud providers** tab and click **+ Add Cloud Providers.**
3. In the **Add Cloud Providers.** dialog, select the check-mark to the right of **Alibaba Cloud** and click **Next**
4. Enter your **Alibaba Cloud access** and **secret keys**, and choose an option for **Alibaba Cloud route injection**.



Name: alibaba-user

Alibaba Cloud access key: ••••••••••

Alibaba Cloud secret key: ••••••••••

Alibaba Cloud route injection: Individual traffic

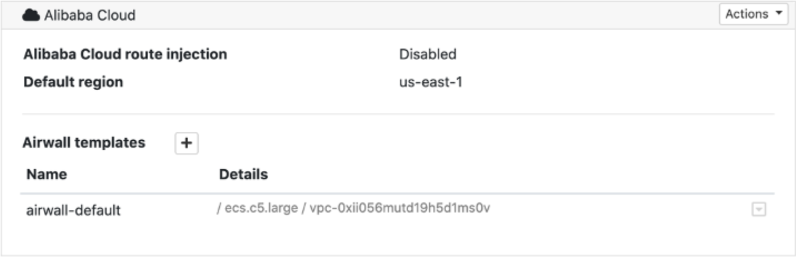
Default region: us-east-1

5. The **Alibaba Cloud route injection** setting determines how new routes are added to the Alibaba Cloud routing table. The routes are for traffic on your protected overlay network between protected devices and the Airwall Gateway. Here are the recommended settings depending on your deployment details:

    - If you are using a Airwall Relay, set to **Disabled**.
    - If you want to handle traffic for devices individually, set to **Individual traffic**.
    - If you want one route to send all traffic to the overlay port on the Airwall Gateway, set to **All traffic**.

    Note: All traffic is effectively 'full tunnel' mode. With Individual traffic, you could add routes that send traffic around the Airwall Gateway.
6. By **Default region**, select the Refresh icon to get the list of regions from the provider, and then select your default region.
7. Click **Finish**

    Your Alibaba Cloud provider is displayed in the **Configured Cloud Providers** list.



Alibaba Cloud route injection	Disabled
Default region	us-east-1

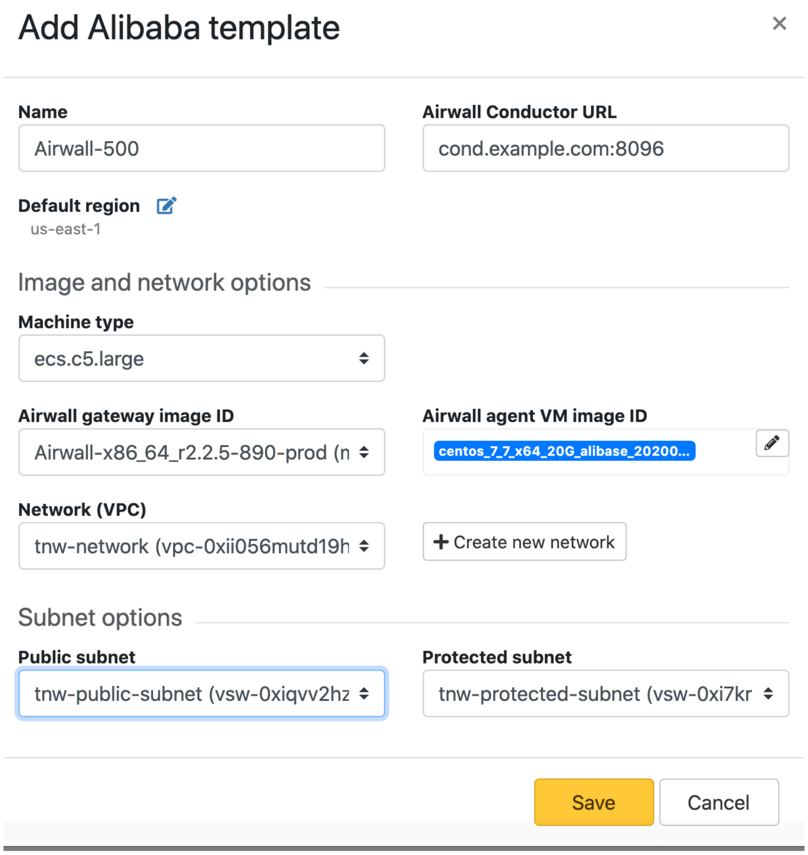
Airwall templates

Name	Details
airwall-default	/ ecs.c5.large / vpc-0xii056mutd19h5d1ms0v

Step 2: Create an Airwall Gateway template on Alibaba Cloud

1. In the Conductor, select the gear icon in the upper-right to access the **Settings** page, and go to the **Cloud providers** tab.
2. In the **Configured Cloud Providers** list, under **Alibaba Cloud**, select the + next to **Airwall templates**.
3. Give your template a descriptive name, and then select the **Image and network options** you want for Airwall Gateways created with this template.

    Note: To select subnets, you need to select a **Network (VPC)** first.



Add Alibaba template

Name: Airwall-500

Airwall Conductor URL: cond.example.com:8096

Default region: us-east-1

Image and network options

Machine type: ecs.c5.large

Airwall gateway image ID: Airwall-x86_64_r2.2.5-890-prod (n

Airwall agent VM image ID: centos_7_7_x64_20G_alibase_20200...

Network (VPC): tnw-network (vpc-0xii056mutd19h

Subnet options

Public subnet: tnw-public-subnet (vsw-0xiqvv2hz

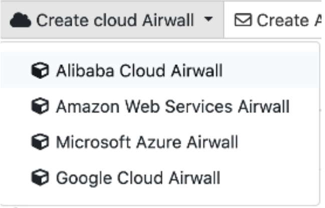
Protected subnet: tnw-protected-subnet (vsw-0xi7kr

4. Select **Save**

Step 3: Deploy Airwall Gateways on Alibaba Cloud

You must Set up Alibaba Cloud as a cloud provider on page 439 before you can add an Airwall Gateway in the Conductor

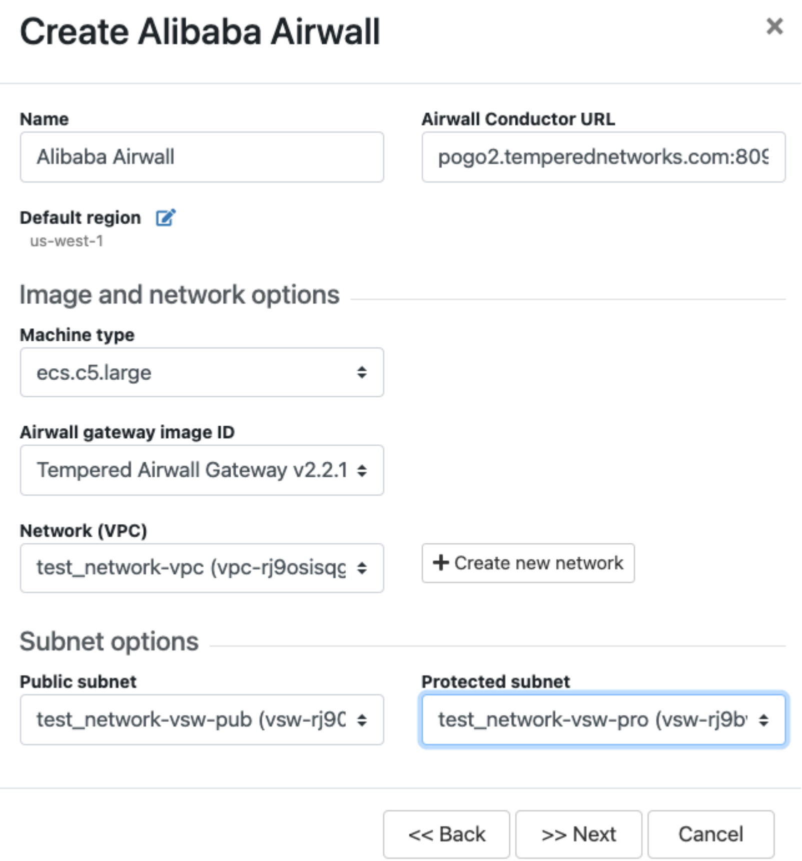
1. On the **Airwalls** page, (or in Conductor **Settings**, under **Cloud providers**), click **Create cloud Airwall**, and select **Alibaba Cloud Airwall**.



2. In v2.2.8 and later, select the type of Airwall to create, and select **Next**.
3. In v2.2.8 and later, **if you want to use a template** to create the Airwall Gateway, select the template, select **Next**, and then give the Airwall Gateway a descriptive name. You can then skip to the next step.

   To continue without a template and enter the information manually, just select **Next**.

   a) If you are filling in information manually, or want to change the template, fill in the **Name** and **Image and network options** for this Airwall Gateway. For **Machine type**, the default typically works. You can select a different size if needed for your purposes.



Create Alibaba Airwall

Name: Alibaba Airwall

Airwall Conductor URL: pogo2.temperednetworks.com:809

Default region: us-west-1

Image and network options

Machine type: ecs.c5.large

Airwall gateway image ID: Tempered Airwall Gateway v2.2.1

Network (VPC): test_network-vpc (vpc-rj9osisqg

Subnet options

Public subnet: test_network-vsw-pub (vsw-rj9C

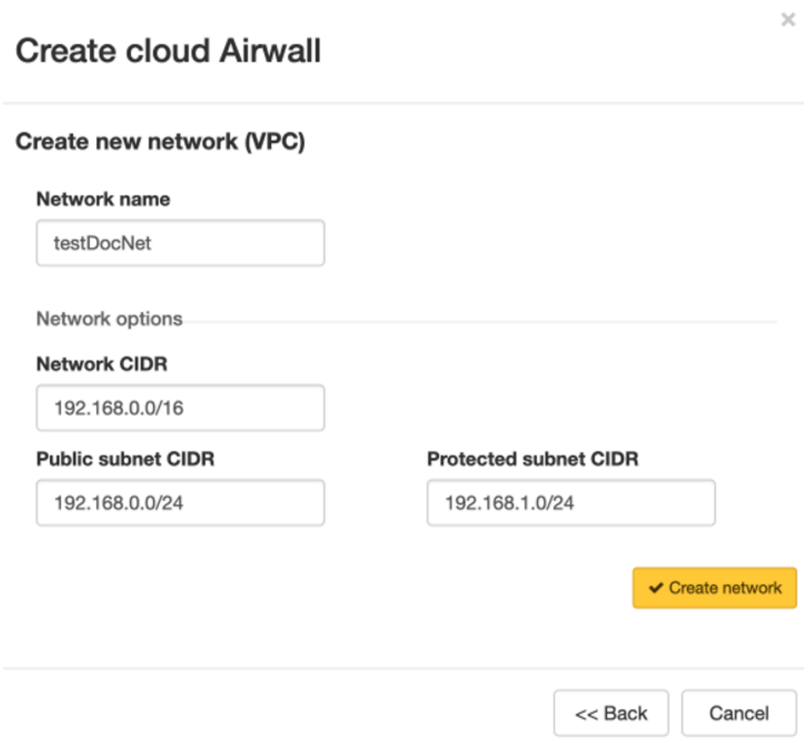
Protected subnet: test_network-vsw-pro (vsw-rj9b

b) Under **Airwall gateway image ID**, pick the Airwall Gateway image you want to use. The list shows the Airwall Gateway images available on your cloud provider.

c) If you do not have a pre-configured virtual network, you need to create a new network. Click **Create new network** and fill in the form:

- **Network CIDR** – Enter an available network address and subnet mask in CIDR notation.
- **Public subnet CIDR** – Must be a subnet of the main network. Traffic flows between the underlay interface of the Airwall Gateway and the Public IP address object in Azure.
- **Protected subnet CIDR** – Must be a subnet of the main network. Traffic must pass through theAirwall Gateway or through manually-crafted routes.

When you're finished entering the information, click **Create network**, and when processing is complete, click **Back**.



Create cloud Airwall

Create new network (VPC)

Network name: testDocNet

Network options

Network CIDR: 192.168.0.0/16

Public subnet CIDR: 192.168.0.0/24

Protected subnet CIDR: 192.168.1.0/24

d) Back on the **Create cloud Airwall** page, select the network and public and protected subnets you just created.

4. Click **Next**.
5. Check the summary. If everything is correct, click **Create cloud Airwall**.
6. Click **Finish**. It may take up to 5 minutes for Alibaba Cloud to create the Airwall Gateway.

You've completed creating an Airwall Gateway on Alibaba Cloud, and now need to provision, License, and configure it. For help, see Provision and License Airwall Edge Services on page 193 and Configure Airwall Edge Service Settings on page 359.

Step 4: (Optional) Change your Elastic IP Bandwidth Setting

The Airwall Gateway images on Alibaba Cloud use the following default values for elastic IP:

- **Bandwidth**: 5 Mbps
- **InternetChargeType**: PayByTraffic
- **InstanceChargeType**: Postpaid (Pay-As-You-Go)

You can change the bandwidth value once the Airwall Gateway is deployed, however be aware that the bandwidth rate may increase when you edit this value. For more information on how to change the bandwidth, see Alibaba help.

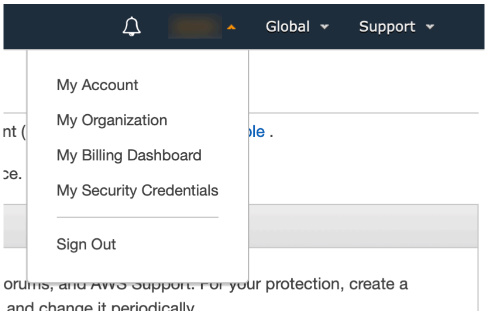
Amazon Web Services – Set up an Airwall Gateway

Prerequisites

Required licenses	An Airwall 300v license for each virtual Airwall Gateway you are setting up.
Supported versions	Conductor v2.2.3 and later

To deploy a cloud Airwall Gateway on Amazon Web Services (AWS) you need the following:

- An AWS access key ID and secret access key pair to create the AWS cloud provider. If you do not already have a key pair created in your AWS account, you need to create one as follows: Click your username and select **My Security Credentials** in the drop-down.



For more information about access keys, see AWS Security Credentials in the AWS documentation.

Note: If you create an access key in your AWS root account, you can only retrieve the secret key portion when you create it. If you anticipate using the same key at a later date, we recommend you create an IAM user with access to your security keys instead of relying on root access keys.

- The address and port of your Conductor.
- An Airwall Gateway AMI, shared to your account by Tempered Fulfillment when you purchased your AWS Airwall Gateway.

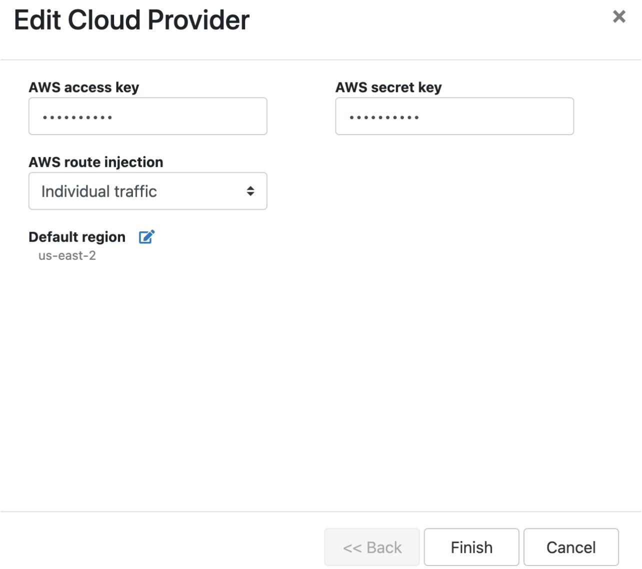
Set up an Airwall Gateway on AWS

There are three steps required to deploy an Airwall Gateway to your AWS account:

1. Add the AWS provider to your Conductor as a cloud provider
2. Create an Airwall Gateway deployment template
3. Deploy one or more Airwall Gateways using the template

Set up AWS as a cloud provider

1. In the Conductor, select the gear icon in the upper-right to access the **Settings** page.
2. Select the **Cloud providers** tab and click **+ Add Cloud Providers**
3. In the **Add Cloud Provider** dialog, select the check-mark to the right of **Amazon Web Services** and click **Next**
4. Enter your **AWS access key**, **AWS secret key**, and **Default region**


Edit Cloud Provider

AWS access key: ••••••••••

AWS secret key: ••••••••••

AWS route injection: Individual traffic

Default region: us-east-2

5. The **AWS route injection** setting determines how new routes are added to the AWS routing table. The routes are for traffic on your protected overlay network between protected devices and the Airwall Gateway. Here are the recommended settings depending on your deployment details:

   - If you are using a Airwall Relay, or want to manage routes on your own, set to **Disabled**.

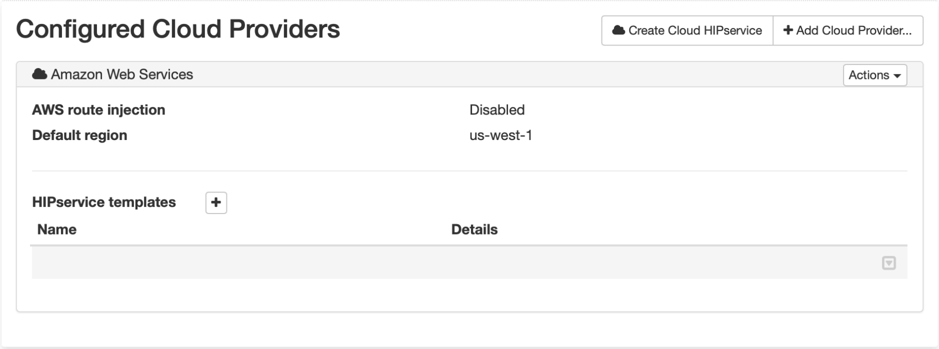
Important: If your Airwall's subnet has a route table with existing or planned future routes, then do not set route injection to **Individual traffic** or **All traffic**. This removes these existing and future routes from the route table, retaining only routes created by Conductor.

- If you want to handle traffic for devices individually, set to **Individual traffic**.
- If you want one route to send all traffic to the overlay port on the Airwall Gateway, set to **All traffic**.

Note: All traffic is effectively 'full tunnel' mode. With Individual traffic, you could add routes that send traffic around the Airwall Gateway.

6. Click **Finish**

Your AWS cloud provider is displayed in the **Configured Cloud Providers** list.



AWS route injection	Disabled
Default region	us-west-1

Name	Details

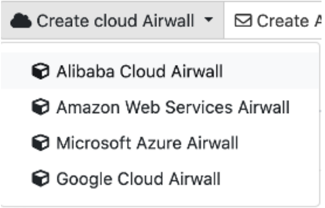
Create an Airwall Gateway deployment template in AWS

In AWS, create an Airwall Gateway deployment template.

Add an AWS Airwall Gateway

You must Set up Amazon Web Services (AWS) as a cloud provider on page 433 before you can add an Airwall Gateway in the Conductor

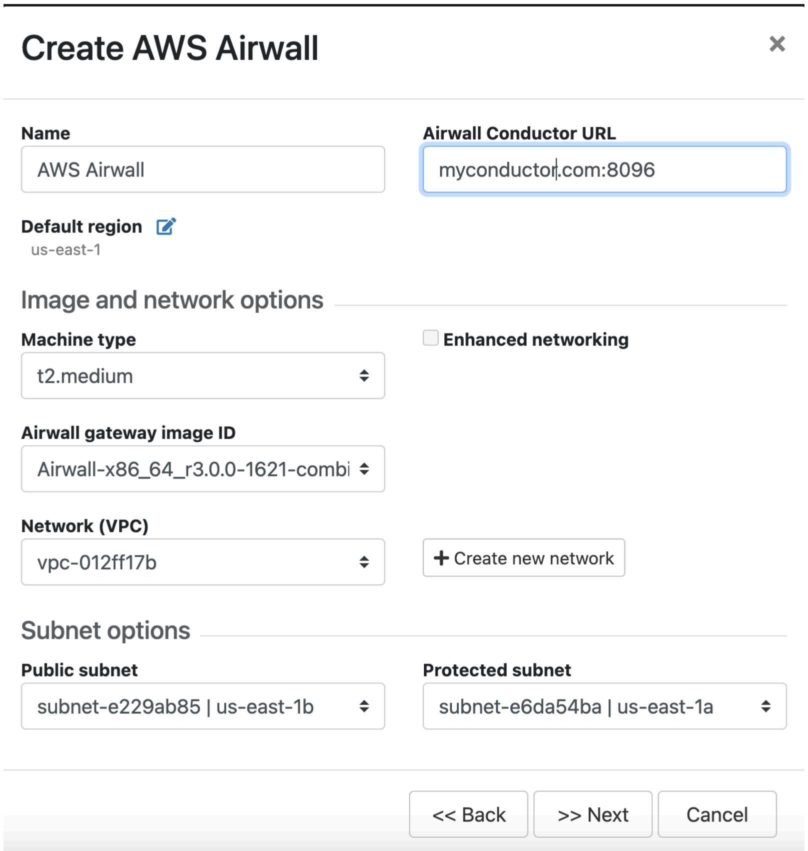
1. On the **Airwalls** page, (or in Conductor **Settings** under **Cloud providers** tab), select **New cloud Airwall**, and then select **Amazon Web Services Airwall**.



2. In v2.2.8 and later, select the type of Airwall to create, and select **Next**.
3. In v2.2.8 and later, **if you want to use a template** to create the Airwall Gateway, select the template, select **Next**, and then give the Airwall Gateway a descriptive name. You can then skip to the next step.

   To continue without a template and enter the information manually, just select **Next**.

   a) If you are filling in information manually, or want to change the template, fill in the **Name** and **Image and network options** for this Airwall Gateway. For **Machine type**, the default typically works. You can select a different size if needed for your purposes.



Create AWS Airwall

Name: AWS Airwall

Airwall Conductor URL: myconductor.com:8096

Default region: us-east-1

Image and network options

Machine type: t2.medium

□ Enhanced networking

Airwall gateway image ID: Airwall-x86_64_r3.0.0-1621-combi

Network (VPC): vpc-012ff17b

Subnet options

Public subnet: subnet-e229ab85 | us-east-1b

Protected subnet: subnet-e6da54ba | us-east-1a

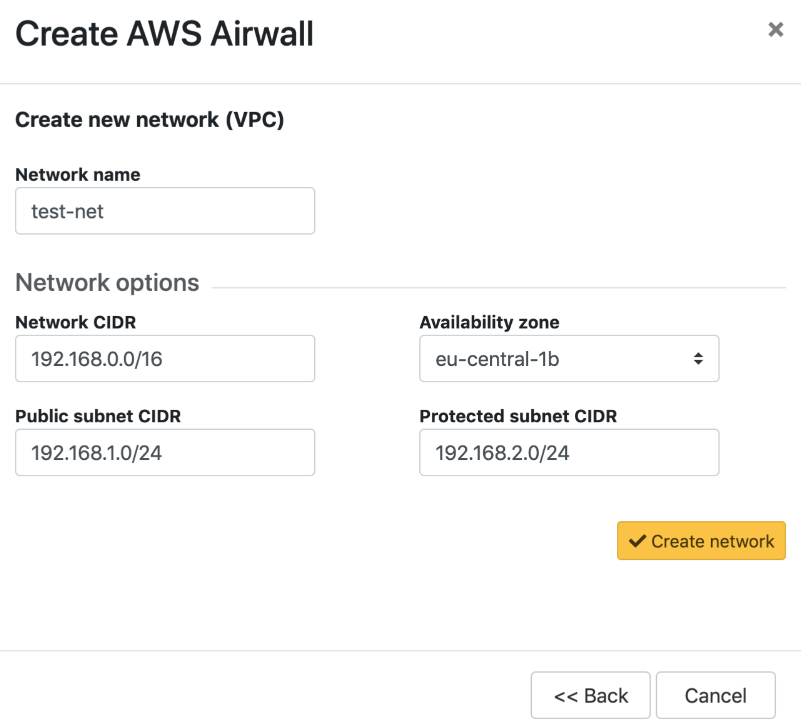
b) Under **Airwall gateway image ID**, pick the Airwall Gateway image you want to use. The list shows the Airwall Gateway images Tempered shared with your account.

Note: If you are not seeing the Airwall Gateway images, check your order email.

c) If you do not have a pre-configured virtual network, you need to create a new network. Select **Create new network** and fill in the form:

- **Network CIDR** – Enter an available network address and subnet mask in CIDR notation.
- **Public subnet CIDR** – Must be a subnet of the main network. Traffic flows between the underlay interface of the Airwall Gateway and the Public IP address object in AWS.
- **Protected subnet CIDR** – Must be a subnet of the main network. Traffic must pass through theAirwall Gateway or through manually-crafted routes.

When you're finished entering the information, select **Create network**, and when processing is complete, select **Back**.



Create AWS Airwall

Create new network (VPC)

Network name: test-net

Network options

Network CIDR: 192.168.0.0/16

Availability zone: eu-central-1b

Public subnet CIDR: 192.168.1.0/24

Protected subnet CIDR: 192.168.2.0/24

d) Back on the **Create cloud Airwall** page, select the network and public and protected subnets you just created.

4. Check the summary and if everything is correct, select **Create cloud Airwall**.
5. Select **Finish**. It may take up to 5 minutes for Amazon Web Services to complete creating the Airwall Gateway.

You've completed creating an AWS cloud Airwall Gateway, and now need to configure Provision, License, and configure it. For help, see Provision and License Airwall Edge Services on page 193 and Configure Airwall Edge Service Settings on page 359.

Microsoft Azure – Set up an Airwall Gateway

You can configure cloud Airwall Gateways on Azure from your Conductor.

Prerequisites

Required licenses	An Airwall 300v license for each virtual Airwall Gateway you are setting up.
Supported versions	Conductor v2.2.3 and later

Before you start, you need

- Access to a Microsoft Azure account with billing set up. If you do not have an account, you can create a free Microsoft Azure account and upgrade it to a full account later.
- Set up and license an Airwall Conductor.

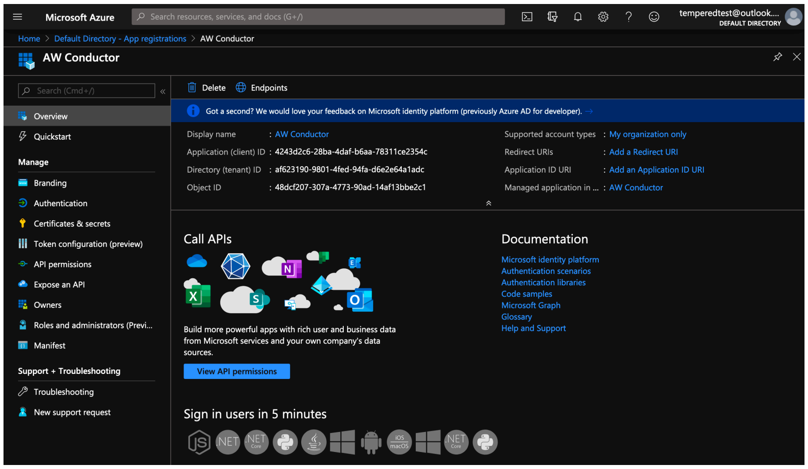
Create an Azure Application to connect to the Airwall Conductor

Check your Azure documentation for the most recent instructions on creating an application.

1. In Azure, in **Active directory**, under **App registrations**, register or choose an application to act as Airwall API endpoint.
2. In the Azure application, in Certificates & secrets, create a new client secret for the app to connect to Conductor. Copy it to a secure location.

   Important: You must copy the new client secret value at this step, because you won't be able to retrieve the key later.
3. From the Azure application you created, note the following information:

- Azure **Application ID** – Get from the Azure application Overview page.
- Azure **Application key** – The client secret you noted above.
- Azure **Subscription ID** – In Azure, under **Users**, get the subscription details to find the ID. It's also at the top of your **Powershell** window.
- Directory ID – Get **Directory (tenant) ID** from the Azure application Overview page.



Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Display name : AW Conductor
Application (client) ID : 4243d2c6-28ba-4daf-b6aa-78311ce2354c
Directory (tenant) ID : af623190-9801-4fed-94fa-d6e2e64a1adc
Object ID : 48dcf207-307a-4773-90ad-14af13bbe2c1

Supported account types : My organization only
Redirect URIs : Add a Redirect URI
Application ID URI : Add an Application ID URI
Managed application in ... : AW Conductor

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

4. Set up a role for the application you created to use as authorization to create Airwall Gateways in your Azure environment.
   a) From **Subscriptions**, select your subscription, and then select **Access control (IAM)**.
   b) Add a role assignment, and assign the App you created to the role: For **Role**, select **Contributor**, and for **Assign access to**, select **User, group, or service principal**, and then search for your App. You can also select a custom role with the permissions you want. For more information, see Azure help: Create a role in the Azure portal.

Accept Azure Terms for the Airwall Gateway Images

Before you can create Airwall Gateways in the Conductor, you'll need to accept terms on Azure for the versions of the Airwall Gateway that you plan to deploy. You only have to accept terms in your current Azure subscription once for each version.

1. In Azure, open **Powershell**.
2. Enter the following command, changing the `-urn` value to the images for the Airwall Gateways you're trying to deploy. For example:

```
az vm image terms accept --urn tempered-networks-inc:tempered-airwall-
v3:tempered-airwall-byol-v300:3.0.0
```

You can get the value you need for `-urn` in the Conductor from the summary page when you are creating the cloud Airwall Gateway. Copy the value for Airwall image ID, and then change the forward slashes to colons. For example, if the drop down list shows an image id of `tempered-networks-inc/tempered-airwall-v3/tempered-airwall-byol-v300/3.0.0`, edit for the `--urn` to `tempered-networks-inc:tempered-airwall-v3:tempered-airwall-byol-v300:3.0.0`.

Add Azure as a Cloud Provider in Conductor

1. In Conductor **Settings**, open the **Cloud providers** tab.
2. Under **Configured cloud providers**, click **Add cloud provider**, and then select **MS Azure**.
3. Fill in the form, using the values noted when creating an application in Azure:

- **Application ID** – Enter the Azure **Application ID**.
- **Client secret** – Enter the Azure **Application key**.
- **Subscription ID** – Enter the Azure **Subscription ID**.

- **Tenant ID** – Enter the **Directory (tenant) ID**.

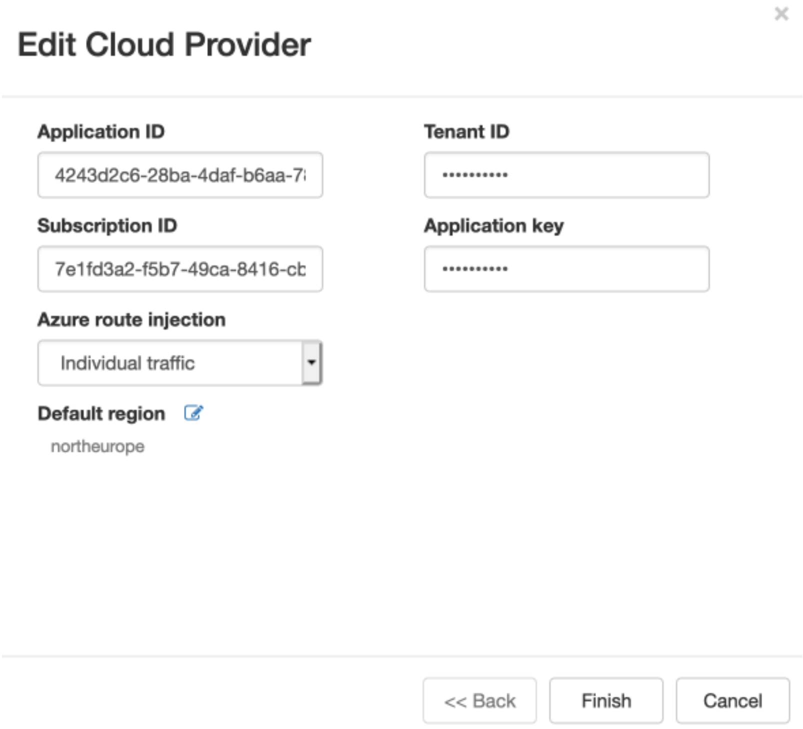
4. The **Azure route injection** setting determines how new routes are added to the Azure routing table. The routes are for traffic on your protected overlay network between protected devices and the Airwall Gateway. Here are the recommended settings depending on your deployment details:

   - If you are using a Airwall Relay, or want to manage routes on your own, set to **Disabled**.

     Important: If your Airwall's subnet has a route table with existing or planned future routes, then do not set route injection to **Individual traffic** or **All traffic**. This removes these existing and future routes from the route table, retaining only routes created by Conductor.
   - If you want to handle traffic for devices individually, set to **Individual traffic**.
   - If you want one route to send all traffic to the overlay port on the Airwall Gateway, set to **All traffic**.

     Note: All traffic is effectively 'full tunnel' mode. With Individual traffic, you could add routes that send traffic around the Airwall Gateway.

5. For **Default region**, click the **Sync** icon to check the connection and fill in your options. When it connects, select your default region from the list.



Edit Cloud Provider

Application ID: 4243d2c6-28ba-4daf-b6aa-7

Tenant ID: ••••••••••

Subscription ID: 7e1fd3a2-f5b7-49ca-8416-cb

Application key: ••••••••••

Azure route injection: Individual traffic

Default region: northeurope

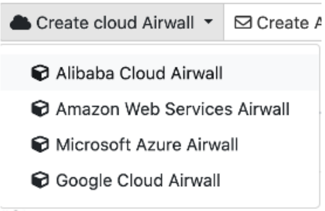
6. Click **Finish**.

You're now ready to create cloud Airwall Gateways in Azure in the Conductor.

Add an Azure Cloud Airwall Gateway

You must Set up Microsoft Azure as a cloud provider on page 434 before you can add an Airwall Gateway in the Conductor

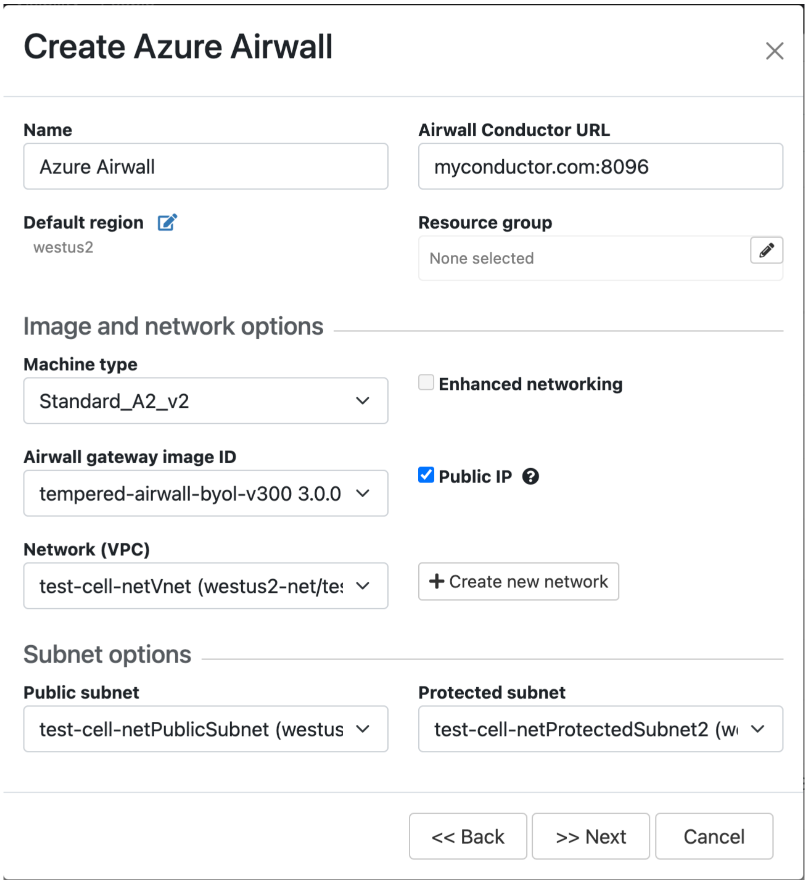
1. On the **Airwalls** page, (or in Conductor **Settings Cloud providers** tab), select **New cloud Airwall**, and then select **Microsoft Azure Airwall**.



2. In v2.2.8 and later, select **Create stand-alone Airwall gateway**, and then **Next**.
3. In v2.2.8 and later, **if you want to use a template** to create the Airwall Gateway, select the template, select **Next**, and then give the Airwall Gateway a descriptive name. You can then skip to the next step.

   To continue without a template and enter the information manually, just select **Next**.

   a) If you are filling in information manually, or want to change the template, fill in the **Name** and **Image and network options** for this Airwall Gateway. For **Machine type**, the default typically works. You can select a different size if needed for your purposes.



Create Azure Airwall

Name: Azure Airwall

Airwall Conductor URL: myconductor.com:8096

Default region: westus2

Resource group: None selected

Image and network options

Machine type: Standard_A2_v2

□ Enhanced networking

Airwall gateway image ID: tempered-airwall-byol-v300 3.0.0

☑ Public IP

Network (VPC): test-cell-netVnet (westus2-net/te:

Subnet options

Public subnet: test-cell-netPublicSubnet (westus

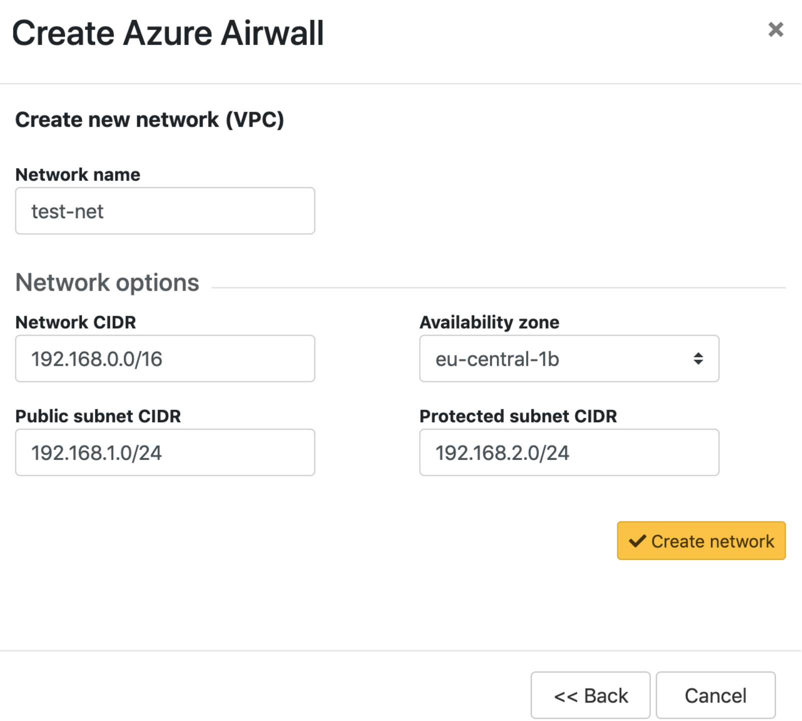
Protected subnet: test-cell-netProtectedSubnet2 (w

   b) Under **Airwall gateway image ID**, pick the Airwall Gateway image you want to use. The list shows the Airwall Gateway images available on your cloud provider.

   c) If you do not have a pre-configured virtual network, you need to create a new network. Click **Create new network** and fill in the form:

   - **Network CIDR** – Enter an available network address and subnet mask in CIDR notation.
   - **Public subnet CIDR** – Must be a subnet of the main network. Traffic flows between the underlay interface of the Airwall Gateway and the Public IP address object in Azure.
   - **Protected subnet CIDR** – Must be a subnet of the main network. Traffic must pass through theAirwall Gateway or through manually-crafted routes.

   When you're finished entering the information, select **Create network**, and when processing is complete, select **Back**.



Create Azure Airwall

Create new network (VPC)

Network name: test-net

Network options

Network CIDR: 192.168.0.0/16

Availability zone: eu-central-1b

Public subnet CIDR: 192.168.1.0/24

Protected subnet CIDR: 192.168.2.0/24

d) Back on the **Create cloud Airwall** page, select the network and public and protected subnets you just created.

4. Check the summary and if everything is correct, select **Create cloud Airwall**.
5. Select **Finish**. It may take up to 5 minutes for Microsoft Azure to complete creating the Airwall Gateway.

You've completed creating an Azure cloud Airwall Gateway, and now need to configure Provision, License, and configure it. For help, see Provision and License Airwall Edge Services on page 193 and Configure Airwall Edge Service Settings on page 359.

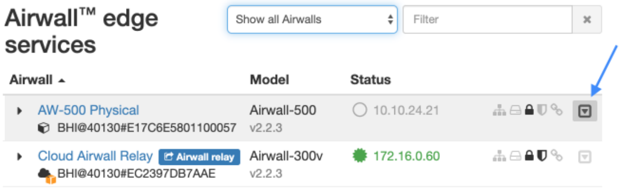
Provision and License Airwall Edge Services

How to provision and license Airwall Edge Services. You need to add Airwall Edge Services licenses to the Conductor before you can provision and license Airwall Edge Services.

1. In Conductor, open **Settings**, and go to the **Licensing** page.
2. If you have a license voucher, Add Airwall Edge Service Licenses to the Conductor on page 192. If you don't have a license voucher, contact sales@tempered.io to get one before continuing.
3. Install the Airwall Edge Services you want to license and connect them to the Conductor. For more information, see Deploy and Configure Airwall Edge Services on page 274 and Connect Airwall Gateways to the Conductor on page 292.
4. Under **Provisioning Requests**, select the check boxes for the Airwall Edge Services you want to provision, and under the **Actions** dropdown, click **Grant Request** to provision your Airwall Edge Services. They should reconnect to the Conductor and appear in your Airwall Edge Services list as unmanaged.

   Note: You can also grant provisioning requests from the **Provisioning** tab on the Dashboard.

5. On pre 2.2x Conductors, click **Sync**.
6. On the Conductor dashboard, click the **Show all Airwalls** box and filter the Airwall Edge Services by unmanaged.
7. In the row for the Airwall Edge Service you want to license, in the far right column, click the arrow to open the drop down menu, and select **Manage Airwalls**.



Airwall™ edge services

Airwall ▲	Model	Status
AW-500 Physical BHI@40130#E17C6E5801100057	Airwall-500 v2.2.3	○ 10.10.24.21
Cloud Airwall Relay Airwall relay BHI@40130#EC2397DB7AAE	Airwall-300v v2.2.3	● 172.16.0.60

Set up an Underlay IP NAT to Connect to your Azure Airwall Gateway

If you want other Airwall Edge Services to be able to connect to your Azure cloud Airwall Gateway, you need to set up a port group on your Underlay to connect to the public IP Azure creates for your Airwall Gateway.

To see if it’s set up yet, open the Azure Airwall Gateway in the Conductor. If you see a **Source IP** next to **Online status**, you need to set it up. The public IP is also accessible from the newly created resource group for your Azure Airwall Gateway.

1. On the Azure **Airwall** page, on the **Airwall** tab, copy the **Source IP** next to **Online status**.
2. Go to the **Ports** tab.
3. Open the **Underlay Port group**, and click **Edit Settings**.
4. In **Underlay IP (NAT)**, enter the Source IP you copied above.
5. Select **Update Settings**.

You now have an Azure cloud Airwall Gateway set up and ready to use.

Troubleshoot Setup on an Azure Cloud Airwall

If you get an “Authorization failed” message when trying to create an Azure cloud Airwall, you need to accept terms for the image you’re using. See Accept Azure Terms for the Airwall Gateway Images on page 325 .

Add network interfaces to an Azure Virtual Machine

If you have resources in multiple virtual subnets within Azure that you want to protect with a single 300v Airwall Gateway, you can add additional network interfaces to the two included in a standard Azure 300v deployment.

Note: You can add as many additional network interfaces as the Azure instance allows.

Supported Versions	Conductor and Azure Cloud Airwall Gateways v3.0 and later
Required Role	• System or network administrators • Permissions to edit the Azure Cloud Airwall Gateways. You need to be a manager of at least one overlay that these Airwall Gateways are in.
Supported on these Airwall Edge Services	Airwall Gateway 300v only.

Before you Begin

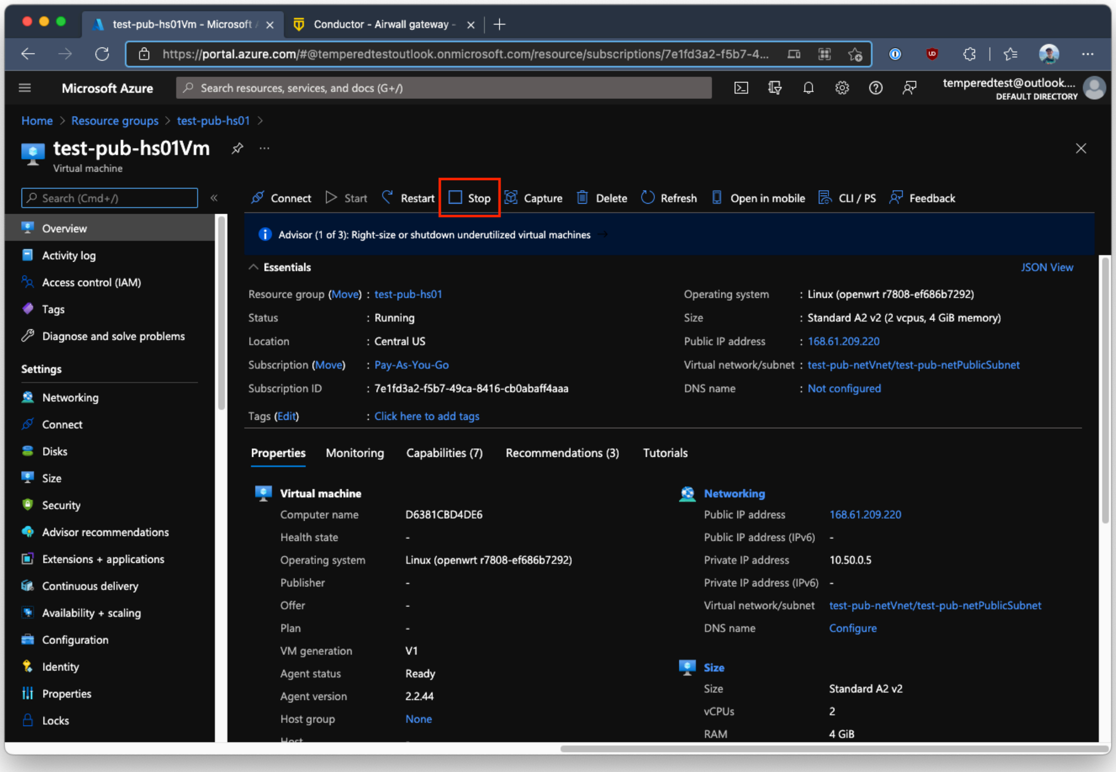
Before you add an interface, consider:

- **Cost** – An Azure virtual machine (VM) that supports multiple interfaces increases the cost, so weigh the costs and benefits of adding more network interfaces versus deploying multiple 300v Airwall Gateways.
- **Machine type** – If you are using the default Azure VM, Standard A2 v2, you must upgrade the machine type to one that supports the number of NICs you want. A list of available NICs per machine type is available in the Azure documentation. Select a machine series from the list (for example, the Av2-series) and scroll to the right in the table to find the maximum number of NICs.
- **Update your Conductor and Airwall Gateway 300v to v3.0** – v3.0 is required to manage the route injection for devices on the additional network interfaces.

Add a Network Interface (NIC) to an Azure 300v deployment

These instructions may change. Please refer to the Azure documentation for updated information.

1. Go to the Azure VM that is hosting your 300v Airwall Gateway.
2. Stop the Azure VM.



Advisor (1 of 3): Right-size or shutdown underutilized virtual machines

Essentials

Resource group (Move) : test-pub-hs01
Status : Running
Location : Central US
Subscription (Move) : Pay-As-You-Go
Subscription ID : 7e1fd3a2-f5b7-49ca-8416-cb0abaff4aaa
Tags (Edit) : Click here to add tags

Operating system : Linux (openwrt r7808-ef686b7292)
Size : Standard A2 v2 (2 vcpus, 4 GiB memory)
Public IP address : 168.61.209.220
Virtual network/subnet : test-pub-netVnet/test-pub-netPublicSubnet
DNS name : Not configured

Virtual machine

Computer name	D6381CBD4DE6
Health state	-
Operating system	Linux (openwrt r7808-ef686b7292)
Publisher	-
Offer	-
Plan	-
VM generation	V1
Agent status	Ready
Agent version	2.2.44
Host group	None

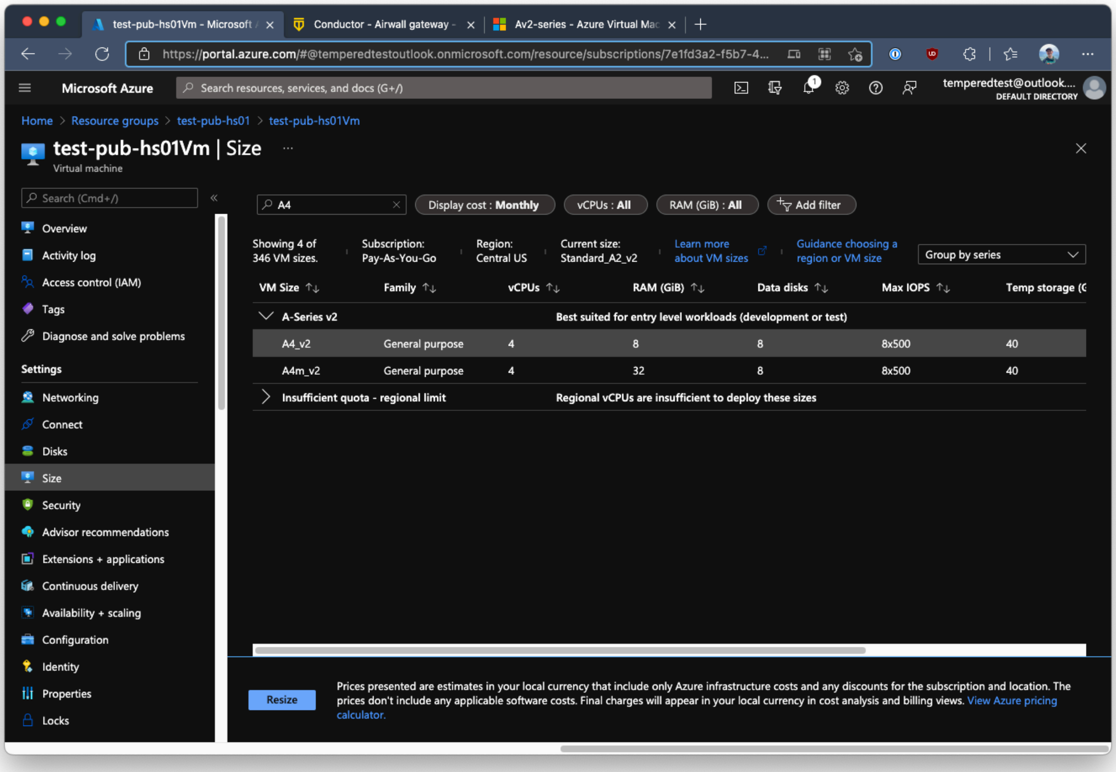
Networking

Public IP address	168.61.209.220
Public IP address (IPv6)	-
Private IP address	10.50.0.5
Private IP address (IPv6)	-
Virtual network/subnet	test-pub-netVnet/test-pub-netPublicSubnet
DNS name	Configure

Size

Size	Standard A2 v2
vCPUs	2
RAM	4 GiB

3. Go to **Settings** > **Size**, and select a new machine type. This screenshot shows upgrading to a Standard A4 v2 that allows up to 4 NICs.



test-pub-hs01Vm | Size

Virtual machine

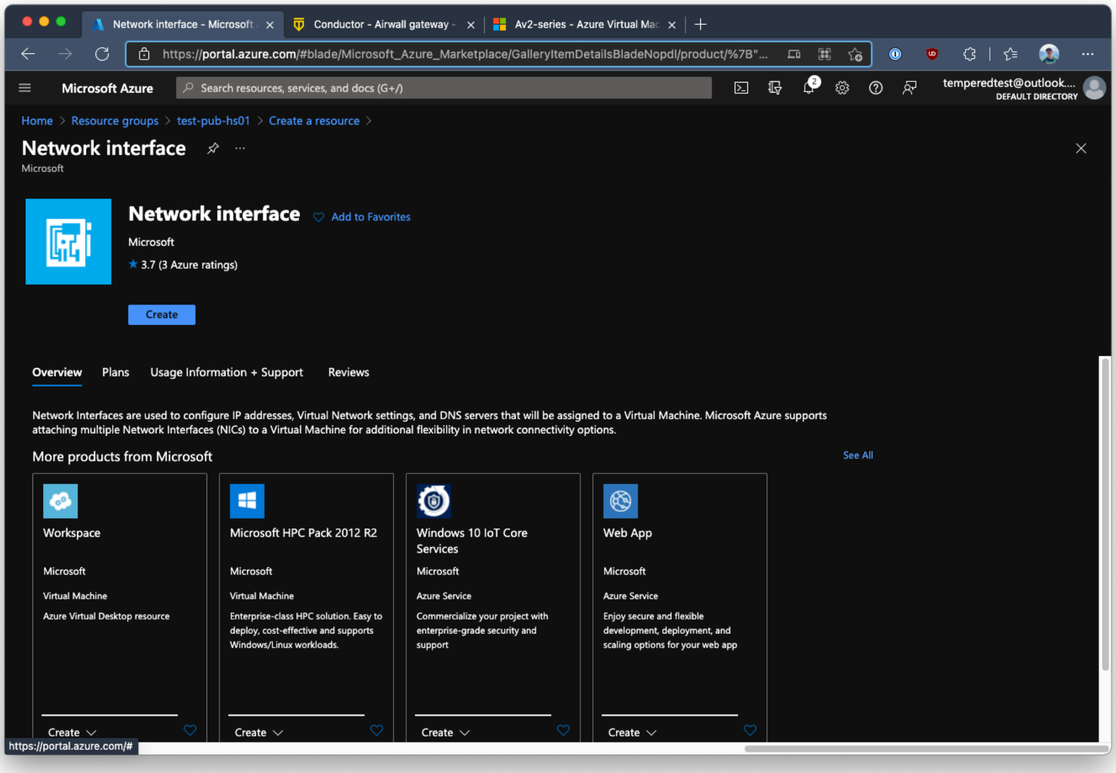
A4 | Display cost : **Monthly** | vCPUs : **All** | RAM (GiB) : **All** | Add filter

Showing 4 of 346 VM sizes. | Subscription: Pay-As-You-Go | Region: Central US | Current size: Standard_A2_v2 | Learn more about VM sizes | Guidance choosing a region or VM size | Group by series

VM Size	Family	vCPUs	RAM (GiB)	Data disks	Max IOPS	Temp storage (G
A-Series v2	Best suited for entry level workloads (development or test)					
A4_v2	General purpose	4	8	8	8x500	40
A4m_v2	General purpose	4	32	8	8x500	40
Insufficient quota - regional limit	Regional vCPUs are insufficient to deploy these sizes					

Prices presented are estimates in your local currency that include only Azure infrastructure costs and any discounts for the subscription and location. The prices don't include any applicable software costs. Final charges will appear in your local currency in cost analysis and billing views. View Azure pricing calculator.

4. In the 300v’s Resource Group, create a new Network Interface object (NIC).


Home > Resource groups > test-pub-hs01 > Create a resource >
Add to Favorites
Create
Overview
Plans
Usage Information + Support
Reviews
See All
Create
Create
Create
Create

Network interface

Microsoft

Network interface

Microsoft

★ 3.7 (3 Azure ratings)

Network Interfaces are used to configure IP addresses, Virtual Network settings, and DNS servers that will be assigned to a Virtual Machine. Microsoft Azure supports attaching multiple Network Interfaces (NICs) to a Virtual Machine for additional flexibility in network connectivity options.

More products from Microsoft

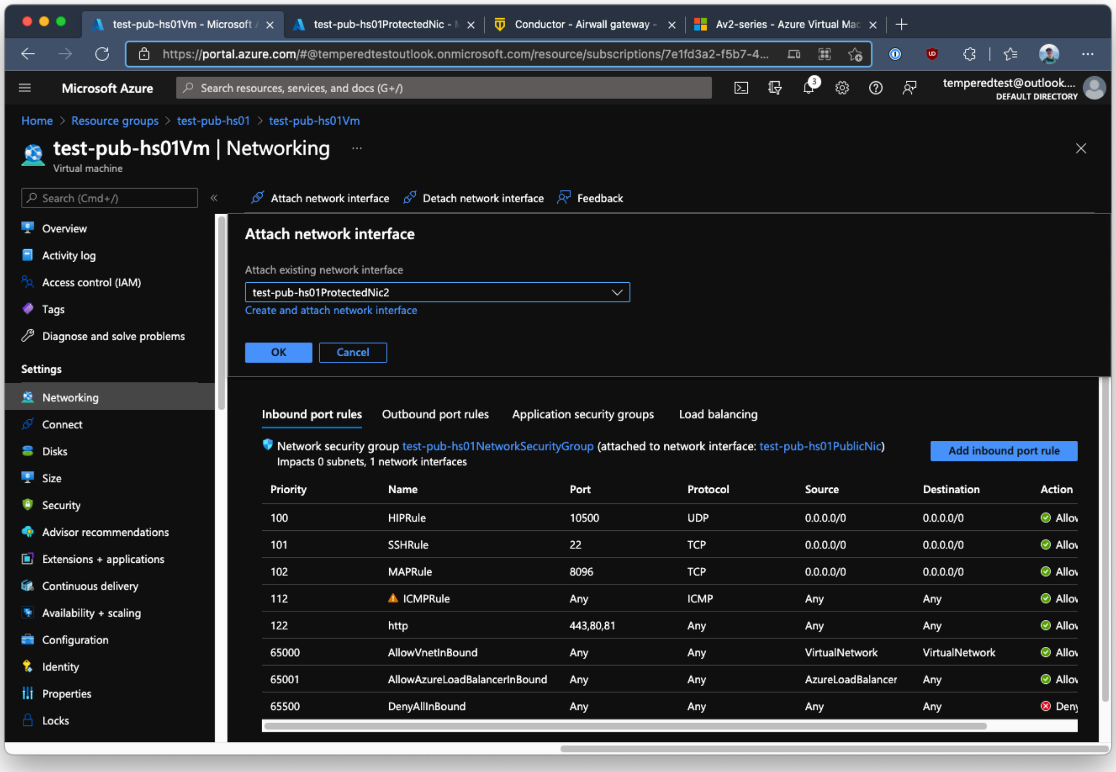
Workspace
Microsoft
Virtual Machine
Azure Virtual Desktop resource

Microsoft HPC Pack 2012 R2
Microsoft
Virtual Machine
Enterprise-class HPC solution. Easy to deploy, cost-effective and supports Windows/Linux workloads.

Windows 10 IoT Core Services
Microsoft
Azure Service
Commercialize your project with enterprise-grade security and support

Web App
Microsoft
Azure Service
Enjoy secure and flexible development, deployment, and scaling options for your web app

5. Under the Azure VM's **SettingsNetworking**, select **Attach network interface** and under **Attach existing network interface**, select the network interface you created.


test-pub-hs01Vm - Microsoft
test-pub-hs01ProtectedNic -
Conductor - Airwall gateway -
Av2-series - Azure Virtual Mac
https://portal.azure.com/#@temperedtestoutlook.onmicrosoft.com/resource/subscriptions/7e1fd3a2-f5b7-4...
Microsoft Azure
Search resources, services, and docs (G+/)
temperedtest@outlook....
DEFAULT DIRECTORY
Home > Resource groups > test-pub-hs01 > test-pub-hs01Vm
test-pub-hs01Vm | Networking
Virtual machine
Search (Cmd+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
Connect
Disks
Size
Security
Advisor recommendations
Extensions + applications
Continuous delivery
Availability + scaling
Configuration
Identity
Properties
Locks
Attach network interface
Detach network interface
Feedback

Attach network interface

Attach existing network interface

test-pub-hs01ProtectedNic2

Create and attach network interface

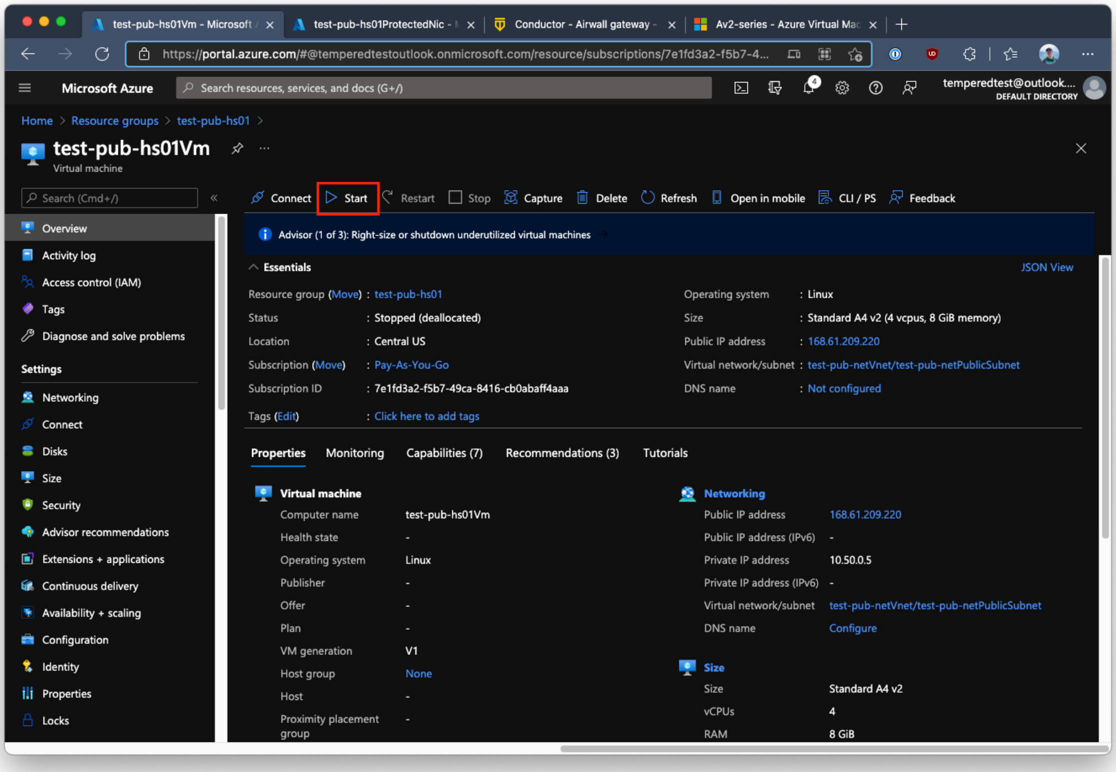
OK Cancel

Inbound port rules
Outbound port rules
Application security groups
Load balancing
Add inbound port rule

Network security group test-pub-hs01NetworkSecurityGroup (attached to network interface: test-pub-hs01PublicNic)
Impacts 0 subnets, 1 network interfaces

Priority	Name	Port	Protocol	Source	Destination	Action
100	HIPRule	10500	UDP	0.0.0.0/0	0.0.0.0/0	✓ Allo
101	SSHRule	22	TCP	0.0.0.0/0	0.0.0.0/0	✓ Allo
102	MAPRule	8096	TCP	0.0.0.0/0	0.0.0.0/0	✓ Allo
112	⚠ ICMPRule	Any	ICMP	Any	Any	✓ Allo
122	http	443,80,81	Any	Any	Any	✓ Allo
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allo
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✓ Allo
65500	DenyAllInBound	Any	Any	Any	Any	⊗ Deny

6. Restart the Azure VM.



Resource group (Move) : test-pub-hs01
Status : Stopped (deallocated)
Location : Central US
Subscription (Move) : Pay-As-You-Go
Subscription ID : 7e1fd3a2-f5b7-49ca-8416-cb0abaff4aaa
Tags (Edit) : Click here to add tags

Operating system : Linux
Size : Standard A4 v2 (4 vcpus, 8 GiB memory)
Public IP address : 168.61.209.220
Virtual network/subnet : test-pub-netVnet/test-pub-netPublicSubnet
DNS name : Not configured

Virtual machine

Computer name	test-pub-hs01Vm
Health state	-
Operating system	Linux
Publisher	-
Offer	-
Plan	-
VM generation	V1
Host group	None
Host	-
Proximity placement group	-

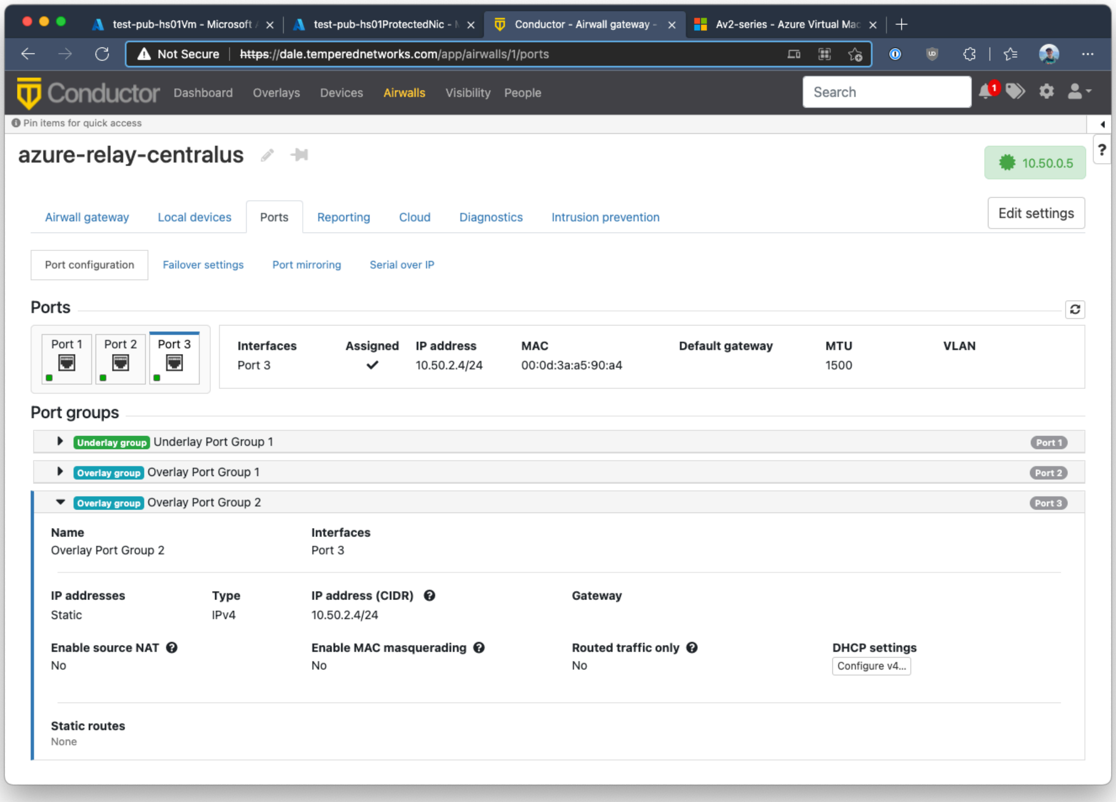
Networking

Public IP address	168.61.209.220
Public IP address (IPv6)	-
Private IP address	10.50.0.5
Private IP address (IPv6)	-
Virtual network/subnet	test-pub-netVnet/test-pub-netPublicSubnet
DNS name	Configure

Size

Size	Standard A4 v2
vCPUs	4
RAM	8 GiB

Once the Azure VM reconnects to the Conductor, the 300v updates its port information with a third network interface with the overlay gateway IP already configured:



azure-relay-centralus

10.50.0.5

Ports

Interfaces	Assigned	IP address	MAC	Default gateway	MTU	VLAN
Port 3	✓	10.50.2.4/24	00:0d:3a:a5:90:a4		1500	

Port groups

- Underlay group Underlay Port Group 1 — Port 1
- Overlay group Overlay Port Group 1 — Port 2
- Overlay group Overlay Port Group 2 — Port 3

Name: Overlay Port Group 2
Interfaces: Port 3

IP addresses: Static
Type: IPv4
IP address (CIDR): 10.50.2.4/24
Gateway:

Enable source NAT: No
Enable MAC masquerading: No
Routed traffic only: No
DHCP settings: Configure v4...

Static routes: None

Google Cloud (GCP) – Set up an Airwall Gateway

To set up an Airwall Gateway in Google Cloud Platform (GCP), complete the following steps.

Prerequisites

Required licenses	An Airwall 300v license for each virtual Airwall Gateway you are setting up.
Supported versions	Conductor v2.2.3 and later

Note: You should be familiar with using Google Cloud before attempting to deploy a Tempered Conductor or Airwall Gateway on the platform. To get started, we recommend you review the following content offered by Google:

- Google Cloud Platform Overview
- Google Cloud Storage
- Virtual Private Cloud
- Google Compute Engine Documentation

Set up an Airwall Gateway on Google Cloud

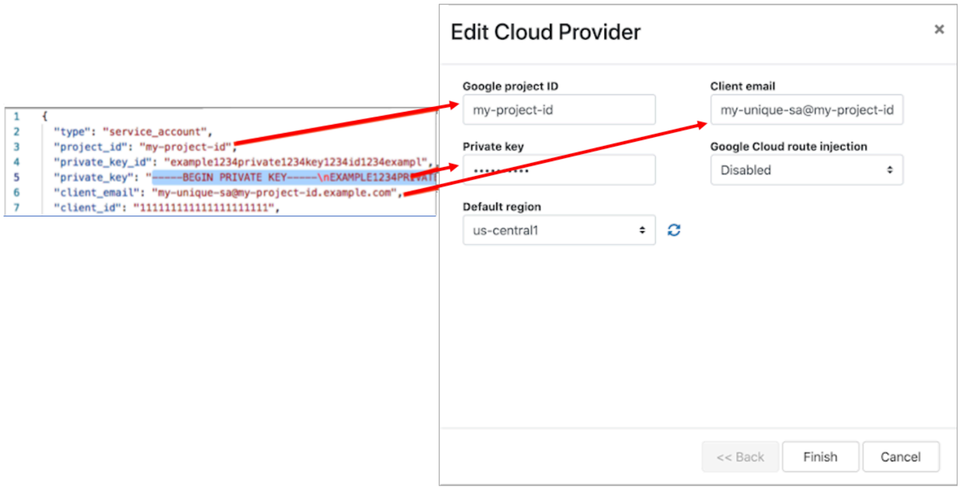
There are two steps required to deploy an Airwall Gateway to your Google Cloud account:

1. Set up Google Cloud as a cloud provider
2. Add one or more Airwall Gateways either from the Conductor or GCP marketplace:
   - Add an Airwall Gateway from the Conductor on page 335
   - Add an Airwall Gateway from GCP marketplace on page 337

Set up Google Cloud as a cloud provider

1. Download a JSON key from your Google Cloud account. For assistance, see Google Cloud help: https://cloud.google.com/iam/docs/creating-managing-service-account-keys.

   Note: Save the key file somewhere you can access it easily. You will need the information in this file when configuring the Google Cloud provider in the Conductor.
2. Log in to your Conductor, and click the gear icon in the upper right to open **Settings**.
3. On the **Cloud providers** tab, select **Add cloud provider**.
4. Select **Google Cloud**, and then **Next**.
5. Fill in the **Google project ID**, **Client email**, and **Private key** fields with the corresponding information from the key file you downloaded.



```
{
  "type": "service_account",
  "project_id": "my-project-id",
  "private_key_id": "example1234private1234key1234id1234exampl",
  "private_key": "-----BEGIN PRIVATE KEY-----\nEXAMPLE1234PRIVAT
  "client_email": "my-unique-sa@my-project-id.example.com",
  "client_id": "111111111111111111111",
```

Edit Cloud Provider

Google project ID: my-project-id

Client email: my-unique-sa@my-project-id

Private key: ••••••••

Google Cloud route injection: Disabled

Default region: us-central1

6. The **Google Cloud route injection** setting determines how new routes are added to the Google Cloud routing table. The routes are for traffic on your protected overlay network between protected devices and the Airwall Gateway. Here are the recommended settings depending on your deployment details:

   - If you are using a Airwall Relay, or want to manage routes on your own, set to **Disabled**.

     Important: If your Airwall's subnet has a route table with existing or planned future routes, then do not set route injection to **Individual traffic** or **All traffic**. This removes these existing and future routes from the route table, retaining only routes created by Conductor.
   - If you want to handle traffic for devices individually, set to **Individual traffic**.
   - If you want one route to send all traffic to the overlay port on the Airwall Gateway, set to **All traffic**.

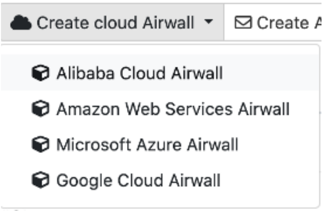
     Note: All traffic is effectively 'full tunnel' mode. With Individual traffic, you could add routes that send traffic around the Airwall Gateway.
7. Click **Finish**.

Note: If you need more information about Google Cloud Service Accounts, see https://cloud.google.com/iam/docs/creating-managing-service-accounts.

Add an Airwall Gateway from the Conductor

You must Set up Google Cloud as a cloud provider on page 334 before you can add an Airwall Gateway in the Conductor

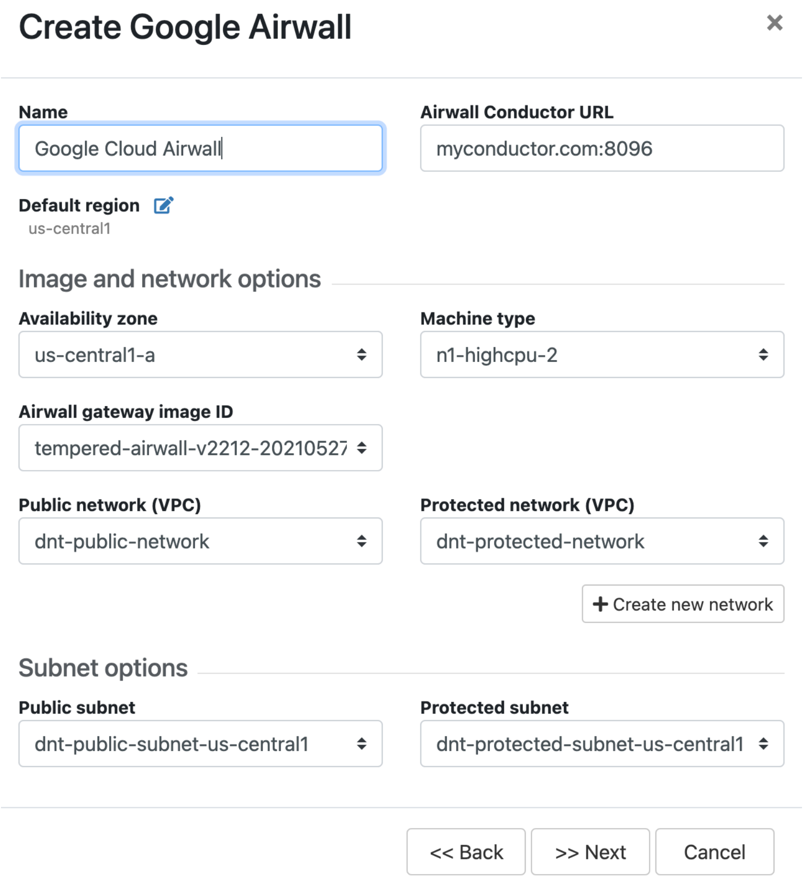
1. On the **Airwalls** page, (or in Conductor **Settings Cloud providers** tab), click **New cloud Airwall**, and select **Google Cloud Airwall**.



2. In v2.2.8 and later, select **Create stand-alone Airwall gateway**, and then **Next**.
3. In v2.2.8 and later, **if you want to use a template** to create the Airwall Gateway, select the template, select **Next**, and then give the Airwall Gateway a descriptive name. You can then skip to the next step.

   To continue without a template and enter the information manually, just select **Next**.

   a) If you are filling in information manually, or want to change the template, fill in the **Name** and **Image and network options** for this Airwall Gateway. For **Machine type**, the default typically works. You can select a different size if needed for your purposes.



Create Google Airwall

Name: Google Cloud Airwall

Airwall Conductor URL: myconductor.com:8096

Default region: us-central1

Image and network options

Availability zone: us-central1-a

Machine type: n1-highcpu-2

Airwall gateway image ID: tempered-airwall-v2212-20210527

Public network (VPC): dnt-public-network

Protected network (VPC): dnt-protected-network

Subnet options

Public subnet: dnt-public-subnet-us-central1

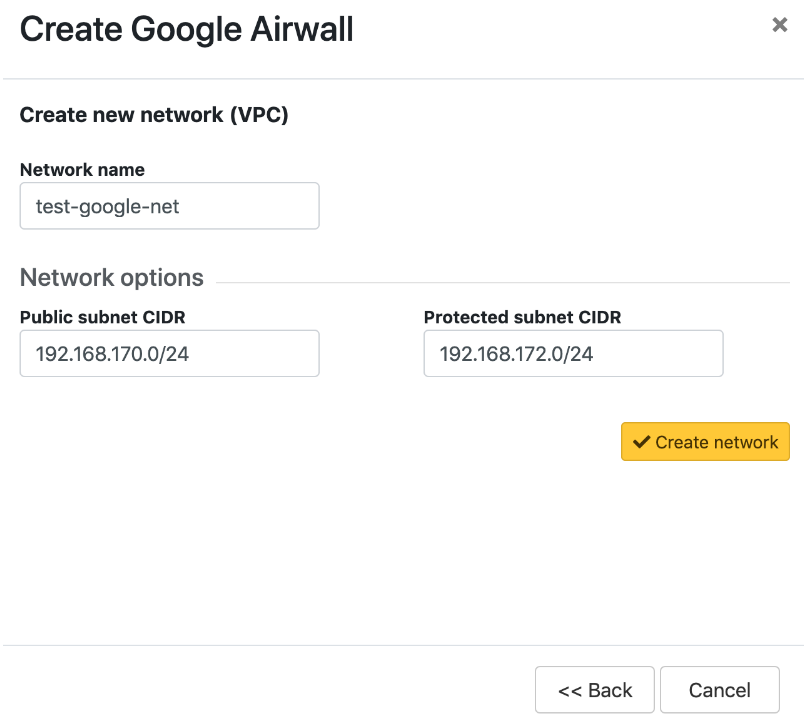
Protected subnet: dnt-protected-subnet-us-central1

   b) Under **Airwall gateway image ID**, pick the Airwall Gateway image you want to use. The list shows the Airwall Gateway images available on your cloud provider.

   c) If you do not have a pre-configured virtual network, you need to create a new network. Click **Create new network** and fill in the form:

   - **Network CIDR** – Enter an available network address and subnet mask in CIDR notation.
   - **Public subnet CIDR** – Must be a subnet of the main network. Traffic flows between the underlay interface of the Airwall Gateway and the Public IP address object in Azure.
   - **Protected subnet CIDR** – Must be a subnet of the main network. Traffic must pass through the Airwall Gateway or through manually-crafted routes.

   When you're finished entering the information, select **Create network**, and when processing is complete, select **Back**.



Create Google Airwall

Create new network (VPC)

Network name: test-google-net

Network options

Public subnet CIDR: 192.168.170.0/24

Protected subnet CIDR: 192.168.172.0/24

d) Back on the **Create cloud Airwall** page, select the network and public and protected subnets you just created.

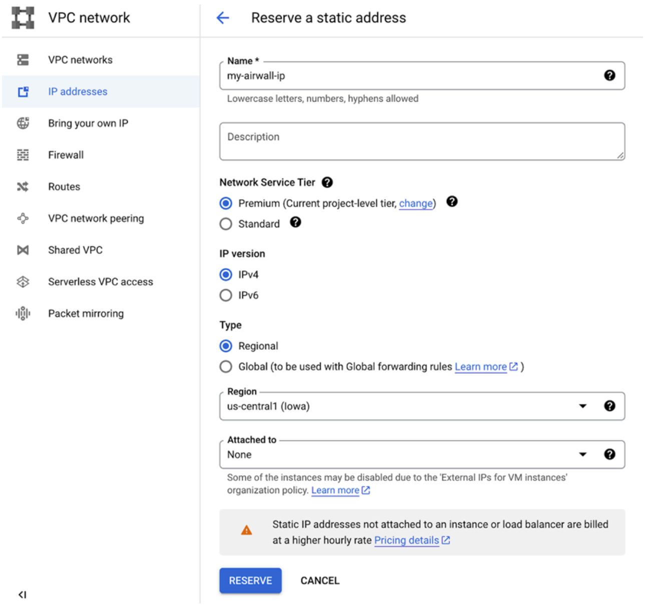
4. Check the summary and if everything is correct, select **Create cloud Airwall**.
5. Select **Finish**. It may take up to 5 minutes for Google Cloud to complete creating the Airwall Gateway.

You've completed creating a Google cloud Airwall Gateway, and now need to configure Provision, License, and configure it. For help, see Provision and License Airwall Edge Services on page 193 and Configure Airwall Edge Service Settings on page 359.

Add an Airwall Gateway from GCP marketplace

To set up an Airwall Gateway in Google Cloud Platform (GCP) from GCP marketplace, complete the following steps.

1. Go to the External IP addresses page. Click **Reserve External Static Address**.
2. Specify the **Name** and select the **Region** where your instance is going to be deployed. Click **Reserve**.



Reserve a static address

Name *: my-airwall-ip

Lowercase letters, numbers, hyphens allowed

Description

Network Service Tier
● Premium (Current project-level tier, change)
○ Standard

IP version
● IPv4
○ IPv6

Type
● Regional
○ Global (to be used with Global forwarding rules Learn more)

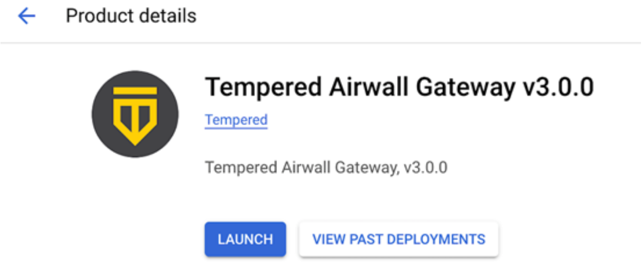
Region: us-central1 (Iowa)

Attached to: None

Some of the instances may be disabled due to the 'External IPs for VM instances' organization policy. Learn more

Static IP addresses not attached to an instance or load balancer are billed at a higher hourly rate Pricing details

3. Go to Tempered Airwall Gateway marketplace page.



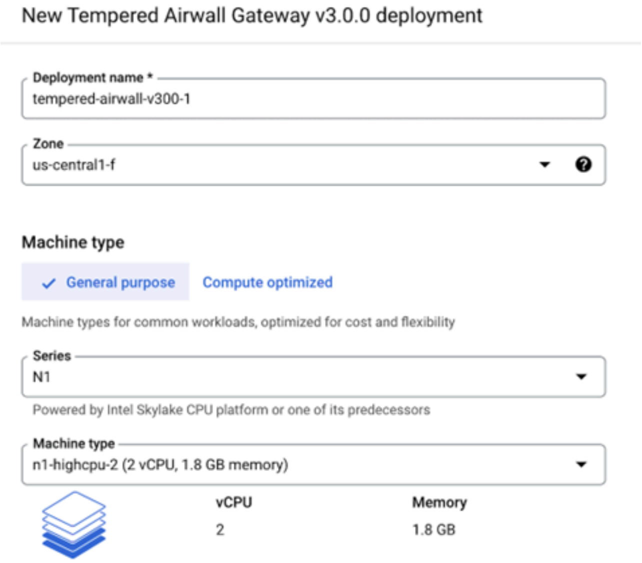
Product details

Tempered Airwall Gateway v3.0.0

Tempered

Tempered Airwall Gateway, v3.0.0

4. Click **Launch**.
5. Specify the **Deployment name**. Select **Zone** and **Machine type**.



New Tempered Airwall Gateway v3.0.0 deployment

Deployment name * tempered-airwall-v300-1

Zone us-central1-f

Machine type

Machine types for common workloads, optimized for cost and flexibility

Series N1

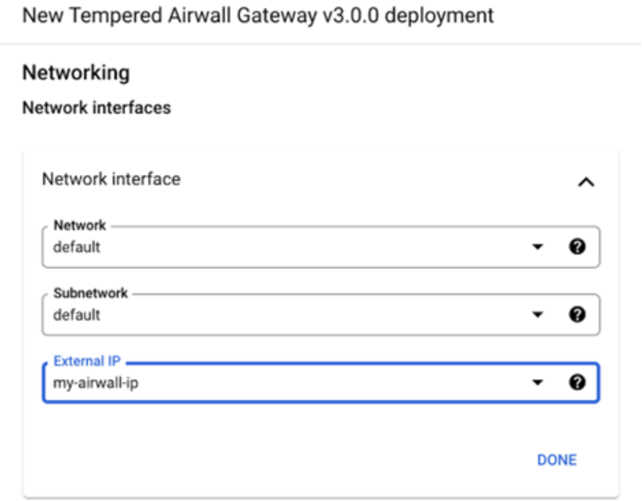
Powered by Intel Skylake CPU platform or one of its predecessors

Machine type n1-highcpu-2 (2 vCPU, 1.8 GB memory)

vCPU	Memory
2	1.8 GB

6. Select **Network** and **Subnetwork** for your shared network interface. Choose the static external IP address that you created in step 2.

Note: Selecting **None** results in the instance having no external internet access.



New Tempered Airwall Gateway v3.0.0 deployment

Networking

Network interfaces

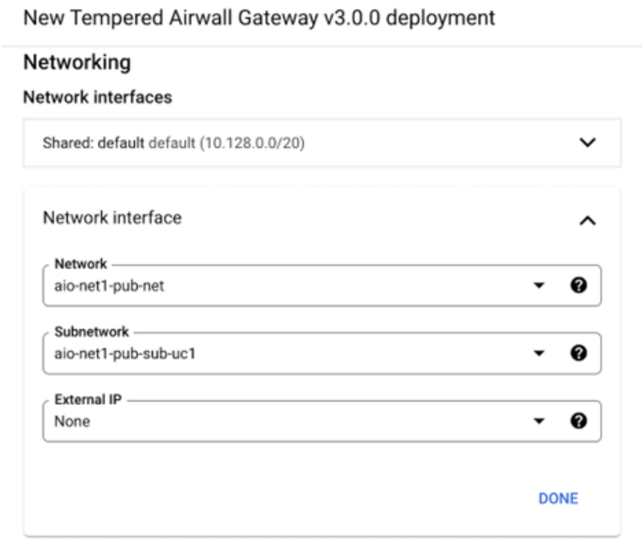
Network interface

Network default

Subnetwork default

External IP my-airwall-ip

7. Select **Network** and **Subnetwork** for your protected network interface. Choose **None** for **External IP**.



New Tempered Airwall Gateway v3.0.0 deployment

Networking

Network interfaces

Shared: default default (10.128.0.0/20)

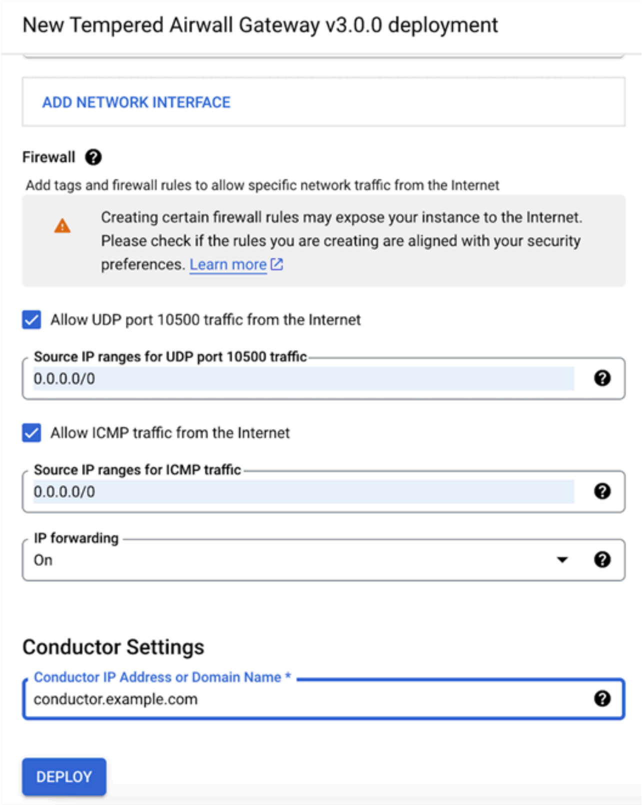
Network interface

Network: aio-net1-pub-net

Subnetwork: aio-net1-pub-sub-uc1

External IP: None

8. Specify the **Source IP ranges** for UDP port 10500 and ICMP traffics. Enter the **Conductor IP Address**. Click **Deploy**.



New Tempered Airwall Gateway v3.0.0 deployment

Firewall

Add tags and firewall rules to allow specific network traffic from the Internet

Creating certain firewall rules may expose your instance to the Internet. Please check if the rules you are creating are aligned with your security preferences. Learn more

☑ Allow UDP port 10500 traffic from the Internet

Source IP ranges for UDP port 10500 traffic: 0.0.0.0/0

☑ Allow ICMP traffic from the Internet

Source IP ranges for ICMP traffic: 0.0.0.0/0

IP forwarding: On

Conductor Settings

Conductor IP Address or Domain Name *: conductor.example.com

Add an interface with an associated route table on a cloud Airwall Gateway

If you need to attach a route table to an interface you're adding in AWS or Azure, you'll need to add the interface and attach the route table before you reboot the Airwall Gateway.

Supported versions	- v3.0.0 Conductors - AWS and Azure Cloud Airwall Gateways

Supported Roles	AWS or Azure cloud administrator, and Conductor system administrator , or network administrator with permissions to create cloud Airwall Gateways

CAUTION: If you reboot the Airwall Gateway before you've associated the route table, the Conductor sees the new interface and checks the route table. When it doesn't find a specific one, it tries to find one, and it may not find the correct one. It doesn't recheck the route table once it's found one.

For the most up-to-date information, see the documentation for your respective cloud provider.

If you've already rebooted, see Get an AWS Airwall Gateway to pull the correct route table on page 492.

1. Associate the route table to your new interface (for example, Port 3) subnet.
2. Create a new interface (for example, Port 3).
3. Attach the new interface to the Airwall Gateway.
4. Reboot the Airwall Gateway.

Here are some suggested resources for AWS and Azure documentation on multiple NICs:

AWS:

- **Associate a protected subnet with a protected route table first**: https://docs.aws.amazon.com/vpc/latest/userguide/WorkWithRouteTables.html#AssociateSubnet
- **Attach an interface to an instance**: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#working-with-enis

Azure:

- **Associate a protected subnet with a protected route table first**:https://docs.microsoft.com/en-us/azure/virtual-network/manage-route-table#associate-a-route-table-to-a-subnet
- **Attach an interface to an instance**:https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface-vm

Airwall Gateway for Google Cloud Platform Quick Start

To get started, make sure you have access to your Google Cloud account. If you do not have an account, you can create a free Google Cloud account and upgrade it to a full account later. If you have an existing Google Cloud account, make sure your billing information is set up. You cannot create a project until you are able to link your billing information to your newly created project.

Log in to Google Cloud

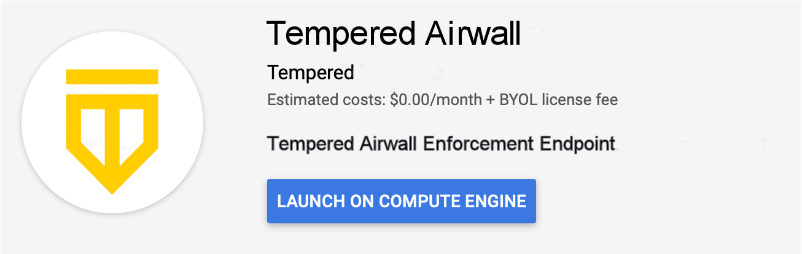
From a Web browser, navigate to https://console.cloud.google.com. You will see one of two pages, the **Getting Started** page if you have no projects or the **Home** page if you have existing projects.

Step 2: Select the Tempered Airwall Gateway from the Marketplace

You will need to locate the Airwall Gateway in the Google Cloud Marketplace.

1. From your GCP Dashboard, select **Marketplace** on the left sidebar.
2. In the **Search** field at the top of the page, enter `tempered airwall` and press enter.
3. In the results list, locate and select Tempered™ Airwall.

This will take you to the product page where you can deploy the Airwall Gateway.



Tempered Airwall

Tempered

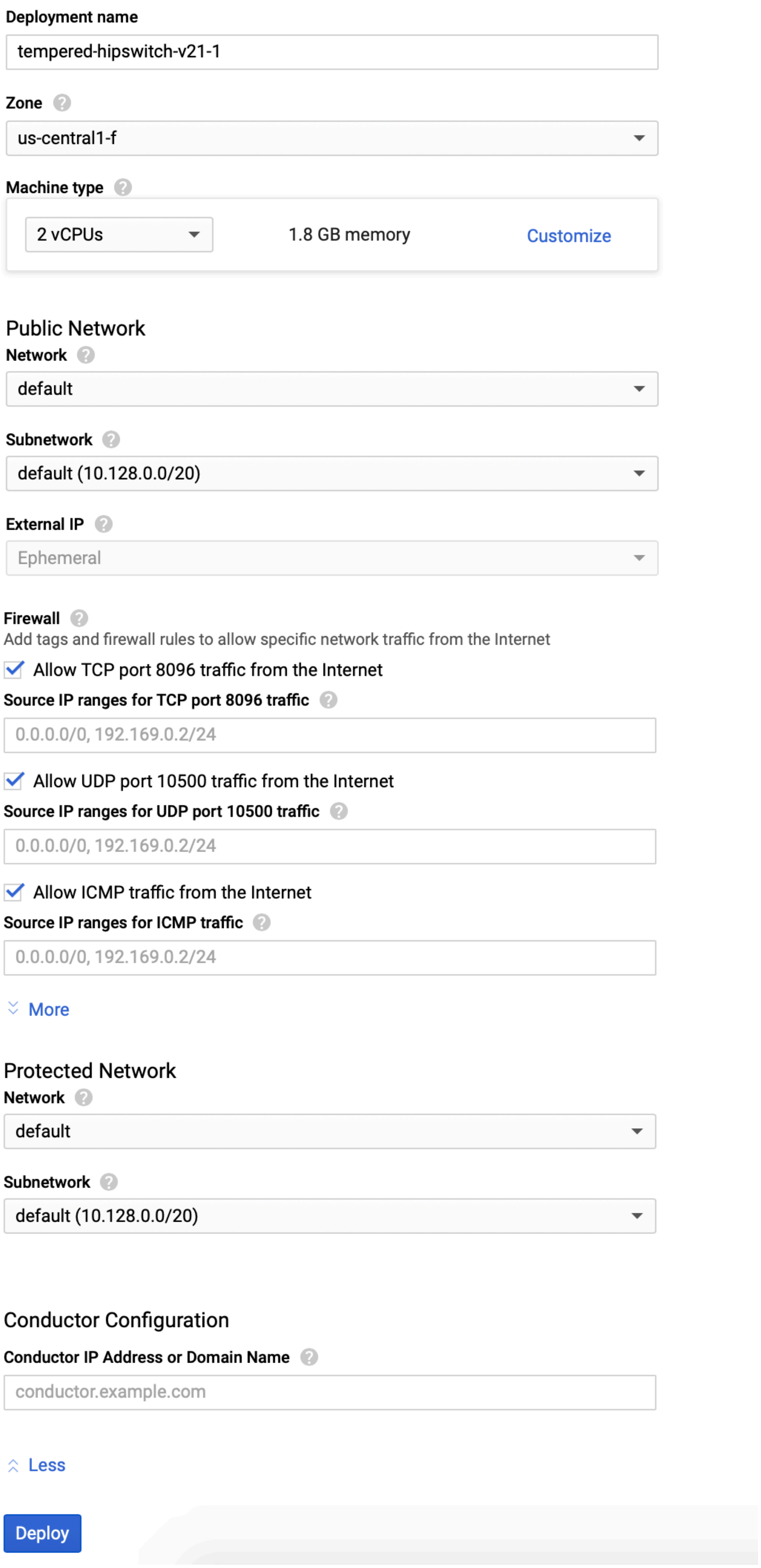
Estimated costs: $0.00/month + BYOL license fee

Tempered Airwall Enforcement Endpoint

Step 3: Install the Airwall Gateway Image

1. On the product page, click **LAUNCH ON COMPUTE ENGINE**.
2. The Airwall Gateway deployment uses a template so most settings you can leave as is, however you may want to make the following changes:
   a) **Deployment name**: Enter a name for your Airwall Gateway.
   b) **Zone**: Select a zone from the drop-down. The zone determines what computing resources are available and where your data is stored and used.
   c) **Machine type**: Leave as is. Machine type determines the amount of memory, virtual cores, and persistent disk limits for the Airwall Gateway. The default settings are required for the instance to function correctly.
   d) **Public network**: You can leave the defaults as is and a new network will be created for you. If you have a previously created network you want to use, you can select it here.
   e) **Networking**: Leave the **Firewall**, and **IP forwarding** fields as is.
   f) **Protected Network**: This network must be different from the network you selected in the **Public Network** section. In the **Network** drop-down, select `protected`. A new network will be created for you. If you have a previously created network you want to use, you can select it here.
   g) Click **Show Conductor configuration options** to expose the **Conductor IP Address ir Domain Name** field, and enter the address to your Conductor. If you do not know this address, you need to obtain it from the owner of your Conductor. You cannot complete the deployment of your Airwall Gateway without it.

   Note: Some fields may be hidden based on your screen size. To view these fields, click **More** button to expand the list.



Deployment name

tempered-hipswitch-v21-1

Zone

us-central1-f

Machine type

2 vCPUs 1.8 GB memory

Public Network

Network

default

Subnetwork

default (10.128.0.0/20)

External IP

Ephemeral

Firewall

Add tags and firewall rules to allow specific network traffic from the Internet

☑ Allow TCP port 8096 traffic from the Internet

Source IP ranges for TCP port 8096 traffic

0.0.0.0/0, 192.169.0.2/24

☑ Allow UDP port 10500 traffic from the Internet

Source IP ranges for UDP port 10500 traffic

0.0.0.0/0, 192.169.0.2/24

☑ Allow ICMP traffic from the Internet

Source IP ranges for ICMP traffic

0.0.0.0/0, 192.169.0.2/24

Protected Network

Network

default

Subnetwork

default (10.128.0.0/20)

Conductor Configuration

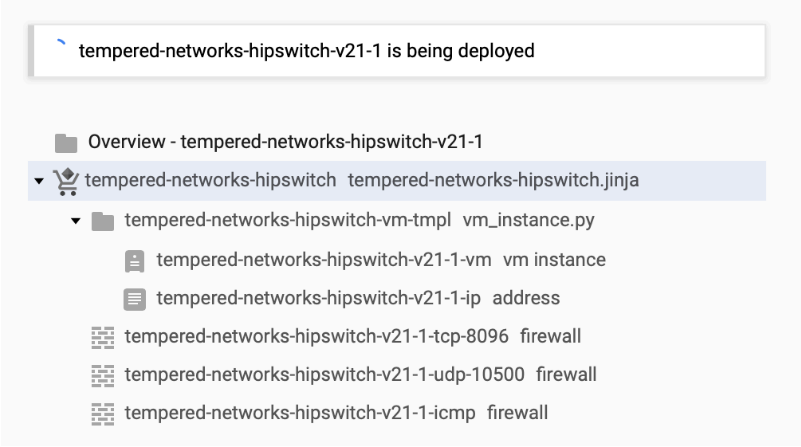
Conductor IP Address or Domain Name

conductor.example.com

3. Click **Deploy** to begin installing the Airwall Gateway.

Step 4: Finalize the Deployment

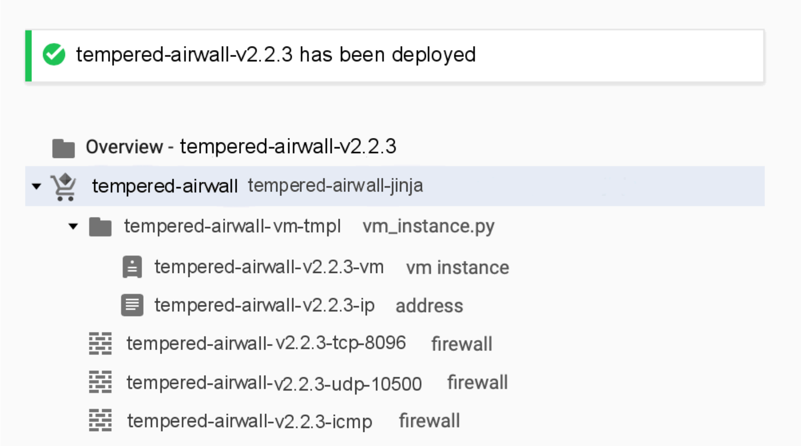
It will take a few moments for the process to complete. You can view the progress of your deployment by viewing the tree hierarchy of your components on the page.



tempered-networks-hipswitch-v21-1 is being deployed

Overview - tempered-networks-hipswitch-v21-1
tempered-networks-hipswitch tempered-networks-hipswitch.jinja
tempered-networks-hipswitch-vm-tmpl vm_instance.py
tempered-networks-hipswitch-v21-1-vm vm instance
tempered-networks-hipswitch-v21-1-ip address
tempered-networks-hipswitch-v21-1-tcp-8096 firewall
tempered-networks-hipswitch-v21-1-udp-10500 firewall
tempered-networks-hipswitch-v21-1-icmp firewall

Once complete, the message will change indicating your deployment is complete.



tempered-airwall-v2.2.3 has been deployed

Overview - tempered-airwall-v2.2.3
tempered-airwall tempered-airwall-jinja
tempered-airwall-vm-tmpl vm_instance.py
tempered-airwall-v2.2.3-vm vm instance
tempered-airwall-v2.2.3-ip address
tempered-airwall- v2.2.3-tcp-8096 firewall
tempered-airwall-v2.2.3-udp-10500 firewall
tempered-airwall-v2.2.3-icmp firewall

Step 5: Verify the Install

At this point the Airwall Gateway instance is running in Google Cloud. It may take several minutes for it to become available after it starts, so if it does not show in the Conductor, try again in a few minutes.

Install Airwall Agents and Servers on people's laptops and devices

How to connect people's cell phones, laptops, and servers to the resources people need access to behind your Airwall secure network.

People connect their devices to your secure network using software installed on their devices. There are Airwall Agent or Server software applications for the most common device types. The easiest way to get your users started is to send them an Airwall Invitation or Activation codes. Help for your users to install the software and connect is here: Connect to Airwall on page 6.

If you need to install the software from the Conductor, see the unattended installation instructions for select platforms in this section.

Operating system requirements for Airwall Agents and Servers

Operating system requirements for the Airwall Solution and Airwall Teams.

System Requirements

Please review the system requirements before installing to make sure your device can run the Airwall Agent or Server.

Microsoft Windows	The Windows Airwall Agent works on Microsoft Windows 7, 8.1, or 10, and runs on both Home and Professional versions. **Airwall only:** The Windows-based Airwall Server works on Microsoft Windows Server 2008R2, 2012R2, or 2016, or later.
Apple macOS	Works on 10.14 Mojave, or 10.15 Catalina, and later.
Apple iOS	Works on iOS 13 and later. Compatible with the iPhone and iPad.
Android	Works on 6.0 (Marshmallow) and later.
Linux	Works on Ubuntu 18.04, 20.04, and 22.04 (v3.1 and later), CentOS 8, and (Airwall only) Fedora 33.
Raspbian (Raspberry Pi)	Raspbian 9 (Stretch) or 10 (Buster)
RPi4/Ubuntu ARM64 (Raspberry Pi)	Raspbian 10 (Buster)

Microsoft Windows or Windows Server: Install and configure an Airwall Agent or Server

If you have received an email or activation code, see Link my Airwall Agent or Server to an Airwall secure network on page 14. If you need to install and configure manually, follow these instructions. You can get the Airwall Agent or Server for Windows from the administrator of your Airwall secure network, or download the latest installation files from Latest firmware and software on page 514. Once installed, you configure a profile on the Airwall Agent or Server to link to the Airwall secure network.

Note: You can start and stop the Airwall Agent or Server service as needed. Keep in mind when an Airwall Agent or Server service is stopped, you cannot connect to anything on the protected network.

To install and configure the Windows Airwall Agent or Server:

1. Log into your Windows computer as an administrator.
2. Download and install the Windows Airwall Agent or Server from Latest firmware and software on page 514.

   Note: If you are asked to install the TAP-Windows Provider as part of the installation procedure, click **Install** when prompted.
3. Once the installation is complete, the Airwall Agent or Server starts automatically.
4. Right-click the Tempered icon in the Windows System Tray
5. Select **Configure**
6. In the **Configure** window, do the following:
   a) Enter the IP address or host name of your Conductor. The default port setting is *8096*. If you have an activation code, enter it here.

      Note: The **Device ID**, **Overlay Device IP**, and **Overlay Netmask** fields are read-only and configurable from the Conductor.

   b) Click **OK**.

If you have used an Airwall Invitation or Activation code, once the Airwall Agent or Server is recognized by the Conductor, you should be able to start connecting to protected resources. If you are connecting manually, send your Device ID to your administrator so they can activate your account.

For information on using your Windows Airwall Agent or Server, see Connect with a Windows Airwall Agent or Server on page 27.

Note: You may need to stop and restart the Airwall Agent or Server to allow it to connect to the Conductor. Right-click the Tempered icon in the Windows System Tray and select **Stop** to suspend the service or **Start** to resume.

Unattended Windows installation of an Airwall Agent or Server

In v2.0 and above, you can install the Windows Airwall Agent or Server in unattended mode as an Administrator.

To do an unattended install of the Windows Airwall Agent or Server you use an .msi file. This method runs the regular installer in silent mode, allowing you to do a silent install through domain (GPO, SCCM).

Here's the recommended command to use to do the unattended install:

```
msiexec /i <msi_file> /l*v msi_out.log InvitationCode="<invite_code>"
 Conductor="<conductor_URL>"
```

For example:

```
msiexec /i AirwallAgent64-bit_UnattendedInstaller_2.2.11.333.msi /
l*v msi_out.log InvitationCode="575a52703294" Conductor="https://
my.conductor.com:8096"
```

Note: If you are not using DNS, you can replace the Conductor entry with its IP address. For example:

```
msiexec /i AirwallAgent64-bit_UnattendedInstaller_2.2.11.333.msi /
l*v msi_out.log InvitationCode="575a52703294"
 Conductor="https://192.168.56.2:8096"
```

Apple (OSX and macOS): Install and configure an Airwall Agent

If you have received an email or activation code, see Link my Airwall Agent or Server to an Airwall secure network on page 14. If you need to install and configure manually, follow these instructions. You must be an administrator of the computer to install and configure the Airwall Agent.

Note: Download the macOS/OSX installation files from the Software Downloads and Release Notes on page 514 Software Downloads section of Airwall help.

Important: In v2.2 and earlier, you may be required to install a TAP device driver. In earlier versions, the TAP driver's certificate may display a developer other than Tempered. If this occurs, you can safely click **Allow** and continue with your installation.

Once the installation is complete, the application starts automatically.

To install and configure manually:

1. To install the Airwall Agent locate the files you downloaded, double-click on them to run the installer, and follow the prompts.
2. Left-click the Tempered icon in the macOS menu bar.
3. Select **Configure**.
4. On the **Airwall Configuration** page, do the following:
   a) Select the plus (+) to add a new profile.
   b) Under **Conductor**, enter the IP address or host name of your Conductor.
   c) Under **Port**, use the default port setting of *8096*, unless your Airwall secure network administrator has told you to use a different port.
   d) If you have an Activation code, under **Invitation**, enter the code. If you do not have a code, copy down or screenshot your **Device ID** and send to your administrator to activate your account.

      Note: **Device ID**, **Overlay Device IP** and **Overlay Netmask** are read-only and configurable from the Conductor.

   e) Select **Save**.

If you have used an Airwall Invitation or Activation code, once the Airwall Agent is recognized by the Conductor, you should be able to start connecting to protected resources. If you are connecting manually, send your Device ID to your administrator so they can activate your account.

Note: You may need to stop and restart the Airwall Agent to allow it to connect to the Conductor. Left-click the Tempered icon in the menu bar and select **Stop Airwall** to disconnect or **Start Airwall** to connect.

For information on using your macOS Airwall Agent, see Connect with an Apple (OSX and macOS) Airwall Agent on page 19.

Perform an unattended macOS installation of an Airwall Agent

In v2.0 and above, you can perform a silent install on the Airwall Agent for macOS.

Note: This action requires administrator rights on the device.

To perform a silent install of the Mac client, from a terminal window, navigate to the location of the Airwall Agent installer package, and enter the command below:

```
sudo installer -pkg ./TemperedNetworksHIP.pkg -target /
```

Set your preferred network in the macOS Airwall Agent (HIPclient-OSX)

The macOS Airwall Agent (HIPclient-OSX) no longer uses the Network option, but instead automatically uses the network preferences on your macOS system settings.

Note: This action requires administrator rights on the device.

You can change the networks used by the agent by changing your macOS system settings.

Note: This setting is a system-wide setting, and affects network preferences for your entire mac system.

1. On your mac, click the WiFi icon, and select **Open Network Preferences**.
2. Under the list of available networks, click the gear icon, and select **Set Service Order**.
3. Drag the network options to set the network order you prefer, and then click **OK.**

2.2.3 macOS Airwall Agent Upgrade Instructions

If you have a previous version of the macOS/OSX Airwall Agent (formerly HIPclient) installed, follow these instructions to upgrade to 2.2.3:

Note: This action requires administrator rights on the device.

1. Check if you have this file on your Mac: /Applications/TemperedNetworksHIP.app. If not, you can upgrade as normal. If it is there, continue to step 2.
2. In your current Airwall Agent (HIPclient) menu, select **Configure**.
3. Note the Device ID and Conductor URL for each profile.
4. Go to the **About** menu, and select **Uninstall**.
5. Install the 2.2.3 macOS Airwall Agent.
6. Add a new profile for each of the Conductor URLs noted in Step 3. These new profiles will create new provisioning requests for each profile in the Conductor.
7. For the new profiles, a Conductor administrator needs to replace the old profiles with the new profiles. For more details, see Replace an Airwall Edge Service.

Apple iOS: Install and configure an Airwall Agent

If you have received an email or activation code, see Link my Airwall Agent or Server to an Airwall secure network on page 14. If you need to install and configure manually, follow these instructions. You can get the Airwall Agent for iOS from Apple's App Store.

Note: If you received an invite, follow the instructions in the email to install and configure your Airwall Agent. The instructions below are for manual installation and configuration.

1. Install the Airwall Agent on your device from the Apple Store: https://itunes.apple.com/US/app/id1233852249.
2. Open the Apple iOS Airwall Agent.
3. From the menu, tap **Profiles**. Tap + to add a new profile.

4. Give the profile a name, and fill in the Conductor URL (and port, if provided to you).
5. If you have an Airwall Invite Code, enter it at the bottom.
6. Tap **ADD**.

If you have used an Airwall Invitation or Activation code, once the Airwall Agent is recognized by the Conductor, you should be able to start connecting to protected resources. If you are connecting manually, send your Device ID to your administrator so they can activate your account.

For information on using your Apple iOS Airwall Agent, see Connect with an iOS Airwall Agent on page 21.

Android: Install and configure an Airwall Agent

If you have received an email or activation code, see Link my Airwall Agent or Server to an Airwall secure network on page 14. If you need to install and configure manually, follow these instructions. You can get the Airwall Agent for Android from the Google Play Store. Once installed, you configure a profile on the Airwall Agent to link to the Airwall secure network.

Note: If you receive an invite, follow the instructions in the email to install and configure your Airwall Agent. These instructions are for manual installation and configuration.

1. Install the Airwall Agent on your device from the Google Play store: https://play.google.com/store/apps/details?id=com.temperednetworks.hipclient
2. Open the Android Airwall Agent.
3. Add a new profile:
   - **v3.0 and later** – Scroll down to **Select Profile**, tap **MANAGE**, and then tap +.
   - **v2.2.12 and earlier** – From the menu, tap **Profiles**, and then tap +.
4. Give the profile a name, and fill in the Conductor URL (and port, if provided to you).
5. If you have an Airwall Invite Code, enter it.
6. Tap **ADD**.

If you have used an Airwall Invitation or Activation code, once the Airwall Agent is recognized by the Conductor, you should be able to start connecting to protected resources. If you are connecting manually, send your Device ID to your administrator so they can activate your account.

For information on using your Android Airwall Agent, see Connect with an Android Airwall Agent on page 22.

Linux: Install and configure an Airwall Server

If you have received an email or activation code, see Link my Airwall Agent or Server to an Airwall secure network on page 14. If you need to install and configure manually, follow these instructions. You can get the Airwall Server for your Ubuntu, Centos, or Fedora Linux server from the administrator for your Airwall secure network, or from Latest firmware and software on page 514. Once installed, you configure a profile on the Airwall Agent to link to the Airwall secure network.

Note:

- For pre-3.0 versions, replace `airsh` with `airctl`. See airctl Reference (pre-v3.0) on page 10.
- For pre-2.2.3 versions, see pre-2.2.3 help.

1. Install the Linux Airwall Server package for your version of Linux. If your secure network administrator has not provided you with a download, you can download the package you need from Latest firmware and software on page 514.
   - **For CentOS 7 or 8 or Fedora 3.3**: `sudo rpm -i <CentOS or Fedora install package>`
   - **For Ubuntu 16.04, 18.04, or 20.04**: `sudo dpkg -i <Ubuntu 16 or 18 package>`
2. Create a profile: `sudo airsh profile create name=<profile name> conductor=<conductor_url> [act=activation_code]`.

   You can optionally enter an Airwall Invitation activation code.
3. Make a profile the active one: `sudo airsh profile activate <profile name or number>`
4. Start the service: `sudo airsh service start`.

Note: If the service is already running, enter `sudo airsh service restart` to stop and start the service.

If you have used an Airwall Invitation or Activation code, once the Airwall Server is recognized by the Conductor, you should be able to start connecting to protected resources on the Airwall secure network. If you are connecting manually, send your Device ID to your administrator so they can activate your account.

For information on getting your Device ID, or using your Linux Airwall Server, see Connect with a Linux Airwall Server on page 26. For more Airshell commands, see Linux Airwall Server Airshell commands on page 372.

Linux Airwall Server or macOS Airwall Agent interface selection

The Linux Airwall Server and macOS Airwall Agent implement an interface auto-selection method. When you first install the Airwall Agent or Server, Linux or macOS determines the default gateway of the host and uses the associated network interface.

Note: Auto-selection is per profile.

Troubleshooting

If your macOS Airwall Agent is reporting as *online*, but does not seem to be working, check that the correct network interface is selected in the profile. See Set your preferred network in the macOS Airwall Agent (HIPclient-OSX) on page 80.

From Tkee: Linux agent conforms to the Gateway link manager operational rules. airsh currently does not have the ability to select the preferred uplink. Conductor is the method for selecting interfaces by port group weights. Short on details, the Gateway documentation might serve as a basis. Ticket to fill this in CD-412.

Connect to an Airwall secure network

Once you have installed and linked your Airwall Agent or Server, you can then start and stop it at any time to connect and disconnect from the Airwall secure network.

Note:

- You can use your Airwall Agent or Server to connect to other Airwall secure networks. Just set up a new profile for each one you need to connect to. For information on how, see Create or Edit Airwall Agent or Server Profiles on page 29
- The Airwall Agent or Server does not disable the wired or wireless interfaces of your device. For example, if you are running an Airwall Agent, you can at the same time be connected to the Internet wirelessly and the corporate network via a wired connection.

Allow an Airwall Agent or Server to access your Airwall secure network

When a person configures an Airwall Agent or Server with your Conductor IP address or hostname, and are online with access to the **Conductor**, their Airwall Agent or Server will appear in the Conductor. How they appear depends on how they've connected:

- If they've activated their Airwall Agent or Server with an Airwall Invitation or Activation code, their Airwall Agent or Server is provisioned and configured as you specified when you set up the invitations or activation codes. You just need to license their Airwall Agent or Server and they will have access to the secure network.
- If the person is connecting manually, you get a provisioning request to allow the Airwall Agent or Server into your secure network. You need to provision and licensed the Airwall Agent or Server, and then add the person's device to the overlay networks and Add and remove device trust on page 427 for the resources they need access to.

CAUTION: When you're accepting provisioning requests, make sure that you know who is connecting and they are authorized to access your network.

If you need to revoke an Airwall Agent or Server, you can also disable trust in one click. For more information, see Revoke and Reactivate an Airwall Edge Service on page 496. Open the **Visualization** tab on an overlay network to get a visual view of trust relationships.

Note: You can also automate Airwall Agent trust using the API. The most recent API documentation is available in your Conductor. See Airwall API on page 508.

Assign Separate DNS Servers to Airwall Agents and Servers

If you need Airwall Agents and Servers to use different DNS servers, you can assign different DNS servers on an overlay or individually for Airwall Agents and Servers that support it.

Supported Versions

Supported Versions	v2.2.11 and later Conductor, and v2.2.11 and later and Airwall Agents and Servers on platforms that support setting DNS servers (currently macOS, Windows, and Linux). iOS and Android support the global DNS server setting.
Required Role	• System or network administrators • Permissions to edit the Airwall Agents and Servers or Overlay where you're updating the settings.

Bulk editing supports setting DNS servers on Airwall Agents and Servers.

DNS Setting Priority

The Conductor has a global DNS setting that applies to all Airwall Agents and Servers on your Airwall secure network. You can override the global setting on individual Airwall Agents and Servers, or on an Overlay to apply the DNS setting to all Airwall Agents and Servers that support it on the Overlay.

Here's how the priority is set on DNS settings:

DNS Setting Priority	Result
1 – Airwall Agents and Servers	• Overrides the global Conductor DNS server setting. • Can be appended to with DNS Servers set on the Overlay. • Only available on platforms that support the DNS setting (currently iOS, macOS, Windows, and Android). • Will not fall back to the global DNS server setting.
2 – Overlay	• Overrides the global Conductor DNS server setting. • DNS servers set on the overlay are appended to the end of the DNS Server list set on individual Airwall Agents and Servers. • Only applies to Airwall Agents and Servers in the Overlay that support the DNS Server setting.
3 – Conductor Global	• Applies to Airwall Agents and Servers that both support the DNS setting, and don't have a DNS setting on an Overlay or individually. • Is overridden by both Overlay or per-Airwall Agent or Server settings.

Note: MacOS DNS Settings – MAC DNS settings only operate on DHCP interfaces. If your underlay is a static IP, no DNS settings will be applied. At product startup and normal shutdown, DHCP interfaces are returned to DHCP DNS defaults.

Note:

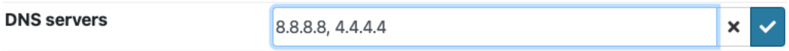
The DNS SRV record covered in Connect an Airwall Gateway with a DNS SRV record on page 294 is only used for specifying a Conductor URL when deploying Airwall Gateways, and is not related to the DNS Server specified in Conductor settings.

Set DNS servers on an Airwall Agent or Server

This option is only available on v2.2.11 or later Airwall Agents and Servers on platforms that support setting DNS servers, currently macOS, Windows, and Linux.

1. In Conductor, go to **Airwalls**, and open the page for the v2.2.11 or later Airwall Agent or Server for which you want to set the DNS servers.
2. On the **Airwall agent** tab, scroll down to the **DNS servers** line.

   Note: If the option is not available, it's not supported on that platform or version.
3. Click the **DNS servers** line to edit.
4. Enter DNS Server IP addresses, separated by commas. For example, enter `8.8.8.8, 4.4.4.4`.



DNS servers 8.8.8.8, 4.4.4.4

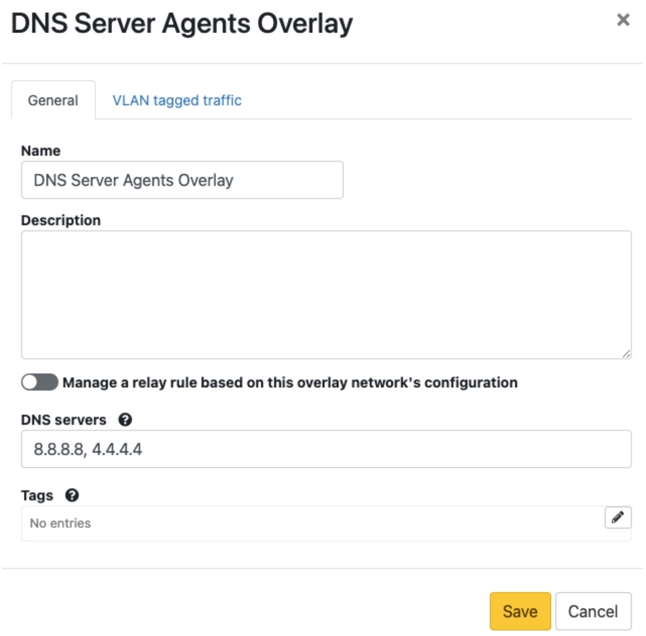
5. Select the check mark to save or the **X** to cancel.

The Airwall Agent or Server now uses the specified DNS servers when connected to the Conductor.

Set DNS servers on an Overlay

Set the DNS servers for all v2.2.11 or later Airwall Agents and Servers in an Overlay that support setting DNS servers.

1. In Conductor, go to an Overlay that has Airwall Agents and Servers for which you want to set DNS servers.
2. On the right, next to **Info**, select **Edit Settings**.
3. Under **DNS servers**, enter DNS Server IP addresses, separated by commas. For example, enter `8.8.8.8, 4.4.4.4`.



DNS Server Agents Overlay

Name
DNS Server Agents Overlay

Description

○ **Manage a relay rule based on this overlay network's configuration**

DNS servers
8.8.8.8, 4.4.4.4

Tags
No entries

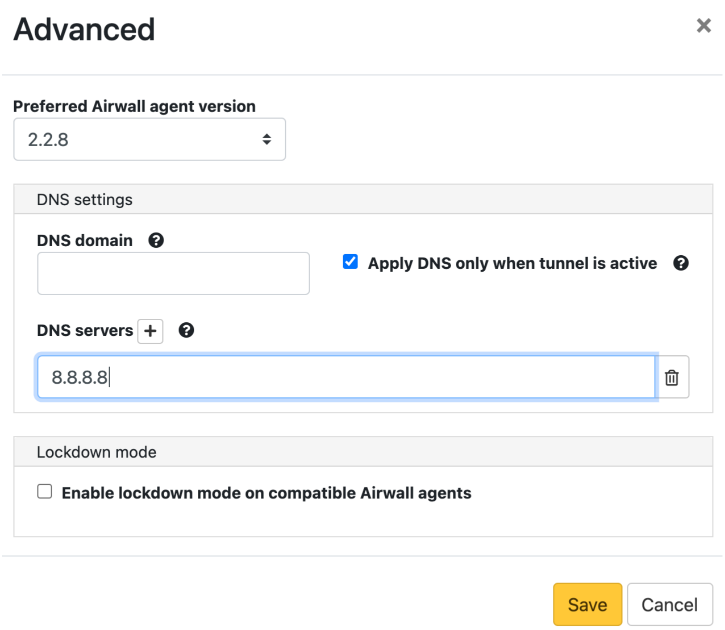
4. Select **Save**.

The Airwall Agents and Servers on the Overlay that support setting the DNS server now use the specified DNS servers when connected to the Conductor.

Set DNS servers globally in Conductor settings

You can set DNS servers globally in Conductor Settings.

1. In Conductor, open **Settings** and scroll down to **Advanced** > **Global Airwall agent settings**.
2. Select **Edit Settings**.
3. Next to **DNS servers**, select the plus sign (+) and add the DNS servers you want Airwall Agents and Servers to use.



Advanced

Preferred Airwall agent version: 2.2.8

DNS settings

DNS domain:

☑ Apply DNS only when tunnel is active

DNS servers: 8.8.8.8

Lockdown mode

☐ Enable lockdown mode on compatible Airwall agents

4. If you want to only apply these DNS settings when the DNS servers have an active tunnel, check the **Apply DNS only when tunnel is active** box. See details for this option below.

   Note: This setting is currently only supported on the macOS Airwall Agent.

5. If desired, enter the **DNS domain** for Airwall Agent overlay DNS Searches. If an Agent is using a per-Agent or Global DNS setting, this global DNS search domain is used (there is no per-agent search domain.)
6. Select **Save**.

The Airwall Agents and Servers that support setting the DNS server now use the specified DNS servers when connected to the Conductor.

Details for the **Apply DNS only when the tunnel is active** Setting

The Apply DNS only when the tunnel is active setting does the following:

- If active, DNS is changed to the DNS servers (and search domain) set on the Global DNS settings.
- If no active DNS servers are found, DNS is returned to the DHCP server defaults.
- If an agent DNS is configured (and not available), the global settings are not used.

Note: The DNS servers are pinged at intervals (about half the session expiration time). If a ping brings the tunnel back up, the DNS server setting is applied. If the tunnel goes down, the DNS servers are retested, and DNS returns to the DHCP setting if no servers can be reached. If a tunnel comes up, DNS servers are retested, and it returns to the DNS server setting if at least one of the DNS servers in the list is up.

Note: If you’ve set separate per-Agent DNS servers and they fail, the agents do not fall back to the global DNS setting.

Automate the Airwall Agent or Server and Airwall Server using the API

Troubleshoot the Airwall Agent and Airwall Server

Follow the instructions below to resolve problems you may encounter using the software.

The Airwall Agent is not connected.

- Determine if the Conductor IP is configured. Follow the steps in the configuration section above.
- Verify that the Airwall Agent has not been given a certificate. Your administrator must grant a license in the Conductor. See the Conductor and Airwall Edge Service Administrator Guide for more information.

The Airwall Agent cannot contact a protected device

Configure the peer Airwall Gateway with an overlay network IP address and reestablish trust.

Set up an Airwall Relay to Route Encrypted Connections

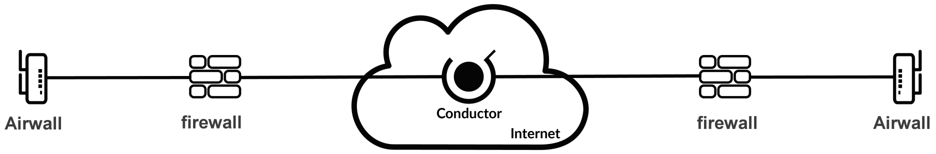
An Airwall Relay routes encrypted Airwall Edge Service connections across all networks and transport options, without modifying the underlying network, for secure end-to-end connectivity.

Supported on these Airwall Gateways:

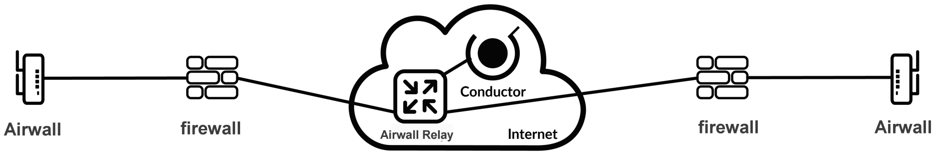
- **Physical** – 300 Series, 400 Series, and 500 Series
- **Virtual** – 300v on VMware ESXi, Hyper-V, RackSpace, Xen, and XenServer
- **Cloud** – 300v on Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and Alibaba Cloud.

With an Airwall Relay in place, you can dynamically and easily network any device or group of devices across any public, private or hybrid network, including subnets that are located on separate underlays. The Airwall Relay brokers connections between Airwall Edge Services, based on policies set by the Conductor.

In the illustration below, two Airwall Gateways exist in different underlays. Each Airwall Gateway can connect to the Conductor, publish their IP addresses, and come online. However, communication between the two cannot occur as both Airwall Gateways do not have publicly available IP addresses.

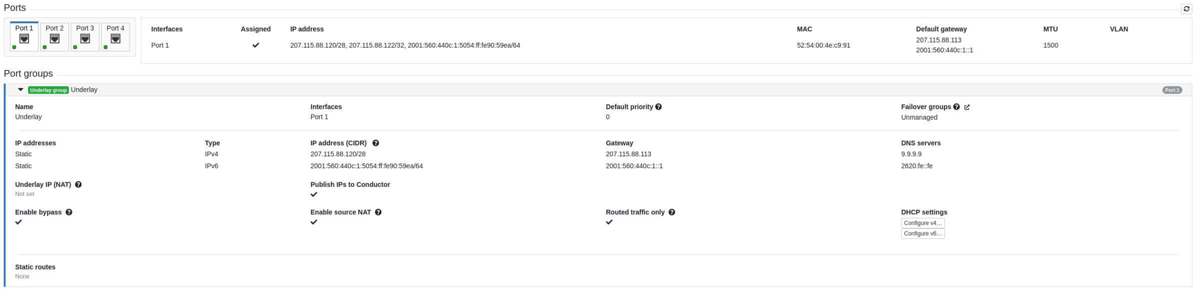


To solve this limitation, add an Airwall Gateway acting as an Airwall Relay. In the Conductor, the Airwall Relay acts as a broker between the two Airwall Gateways.



Note: To set an Airwall Gateway up as an Airwall Relay, you must have an Airwall Relay license.

Note: If you have Airwall Agents or Airwall Gateways that are only getting a IPv6 address on cellular, and you want to connect to other Airwall Edge Services on IPv4, you need to have a relay policy set up on a dual stack (IPv4 + IPv6) Airwall Relay. To do this, set both IPv4 and IPv6 IP addresses on the same underlay on the Airwall Relay, and enable bypass:



Ports

Interfaces	Assigned	IP address	MAC	Default gateway	MTU	VLAN
Port 1	✓	207.115.88.120/28, 207.115.88.122/32, 2001:560:440c:1:5054:ff:fe90:59ea/64	52:54:00:4e:c9:91	207.115.88.113 2001:560:440c:1::1	1500	

Port groups

Underlay group Underlay

Name: Underlay
Interfaces: Port 1
Default priority: 0
Failover groups: Unmanaged

IP addresses	Type	IP address (CIDR)	Gateway	DNS servers
Static	IPv4	207.115.88.120/28	207.115.88.113	9.9.9.9
Static	IPv6	2001:560:440c:1:5054:ff:fe90:59ea/64	2001:560:440c:1::1	2620:fe::fe

Underlay IP (NAT): Not set
Publish IPs to Conductor: ✓
Enable bypass: ✓
Enable source NAT: ✓
Routed traffic only: ✓
DHCP settings:

Static routes: None

Set Up an Airwall Relay

You can set up a compatible Airwall Gateway as an Airwall Relay to route encrypted traffic on your network.

You must have an available Airwall Relay license to complete these instructions. For help with licensing, see How Airwall Licensing Works on page 191.

1. In the Airwall Conductor, open the Airwall Gateway you want to act as an Airwall Relay.
2. On the **Airwall gateway** tab, select **Edit Settings**.
3. Under **Advanced Settings**, check **Allow Airwall to act as an Airwall relay**.
4. Select **Update Settings**.
5. Configure Airwall Relay rules on page 353 for that relay (or add to a group of relays that has policy set up).

Note: Setting an Airwall Gateway as an Airwall Relay automatically uses an available Airwall Relay license. If no licenses are available, you receive an error message.

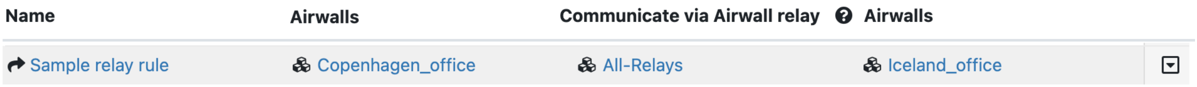
Configure Airwall Relay rules

Configure Airwall Relay rules to establish secure connections between Airwall Edge Services that cannot directly connect.

You must have permission to edit policy for all of the Airwall Edge Services you are adding to the relay rules.

Note: You can also Set an Overlay to Automatically Manage Relay Rules on page 354.

1. In the Conductor, go to **Airwalls** and open **Airwall relay rules**.
2. Select **New relay rule** (before v3.0 Conductors: **Create rule**), name the rule, provide a description, and select **Create**. The relay rule is added to the relay rule table.
3. Scroll down in the table to find the rule you created.
4. Hover over the Communicate via Airwall relay column, select the edit icon ✎, and then pick the Airwall Relay or Airwall Relay group you want to create a rule for. Select **Save**.



Name	Airwalls	Communicate via Airwall relay	Airwalls
Sample relay rule	Copenhagen_office	All-Relays	Iceland_office

5. Optional: If you have already set up your Conductor to run as a relay, you can use it in relay rules by clicking the edit icon ✎ and checking **Use Conductor as an Airwall Relay**. For more information, see Run the Conductor as an Airwall Relay on page 354.
6. Under the **Airwalls** column to the left, select the Airwall Edge Services or groups in one area that you want to connect with the relay. Select **Save**.
7. Under the **Airwalls** column to the right, select the Airwall Edge Services or groups in another area that you want to connect with the relay. Select **Save**.
8. You can continue adding rules to connect any Airwall Edge Services that require an Airwall Relay to communicate.

Note: Managed relay rules do not normally display on the **Airwalls**>**Airwall relay rules** tab. If you want to see them, you can go to **Airwalls** > **Airwall relay rules** and at the top right, check **Display system relay rules**.

Set an Overlay to Automatically Manage Relay Rules

You can easily manage the relay rules for an overlay by setting it to automatically create relay rules that allow the trust relationships in the overlay.

Supported Versions	Conductor 2.2.10 and later
Required Roles	System administrators Network administrators with permissions to the overlay

Note: You must first set up an Airwall Relay before you can enable automatic relay rules.

You can also configure Airwall Relay rules manually. See Configure Airwall Relay rules on page 353.

1. Open the overlay you want to automatically manage your relay rules.
2. Under **Info** on the right sidebar, select **Edit Settings**.
3. On the **General** tab, enable the **Manage a relay rule based on this overlay network's configuration** option.
4. Choose the Airwall Relays or Airwall Relay groups that you want this overlay to use.
5. Select **Save**.

The overlay creates relay rules that allow communication between all Airwall Edge Services in the overlay. Note that you still need to set up device to device trust for them to communicate.

Note: Airwall Edge Services try to connect directly first, and only use the relay if they cannot connect directly.

Note: Managed relay rules do not normally display on the **Airwalls** page. If you want to see them, you can go to **Airwalls** > **Airwall relay rules** and at the bottom right, check **Display system relay rules**.

Run the Conductor as an Airwall Relay

For small to moderate Airwall secure networks, it may make sense to run your Conductor as a relay, rather than having a separate Airwall Relay. Since Airwalls must all be able to reach the Conductor, using it as an Airwall Relay simplifies your deployment.

For cloud deployments, a Conductor relay also reduces costs because it requires fewer instances and saves an elastic IP.

Supported versions	v3.1.0 Conductor v2.2 or later Airwall Gateways

Before you begin

To run your Conductor as a relay, you need:

- Conductor license
- Airwall Relay license

Important: If you use the Conductor as a relay on a busy overlay network, it may impact the performance of the overlay network. if you require more than 100 concurrent tunnels, you should consider deploying dedicated Airwall Gateways as relays.

Note: You can use the Conductor as a relay in addition to having dedicated Airwall Gateway relays.

Set up your Conductor as an Airwall Relay

1. Go to **Settings** > **General Settings**.
2. Under **Orchestration Settings** > **Airwall-Airwall Conductor networking**, select **Edit Settings**.
3. Under **Conductor HIP settings** check **Allow using this Conductor as an Airwall Relay**.
   - Conductor version 3.2.3 and earlier: check **Allow using this Conductor as an Airwall Relay**.

  - Conductor version 3.3.0 and later: check **Enable HIP on Conductor**, then check **Allow using this Conductor as an Airwall Relay**.

4. Select **Save**.
5. On the **Airwall Conductor Reboot** page, select **Reboot**.
6. Allow the Conductor to finish rebooting.
   You can now use the Conductor relay in an overlay and in relay rules. For more information, see Use a Conductor relay in an Overlay on page 355 and Configure Airwall Relay rules on page 353

If you need to monitor relay sessions, see Monitor Relay Sessions on page 355.

Use a Conductor relay in an Overlay

Once you've configured the Conductor to allow it acting as a relay, you can use it in an overlay.

1. Open or create an overlay where you want the Conductor to act as an Airwall Relay.
2. On the overlay, set up device trust as desired.
3. On right side **Info** tab, under **Managed relay**, toggle to **Enabled**.
4. Check **Use Conductor as an Airwall Relay**.
5. You can also select other relays if you have configured additional Airwall Gateways to be used as relays.

Monitor Relay Sessions

You can monitor how your Airwall Relays are doing for troubleshooting or diagnostics. This monitor includes sessions for the Conductor acting as a relay.

1. Go to **Settings** > **Diagnostics**.
2. Go to **Active relay connections on this Conductor** and select **Update data**to see detailed information about ongoing relay sessions.

Deploy a cloud Airwall Server

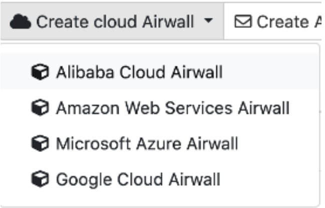
You can deploy an Airwall Server on a cloud provider, which gives you a Windows Server machine with an Airwall Server installed and configured to connect with your Conductor.

To deploy a cloud Airwall Server, you need to first do the following:

- Set up an Alibaba Cloud, AWS, Microsoft Azure, or Google Cloud account as a cloud provider on your Conductor. See Set up Cloud Providers on page 433
- Add one or more supported Linux or Windows server VM images to your cloud provider account. See your cloud provider help for instructions. See Operating system requirements for Airwall Agents and Servers on page 7.
- If you want to automate the provisioning and licensing of the Airwall Server, create an Activation code for it, and enter the code when creating the server.

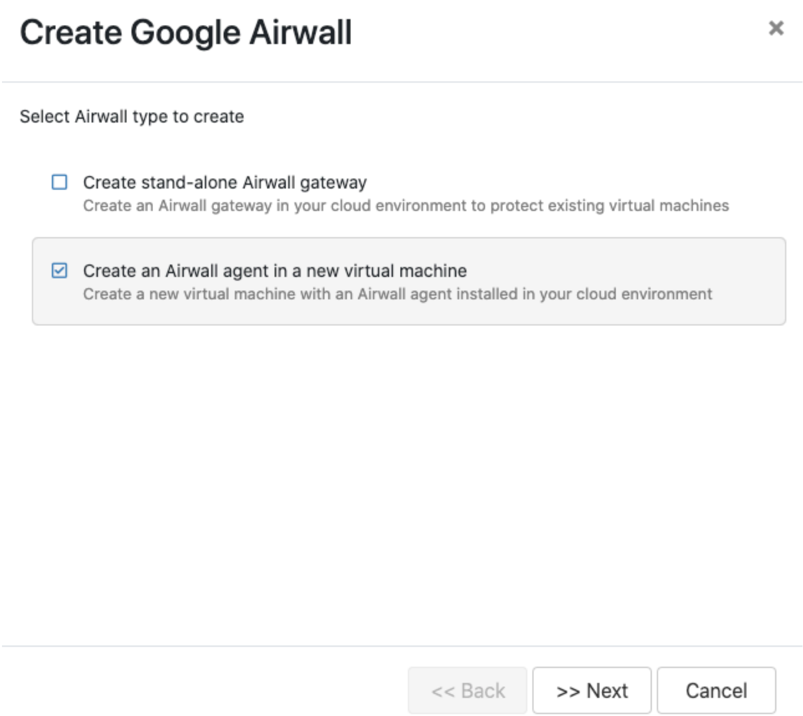
Here's how to deploy an Airwall Server to your cloud provider:

1. On the **Airwalls** page, (or in Conductor **Settings**, under **Cloud providers**), click **Create cloud Airwall**, and select your cloud provider Airwall.



Note: This procedure uses screenshots for Google Cloud, but the process is the same for other cloud providers.

2. Select **Create an Airwall agent in a new virtual machine**, and select **Next**.



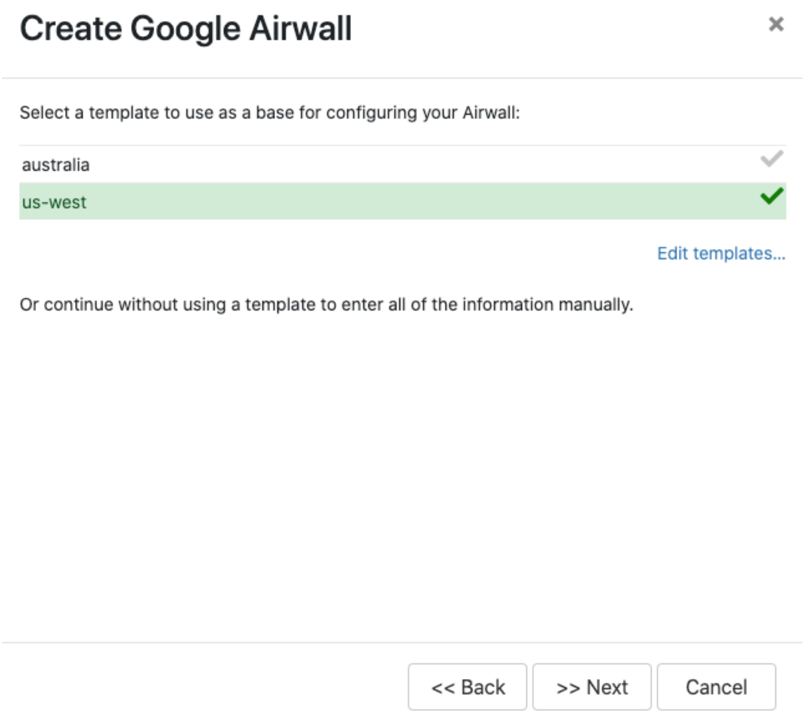
Create Google Airwall

Select Airwall type to create

□ Create stand-alone Airwall gateway
Create an Airwall gateway in your cloud environment to protect existing virtual machines

☑ Create an Airwall agent in a new virtual machine
Create a new virtual machine with an Airwall agent installed in your cloud environment

3. Select a template, if desired, and then select **Next**.



Create Google Airwall

Select a template to use as a base for configuring your Airwall:

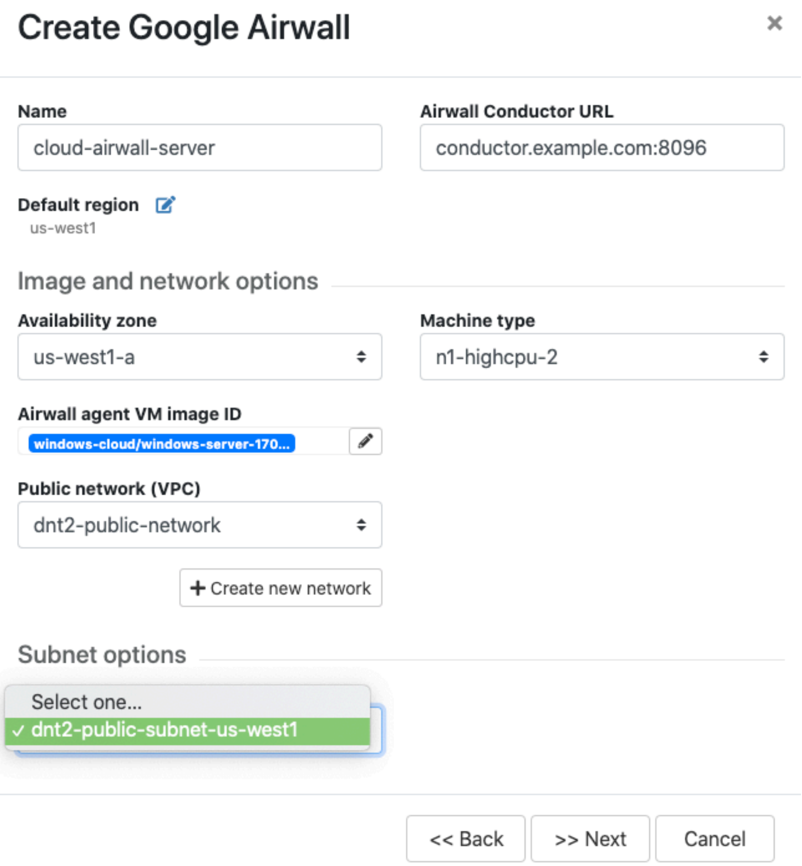
australia ✓
us-west ✓

Edit templates...

Or continue without using a template to enter all of the information manually.

To continue without a template and enter the information manually, just select **Next**.

4. Give the Airwall Server a descriptive name. If you've used a template, you can skip to the next step.
   a) If you are filling in information manually, or want to change the template, fill in the **Name** and the **Image and network options**. For **Machine type**, the default typically works. You can select a different size if needed for your purposes.



Create Google Airwall

Name: cloud-airwall-server

Airwall Conductor URL: conductor.example.com:8096

Default region: us-west1

Image and network options

Availability zone: us-west1-a

Machine type: n1-highcpu-2

Airwall agent VM image ID: windows-cloud/windows-server-170...

Public network (VPC): dnt2-public-network

Subnet options

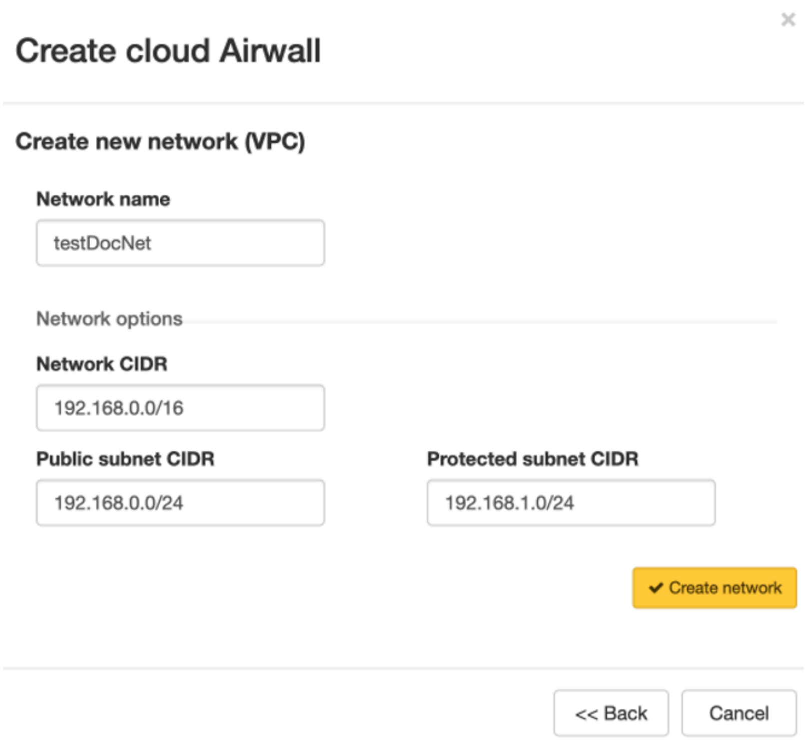
Select one...
✓ dnt2-public-subnet-us-west1

b) Under **Airwall agent VM image ID**, pick the type of server you want to create. The list populates with supported Linux and Windows server virtual machine images available on your cloud provider.

c) If you do not have a pre-configured virtual network, you need to create a new network. Click **Create new network** and fill in the form:

- **Network CIDR** – Enter an available network address and subnet mask in CIDR notation.
- **Public subnet CIDR** – Must be a subnet of the main network. Traffic flows between the underlay interface of the Airwall Gateway and the Public IP address object in Azure.
- **Protected subnet CIDR** – Must be a subnet of the main network. Traffic must pass through theAirwall Gateway or through manually-crafted routes.

When you're finished entering the information, click **Create network**, and when processing is complete, click **Back**.



Create cloud Airwall

Create new network (VPC)

Network name: testDocNet

Network options

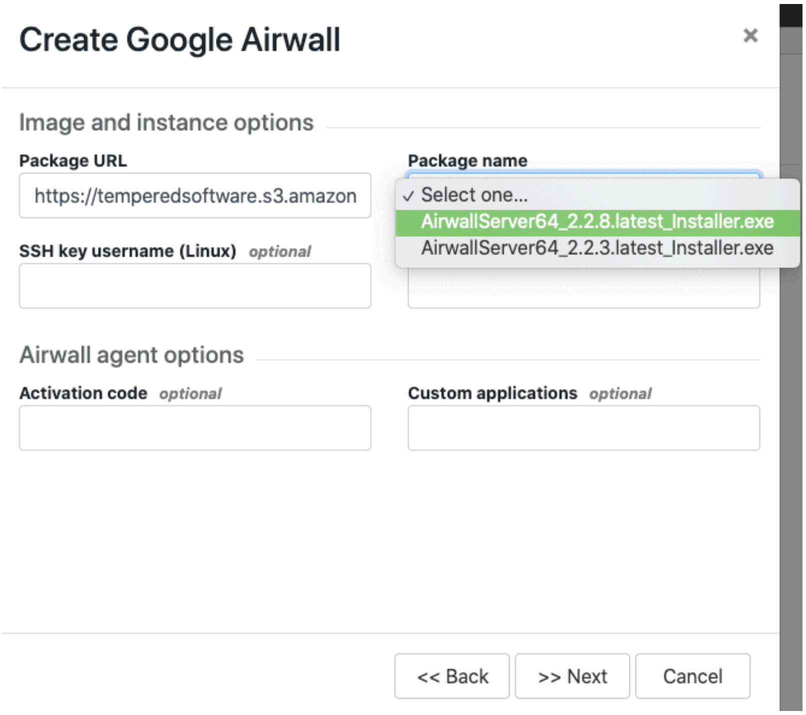
Network CIDR: 192.168.0.0/16

Public subnet CIDR: 192.168.0.0/24

Protected subnet CIDR: 192.168.1.0/24

d) Back on the **Create cloud Airwall** page, select the network and public and protected subnets.

5. Click **Next**.
6. Select the package name for the Airwall Server you want to install on the cloud server virtual machine. The package name shows the packages available at the Package URL, which defaults to the Tempered release location.



Create Google Airwall

Image and instance options

Package URL: https://temperedsoftware.s3.amazon

Package name: ✓ Select one... / AirwallServer64_2.2.8.latest_Installer.exe / AirwallServer64_2.2.3.latest_Installer.exe

SSH key username (Linux) *optional*

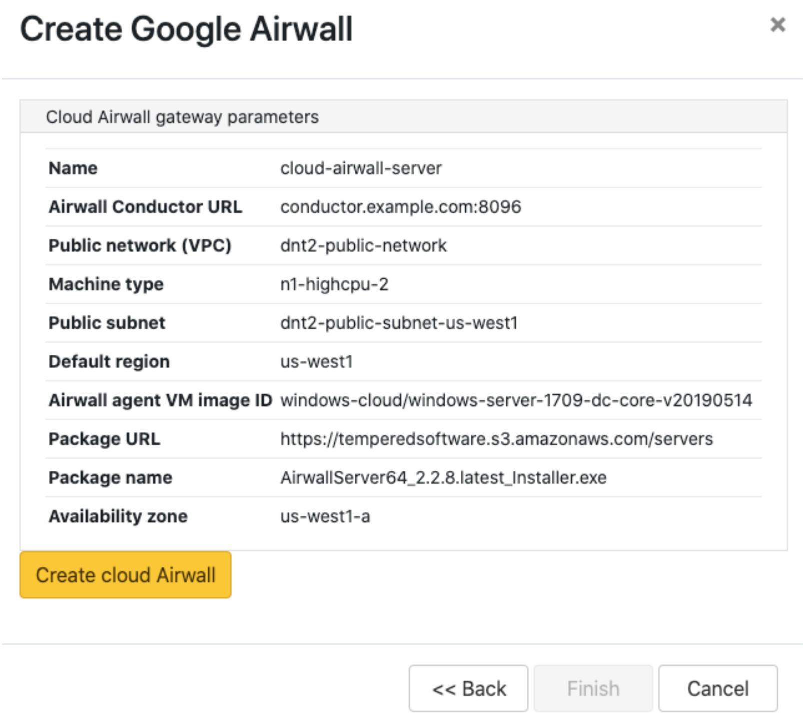
Airwall agent options

Activation code *optional*

Custom applications *optional*

7. If you have an Activation code for the Airwall Server, enter it under Activation code. You can also install custom applications.
8. Click **Next**.

9. Check the summary of your choices. If everything is correct, click **Create cloud Airwall**.



Create Google Airwall

Cloud Airwall gateway parameters

Name	cloud-airwall-server
Airwall Conductor URL	conductor.example.com:8096
Public network (VPC)	dnt2-public-network
Machine type	n1-highcpu-2
Public subnet	dnt2-public-subnet-us-west1
Default region	us-west1
Airwall agent VM image ID	windows-cloud/windows-server-1709-dc-core-v20190514
Package URL	https://temperedsoftware.s3.amazonaws.com/servers
Package name	AirwallServer64_2.2.8.latest_Installer.exe
Availability zone	us-west1-a

10. Click **Finish**. It may take up to 5 minutes for your cloud provider to create the Airwall Server.

You've completed creating an Airwall Server on your cloud provider, and may need to provision, License, and configure it. For help, see Provision and License Airwall Edge Services on page 193 and Configure Airwall Edge Service Settings on page 359.

Configure Airwall Edge Service Settings

Edit Airwall Edge Service settings on **Airwalls** page.

1. Go to **Airwalls**.
2. In the table, select the drop-down to the right of the Airwall Edge Service you want to edit, and select **Properties**.
3. Click **Edit Settings**. You can change the following information:

Basic Settings

- **Name**: A user-friendly name for the Airwall Edge Service.
- **Description**: An optional field for additional information about the Airwall Edge Service.
- **Location**: An optional field for information of about the Airwall Edge Service location.

Advanced Settings

- **Network policy communications**: Enable or disable communication with the Airwall Edge Service.
- **Shared network public IP address (NAT)**: If the Airwall Edge Service has a public IP address on the Internet, enter it here. Remote Airwall Edge Services can use this address to connect to the Airwall Edge Service.

- **Enable auto-connect**: If enabled, the Airwall Edge Service securely connects to peer Airwall Edge Services without the presence of device traffic.

4. When finished, click **Update Settings**.

Manage Cloud Airwall Gateway Virtual Machines on page 98
You can do several management tasks for the virtual machines that host cloud Airwall Gateways from the Conductor.

Set a Private APN for your Cellular Provider on an Airwall Gateway on page 378
You can set the APN of the cell modem on an Airwall Gateway (100, 110, 150, 250) on the Airwall Gateway from Diagnostic mode or using `airsh`, or from the Conductor.

Airshell Command Line

The Airshell command line allows you to manage certain aspects of Airwall Gateways and Airwall Servers from the command line.

Airshell Common Commands

For Airwall Gateways that have a console port, you can deploy and configure the Airwall Gateway with the **Airshell** (airsh) command-line interface. You can deploy & configure an Airwall Gateway directly without going into diagnostic mode.

Connect a computer to the console port on the back of the Airwall Gateway or Conductor hardware, and use a terminal (macOS, Linux) or terminal emulator (Windows) to open the console. See the platform guide for your Airwall Gateway for specific connection instructions.

At the console:

- v2.2.8 and later: log in with name: `airsh`, and no password
- v2.2.5 and earlier: log in with name: `airsh`, and password: `airsh`.

You can then enter commands at the `airsh»` prompt.

For the full reference of command-line commands, see Airshell Command Line on page 360.

No Default Password in v2.2.8 and later

Starting with v2.2.8, the Airshell console default login has no default password. If you are concerned about securing physical access to Airshell, set a password by entering conf password and following the prompts to set and confirm a new password. Keep this password in a secure location, as it cannot be recovered. This password is only for Airshell physical console access and is not used when you access Airshell remotely.

⚠ **CAUTION:** If this password is lost, you will need to do a factory reset to clear the password.

Common Airwall Gateway Commands

`help [command]`	Show help for the specified command.
`help [tree]`	List available commands. Use `help tree` to list available commands with their options.
`setup-ui`	Open the setup wizard to set up an Airwall Gateway. See Configure an Airwall Gateway with the airsh Setup Wizard on page 274.
`conf network`	**v2.2.10 and later** – Configure port groups, see Configure Port Groups with Airshell on page 376. For example:

to modify port group (pg) 2 with an IP of 192.168.1.1/24, enter:

```
conf net modify pg=2
 ip=192.168.1.1/24
```

v2.2.8 and earlier – Set up static IP addresses.

`conf net list`

Display a list of port groups and their configured options.

`ping`

Test network connectivity

`status`

See Airwall status:

- **Hostname** – Shows the Airwall Gateway's identity used when it connects to the Conductor. You use this name to confirm the provisioning request from the Airwall Gateway.
- **HIT** – The Host Identity Tag is a hash of the Airwall Gateway's Host Identity, the public key identifier. This IPv6-like identifier is used for secure communication.
- **LSI** –The Local Scoped Identifier is a shortened IPv4 version of the HIT, used for secure communication.
- **Device cert.** – Present indicates the presence of a device certificate, which means the Airwall Gateway has been provisioned by the Conductor.
- **Device key** – Present indicates the presence of the device identity private key.
- **Keystore** – Indicates where the device identity private key is stored: TPM, Operating System, or file-based keystore.
- **Annunciator** – Displays the status of the annunciator. On some models this affects LEDs and/or LCD display.
- **Run mode** – Indicates the mode the Airwall Gateway is running in:
  - **Protected** – Normal operation mode.
  - **Transparent** – Running with non-encrypted bridging.
  - **Diagnostic** – In diagnostic mode.
  - **Factory reset** – In factory reset mode.
  - **HA primary/secondary/active** – Indicates the High Availability role of the Airwall Gateway.
- **Conductor** – See status of the connection to the Conductor. For more details, see `status conductor` below.
- **IP address** – Shows the active IP addresses for this Airwall Gateway. An IP address displayed in green indicates it has been selected as active.

`status conductor`

Shows the status of the Airwall Edge Service's connection to the Conductor. Disconnected indicates the Airwall Edge Service is not connected to the Conductor.

Note: For Airwall Agents and Servers that support it, if Disconnected mode is On, you can still access resources on the Airwall secure network, and your Airwall Agent or Server will reconnect at intervals for configuration and trust policy updates. If you want to reconnect manually, use `conductor sync`.

`conductor set`

Set or remove a Conductor IP address or URL and port (optional). For example: `conductor set my-conductor.tempered` or just `conductor set` to remove.

`conductor sync`

If an Airwall Agent or Server is set to Disconnected mode on the Conductor, this command manually reconnects to retrieve any changes to configuration or trust policies. In Disconnected mode, you can still access resources on the Airwall secure network. See Sync an Airwall Agent or Server in Disconnected Mode on page 29.

`diag`

Put the Airwall Gateway in diagnostic mode

`factory-reset [keep-networking|clear-identity]`

Reset Airwall Gateway back to factory default settings.

- Use the keep-networking option to preserve the network configuration.
- Use clear-identity to remove the device identity and licensing, and to re-license the Airwall Gateway.

If you want to preserve the network configuration, use the keep-networking option:

```
airsh>> factory-reset keep-
networking
```

`exit` or **`quit`**

Exit Airshell

`history`

See the history of commands entered into Airshell. Enter `history clear` to delete history.

`color on|off`

Turn on or off color on the text output from the serial console.

`reboot`

Restart the Airwall Gateway.

`shutdown`

Shut down the Airwall Gateway.

Airshell (`airsh`) Command Reference

For Airwall Gateways that have a console port, and for Linux Airwall Servers you can deploy and configure them with the Airshell (`airsh`) command-line interface. It provides tab-completion, inline help, and the ability to deploy and configure directly without going into diagnostic mode.

Get started

Connect a computer to the console port on the back of the Airwall™ or Conductor hardware, and use a terminal (macOS, Linux) or terminal emulator (Windows) to open the console. See the platform guide for your Airwall for specific connection instructions.

To access Airwall Gateways with `airsh` remotely, see Set up Remote Access to Airshell via SSH on page 374.

At the console:

- v2.2.8 and later: log in with name: `airsh`, and no password
- v2.2.5 and earlier: log in with name: `airsh`, and password: `airsh`.

You can then enter commands at the `airsh»` prompt.

Note: See also Linux Airwall Server Airshell commands on page 372.

Advantech Note: To configure an Advantech machine, you can put it into diagnostic mode. See Put an Airwall Gateway into diagnostic mode on page 478.

No Default Password in v2.2.8 and later

Starting with v2.2.8, the Airshell console default login has no default password. If you are concerned about securing physical access to Airshell, set a password by entering conf password and following the prompts to set and confirm a new password. Keep this password in a secure location, as it cannot be recovered. This password is only for Airshell physical console access and is not used when you access Airshell remotely.

CAUTION: If this password is lost, you will need to do a factory reset to clear the password.

Common Commands

`help [command]`	Show help for the specified command.
`help [tree]`	List available commands. Use `help tree` to list available commands with their options.
`setup-ui`	Open the setup wizard to set up an Airwall Gateway. See Configure an Airwall Gateway with the airsh Setup Wizard on page 274.

`conf network`	**v2.2.10 and later** – Configure port groups, see Configure Port Groups with Airshell on page 376. For example: to modify port group (pg) 2 with an IP of 192.168.1.1/24, enter:
	`conf net modify pg=2`
	`ip=192.168.1.1/24`
	v2.2.8 and earlier – Set up static IP addresses.

`conf net list`	Display a list of port groups and their configured options.
`ping`	Test network connectivity
`status`	See Airwall status: • **Hostname** – Shows the Airwall Gateway's identity used when it connects to the Conductor. You use this name to confirm the provisioning request from the Airwall Gateway. • **HIT** – The Host Identity Tag is a hash of the Airwall Gateway's Host Identity, the public key identifier. This IPv6-like identifier is used for secure communication. • **LSI** –The Local Scoped Identifier is a shortened IPv4 version of the HIT, used for secure communication.

- **Device cert.** – Present indicates the presence of a device certificate, which means the Airwall Gateway has been provisioned by the Conductor.
- **Device key** – Present indicates the presence of the device identity private key.
- **Keystore** – Indicates where the device identity private key is stored: TPM, Operating System, or file-based keystore.
- **Annunciator** – Displays the status of the annunciator. On some models this affects LEDs and/or LCD display.
- **Run mode** – Indicates the mode the Airwall Gateway is running in:
  - **Protected** – Normal operation mode.
  - **Transparent** – Running with non-encrypted bridging.
  - **Diagnostic** – In diagnostic mode.
  - **Factory reset** – In factory reset mode.
  - **HA primary/secondary/active** – Indicates the High Availability role of the Airwall Gateway.
- **Conductor** – See status of the connection to the Conductor. For more details, see `status conductor` below.
- **IP address** – Shows the active IP addresses for this Airwall Gateway. An IP address displayed in green indicates it has been selected as active.

`status conductor`

Shows the status of the Airwall Edge Service's connection to the Conductor. Disconnected indicates the Airwall Edge Service is not connected to the Conductor.

Note: For Airwall Agents and Servers that support it, if Disconnected mode is On, you can still access resources on the Airwall secure network, and your Airwall Agent or Server will reconnect at intervals for configuration and trust policy updates. If you want to reconnect manually, use `conductor sync`.

`conductor set`

Set or remove a Conductor IP address or URL and port (optional). For example: `conductor set my-conductor.tempered` or just `conductor set` to remove.

`conductor sync`

If an Airwall Agent or Server is set to Disconnected mode on the Conductor, this command manually reconnects to retrieve any changes to configuration or trust policies. In Disconnected mode, you can still access resources on the Airwall secure network. See Sync an Airwall Agent or Server in Disconnected Mode on page 29.

`diag`

Put the Airwall Gateway in diagnostic mode

`factory-reset [keep-networking|clear-identity]`

Reset Airwall Gateway back to factory default settings.

- Use the keep-networking option to preserve the network configuration.
- Use clear-identity to remove the device identity and licensing, and to re-license the Airwall Gateway.

If you want to preserve the network configuration, use the keep-networking option:

```
airsh>> factory-reset keep-
networking
```

`exit` or **`quit`**

Exit Airshell

`history`

See the history of commands entered into Airshell. Enter `history clear` to delete history.

`color on|off`

Turn on or off color on the text output from the serial console.

`reboot`

Restart the Airwall Gateway.

`shutdown`

Shut down the Airwall Gateway.

Configuration Commands

`activate [`*`activation_code`*`]`

Activate a profile, and optionally, enter an activation code to connect an Airwall Gateway to the Conductor. For example:

```
airsh» activate 8z130f85eed9
```

Entering an activation code means the Airwall Edge Service can connect to the Conductor without an administrator needing to provision it.

`conf`

Configure Airwall Gateway or Conductor. You can configure these settings

- `conf conductor` *`URL|IP_address`* – Set Conductor URL. Same as `conductor set` above.
- `conf name` – prior to provisioning, configure the Airwall name shown in the Conductor.
- `conf cell [apn=auto|<apn>] [carrier=auto|<carrier>] [mode=3g|4g][pin=<code>][auth=none|pap|chap|both] [user=<user>] [pw=<password>] [ip-type=<default,ipv4,ipv6,ipv4v6>] [roaming=<0|1>]` – Get or set cellular modem configuration. Supported cellular carriers are: "AT&T", "Bell", "GCI", "Generic", "Rogers", "T-Mobile", "Telus", "VTel", and "Verizon". **See also –** U.S. Cellular Carrier Certifications on page 377
  - When you set the carrier to “auto”, the Airwall Gateway looks up the operator ID from the SIM card.

  - If your carrier name is not listed, use “Generic”.
  - When you set the APN to “auto”, the Airwall Gateway uses a default APN from the detected or specified carrier, or you can specify the APN provided to you.
- `conf cell2 [apn=auto|<apn>] [carrier=auto|<carrier>] [mode=3g|4g][pin=<code>][auth=none|pap|chap|both] [user=<user>] [pw=<password>] [ip-type=<default,ipv4,ipv6,ipv4v6>] [roaming=<0|1>]` – Get or set second cellular modem configuration.
- `conf network` –

  v2.2.10 and later – Configure port groups, see Configure Port Groups with Airshell on page 376. For example: to modify port group (pg) 2 with an IP of 192.168.1.1/24, enter:

  ```
  conf net modify pg=2
   ip=192.168.1.1/24
  ```

  v2.2.8 and earlier – Set up static IP addresses.
- `conf password [delete]` – Set (or delete) the password for the current Airshell user. Use `conf password delete` to remove the password. (`conf password delete` not available remotely)
- `conf ssh on|off|status` – Enable, disable, or see the status of remote log in through SSH. See Set up Remote Access to Airshell via SSH on page 374 for full details.
- `conf ssh-key add` *ssh_public_key* – Add or remove public SSH keys you use to log in remotely. See Set up Remote Access to Airshell via SSH on page 374 for full details.
- `conf ssh-key remove` – Remove the public SSH key you use to log in remotely. See Set up Remote Access to Airshell via SSH on page 374 for full details.
- `conf wifi` – On WiFi-enabled Airwall Gateways, walks you through the steps to configure a WiFi connection.

`setup-ui`

v2.2.10 and later – Open the setup wizard to set up an Airwall Gateway. See Configure an Airwall Gateway with the airsh Setup Wizard on page 274.

Diagnostic commands

`conductor ping`

Checks name resolution and performs TLS connection attempt with every configured Conductor URI.

`conductor status`

Show Conductor settings and status.

`conductor set`

Set or remove a Conductor IP address or URL and port (optional). For example: `conductor set my-conductor.tempered` or just `conductor set` to remove.

`diag`

Put the Airwall Gateway in diag mode.

`diag_report`

Get a diagnostic report.

`firmware-upgrade`

Update the Airwall Gateway firmware from a file hosted on a reachable file server.

`network-restart`

Restart the network interfaces on the Airwall Gateway.

`nmap [overlay_port_group] [Scan Type(s)] [Options] {target specification}`

Map your network for discovery or security audits. For more information, see Do network discovery and security audits in Airshell (nmap) on page 377.

`policy [ -v | clear]`

Show HIP policy information. Only valid on Airwall Edge Services.

- `-v` – Show additional columns.
- `clear` – Clear HIP policy cache.

Here are the columns in the output:

- PGID = Ingress port group ID
- IP SRC/DST = source/destination IP address
- AGE = seconds since last matching packet
- Additional columns shown with -v:
    - PEER_HIT – HIT of incoming (ingress) peer
    - MAC SRC/DST – source/destination Ethernet address
    - VLAN = 802.1Q VLAN ID
    - ETH = EtherType
    - PKTS = Total packets
    - BYTES = Total bytes (including Ethernet headers)

Actions:

TX_PG <id> = Transmit to port group.

TX_LSI <hit> = Transmit to peer.

DROP = Drop due to policy

`ping` *`IP_address`* `[-I` *`interface`* `]`

Ping the IP address, optionally with the interface specified with -I.

`rpc`

Sent JSON-RPC message.

`time`

Query or time set.

`table [TABLE] [ --OPTION=ARG[,ARG]... | KEY=VALUE ]...`

Query status table. These tables that show the real-time internal state of Airwall Gateways and a Conductor. All of these tables are included when you run a diagnostic report. For more information and all options, see Airshell table command on page 369.

Common Options:

- `--select COL[,COL]...` – Display only the specified columns.

KEY=VALUE

Allows you to filter the results by a value in one of the columns of the table. KEY is the column name, and VALUE is the value to filter on. For example, to return only rows with the value of ESTABLISHED in the state column, enter:

```
table hip_assoc state=ESTABLISHED
```

TABLE

These are the available tables. For descriptions, see Airshell table command on page 369.

Conductor tables:

```
file_descriptors, m2_connections,
 m2_denied, m2_allowed,
 map_connection
```

Airwall Gateway tables:

```
file_descriptors, map_connection,
 hip_proto, hip_assoc_events,
policy_engine, encrypt_engine,
 decrypt_engine, reader, writer,
 io_worker,
worker, decrypt_sadb, encrypt_sadb,
 hip_assoc, peers, jet_ip4_relay,
 jet_engine
```

Status Commands

`license`

Display open source license information

`log [follow | status [hip|ebm2]hep]`

Show the latest lines of the system log, or rating limiting details.

- `follow` – Follow the log output until you quit with CTRL+C
- `status [hip|ebm2]` – Show rate limiting details for HIP or ebm2 traffic.

`status [<option>]`

Display the status of the Airwall Gateway, including the installed cellular firmware package. With an option, displays the status of one of the following:

- `cell` – Get Cellular information
- `conductor` – Get the status of connection to the Conductor
- `dnscache [flush | flush <pattern>]` – For Airwall Gateways, dumps or flushes the

entire DNS cache, or specific entries. For example, `flush dnscache example.com` or `flush dnscache *.example.net`

- `hip` – Get HIP state
- `hipvars` – Get additional HIP state
- `linkmanager` – Get Linkmanager status.
- `macs` – Get the MAC addresses for all of the network interfaces on this Airwall Gateway.
- `network` – Get network information
- `peers` – Get a list of peer Airwall Edge Services
- `ps` – Get the running processes on this Airwall Gateway.
- `relays` – Get relay probe information
- `routes` – Get routing tables
- `threads` – Reports CPU and memory usage of threads of major services running on an Airwall secure network.
- `tunnels` – Get a list of tunnels on this Airwall Gateway
- `wifi` – Get Wifi information

Airshell table command

Full details for the Airshell table command

These tables that show the real-time internal state of Airwall Gateways and a Conductor. All of these tables are included when you run a diagnostic report.

Options

Options:

- `--limit=COUNT` – Display up to COUNT rows.
- `--offset COUNT` – Start after COUNT rows.
- `--scope=SCOPE` – Limit query to SCOPE.
- `--select COL[,COL]...` – Display only the specified columns.

KEY=VALUE

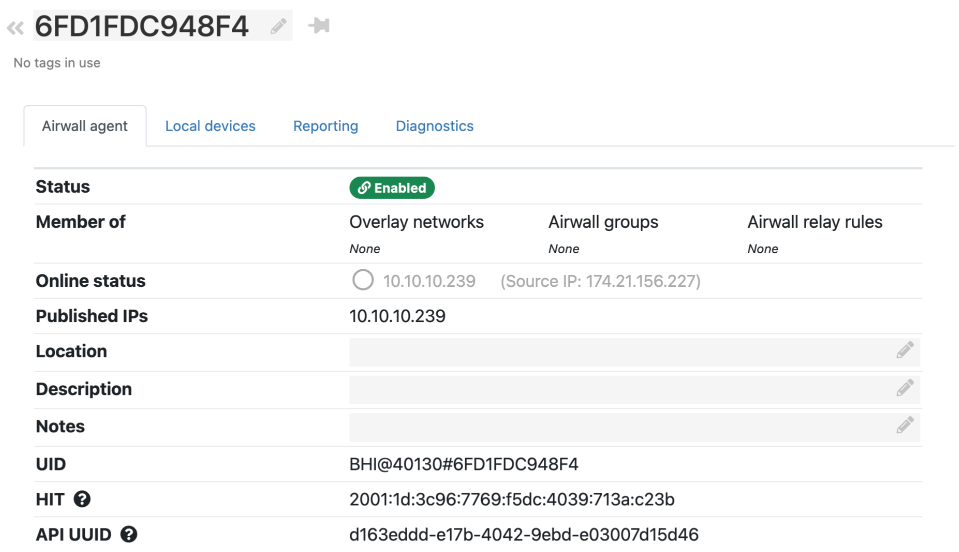
Allows you to filter the results by a value in one of the columns of the table. KEY is the column name, and VALUE is the value to filter on. For example, to return only rows with the value of ESTABLISHED in the state column, enter:

```
table hip_assoc state=ESTABLISHED
```

Examples

To troubleshoot a single tunnel:

1. Find the HIT for the peer Airwall Edge Service on its page in the Conductor:



6FD1FDC948F4

No tags in use

Status	Enabled		
Member of	Overlay networks *None*	Airwall groups *None*	Airwall relay rules *None*
Online status	○ 10.10.10.239 (Source IP: 174.21.156.227)		
Published IPs	10.10.10.239		
Location			
Description			
Notes			
UID	BHI@40130#6FD1FDC948F4		
HIT	2001:1d:3c96:7769:f5dc:4039:713a:c23b		
API UUID	d163eddd-e17b-4042-9ebd-e03007d15d46		

2. On the peer Airwall Edge Service, use the following Airshell table commands to restrict output to a single peer:

- table hip_assoc peer_hit=2001:19:ce64:2399:3870:3531:3e20:735d
- table decrypt_sadb hit=2001:19:ce64:2399:3870:3531:3e20:735d
- table encrypt_sadb hit=2001:19:ce64:2399:3870:3531:3e20:735d

Note: You can also search for an Airwall Edge Service by HIT in the Conductor using Conductor Query Language: hit=='2001:19:ce64:2399:3870:3531:3e20:735d'. For more information, see Search by Expression with the Conductor Query Language on page 45.

TABLE

These are the available tables, grouped by the area for which they provide information. If you do not specify a table, you get the list of available tables.

File tables

- file_descriptors

MAP (Conductor) Connection tables

These tables show MAP connection (Airwall Gateway<->Conductor) information

- **map_connection (on Airwall Gateways)** – Connection information on Airwalls
- **m2_connections (on Conductor)** – Connection information on the Conductor. Shows two tables, the first allowed connections and the second, denied connections.table
- **m2_denied** – Denied connections
- **m2_allowed** – Allowed connections

Tunnel tables

These tables show tunnel information.

- **hip_assoc** – HIP protocol state of active tunnels. A tunnel (not relayed) will have an encrypt_sadb and decrypt_sadb entry once the HIP base exchange is complete.
- - pid – Process ID of openhip/airwall process
  - id – Protocol thread ID – always 0
  - idx – Array index in hip_assoc_table. Entries should be densely packed in the beginning. By default, Airwall Edge Services support up to 1024 HIP associations
  - local_hit – Host Identity Tag (HIT) of local Airwall, or lesser of two HITs for relayed association

  - peer_hit – HIT of remote Airwall Edge Service, or greater of two HITs for relayed association
  - state – HIP association state - https://datatracker.ietf.org/doc/html/rfc7401#section-4.4.4
  - last_state_change – Time of last state change, expressed as seconds from now
  - last_hip_keepalive – Last HIP UPDATE keepalive, expressed as seconds from now
  - local_addr – Local IP address and UDP port
  - peer_addr – Remote IP address and UDP port
  - update_id – Sequence number of last HIP UPDATE sent
  - path_mtu – Path MTU discovered from local interface MTU, Overlay MTU configuration via Conductor, ICMP unreachable or peer Airwall Edge Service
  - dh_group – Diffie Hellman group ID
  - hip_xfrm – HIP transform (encryption and digest algorithm)
  - esp_xfrm - EPS transform (encryption and digest algorithm), corresponds to a_type, e_type in SADB
  - keymat_idx – Index of next available key material in HIP association ephemeral key material. This index resets after a rekey UPDATE
  - spi_in – Inbound (decrypt) SPI (Security Parameter Index)
  - spi_out - Outbound (encrypt) SPI (Security Parameter Index)
- **hip_assoc_events** – Circular log of recent HIP association events
- **encrypt_sadb**– Outbound ESP state of tunnels

  - pid – Process ID of openhip/airwall process
  - id – Protocol thread ID – always 0
  - hit – Peer Airwall HIT
  - expire – Expiration time, expressed as seconds from now
  - last_used – Last packet time, expressed as seconds from now
  - a_type – Authentication algorithm
  - e_type - Encryption algorithm
  - a_len – Authentication key length
  - e_len – Encryption key length
  - sequence – Next ESP sequence number
  - ifindex – Outbound interface index
  - src – Source IP address and UDP port
  - dst – Destination IP address and UDP port
  - spi – ESP SPI
  - mtu – Overlay MTU, reflects hip_assoc path_mtu minus encapsulation overhead.
  - next_hop – Next Hop MAC address for routed packets
  - ndp_probes – Number of NDP probes sent to discover next hop MAC
  - arp_probes – Number of ARP probes sent to discover next hop MAC
  - ipv6 – Peer supports IPv6 and ICMPv6 keepalive messages
  - icmp6_seqno – Next Sequence number of ICMPv6 keepalives
  - pkts_tx – Number of packets transmitted
  - pkts_dropped – Number of packets dropped, if any.
  - bytes_rx – Number of bytes transmitted
- **decrypt_sadb** – Inbound ESP state of tunnels including relayed tunnels

  - pid – Process ID of openhip/airwall process
  - id – Protocol thread ID – always 0
  - spi – ESP SPI (security parameter index)
  - hit – Peer Airwall HIT
  - expire – Expiration time, expressed as seconds from now
  - last_used – Last packet time, expressed as seconds from now
  - a_type – Authentication algorithm

- e_type - Encryption algorithm
- a_len – Authentication key length
- e_len – Encryption key length
- sequence – Last ESP sequence number
- relay_dst_hit – For relayed associations, HIT of destination Airwall Edge Service.
- relay_ifindex - For relayed associations, outbound interface index.
- relay_src - For relayed associations, outbound source IP address and UDP port
- relay_dst - For relayed associations, outbound destination IP address and UDP port
- pkts_rx – Number of packets received and successfully decrypted
- pkts_dropped – Number of packets dropped, if any
- pkts_lost – Number of packets lost, determined from gaps ESP sequence number
- bytes_rx – Bytes received

Relay tables

These tables show information on relays and relay traffic.

- `decrypt_sadb` – Inbound ESP state of tunnels, including relayed tunnels. A relay has two decrypt_sadb entries for each relay connection.
- `hip_assoc` – HIP state of active tunnels. A tunnel (not relayed) has an encrypt_sadb and decrypt_sadb entry once the HIP base exchange is complete.
- `jet_ip4_relay` - Offloaded relay connections - should reflect decrypt_sadb state.
- `peers` - Relay client (indexed by client HIT) underlay IP of the last relay probe.

Overlay trust policy tables

These tables show information on overlay trust policies.

- `policy_engine` - Policy enforcement and east-west / bypass.
- `.policy_drops` – Recently dropped packets by policy. A closed hashtable of policy drops.

Overlay Configuration tables

This table shows overlay information.

- `.overlay` – Port group information. Can be useful to look up "pgid" to "pg_id" mapping.

Performance tables

These tables can be useful in troubleshooting.

- **decrypt_engine**– Inbound tunnel handling including relayed traffic
- **encrypt_engine** – Outbound tunnel handling
- **jet_engine** –
- **hip_proto** - HIP protocol processing
- **io_worker** – Combined dataplane thread
- **reader** – Dataplane thread counter
- **worker** – Dataplane thread counter
- **writer** – Dataplane thread counter

Internal Only

Tables not listed are used internally.

Linux Airwall Server Airshell commands

These are the common Airshell commands for the Linux Airwall Server.

`help`	List available commands. Use `help tree` to see commands and options.
`service [ start | stop | restart]`	Start, stop, or restart the Linux Airwall Server.
`profile [activate | create | list | modify]`	Manages profiles for your Linux Airwall Server. • `activate` – Make a profile the active one. For example: `sudo airsh profile activate <profile name or number>` • `create` – Create and configure a new profile. For example: `sudo airsh profile create name=<new profile name> conductor=<conductor_url> [act=<activation_code>]` • `list` – List your profiles. Use `list verbose` to get profile details as well. • `modify` – Modify a profile. For example `sudo airsh profile modify <name| number> [name=<new-name>] [conductor=<conductor-url>] [act=<activation-code>]`
`conductor [ set | sync | status ]`	• `conductor set` – Set or remove a Conductor IP address or URL and port (optional). For example: `conductor set my-conductor.tempered`. To remove a Conductor, run without a URL: `conductor set`. • `conductor sync` – If the Airwall Server is set to Disconnected mode on the Conductor, run this command to manually reconnect and retrieve any changes to configuration or trust policies. In Disconnected mode, you can still access resources on the Airwall secure network. See Sync an Airwall Agent or Server in Disconnected Mode on page 29. • `conductor status` – Same as `status conductor`, shows the status of the Linux Airwall Server connection to the Conductor.
log follow	Watch the log file (usually for troubleshooting).
`status [conductor | wifi | network]`	Shows the status of the Linux Airwall Server connection to the Conductor, status of the WiFi connection, or status of the network. **Note:** A Conductor status of Disconnected indicates the Linux Airwall Server is not connected to the Conductor. If Disconnected mode is On, you can still access resources on the Airwall secure network, and your agent will reconnect at intervals for configuration and trust policy updates. If you want to reconnect manually, use `conductor sync`.

Note: If your status is Disconnected and Disconnected mode is Off, you will not be able to access resources. Contact your Conductor administrator.

Run Airshell remotely from the Conductor

For remote administration of Airwall Gateways, you can use Airshell to run diagnostic and configuration commands from the Conductor.

Supported Roles	System administrators can assign **Allow Remote Airsh** permissions to system and network administrators. See Customize Permissions for System and Network Administrators on page 56. • Permission extends to any Airwall Edge Service the user has edit permissions for • Permissions apply to network as well as system administrators
Supported Versions	v3.1.0 Conductor
Supported Airwall Edge Services	• v3.1.0 Airwall Gateways that are online • Conductors
Supported Airshell commands	You can run most Airshell commands that are available when running Airshell locally. Exceptions are commands that risk disconnecting the Airwall Gateway permanently from the Conductor, such as the shutdown command or commands to reconfigure the network. You can use the help command for the list of available commands.

1. In the Conductor, open the page for an Airwall Edge Service, then select the **Airshell** tab. For Conductor Airshell, go to **Settings** > **Airshell**.
2. Select **Open Remote Airshell**.
3. Enter the Airshell commands you need.
4. When done, enter `exit`, or just navigate to a different page.

Note: Airshell sessions automatically disconnect after 10 minutes of inactivity. If your session is disconnected, select **Reconnect**.

Set up Remote Access to Airshell via SSH

You can enable and set up a secure shell (SSH) public key on physical Airwall Gateways to allow you to remotely log in to run `airsh` commands. Remote access is limited to running `airsh` commands, and only to the Overlay IPs, not any Underlay IPs. Remote access uses SSH public/private key pairs, where the Airwall Gateways only see the public key.

Note: You can also run Airshell on Airwall Gateways remotely from the Conductor. For details, see Manage Airwall Gateways remotely with Airshell on page 98.

Setting up remote access provides a way to configure and troubleshoot your physical hardware without a site visit.

Note: To enable SSH access and add the SSH keys, you first need physical access to the Airwall Gateway.

Before you begin:

To set up remote access, you need:

- SSH public and private keys for the people's computers that require access – For example, these can be generated using OpenSSH's `ssh-keygen` command. For example, `ssh-keygen -t rsa`.

CAUTION: You should protect your SSH private key with a passphrase.

- The Airwall Gateway's Overlay IP address where SSH will be used.

1. If you need to configure an Overlay IP for this Airwall Gateway, you can do it from the Conductor or using Diagnostic Mode on the Airwall Gateway:
   - **From the Conductor**: Open the Airwall Gateway and go to the **Ports** tab. Expand the **Overlay Port Group**, and under **IP addresses**, configure one or more static IP addresses.
   - **From the Diagnostic Mode web interface**: Navigate to http://192.168.56.3, open **Settings**, **Port Settings**, and under **Port Groups**, configure an IP address for an Overlay Port Group.
2. See Connect to a physical Airwall Gateway or Conductor with a console port on page 293 to connect to the Airwall Gateway and log in to `airsh`.
3. Enable SSH access by entering:

   ```
   airsh» conf ssh on
   ```

   This enables SSH access via the Overlay IP (not the Underlay IP addresses).
4. Password-based SSH login is not allowed. Configure at least one public SSH key by entering:

   ```
   airsh» conf ssh-key add <public_SSH_key>
   ```

   Note: There is a potential issue on Airwall Gateway 150s v2.2.8 and earlier when copying and pasting long values (over 35 characters) into the console. If the console becomes unresponsive, try pasting the key in smaller parts.
5. In `airsh`, type status to get the IP address to log in to.
6. To log in remotely, ssh into the IP address, and then log in to `airsh`:

   ```
   login airsh
   ```

You can now run airsh commands remotely on the Airwall Gateway. See Access an Airwall Gateway Remotely on page 375.

Access an Airwall Gateway Remotely

Once you've Set up Remote Access to Airshell via SSH on page 374 on an Airwall Gateway, you can use the configured SSH key to log in remotely and run a limited set of `airsh` commands with airsh as a username.

Note: Remote access is limited to running `airsh` commands, and only to the Overlay IPs, not any Underlay IPs.

For example, if the Overlay IP for the Airwall Gateway is 192.168.50.5, use a command such as:

```
ssh airsh@192.168.50.5
```

You can configure the Overlay IP as a protected device. When policy has been granted to the Overlay IP, you can access remote SSH from a device behind another Airwall Gateway, or from an Airwall Agent.

For full descriptions of airsh commands, see Airshell (airsh) Command Reference on page 362.

Configure an Airwall Gateway with the `airsh` Setup Wizard

Configure the most common Airwall Gateway setup options using the `airsh` Setup Wizard.

Supported Versions	2.2.10 and later Airwall Gateways
Supported on these Airwall Edge Services	All Airwall Gateways

Before you begin

Collect the following information to set up your Airwall Gateway:

- **Underlay network information** – The protocol (DHCP or static) and type (IPv4 or IPv6) of your underlay network, both wired and Wifi, if enabled. If you are using cell, also your APN (for both modems if you have 2).
- **Conductor address** – The IP address or hostname and port for the Airwall Conductor you want this Airwall Gateway to connect to.
- **Wifi information (if enabled)** – The authentication type, and SSID (network name) and key for your wireless network.
- **Cellular information (if included)** – Your active carrier, preferred access type (3G or 4G), pin code, authentication type (None, PAP, CHAP, PAP/CHAP), username and password (if applicable), IP connection type (default, IPv4, IPv6, IPv4/IPv6) and whether you want to enable or disable roaming.

Set up an Airwall Gateway with the `airsh` Setup Wizard

1. Connect a computer or Configure an Airwall Gateway with the airsh Setup Wizard on page 274 to access it remotely.
2. Log in to `airsh`. For information on how, see Airshell (airsh) Command Reference on page 362.
3. At the `airsh` prompt, enter:

   ```
   setup-ui
   ```

4. Fill in the information to set up your Airwall Gateway.
5. When you're finished, the status page shows the options you've selected and whether you are connected to your Wifi or cellular network. You may want to note your underlay IPs.

You can reboot to start using the Airwall Gateway, or go into Diagnostic mode to configure more options.

To troubleshoot connection issues, see Troubleshoot Initial Airwall Gateway connections on page 491.

Configure Port Groups with Airshell

You can use Airshell to add, delete, and configure port groups on an Airwall Gateway, including adding an Overlay IP.

Supported Versions	2.2.10 and later Airwall Gateways
Supported on these Airwall Edge Services	All Airwall Gateways

Before you begin

By default, port 1 of the Airwall Gateway is an underlay port set to acquire its IP address using DHCP. To configure the underlay port with a static IP address, you'll need:

- IP address/subnet, gateway, and DNS servers for the port group.
- If you are using DHCP, set up your DHCP server on your network.

Note: This procedure uses the conf net menus, but you can accomplish the same thing in one command. Enter `help conf net` to see options, and see the one command example after the procedure.

Set up port groups on an Airwall Gateway

1. Connect a computer or Set up Remote Access to Airshell via SSH on page 374 to access it remotely.
2. Log in to Airshell. For information on how, see Airshell (airsh) Command Reference on page 362.
3. At the `airsh>>` prompt, type:

   ```
   airsh>> conf network
   ```

   Airshell displays the Port Groups configuration menu:

   ```
   Port Groups:
     1: Underlay Port Group 1 [underlay]
        (static) 10.0.1.99/24 gateway: 10.0.1.1 dns: 8.8.8.8
     2: Overlay Port Group 1 [overlay]

     a. Add port group
   ```

```
  d. Delete port group
  s. Save port group changes
  q. Quit (cancel changes)
```

Note: You can also accomplish the same thing in one command. Enter `help conf net` to see options.

4. Follow the menus to configure the port groups and port group settings for the Airwall Gateway. Type `q` to back up to the main menu, then type `s` to save your changes.

   For more information about editing port groups and port group settings, see Set up Port Groups on an Airwall Gateway on page 386.

For example, here's how you add an Overlay IP address:

One command line:

```
airsh conf net modify pg="Overlay Port Group 1" ip=[ip_in_CIDR_format]
```

Using the conf net menus:

1. At the `airsh>>` prompt, type:

   `airsh>> conf network`
2. Select `2` to edit Overlay Port Group 1.
3. Select `a` to add an Overlay IP group. This adds a static IP address.
4. Select `1` (one) to change the static IP address. Airshell displays the IP configuration menu:

```
===========================
Configuring IP for Port Group 1
  t. Toggle dhcp/static  (static)
     i. IP address       (not set)
     g. Gateway          (not set)
     d. DNS Servers      (not set)
  q. Quit to previous menu
```

5. Select `i` to enter an IP.
6. Enter the IP address you want in CIDR format, and press `Enter`.
7. Select `q` twice to go back to the main menu, and then select `s` to save the configuration.

Do network discovery and security audits in Airshell (nmap)

Map your network for discovery or security audits with the Airshell command `nmap`.

Run `nmap` from the overlay side of an Airwall Gateway. This reference includes examples for the most common and useful options. This command is based on the publicly-available Nmap Reference guide, where you can find additional examples.

You can optionally specify which overlay port group to scan. For example, `nmap ovl1 -n -sP 192.168.3.1-10` or `nmap 1 -n -sP 192.168.3.1-10`. If you do not specify an overlay port group (for example, `nmap -n -sP 192.168.3.1-10`), the scan is run from the first overlay port group.

For `nmap` options, enter `nmap --help`.

For more options and examples, see the Nmap Reference guide (external link).

U.S. Cellular Carrier Certifications

Here are the modems in Airwall Gateway and Advantech hardware and the cellular carriers for which they are certified.

Airwall Gateway	Verizon	AT&T
110g (Quectel EG25-G)	X	X
Advantech AV3200 (Quectel EC25-AF)	X	X

Airwall Gateway	Verizon	AT&T
150 (Sierra HL7588 - see note)	X	X
250g/gd (Sierra HL7588 – see note)	X	X

Note: The NimbeLink Sierra HL7588 modem is pre-certified for PTCRB approved networks. Its certification covers the device it is installed in.

Set a Private APN for your Cellular Provider on an Airwall Gateway

You can set the APN of the cell modem on an Airwall Gateway (100, 110, 150, 250) on the Airwall Gateway from Diagnostic mode or using `airsh`, or from the Conductor.

Note: If you are using the default APN of your cellular provider for Internet access, this APN is automatically used when the APN is set to "auto". These instructions are if you have a private APN that you need to set.

Set the APN from Diagnostic Mode

1. Put your Airwall Gateway into Diagnostic mode. See your platform guide or Put an Airwall Gateway into diagnostic mode on page 478 for instructions.
2. In **Diagnostic** mode, open the **Settings** page, and the **Port Settings** tab. (*Note: Not the **Cellular Settings** tab.*)
3. Select **Edit Settings**.
4. For **APN**, enter the APN needed to connect to your cellular service.
5. Select **Update Settings**.

Set the APN with `airsh`

On the Airwall Gateway, you can use the following `airsh` command to set the APN, replacing <APN> with the APN (no spaces allowed):

```
airsh> conf cell apn=<APN>
```

For example,

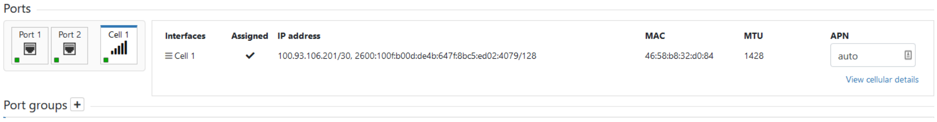
```
airsh> conf cell apn=my_private_apn
```

For more information on using `airsh`, see Airshell (airsh) Command Reference on page 362.

Set the APN in the Conductor

If the Airwall Gateway is on Ethernet and connected to the Conductor, you can set the APN from the ports page of the Airwall in Conductor.

1. On the page for the Airwall Gateway, open the **Ports** tab.
2. Select **Edit Settings**.
3. Under **Ports**, select the **Cell** Interface.
4. To the right, under **APN**, enter or change to the APN needed to connect to your cellular service.



Interfaces	Assigned	IP address	MAC	MTU	APN
☰ Cell 1	✓	100.93.106.201/30, 2600:100f:b00d:de4b:647f:8bc5:ed02:4079/128	46:58:b8:32:d0:84	1428	auto

5. Select **Update Settings**.

Bulk Configuration of Airwall Edge Services

Configure certain settings in bulk for Airwall Edge Services or Airwall groups.

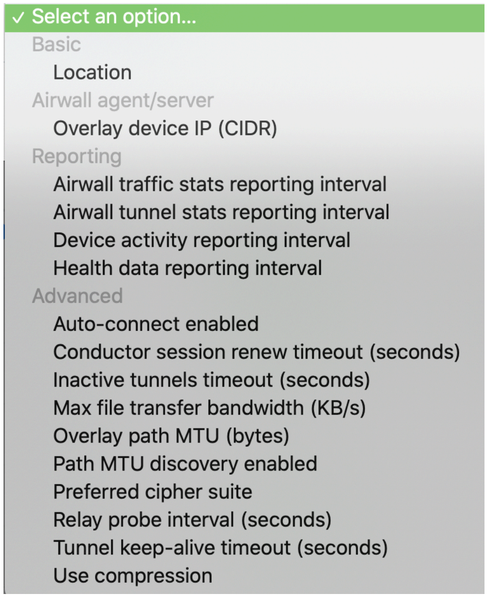
Supported Versions	Conductor 2.2.10 and later

Required Role	System Administrators, and Network administrators with permissions to change the selected Airwall Edge Services
Supported on these Airwall Edge Services	Provisioned and managed

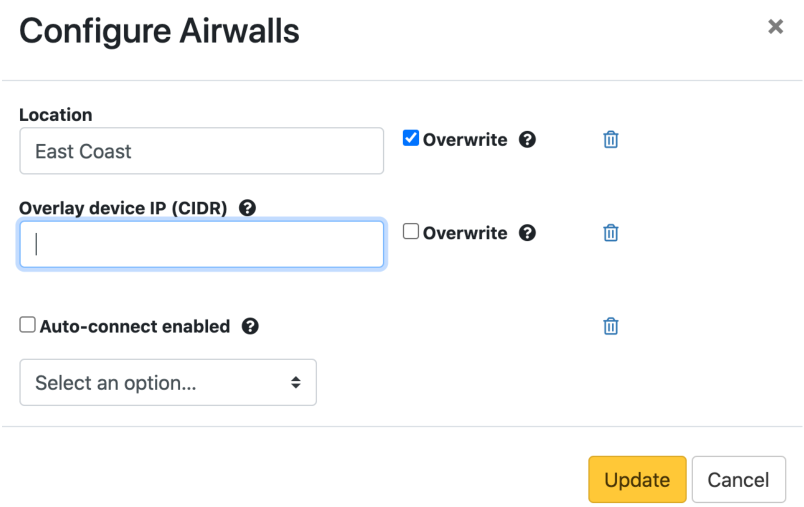
CAUTION: For most options, bulk editing **overwrites** any existing values on the selected Airwall Edge Services. There are a few that you must specifically choose overwrite.

To configure Airwall Gateways in bulk

1. On the **Airwalls** page, select the Airwall Edge Services or Airwall groups you want to configure.
2. Select **Airwall actions** > **Configure selected Airwalls**.
3. Select the options you want to change for all selected Airwall Edge Services. You can select all of the options you want first, and then fill them all in:


✓ Select an option...
Basic
Location
Airwall agent/server
Overlay device IP (CIDR)
Reporting
Airwall traffic stats reporting interval
Airwall tunnel stats reporting interval
Device activity reporting interval
Health data reporting interval
Advanced
Auto-connect enabled
Conductor session renew timeout (seconds)
Inactive tunnels timeout (seconds)
Max file transfer bandwidth (KB/s)
Overlay path MTU (bytes)
Path MTU discovery enabled
Preferred cipher suite
Relay probe interval (seconds)
Tunnel keep-alive timeout (seconds)
Use compression

4. Fill in the values for the options you've chosen.



Configure Airwalls

Location: East Coast ☑ Overwrite

Overlay device IP (CIDR): ☐ Overwrite

☐ Auto-connect enabled

Select an option...

5. For most options, bulk editing by default overwrites any existing values on the selected Airwall Edge Services. On options that do not automatically overwrite values, you have the option to overwrite. Check **Overwrite** if you want to also overwrite these option values.
6. Select **Update** to apply the bulk configuration.

Bulk Edit Settings Descriptions

Here are descriptions for the Airwall Edge Service settings you can configure in bulk.

CAUTION: Most of these options **overwrite** the current setting on selected Airwall Edge Services. A few options (*starred) will not overwrite by default, and instead only apply the change if the setting is blank or has not been changed from the default. For these options, check **Overwrite** to overwrite these option values.

Note: If an option doesn't apply to a particular Airwall Edge Service, it is ignored.

Basic

- **Location*** – Physical location of the Airwall Edge Services.

Airwall agent/server

- **Overlay device IP (CIDR)*** – Assign IPs to the selected Airwall Agents and Servers in order from the specified IP CIDR.

Reporting

Set reporting intervals. All of these settings default to 5 minutes:

- **Airwall traffic stats reporting interval** – How often to report traffic stats to the Conductor. Traffic stats are shown on the page for each Airwall Edge Service under **Reporting** > **Traffic stats**.
- **Airwall tunnel stats reporting interval** – How often to report tunnel stats. Tunnel stats are shown on the page for each Airwall Edge Service under **Reporting** > **HIP tunnel stats**.
- **Device activity reporting interval** – How often to report device activity.
- **Health data reporting interval** – How often to report health data. Health data is shown on the page for each Airwall Edge Service under **Reporting** > **Health data**.

Advanced

- **Auto-connect enabled** – Enable to build secure tunnels between devices even if there is no traffic. Useful when devices are behind NAT. **Default**: Enabled
- **Conductor session renew timeout** – Number of seconds before a Conductor session times out. **Default**: 120 seconds.
- **Inactive tunnels timeout** – Number of seconds before an inactive tunnel is closed.
- **Max file transfer bandwidth** – Limit the bandwidth used for large file downloads (such as firmware updates). **Default**: 1000 Kb/second.
- **Overlay path MTU** – Maximum transmission unit (MTU) in bytes sent through the overlay. Must be between 1280 and 9022. **Default**: 1400 bytes.
- **Path MTU discovery enabled** – Check to have the Airwall Edge Service adjust packet sizes if the intermediate routings only support limited maximum transmission unit (MTU) settings. **Default**: Disabled.
- **Preferred cipher suite** – Select the cipher suite to use when encrypting traffic. Default: Use Global setting (set in Conductor Settings under **Advanced** > **Global Airwall settings**).
- **Relay probe interval** – If enabled, the Airwall Gateway periodically sends probe packets to all of its relays and uses the closest relay when initiating secure tunnels. This option can reduce the amount of network traffic used to build new tunnels and allows auto-connect to be turned off. **Default**: 30 seconds.
- **Tunnel keep-alive timeout** –Enable to have the Airwall send keep-alive packets to peer Airwalls to keep the tunnel from expiring if no device traffic is available. **Default**: 75 seconds.
- **Use compression** – Turn on to have Airwall Edge Services compress encrypted traffic before sending. **Default**: Use Global setting (set in Conductor Settings under **Advanced** > **Global Airwall settings**).

Set up a secure IPv6 overlay

You may want to set up IPv6 to provide encrypted communication to the IPv6 Internet or between Airwall Gateways, to secure IPv6 communication, and carry IPv6 traffic across an IPv4 only network.

Supported Versions	v2.2.10 and later Conductor and Airwall Gateways
Supported Airwall Edge Services	v2.2.10 and later Airwall Gateways, plus any version of Airwall Relay since they do not decrypt traffic, they will relay IPv6 traffic.
Required Role	System and network administrators with permissions to the Airwall Gateways.

Note: IPv6 is not yet supported on:

- L2 (aka subnet extension) – Having the same subnet behind multiple Airwall Gateways or multiple port groups on a single Airwall Gateway

The steps are:

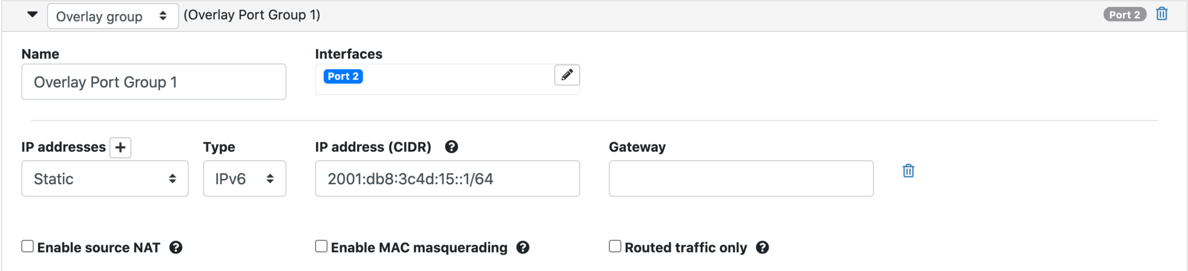
1. Configure an IPv6 static address for an Airwall Gateway
2. Configure DHCPv6 (Optional if you configure a static IPv6 address and a default route to the Airwall's overlay IPv6 address on each IPv6 protected device)
3. Discover devices, or create an /64 network object device on the Airwall Gateway
4. Repeat steps 1-3 for other Airwall Gateways you want to communicate over IPv6.
5. Set up an overlay and add trust between the /64 network object devices.

These steps are covered in more detail in the following sections.

Step 1: Configure an IPv6 static address

On an Airwall Gateway that supports IPv6, add an IPv6 overlay IP address:

1. Go to **Ports**, select **Edit Settings**, and open an Overlay port group.
2. Set the following options:
   - **IP addresses** – Select `Static`. If you need to add an address, click the plus (you can have both IPv4 and IPv6 static addresses assigned).
   - **Type** – Select `IPv6`.
   - **IP address** – Enter a /64 block and assign the overlay IPv6 address (best practice is to use ::1):



Overlay group (Overlay Port Group 1)

Name: Overlay Port Group 1

Interfaces: Port 2

IP addresses: Static

Type: IPv6

IP address (CIDR): 2001:db8:3c4d:15::1/64

Gateway:

□ Enable source NAT

□ Enable MAC masquerading

□ Routed traffic only

Note: Assign unique IP addresses for each Airwall Gateway you set up.

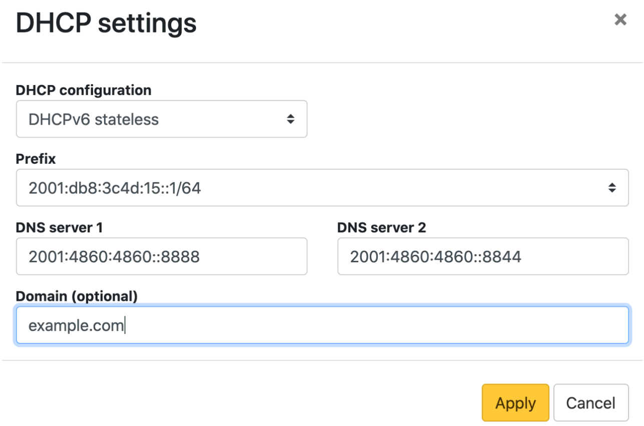
3. Select **Update Settings**.

Step 2: Configure DHCPv6

Note: This step is optional if you configure a static IPv6 address and a default route to the Airwall Gateway's overlay IPv6 address on each IPv6 protected device.

On the Airwall Gateway, configure your DHCP settings for DHCPv6:

1. Next to **DHCP settings**, select **Configure**.
2. Enter your DNS servers and Domain. The rest should be filled in for you.



DHCP settings

DHCP configuration: DHCPv6 stateless

Prefix: 2001:db8:3c4d:15::1/64

DNS server 1: 2001:4860:4860::8888

DNS server 2: 2001:4860:4860::8844

Domain (optional): example.com

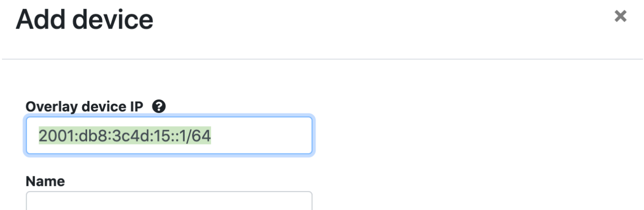
3. Select **Apply**.

Step 3: Discover devices, or create a /64 network object

You can wait for automatic device discovery to detect IPv6 devices and accept them, or you can create an IPv6 network object if you do not need to set policy for individual devices. If you choose to discover and accept individual IPv6 devices, be aware that the devices may have IPv6 privacy extensions enabled that cause the device to obtain a new IPv6 address frequently (approximately every 15 minutes).

To create a IPv6 network object device on the Airwall Gateway for your local /64 network:

1. Go to **Local devices**.
2. Select **Add device**.
3. Under **Overlay device IP**, enter the static IPv6 IP address you set up on the Overlay port group:



Add device

Overlay device IP: 2001:db8:3c4d:15::1/64

Name:

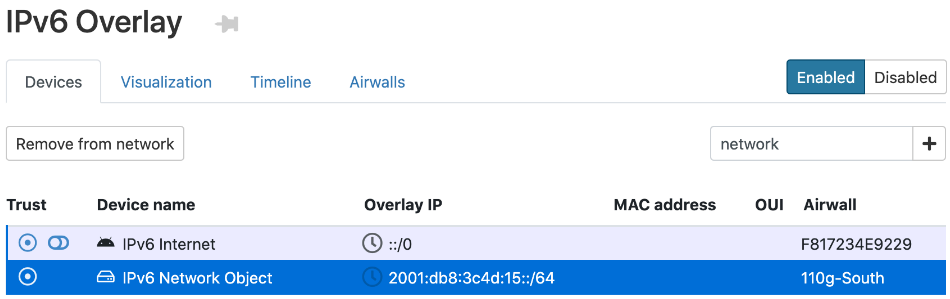
4. Fill in other device details, and then select **Create**.

Step 4: Repeat for one or more Airwall Gateways

Repeat steps 1-3 above for additional Airwall Gateways.

Step 5: Set up trust between IPv6 devices

Add the IPv6 network objects (or discovered IPv6 devices) to an overlay, and set up trust between them. See Create an overlay network on page 418 and Add and remove device trust on page 427.



IPv6 Overlay

Trust	Device name	Overlay IP	MAC address	OUI	Airwall
⊙ ◯◯	IPv6 Internet	::/0			F817234E9229
⊙	IPv6 Network Object	2001:db8:3c4d:15::/64			110g-South

Result

IPv6-capable devices connected to these Airwall Gateways can now:

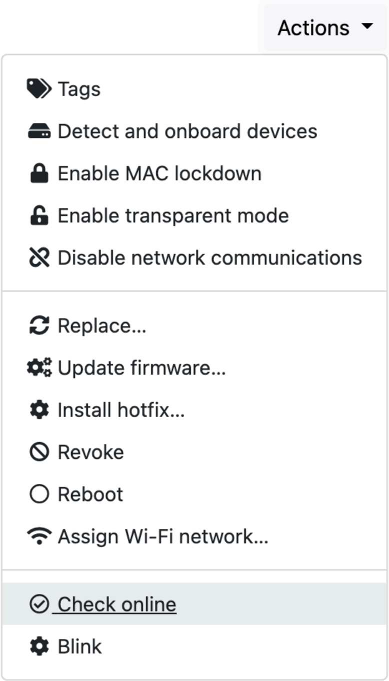
- Obtain an IPv6 address
- Use the Airwall Gateway as their IPv6 default gateway
- Communicate with each other

Note: Some devices may require special configuration to enable IPv6 or IPv6 auto configuration.

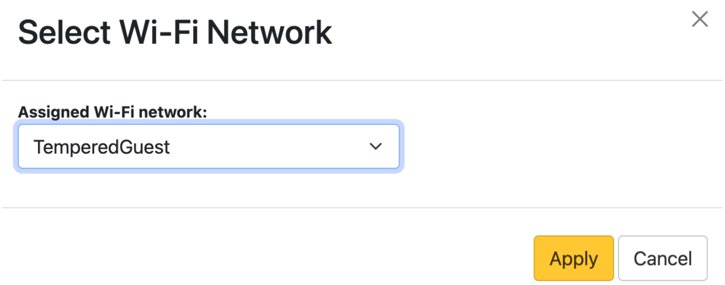
Set the Wi-Fi network for an Airwall Gateway

You can set the Wi-Fi network for an Airwall Gateway to use.

1. Configure the Wi-Fi network on your Conductor. For details, see Configure Wi-Fi Settings on page 241.
2. In the Conductor, open an Airwall Gateway with wireless capabilities.
3. On the right, open **Actions**, and select **Assign Wi-Fi network**.



4. Under Assigned Wi-Fi network, select the Wi-Fi network you want this Airwall Gateway to use.


Select Wi-Fi Network

Assigned Wi-Fi network: TemperedGuest

If you're having problems connecting, try some of the troubleshooting suggestions in Troubleshoot Initial Airwall Gateway connections on page 491 or Measure wireless signal strength - WiFi and cellular on page 497.

You can also set the Wi-Fi network directly on the Airwall Gateway:

- **Airshell `setup-ui` command** – For more information, see Configure an Airwall Gateway with the airsh Setup Wizard on page 274.
- **Diagnostic mode** – For more information, see Put an Airwall Gateway into diagnostic mode on page 478.

Configure an authenticated Airwall Agent or Server session

An authenticated Airwall Agent or Server session requires users to authenticate before the Airwall Agent or Server can communicate in an overlay network. The authentication is based on a user's Conductor login credentials.

Note: Authenticated Airwall Agent or Server sessions expire after 15 minutes of inactivity, or within 24 hours of user log in.

To configure authenticated Airwall Agent or Server sessions:

1. Go to **Airwalls** and select an Airwall Agent or Server.
2. Select **Edit Settings**.
3. Under **Airwall agent authentication**, check **Require authenticated Airwall session**
4. Select **Update Settings**.
5. Point your web browser to a secure (HTTPS) web URL using one of the remote device IP addresses.
6. In the HTTPS login page, enter the Airwall Agent or Server Conductor username and password.

   Note: If the Airwall Agent or Server is a member of two or more overlay networks, select the overlay networks in which the Airwall Agent or Server will participate.

Once authenticated, the Airwall Agent or Server participates in the selected overlay network.

Note: To activate an Airwall Agent or Server in a different overlay network, you must reboot the Airwall Agent or Server, re-authenticate, and select the new overlay network.

Configure Advanced Airwall Edge Service Options

Add or Replace a Signed Certificate on an Airwall Gateway for Conductor Communication

By default, the Airwall Gateways come with a Tempered factory-installed certificate. You can add your own custom CA certificate to use for Conductor communication.

Supported Versions	2.2.10 Airwall Gateways and Conductor
Supported on these Airwall Edge Services	Airwall Gateways

Note: When you are in the process of replacing a certificate, the Airwall Gateway uses the existing certificate until the replacement is complete.

Note: For HA-paired Airwall Gateways, you can have a custom certificate on one or both.

Before you Begin

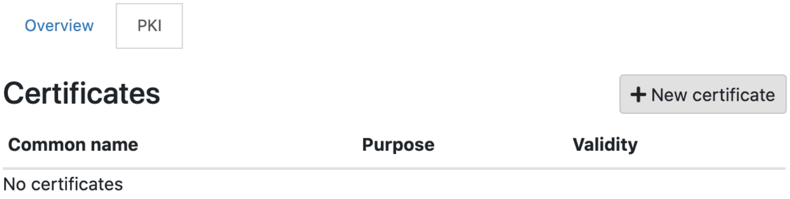
Before you can upload or replace a signed certificate, you need to have a CA certificate chain installed so that the Conductor can verify the certificates. For more information, see Install a Custom CA Certificate Chain on page 239.

Requesting and copying a CSR (Certificate Signing Request) for the Airwall Gateway

Once you have installed CA certificates (see Install a Custom CA Certificate Chain on page 239), you can generate a Certificate Signing Request (CSR) to create a certificate (for example, with a PKI Registration Authority) for Airwall Gateway to Conductor Communication:

1. In Conductor, open the Airwall Gateway to which you want to add a custom CA certificate.
2. Go to **Airwall gateway** > **PKI**.

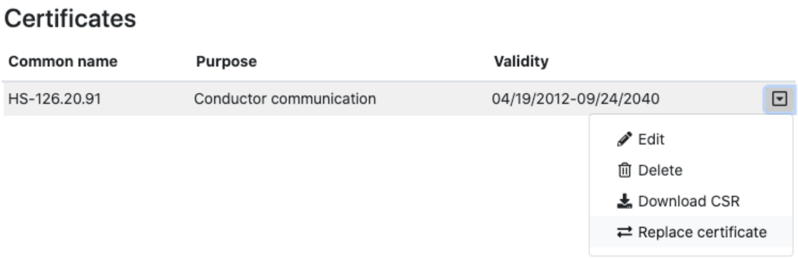
   Note: If the **PKI** tab is not visible, either the Conductor does not have custom CA certificate chain uploaded and you need to Install a Custom CA Certificate Chain on page 239, or the Airwall version is not 2.2.10 or later.
3. Select **Get certificate**.



Certificates

Common name	Purpose	Validity
No certificates		

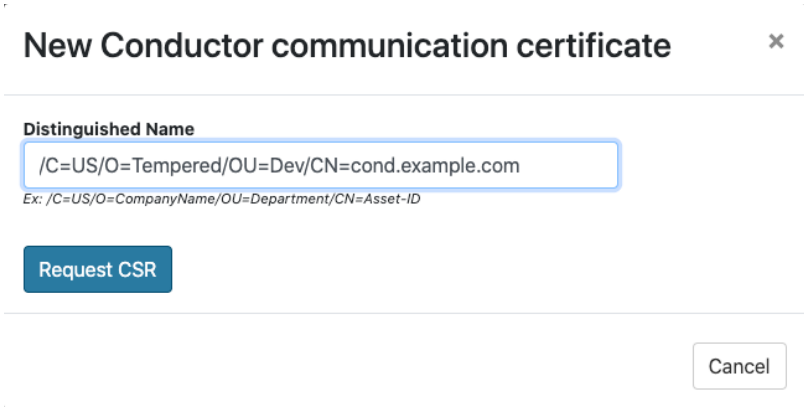
If you are replacing a certificate, open the **Actions** menu on the existing certificate and select **Replace certificate**.



Certificates

Common name	Purpose	Validity
HS-126.20.91	Conductor communication	04/19/2012-09/24/2040

4. If you are adding a new certificate, under **Distinguished Name**, enter the Identity (Distinguished Name) for the certificate. For example, `/C=US/O=Tempered/OU=Dev/CN=cond.example.com`



New Conductor communication certificate

Distinguished Name

/C=US/O=Tempered/OU=Dev/CN=cond.example.com

Ex: /C=US/O=CompanyName/OU=Department/CN=Asset-ID

Note: If you are replacing a certificate, the Distinguished name remains the same.

5. Select **Request CSR**.
6. Under **CSR**, select either **Copy** or **Download** to generate and get the CSR you need to get a signed certificate.
7. Select **Cancel** to close the dialog, or leave it up while you get the signed certificate.

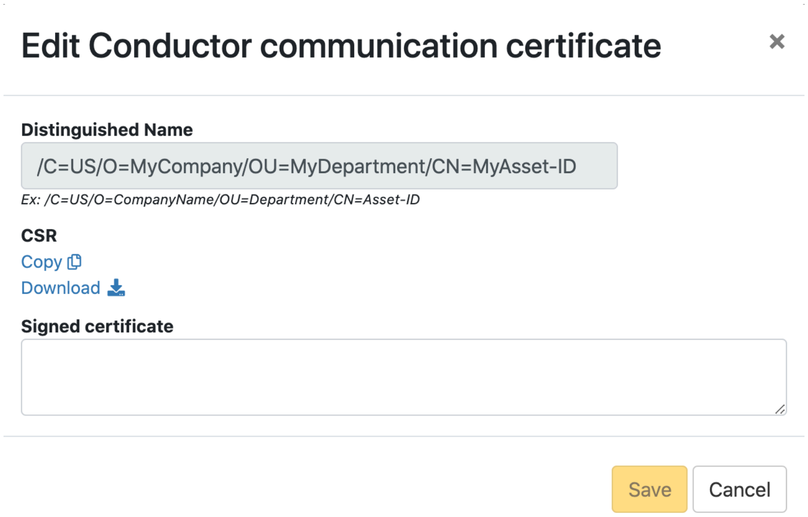
Getting a signed certificate

Use the CSR to request a new signed certificate. You can generate a new signed certificate using your organization's own process, or with a public PKI Registration Authority.

1. Submit the Certificate Signing Request (CSR) you copied or downloaded to your Enterprise PKI Registration Authority. They use it to create your certificates.
2. When you get the certificates, download or copy them.

Uploading the signed certificate to the Airwall Gateway

1. In Conductor, open the Airwall Gateway for which you have a custom CA certificate.
2. Go to **Airwall gateway** > **PKI**.
3. Open the **Actions** menu on the existing certificate and select **Edit**
4. Under **Signed Certificate**, paste the custom-CA signed certificate to install the certificate on the Airwall Gateway.



Edit Conductor communication certificate

Distinguished Name

/C=US/O=MyCompany/OU=MyDepartment/CN=MyAsset-ID

Ex: /C=US/O=CompanyName/OU=Department/CN=Asset-ID

CSR

Signed certificate

5. Select **Save**.

Set up Port Groups on an Airwall Gateway

The default port groups work for some deployments. You may need to set up underlay or overlay port groups if your deployment requires it.

Set up Overlay Port Groups

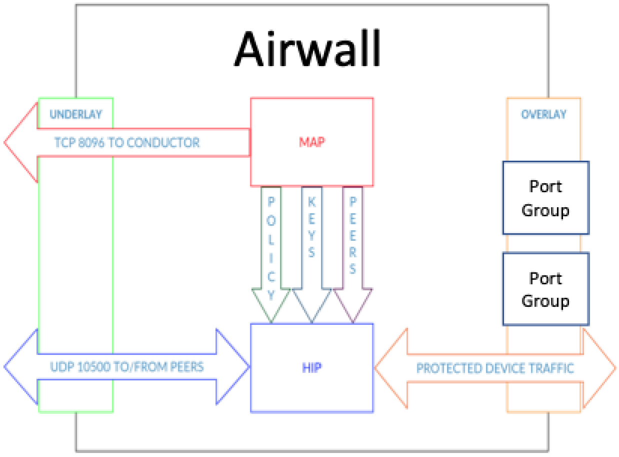
The default port groups work for some deployments. You may need to set up overlay port groups if your deployment requires it.

Overlay Port Groups are used to connect your Airwall Gateway to your protected networks. Airwall Gateways default to having a single overlay Port Group, but you may need to configure your overlay port groups when you want to:

- Micro-segment your network for fine grain security control
- Configure IP addresses or Source NAT (SNAT) for routed deployments
- Set up two Airwall Gateways for High Availability

If your Airwall Gateway is only providing relay functionality, it only needs an Underlay Port Group, and does not use any configured Overlay port group.

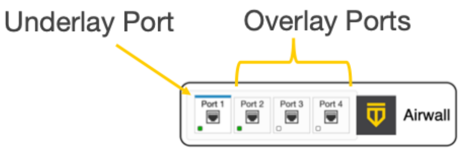
You can set up multiple port groups for an overlay, assigned to different physical or VLAN tagged sub-interface ports. When multiple ports are included in a Port Group, they are bridged. Port groups are also connected to the overlay through routing and/or bridging.

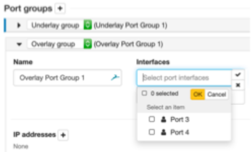


Get to Know Your Airwall Gateway Ports

Here is how the physical ports are assigned on most Airwall Gateways:

- Port 1 – Connects to the initial underlay network, and is assigned to the underlay Port Group.
- Port 2 & Up – Connect to overlay networks, and are assigned to an overlay Port Group.




Port groups +

Underlay group (Underlay Port Group 1)

Overlay group (Overlay Port Group 1)

Name: Overlay Port Group 1

Interfaces: Select port interfaces

□ 0 selected OK Cancel

Select an item

□ Port 3

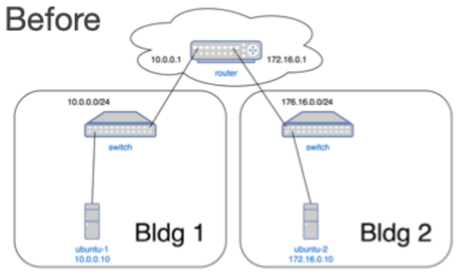
□ Port 4

IP addresses +

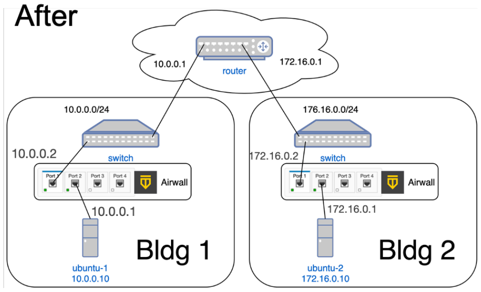
None

Basic Airwall Gateway Deployment

The most basic Airwall Gateway deployment design is to put Airwall Gateways inline in front of protected devices. If you don't want to, or can't, change IP addresses, you replicate the default gateway of the router on the overlay Port Group. (If these devices are using DHCP, see Protected devices with static routing on page 409 to configure DHCP on the overlay port group.)



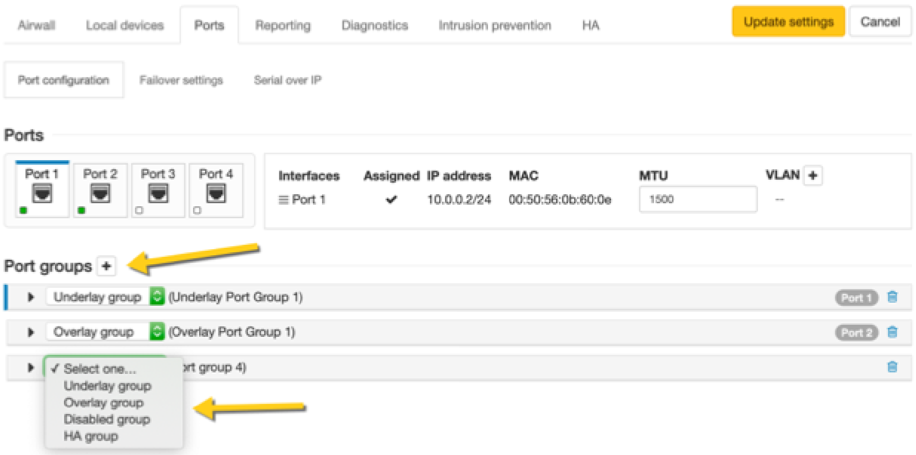
The underlay IP address can be any address on the network. DHCP is common, or you can configure a static IP if needed. The overlay IP address is the same as the default gateway on the router.



Set up an Overlay Port Group

By default, an Airwall Gateway has two port groups. One underlay port group assigned to Port 1 and one overlay port group assigned to the remaining ports. On virtual and cloud Airwall Gateways, you may be able to configure more ports if supported by the virtual or cloud platform.

1. In the Conductor, go to the Airwall Gateway on which you want to set Port Groups, open the **Ports** tab, and select **Edit Settings**.
2. Select an Overlay port group you want to use, or add a new port group by clicking the + to the right of **Port groups**, and select **Overlay group**.



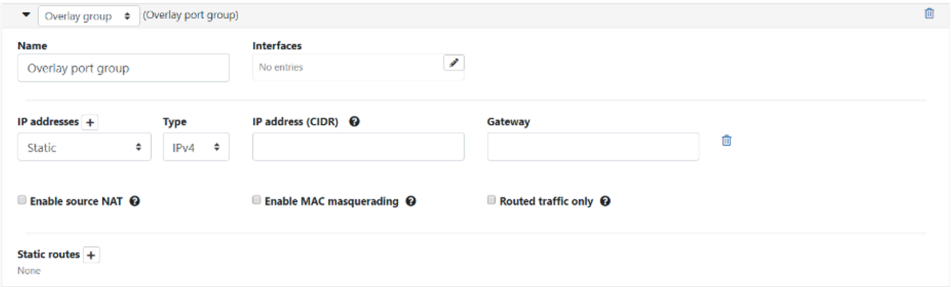
Interfaces	Assigned	IP address	MAC	MTU	VLAN +
≡ Port 1	✓	10.0.0.2/24	00:50:56:0b:60:0e	1500	--

Underlay group (Underlay Port Group 1)

Overlay group (Overlay Port Group 1)

rt group 4)

3. Click the arrow on the left of your **Overlay group** header to expand the settings for that Port Group.



Name: Overlay port group

Interfaces: No entries

IP addresses: Static | Type: IPv4

□ Enable source NAT □ Enable MAC masquerading □ Routed traffic only

Static routes: None

4. Enter a name for the group, and under **Interfaces**, select the ports or other interfaces for the group.
5. Under **IP addresses**, click the + to add IP addresses. For example, 10.0.1.1/24 (be sure to include the prefix length). Your protected devices will use this address as their gateway to reach the rest of your overlay network.
6. Select the network options that apply for your implementation:
   a) **Enable Source NAT** – Check this box to rewrite the source IP address of traffic arriving from other port groups or tunnels with the overlay IP address of this port group. You must also configure an overlay IP address. Use this option when your local protected devices do not use this Airwall Gateway as their default gateway. This setting enables connections, permitted by policy, from remote overlay devices to local protected devices. When you enable Source NAT, local protected devices cannot initiate connections to remote overlay devices.
   b) **Enable MAC masquerading** – Check this box to rewrite the source MAC address of all traffic arriving from other port groups or tunnels with the Airwall's MAC address. Use this option if the network you are connected to doesn't permit foreign MAC addresses. Note: Checking the Routed traffic only box enables MAC masquerading by default.
   c) **Enable spanning tree protocol** – Leave this box checked to enable spanning tree protocol on the overlay bridge to avoid potential bridge loops. Only clear this box if this port group is free of any bridge loops, and you do not wish to run STP. One example is if this port group is connected to a Cisco switch running BPDU guard. A recommended alternative is to configure the port group with only a single port and use routed traffic only mode to make bridge loops impossible.
   d) **Routed traffic only** – Check this box to permit only routed bypass traffic. You must also configure an overlay IP address. Local protected devices should use this overlay IP as a gateway (either their default gateway or a static route) or Source NAT to allow incoming connections. Typically, you check Routed traffic only, unless you specifically need to bridge traffic. For example, if you have IP addresses in the same subnet on both sides of the tunnel, you are bridging traffic, so clear this box.

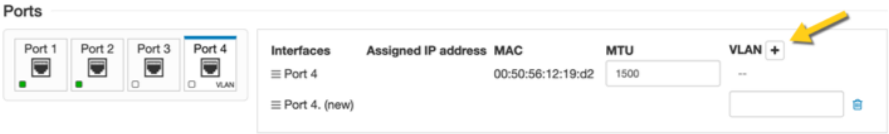
      This setting prevents inadvertently carrying broadcast and multicast traffic sent by protected devices and can improve performance by using only a single port in the port group.
7. If you are connecting this port group to a router connected to a larger overlay network, you can configure static routes or even a default gateway.

8. Select **Update Settings**.

Add Interfaces to a Port

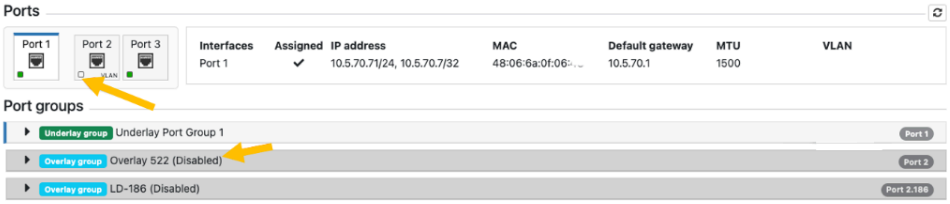
Each physical or logical port on an Airwall Gateway has a single interface by default, that can be assigned to a port group. If you are connecting an Airwall Gateway port to a switch using an 802.1q trunk allowing multiple VLANs, you need to add additional interfaces. To do this:

1. Up above the **Port Groups** section, select the **Port** and then click **Edit Settings**.
2. Next to **VLAN**, click the **+** to add a new VLAN for this overlay.
3. Enter the VLAN tag to match the VLAN config on the switch.



Interfaces	Assigned IP address	MAC	MTU	VLAN +
≡ Port 4		00:50:56:12:19:d2	1500	--
≡ Port 4. (new)				

Note: If you disable the VLAN parent interface, the child interfaces are also disabled.



Interfaces	Assigned	IP address	MAC	Default gateway	MTU	VLAN
Port 1	✓	10.5.70.71/24, 10.5.70.7/32	48:06:6a:0f:06:...	10.5.70.1	1500	

Port groups

- Underlay group Underlay Port Group 1 — Port 1
- Overlay group Overlay 522 (Disabled) — Port 2
- Overlay group LD-186 (Disabled) — Port 2.186

Do I need a gateway?

You only need a gateway if the Airwall Gateway needs to know how to reach additional networks from this port. The Airwall Gateway is the gateway for its protected devices. In general, using static routes (for example, 10.0.0.0/8) for your corporate network is preferable to using a default gateway (which is a 0.0.0.0/0 route), particularly if you have a bypass destination of 0.0.0.0/0 set up, since that will cause a conflict.

Set up an Underlay Port Group

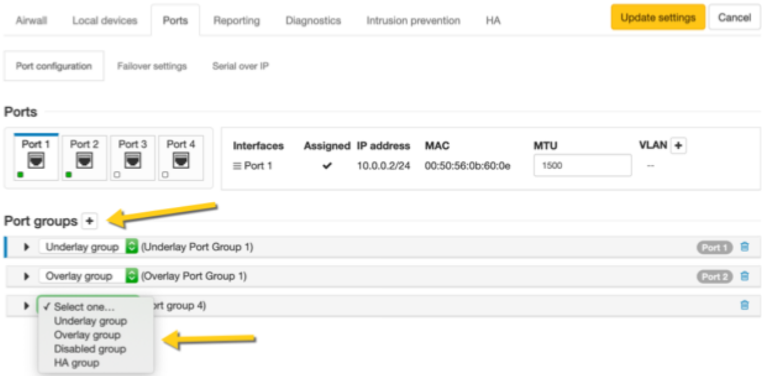
By default, an Airwall Gateway has two port groups. One underlay port group assigned to Port 1 and one overlay port group assigned to the remaining ports. On virtual and cloud Airwall Gateways, you may be able to add additional ports by creating new virtual network adapters on the hypervisor. Some hardware models allow you to add new ports by inserting port expansion modules.

All non-cellular ports allow adding VLAN sub interfaces.

You may want multiple underlay port groups on wireless Airwall Gateways. You can configure one port group for the wireless port and one for a wired port and assign different priorities to the two port groups. This allows the Airwall Gateway to automatically fail over to whichever port is available based on the assigned priorities.

It can also be useful to have multiple wired underlay port groups to allow an Airwall Gateway to communicate on separate networks at the same time. For example on a relay Airwall Gateway, you could configure one underlay port group on a DMZ and the other on the corporate network (multi-homing).

1. In the Conductor, go to the Airwall Gateway on which you want to configure port groups, go to **Ports** > **Port configuration**, and select **Edit Settings**.
2. Select an Underlay port group you want to use, or add a new port group by clicking the + to the right of Port groups, and select Underlay group.



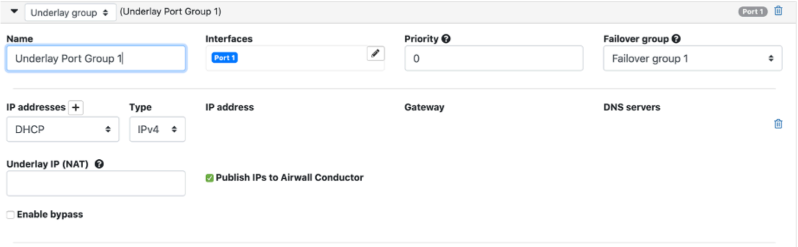
Interfaces	Assigned	IP address	MAC	MTU	VLAN +
Port 1	✓	10.0.0.2/24	00:50:56:0b:60:0e	1500	--

Underlay group (Underlay Port Group 1) Port 1

Overlay group (Overlay Port Group 1) Port 2

✓ Select one... / Underlay group / Overlay group / Disabled group / HA group (Port group 4)

3. Click the arrow on the left of your Underlay group header to expand the settings for that Port Group.



Underlay group (Underlay Port Group 1) Port 1

Name: Underlay Port Group 1

Interfaces: Port 1

Priority: 0

Failover group: Failover group 1

IP addresses: DHCP, Type: IPv4

Underlay IP (NAT):

☑ Publish IPs to Airwall Conductor

□ Enable bypass

4. Enter a name for the group, and under **Interfaces**, select the port interfaces for the group.
5. Under **Priority**, set the priority for this underlay port group. 0 is the highest priority. The Airwall Gateway will always try to use the underlay port with the lowest priority value if the network is available.
6. (Optional) **Under Failover group**, select the Failover group. Failover groups allow traffic monitoring for a given traffic type (Conductor traffic or data plane traffic). The failover groups define how to monitor the availability of the port groups contained in the failover group, and when port groups should fail over to another port group. Only a single port group is used at a time. Failover groups are configured separately on the **Failover settings** tab.

   You can select `Stand-alone` to make the port group permanently available independent of any other underlay port group.
7. Under **IP addresses**, click the + to add an IP address. You can choose between DHCP or static address configuration. The **Underlay Port Group IP address** may be already configured if you configured its initial IP address when setting up the Airwall Gateway.
8. Under **Underlay IP (NAT)**, If this Airwall has a public IP, you can add it here. Remote Airwall Edge Services will then attempt to connect to the public IP instead of the IP configured on the underlay port group.
9. Check **Publish IPs to Airwall Conductor** to advertise the IP address of this underlay port group to remote Airwall Edge Services to build secure tunnels. In a hub and spoke Airwall deployment you may want to leave this unchecked on the spoke Airwall Gateways if tunnels are always established from the spoke to the hub. This configuration reduces network traffic related to IP address advertising.
10. Check **Enable bypass** to allow traffic from protected devices behind this Airwall Gateway to reach destinations on the underlay network. Traffic to these destinations can be configured just like normal overlay traffic using the policy editor. You can configure bypass destinations on the **Devices** tab. Clear this box to disable bypass traffic over this underlay. You can only enable bypass on a single underlay port group on each Airwall Gateway.
11. If you have enabled bypass, you can choose to **Enable source NAT**. This option replaces the source IP of packets leaving the Airwall Gateway with the IP of the port group, and may be required to allow routing between the IP addresses on the device network and the bypass destinations.
12. If your network requires it, you can add additional static routes as needed.
13. Select **Update Settings**.

Replicate Port Settings

For minimal disruption and less room for error, you can replicate the port configuration between two Airwall Gateways when setting up an Airwall Gateway HA pairing, or when replacing an Airwall Gateway.

Follow these links for more information on how it works in each situation:

- Configure High Availability Airwall Gateways (v2.2.8 and later) on page 399
- Replace an Airwall Gateway on page 132

Configure an Underlay Port Failover Group

Starting in v2.2.8, a failover group is created and set by default. For earlier and updated Airwalls, you may need to create and set it yourself.

1. On an Airwall Gateway, go to **Ports** > **Failover settings**.
2. Next to **Failover Groups**, click the plus sign (+) to create a new Failover group.
3. Name your group, and if needed, change the default settings for the Failover group.
4. Go to **Ports** > **Port configuration**, and select **Edit Settings**.
5. Under **Failover group**, select the new group you created.
6. Select **Update Settings**.

Best Practices for Underlay Port Failover Groups

Set your underlay failover settings to a Failover group as a best practice.

Find your version below for guidelines, and for detailed instructions, see Configure an Underlay Port Failover Group on page 391.

Best Practice for v2.2.8 and later

In v2.2.8 and later, Underlay failover settings are set to an auto-created failover group, “Failover Group 1,” by default. You can create additional groups or edit the default group settings to adjust failover behavior for your underlay port groups. **Stand-alone** is still available, but it is deprecated and not recommended. See Configure an Underlay Port Failover Group on page 391.

CAUTION: Do not enable HIP on multiple underlay port groups connected to the same network or networks that egress through the same NAT gateway. If you do this, and then connect to a relay or other Airwall Edge Service outside, the NAT gateway can cause the HIP tunnel to flap between states through the NAT gateway.

Best Practice for v2.2.1 to v2.2.5

In v2.2.1 to v2.2.5, underlay failover settings are set to **Stand-alone** by default. Configure an Underlay Port Failover Group on page 391 and then change the Port Group failover setting from **Stand-alone** to the new Failover Group you created. See Configure an Underlay Port Failover Group on page 391.

Manage Failover between Underlay Port Groups

Set up your Airwall Gateways with multiple wired and wireless underlay port groups and configure which port group to use based on simple network criteria.

Supported roles	• System Administrator • Network administrator with permissions to edit Airwall settings

Managing the Active Network with Failover Groups

You can assign one or more failover groups to underlay port groups on an Airwall Gateway. Failover groups continuously monitor health indicators on the networks of their assigned port groups and manage which one is active based on both the current network health indicators and a relative priority assigned to each port group within the failover group.

The health criteria that a failover group monitors on the network are:

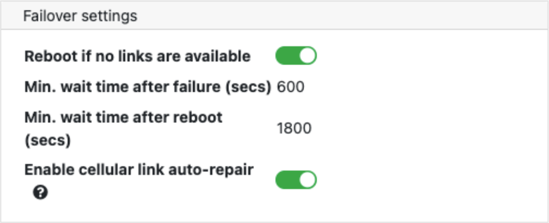
- **Wired interface link status** – If the failover group detects that a port is missing a link, or the layer 3 configuration is bad (for example, has no IP address), the port group is considered failed and is not selected.
- **Cellular modem status** – If there are error conditions on the cellular modem, the failover group sets the corresponding cellular port group as failed.

- **Active monitoring of selected destinations** – You can specify destinations to have the failover group actively check if they are responding. It will ping these destinations and monitor their response. If the pings are successful, the corresponding underlay port group is considered functional. See **Ping Settings** below.
- **Passive monitoring** – The Airwall Gateway uses the currently active Conductor connection as a secondary indicator to determine network health if no active monitor is running.

Based on these monitoring criteria, the failover group scores each assigned port group and selects the one with the highest score. If more than one port group gets the highest score, the failover group selects the port group that has the highest priority.

Set Failover group settings for the Airwall Gateway

1. Go to **Airwalls** and select an Airwall Gateway.
2. Go to **Ports** > **Failover settings**.
3. Under **Failover settings**, set the common settings to be used by all port failover groups on the Airwall Gateway:



Failover settings

Reboot if no links are available ●

Min. wait time after failure (secs) 600

Min. wait time after reboot (secs) 1800

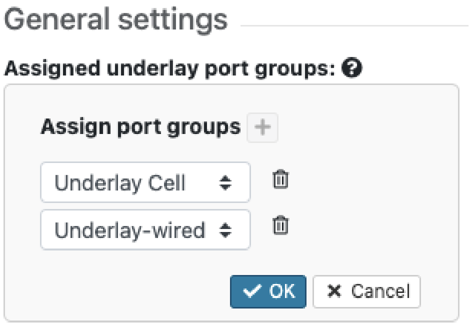
Enable cellular link auto-repair ●

   - **Reboot if no links are available** – Enable to reboot the Airwall Gateway if none of the failover groups have any healthy networks, in an attempt to restore the network. The following additional settings also apply to the reboot:
     - **Min. wait time after failure** – Specify how many seconds to wait after detecting that all **port groups** have failed before rebooting. **Default**: 600 seconds
     - **Min. wait time after reboot** – Specify how many seconds to wait before the next reboot if the network remains unavailable after a reboot. Set this to a higher value than the initial wait time to prevent constant reboot loops if the network is unavailable for extended time periods. **Default**: 1800 seconds
   - **Enable cellular link auto-repair** – Enable on cellular Airwall Gateways only to attempt to restore a failed cellular modem after detecting that the cellular network is not responding (by re-initializing the modem drivers).

Note: For these settings to take effect, you need to set up at least one failover group on this Airwall Gateway.

Create a Port Failover Group

1. Under **Failover group**, select the + (plus sign) to create a new failover group. The Conductor creates a new failover group with default values. You can click on the name to edit it.
2. Under **General settings** > **Assigned underlay port group**, assign underlay port groups to this failover group:



General settings

Assigned underlay port groups:

Assign port groups

Underlay Cell

Underlay-wired

   a) Click on this setting to edit it.

b) Next to **Assign port groups**, select the + (plus sign) to add one of the unassigned underlay port groups to this failover group.

c) Select the arrows to choose a different port group, and arrange them from top to bottom in priority order.

d) Select **OK** to save your settings.

3. Still under **General settings**, select the traffic types:

   a) **Allowed traffic types** – Click on this setting to edit it. Select one or more underlay traffic types for the failover group to manage. Select **OK** to save:

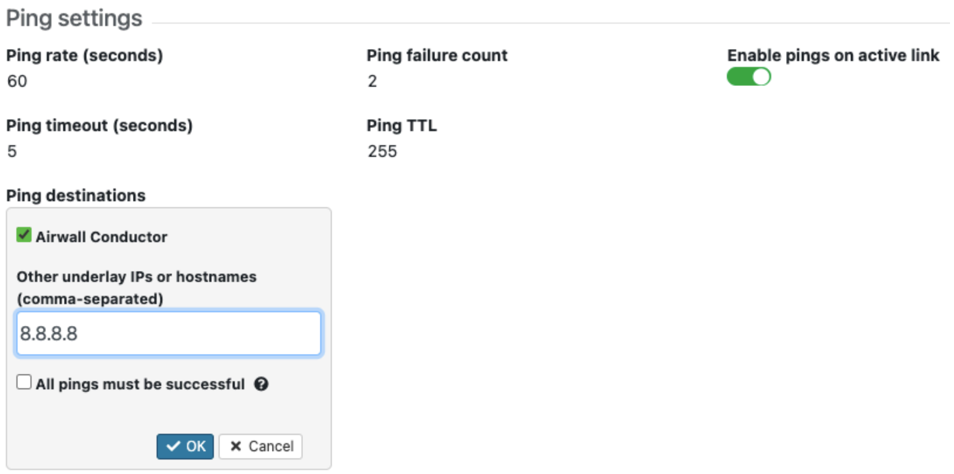
      - **HIP** – Encrypted overlay traffic between Airwall peers

        CAUTION: Do not enable HIP on multiple underlay port groups connected to the same network or networks that egress through the same NAT gateway. If you do this, and then connect to a relay or other Airwall Edge Service outside, the NAT gateway can cause the HIP tunnel to flap between states through the NAT gateway.

      - **Conductor** – TLS-encrypted traffic between the Airwall Gateway and the Conductor
      - **Bypass** – Bypass traffic leaving the overlay to the underlay. Selecting Bypass is only useful if you have set up at least one bypass port group on the Airwall Gateway.

   b) Select **OK** to save your settings.

4. Under **Ping settings**, configure any destinations you want to ping to actively monitor the network, along with the ping settings.



Ping settings

Ping rate (seconds)
60

Ping failure count
2

Enable pings on active link

Ping timeout (seconds)
5

Ping TTL
255

Ping destinations

☑ Airwall Conductor

Other underlay IPs or hostnames (comma-separated)

8.8.8.8

□ All pings must be successful

- **Ping rate** – Set the rate at which the failover group sends out pings, in seconds.
- **Ping failure count** – The number of successive ping failures required to consider the ping monitor failed. If the pings are unreliable, you can set a higher number to help stabilize the network selection.
- **Enable pings on active link** – Disable to suspend pings for the port group that is currently active. The failover group then does only passive monitoring to detect status changes on the port group.
- **Ping timeout** – The time to wait for ping replies before setting the ping as failed, in seconds.
- **Ping TTL** – The time-to-live counter. You usually do not need to change this setting. If you want to speed up the time to failure and know the maximum number of hops to the ping destination, you can set the **Ping TTL** to a lower value.
- **Ping destinations** –

  - Check **Airwall Conductor** to ping the Conductor configured on this Airwall Gateway. Note that checking this option includes any additional Conductors configured on the Airwall Gateway as well as the High-availability (HA)-peer Conductor if Conductor HA is configured.
  - **Other underlay IPs or hostnames** – Add any IP addresses and hostnames to ping, separating them with commas.
  - **All pings must be successful** – Leave this box clear so that only a single ping to any of the IPs must be successful for the ping monitor to be successful (recommended). Check to require that all specified IPs and hostnames must respond to be considered successful.

5. Select **OK** to save your settings.

Managed and unmanaged port groups

By default, when you first create an underlay port group, it is unmanaged, meaning it won't be automatically assigned to any failover group. If a port group is unmanaged, the Airwall Gateway does not monitor health indicators and won't fail over. The Conductor may still use unmanaged ports for any type of traffic, but if an unmanaged port fails, the Airwall Gateway relies on the underlay networking to recover.

Cellular Airwall Gateways automatically create and assign a failover group when initialized or factory reset. This failover group is configured with cellular and wired ports, and assigns the wired port a higher priority than the cellular. Wired-only Airwall Gateways do not create a default failover group and any wired port groups are left unmanaged.

Local Bypass

With local bypass you can separate traffic (split tunnel) going through your Airwall Gateway, where you selectively encrypt and tunnel some traffic, while allowing other traffic to pass through the Airwall Gateway unchanged. This ability also allows protected devices to securely communicate with devices or network locations that are not protected by Airwall Edge Services.

For example, some devices need to communicate with software update servers on the Internet. You can configure the software update servers as a bypass destination and establish trust between the bypass destination and the protected devices. This gives the devices the ability to communicate with the bypass destination, while requiring all other access to pass through encrypted tunnels from other Airwall Gateways.

This configuration of local bypass permits traffic between the secure overlay network and an insecure underlay network, where the Airwall Gateway acts similarly to a SNAT (Source Network Address Translation) gateway. Connections initiated from the underlay network are still blocked, but connections initiated from a protected device to a permitted bypass destination are allowed.

You set up a bypass destination to:

- permit traffic to exit your secure overlay to destinations not protected by an Airwall Edge Service.
- protect all your traffic with Airwall Edge Services as an intermediate step during migration.
- allow local devices to continue to access a protected device.

Prerequisites

- Any other network traffic that you want to send to remote Airwall Gateways must support being routed between subnets, and cannot include broadcast or multicast protocols.
- Devices protected by the Airwall Gateway must either use DHCP, or must be reconfigured to use the new subnet.
- You can set many types of network destinations as bypass destinations. For example:
  - Active Directory Servers
  - Software Update Servers
  - Equipment control systems, such as for HVAC installations
  - The Internet, to bypass to everything on the Internet

Before you begin

Before you begin, you need to:

- Have the IP address or hostname of the device or destination for which you want to create a local bypass.
- If you need or want to use a fully qualified domain name (FQDN) instead of IP for your bypass destination, you need to enable bypass DNS. See Enable DNS lookup for bypass destinations on page 398.

Enabling bypass on the Airwall Gateway

Set up a bypass port on the Airwall Gateway that protects devices that need access to the bypass destination.

1. On the **Airwalls** page, in the **Ports** tab, go to the Underlay Port Group, and select **Edit Settings**.
2. Check **Enable bypass**.

3. If you are setting up an L3 or combined L2 and L3 bypass (recommended), also check **Enable source NAT** and **Routed traffic only**.

Creating a bypass destination

Note: The bypass destination can be shared between all Airwall Gateways on the Conductor that support bypass and have bypass enabled. If you have already set up a bypass destination, you can skip this step.

1. In the Conductor, go to the **Devices** page.
2. On the **Devices** tab, click **New bypass destination**.
3. Enter the bypass destination:
   - Under **IP address**, enter the IP for the destination of the local bypass device. For example, to create a bypass destination for the Internet, enter 0.0.0.0/0.
   - Or, if you have enabled DNS for bypass destinations, under **Hostname**, enter a fully-qualified domain name (FQDN) instead of an IP address. For example, google.com. For more information, see Enable DNS lookup for bypass destinations on page 398.
4. Ignore the MAC options.
5. Optional: Add a description and tags to help identify the bypass destination.
6. Click **Create**.
7. Set trust between the bypass destination and protected devices, see Create an overlay network and Add and remove device trust.

   Note: If you intend to add trust to a DNS bypass location, you must first add trust to a DNS server bypass destination.
8. To view and edit bypasses, click **Devices** > **Show all devices** > **Bypass destinations**.

Backhaul Bypass

Set up backhaul bypass to allow any v3.0 or later Airwall Gateway to reach bypass destinations by tunneling traffic using designated bypass egress Airwall Gateways. Optionally, you can use a regional backhaul bypass pool for Airwall Gateways that support backhaul bypass and are not gateways themselves. See Region Bypass.

Supported roles	• System Administrators • Network Administrators with the “Can view and edit bypass destinations” permission
Supported versions	• Airwall Gateways and Conductor v3.0 and later. • For region bypass both the Conductor and the Airwall Gateways must be v3.2.3 or later.

Note:

- You can use backhaul bypass for any bypass destination including destinations using hostnames.
- Backhaul bypass can use relays just like normal overlay traffic. The Airwall Relay does not require any special configuration.
- You can set up backhaul Airwall Gateways with multiple bypass-enabled underlay port groups and use link manager to fail over between them. See Manage Failover between Underlay Port Groups on page 391.

Prerequisites

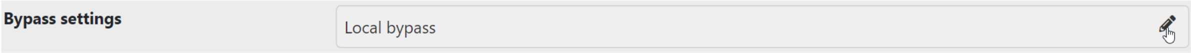
- As a best practice, enable source NAT (SNAT) and routed-only mode on the bypass port group.
- When using hostname bypass destinations, they must meet these requirements:
  - The DNS server used by the overlay device must be on the Conductor-configured allow-list for bypass DNS.
  - The traffic path to resolve hosts must follow the same path on the overlay as the traffic to the actual bypass destination. This means that the DNS server itself must be a bypass destination and the overlay devices using it must have policy to it.

Configuring an Airwall Gateway as a bypass egress gateway

Configuring an Airwall Gateway as a bypass egress gateway allows other Airwall Gateways to use it to access bypass destinations.

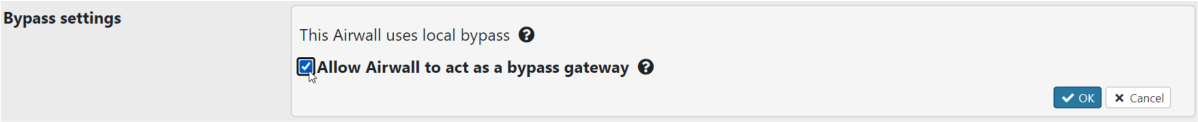
Note: Before you begin, you must set up one or more Airwall Gateways with local bypass, including creating bypass destinations, creating an overlay with devices and the bypass destination, and adding trust. See Local Bypass on page 394.

1. Go to the **Airwalls** page and open an Airwall Gateway.
2. In Bypass settings, click the edit icon ✎. If Bypass settings reads **Bypass is disabled**, go to the **Port** tab, click **Edit Settings**, select an underlay port, and click **Bypass enabled**.



Bypass settings: Local bypass

3. Check **Allow Airwall to act as a bypass gateway**.



Bypass settings

This Airwall uses local bypass

☑ Allow Airwall to act as a bypass gateway

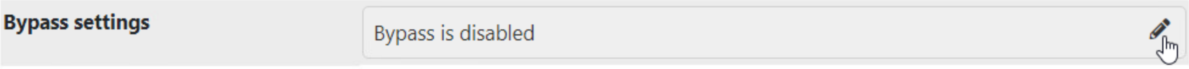
4. Click **OK**.
5. Optional: Set up a bypass Airwall Gateway to be the default for your Airwall secure network. The default is used for all v3.0 Airwall Gateways that do not have a local bypass set up and do have trust set up to the bypass destination on an overlay. You can assign a bypass gateway using Bulk Configuration of Airwall Edge Services on page 378.

   Note: If you want to use FQDNs for your DNS servers, check that the DNS resolver has access through the same tunnel as backhaul bypass. For example, backhaul to your corporate office and use the DNS resolver there. This access allows the egress gateway to learn the DNS FQDNs. Also, note that some common DNS over HTTPs (DoH) or DNS over TLS (DoT) settings (for example, on Google Chrome) can prevent hostname based policies from working.

Selecting a specific bypass egress Airwall Gateway

Once you set up a bypass egress Airwall Gateway, you can set up other Airwall Gateways to use it to reach bypass destinations.

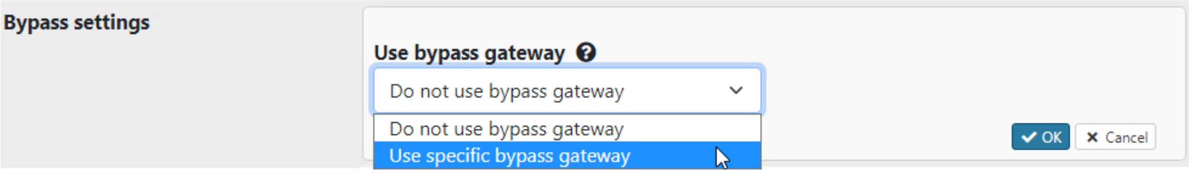
1. Go to the **Airwalls** page and open the Airwall Gateway that you want to reach a bypass destination through a bypass egress Airwall Gateway.
2. Go to the **Airwall Gateway** tab and click the edit icon ✎ in **Bypass settings**.



Bypass settings: Bypass is disabled

Note: You must not have bypass enabled on any of the underlay port groups. If Bypass settings reads **Local bypass**, go to the **Ports** tab and uncheck **Bypass enabled** in all underlay port groups.

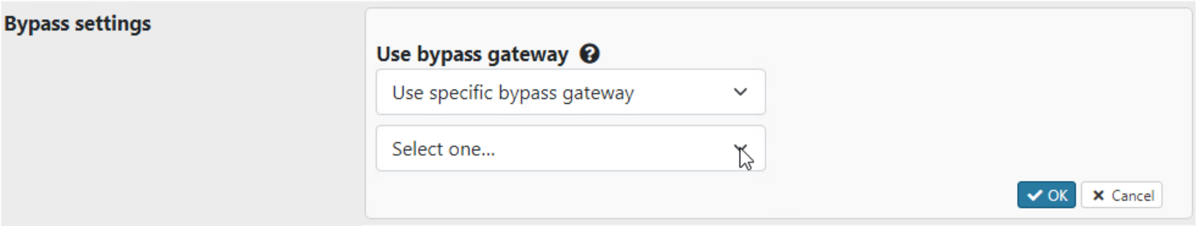
3. From the dropdown menu, select **Use specific bypass gateway**.



Bypass settings

Use bypass gateway: Do not use bypass gateway

4. In the additional dropdown menu, select the required bypass egress gateway and click **OK**.



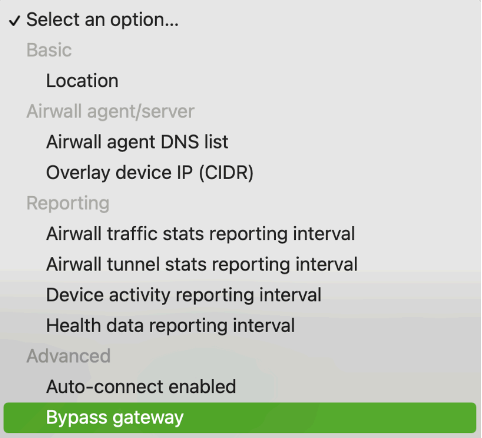
Bypass settings

Use bypass gateway

Use specific bypass gateway

Select one...

Note: You can also set this option in bulk. See Bulk Configuration of Airwall Edge Services on page 378, and choose the bypass gateway option:

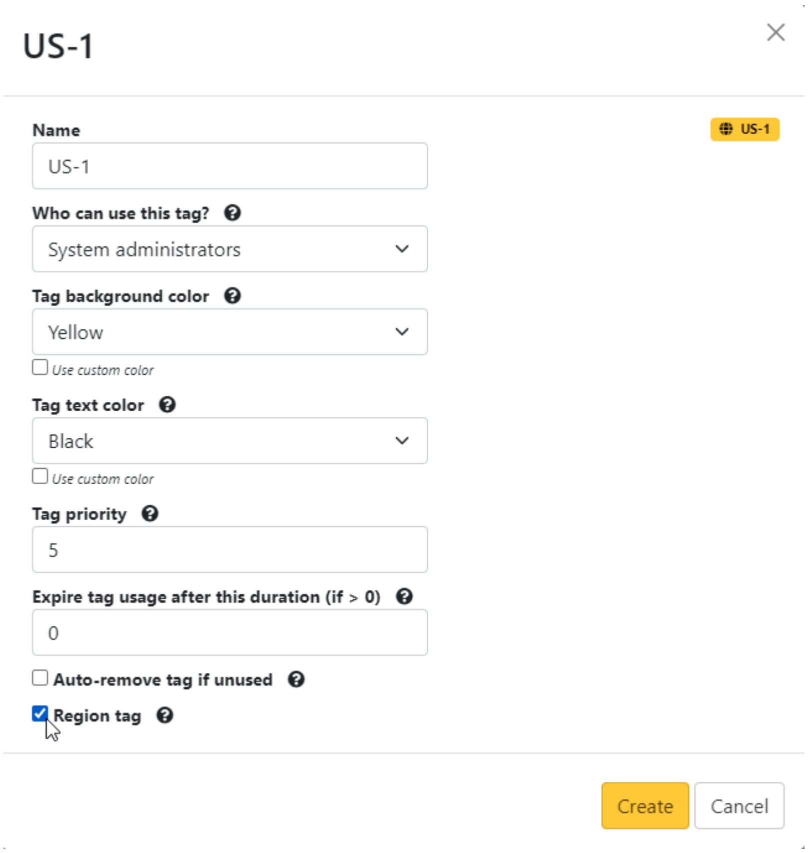


5. In an Overlay, add trust from this Airwall Gateway's local devices to the bypass destination.

Region bypass

Use a region bypass to group and load balance bypass Airwall Gateways by region. A region bypass is configured by creating a region tag. Add the region tag (or tags) to one or more bypass egress gateways and to the Airwall Gateways you want to use with the region bypass egress gateways. To create a tag in the Conductor, complete the following steps:

1. Select the Tags icon 🏷.
2. Click **New tag**.
3. Give the tag a name and fill in the required information. See Create a Tag on page 100.
4. Select **Region tag**.


US-1

🌐 US-1

Name: US-1

Who can use this tag?: System administrators

Tag background color: Yellow

☐ Use custom color

Tag text color: Black

☐ Use custom color

Tag priority: 5

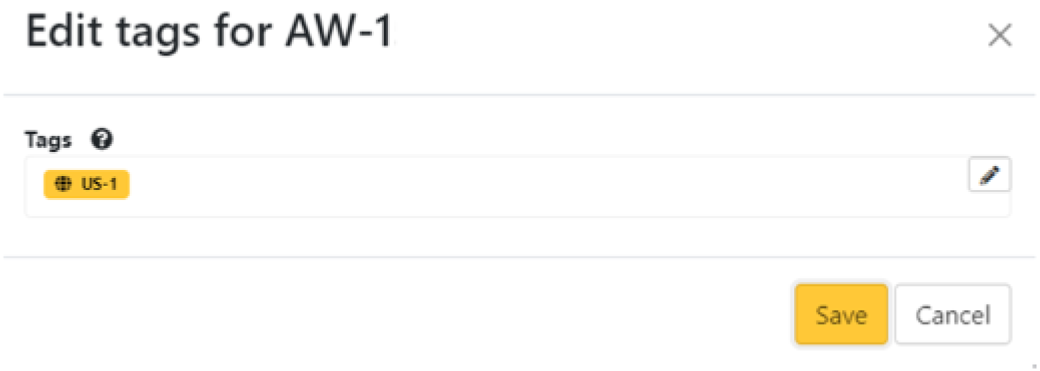
Expire tag usage after this duration (if > 0): 0

☐ Auto-remove tag if unused

☑ Region tag

5. Select **Create**.

   Note the region tag icon 🌐 for easy identification.
6. Go to the Airwall tab and select the Airwall you want to use with the region bypass egress gateway.
7. Select **Actions** > **Tags** and choose the region tag from the drop down menu.


Edit tags for AW-1

Tags: 🌐 US-1

8. In Bypass Settings, click the edit icon and then select **Use regional bypass gateway pool** from the drop down menu.
9. Return to the Airwall list and find the bypass egress gateway you want to use.

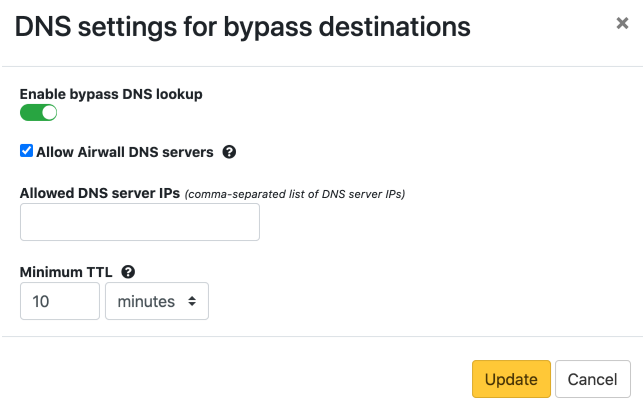
   Note: To be a bypass egress gateway, the Bypass Settings must be set to **Acting as a bypass egress gateway**.
10. Select **Actions** > **Tags** and choose the same region tag you choose for the Airwall from the drop down menu.

Enable DNS lookup for bypass destinations

If you want or need to use a fully-qualified domain name (FQDN) when specifying a bypass destination, you can enable DNS lookup for bypass. An FQDN may be necessary if the bypass destination IP is not static.

Supported Versions	2.2.10 and later Conductors
Required Role	System administrators

1. Go to **Settings** > **Bypass DNS**.
2. Select **Edit Settings**.
3. Toggle **Enable bypass DNS lookup** to On.



DNS settings for bypass destinations

Enable bypass DNS lookup: On

☑ Allow Airwall DNS servers

Allowed DNS server IPs *(comma-separated list of DNS server IPs)*

Minimum TTL: 10 minutes

4. To automatically allow the DNS servers configured on an Airwall Gateway underlay port (instead of listing them under **Allowed DNS server IPs**), check **Allow Airwall DNS servers**. Note this means the DNS servers being used could be different per Airwall Gateway.
5. Set trust to the DNS server on the overlay.

   Note: The traffic path to resolve hosts must follow the same path on the overlay as the traffic to the actual bypass destination. This requirement means that the DNS server must itself be a bypass destination and the overlay devices using it must have policy to it.
6. Under **Allowed DNS server IPs**, enter trusted DNS server IPs that you want bypass destinations to have access to for DNS lookup. Separate IPs with commas.
7. Under **Minimum TTL**, change the minimum amount of time to accept traffic from resolved IP addresses.
8. Select **Update**.

You can now use an FQDN when specifying a bypass destination. See step 4 under Local Bypass on page 394.

Airwall Edge Service High Availability (HA)

High Availability (HA) Airwall Gateways provide hardware redundancy in a hot-standby mode. Airwall Gateways installed in an HA configuration maintain a heartbeat on a dedicated Ethernet link where only the current primary is participating in overlay network communications. If the primary fails to send heartbeat messages to the secondary, the secondary takes over overlay network communications for the HA pair.

Configure High Availability Airwall Gateways (v2.2.8 and later)

Configuring high-availability (HA) Airwall Gateways in v2.2.8 and later. For v2.2-v2.2.5, see Configure High Availability for Airwall Gateways (v2.2-v2.2.5) on page 404.

The high-availability architecture for Airwall Gateways distinguishes between the following Airwall Gateway roles:

- *Primary vs. secondary*: These roles are assigned when the HA pairing is created. The Primary Airwall Gateway is the one that is added to the overlay in the Conductor. The secondary Airwall Gateway has no configuration on its own with the exception of identity-related information and port configuration. The primary and secondary role assignment can't be changed during the lifetime of the HA pairing.
- *Active vs. standby*: At any given time only one Airwall Gateway is active and participating in overlay network communications. The active Airwall Gateway maintains a heartbeat on a dedicated Ethernet link. If the active Airwall Gateway fails to send heartbeat messages to the standby, the standby takes over the overlay network communications for the HA pair.

Before You Begin

Before you configure a High-availability (HA) pair, you must:

- Have a Conductor set up and running.
- Configure and connect the physical or virtual v2.2.8 or later Airwall Gateways you wish to configure for high availability. You need two physical or two virtual Airwall Gateways. See Set up physical Airwall Gateways on page 275 for more information.
- Connect both Airwall Gateways to the same underlay and overlay network.

Note: Cloud Airwall Gateways do not support HA.

Create a High-availability Airwall Gateway pairing

High availability Airwall Gateway pairing is supported in v2.2 and later.

To configure High-availability Airwall Gateways, you need to:

1. **For virtual Airwall Gateways only** – Add an ethernet port
2. Connect the Airwall Gateways
3. Pair the Airwall Gateways for High Availability
4. Make sure the Overlay Port Group settings match

These steps are described in more detail below.

1 For Virtual Airwall Gateways only – Add an ethernet port

For virtual Airwall Gateways, you need to add an ethernet port for the heartbeat the high-availability Airwall Gateways use to communicate status. See your Hypervisor for instructions on adding a network port.

2 Connect the Airwall Gateways

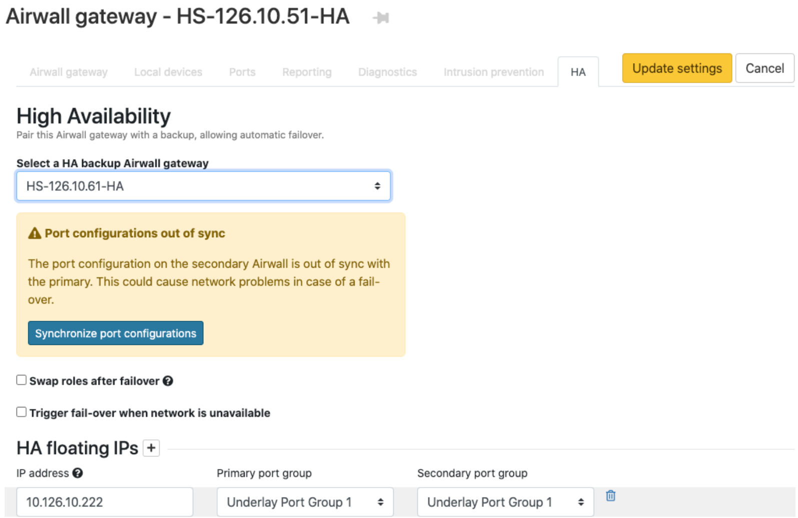
You can configure a pair of physical or virtual Airwall Gateways as a high-availability pair.

1. Select the primary Airwall Gateway and select or add an HA Port Group
   a) At the top right of the **Ports** tab, select **Edit Settings**.
   b) Select an available HA Port Group, or, to create one, go to **Ports** and select an available port, and create an HA Port Group. The port group sets up a virtual connection between the Airwall Gateways you're configuring as an HA pair. A virtual Airwall Gateway is expandable up to six (6) ports. You must configure one port for HA heartbeats with the HA role.
2. Repeat step 1 with the secondary Airwall Gateway.
3. **If you are using physical Airwall Gateways**, physically connect the primary to the secondary using an ethernet cable between the dedicated HA ethernet ports on both Airwall Gateways with an ethernet cable (so you have both a port and a physical connection between the two Airwall Gateways).
4. **If you are using virtual Airwall Gateways**, connect the port created above to each other in the virtual network. See your Hypervisor help for instructions.

Next, you will pair the Airwall Gateways.

3 Pair the Airwall Gateways for High Availability

1. Open the page for the Airwall Gateway you want to be Active in the HA pairing.
2. Open the **HA** tab and select **Edit Settings**.
3. Under **Select a high-availability backup** Airwall Gateway, select the secondary/standby Airwall Gateway.
4. If the port configuration on the selected secondary Airwall Gateway is different from the configuration on the primary Airwall Gateway, you will see an alert with the option to transfer the configuration of the primary Airwall Gateway to the secondary Airwall Gateway. Select **Synchronize port configurations** to copy the configuration from the primary to the secondary Airwall Gateway.



Airwall gateway - HS-126.10.51-HA

High Availability

Pair this Airwall gateway with a backup, allowing automatic failover.

Select a HA backup Airwall gateway: HS-126.10.61-HA

Port configurations out of sync

The port configuration on the secondary Airwall is out of sync with the primary. This could cause network problems in case of a fail-over.

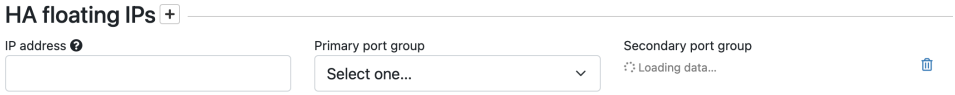
□ Swap roles after failover

□ Trigger fail-over when network is unavailable

HA floating IPs

IP address	Primary port group	Secondary port group
10.126.10.222	Underlay Port Group 1	Underlay Port Group 1

5. Set HA Heartbeat settings for an Airwall Gateway HA pair on page 403.
6. Check **Swap roles after failover** if you want the standby Airwall Gateway to remain active in the event of a failover. If this is not checked, the failed Airwall Gateway will automatically become active again once it back online.
7. Check **Trigger fail-over when network is unavailable** if you want to initiate a failover if the Airwall Gateway detects that it has no network connectivity. With this option checked, the standby will become active if the current active Airwall Gateway has no underlay connectivity on any underlay port group but the standby still does.
8. Next to **HA floating IPs**, select the + (plus sign), and enter an IP address that the HA-pair will share. This IP address will be advertised by the Conductor to all peer Airwall Gateways, but only the active Airwall Gateway owns it. This IP address should be routable and in the same subnets as the underlay IPs of the HA-pair. You may skip this if the HA Airwall Gateways always communicate through a relay. You can configure more than one floating IP if the HA Airwall Gateways have multiple underlay ports.



HA floating IPs

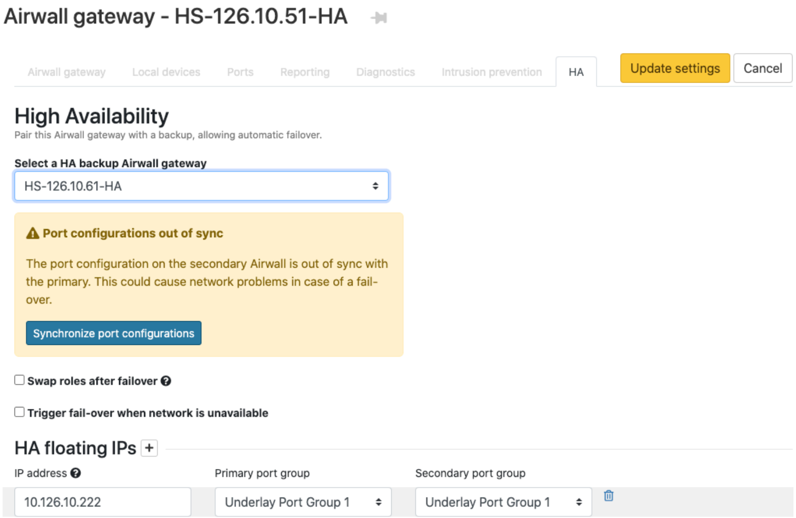
IP address	Primary port group	Secondary port group
	Select one...	Loading data...

9. Select **Update Settings**.

The shared High Availability (HA) IP address is a virtual IP address that moves between the two Airwall Gateways and is only set on the active one, so that remote Airwall Gateways have a consistent destination IP address for their connections to the HA Pair. The shared HA IP address must be a static IP address assigned for this specific purpose.

4 Make sure the Overlay Port Group settings match

1. Check the **Overlay Port Group** of your primary Airwall Gateway for an IP address or any other configured settings (such as DHCP, source NAT, etc).
2. The Conductor displays an alert on the **Port configuration** and **HA** tabs if there are discrepancies between the port configurations. Click **Synchronize port configurations** to replicate the configuration of the primary Airwall Gateway to the secondary. Note that the secondary Airwall Gateway must be online to replicate the settings.



Airwall gateway - HS-126.10.51-HA

High Availability

Pair this Airwall gateway with a backup, allowing automatic failover.

Select a HA backup Airwall gateway: HS-126.10.61-HA

⚠ Port configurations out of sync

The port configuration on the secondary Airwall is out of sync with the primary. This could cause network problems in case of a fail-over.

□ Swap roles after failover

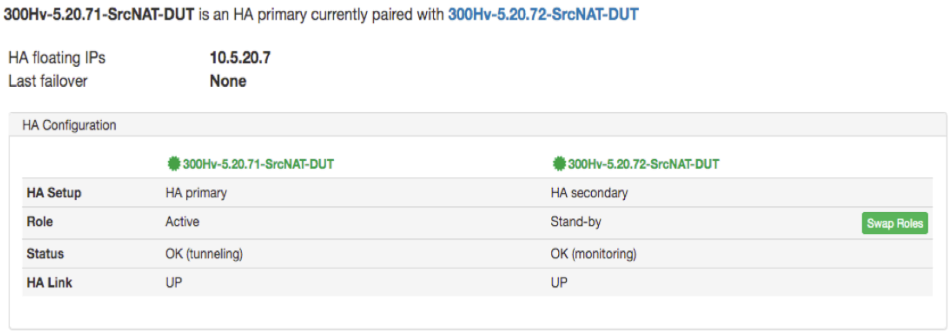
□ Trigger fail-over when network is unavailable

HA floating IPs +

IP address	Primary port group	Secondary port group
10.126.10.222	Underlay Port Group 1	Underlay Port Group 1

Test the High-Availability Pair

The **HA** tab on either HA-paired Airwall Gateway displays the setup of the HA pair, identifying the primary and secondary, along with their current roles and status. Immediately after setting up the HA pair, the status displays Setting up. After a few seconds, the status of both Airwall Gateways will change: to **OK (tunneling)** on the active and to **OK (monitoring)** on the standby.



300Hv-5.20.71-SrcNAT-DUT is an HA primary currently paired with **300Hv-5.20.72-SrcNAT-DUT**

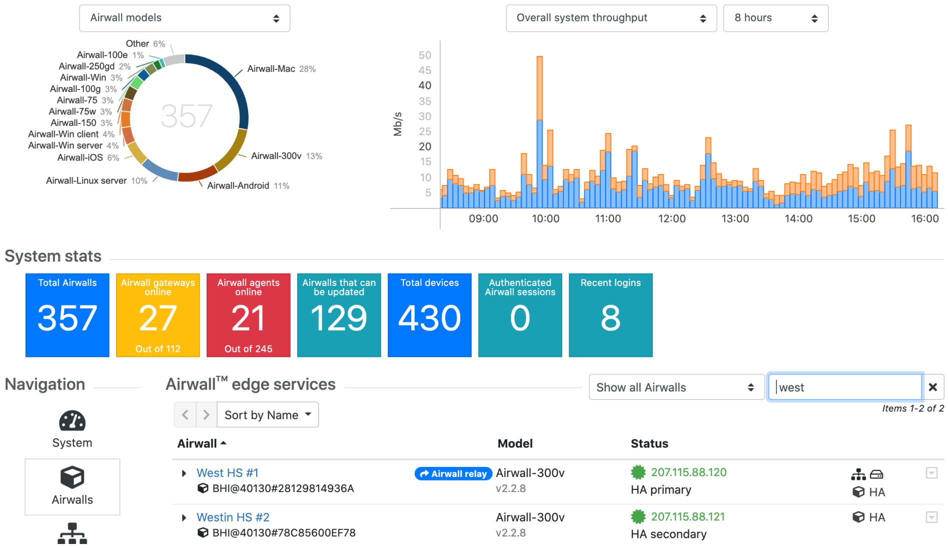
HA floating IPs	**10.5.20.7**
Last failover	**None**

HA Configuration

	300Hv-5.20.71-SrcNAT-DUT	300Hv-5.20.72-SrcNAT-DUT
HA Setup	HA primary	HA secondary
Role	Active	Stand-by
Status	OK (tunneling)	OK (monitoring)
HA Link	UP	UP

You can manually reverse the active and standby roles by selecting **Swap Roles**. This option initiates a failover from the current active Airwall Gateway to the standby, and permanently reverse the roles irrespective of the **Swap roles after failover** setting.

You can also see that the Airwall Gateways are paired on the Dashboard.



System stats

Total Airwalls	Airwall gateways online	Airwall agents online	Airwalls that can be updated	Total devices	Authenticated Airwall sessions	Recent logins
357	27 Out of 112	21 Out of 245	129	430	0	8

Airwall™ edge services

Items 1-2 of 2

Airwall	Model	Status	
West HS #1 BHI@40130#28129814936A	Airwall-300v v2.2.8	207.115.88.120 HA primary	HA
Westin HS #2 BHI@40130#78C85600EF78	Airwall-300v v2.2.8	207.115.88.121 HA secondary	HA

Remove a High-Availability Pairing

You remove an HA pairing from the primary Airwall Gateway.

1. Open the page for the primary Airwall Gateway, and on the **HA** tab, select **Edit Settings**.
2. Select **Remove HA pairing**.
3. Select **Update Settings**.

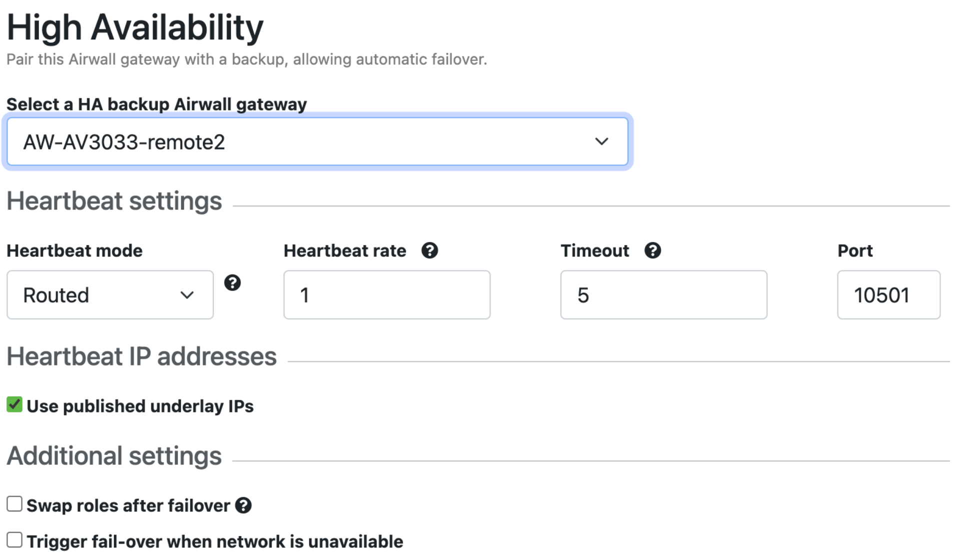
When an HA Pair is removed, the primary Airwall Gateway stays in the Overlay Network and the secondary Airwall Gateway is removed from the Overlay network.

Set HA Heartbeat settings for an Airwall Gateway HA pair

When setting up an Airwall Gateway HA pair you must set up a heartbeat between the two HA units. There are two options: LAN mode or routed mode:

- LAN mode – This mode is recommended for side-by-side physical Airwall Gateway models and requires setting up a dedicated port group for the heartbeat (HA port) on both Airwall Gateways. As a best practice, connect the two ports directly using a private network cable. You may also connect the ports via a switch on the same LAN.
- **Routed mode** – In routed mode, the heartbeat is sent over UDP and no HA port is needed and both Airwall Gateways may reside on separate underlay networks. In both cases, it is assumed the overlay ports of both units are set up to connect to the same device network. Unlike LAN mode, the heartbeat packets are encrypted and may be sent over a WAN.

1. Go to the Airwall Gateway that is the primary in the High Availability pair.
2. Open the **HA** tab.
3. If you haven’t yet, select the secondary Airwall Gateway and synchronize the port configurations.
4. Under **Heartbeat settings**, set the following:
    - **Heartbeat mode** – Select Routed or LAN.
    - **Heartbeat rate** – Enter the rate in seconds that the active Airwall Gateway will send a heartbeat to the standby Airwall Gateway. A faster rate will result in a faster failover if the active Airwall Gateway fails.
    - **Timeout** – Enter how long in seconds that the standby Airwall Gateway will wait after not receiving a heartbeat before failing over. Increasing the timeout will delay the failover in case of failure but helps reduce the likelihood of spurious failovers in situations where heartbeats are delayed because the active Airwall Gateway is under heavy load or because of network congestion.
    - **Port** – The port used for sending the heartbeat in routed mode. The default option should work in most cases, but you can change it if needed.



High Availability

Pair this Airwall gateway with a backup, allowing automatic failover.

Select a HA backup Airwall gateway: AW-AV3033-remote2

Heartbeat settings

Heartbeat mode	Heartbeat rate	Timeout	Port
Routed	1	5	10501

Heartbeat IP addresses

☑ Use published underlay IPs

Additional settings

☐ Swap roles after failover

☐ Trigger fail-over when network is unavailable

5. Under Heartbeat IP addresses, leave **Use published underlay IPs** checked, or clear it and manually enter IPs for the primary and secondary Airwall Gateways. You might want to change this in deployments where the published IP will be a publicly routable IP, but you want to make sure the heartbeat takes a direct path using a non-published private IP.

Return to Configure High Availability Airwall Gateways (v2.2.8 and later) on page 399 to complete setup.

Configure High Availability for Airwall Gateways (v2.2-v2.2.5)

Configuring high-availability (HA) Airwall Gateways in v2.2-v2.2.5. For v2.2.8 and later, see Configure High Availability Airwall Gateways (v2.2.8 and later) on page 399.

Before You Begin

Before you configure a High-availability (HA) pair, you must:

- Have a Conductor installed
- Configure and connect the physical or virtual v2.2 to v2.2.5 Airwall Gateways you wish to configure for high availability. You need two physical or two virtual Airwall Gateways. See Set up physical Airwall Gateways on page 275 for more information.

Note: Cloud Airwall Gateways do not support HA at this time.

To create a high-availability Airwall Gateway pairing

To configure High-availability Airwall Gateways, you need to:

1. **For virtual Airwall Gateways only** – Add an ethernet port
2. Connect the Airwall Gateways
3. Pair the Airwall Gateways for High Availability
4. Make sure the **Overlay Port Group** settings match

These steps are described in more detail below.

1 For Virtual Airwall Gateways only – Add an ethernet port

For virtual Airwall Gateways, you need to add an ethernet port for the heartbeat the high-availability Airwall Gateways use to communicate status. See your Hypervisor help for instructions on adding a network port.

2 Connect the Airwall Gateways

You can configure a pair of physical or virtual Airwall Gateways as a high-availability pair.

1. Select the primary Airwall Gateway and select or add an HA Port Group
   a) At the top right of the **Ports** tab, select **Edit Settings**.

b) Select an available HA Port Group, or, to create one, go to **Ports** and select an available port, and create an HA Port Group. The port group sets up a virtual connection between the Airwall Gateways you're configuring as an HA pair. A virtual Airwall Gateway is expandable up to six (6) ports. You must configure one port for HA heartbeats with the HA role.

2. Repeat step 1 with the secondary Airwall Gateway.
3. **If you are using physical Airwall Gateways**, physically connect the primary to the secondary using an ethernet cable between the dedicated HA ethernet ports on both Airwall Gateways with an ethernet cable (so you have both a port and a physical connection between the two Airwall Gateways).
4. **If you are using virtual Airwall Gateways**, connect the port created above to each other in the virtual network. See your Hypervisor instruction.

Next, you will pair the Airwall Gateways.

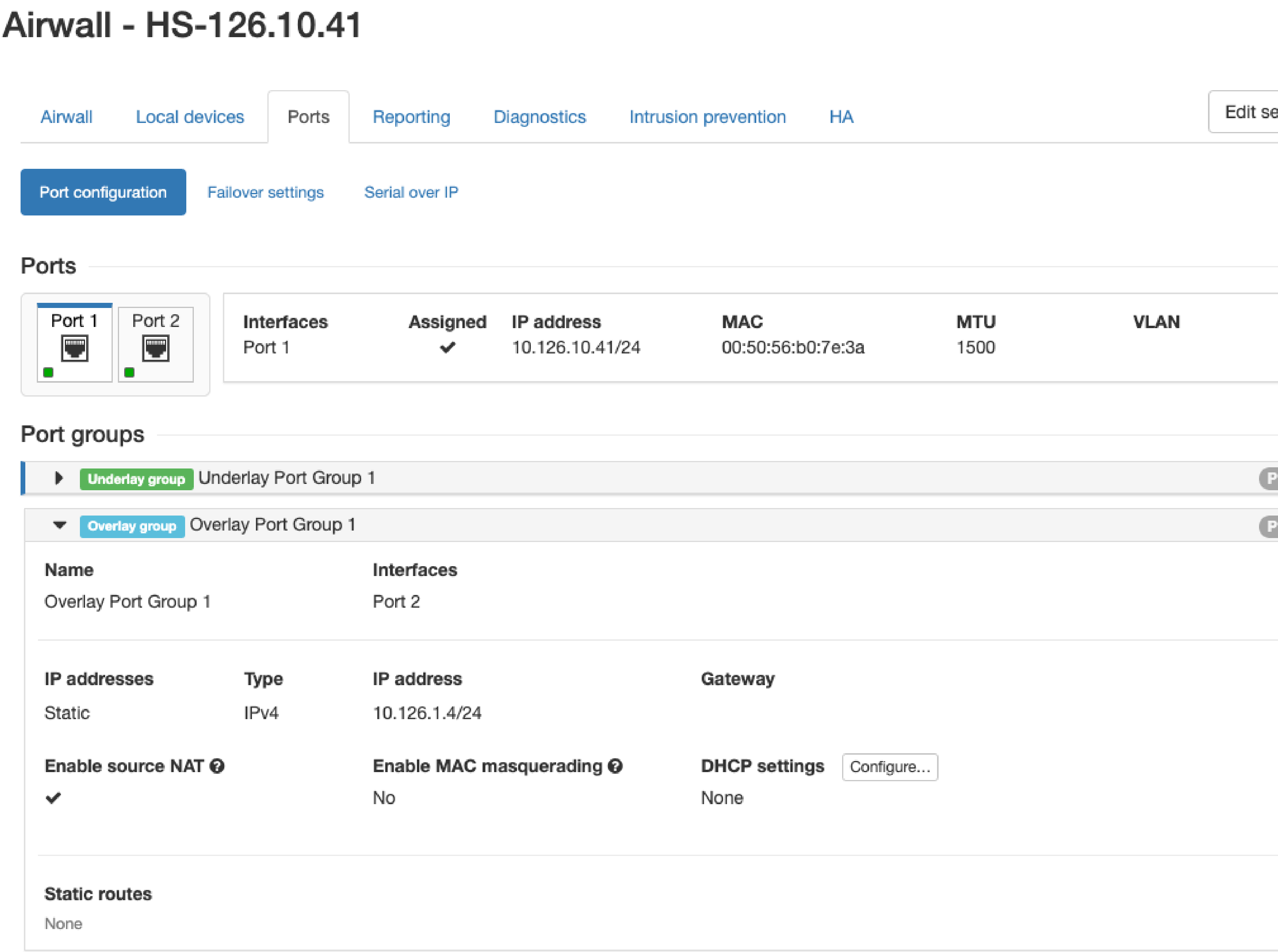
3 Pair the Airwall Gateways for High Availability

1. Select the **HA** tab and click **Edit Settings**.
2. Under **Select a high-availability backup** Airwall Gateway, select the secondary Airwall Gateway.
3. Under **IP address**, enter an available IP address to act as the shared HA IP address for the High Availability pair (see note below). You may need to select a Primary port group as well.
4. Click **Update Settings**.
5. If you want to swap the primary Airwall Gateway with the secondary one, go to the **HA** tab, and by **Role**, select **Swap Roles**.

The shared High Availability (HA) IP address is a virtual IP address that moves between the primary and secondary Airwall Gateways, so that remote Airwall Gateways have a consistent destination IP address for their connections to the HA Pair. The shared HA IP address must be a static IP address assigned for this specific purpose.

4 Make sure the Overlay Port Group settings match

1. Check the **Overlay Port Group** of your primary Airwall Gateway for an IP address or any other configured settings (such as DHCP, source NAT, etc).
2. If there are settings there, copy them to the standby Airwall Gateway's **Overlay Port group**.



Airwall - HS-126.10.41

Ports

Interfaces	Assigned	IP address	MAC	MTU	VLAN
Port 1	✓	10.126.10.41/24	00:50:56:b0:7e:3a	1500	

Port groups

Underlay group Underlay Port Group 1

Overlay group Overlay Port Group 1

Name	Interfaces
Overlay Port Group 1	Port 2

IP addresses	Type	IP address	Gateway
Static	IPv4	10.126.1.4/24	

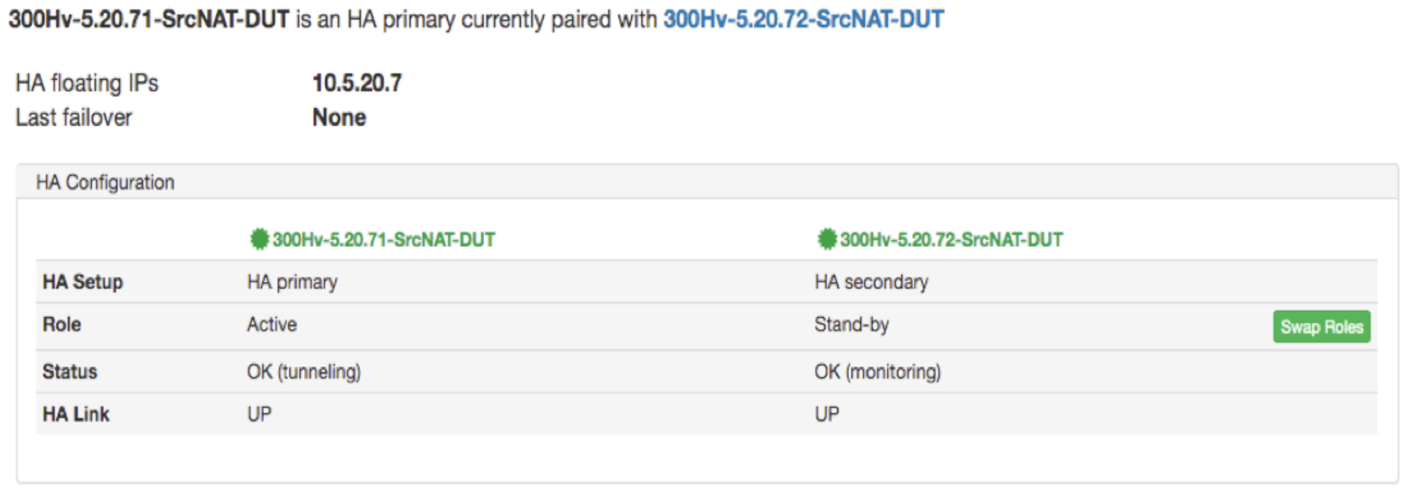
Enable source NAT	Enable MAC masquerading	DHCP settings
✓	No	None

Static routes

None

Test the High-Availability Pair

In either HA paired Airwall Gateway, on the **HA** tab under **Status**, notice the screens are trying to talk to each other. The primary status is **OK (tunneling)** and the secondary status is **OK (monitoring)**.



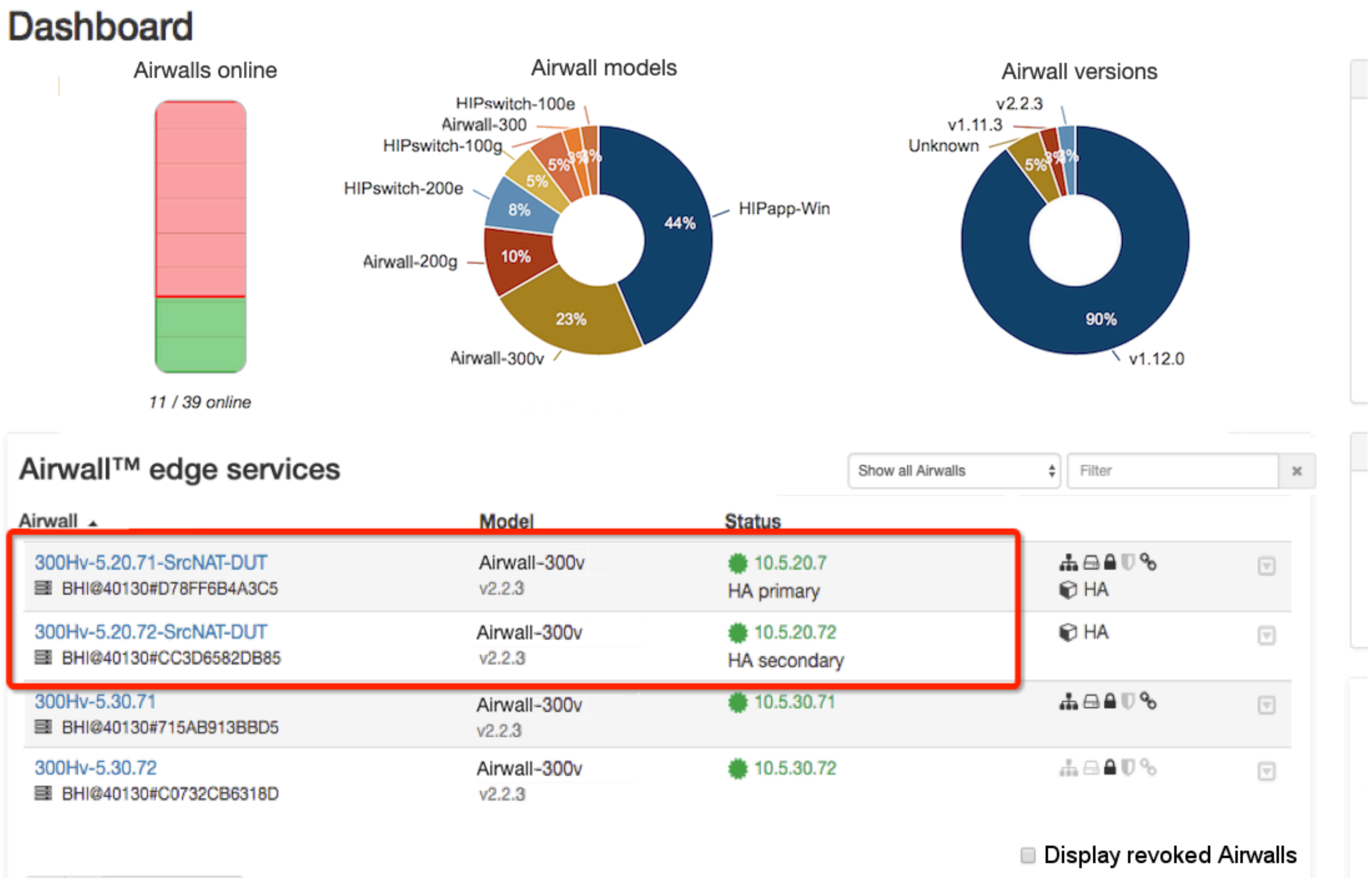
300Hv-5.20.71-SrcNAT-DUT is an HA primary currently paired with **300Hv-5.20.72-SrcNAT-DUT**

HA floating IPs	**10.5.20.7**
Last failover	**None**

HA Configuration

	300Hv-5.20.71-SrcNAT-DUT	300Hv-5.20.72-SrcNAT-DUT	
HA Setup	HA primary	HA secondary	
Role	Active	Stand-by	Swap Roles
Status	OK (tunneling)	OK (monitoring)	
HA Link	UP	UP	

You can also see that the Airwall Gateways are paired on the Dashboard.



Dashboard

Airwall™ edge services

Show all Airwalls | Filter

Airwall ▲	Model	Status		
300Hv-5.20.71-SrcNAT-DUT BHI@40130#D78FF6B4A3C5	Airwall-300v v2.2.3	10.5.20.7 HA primary	HA	
300Hv-5.20.72-SrcNAT-DUT BHI@40130#CC3D6582DB85	Airwall-300v v2.2.3	10.5.20.72 HA secondary	HA	
300Hv-5.30.71 BHI@40130#715AB913BBD5	Airwall-300v v2.2.3	10.5.30.71		
300Hv-5.30.72 BHI@40130#C0732CB6318D	Airwall-300v v2.2.3	10.5.30.72		

□ Display revoked Airwalls

Remove a High-Availability Pairing

You can remove an HA pairing from the primary Airwall Gateway.

1. In the primary Airwall Gateway, on the **HA** tab, click **Edit Settings**.
2. Click **Remove HA pairing**.

When an HA Pair is removed, the primary Airwall Gateway stays in the Overlay Network and the secondary Airwall Gateway is removed from the Overlay network.

One-arm mode

You can configure an Airwall Gateway to use a single network connection in cases where you want to prevent common routing errors caused by multiple interfaces.

One-arm mode is simple to configure, but consider the following before configuring an Airwall Gateway in one-arm mode.

- You cannot place an Airwall Gateway in transparent mode while in one-arm mode
  - You must use a wired port. One-arm mode will not function using a wireless or cellular interface.
  - The overlay IP and netmask in **Local Devices** -> **Device Network Configuration** is ignored; however, the information is retained if you revert your settings from one-arm mode later.
  - Overlay routes on the **Local Devices** tab are also ignored but retained if you revert.

Configure one-arm mode

To configure an Airwall Gateway for one-arm mode:

1. Select the desired Airwall Gateway from the **Airwalls** tab in the Conductor.
2. Select the **Airwalls** tab and click **Edit Settings**
3. In the **Advanced Configuration** section, uncheck **Enable spanning tree protocol**
4. Click **Update Settings**
5. Select the **Local Devices** tab and click **Edit Settings**
6. In the **Configuration** section, uncheck **Enable device discovery**
7. In the **Device Network Configuration** section, uncheck **Enable NAT** and **Enable source NAT**
8. In the **Local Device DHCP** section, uncheck **Enable DHCP server**
9. Click **Update Settings**
10. Select the **Ports** tab and then **Shared Network**
11. Click **Edit Settings**
12. In the **Port 1** section, select **Static** from the **Protocol** drop-down and enter the IP address, netmask, and any other required fields for your shared network
13. Click **Update Settings**

    Note: You will get a message that the Airwall Gateway is reconnecting.

    Once the configuration process is complete, you will get a Network configuration successful message.
14. Select the **Port** assignment tab and click **Edit Settings**
15. For **Port 1**, select **Dual-Use (Shared + Device)** from the **Assigned to** drop-down
16. For **Port 2**, select **Disabled** from the **Assigned to** drop-down
17. Click **Update Settings**
18. In the **Confirm Dual-Use Port Configuration** dialog, click **OK**
19. The Airwall Gateway will re-configure and you will receive the same messages you received when configuring the port assignments

Your Airwall Gateway is now correctly configured for dual-use mode.

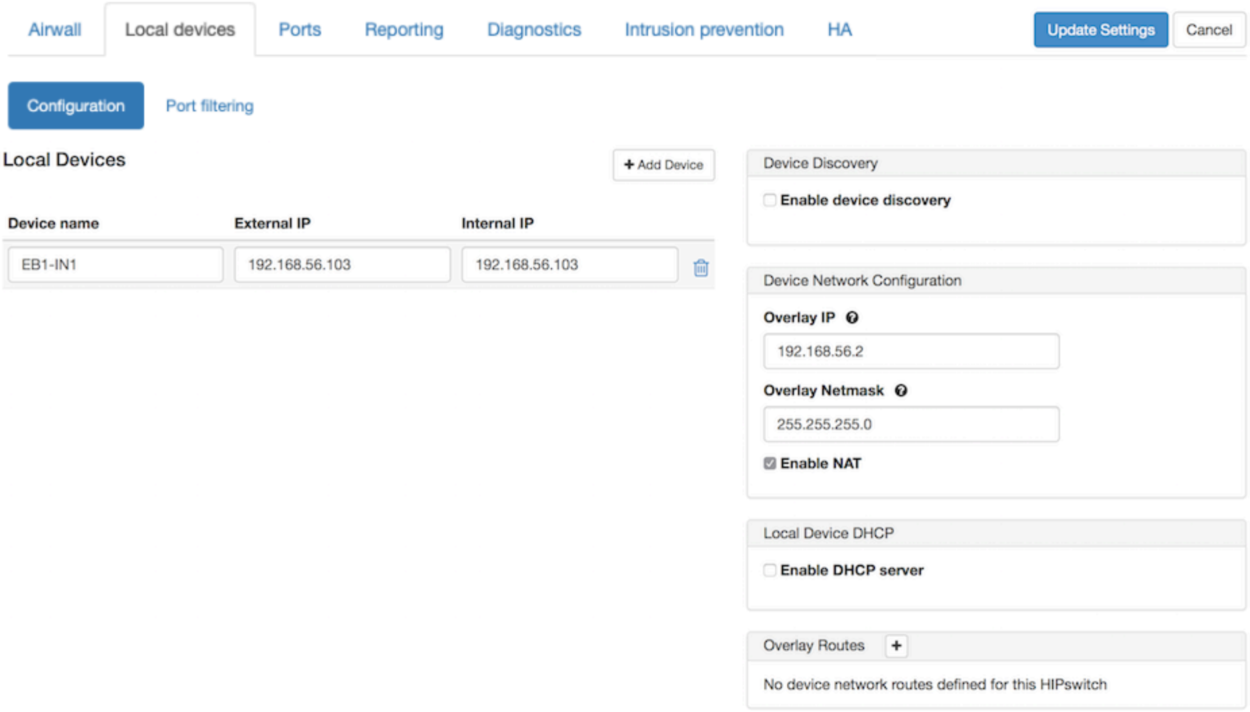
Network address translation (NAT)

Network Address Translation (NAT) translates an IP address in one network to a different IP address in another network. The two IP addresses are referred to as the External IP address and the Internal IP address. The External IP address is the IP address of the device in the overlay network and the Internal IP address is the actual IP address of the device.

NAT is used in conjunction with Airwall Gateway subnet routing. To use NAT, the private IP address of a local device must be in a different subnet than the public IP address of a remote device. For example, if a local device's private IP address is 192.168.56.99, the device cannot be reached by a remote device that is configured with a public IP address of 192.168.56.xxx, assuming a subnet mask of 255.255.255.0.

To enable NAT on a device or multiple devices:

1. Go to **Airwalls** and select the Airwall Gateway to which the device or devices belong.
2. Select **Local Devices** and click **Edit Settings**.
3. Check **Enable NAT** and enter the gateway external IP address.
4. Click **Update Settings** to save the configuration.



Local Devices

Device name	External IP	Internal IP
EB1-IN1	192.168.56.103	192.168.56.103

Device Discovery

□ Enable device discovery

Device Network Configuration

Overlay IP: 192.168.56.2

Overlay Netmask: 255.255.255.0

☑ Enable NAT

Local Device DHCP

□ Enable DHCP server

No device network routes defined for this HIPswitch

Encryption and tunnel compression on an Airwall Gateway

You can change the encryption or compression of Airwall Gateways.

1. Go to **Airwalls** and select an Airwall Gateway.
2. Click **Edit Settings**.
3. In the **Advanced settings** section, select one of the following from the **Default encryption** drop-down:
   - AES-256-GCM and compression
   - AES-256-GCM
   - AES-256-CBC and compression
   - AES-256-CBC

   Note: Enabling compression may result in improved throughput
4. Click **Update Settings**.

Important: If the encryption or compression settings of two communicating Airwall Gateways differ, the settings of the peer Airwall Gateway are used by default.

Protected devices with static routing

You can configure static routing for protected devices with IP addresses not directly connected to an Airwall Gateway.

To use static routing :

1. Go to **Airwalls** and select an Airwall Gateway.
2. Select **Ports** and click **Edit Settings**.
3. Click + **Add route** and enter the target network in CIDR format and gateway.
4. Add additional routes as necessary by repeating the previous step.

5. Click **Update Settings**.

Protected devices with DHCP

If you have protected devices that use DHCP to obtain an IP address, you need to configure DHCP on the Airwall Gateway that protects that device.

Note: You must have an overlay gateway IP address on the Overlay port group on which you are enabling DHCP.

To use DHCP to configure protected devices with IP addresses:

1. On the **Airwalls** page, select the Airwall Gateway to which the device or devices belong.
2. On the **Ports** tab, open the Overlay you are enabling DHCP on.
3. Under **DHCP Settings**, click **Configure**.
4. Under **DHCP Configuration**, select **DHCP server**.
5. Enter the range of IP addresses in the Start and End boxes.
6. Enter the netmask.
7. Under **Gateway**, enter the IP address of the Airwall Gateway.
8. Optional. Enter DNS server information, if required.
9. Click **Apply**.

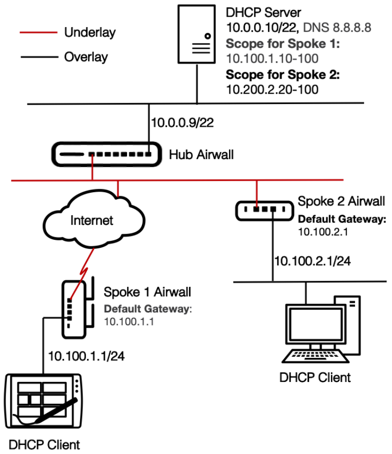
Protected devices are now dynamically assigned IP address when connected to the Airwall Gateway.

DHCP relay on an Airwall Gateway

If you have protected devices that use DHCP to obtain an IP address, you can configure the Airwall Gateway to relay the DHCP address to your DHCP server.

Note: You must have an overlay IP address on the Overlay port group of the Airwall Gateway that has your DHCP clients behind it (10.100.2.1/24 in the diagram below). This overlay IP address should be the default gateway that is handed out by the DHCP Server for the DHCP clients..

Deploy the DHCP server so it routes traffic to DHCP-relay-enabled spokes via the hub Airwall. The DHCP server needs to connect to an Overlay port and the DHCP relay traffic needs to traverse the tunnel to the Spoke Airwall, as shown in the following diagram.



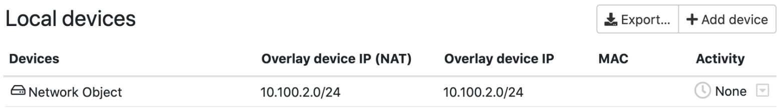
1. Make sure that the DHCP server is a protected device of the hub Airwall Gateway.
2. For each Airwall Gateway (Spoke 1 and Spoke 2 in the diagram) that has a DHCP device behind it:
   a) From the **Airwalls** page, open the Airwall Gateway to which the DHCP client device or devices belong.
   b) On the **Ports** tab, open the Overlay you are enabling DHCP on.
   c) Under **DHCP Settings**, click **Configure**
   d) Under **DHCP Configuration**, select **DHCP relay**.
   e) Set the **Upstream DHCP server** (for example, 10.0.0.10).

f) Click **Apply**.

3. Add a network object that includes the DHCP scope as a protected device to each Spoke Airwall Gateway. For example, for Spoke 2, add a device with IP Address = 10.100.2.0/24 (this is referred to as a Network Object).
4. Create an Overlay for the DHCP traffic:

a) On the **Overlays** page, select **New overlay network**. Select **Manual**, name the Overlay, and select **Finish**.

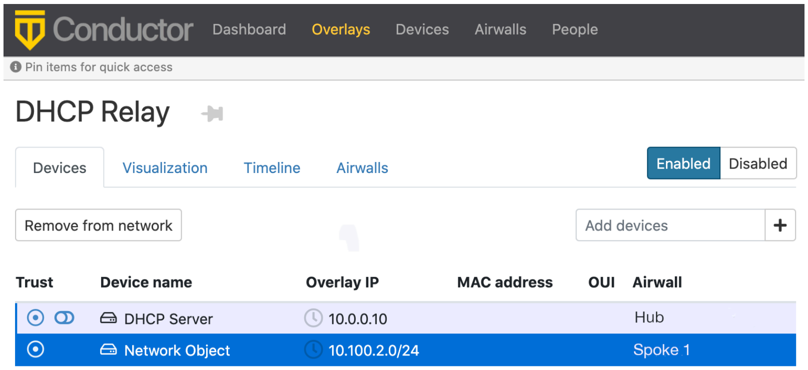
b) On the **Devices** tab, click the + and add the network object created in step 3 (that is, 10.100.2.0/24) to the Overlay.



Devices	Overlay device IP (NAT)	Overlay device IP	MAC	Activity
Network Object	10.100.2.0/24	10.100.2.0/24		None

c) Add the DHCP server (10.0.0.10 in the diagram) to the Overlay.

d) Establish trust between the network object and the DHCP server.



Trust	Device name	Overlay IP	MAC address	OUI	Airwall
	DHCP Server	10.0.0.10			Hub
	Network Object	10.100.2.0/24			Spoke 1

Note: The DHCP Scope Default gateway (i.e 10.100.2.1) needs to match the Overlay IP for the port group connected to DHCP clients. And, the subnet mask of the DHCP scope must match the subnet mask of the Overlay IP port group.

Limit Device Traffic on an Airwall Gateway with Port Filtering

You can use Airwall Gateway port filtering to limit what traffic can pass over an Overlay based on TCP/UDP Ports. With port filtering enabled, all communication from remote to local devices is disabled, and you create custom rules to tell the local Airwall Gateway what to allow as incoming connections to local devices.

Note: When removing a port filtering rule that allows connections, any ongoing connections at the time the rule is deleted are not blocked. Rules are checked when a new connection is attempted.

Note: To establish communication between local and remote devices, you must also Add and remove device trust on page 427 on the overlay, in addition to specifying custom port filtering rules

Remote Device communication

Remote devices are devices that are behind different Airwall Gateways and are reachable in the overlay network. Remote devices send connection requests to local devices, and typically use random port numbers for their connection attempts, so typically you leave the remote device port range blank.

Local Device communication

Local devices are devices that are connected locally to the Airwall Gateway you are configuring. Local devices receive incoming connections from remote devices. Most local device services are listening on a specific port or ports that you typically specify as part of the custom rule.

TCP or UDP protocol

You can specify TCP or UDP as the underlying communication protocol used by devices. If you are using a different IP protocol, select **IP (any)** from the Protocol list, which allows devices to use any IP protocol.

What happens to Port Filtering Rules when you delete devices?

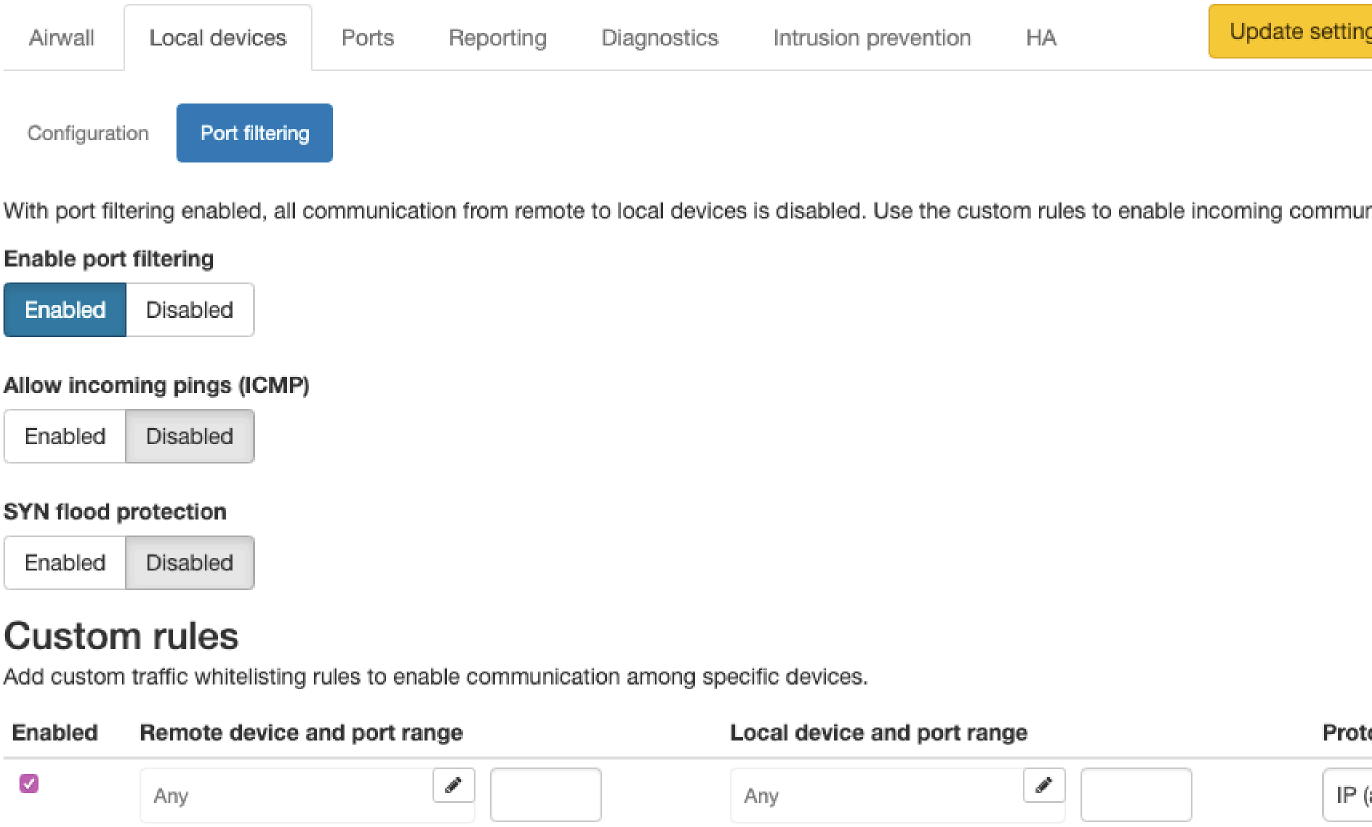
When you delete local devices from an Airwall Gateway or delete remote devices from remote Airwall Gateways, the port filtering rules associated with the devices are deleted. If you remove an Airwall Gateway from the overlay network, the rules associated with the Airwall Gateway are labeled `not reachable`.

Related tasks

Set up Port Filtering on an Airwall Gateway on page 412

Set up Port Filtering on an Airwall Gateway

1. In Conductor, open the page for the Airwall Gateway you want to set up port filtering for.
2. Open the **Local devices** tab, and **Port filtering** subtab, and select **Edit Settings**.
3. Under **Enable port filtering**, select **Enabled**.



With port filtering enabled, all communication from remote to local devices is disabled. Use the custom rules to enable incoming commur

Enable port filtering: [✓ Enabled] Disabled

Allow incoming pings (ICMP): Enabled [✓ Disabled]

SYN flood protection: Enabled [✓ Disabled]

Custom rules

Add custom traffic whitelisting rules to enable communication among specific devices.

Enabled	Remote device and port range		Local device and port range		Proto
☑	Any		Any		IP (

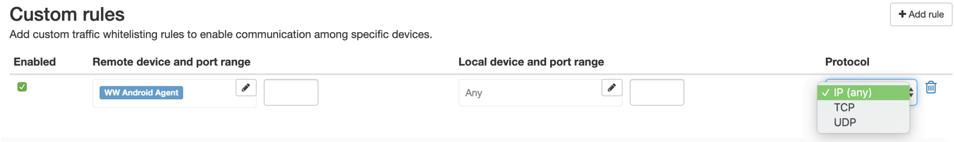
Note: With port filtering enabled, all communication from remote to local devices is disabled, and you create custom rules to tell the local Airwall Gateway what to allow as incoming connections to local devices.

4. To allow remote devices to ping local devices, enable **Allow incoming pings (ICMP)** to allow remote devices to ping local devices.
5. If you need to protect against Denial-of-service attacks, enable **SYN flood protection**.
6. Under **Custom rules**, select **Add Rule** and set up the rules to allow traffic between the local devices behind this Airwall Gateway and remote devices behind other Airwall Gateways:

a) Under **Remote device and port range**, select one or more remote devices you want to be able to communicate with local devices. Since remote devices usually use random port numbers when they attempt to connect, most of the time, leave the port range blank.

b) Under **Local device and port range**, select one or more local devices you want to communicate with the selected remote devices. Since local device ports usually remain the same, specify the port range for the local devices.

c) Under **Protocol**, if you are using TCP or UDP, specify the underlying communication protocol used by devices. If you are using a different IP protocol, select `IP (any)` from the **Protocol** list, which allows any IP protocol to be used.



Custom rules

Add custom traffic whitelisting rules to enable communication among specific devices.

Enabled	Remote device and port range	Local device and port range	Protocol
☑	WW Android Agent	Any	✓ IP (any)

d) Select **Add Rule** to add additional rules, as needed.

7. When you are finished creating rules, select **Update Settings** to save your port filtering settings.

You must also add devices to an overlay and establish trust before communication is fully enabled. See Add and remove device trust on page 427.

For more information on Port Filtering, see Limit Device Traffic on an Airwall Gateway with Port Filtering on page 411.

Spanning Tree Protocol on the Overlay Network

Overview

Airwall Gateways can emit and participate in Spanning Tree Protocol (STP), helping reduce network loops and allowing for link redundancy.

How an Airwall Gateway interacts with existing STP infrastructure varies depending on the installed firmware version.

1.12.4 - 1.12.6

Airwall Gateways/HIPswitches running versions 1.12.4 through 1.12.6 have STP enabled on the overlay network interface by default. It is not configurable or able to be disabled.

STP bridge priority is 32768

2.0.x

Airwall Gateways/HIPswitches running versions 2.0.x provide an option to disable STP if not needed. The feature is enabled by default.

STP bridge priority is 32767.

2.1.x

Airwall Gateways/HIPswitches running versions 2.1.x or greater will not enable STP if there is only one network interface configured for the overlay network. By default, -100 and -200 series Airwall Gateway/HIPswitches enable the feature.

Note: Conductor provides a setting to enable or disable STP for these platforms; however, this has no affect to the running unit, as it will not enable.

STP bridge priority is 61440.

Recommendations

If multiple network interfaces are configured with the Underlay role, they are put into a bridge, and STP is enabled. STP on this bridge does is not configurable, nor can it be disabled.

Connect and Configure Devices

As you prepare to connect devices to Airwall Gateways, you may want your Airwall Gateway product guide available to identify the ports reserved for connecting devices you want to protect.

Different Airwall Gateway models support different numbers of devices, and some older models may use different port names such as:

- Device Network
- Private Network
- Equipment Network

CAUTION: Avoid duplicate device IP addresses, even if the devices are members of different Overlay networks. If more than one Airwall Gateway is a member of both Overlay networks, it creates an unresolved network routing conflict.

Add devices to the Conductor

After you connect devices to Airwall Gateway hardware, there are four ways to add a device to the Conductor.

- Enable passive device discovery on page 414
- Detect devices manually on page 414
- Import and export devices using a CSV file on page 415
- Add devices manually on page 416

If you are working with a large number of devices, you may want to create device groups for ease of administration, once the devices have been added to Conductor. See Use device groups and smart device groups on page 416 for more information on creating groups.

Use device discovery

Airwall Gateways are able to auto discover devices as soon as they are plugged in. Please note however, a discovered device cannot communicate with other devices in an overlay network until an administrator explicitly accepts the device.

There are two different ways to enable device discovery:

1. Enable passive device discovery on page 414
2. Detect devices manually on page 414

Enable passive device discovery

Enabling device discovery option allows an Airwall Gateway to passively discover devices within the overlay device network it is connected to.

To enable device discovery:

1. Go to **Airwalls** and select an Airwall Gateway.
2. Go to **Local Devices** > **Configuration** and click **Edit Settings**.
3. Select your version:
    - **In v3.0 and later** – Under **Settings**, check **Enable passive device discovery**.
    - Before v3.0 – In the **Device Discovery** section on the right, check **Enable device discovery**.
4. Select **Update Settings**.

Detect devices manually

If you instead want to use passive device detection, enable **Passive device discovery** and set up **Device Network Configuration** for the Airwall Gateway.

1. Go to **Airwalls** and open an Airwall Gateway from the list.

2. Go to **Local devices** > **Configuration**.
3. To the right of **Local devices**:
    - **v3.1.0 and later** – Select **Detect and onboard devices**.
    - **v3.0.3 and earlier** – Open the **Other actions** menu and select **Detect devices**.

Once detected, the protected device appears in the Conductor and the device can then be added to your Overlay networks.

You can also delete detected devices by opening the **Other actions** menu and selecting **Delete discovered devices**

Import and export devices using a CSV file

Device import and export is useful if you have a large number of devices to manage in your Airwall deployment.

A .csv file contains plain text data sets separated by commas with each row consisting of one or more fields.

Note: Importing devices is not destructive, it is additive - so devices in the import are added, but none are deleted.

To make the management of your devices easier, you can download a device import .csv template from here, export and modify the existing device file, or create the file yourself. A typical .csv file looks like the following example:

```
airwall_id,device_name,overlay_device_ip,overlay_device_ip_nat,mac_address,mac_lockdown
BHI@40130#35C1B68998D9,Local
 Workstation,192.168.59.101,,08:00:27:05:03:2e,FALSE
BHI@40130#4F6B8FD47B90,Local Workstation
 2,192.168.59.102,,08:00:27:67:e6:6e,FALSE
```

The first line contains field names with each successive line containing data corresponding to the fields.

airwall_id
This is the UID of the Airwall Edge Service you want your devices to use. You can find this information in the **UID** field for the Airwall Edge Service in the Conductor. The UID looks like this: `BHI@40130#101E20100067`

device_name
A friendly name for the device.

overlay_device_ip
The IP address of the device.

overlay_device_ip_nat
(Optional) If your network topology requires you also use NAT you can enter the internal IP address here.

mac_address
(Optional) Enter the MAC address of your device. This field is required if you want to enable MAC lockdown (*mac_lockdown=TRUE*).

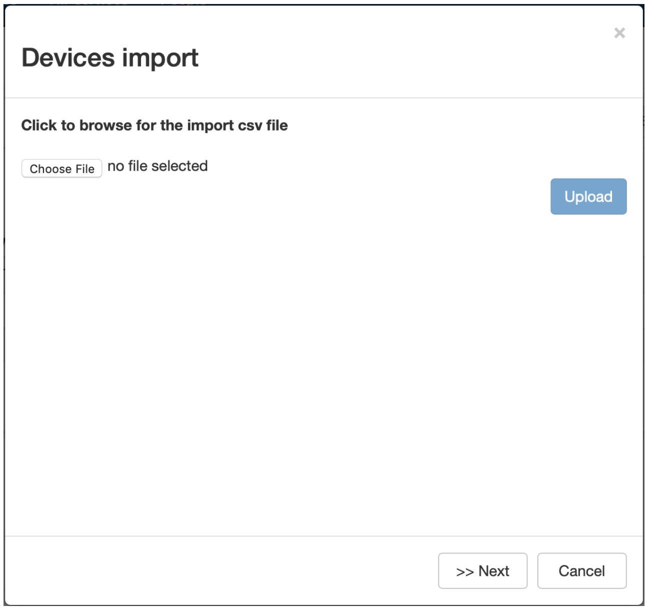
mac_lockdown
Enter TRUE if you require static addressing for the device, otherwise enter FALSE.

Import devices using a .csv file

You can import devices into your Conductor using a .csv file.

Note: You cannot import emojis using the .csv file.

1. If you want to use the template .csv file, go to **Devices** and from the **Other Actions** menu, select **Export devices template**. Add devices by adding rows to the template, following the column headers detailed above.
2. Go to **Devices** and from the **Other Actions** menu, select **Import devices list**.
3. Select **Choose File** and then open the .csv file containing your device list.



Devices import

Click to browse for the import csv file

4. Click **Upload** and the devices will be listed, grouped by their associated Airwall Edge Services.

   Note: If you receive any errors, correct the .csv file and try to import it again.

5. Select **Next**, review the results, and then select **Commit**. When it is done, select **Finish**.

Export devices to a .csv file

Export the devices in the Conductor to a .csv file.

1. Go to **Devices** and from the **Other Actions** menu, select **Export devices list**.
2. Select **Export** to confirm.

Add devices manually

You can manually add devices in the Airwall Gateways tab.

1. Go to **Airwalls** and select an Airwall Gateway from the list.
2. Go to **Local Devices** and click **Add Device**.
3. In the dialog, enter a device name, IP address, and optionally a MAC address.
4. Click **Create**.

Note: Adding devices from the **Airwalls** list is also possible. Select the drop-down to the right of an Airwall Gateway, and click **Add Device**.

Use device groups and smart device groups

Device groups streamline the management of a large number of devices, allowing you to manage them as a group. Not that a device group does not create device trust policy between them. See Configure Device Trust on page 427.

There are two types of device groups:

- **Standard** – Create standard device groups to manage the devices in them manually. See Create standard device groups on page 104.
- **Smart** – Use Smart Device Groups to greatly simplify the creation and management of large groups of devices. Dynamically add devices to a group by defining rules to create a Smart Device Group. Rules can match criteria such as organizational hierarchy, geographic location, or network domain. When you create a Smart Device Group, any new devices that match the rules you defined are added to the group automatically. See Manage devices dynamically with Smart Device Groups on page 105.

Wildcard Devices

Some overlay network configurations require allowing all traffic inbound or outbound to a specific IP. This can be accomplished with a wildcard 0.0.0.0 network device.

Applies to:	2.1.3 and above

A 0.0.0.0 device functions as a wildcard, and when configuring trust, selecting the 0.0.0.0 device applies the trust policy to all devices behind the parent Airwall Gateway. However, there are several things to consider when planning a configuration that uses the 0.0.0.0 wildcard device.

- Each overlay network can only have one 0.0.0.0 address to avoid the possibility of IP address conflicts.
- If your Airwall Gateway is running a version prior to 2.1.3, overlay networks containing a 0.0.0.0 device cannot use subnet routing or NAT.
- Airwall Gateways running version 2.1.3 or above support subnet routing, NAT, and SNAT. It is recommended all Airwall Edge Services in an overlay network with the 0.0.0.0 wildcard device run version 2.1.3 or later.
- Airwall Agents and Airwall Servers do not support the 0.0.0.0 wildcard device.

How to configure wildcard devices

1. Go to **Airwalls** and select an Airwall Edge Service.
2. Add a new device with the IP address set to 0.0.0.0. See Add devices to the Conductor on page 414 for more information about adding devices.
3. Go to **Overlays** and select the overlay network for which you are configuring trust.
4. On the **Devices** tab, click the button for the 0.0.0.0 device, and then select the other devices and groups in the overlay network that require communications with the devices represented by the 0.0.0.0 wildcard device.

Overlay network default route

Starting in version 2.1.3, Airwall Gateways now support the option of setting a default route on the overlay network. This can be set on a per Airwall Gateway basis under the **Local Devices > Overlay Routes** section.

Advantages of setting a default route on the overlay helps simplify network deployments and architectures where the Airwall Gateway's local devices are in multiple subnets more than one hop away.

CAUTION: If you set an overlay network default route on Airwall Gateways running versions prior to 2.1.3, it might cause internal routing issues, leading to the Airwall Gateway not reporting as online in Conductor.

See also

- https://www.temperednetworks.com/sites/default/files/webhelp/content/topics/support_kb_110.html
- Wildcard Devices on page 416

Create an overlay network default route

To create an overlay network default route:

1. Navigate to the **Airwalls** page and select an Airwall Edge Service.
2. Add a new overlay route with a Target Network Address set to 0.0.0.0/0 and set the Gateway to the next hop gateway.

   Note: This next hop gateway needs to be within the same subnet as the subnet used for the Airwall Gateway's **Overlay Gateway IP**.

Device page

The device page shows you the details for the device.

Information on this page includes:

- Overlay device IP
- UUID for access using the Conductor API
- Device type
- The Airwall Gateway or Airwall Server that protects the device.
- Device's membership in overlays, Device groups, and Airwall groups
- What devices it has trust to and which overlay controls that trust policy

Manage a device

You can manage a device from the device page:

- **Enable or disable network communication** – Under **Network Communication**, use the **Enabled/Disabled** toggle. If a device is causing issues on the network, you can disable it while you troubleshoot.
- **Manage device membership** – Select any link (Overlay, device group, Airwall group, or remote device) to go to that page and manage the device's membership.

Create and Manage an Overlay (Protected) Network

Create an overlay (protected) network for your deployment.

Supported roles	Create or delete overlays – System administrators Modify – System and Network administrators

Before you begin, check that:

- Airwall Gateways are connected to the Conductor, and Airwall Gateway groups are created, if desired. See Set up physical Airwall Gateways on page 275 for more information.
- Devices are connected to Airwall Gateways and device groups created, if desired. See Connect and Configure Devices on page 414 for more information.
- Determine whether you want to enable VLAN tagged traffic on the overlay network. See Allow VLAN tagged traffic in your overlay network on page 419 for more information.
- Determine the users and administrative roles needed to manage the overlay network. See Edit people who can access an overlay network on page 419 for more information.

Create an overlay network

The last step in deploying the Airwall secure network is to create an overlay. An overlay is a fabric of secured communications channels that allow trusted devices to communicate securely with each other. Overlays are controlled by Airwall Edge Services and administered by the Conductor.

To create an overlay network:

1. Go to **Overlays** and click **New overlay network**.
2. Enter a name and description (optional) for the overlay network.
3. ***In 2.2.10 and later***, if you want the overlay to manage relay rules automatically, enable the **Manage a relay rule based on this overlay network's configuration** option, and choose the Airwall Relays or Airwall Relay groups that you want this overlay to use..

   Note: You must first set up an Airwall Relay before you can enable automatic relay rules.

4. Select **Save**.
5. Select the overlay you added and on the **Devices** tab, click the button to the right of **Add devices**.
6. In the **Add Devices** dialog, select each device or device group that you want to add to the overlay network and click **Add Devices**.
7. In the **People** section on the right side of the **Devices** tab, click **Update** to assign managers or members of the overlay network.
8. Optional: Select the **VLAN tagged traffic** tab and select the appropriate options if you want to allow VLAN tagged or untagged traffic.

Basic overlay network creation is now complete. For more information, see the following sections:

- Add devices or device groups to an overlay network on page 419
- Set up Overlay Port Groups on page 386
- Configure Device Trust on page 427
- Set an Overlay to Automatically Manage Relay Rules on page 354

Add devices or device groups to an overlay network

Once an overlay network is created, you can add devices or groups of devices.

To add devices to an overlay network:

1. Go to **Overlays** and select an overlay network
2. Click the button to the right of the **Add devices** field and a list of available devices is displayed.

   Note: If the name of the device is known, you can enter the device name directly into the text box and a list of matching devices and device groups will be displayed.
3. Select the devices you want to add to the overlay network and click **Add Devices**.

If you have a large number of devices, you may want to consider creating device groups. See Use device groups and smart device groups on page 416 for more information.

Important: Adding devices to an overlay network does not enable communications to or from that device. To enable communications, you must enable trust between devices. See Configure Device Trust on page 427 for information on device trust.

Edit people who can access an overlay network

Overlay networks can only be modified by users who are editors of that network. After creating an overlay network, you may want to add additional editors, viewers, or users to your overlay network or edit their roles.

To edit members of an overlay network:

1. Go to **Overlays** and select the overlay network.
2. In **People** click **Update**.
3. The **Add People** dialog displays the list of users. You can add a user as a viewer, user, or editor (in earlier versions, you can select member (viewer) or manager (editor)) by checking the appropriate column in the list.
4. When finished, click **Close**.

Allow VLAN tagged traffic in your overlay network

If your overlay network needs to support VLAN tagged traffic, you must explicitly allow VLAN tagging:

1. Go to **Overlays** and select an overlay network.
2. In the **Info** section, click **Edit Settings**.
3. In the overlay dialog, click the **VLAN tagged traffic** tab and set the following:
   a) Specify if tagged or untagged traffic is allowed on your network.
   b) In **Allowed tags**, enter VLAN tags separated by commas. You may specify tags from 0 to 4095. Leave the field blank if you want to accept any VLAN tag.
4. Click **Save**.

Set up Overlay Port Groups

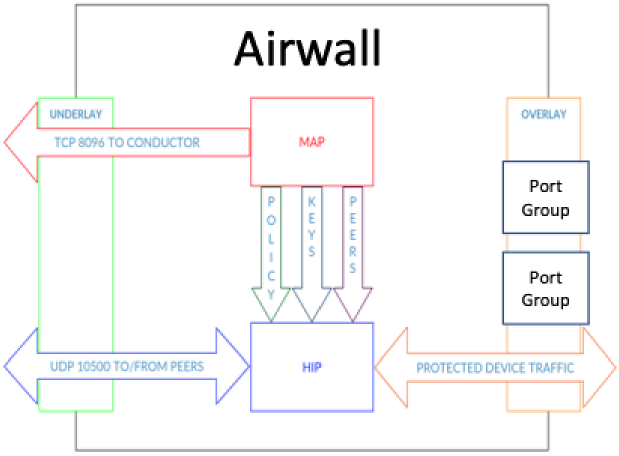
The default port groups work for some deployments. You may need to set up overlay port groups if your deployment requires it.

Overlay Port Groups are used to connect your Airwall Gateway to your protected networks. Airwall Gateways default to having a single overlay Port Group, but you may need to configure your overlay port groups when you want to:

- Micro-segment your network for fine grain security control
- Configure IP addresses or Source NAT (SNAT) for routed deployments
- Set up two Airwall Gateways for High Availability

If your Airwall Gateway is only providing relay functionality, it only needs an Underlay Port Group, and does not use any configured Overlay port group.

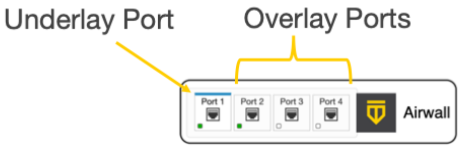
You can set up multiple port groups for an overlay, assigned to different physical or VLAN tagged sub-interface ports. When multiple ports are included in a Port Group, they are bridged. Port groups are also connected to the overlay through routing and/or bridging.

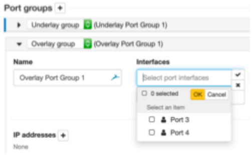


Get to Know Your Airwall Gateway Ports

Here is how the physical ports are assigned on most Airwall Gateways:

- Port 1 – Connects to the initial underlay network, and is assigned to the underlay Port Group.
- Port 2 & Up – Connect to overlay networks, and are assigned to an overlay Port Group.




Port groups +

Underlay group (Underlay Port Group 1)

Overlay group (Overlay Port Group 1)

Name: Overlay Port Group 1

Interfaces: Select port interfaces

□ 0 selected OK Cancel

Select an item

□ Port 3

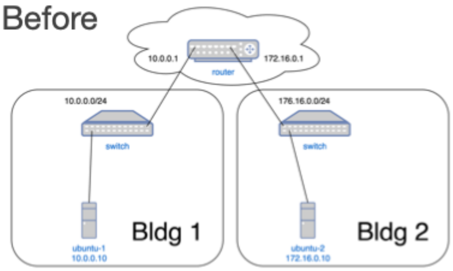
□ Port 4

IP addresses +

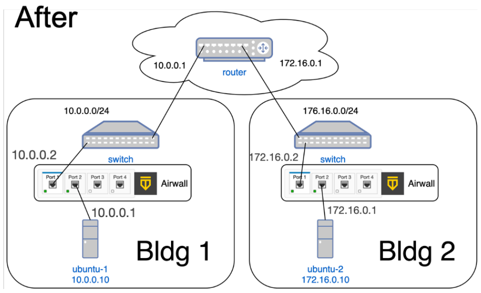
None

Basic Airwall Gateway Deployment

The most basic Airwall Gateway deployment design is to put Airwall Gateways inline in front of protected devices. If you don't want to, or can't, change IP addresses, you replicate the default gateway of the router on the overlay Port Group. (If these devices are using DHCP, see Protected devices with static routing on page 409 to configure DHCP on the overlay port group.)



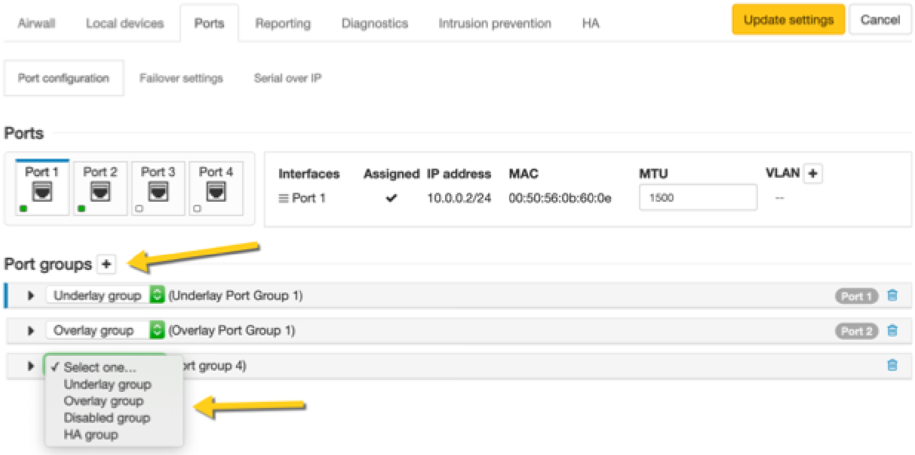
The underlay IP address can be any address on the network. DHCP is common, or you can configure a static IP if needed. The overlay IP address is the same as the default gateway on the router.



Set up an Overlay Port Group

By default, an Airwall Gateway has two port groups. One underlay port group assigned to Port 1 and one overlay port group assigned to the remaining ports. On virtual and cloud Airwall Gateways, you may be able to configure more ports if supported by the virtual or cloud platform.

1. In the Conductor, go to the Airwall Gateway on which you want to set Port Groups, open the **Ports** tab, and select **Edit Settings**.
2. Select an Overlay port group you want to use, or add a new port group by clicking the + to the right of **Port groups**, and select **Overlay group**.



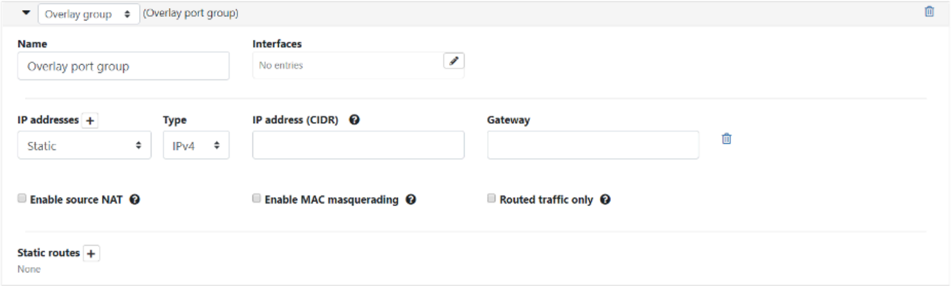
Ports

Interfaces	Assigned	IP address	MAC	MTU	VLAN +
≡ Port 1	✓	10.0.0.2/24	00:50:56:0b:60:0e	1500	--

Port groups +

- Underlay group (Underlay Port Group 1) Port 1
- Overlay group (Overlay Port Group 1) Port 2
- ✓ Select one... (...rt group 4)

3. Click the arrow on the left of your **Overlay group** header to expand the settings for that Port Group.


Overlay group (Overlay port group)

Name: Overlay port group

Interfaces: No entries

IP addresses +	Type	IP address (CIDR)	Gateway
Static	IPv4		

☐ Enable source NAT ☐ Enable MAC masquerading ☐ Routed traffic only

Static routes +

None

4. Enter a name for the group, and under **Interfaces**, select the ports or other interfaces for the group.
5. Under **IP addresses**, click the **+** to add IP addresses. For example, 10.0.1.1/24 (be sure to include the prefix length). Your protected devices will use this address as their gateway to reach the rest of your overlay network.
6. Select the network options that apply for your implementation:
   a) **Enable Source NAT** – Check this box to rewrite the source IP address of traffic arriving from other port groups or tunnels with the overlay IP address of this port group. You must also configure an overlay IP address. Use this option when your local protected devices do not use this Airwall Gateway as their default gateway. This setting enables connections, permitted by policy, from remote overlay devices to local protected

devices. When you enable Source NAT, local protected devices cannot initiate connections to remote overlay devices.

b) **Enable MAC masquerading** – Check this box to rewrite the source MAC address of all traffic arriving from other port groups or tunnels with the Airwall's MAC address. Use this option if the network you are connected to doesn't permit foreign MAC addresses. Note: Checking the Routed traffic only box enables MAC masquerading by default.

c) **Enable spanning tree protocol** – Leave this box checked to enable spanning tree protocol on the overlay bridge to avoid potential bridge loops. Only clear this box if this port group is free of any bridge loops, and you do not wish to run STP. One example is if this port group is connected to a Cisco switch running BPDU guard. A recommended alternative is to configure the port group with only a single port and use routed traffic only mode to make bridge loops impossible.

d) **Routed traffic only** – Check this box to permit only routed bypass traffic. You must also configure an overlay IP address. Local protected devices should use this overlay IP as a gateway (either their default gateway or a static route) or Source NAT to allow incoming connections. Typically, you check Routed traffic only, unless you specifically need to bridge traffic. For example, if you have IP addresses in the same subnet on both sides of the tunnel, you are bridging traffic, so clear this box.

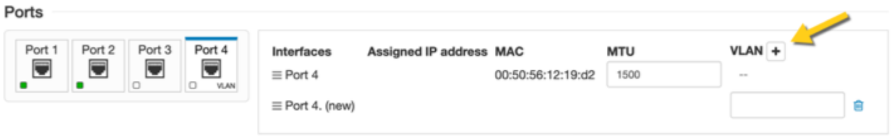
This setting prevents inadvertently carrying broadcast and multicast traffic sent by protected devices and can improve performance by using only a single port in the port group.

7. If you are connecting this port group to a router connected to a larger overlay network, you can configure static routes or even a default gateway.
8. Select **Update Settings**.

Add Interfaces to a Port

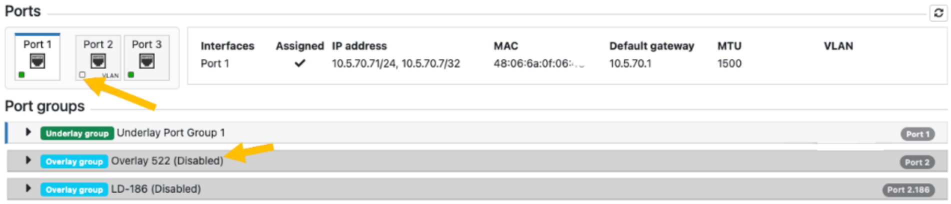
Each physical or logical port on an Airwall Gateway has a single interface by default, that can be assigned to a port group. If you are connecting an Airwall Gateway port to a switch using an 802.1q trunk allowing multiple VLANs, you need to add additional interfaces. To do this:

1. Up above the **Port Groups** section, select the **Port** and then click **Edit Settings**.
2. Next to **VLAN**, click the **+** to add a new VLAN for this overlay.
3. Enter the VLAN tag to match the VLAN config on the switch.



Interfaces	Assigned IP address	MAC	MTU	VLAN +
≡ Port 4		00:50:56:12:19:d2	1500	--
≡ Port 4. (new)				

Note: If you disable the VLAN parent interface, the child interfaces are also disabled.



Interfaces	Assigned	IP address	MAC	Default gateway	MTU	VLAN
Port 1	✓	10.5.70.71/24, 10.5.70.7/32	48:06:6a:0f:06:...	10.5.70.1	1500	

- Underlay group Underlay Port Group 1 — Port 1
- Overlay group Overlay 522 (Disabled) — Port 2
- Overlay group LD-186 (Disabled) — Port 2.186

Do I need a gateway?

You only need a gateway if the Airwall Gateway needs to know how to reach additional networks from this port. The Airwall Gateway is the gateway for its protected devices. In general, using static routes (for example, 10.0.0.0/8) for your corporate network is preferable to using a default gateway (which is a 0.0.0.0/0 route), particularly if you have a bypass destination of 0.0.0.0/0 set up, since that will cause a conflict.

Set overlay traffic logging for an Airwall Gateway

Airwall Gateways log overlay traffic from local device to local device, and you can set the log level and frequency per Airwall Gateway. Use this setting in conjunction with remote syslog to log a summary of overlay traffic flow from an Airwall Gateway.

Tech Preview: This feature is currently included as a tech preview, and features and formatting may change. Logging is currently sent over a separate channel from HIP or MAP, and the log format is not currently stable.

Supported Airwall Edge Services	All v3.1.0 Airwall Gateways All v3.1.0 Airwall Agents and Servers

Set overlay logging

1. Open the page for an Airwall Gateway and go to **Diagnostics** > **Data capture**.
2. On the right, scroll down to **Airwall log level** > **Data plane event logging**.
3. Next to **Overlay network activity**, select the pencil to edit settings.
4. Edit the options for overlay network activity logging:
   - **Log level** – Select the log level at which traffic is logged. You may need to also adjust the logging level elsewhere in your log pipeline. For example, Airwall Gateways default to suppressing log messages with a severity less than INFO.
   - **Time interval** – Enter the number of seconds before logging additional device activity for a flow. To disable, select 0. To use the system default, leave blank.
   - **Packet interval** – Enter the number of packets before logging additional device activity for a flow. To disable, select 0. To use the system default, leave blank.
5. You can filter the output through a security information and event management (SIEM) tool.

Example

Here's an example of the FLOWLOG messages that you'll see in the remote syslog server you set up in the Conductor.

```
root@aw300v-B1D3ACB87C8B:~# grep FLOWLOG /var/log/messages
Aug 23 16:38:04 aw300v-B1D3ACB87C8B openhip: [INFO] FLOWLOG:
 flow_key=[-1, 2001:14:2ca2:24f7:4bd1:28d8:de5d:ddf8, 4a:06:6a:5d:dd:f8,
 01:00:5e:00:00:fb, 0, 0x800, 1.93.221.248, 224.0.0.251]
 action=TX_FLOOD_LOCAL age=253 packets=13 bytes=4955
Aug 23 16:38:11 aw300v-B1D3ACB87C8B openhip: [INFO] FLOWLOG:
 flow_key=[-1, 2001:14:2ca2:24f7:4bd1:28d8:de5d:ddf8, 4a:06:6a:5d:dd:f8,
 4a:06:6a:20:73:5d, 0, 0x800, 1.93.221.248, 10.192.204.105] action=TX_PG 2
 age=247 packets=11 bytes=870
Aug 23 16:38:11 aw300v-B1D3ACB87C8B openhip: [INFO] FLOWLOG:
 flow_key=[2, ::, 4a:06:6a:20:73:5d, 4a:06:6a:20:73:5d, 0,
 0x800, 10.192.204.105, 1.93.221.248] action=TX_HIT_ROUTED
 2001:14:2ca2:24f7:4bd1:28d8:de5d:ddf8 age=247 packets=9 bytes=1710
```

Here are the fields included after flow_key (these are the same as the output for `airsh policy details`):

- `PGID` – Ingress port group ID
- `PEER_HIT` – Ingress peer Airwall Edge Service HIT
- `MAC SRC` – Source Ethernet MAC address
- `MAC DST` – Destination Ethernet MAC address
- `ETH` – EtherType
- `VLAN` – VLAN ID (if 802.1q VLAN tag is present, otherwise 0)
- `IP SRC` – Source IP address
- `IP DST` – Destination IP address
- `Action` – The action the Airwall Edge Service is performing on this flow
- `AGE` – Age of flow (either since first packet, or first packet after the last policy change
- `Packets` - The number of packets processes in this flow
- `Bytes` - The total number of bytes in Ethernet frames in this flow

Set an Overlay to Automatically Manage Relay Rules

You can easily manage the relay rules for an overlay by setting it to automatically create relay rules that allow the trust relationships in the overlay.

Supported Versions	Conductor 2.2.10 and later
Required Roles	System administrators Network administrators with permissions to the overlay

Note: You must first set up an Airwall Relay before you can enable automatic relay rules.

You can also configure Airwall Relay rules manually. See Configure Airwall Relay rules on page 353.

1. Open the overlay you want to automatically manage your relay rules.
2. Under **Info** on the right sidebar, select **Edit Settings**.
3. On the **General** tab, enable the **Manage a relay rule based on this overlay network's configuration** option.
4. Choose the Airwall Relays or Airwall Relay groups that you want this overlay to use.
5. Select **Save**.

The overlay creates relay rules that allow communication between all Airwall Edge Services in the overlay. Note that you still need to set up device to device trust for them to communicate.

Note: Airwall Edge Services try to connect directly first, and only use the relay if they cannot connect directly.

Note: Managed relay rules do not normally display on the **Airwalls** page. If you want to see them, you can go to **Airwalls** > **Airwall relay rules** and at the bottom right, check **Display system relay rules**.

East-West Security Policy Best Practice Guide

Setting up East-West access is not any more difficult than setting up North-South access. You work with Local Devices and Overlays.

Set up an East-West policy to allow devices cloaked by a Airwall Gateway to communicate with an uncloaked network resource. You may want to do this if you're not ready or don't want to put the network resource behind a Airwall Gateway, or if you're unable to run an Airwall Server on it. When you set up the overlays following this guide, the East-West traffic is isolated to the appropriate overlay networks and clearly indicates which resources are available for East-West communication.

Before you begin

Check the following requirements before setting up an East-West security policy.

Supported Versions	v2.2.1 Conductors and Airwall Gateways
Supported Airwall Gateways	Physical and virtual Airwall Gateways **CAUTION:** Do not attempt to set up an East-West security policy on any cloud Airwall Gateway deployments. It breaks the cloud access and cloud route insertion for the cloud Airwall Gateway.
Supported Roles	System administrator, or a network administrator with access to the Airwall Gateways and overlays involved in the configuration.

Set up an East-West security policy

Setting up East-West access is not any more difficult than setting up North-South access. You work with Local Devices and overlays.

Here is an overview of the steps:

1. Physically or virtually connect the underlay Port Group to the unprotected network, and the Overlay Port Group to the protected network.
2. Create an additional Overlay Port Group (called a Bypass Port Group) to access the unprotected network resource.
3. Add the network resources as local devices on the Airwall Gateway.
4. Create device groups to manage permissions.
5. Add a bypass overlay to connect and set trust between the protected and unprotected device groups.

These steps are outlined in more detail below.

Step 1: Connect the Networks to the Underlay and Overlay port groups

Connect the networks you want to use to the Underlay and Overlay port groups on the Airwall Gateway.

Step 2: Create a Bypass Port Group

Set up an additional Overlay Port Group (called the Bypass Port Group) to provide access to the unprotected resources.

1. On the page for the Airwall Gateway, open the **Ports tab.**
2. Select **Edit Settings** in the upper right.
3. Click the + that appears beside **Port groups**.
4. In the **New Port Group**, select **Overlay group** from the dropdown box.
5. Click the down arrow by the new port group to open its settings.
6. Change the name from Port Group *x* to **Bypass Port Group**.
7. Assign the appropriate interface to the Overlay (usually Port 3).
8. By **IP addresses**, click the +.
9. Enter an available IP address for this Overlay in the unprotected subnet.

   Note: Make sure this is an available IP address and includes the appropriate Subnet Mask.

10. Enter the IP of the gateway of the unprotected network resource.

    Note: If you are working with unprotected resources that are not in the same VLAN/Subnet, also check the **Enable source NAT** box.

11. At the top of the **Ports** tab, click **Update Settings**.

You've finished creating the Bypass Port Group and are ready to add the network resources as devices.

Step 3: Add the Network Resources as Devices on the Airwall Gateway

The Network Resources that the protected devices need to reach must be listed as **Local Devices** to the Airwall Gateway, just like the protected devices are.

Add protected network resources as Local devices

Repeat these steps for all **Protected Network Resources** you want to include.

1. In the Conductor, go to the Airwall Gateway that has the devices for which you want to create an East-West security policy.
2. Go to **Local Devices** > **Configuration** and under **Local devices**, select **+ Add device**.
3. On the **Add Device** page:
   a) In **Overlay device IP**, enter the IP Address for the protected network resource.
   b) In **Name**, enter a name for the network device.
4. Select **Create**.

Add unprotected network resources as Local devices

Repeat these steps for all **Unprotected Network Resources** you want to include.

1. Go to **Local Devices** > **Configuration** and under **Local devices**, select **+ Add**.
2. On the **Add Device** page:
   a) In **Overlay device IP**, enter the IP Address for the protected network resource.
   b) In **Name**, enter a name for the network device.
3. Set the **Port Group affinity** to the Bypass Port Group you created earlier, and then click **Create**.

You've now finished adding the network resources as devices on the Airwall Gateway and are ready to create device groups.

Step 4: Create Device Groups to Manage Permissions

To make management easier, and the permissions more explicit, you now organize the network resources using **Device Groups**.

Create a Device Group for protected devices

1. Go to **Devices** > **Device groups**.
2. Select **+ New Group**.
3. Give the group a name, such as "Protected Devices," add a description and tags, if desired, and then select **Create**.
4. On the device group page, next to **Add devices**, enter text to search on or select the +, and add the protected devices to the group.

Create a Device Group for unprotected resources

1. Go to **Devices** > **Device groups**.
2. Select **+ New Group**.
3. Give the group a name, such as "Network resources," add a description and tags, if desired, and then select **Create**.
4. On the device group page, next to **Add devices**, enter text to search on or select the +, and add the unprotected resources to the group.

Step 5: Add a Bypass Overlay to Connect the Protected and Unprotected device groups

The last step is to add an Overlay (also called Bypass) to establish trust between the two device groups.

1. Go to **Overlays**, select **+ New overlay network**, and then select **Next** for manual configuration.
2. Name the overlay "Bypass", fill in description and network editors, if desired, and then select **Finish**.
3. On the Bypass overlay page, open the **Devices** tab on the right, and next to **Add devices**, select the **+**.
4. On the **Add Devices** page, select **Device groups**, check the Protected Devices and the Network Resources device groups you created earlier, and then select **Add devices**.
5. On the Bypass overlay page, on the trust graph, select **Edit trust** and drag a line between the two device groups to set trust between them.

   If you are seeing the overlay page Advanced view, under **Trust**, fill in the Trust button for both device names to set trust between the groups.

   For more help in setting device trust, see Add and remove device trust on page 427.

You've completed setting up an East-West security policy.

Additional Considerations

Review these considerations if you are connecting to the Internet, or if you're setting this up on VMware.

Using East-West over the Internet

Important: If you are going to have the East-West connect to the Internet, and set up a 0.0.0.0/0 local device, this can collide with your local DHCP settings if there are any on the unprotected network.

Setting up East-West Security Policy over VMware

If you are setting this up in VMware, you'll need to set up VMware Port groups as well as Airwall Gateway Port groups with settings of *Allow Promiscuous* and *Forged Transmit* on the VMware port groups. For more details, see Set up a virtual Airwall Gateway in VMware ESX/ESXi on page 306.

Overlay Timelines

The **Timelines** page shows recent activity on your overlay.

To start and stop recording activity – Use the **Enabled-Disabled** toggle to start and stop recording activity for the Timeline.

To move forward or backward in time – Click and drag on the timeline.

Return to the present – Select **Reset** to return to the latest activity.

Manage Airwall Edge Services from an Overlay

The Airwalls tab shows Airwall Edge Services that have devices in the overlay.

You can manage Airwall Edge Services from this page by selecting the down arrow to the right of any Airwall Edge Service. You can manage many Airwall settings from this page. Options vary depending on the Airwall version, model, and online status.

- **Airwall properties** – Select Properties to open the Airwall page. You can also add tags or onboard devices, plus other Airwall management settings.
- **Airwall diagnostics** – Check if the Airwall is online (online status is also indicated in the Airwall table – see), or set a physical Airwall to blink (see Identify a Physical Airwall Gateway on page 480).

Configure Device Trust

Configure device trust to set up secure communication between devices in your Airwall secure network.

To add trust between devices, you create or edit an Overlay network, and add the Airwall Edge Services that protect the devices you want to connect.

From **Overlays**, create or select the Overlay network for which you want to add trust.

You can see and add trust visually, or using the list of Devices.

Note: The default **Devices** tab list view does not show device trust relationships until you select a specific device or group. If trust has been configured for the selected device or group, your selected device or group is highlighted in blue, and the devices and groups it trusts are highlighted in a lighter blue.

In Advanced view:

- The **Visualization** tab shows trust relationships and allows you to add and remove trust visually.
- The **Devices** tab shows the list of devices and device groups in the Overlay, and allows you to add and remove trust.

Add and remove device trust

Set communication policies by adding trust between devices and device groups. You can use drag and drop to add and remove trust visually, or add trust on the **Devices** tab.

Supported Roles	System administrator Network administrator who is a manager of the overlay.
Supported Versions	Drag and drop trust is available for v3.0.0 and later Multi-select on the network graph is available for v3.1.0 and later

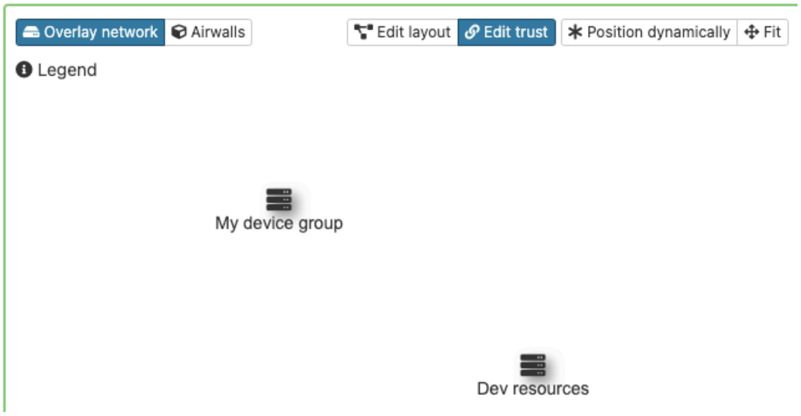
You are configuring trust only between your primary device or group and each additional device and group respectively. This setting does not configure trust between all devices selected. Devices highlighted in gray trust only the primary device. Trust between the gray devices and groups must be configured separately. For a detailed example configuration and steps to set it up, see Example: Complex device trust on page 430

Note: Network object trust policies work between a device and an IP range on a remote Airwall Edge Service. Similarly, blocking trust with a network object only prevents communication with that IP range on the remote Airwall that contains the network object. Therefore, a block policy to a network on Airwall 1 will not block communications to an IP in that range on Airwall 2. For more information, see How block and allow Overlay policies interact on page 432.

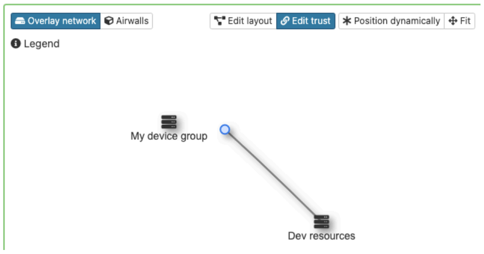
Add and remove device trust using drag-and-drop (v3.1.0)

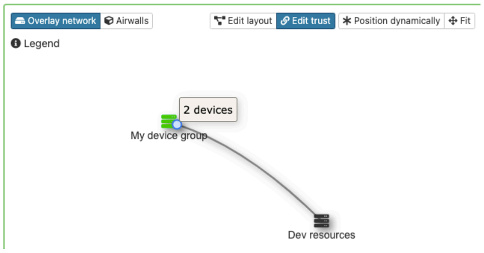
Drag and drop trust is available in v3.0.0 and later.

1. Go to **Overlays** and select the Overlay network for which you want to set up trust.
2. If you are in the **Advanced view**, go to the **Visualization** tab.
3. To see the trust for a device or device group, select a device on the graph.
4. To add trust between devices and device groups:
   a) Select **Edit trust** (in v3.0.0, select **Edit mode**) in the upper right of the visual network display.
   b) If needed, select **Position dynamically** or **Fit** to arrange the devices and device groups so you can see them.



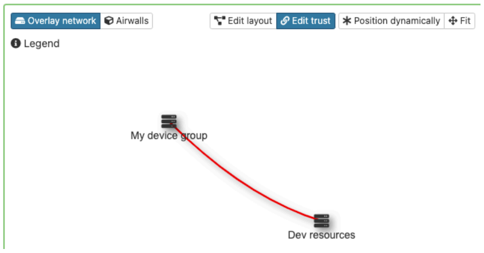
   c) Click and hold one device or device group, and drag a line to another to establish trust.





Note: **In v3.1.0**, you can select more than one item on the network graph using the meta key for your platform (Ctrl on Windows, or cmd on macOS) and either create a device group, or remove the items from the network.

5. Continue dragging and dropping to add trust as needed on the overlay network.
6. **To remove trust** – In Edit mode, click the line between the devices you no longer want to have trust. When the line turns red, click to remove it:



Tip: If you right-click a device or trust line on the graph, you get a context menu where you can quickly add or remove trust between a device and all other devices in the network.

7. To stop editing trust, select **Edit layout**. (In v3.0.0, to leave Edit mode, select **Stop edit**.)

For help in the graph, select **Legend** at the top left of the graph to show what you can do on the graph.

In a v3.1.0 Conductor, you can select more than one item on the network graph using the meta key for your platform (Ctrl on Windows, or cmd on macOS) and either create a device group, or remove the items from the network.

Add and remove device trust using drag-and-drop (before v3.1.0)

Drag and drop trust is available in v3.0.0 and later.

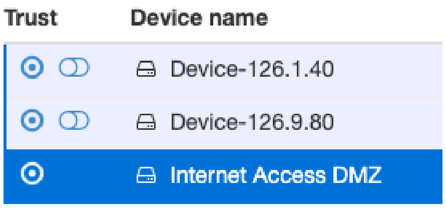
1. Go to **Overlays** and select the Overlay network for which you want to set up trust.
2. If you are in the **Advanced view**, go to the **Visualization** tab.
3. To see the trust for a device or device group, select a device on the graph.
4. To add trust between devices and device groups:
   a) Select **Edit mode** in the upper right of the visual network display.
   b) If needed, select **Position dynamically** or **Fit** to arrange the devices and device groups so you can see them.
   c) Click and hold one device or device group, and drag a line to another to establish trust.
5. Continue dragging and dropping to add trust as needed on the overlay network.
6. **To remove trust** – In Edit mode, click the line between the devices you no longer want to have trust. When the line turns red, click to remove it:
7. To leave Edit mode, select **Stop edit**.

For help in the graph, select **Legend** at the top left of the graph to show what you can do on the graph.

Note: Network object trust policies work between a device and an IP range on a remote Airwall. Similarly, blocking trust with a network object only prevents communication with that IP range on the remote Airwall that contains the network object. Therefore, a block policy to a network on Airwall 1 will not block communications to an IP in that range on Airwall 2.

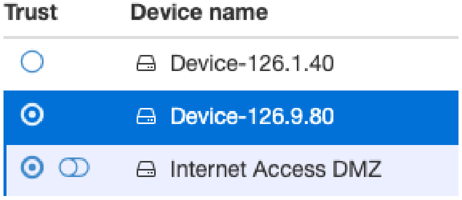
Add and remove device trust from the Devices tab

1. Go to **Overlays** and select the Overlay network for which you want to add trust.
2. On the **Devices** tab, click the Device name of the device or device group that you want to add trust for. The line will be highlighted in blue.
3. To establish trust with other devices or device groups, click the radio buttons next to them. The line will be highlighted in light blue/gray and you receive a message in the upper right of your screen that trust has been established. The following image shows trust between the Internet Access DMZ device and the other two devices.



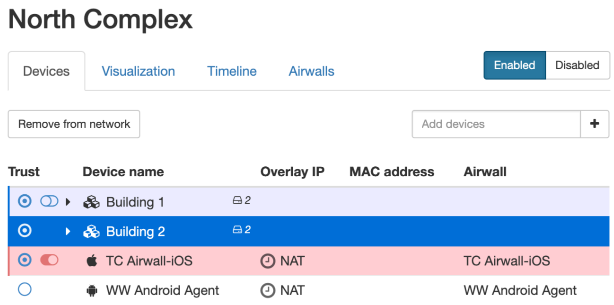
Trust	Device name
⦿ ◯◯	Device-126.1.40
⦿ ◯◯	Device-126.9.80
⦿	Internet Access DMZ

Compare to this image, when you select one of the devices, the other device is not highlighted, which indicates the devices do not trust each other - they both only trust the Internet Access DMZ device. This is a hub-and-spoke arrangement.



Trust	Device name
○	Device-126.1.40
◉	Device-126.9.80
◉ ⊂⊃	Internet Access DMZ

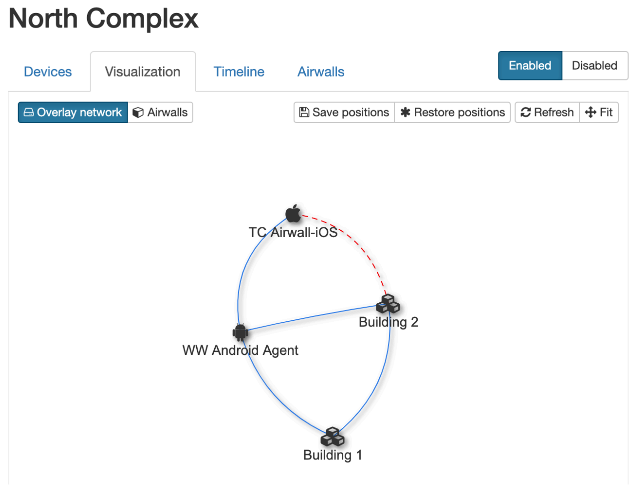
4. **To remove trust**, click the radio button again to remove it from the trust policy.
5. If you want to add a device group, but block certain devices in that group from the trust relationship, set trust for the group, and then use the toggle button next to the radio button to block trust with that device.



North Complex

Trust	Device name	Overlay IP	MAC address	Airwall
◉ ⊂⊃ ▸	Building 1 ⊟2			
◉ ▸	Building 2 ⊟2			
◉ ⊂●	TC Airwall-iOS	NAT		TC Airwall-iOS
○	WW Android Agent	NAT		WW Android Agent

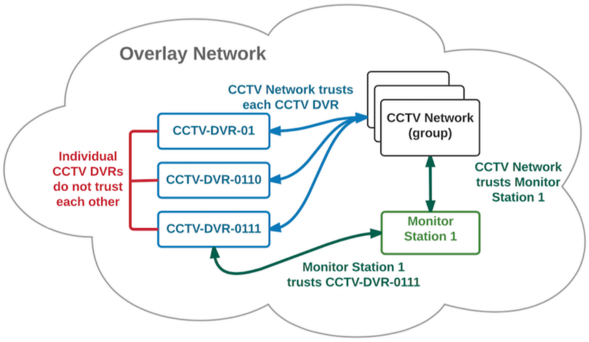
6. You can see the trust relationships on the left. (In the Advanced view, go to the **Visualization** tab.)



North Complex

Example: Complex device trust

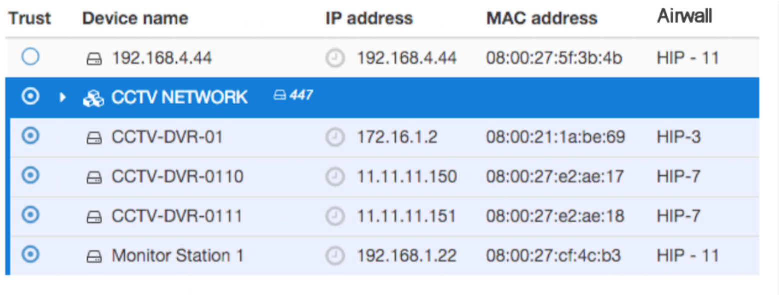
The example below shows a configuration in CCTV network that has multiple trust policies configured.



Overlay Network
CCTV Network trusts each CCTV DVR
CCTV Network (group)
Individual CCTV DVRs do not trust each other
CCTV-DVR-01
CCTV-DVR-0110
CCTV-DVR-0111
CCTV Network trusts Monitor Station 1
Monitor Station 1
Monitor Station 1 trusts CCTV-DVR-0111

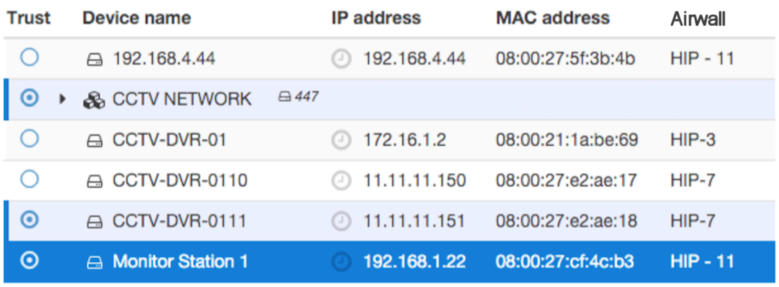
This example highlights a key concept to keep in mind when configuring device trust: you are only allowing trust between the initial device selected, highlighted in blue, and each individual device, highlighted in gray. Configuring trust between individual devices in gray is a separate step, as shown below.

1. First, configure the trust relationships for the CCTV Network device group.
   a) In the **Devices** tab, click the button for `CCTV NETWORK`
   b) Click the button for device group `CCTV-DVR-0110`
   c) Click the button for device `CCTV-DVR-0111`
   d) Click the button for device `CCTV-DVR-01`
   e) Click the button for device `Monitor Station 1`



Trust	Device name	IP address	MAC address	Airwall
○	192.168.4.44	192.168.4.44	08:00:27:5f:3b:4b	HIP - 11
◉	▸ CCTV NETWORK 447			
◉	CCTV-DVR-01	172.16.1.2	08:00:21:1a:be:69	HIP-3
◉	CCTV-DVR-0110	11.11.11.150	08:00:27:e2:ae:17	HIP-7
◉	CCTV-DVR-0111	11.11.11.151	08:00:27:e2:ae:18	HIP-7
◉	Monitor Station 1	192.168.1.22	08:00:27:cf:4c:b3	HIP - 11

2. Next configure the additional trust required between `Monitor Station 1` and `CCTV-DVR-0111`.
   a) In the **Devices** tab, click the button for `CCTV-DVR-0111`. Note that the `CCTV NETWORK` device is automatically highlighted in gray, because trust between the two was already configured in step one.
   b) Click the button for CCTV-DVR-0111 to add it to the policy.



Trust	Device name	IP address	MAC address	Airwall
○	192.168.4.44	192.168.4.44	08:00:27:5f:3b:4b	HIP - 11
◉	▸ CCTV NETWORK 447			
○	CCTV-DVR-01	172.16.1.2	08:00:21:1a:be:69	HIP-3
○	CCTV-DVR-0110	11.11.11.150	08:00:27:e2:ae:17	HIP-7
◉	CCTV-DVR-0111	11.11.11.151	08:00:27:e2:ae:18	HIP-7
◉	Monitor Station 1	192.168.1.22	08:00:27:cf:4c:b3	HIP - 11

3. Refresh the screen to return to the default **Devices** view.

Configure Large scale device trust behind an Airwall Gateway

If you have an advanced configuration with a large number of devices that are one or more hops away behind a single Airwall Edge Service, you can use a special type of device with a 0.0.0.0 IP address. A 0.0.0.0 device effectively functions as a wildcard, and when configuring trust, selecting the 0.0.0.0 device effectively applies the trust policy to all devices behind the parent Airwall Edge Service.

CAUTION: If you use the 0.0.0.0 device type, your Overlay network cannot use subnet routing or NAT, since each overlay network can only have one 0.0.0.0 address.

To create the 0.0.0.0 device and use it for trust configuration

1. Go to **Airwalls** and select an Airwall Edge Service.
2. Add a new device with the IP address set to 0.0.0.0. See Add devices to the Conductor on page 414 for more information about adding devices.
3. Go to **Overlays** and select the overlay network for which you are configuring trust.
4. On the **Devices** tab, click the button for the 0.0.0.0 device, and then select the other devices and groups in the overlay network that require communications with the devices represented by the 0.0.0.0 wildcard device.

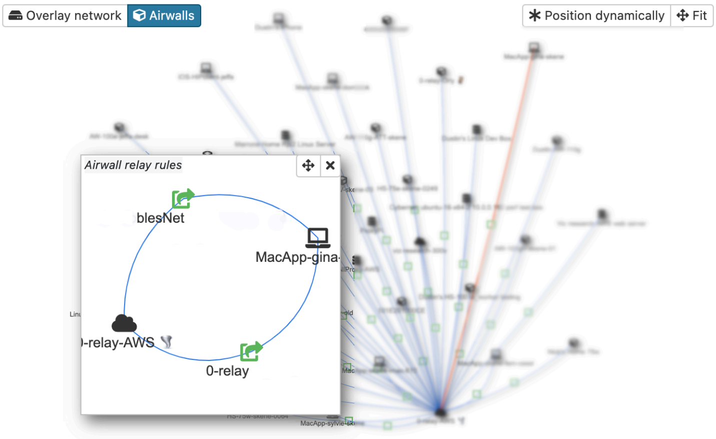
See the Trust Relationships in an Overlay network

You can see and change trust relationships visually for an overlay on its page.

For how to edit trust relationships, see Add and remove device trust on page 427.

1. Go to **Overlays** and select the Overlay network for which you want to see trust.
2. If you are in the Advanced view, go to the **Visualization** tab.
3. Trust relationships are shown as lines drawn between devices and device groups. On this page you can:
   - **See the trust for a device or device group** – Select a device or device group, and its trust relationships are highlighted. In the simplified view, they also are highlighted on the device trust list on the right.
   - **Rearrange devices** – Select **Position dynamically** or **Fit** to automatically rearrange the visualization. Or, click and drag a device or device group to reposition it.

     Note: In Edit mode, click and drag adds trust.
   - **See the communication pathways and relays** – Select Airwalls to see how Airwall Edge Services are connected and the relays used in the overlay network



How block and allow Overlay policies interact

Understand how overlay policies behave when you combine block and allow policies.

Default deny

Trust policy follows a strict secure-by-default approach. For two devices to be allowed to communicate across the overlay, there must be at least one overlay network that has trust policy between the two devices. This policy can be either between the individual device IPs or policy between network objects that include the device IPs.

Overlay policies are additive among all overlay networks

The complete set of overlay policies for a Conductor deployment is the union of all policies from each overlay network ignoring disabled overlay networks as well as disabled Airwall Edge Services or Airwall groups and devices/device groups.

Bypass device policies work the same as policies for normal devices

The main difference between normal and bypass devices is that bypass devices have no fixed Airwall ownership. Any Airwall with a bypass port can become the egress point of a bypass device depending on the peer device that sends packets to it. For policy enforcement, it makes no difference.

Block policies override normal policies

Block policies take system-wide precedence over allow policies. If two devices have block policies in any overlay, the block policy overrides all allow policies that might exist for the same two devices. Note that this is true even if the block policy is using less-specific network objects.

Example:

- Overlay 1 has allow policy between two network objects 10.0.3.0/24 and 192.168.10.100/30
- Overlay 2 has a block policy between 10.0.0.0/16 and 192.168.10.0/24
- This configuration results in traffic being blocked between all IPs from the block policy – including those from the more specific allow rule.

Policies are tied to the Airwall Gateways that own the respective network objects

This rule is intuitive if there are only allow policies, but it can lead to surprising results when allow- and block policies are present. As an example, consider the following scenario:

- Airwall 1 has a device 192.168.1.100
- Airwall 2 has a network object 10.0.3.0/24
- Airwall 3 has a network object 10.0.0.0/16
-
- Allow policy between 192.168.1.100 and 10.0.3.0/24
- Block policy between 192.168.1.100 and 10.0.0.0/16

Result: Any traffic from 192.168.1.100 to any IP included in 10.0.3.0/24 will be allowed, because the Airwall that owns the 10.0.0.0/16 network object (Airwall 3) associated with the block policy is different from the Airwall that has the allow policy (Airwall 2). If both network objects were owned by Airwall 2, the block policy would apply and prevent network communications.

Set up Cloud Providers

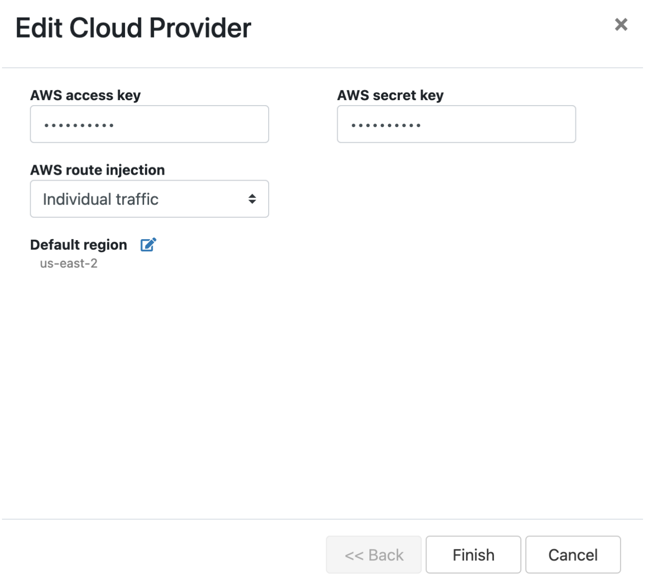
Setting up one of the supported cloud providers in your Conductor makes it easier to deploy Airwall Gateways and High-Availability Conductors directly from your Conductor.

Set up Amazon Web Services (AWS) as a cloud provider

Set up AWS as a cloud provider in your Conductor to make deploying cloud Airwall Gateways and High-availability standby Conductor easier.

Set up AWS as a cloud provider

1. In the Conductor, select the gear icon in the upper-right to access the **Settings** page.
2. Select the **Cloud providers** tab and click **+ Add Cloud Providers**
3. In the **Add Cloud Provider** dialog, select the check-mark to the right of **Amazon Web Services** and click **Next**
4. Enter your **AWS access key**, **AWS secret key**, and **Default region**



Edit Cloud Provider

AWS access key: ••••••••••

AWS secret key: ••••••••••

AWS route injection: Individual traffic

Default region: us-east-2

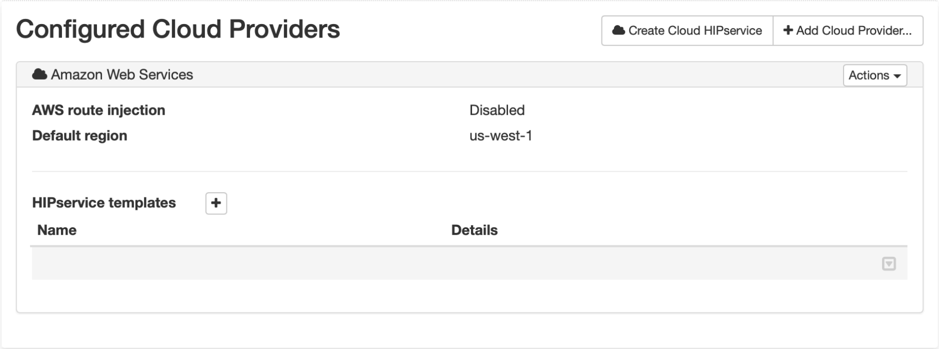
5. The **AWS route injection** setting determines how new routes are added to the AWS routing table. The routes are for traffic on your protected overlay network between protected devices and the Airwall Gateway. Here are the recommended settings depending on your deployment details:

   - If you are using a Airwall Relay, or want to manage routes on your own, set to **Disabled**.

     Important: If your Airwall's subnet has a route table with existing or planned future routes, then do not set route injection to **Individual traffic** or **All traffic**. This removes these existing and future routes from the route table, retaining only routes created by Conductor.
   - If you want to handle traffic for devices individually, set to **Individual traffic**.
   - If you want one route to send all traffic to the overlay port on the Airwall Gateway, set to **All traffic**.

     Note: All traffic is effectively ‘full tunnel’ mode. With Individual traffic, you could add routes that send traffic around the Airwall Gateway.
6. Click **Finish**

Your AWS cloud provider is displayed in the **Configured Cloud Providers** list.



Configured Cloud Providers

Amazon Web Services

AWS route injection	Disabled
Default region	us-west-1

HIPservice templates

Name	Details

Set up Microsoft Azure as a cloud provider

Set up Microsoft Azure as a cloud provider in your Conductor to make deploying cloud Airwall Gateways and High-availability standby Conductor easier.

Create an Azure Application to connect to the Airwall Conductor

Check your Azure documentation for the most recent instructions on creating an application.

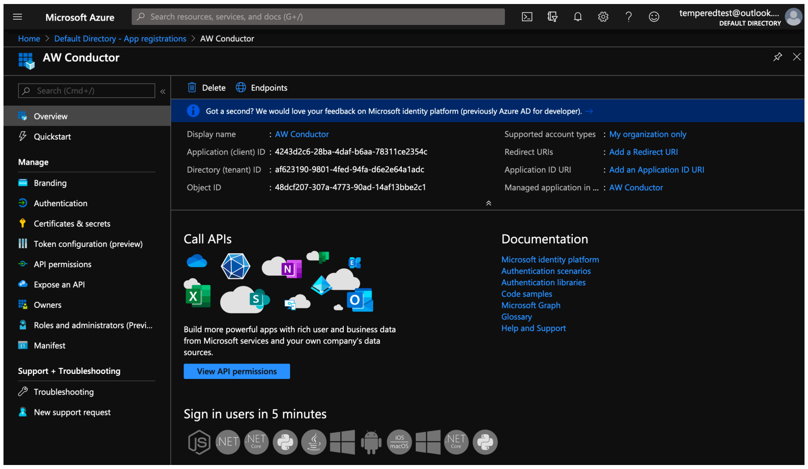
1. In Azure, in **Active directory**, under **App registrations**, register or choose an application to act as Airwall API endpoint.

2. In the Azure application, in Certificates & secrets, create a new client secret for the app to connect to Conductor. Copy it to a secure location.

   Important: You must copy the new client secret value at this step, because you won't be able to retrieve the key later.

3. From the Azure application you created, note the following information:

   - Azure **Application ID** – Get from the Azure application Overview page.
   - Azure **Application key** – The client secret you noted above.
   - Azure **Subscription ID** – In Azure, under **Users**, get the subscription details to find the ID. It's also at the top of your **Powershell** window.
   - Directory ID – Get **Directory (tenant) ID** from the Azure application Overview page.



Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Display name : AW Conductor
Application (client) ID : 4243d2c6-28ba-4daf-b6aa-78311ce2354c
Directory (tenant) ID : af623190-9801-4fed-94fa-d6e2e64a1adc
Object ID : 48dcf207-307a-4773-90ad-14af13bbe2c1
Supported account types : My organization only
Redirect URIs : Add a Redirect URI
Application ID URI : Add an Application ID URI
Managed application in ... : AW Conductor

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

4. Set up a role for the application you created to use as authorization to create Airwall Gateways in your Azure environment.

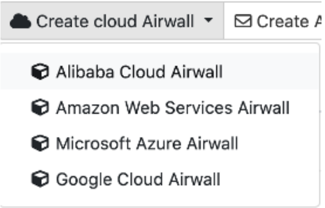
   a) From **Subscriptions**, select your subscription, and then select **Access control (IAM)**.

   b) Add a role assignment, and assign the App you created to the role: For **Role**, select **Contributor**, and for **Assign access to**, select **User, group, or service principal**, and then search for your App. You can also select a custom role with the permissions you want. For more information, see Azure help: Create a role in the Azure portal.

Add an Azure Cloud Airwall Gateway

You must Set up Microsoft Azure as a cloud provider on page 434 before you can add an Airwall Gateway in the Conductor

1. On the **Airwalls** page, (or in Conductor **Settings Cloud providers** tab), select **New cloud Airwall**, and then select **Microsoft Azure Airwall**.

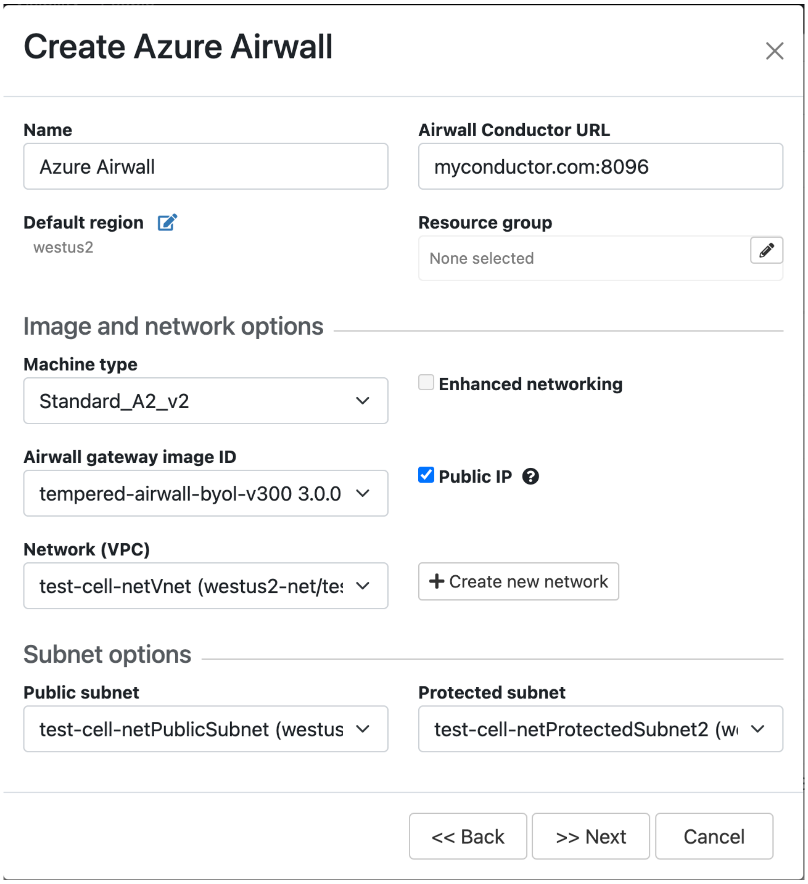


2. In v2.2.8 and later, select **Create stand-alone Airwall gateway**, and then **Next**.

3. In v2.2.8 and later, **if you want to use a template** to create the Airwall Gateway, select the template, select **Next**, and then give the Airwall Gateway a descriptive name. You can then skip to the next step.

   To continue without a template and enter the information manually, just select **Next**.

   a) If you are filling in information manually, or want to change the template, fill in the **Name** and **Image and network options** for this Airwall Gateway. For **Machine type**, the default typically works. You can select a different size if needed for your purposes.



Create Azure Airwall

Name: Azure Airwall

Airwall Conductor URL: myconductor.com:8096

Default region: westus2

Resource group: None selected

Image and network options

Machine type: Standard_A2_v2

□ Enhanced networking

Airwall gateway image ID: tempered-airwall-byol-v300 3.0.0

☑ Public IP

Network (VPC): test-cell-netVnet (westus2-net/te:

Subnet options

Public subnet: test-cell-netPublicSubnet (westus

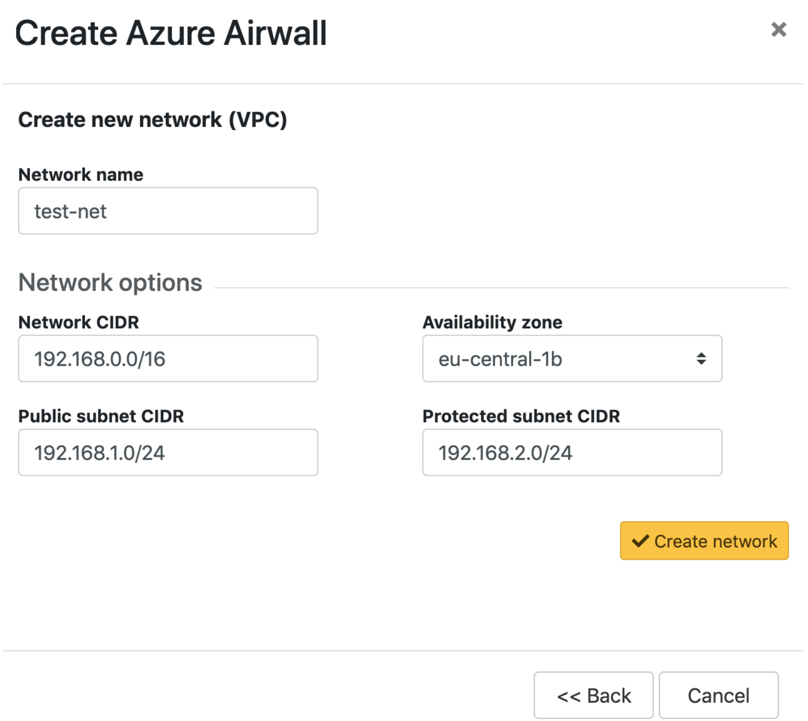
Protected subnet: test-cell-netProtectedSubnet2 (w

b) Under **Airwall gateway image ID**, pick the Airwall Gateway image you want to use. The list shows the Airwall Gateway images available on your cloud provider.

c) If you do not have a pre-configured virtual network, you need to create a new network. Click **Create new network** and fill in the form:

- **Network CIDR** – Enter an available network address and subnet mask in CIDR notation.
- **Public subnet CIDR** – Must be a subnet of the main network. Traffic flows between the underlay interface of the Airwall Gateway and the Public IP address object in Azure.
- **Protected subnet CIDR** – Must be a subnet of the main network. Traffic must pass through theAirwall Gateway or through manually-crafted routes.

When you’re finished entering the information, select **Create network**, and when processing is complete, select **Back**.



Create Azure Airwall

Create new network (VPC)

Network name: test-net

Network options

Network CIDR: 192.168.0.0/16

Availability zone: eu-central-1b

Public subnet CIDR: 192.168.1.0/24

Protected subnet CIDR: 192.168.2.0/24

d) Back on the **Create cloud Airwall** page, select the network and public and protected subnets you just created.

4. Check the summary and if everything is correct, select **Create cloud Airwall**.
5. Select **Finish**. It may take up to 5 minutes for Microsoft Azure to complete creating the Airwall Gateway.

You've completed creating an Azure cloud Airwall Gateway, and now need to configure Provision, License, and configure it. For help, see Provision and License Airwall Edge Services on page 193 and Configure Airwall Edge Service Settings on page 359.

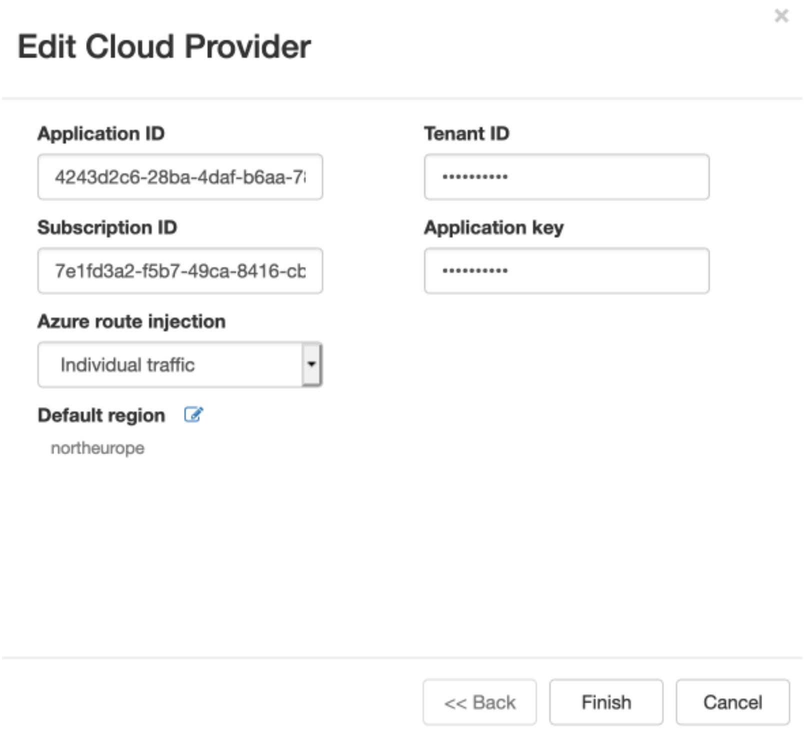
Add Azure as a Cloud Provider in Conductor

1. In Conductor **Settings**, open the **Cloud providers** tab.
2. Under **Configured cloud providers**, click **Add cloud provider**, and then select **MS Azure**.
3. Fill in the form, using the values noted when creating an application in Azure:
   - **Application ID** – Enter the Azure **Application ID**.
   - **Client secret** – Enter the Azure **Application key**.
   - **Subscription ID** – Enter the Azure **Subscription ID**.
   - **Tenant ID** – Enter the **Directory (tenant) ID**.
4. The **Azure route injection** setting determines how new routes are added to the Azure routing table. The routes are for traffic on your protected overlay network between protected devices and the Airwall Gateway. Here are the recommended settings depending on your deployment details:
   - If you are using a Airwall Relay, or want to manage routes on your own, set to **Disabled**.

     Important: If your Airwall's subnet has a route table with existing or planned future routes, then do not set route injection to **Individual traffic** or **All traffic**. This removes these existing and future routes from the route table, retaining only routes created by Conductor.
   - If you want to handle traffic for devices individually, set to **Individual traffic**.
   - If you want one route to send all traffic to the overlay port on the Airwall Gateway, set to **All traffic**.

     Note: All traffic is effectively 'full tunnel' mode. With Individual traffic, you could add routes that send traffic around the Airwall Gateway.

5. For **Default region**, click the **Sync** icon to check the connection and fill in your options. When it connects, select your default region from the list.



Edit Cloud Provider

Application ID: 4243d2c6-28ba-4daf-b6aa-7

Tenant ID: ••••••••••

Subscription ID: 7e1fd3a2-f5b7-49ca-8416-cb

Application key: ••••••••••

Azure route injection: Individual traffic

Default region: northeurope

6. Click **Finish**.

You're now ready to create cloud Airwall Gateways in Azure in the Conductor.

Set up Google Cloud as a cloud provider

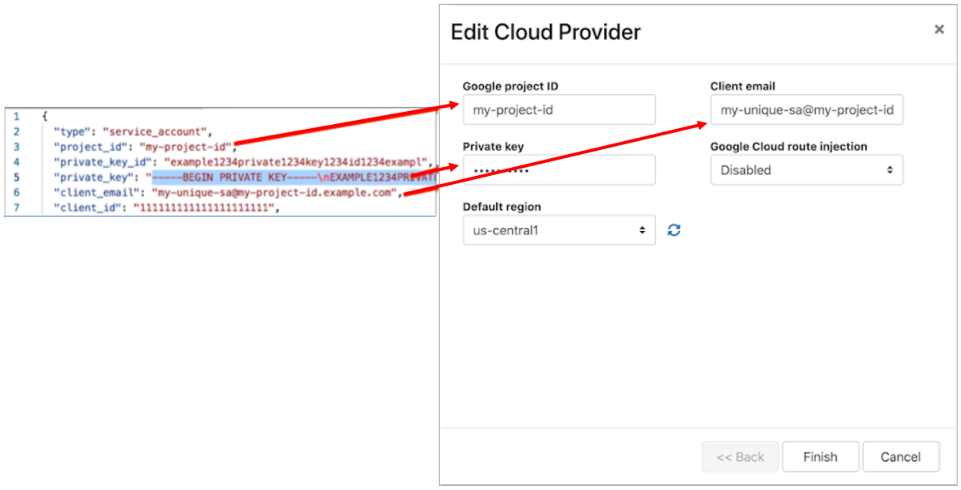
Set up Google Cloud Platform as a cloud provider in your Conductor to make deploying cloud Airwall Gateways and High-availability standby Conductor easier.

Set up Google Cloud as a cloud provider

1. Download a JSON key from your Google Cloud account. For assistance, see Google Cloud help: https://cloud.google.com/iam/docs/creating-managing-service-account-keys.

   Note: Save the key file somewhere you can access it easily. You will need the information in this file when configuring the Google Cloud provider in the Conductor.

2. Log in to your Conductor, and click the gear icon in the upper right to open **Settings**.
3. On the **Cloud providers** tab, select **Add cloud provider**.
4. Select **Google Cloud**, and then **Next**.
5. Fill in the **Google project ID**, **Client email**, and **Private key** fields with the corresponding information from the key file you downloaded.



```
{
  "type": "service_account",
  "project_id": "my-project-id",
  "private_key_id": "example1234private1234key1234id1234exampl",
  "private_key": "-----BEGIN PRIVATE KEY-----\nEXAMPLE1234PRIVAT
  "client_email": "my-unique-sa@my-project-id.example.com",
  "client_id": "11111111111111111111",
```

Edit Cloud Provider

Google project ID: my-project-id

Client email: my-unique-sa@my-project-id

Private key: ••••••••••

Google Cloud route injection: Disabled

Default region: us-central1

6. The **Google Cloud route injection** setting determines how new routes are added to the Google Cloud routing table. The routes are for traffic on your protected overlay network between protected devices and the Airwall Gateway. Here are the recommended settings depending on your deployment details:

   - If you are using a Airwall Relay, or want to manage routes on your own, set to **Disabled**.

     Important: If your Airwall's subnet has a route table with existing or planned future routes, then do not set route injection to **Individual traffic** or **All traffic**. This removes these existing and future routes from the route table, retaining only routes created by Conductor.
   - If you want to handle traffic for devices individually, set to **Individual traffic**.
   - If you want one route to send all traffic to the overlay port on the Airwall Gateway, set to **All traffic**.

     Note: All traffic is effectively 'full tunnel' mode. With Individual traffic, you could add routes that send traffic around the Airwall Gateway.
7. Click **Finish**.

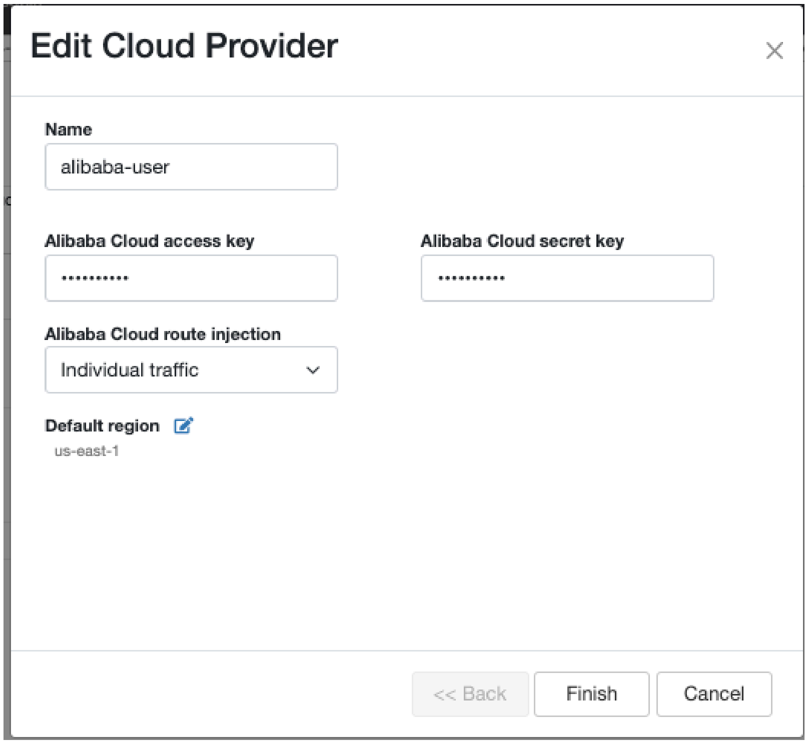
Note: If you need more information about Google Cloud Service Accounts, see https://cloud.google.com/iam/docs/creating-managing-service-accounts.

Set up Alibaba Cloud as a cloud provider

Set up Alibaba Cloud as a cloud provider in your Conductor to make deploying cloud Airwall Gateways and High-availability standby Conductor easier.

Set up Alibaba Cloud as a cloud provider

1. In the Conductor, select the gear icon in the upper-right to access the **Settings** page.
2. Select the **Cloud providers** tab and click **+ Add Cloud Providers.**
3. In the **Add Cloud Providers.** dialog, select the check-mark to the right of **Alibaba Cloud** and click **Next**
4. Enter your **Alibaba Cloud access** and **secret keys**, and choose an option for **Alibaba Cloud route injection**.



Edit Cloud Provider

Name: alibaba-user

Alibaba Cloud access key: ••••••••••

Alibaba Cloud secret key: ••••••••••

Alibaba Cloud route injection: Individual traffic

Default region: us-east-1

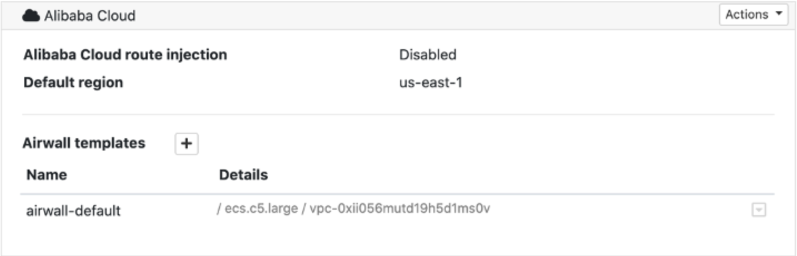
5. The **Alibaba Cloud route injection** setting determines how new routes are added to the Alibaba Cloud routing table. The routes are for traffic on your protected overlay network between protected devices and the Airwall Gateway. Here are the recommended settings depending on your deployment details:

   - If you are using a Airwall Relay, or want to manage routes on your own, set to **Disabled**.

     Important: If your Airwall's subnet has a route table with existing or planned future routes, then do not set route injection to **Individual traffic** or **All traffic**. This removes these existing and future routes from the route table, retaining only routes created by Conductor.
   - If you want to handle traffic for devices individually, set to **Individual traffic**.
   - If you want one route to send all traffic to the overlay port on the Airwall Gateway, set to **All traffic**.

     Note: All traffic is effectively 'full tunnel' mode. With Individual traffic, you could add routes that send traffic around the Airwall Gateway.
6. By **Default region**, select the Refresh icon to get the list of regions from the provider, and then select your default region.
7. Click **Finish**

   Your Alibaba Cloud provider is displayed in the **Configured Cloud Providers** list.



Alibaba Cloud

Alibaba Cloud route injection: Disabled

Default region: us-east-1

Airwall templates

Name	Details
airwall-default	/ ecs.c5.large / vpc-0xii056mutd19h5d1ms0v

Integrate Third-party Services

How to integrate the Airwall Solution with third-party services.

Integrate Third-party Authentication with OpenID Connect

You can integrate a third-party authentication provider with person authentication in the Conductor using OpenID Connect (OIDC). If your users are already configured for single sign-on (SSO) with a third party, or if you have a large number of users, this integration streamlines your user management.

Note: You can only configure one OpenID Connect provider on the Conductor at a time. If you need to support many OIDC authentication providers simultaneously, you can choose providers that support federated login so you can connect to one provider and have that provider connect to other providers to authenticate users.

Important: To use OpenID Connect on macOS or iOS Airwall Agents, you must have a public certificate on your Conductor.

User Roles

In the Airwall Conductor, you configure person roles in OIDC by including them in groups. The OIDC group names are pre-configured in the Conductor, so when you make a person a member of one of the OIDC groups in the OIDC provider, they are automatically given that role in the Conductor. For instance, you can declare that all members of the OIDC provider's cond_system_admins group are system administrators in the Conductor, and that members of the OIDC cond_remote_users group are remote-access users.

Multi-factor Authentication

If your OIDC provider supports a multi-factor authentication (MFA) protocols, you can use MFA on your provider to require MFA for logging into your Conductor or for Airwall Agent session authentication.

Integrate Authentication with the Conductor

To successfully integrate authentication, you must

1. Create and configure an application in your authentication provider.
2. Configure OIDC on the Conductor.
3. Set up Airwall Agents.
4. Verify third-party authentication is working on page 255

Since each provider is different, refer to the basics required here, and then the Provider-specific instructions that follow for integrating with some popular providers that support OIDC.

1. Create and configure an application in your authentication provider

Create and configure the application in your provider using the Provider-specific Instructions on page 249 before connecting it to the Airwall Conductor. Each provider's workflow is different, but here are the general steps:

1. Create an OpenID Connect application.
2. Configure it with the following information:

Field	Enter
Name	Whatever you want. For example, "Airwall Conductor"
Login Redirect URI	Your Conductor URI followed by `/user/auth/openid_connect/callback`. For example: `https://conductor.mycompany.com/user/auth/openid_connect/callback.` Note – If your Conductor is HA paired, add a second login redirect URI, with the same path added.
Logout Redirect URI	Your Conductor URI: https://conductor.mycompany.com

3. Depending on your provider, set the authentication method to **basic**, or indicate you are using an **authorization code** for authentication (not a refresh token).
4. Allow the **groups** claim for grant. The **groups** claim is what allows the Conductor to match a user's group with what role they are given. Because **groups** is not a default OIDC claim, it must be turned on in the provider. For more details, see the Provider-specific instructions.
5. Create four groups: `cond_system_admins`, `cond_readonly_admins`, `cond_network_admins`, and `cond_remote_users` to indicate the four different Conductor roles.
6. Add users to each group so they are assigned the correct role when logging into Conductor.
7. Give your users access to the application you created in your provider.
8. If you want to require MFA to log in, set it up in the OIDC provider. Generally MFA is associated with the app. Please consult your provider documentation for detailed instructions on setting up MFA.

2. Configure OIDC on the Airwall Conductor

1. Go to Conductor **Settings**.
2. Next to **Authentication**, select **Add provider**.
3. Select **OpenID Connect** and then select **Next**.
4. On the **Add Authentication Provider** page, under **General settings**, configure the Provider settings as follows (see the Provider-specific Instructions for help in finding this information):

For this Setting	Enter
Provider Name	Give your provider a descriptive name. This name appears as an option when logging into the Conductor.
Conductor host	Host of your Conductor. Must be in the format `https://conductor.mycompany.com` (no trailing slash)
OpenID Connect host	Must be in the format `https://hostname.com:{optional port}`
Issuer	Issuer provided by your OIDC provider. Sometimes this value is the same as the OpenID Connect host depending on the provider.
Client ID (sometimes called Identifier)	Token provided by your OIDC provider associated with the provider application
Secret	Secret token that goes with the Client ID

5. For **HA-paired Conductor host**, enter the Host of your HA Conductor (if applicable).
6. Configure the **Group** settings as follows, and then click **Next**:

For this Setting	Enter
Use groups to manage roles	Checked
System admin groups	Comma-separated list of groups from your provider that will give your user this role.
Read-only admin groups	Comma-separated list of groups from your provider that will give your user this role.
Network admin groups	Comma-separated list of groups from your provider that will give your user this role.
Remote-access user groups	Comma-separated list of groups from your provider that will give your user this role.

Note: If users are in groups that match more than one of the roles, they are given the highest level of access possible (system admin, read-only admin, network admin, then remote-access user).

7. Configure any Group filters you want, and click **Finish**.
8. If you have non-public DNS servers configured in the Conductor under **Global Airwall Agent/client settings**, your users won't be able to reach the public addresses on their devices that include the OpenID Connect providers. You may need to configure DNS servers on the Conductor to add your OpenID Connect provider's DNS server.
9. After changing OIDC configuration, you need to log out and log back in to the Conductor to restart it. When you log back in, you can now choose your third-party authentication provider.

3. Set up the Airwall Agents

Any Airwall Agents authenticating using your third-party provider also need to be set up:

1. Provision and License Airwall Edge Services on page 193 in the Conductor.
2. Go to the **Overlays** page, scroll down to **People**, and click **Update**, and add the Airwall Agent as a member.
3. Also check that:
   a) Airwall Agents are included in your Airwall Relay rules.
   b) Airwall Agent devices have been added to the appropriate Overlays, and you've set device trust on the Overlays as needed.

Your users should now be able to log in using the third-party authentication provider.

Require third-party authentication

You can also require users to authenticate using the third-party provider either individually or as a group (in 2.2.3 and later Conductors). On the agent's **Airwall Agent** tab, or on a **People Group Properties** tab:

- Check the **Require authenticated Airwall session** box.
- Under **Provider**, choose the third-party authentication provider you created.

Provider-specific Instructions

Here are specific instructions for a few of the common third-party authentication providers. Note your provider's documentation may be more up-to-date.

Okta - Create Application and Set Up Group Claims

Create an Application

1. In Okta, go to **Applications**.
2. Select **Add Application**.
3. Under **Create New Application**, select **Web**.
4. Set **Allowed grant type** to **Authorization code**.
5. Set the **OpenID Connect host** to the same value as the **Issuer** in Conductor. This value is found on the under **OpenID Connect ID Token** on the **Sign on** tab.
6. Note the Client ID and Secret that are in your application, on the **General** tab under **Client Credentials**.
7. Set up Groups Claim (see below).

Set up Groups Claim

To set up Okta to allow the groups claim in OpenID Connect, use the Classic UI.

1. In Okta Authentication, go to **Security**, and select **API**.
2. From the **Authorization Servers** tab, open the default API (or whatever API you are assigning to your application).
3. On the **Scopes** tab:
   a) Add a scope named `groups`.
   b) Uncheck **Set as Default**.
   c) Check **Include in Public Metadata**.

4. On the **Claims** tab:
   a) Add a claim named `groups`.
   b) Set **Include in token type** to **ID Token / Always**
   c) Set **Value type** to **Groups**
   d) Set a filter of **Matches regex** to `.*`. Alternatively, set a filter of **Starts with** and set to the prefix for your group names that you want to use in Conductor. For example, set **Starts with** to `cond_`.
   e) Set **Include in** to **Any scope**.

OneLogin - Create Application

1. In OneLogin, select **Add App,** and then choose **OpenID Connect (OIDC)**.
2. Set **Authentication method** to **basic**.
3. Add users to the roles you want. For example, to make them a system admin, add them to **cond_sysadmins**.

   Note: In OneLogin, roles are mapped to OIDC groups (groups mean something else), so add users to roles, not groups.
4. In your OneLogin application, on the **Parameters** tab, configure the roles-to-groups mapping. Edit the groups and modify the default on the **Roles** field to: **User roles, --No transform—**.
5. Note the information you'll need to configure the Conductor:
   a) **OpenID Connect host**: This is your OneLogin login URL, for example, `https://my-company.onelogin.com`.
   b) **Issuer**: On the **SSO** tab, select **OpenID Provider Configuration Information** for the **Issuer**.
   c) **Client ID and Secret**: These are both on the **SSO** tab.

Auth0 - Create Application

1. In Auth0, under **Applications**, select **Create Application**, and then **Regular Web Application**.
2. Skip the quick start.
3. On your new application's **Settings** page:
   a) Change **Application Properties** > **Token Endpoint Authentication Method** to **Basic**.
   b) In **Application URIs** > **Allowed Callback URLs**, add the login redirect URI. See the Login Redirect URI near the top of this page.
   c) In **Application URIs** > **Allowed Logout URLs**, add the logout redirect URI. See the Logout Redirect URI near the top of this page.

      Note: Auth0 does not currently support OpenID Connect Logout.
   d) Note the following information in Auth0 that you'll need to configure the Conductor:
      - **Basic Information** > **Domain**: On the Conductor, you enter this information as **Open Connect host** and **Issuer** (note that the https is required).
      - **Basic Information** > **Client ID** and **Client Secret**: On the Conductor, you enter this information as Client ID and Secret.
   e) When finished, select **Save Changes** at the bottom of the **Settings** page.
4. Add the rule required by Auth0 to set OIDC groups. (In Auth0, roles map to groups on the Conductor.)
   a) Under **Auth Pipeline** > **Rules**, select **Create Rule**.
   b) Select **Empty Rule**.
   c) Set the name to **Add groups to OIDC token**.
   d) Add this rule:

```
function (user, context, callback) {
    const namespace = 'https://<your issuer>';
    const assignedRoles = (context.authorization || {}).roles;
    let idTokenClaims = context.idToken || {};
    let accessTokenClaims = context.accessToken || {};

    idTokenClaims[`${namespace}/groups`] = assignedRoles;
    accessTokenClaims[`${namespace}/groups`] = assignedRoles;

    context.idToken = idTokenClaims;
    context.accessToken = accessTokenClaims;

    callback(null, user, context);
}
```

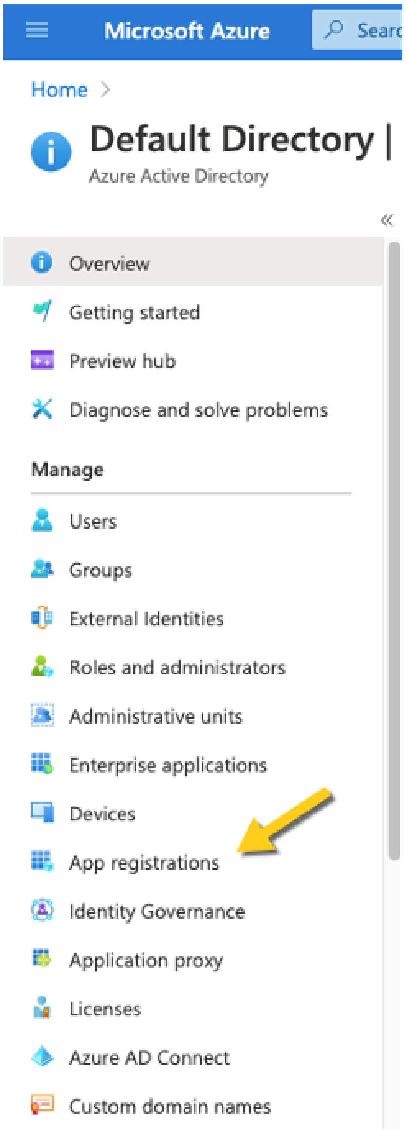
e) Change the namespace in the rule to be your Auth0 issuer. Example: `https://dev-abc123.auth0.com`

5. Following Auth0 instructions, add roles to users that give them the proper role in the Conductor.

Azure Active Directory - Create Application

Note that the Azure AD documentation may be more up-to-date and the settings in your Azure AD account may vary.

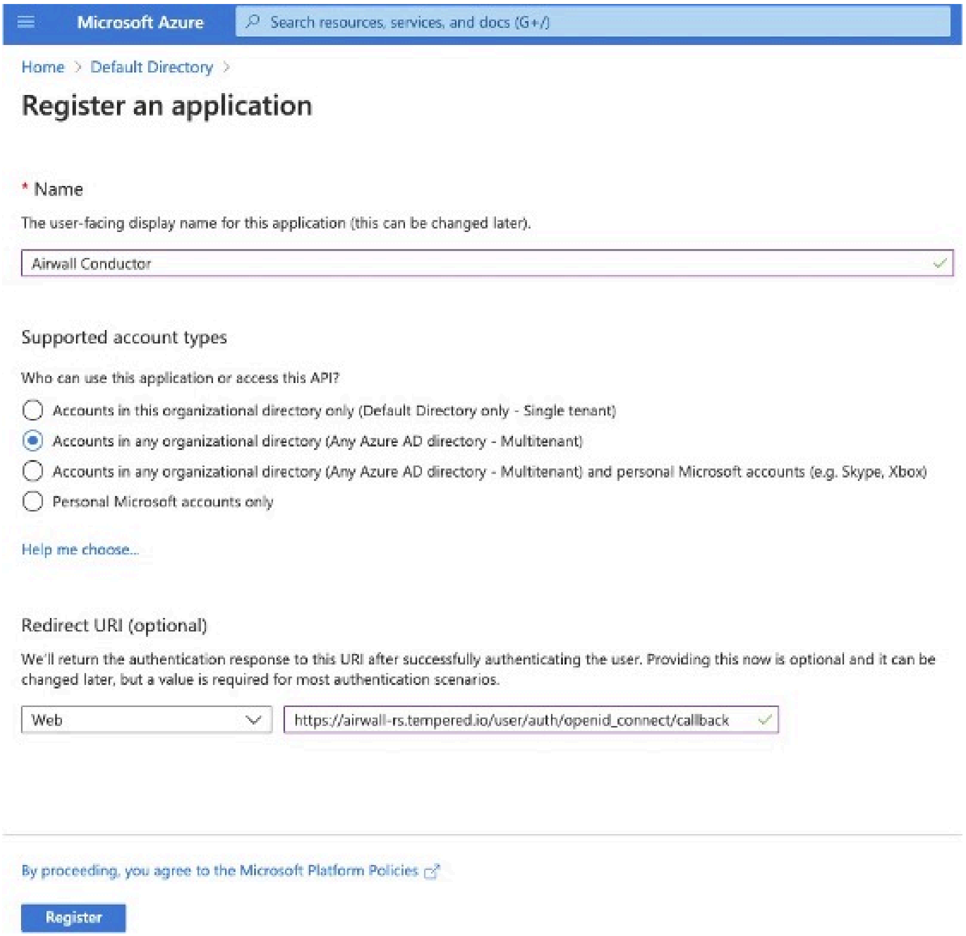
1. In Azure Active Directory (AD), select **App registrations**.



2. Select **New Registration**, and fill in the form as follows:

- **Name** – Enter a name for the Application (for example, "Airwall Conductor").

- **Supported account types** – Select **Accounts in any organizational directory (Any Azure AD directory – multitenant)**.
- **Redirect URI** – Select **Web**, and then enter the URL of your Conductor followed by `/user/auth/openid_connect/callback`:



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Default Directory >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

Airwall Conductor

Supported account types

Who can use this application or access this API?

○ Accounts in this organizational directory only (Default Directory only - Single tenant)
● Accounts in any organizational directory (Any Azure AD directory - Multitenant)
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
○ Personal Microsoft accounts only

Redirect URI (optional)

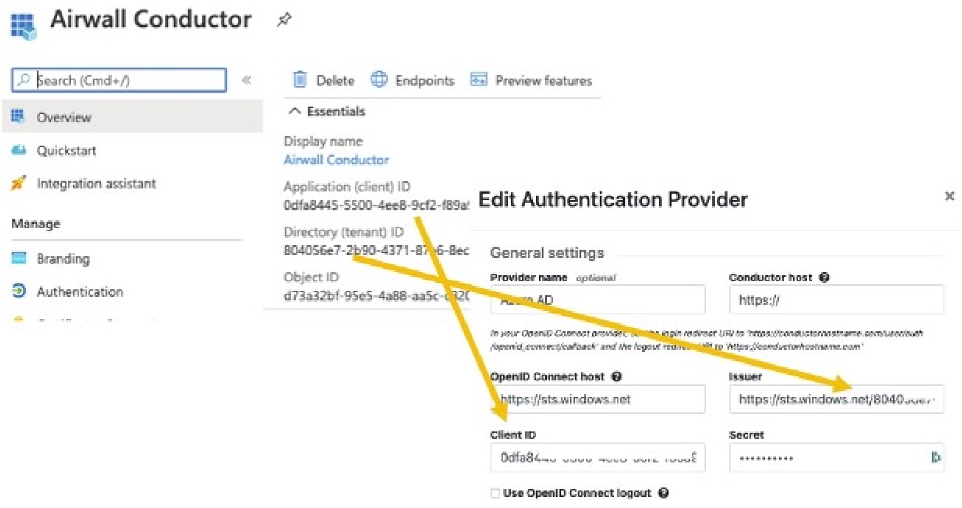
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | https://airwall-rs.tempered.io/user/auth/openid_connect/callback

By proceeding, you agree to the Microsoft Platform Policies

3. Click **Register**. Take a note of the Application (client) ID and the Directory (tenant) ID provided by Azure AD.

   Once you've registered the Application, Azure AD provides a set of IDs that you configure in the Conductor when you set up Azure AD as an OIDC provider. Here is how they map to the Edit Authentication Provider options in the Conductor:



Display name
Airwall Conductor

Application (client) ID
0dfa8445-5500-4ee8-9cf2-f89a

Directory (tenant) ID
804056e7-2b90-4371-87 6-8ec

Object ID
d73a32bf-95e5-4a88-aa5c-c32(

Edit Authentication Provider

General settings

Provider name *optional*: Azure AD

Conductor host: https://

In your OpenID Connect provider, set the login redirect URI to 'https://conductorhostname.com/user/auth/openid_connect/callback' and the logout redirect URI to 'https://conductorhostname.com'

OpenID Connect host: https://sts.windows.net

Issuer: https://sts.windows.net/8040

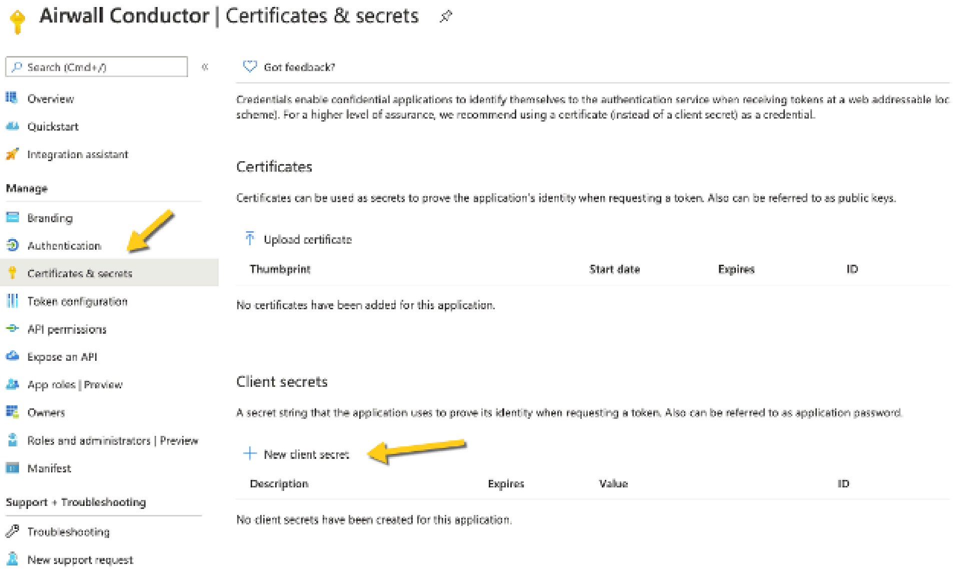
Client ID: 0dfa84

Secret: ••••••••••

□ Use OpenID Connect logout

- Application (client) ID – Enter in the **Client ID** box.
- Directory (tenant) ID – Append this ID to `https://sts.windows.net/`and enter in the **Issuer** box .

4. In Azure AD, create a Client Secret:
   a) Select **Certificates & secrets**.
   b) Select **New client secret**.



Airwall Conductor | Certificates & secrets

Search (Cmd+/)

Overview
Quickstart
Integration assistant

Manage
Branding
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles | Preview
Owners
Roles and administrators | Preview
Manifest

Support + Troubleshooting
Troubleshooting
New support request

Got feedback?

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable loc scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Start date	Expires	ID

No certificates have been added for this application.

Client secrets

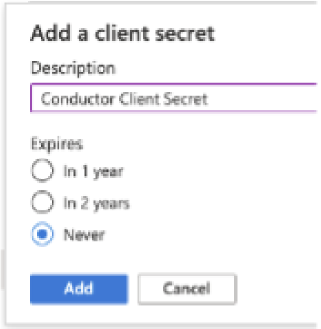
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	ID

No client secrets have been created for this application.

   c) Add a description, and select when the secret expires.



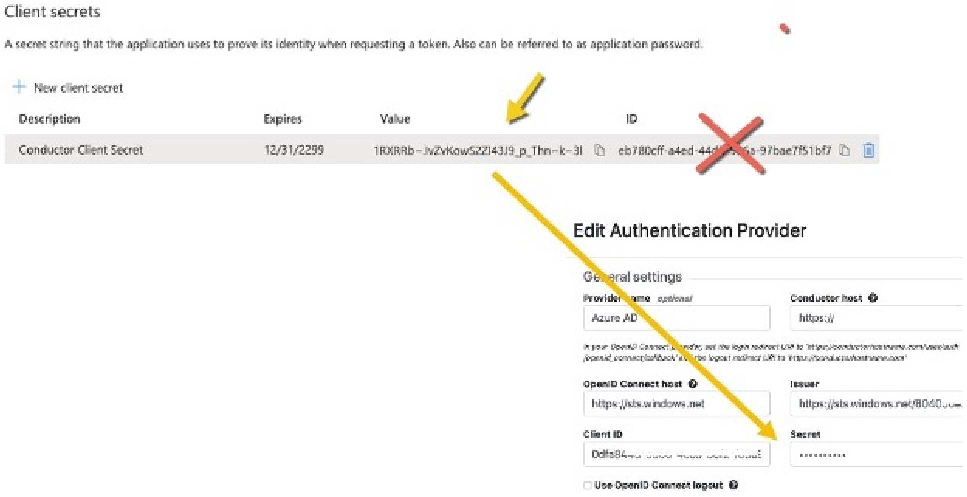
Add a client secret

Description: Conductor Client Secret

Expires
○ In 1 year
○ In 2 years
● Never

   d) Select **Add**.

5. On the **Client secrets** page, copy the **Value** (not the ID). Enter the Value as the secret in the Conductor.



Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	ID
Conductor Client Secret	12/31/2299	1RXRRb~JvZvKowS2Zl43J9_p_Thn-k-3l	eb780cff-a4ed-44d[illegible]a-97bae7f51bf7

Edit Authentication Provider

General settings

Provider name *optional*: Azure AD

Conductor host: https://

In your OpenID Connect provider, set the login redirect URI to 'https://conductorhostname.com/user/auth/openid_connect/callback' and the logout redirect URI to 'https://conductorhostname.com'

OpenID Connect host: https://sts.windows.net

Issuer: https://sts.windows.net/8040...

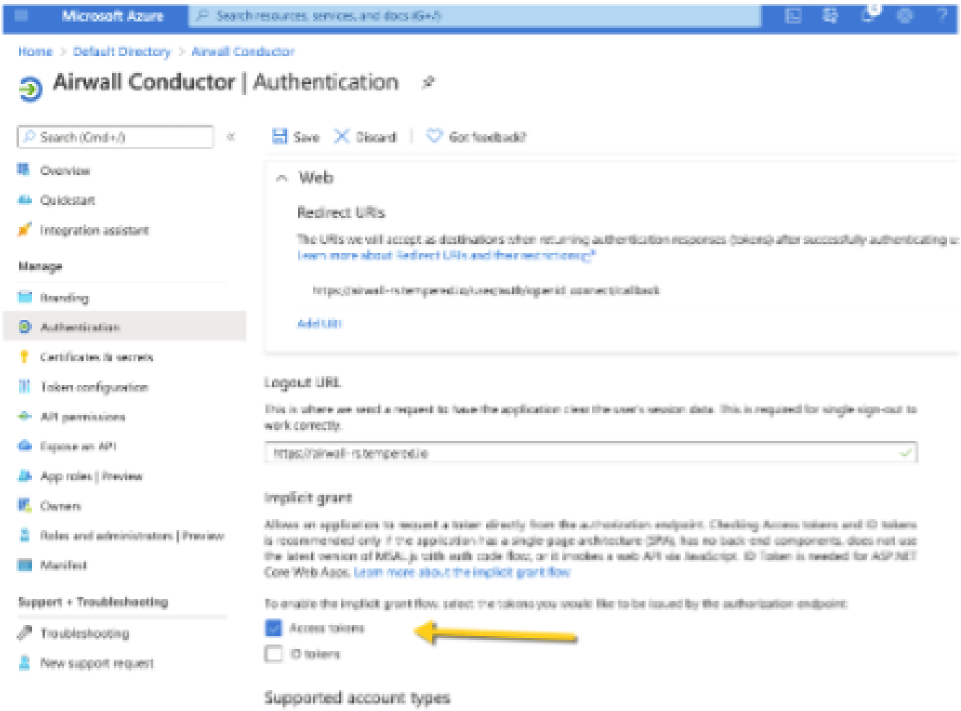
Client ID: 0dfa84...

Secret: ••••••••••

□ Use OpenID Connect logout

6. From the newly registered application in Azure AD, select **Authentication**.

7. Under **Implicit grant**, verify that **ID tokens** is checked.



The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating u

https://airwall-rs.tempered.io/users/auth/openid_connect/callback

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

https://airwall-rs.tempered.io

Allows an application to request a token directly from the authorization endpoint. Checking Access tokens and ID tokens is recommended only if the application has a single page architecture (SPA), has no back-end components, does not use the latest version of MSAL.js with auth code flow, or it invokes a web API via JavaScript. ID Token is needed for ASP.NET Core Web Apps. Learn more about the implicit grant flow

To enable the implicit grant flow, select the tokens you would like to be issued by the authorization endpoint:

☑ Access tokens

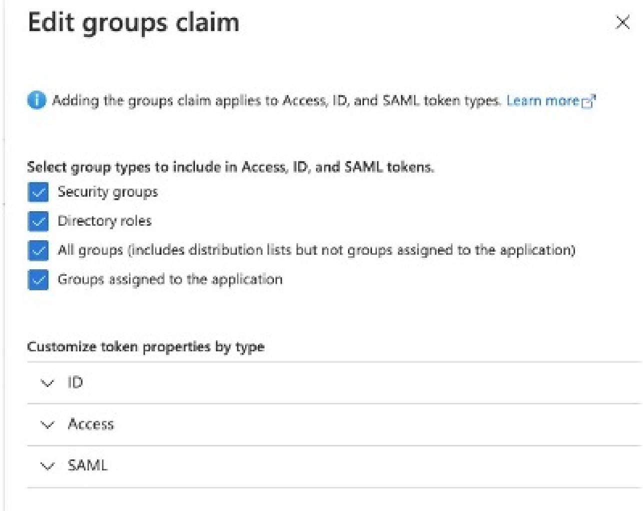
☐ ID tokens

8. In the Azure AD application, set up the groups claim:

a) From the menu on the left, select **Token configuration**.

b) Select Add groups claim.

c) Check all of the group types:



Adding the groups claim applies to Access, ID, and SAML token types. Learn more

Select group types to include in Access, ID, and SAML tokens.

☑ Security groups

☑ Directory roles

☑ All groups (includes distribution lists but not groups assigned to the application)

☑ Groups assigned to the application

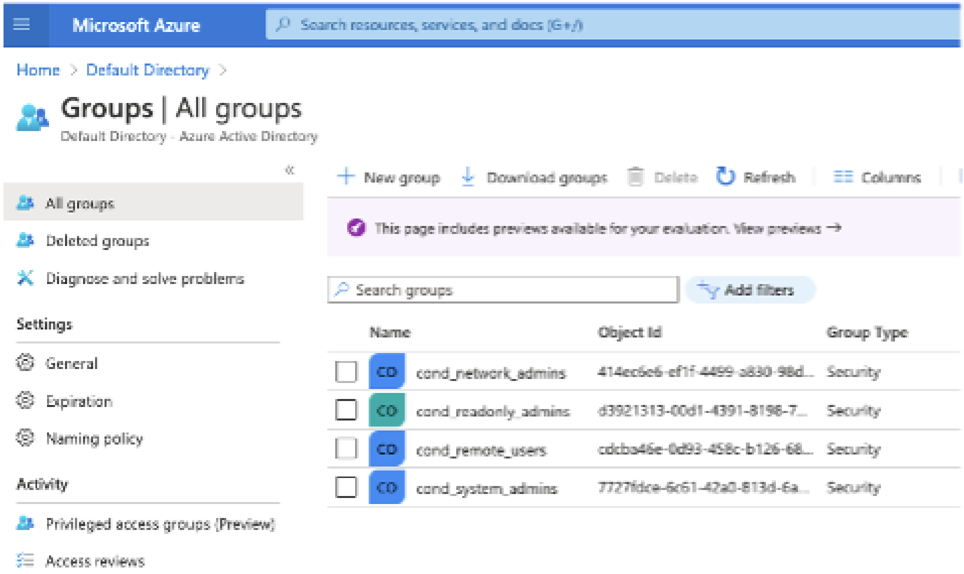
Customize token properties by type

d) Under Customize token properties by type, expand and configure the properties as follows:

- **ID** – Select **sAMAccountName**.
- **Access** – Select **sAMAccountName**.
- **SAML** – This is not used.

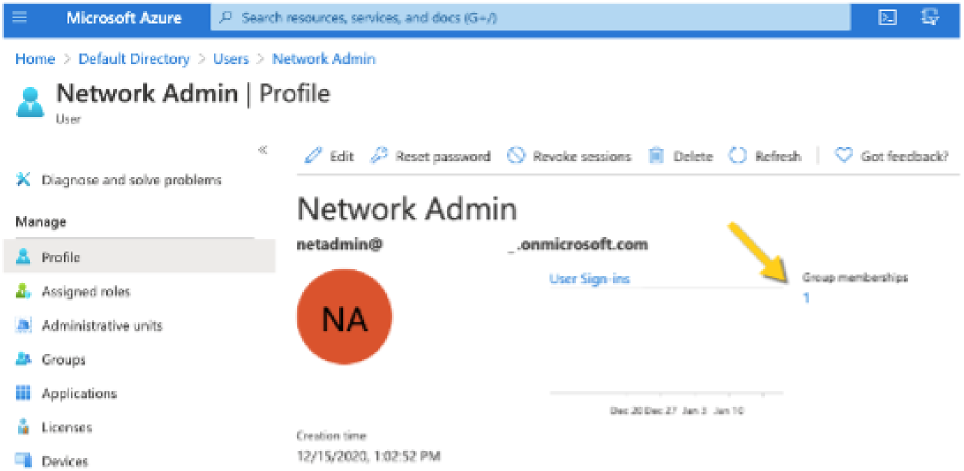
9. In Azure AD, create the groups you want to use for the Conductor. Here are some suggested groups:

- cond_network_admins
- cond_readonly_admins
- cond_remote_users
- cond_system_admins


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Default Directory >
Groups | All groups
Default Directory - Azure Active Directory
All groups
Deleted groups
Diagnose and solve problems
Settings
General
Expiration
Naming policy
Activity
Privileged access groups (Preview)
Access reviews
New group
Download groups
Delete
Refresh
Columns
This page includes previews available for your evaluation. View previews →
Search groups
Add filters

	Name	Object Id	Group Type
□	CO cond_network_admins	414ec6e6-ef1f-4499-a830-98d...	Security
□	CO cond_readonly_admins	d3921313-00d1-4391-8198-7...	Security
□	CO cond_remote_users	cdcba46e-0d93-458c-b126-68...	Security
□	CO cond_system_admins	7727fdce-6c61-42a0-813d-6a...	Security

10. Add users to Azure AD, and assign them to the appropriate groups for Conductor access:



Network Admin

netadmin@ .onmicrosoft.com

Creation time
12/15/2020, 1:02:52 PM

You are now ready to configure Azure AD as an OIDC provider in the Conductor as described in 2. Configure OIDC on the Airwall Conductor on page 248. For the mappings from Azure AD to the Conductor, see steps 3 to 7 above.

Verify third-party authentication is working

To verify your configuration:

1. Log out of the Conductor.
2. Open an incognito window and log in, choosing the provider name you chose in the Conductor.
3. Log in as a user you've set up with third-party provider. You should be able to log in to the Conductor using your third-party provider credentials.

To verify a client can connect:

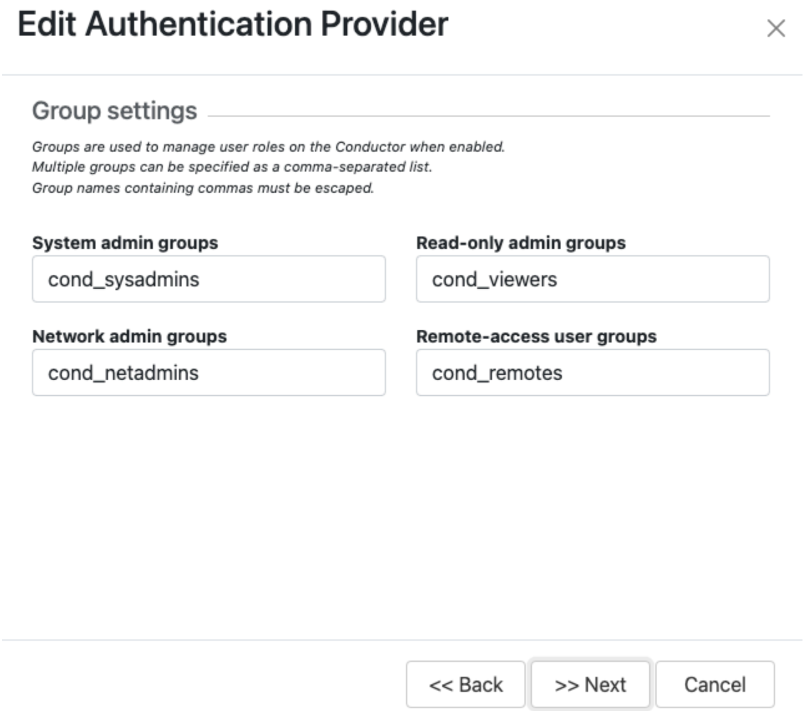
- After the client logs in using the third-party provider, ping the client.

Troubleshooting Third-party Authentication User Login

If user login is failing with "Could not find that username/password combination," usually the integration between the Conductor and OpenID Connect (OIDC) provider is working, but something about group membership is not correctly configured. Use these suggestions to troubleshoot what the issue is.

Check Conductor and OIDC provider group settings

1. On the Conductor, go to **Settings** > **General settings** > **Authentication** > **Your OIDC provider**.
2. Select **Actions** > **Edit**.
3. Select **Next**, and confirm that **Group settings** on the second page are filled out.



Edit Authentication Provider

Group settings

Groups are used to manage user roles on the Conductor when enabled.
Multiple groups can be specified as a comma-separated list.
Group names containing commas must be escaped.

System admin groups: cond_sysadmins

Read-only admin groups: cond_viewers

Network admin groups: cond_netadmins

Remote-access user groups: cond_remotes

4. In your OIDC provider, confirm that the groups you have chosen for each role have been created.
5. Confirm that the user that is trying to log in is a member of one of the groups that will give them a role on the Conductor. For example, if this user should be a Read-only admin then they should be in the "cond_viewers" group in the OIDC provider.

Follow the Log

If you've confirmed steps 1-3 are configured and are still having issues, follow the log to gain more information.

1. Under **Settings** > **General Settings** > **Other settings** > **Logging settings**, if you are logging at warn or error levels, change logging to at least info.
2. Go to **Settings** > **Airshell** > **Open remote Airshell**.
3. Enter the command: `log follow`. You should now see Conductor logs in the virtual terminal.
4. Have the user attempt to log in again with OIDC. If this is you, do not log out of the Airshell terminal – use a private browser window.
5. When the user completes login, there should be a log message for the user attempting to login such as

```
1Mar 11 20:57:34 kibbles SCMP[30051]: OpenID user
'google-oauth2|115620360600894761234' allowed groups: ["cond_netadmins"]
```

6. If the allowed groups is empty, the optional "groups" claim may not be correctly configured on the OIDC provider. Please refer to the specific documentation for your OIDC provider to allow the Conductor to receive the "groups" claim.
7. If there are allowed groups but none apply to a Conductor role are there three possible problems:
   a) The user is not a member of the group you expected
   b) The groups are being filtered by the OIDC provider. Please check your OIDC provider configuration.

c) The groups are being filtered by the Conductor configuration. Check the configuration for your OIDC provider. The Conductor does attempt to prevent you from creating a filter that would invalidate groups assigned for roles.

Configure LDAP authentication on Conductor and Airwall Edge Services

You can use Active Directory and LDAP authentication with the Conductor to streamline user account management. When LDAP is configured, users can choose to log in with an LDAP account on the Conductor login page.

There are currently three different ways to authenticate with Conductor.

- With a Conductor account. These are local accounts that log directly into the device
- With LDAP authentication. This allows you to authenticate with any LDAP server, including Microsoft Active Directory services.
- With a third-party authentication provider that supports OpenID Connect. See Integrate Third-party Authentication with OpenID Connect on page 247.

To set up a LDAP authentication, you need to already have an LDAP server accessible to the Conductor.

Note: These instructions use Microsoft Active Directory, but other LDAP services also work.

There are four different roles in the Conductor:

- **System Administrator** – These users have full access to the Conductor and can adjust any settings. Note that to edit LDAP settings, you must be logged in locally to the Conductor, not through LDAP.
- **Read-only System Administrator** – These users have read access to the Conductor, but cannot make changes.
- **Network Administrator** – These users have access to and can adjust any overlay network they are a manager of. They do not have access to Conductor Settings.
- **Remote Access User** – These users can only see their own information, and can log in with their credentials if authentication is required for their Airwall Agent or Server.

For more detailed role information, see Understand People Roles and Permissions on page 58.

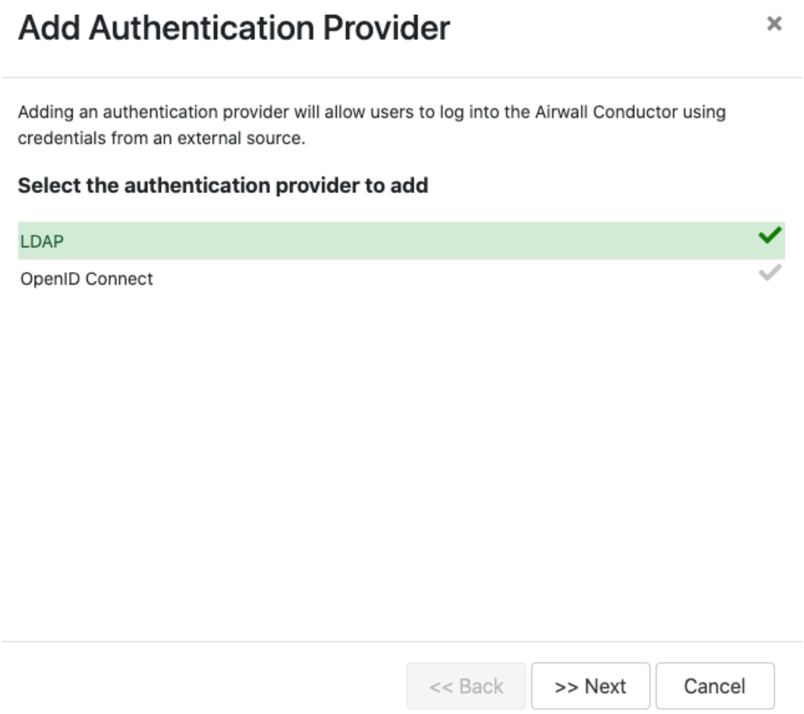
Step 1: Set up and configure your LDAP server

LDAP is not enabled in Active Directory by default, so you will have to turn it on. Once you have LDAP working and running, you can start.

Create a dedicated account with the necessary permissions to authenticate. In Active Directory, you could create a service account under the root "Users" OU, and make it a Domain Admin.

Step 2: Enter and verify your local Conductor admin account credentials, and select Authentication provider

1. Log into Conductor locally (not through LDAP) as a System Administrator. (Only local administrators have access to authentication provider settings.)
2. Open **Settings**, and next to **Authentication**, select **Add Provider**.
3. Select **LDAP** from the list of providers.



Add Authentication Provider

Adding an authentication provider will allow users to log into the Airwall Conductor using credentials from an external source.

Select the authentication provider to add

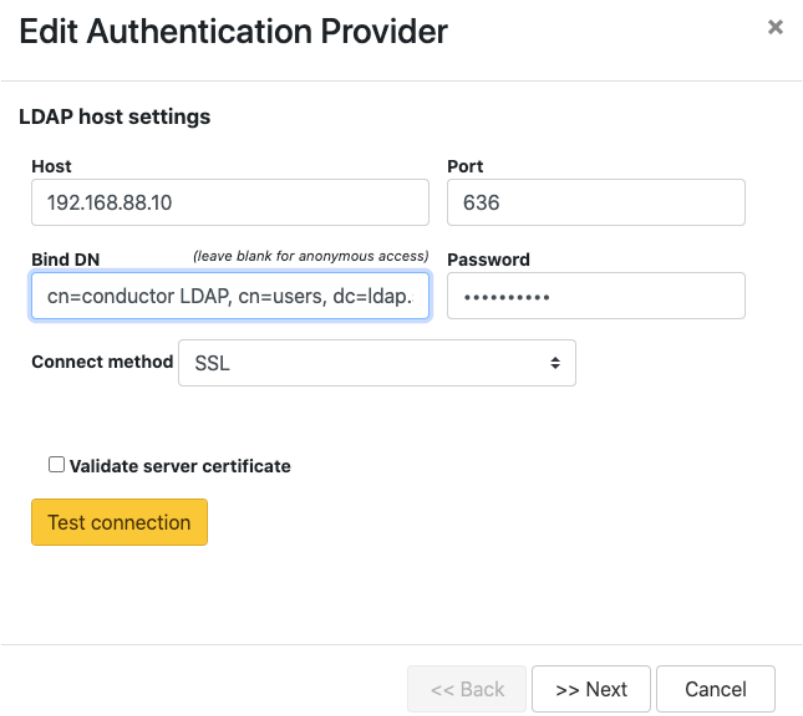
- LDAP ✓
- OpenID Connect

Step 3: Enter your LDAP settings

You will need to know the following values:

- Host (Hostname or IP address)
- Port (636 is the default)
- If you are using a dedicated LDAP service account, the fully-distinguished path for the user account, and the password

Under **LDAP host settings**, enter the information for your LDAP host, and select **Next**. For more details on these settings, see LDAP host settings on page 263.



Edit Authentication Provider

LDAP host settings

Host: 192.168.88.10

Port: 636

Bind DN *(leave blank for anonymous access)*: cn=conductor LDAP, cn=users, dc=ldap.

Password: ••••••••••

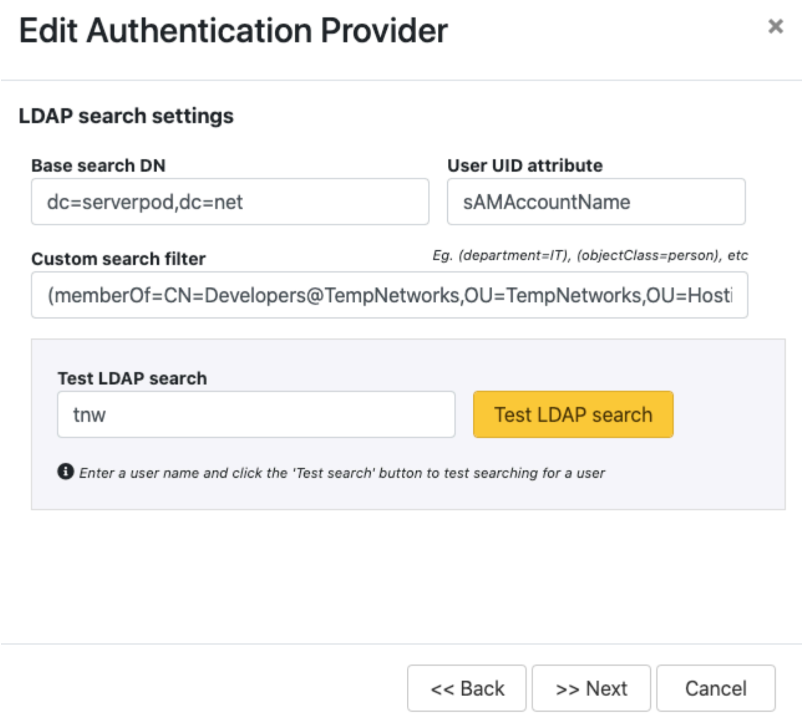
Connect method: SSL

□ Validate server certificate

Note: TLS LDAPS communication occurs over port TCP 636. LDAPS communication to a global catalog server occurs over TCP 3269. When connecting to ports 636 or 3269, SSL/TLS is negotiated before any LDAP traffic is exchanged.

Step 4: Configure Search Settings

This page can mostly be left as-is, unless you have special settings you wish to set. You can search for user accounts here to ensure that the Conductor can search the directory. Select **Next**. For more details on these settings, see LDAP search settings on page 264.



Edit Authentication Provider

LDAP search settings

Base search DN: dc=serverpod,dc=net

User UID attribute: sAMAccountName

Custom search filter *Eg. (department=IT), (objectClass=person), etc*: (memberOf=CN=Developers@TempNetworks,OU=TempNetworks,OU=Hosti

Test LDAP search: tnw

Enter a user name and click the 'Test search' button to test searching for a user

You can test the search by entering a search term and selecting **Test LDAP search**.

Step 5: Configure Group Settings

The Conductor assigns LDAP users to one of the four account types above by making them a member of a security group.

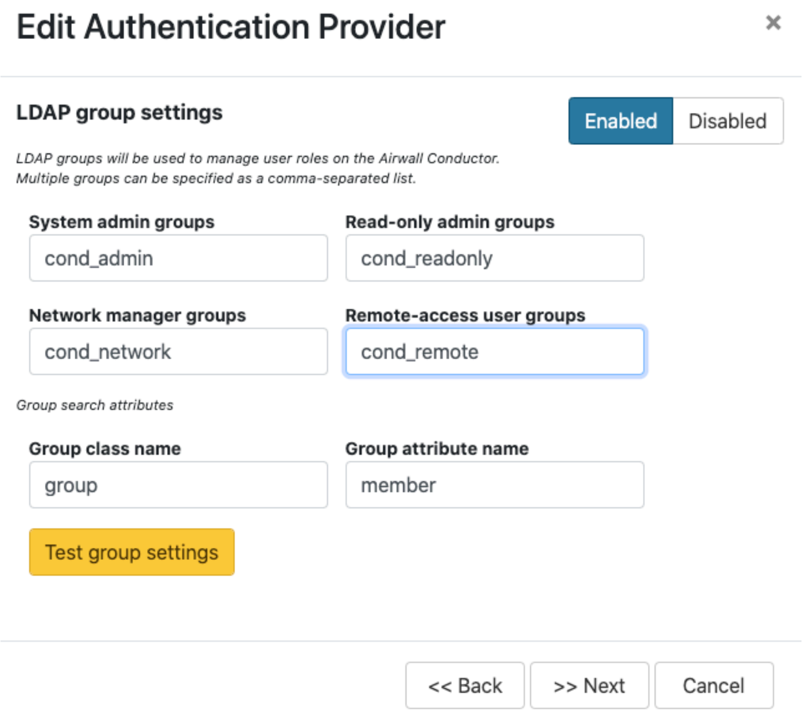
If you do not have appropriate groups already, create these groups in LDAP to link to Conductor roles (you can use different names – using cond_ makes it easier to see which roles are for the Conductor). By default, these groups place the users into the following roles:

- **cond_admin** – System Administrator
- **cond_readonly** – Read-only System Administrator
- **cond_network** – Network Administrator
- **cond_remote** – Remote Access User

Since users cannot have more than one role at a time, if they are members of multiple groups, they'll be assigned the role with the most permissions.

Remember to test the settings to ensure that Conductor can see all of the groups you reference on your LDAP server.

1. For **LDAP group settings**, enter the groups for the roles you want LDAP users to have, and **Group search attributes**, and select **Next**. For more details on these settings, see LDAP group settings on page 264.



Edit Authentication Provider

LDAP group settings

LDAP groups will be used to manage user roles on the Airwall Conductor. Multiple groups can be specified as a comma-separated list.

System admin groups: cond_admin

Read-only admin groups: cond_readonly

Network manager groups: cond_network

Remote-access user groups: cond_remote

Group search attributes

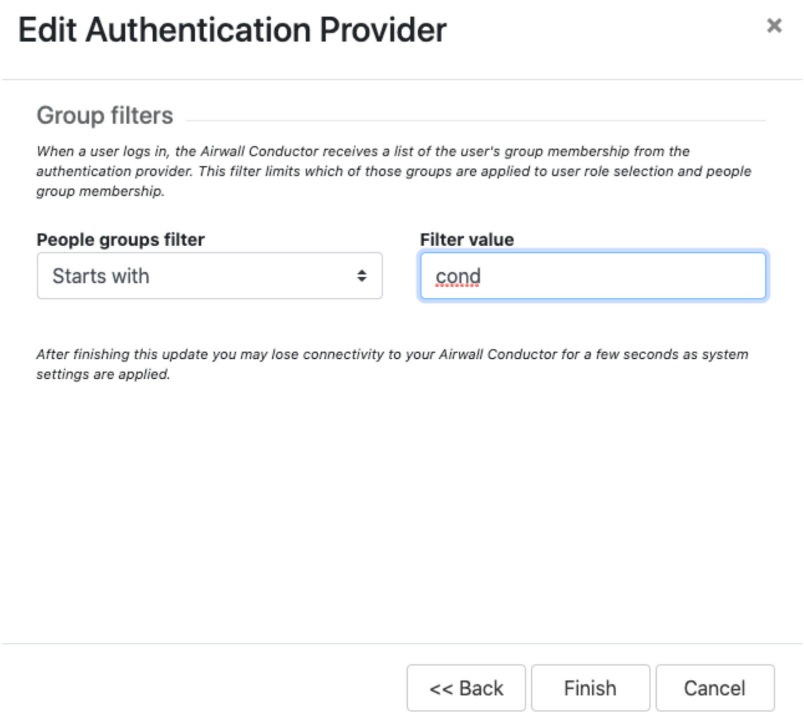
Group class name: group

Group attribute name: member

You can also add other security groups to the configuration, separated by commas.

Note: You can set up these groups on your LDAP server after setting up LDAP on the Conductor, but **Test group settings** will fail.

2. For **Group filters**, enter filters to specify which LDAP groups the Conductor sees. For example, if you've created the cond_ groups above, you may want to set the filter to **Starts with** with a value of `cond`.



Edit Authentication Provider

Group filters

When a user logs in, the Airwall Conductor receives a list of the user's group membership from the authentication provider. This filter limits which of those groups are applied to user role selection and people group membership.

People groups filter: Starts with

Filter value: cond

After finishing this update you may lose connectivity to your Airwall Conductor for a few seconds as system settings are applied.

3. Select **Finish**
   You may lose connection briefly as the new settings are applied.

Step 6: Configure user onboarding

Configure user onboarding for the people groups created above to give users access to overlay networks through Airwall Agents and Servers. Setting the groups up beforehand simplifies user onboarding.

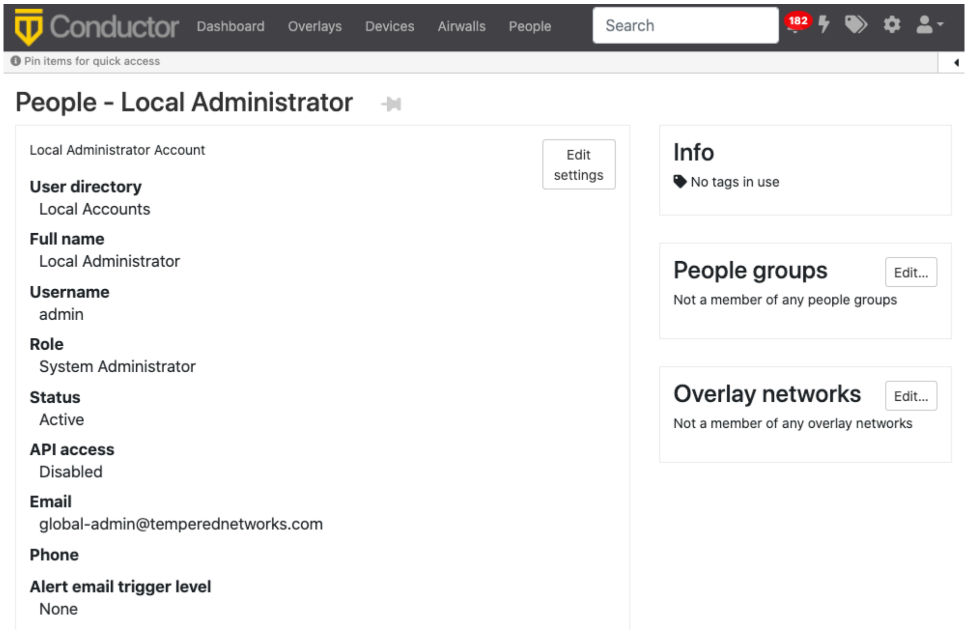
1. In the Conductor, create **People groups** that match the LDAP groups you specified above (for example, cond-admin)
2. Specify user onboarding options as you create the groups. For details, see Set up a People Group on page 89.

As users log in through LDAP, they are added to these **People groups** and given an activation code that activates the permissions and other options you specified for the **People groups**.

Step 7: Set up Conductor management access

You can also set up access for your Conductor system and network admins individually.

1. **Add administrators to Overlays** – Add administrators individually as members of Overlay networks to give them access to the resources they need. You can add them from their **People** page, or from an Overlay page:
   - **From the person's People page**, next to **Overlay networks**, select **Edit**. Add the person as a member or manager of Overlays.



People - Local Administrator

Local Administrator Account

User directory
Local Accounts

Full name
Local Administrator

Username
admin

Role
System Administrator

Status
Active

API access
Disabled

Email
global-admin@temperednetworks.com

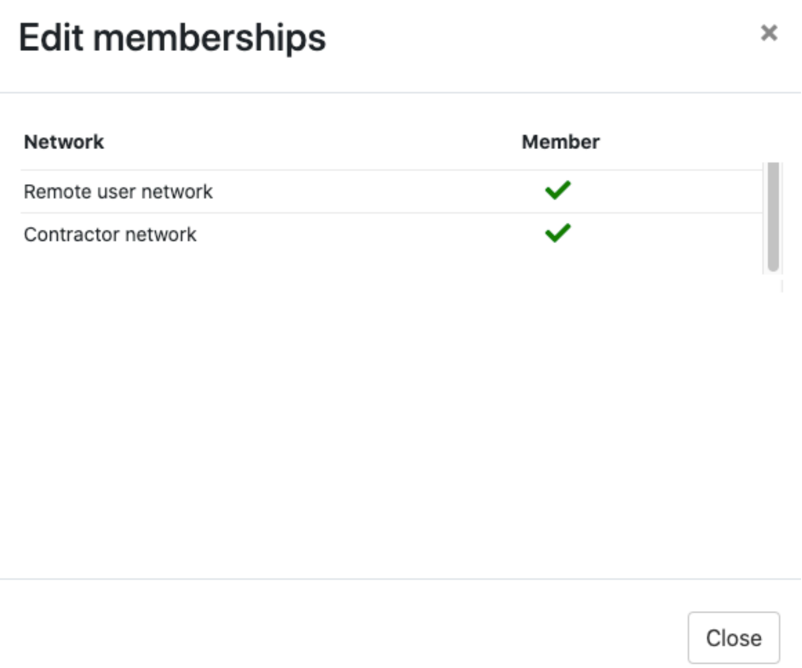
Phone

Alert email trigger level
None

Info
No tags in use

People groups
Not a member of any people groups

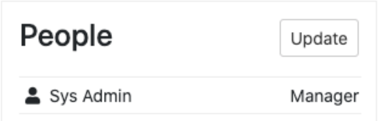
Overlay networks
Not a member of any overlay networks



Edit memberships

Network	Member
Remote user network	✓
Contractor network	✓

- **From the Overlays page**, open the overlay, and under **People**, select **Update**. Add the administrators as members or managers of the overlay.



People

Sys Admin	Manager

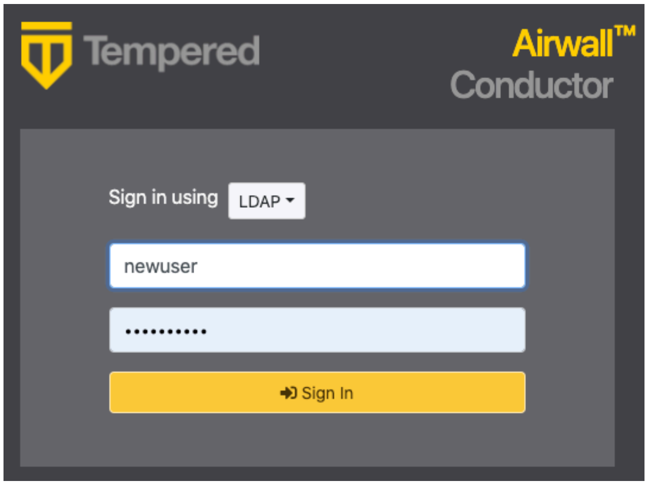
2. **Add administrators to People groups** – Similarly, you can add administrators to **People groups**, from their People page or add several administrators from the People group:

   - **From a person's People page** – Next to **People groups**, select **Edit** and select the **People groups** with the permissions they need.
   - **From a People group** – Open the **People group**, and on the **People** tab, select the people to add.

Step 8: Verify by logging in to the Conductor

Verify that LDAP is set up by logging in and checking permissions.

1. Log out from your local administrator account.
2. Next to **Sign in using**, select **LDAP**, and log into the Conductor with an LDAP account.



3. Check that permissions are set correctly for that user.

See also: Configure user authentication for Airwall Agents and Airwall Servers on page 243.

Mirror traffic from your Airwall Gateways to a packet analyzer tool

You can mirror traffic from your Airwall Gateways to allow common packet analyzer/visibility tools (like Nozomi or Wireshark) to see what's going on in your Airwall secure network.

Caution: Packet analysis is a notoriously risky activity for security. Parsing unknown, uncontrolled inputs for a wide range of protocols is error prone. When employing a packet analysis tools, it's best practice to segment off the packet processing into an isolated security sandbox.

Supported Versions	Conductor and Airwall Gateways v2.2.11 and later
Required Role	• System or network administrators • Permissions to edit the Airwall Gateways used as the Mirror Destination and Sources. You need to be a manager of at least one overlay that these Airwall Gateways are in.
Supported on these Airwall Edge Services	Airwall Gateways: 2.2.11 hardware and virtual gateways: • **For Mirror Destination**: *Production environments*: Recommend Airwall Gateway 300v or 500 only. *Testing*: Airwall Gateway 75, 150, or 250. • **For Mirror Source:** Any Airwall Gateway.

Bulk editing does not support this configuration.

Before you begin

⚠ **CAUTION:**

To allow a packet analyzer to view traffic on an Airwall secure network, port mirroring requires copying potentially-sensitive traffic and delivering a copy of it where your packet analyzer can access it. This additional copy can introduce a security risk and impact the performance of your network:

- **Security risk and impact** – A security risk is introduced in handling the copy of sensitive traffic that must also be secured.
- **Performance impact** – Mirroring traffic to a remote Airwall Gateway may incur up to a 3-5x performance penalty due to the overhead of processing additional copies of the traffic and fragmenting large packets. The more traffic you mirror, the higher the impact. See Adjust performance for mirrored traffic on page 462 for suggestions on mitigating the performance impact.

Requirements

To set up port mirroring, you need:

- A Packet Analysis Tool (such as Nozomi or Wireshark)
- The permissions listed under **Required Role** above.
- An Airwall Gateway to use as the Mirror Destination (see **Supported on these Airwall Gateways** for recommended models)
- One or more Airwall Gateways that you want to mirror the traffic on (to use as Mirror sources)

Note: If you are using GRE or ERSPAN source to packet analyzer, you can use an existing overlay port group. If you're using a Mirror Destination port group, the Mirror Destination Airwall Gateway needs a free port.

How does it work?

The following diagram shows how to set up port mirroring to avoid leaking sensitive network information.

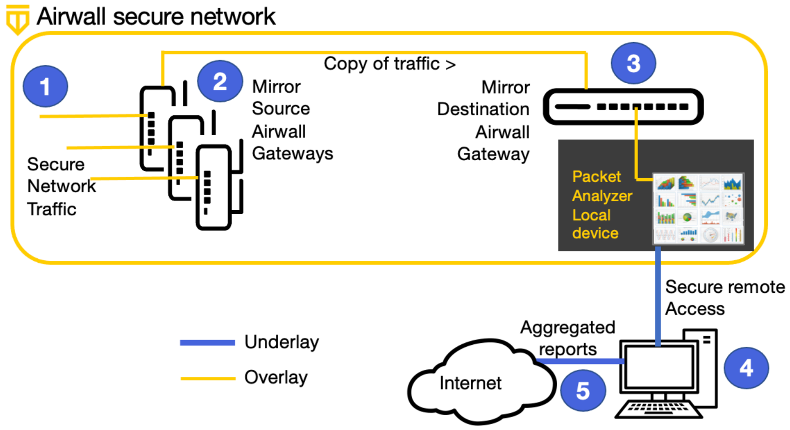


Diagram Flow:

1. Secure network traffic to and from the Mirror Source Airwall Gateways is collected.
2. Mirror Source Airwall Gateways send a copy of traffic data to the Mirror Destination Airwall Gateway.
3. Mirror Destination Airwall Gateway sends the data to the Local device for the Packet Analyzer.
4. Admin securely logs in to packet analyzer to access and analyze data and export reports.
5. Admin releases reports that aggregate the data.

For more ways to configure mirrored traffic, see More Mirrored Traffic Scenarios on page 466.

Choose how to mirror traffic

There are two ways you can set up the Mirror Destination Airwall Gateway, depending on how you are connecting your packet analyzer to it:

- **Local Device Destination** – The recommended way to mirror traffic is to send the traffic to a local device for your packet analyzer. See Mirror Traffic to a Local Device destination (Recommended Way). This method uses GRE or ERSPAN to send traffic to a local device for the packet analyzer on the Mirror Destination Airwall Gateway.
- **Mirror Destination Group** – You can also send mirrored traffic to a dedicated port group attached to a physical cable. See Mirror traffic to a dedicated port on page 467. This method uses a special type of port group (Mirror Destination group).

  If you are using a Mirror Destination group, you can't use a physical or virtual switch without special configuration. This particularly impacts the Airwall Gateway 300v, since the hypervisor uses a virtual switch. You must either use a physical cable to directly connect the Airwall Gateway to the packet analyzer, or consult your switch vendor's documentation on how to configure it to carry mirrored traffic.

Mirror Traffic to a Local Device destination (Recommended Way)

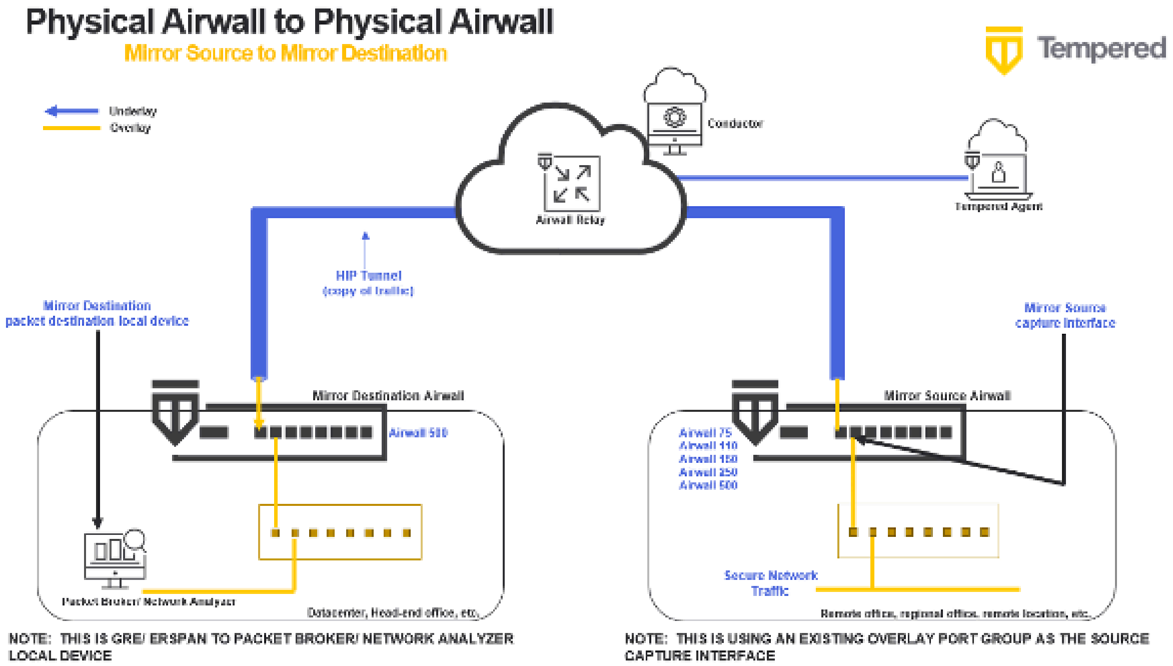
The recommended way to mirror traffic is to send the traffic to a local device for your packet analyzer.

To mirror traffic to a local device, you need to:

1. Create a local device for your packet analyzer tool.
2. Configure a Mirror Destination to send to a Local Device.
3. Configure Airwall Gateways to act as Mirror Sources.
4. Adjust performance for mirrored traffic.
5. Set up security for mirrored traffic.
6. Configure your packet analyzer tool.

These steps are described in more detail in the following sections.

Here is a diagram showing this scenario:


Physical Airwall to Physical Airwall
Mirror Source to Mirror Destination
Tempered
Underlay
Overlay
Conductor
Airwall Relay
Tempered Agent
HIP Tunnel
(copy of traffic)
Mirror Destination
packet destination local device
Mirror Source
capture interface
Mirror Destination Airwall
Airwall 500
Mirror Source Airwall
Airwall 75
Airwall 110
Airwall 150
Airwall 250
Airwall 500
Packet Broker/ Network Analyzer
Datacenter, Head-end office, etc.
Secure Network
Traffic
Remote office, regional office, remote location, etc.
NOTE: THIS IS GRE/ ERSPAN TO PACKET BROKER/ NETWORK ANALYZER LOCAL DEVICE
NOTE: THIS IS USING AN EXISTING OVERLAY PORT GROUP AS THE SOURCE CAPTURE INTERFACE

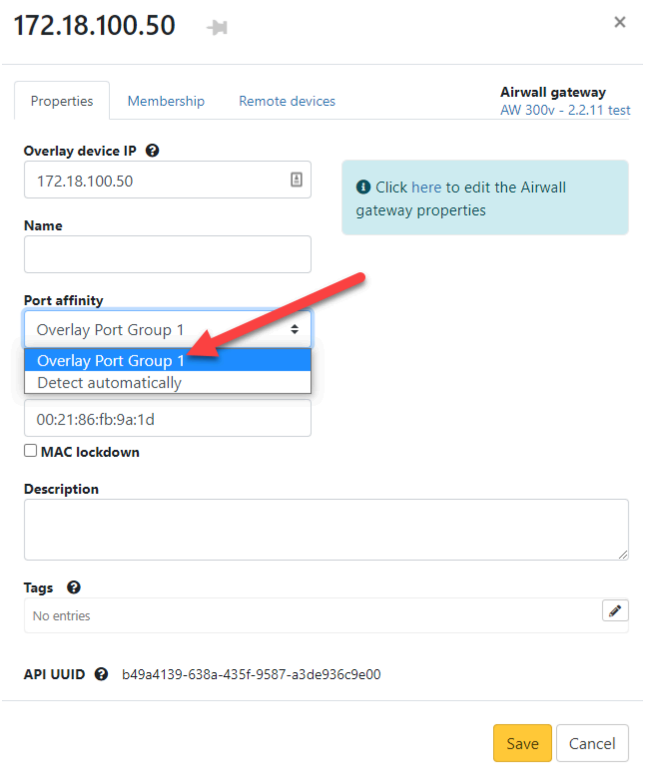
Create a local device for your packet analyzer tool

Create a local device on a dedicated overlay port group for your packet analyzer tool (protocol analyzer, packet broker, or other tool that consumes network traffic information).

The destination for your mirrored traffic can be your packet analyzer set up as a local device on your Mirror Destination Airwall Gateway.

1. Add the packet analyzer tool as a local device to the Airwall Gateway that you're going to use as your Mirror Destination (the one that receives the mirrored traffic and sends it to the destination, which is your analyzer).

2. When you're adding the device (either manually or through auto-discovery), you must set Port affinity (it cannot be left on auto).



172.18.100.50

Properties | Membership | Remote devices

Airwall gateway
AW 300v - 2.2.11 test

Overlay device IP: 172.18.100.50

Click here to edit the Airwall gateway properties

Name:

Port affinity: Overlay Port Group 1

Overlay Port Group 1
Detect automatically

00:21:86:fb:9a:1d

□ MAC lockdown

Description:

Tags: No entries

API UUID: b49a4139-638a-435f-9587-a3de936c9e00

For more information, see Add devices to the Conductor on page 414.

If you are using this method to connect your packet analyzer tool, you need to configure your mirror destination as described on this page: Configure a Mirror Destination to send to a Local Device on page 460

Configure a Mirror Destination to send to a Local Device

The Mirror Destination Airwall Gateway receives the mirrored traffic and sends it to your packet analyzer (or network analyzer or packet broker).

If your packet analyzer supports receiving packets encapsulated in GRE or ERSPAN, this is the preferred configuration. It avoids the possibly of mirrored traffic being recirculated on your network and the MAC address table issues with switches. It also provides additional fields to your packet analyzer that allow it to distinguish between traffic captured by multiple Airwall Gateways (using GRE key/ERSPAN session ID) and detect lost or reordered packets (using ERSPAN sequence number).

1. On the Airwall Gateway page, go to **Ports** > **Port mirroring**.
2. Select **Edit Settings**.
3. Next to **Configurations**, select the + to add a mirroring configuration.
4. In your new configuration:
   a) Set the **Enabled** toggle to On.

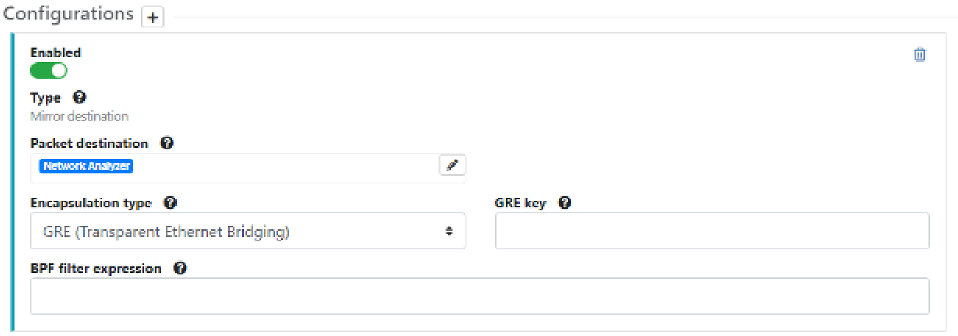
      Note: After configuration, use this toggle to turn mirroring on and off.

   b) Under **Type**, select `Mirror Destination`.

   c) Under **Packet destination**, select the local device for your packet analyzer you set up earlier.

      Note: The device will not show up as destination when you're selecting the Mirror Destination Airwall Gateway unless you've set a specific port group affinity (not `Auto`). See Create a local device for your packet analyzer tool on page 459.

d) Under **Encapsulation type**, select the encapsulation (`GRE` or `ERSPAN Type I, II, or III`) supported by your packet analyzer. For example, for Nozomi, pick ERSPAN type II. Refer to documentation of your packet analyzer to determine which encapsulations it supports.



Configurations +

Enabled

Type

Mirror destination

Packet destination

Network Analyzer

Encapsulation type

GRE (Transparent Ethernet Bridging)

GRE key

BPF filter expression

e) ***Optional*** – Enter any information allowed for the type you selected (for example, GRE key or session ID).

f) ***Optional*** – Under BPF filter, add any BPF filters you would like to use to filter the traffic that is mirrored to this Mirror Destination. See BPF Settings for Port Mirroring on page 464.

> **Note:** If you use a BPF expression on the Mirror Destination, that's the default for all of the Mirror Sources, unless you set a BPF expression on the source, which overrides this default.

5. Select **Update Settings**.

You should be able to see some traffic from the Mirror Destination to the packet analyzer local device.

Configure Airwall Gateways to act as the Mirror Sources

You configure Mirror Source Airwall Gateways to send network information to the Mirror Destination Airwall Gateway.

> **CAUTION:** If you capture traffic on all ports of the overlay port group, you may set up a loop. To avoid this, in your configuration set a BPF filter of "ip proto not 47" to exclude mirrored traffic. See BPF Settings for Port Mirroring on page 464.

If you use GRE Transparent Ethernet Bridging, ERSPAN type II or ERSPAN type III – You can use GRE key or Session ID to identify which source the packets arrived on.

> **Note:** You can set up the Mirror Destination to also be a Mirror Source, to include that Airwall Gateway's traffic in the information sent to the packet analyzer. In this case, be sure to set a BPF filter to exclude the mirrored traffic.

1. On a Mirror Source Airwall Gateway, go to **Ports** > **Port mirroring**.

2. Select **Edit Settings**.

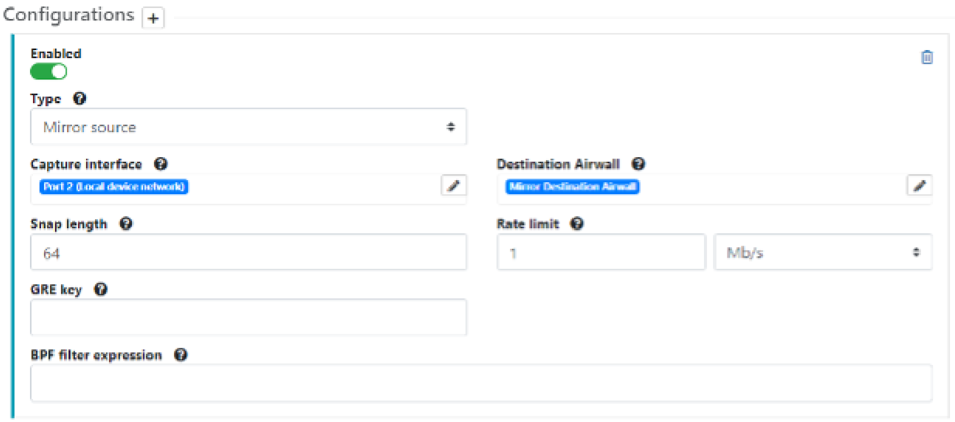
3. Next to **Configurations**, select the + to add a mirroring configuration.

4. In your new configuration:

a) Under **Type**, select `Mirror Source`.

b) Under **Destination Airwall**, select the Airwall Gateway you set up as the Mirror Destination.

c) Under **Capture interface**, select the interface you want to capture network information from. Ports in overlay port groups and the overlay hipbr bridge interfaces are supported.



Configurations +

Enabled

Type: Mirror source

Capture interface: Port 2 (Local device network)

Destination Airwall: Mirror Destination Airwall

Snap length: 64

Rate limit: 1 Mb/s

GRE key:

BPF filter expression:

d) ***Optional*** – If using a local device as the Mirror Destination, you can enter a GRE or session ID to distinguish the traffic being sent from this Mirror Source by including this value in the GRE/ERSPAN header of packets sent to a local device sync.

e) ***Recommended*** – Set performance settings for suggestions on setting Snap length, Rate limit, and source-specific BPF filters that override the Mirror Destination BPF filters (Example (BPF filter of "ip proto not 47" to exclude mirrored traffic and avoid loops). See Adjust performance for mirrored traffic on page 462 for guidance, or for more information on BPF filters, see BPF Settings for Port Mirroring on page 464.

5. Select **Update Settings**.

Note: You can set up different configurations for a Mirror Source Airwall Gateway to send traffic to different Mirror Destinations.

Adjust performance for mirrored traffic

Because mirroring traffic can impact your network performance, it is best practice to set one or all of the following performance adjustments on the Mirror Destination and Source Airwall Gateways to mitigate the performance impact.

Here are the performance adjustments you can make:

Snap length

Specify that when mirroring traffic, a Mirror Source Airwall Gateway should only copy this many bytes of the original packet. You can use this setting to get "headers only" with a small value (~64 bytes), and/or avoid fragmentation with a larger value (~1000 bytes). Specifying a full Ethernet frame size of 1514 bytes will avoid truncating packets (if you are using 802.1q VLAN tags or jumbo frames you will need to increase this value), but results in fragmenting every full-size mirrored packet, doubling the number of packets which must be processed.

Rate limits

Set a rate limit for mirrored traffic. This limit is only applied to the mirrored copy of the traffic. It is a best practice to configure a rate limit to limit the performance impact of using mirroring so you do not negatively impact other traffic secured by the Airwall Gateway. This limit also protects against misconfigurations where the mirrored traffic itself is mirrored, resulting in infinitely mirroring the same packet.

As a starting point, here are some recommended values to not significantly impact existing traffic, based on the relative performance for specific Airwall Gateway models:

Airwall Gateway model	Suggested Rate Limit
100	1 Mb/s
110	3 Mb/s
75	5 Mb/s
150	10 Mb/s
250	15 Mb/s

300v	20-100Mb/s
500	100 Mb/s

Note: You may want to set these limits lower, depending on your network bandwidth, particularly if your network connection is metered, as with a cellular provider.

When setting rate limits, also consider the performance of the Mirror Destination Airwall Gateway, the packet analyzer, and network connection between these Airwall Gateways.

BPF Filters

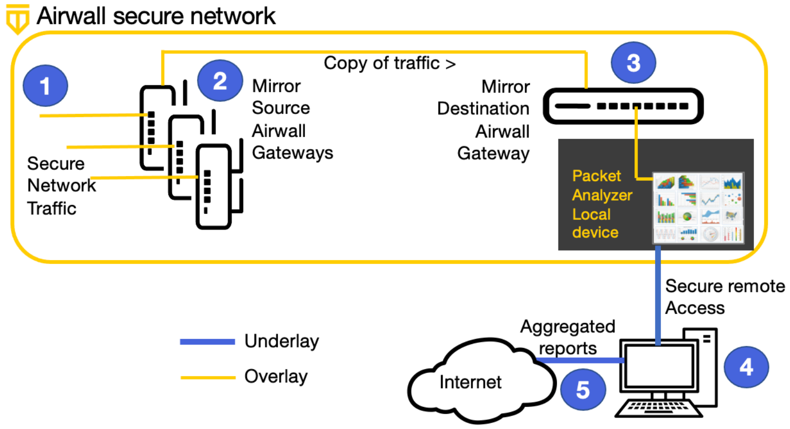
You can select which traffic is mirrored by specifying a BPF filter. If no filter is specified, all traffic is mirrored. By default, Mirror Source Airwall Gateways use the BPF filters specified on the Mirror Destination Airwall Gateway. You can override this default by setting different filters on any of the Mirror Source Airwall Gateways. BPF filters will filter mirrored traffic to specific protocols using BPF filter expressions. For information on the BPF filters most helpful for port mirroring, see BPF Settings for Port Mirroring on page 464.

Set up security for mirrored traffic

Protect your mirrored traffic.

Because your packet analyzer can be a back door to sensitive information about your network (impacting your Airwall secure network invisibility), you need to set up security policies to limit access to your packet analyzer and mirrored traffic so that only trusted devices can access it.

CAUTION: It is a best practice to keep all of the information being sent to your packet analyzer within the Airwall secure network. Since you are essentially making a copy of potentially-sensitive overlay traffic and decrypting it for the packet analyzer, there is a risk of exposure if your packet analyzer is compromised, not secured, or if the network information you are capturing is sent over an unsecured network. You can secure the packet analyzer management interface within the Airwall secure network, with access to the interface limited to authorized personnel.



Configure your packet analyzer tool

Make sure your packet analyzer tool is set up to receive the mirrored network traffic data.

You should now be getting traffic to your packet analyzer tool (protocol analyzer, packet broker, or other tool that consumes network traffic information) and can configure your packet analyzer software to consume the data being received from the Mirror Destination Airwall Gateway. For assistance, see the documentation for your packet analyzer software.

Verify Port Mirroring

To verify that port mirroring is working, check that data is flowing to your packet analyzer.

You can also:

- Check the Diagnostics reports on the Mirror Source and Destination Airwall Gateways and look for `aircap` processes. Aircap is the process that implements port mirroring.
- Check that there is a tunnel established from the Mirror Source Airwall Gateways to the Mirror Destination Airwall Gateway.
- You can check that there is traffic flowing from the Mirror Destination Airwall Gateway to the packet analyzer local device or Mirror Destination group.

BPF Settings for Port Mirroring

Specifying BPF filters for port mirroring will filter the traffic that is mirrored to your Mirror Destination Airwall Gateway. If you do not specify any filters, it will mirror all traffic.

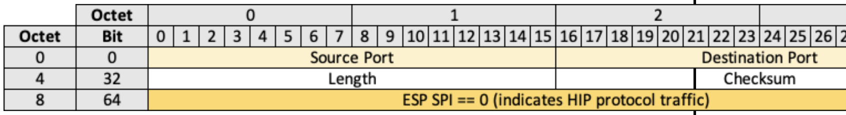
Here are some sample BPF filters:

Filter Mirrored Traffic to Include/ Exclude	BPF Filter Format	Description and Examples

Traffic using a specific IP protocol	ip proto <protocol_to_include>
	ip proto not <protocol_to_exclude>
		Mirror only traffic using IP protocol of IPv6. Examples:
		Only include IPv6 traffic:
		`ip proto 41`
		do not include IPv4 traffic:
		`ip proto not 4`

All traffic on the specified host	host <host_ip>	`host 192.0.2.10`
All traffic where the specified host is the source	src host <host_ip>	`src host 192.0.2.10`
Exclude IP traffic	no ip	`no ip`
All traffic on the specified port	port <port_#>	`port 443`
All traffic on the ports in the specified range	portrange <port1_#>-<port2_#>	`portrange port 443-450`

Filter Mirrored Traffic to Include/ Exclude	BPF Filter Format	Description and Examples

Specific data		You can combine conditions to narrowly match specific protocols like:
		`udp port 10500 and udp[8:4] == 0`
		This filter matches UDP traffic with a source or destination port of 10500 and the first 32 bits of the UDP payload is zero. This matches HIP (control) protocol traffic excluding tunneled overlay traffic.
		
		Match HTTP packets where the payload starts with GET:
		`tcp port 80 and tcp[20:4] == 1195725856`
		1195725856 is GET represented as a 32-bit network byte order integer.

Specific devices and protocols		Mirror traffic for devices on specific hosts and ports:
		`ip host 192.0.2.10 and (tcp port 80 or tcp port 443)`
		`ip host 192.0.2.11 and udp port 53`

Exclude high bandwidth service or known traffic	not (ip net <high_bandwidth_IP address> and tcp port <port_number>	Exclude all HTTPS traffic to/from 192.0.2.0/24: `not (ip net 192.0.2.0/24 and tcp port 443)` **Note:** This filter can also work well with rate limiting. By excluding the known traffic (legitimate), you can mirror all of the other traffic and capture a greater portion of the anomalies with a small throughput and processing overhead.

	Octet	0								1								2										
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
0	0	Source Port																Destination Port										
4	32	Length																					Checksum					
8	64	ESP SPI == 0 (indicates HIP protocol traffic)																										

Port Mirroring BPF Reference

To create your own variations, here are the most useful BPF filter choices:

What to Filter

- IP host / network
- IPv6 host / network
- TCP / UDP port

Logical Operators

- and
- or
- not

Note: Identifiers that are also a keyword must be escaped using a backslash (\). For example: `ip proto \icmp`. You can also refer to protocols by number. See https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml as a reference. In this case, the above would be `ip proto 1`.

For more information on BPF filters, refer to one of the BPF references available online, such as https://biot.com/capstats/bpf.html.

Mirrored Traffic Definitions

Port Mirroring	Making a copy of some/all traffic crossing a specific physical port (for example, a network interface) and delivering this copy elsewhere. Usually used in conjunction with a packet analyzer.
SPAN	'Switch Port Analyzer' Cisco term for port mirroring.
TAP	An old way to mirror traffic – literally tap into network cable and connect to another network interface to receive a copy (wiretap).
Aircap	Airwall Solution's internal process used to implement port mirroring.
Packet analysis / packet dissection	Parsing packets to extract analytics.
Packet brokers	Industry term for packet analysis tools and related tools to transport mirrored packet to analysis tools.
GRE	'Generic Routing Encapsulation' an IP protocol used for encapsulation.
Mirror Destination	The Airwall Gateway mirrored traffic is sent to, either to a dedicated Mirror Destination group or to a packet analyzer connected as a local device to the overlay side of the Mirror Destination Airwall Gateway.
Mirror Sources	Airwall Gateways mirroring traffic and sending it to the Mirror Destination Airwall Gateway.

More Mirrored Traffic Scenarios

Typical scenarios for securely mirroring traffic to a packet analyzer and how to configure them.

There are many ways you can set up mirrored traffic. These scenarios give you an idea of how you can configure it so you are mirroring the traffic you want, and that mirrored traffic stays encrypted until it reaches its destination.

Mirroring Traffic on Airwall Gateways

- Mirror Traffic to a Local Device destination (Recommended Way)

- Mirror traffic to a dedicated port on page 467

Mirroring network traffic not on Airwall Gateways

- Mirror non-Airwall network traffic on page 471

Configuration Options

You can set up your network to mirror traffic in many different ways. Most combinations of Mirror Destination and Sources are valid. Whichever way you choose, you will also need to do the following to ensure the security of mirrored traffic and make sure your port mirroring configuration is not negatively impacting performance on your network:

- Adjust performance for mirrored traffic on page 462
- Set up security for mirrored traffic on page 463
- Configure your packet analyzer tool on page 463
- Verify Port Mirroring on page 463

Options to connect your packet analyzer tool

You can connect your packet analyzer tool to your mirror destination in two ways:

- Create a local device for your packet analyzer tool on page 459
- Connect your packet analyzer tool to a dedicated port on page 468

Mirror Destination Options

- Configure a Mirror Destination to send to a Local Device on page 460
- Configure a Mirror Destination to send to a Mirror Destination Group on page 469

Mirror Source Options

- Configure Airwall Gateways to act as the Mirror Sources on page 461
- Mirror non-Airwall traffic to an Overlay port group on page 474

More Port Mirroring Possibilities

These diagrams show more supported ways to mirror traffic and connect a packet analyzer tool: Diagrams for Port Mirroring on page 476

Mirror traffic to a dedicated port

You can send mirrored traffic to a dedicated port group attached to a physical cable.

When using a dedicated port to connect the Mirror Destination Airwall Gateway to your packet analyzer, normal switches don’t work. Since port mirroring captures traffic both directions, MAC flows are both directions. The switch learns all the MACs are connected to the Mirror Destination group and suppresses all traffic but broadcast, multicast, and unknown unicast MAC destinations.

Note: This configuration is not supported on the Airwall Gateway 300v model, because hypervisor has a switch.

Mirror traffic to a dedicated port

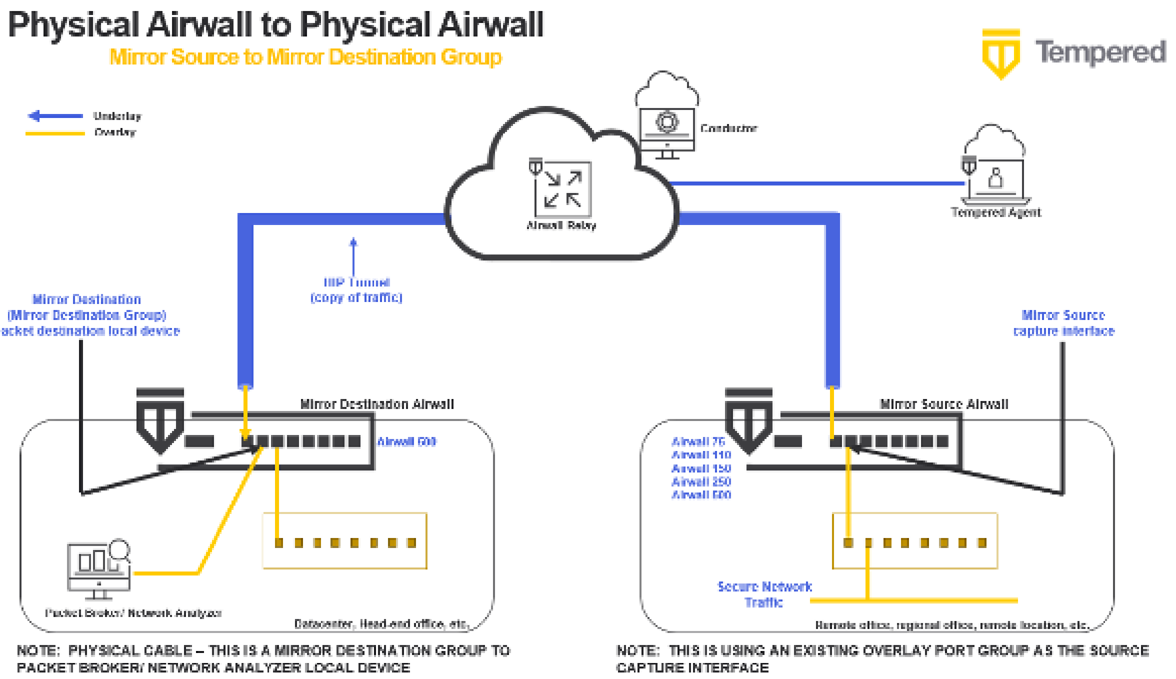
To mirror traffic to a dedicated port, you need to:

1. Connect your packet analyzer tool to a dedicated port on the Airwall Gateway you want to use as the Mirror Destination.
2. On the same Airwall Gateway, create a Mirror Destination port group, and assign the port your analyzer is plugged into to that group.
3. Configure a Mirror Destination to send to that Mirror Destination port group.

4. Configure Airwall Gateways to act as the Mirror Sources.
5. Adjust performance for mirrored traffic.
6. Set up security for mirrored traffic.
7. Configure your packet analyzer tool.

These steps are described in more detail in the following sections.

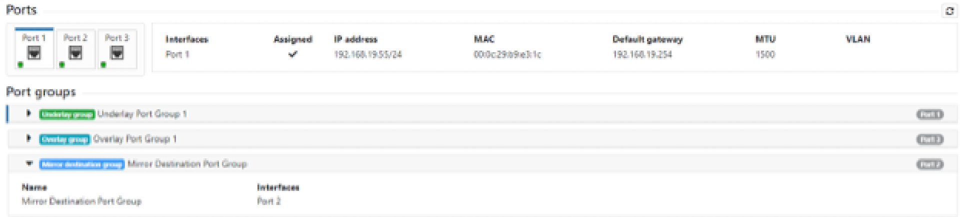
Here is a diagram showing this scenario:


Physical Airwall to Physical Airwall
Mirror Source to Mirror Destination Group
Tempered
Underlay
Overlay
Conductor
Airwall Relay
Tempered Agent
HIP Tunnel
(copy of traffic)
Mirror Destination
(Mirror Destination Group)
packet destination local device
Mirror Source
capture interface
Mirror Destination Airwall
Airwall 500
Mirror Source Airwall
Airwall 75
Airwall 110
Airwall 150
Airwall 250
Airwall 500
Packet Broker/ Network Analyzer
Datacenter, Head-end office, etc.
Secure Network
Traffic
Remote office, regional office, remote location, etc.
NOTE: PHYSICAL CABLE – THIS IS A MIRROR DESTINATION GROUP TO PACKET BROKER/ NETWORK ANALYZER LOCAL DEVICE
NOTE: THIS IS USING AN EXISTING OVERLAY PORT GROUP AS THE SOURCE CAPTURE INTERFACE

Connect your packet analyzer tool to a dedicated port

Directly connect your packet analyzer tool to a dedicated port on a physical Airwall Gateway.

1. Use a physical cable to connect your packet analyzer to a free port on the Airwall Gateway you will be using as the Mirror Destination.
2. In Conductor, on this Airwall Gateway, go to **Ports** > **Port configuration**.
3. Select **Edit Settings**.
4. Next to **Port Groups**, select the + to add a port group.
5. Choose `Mirror Destination group`.
6. Expand the group, and give it a descriptive name.
7. Under **Interfaces**, select an unused port:



Ports

Port 1 Port 2 Port 3

Interfaces	Assigned	IP address	MAC	Default gateway	MTU	VLAN
Port 1	✓	192.168.19.55/24	00:0c:29:b9:e3:1c	192.168.19.254	1500	

Port groups

Underlay group Underlay Port Group 1

Overlay group Overlay Port Group 1

Mirror destination group Mirror Destination Port Group

Name	Interfaces
Mirror Destination Port Group	Port 2

8. Select **Update Settings**.

If you are using this method to connect your packet analyzer tool, you need to configure your mirror destination as described on this page: Configure a Mirror Destination to send to a Mirror Destination Group on page 469.

Configure a Mirror Destination to send to a Mirror Destination Group

The Mirror Destination Airwall Gateway is where the network information your packet analyzer needs to consume is sent.

When using a port group, you connect your packet analyzer to the Mirror Destination Airwall Gateway using a physical cable.

CAUTION: When you are using a Mirror Destination group as the destination, you can't use a normal or virtual switch – you must connect the Mirror Destination to the packet analyzer directly with a cable. Because of this, this configuration is not supported on the 300v.

1. On the Mirror Destination Airwall Gateway, go to **Ports** > **Port mirroring**.
2. Select **Edit Settings**.
3. Next to **Configurations**, select the + to add a port mirroring configuration.
4. In your new configuration:
   a) Set the **Enabled** toggle to On.

      Note: After configuration, use this toggle to turn port mirroring on and off.

   b) Under **Type**, select `Mirror Destination`.
   c) Under **Packet destination**, select the Mirror Destination group you set up earlier.
   d) ***Optional*** – Under **Overlay IP**, change the Airwall Gateway mirroring configuration IP address. This IP is used for internal addressing only and is set by default to fd00:/8.

      CAUTION: When using Mirror Destination group, make sure it's not connected back to the original network, as this can cause loops with ever-increasing traffic as you're mirroring mirrored traffic (with the potential for overloading your network).

   e) ***Optional*** – Under **BPF filter**, Leave blank unless you are only interested in a single type of traffic, or want to exclude traffic from all sources.

      Note: If you use a BPF expression on the Mirror Destination, that's the default for all of the Mirror Sources, unless you set a BPF expression on the source, which overrides this default.
5. Select **Update Settings**.

You should be able to see some traffic from the Mirror Destination Airwall Gateway to the Mirror Destination group.

Configure Airwall Gateways to act as the Mirror Sources

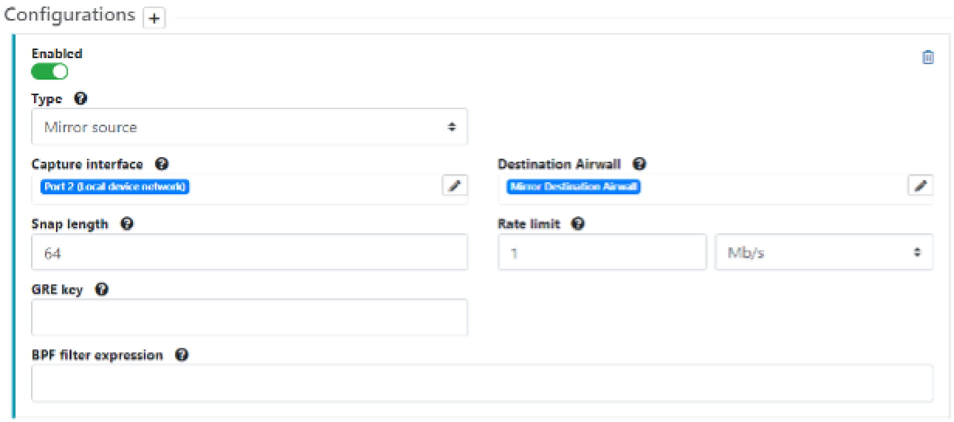
You configure Mirror Source Airwall Gateways to send network information to the Mirror Destination Airwall Gateway.

CAUTION: If you capture traffic on all ports of the overlay port group, you may set up a loop. To avoid this, in your configuration set a BPF filter of "ip proto not 47" to exclude mirrored traffic. See BPF Settings for Port Mirroring on page 464.

If you use GRE Transparent Ethernet Bridging, ERSPAN type II or ERSPAN type III – You can use GRE key or Session ID to identify which source the packets arrived on.

Note: You can set up the Mirror Destination to also be a Mirror Source, to include that Airwall Gateway's traffic in the information sent to the packet analyzer. In this case, be sure to set a BPF filter to exclude the mirrored traffic.

1. On a Mirror Source Airwall Gateway, go to **Ports** > **Port mirroring**.
2. Select **Edit Settings**.
3. Next to **Configurations**, select the + to add a mirroring configuration.
4. In your new configuration:
   a) Under **Type**, select `Mirror Source`.
   b) Under **Destination Airwall**, select the Airwall Gateway you set up as the Mirror Destination.
   c) Under **Capture interface**, select the interface you want to capture network information from. Ports in overlay port groups and the overlay hipbr bridge interfaces are supported.


Configurations +

Enabled

Type: Mirror source

Capture interface: Port 2 (Local device network)

Destination Airwall: Mirror Destination Airwall

Snap length: 64

Rate limit: 1 Mb/s

GRE key

BPF filter expression

d) ***Optional*** – If using a local device as the Mirror Destination, you can enter a GRE or session ID to distinguish the traffic being sent from this Mirror Source by including this value in the GRE/ERSPAN header of packets sent to a local device sync.

e) ***Recommended*** – Set performance settings for suggestions on setting Snap length, Rate limit, and source-specific BPF filters that override the Mirror Destination BPF filters (Example (BPF filter of “ip proto not 47” to exclude mirrored traffic and avoid loops). See Adjust performance for mirrored traffic on page 462 for guidance, or for more information on BPF filters, see BPF Settings for Port Mirroring on page 464.

5. Select **Update Settings**.

Note: You can set up different configurations for a Mirror Source Airwall Gateway to send traffic to different Mirror Destinations.

Adjust performance for mirrored traffic

Because mirroring traffic can impact your network performance, it is best practice to set one or all of the following performance adjustments on the Mirror Destination and Source Airwall Gateways to mitigate the performance impact.

Here are the performance adjustments you can make:

Snap length

Specify that when mirroring traffic, a Mirror Source Airwall Gateway should only copy this many bytes of the original packet. You can use this setting to get “headers only” with a small value (~64 bytes), and/or avoid fragmentation with a larger value (~1000 bytes). Specifying a full Ethernet frame size of 1514 bytes will avoid truncating packets (if you are using 802.1q VLAN tags or jumbo frames you will need to increase this value), but results in fragmenting every full-size mirrored packet, doubling the number of packets which must be processed.

Rate limits

Set a rate limit for mirrored traffic. This limit is only applied to the mirrored copy of the traffic. It is a best practice to configure a rate limit to limit the performance impact of using mirroring so you do not negatively impact other traffic secured by the Airwall Gateway. This limit also protects against misconfigurations where the mirrored traffic itself is mirrored, resulting in infinitely mirroring the same packet.

As a starting point, here are some recommended values to not significantly impact existing traffic, based on the relative performance for specific Airwall Gateway models:

Airwall Gateway model	Suggested Rate Limit
100	1 Mb/s
110	3 Mb/s
75	5 Mb/s
150	10 Mb/s
250	15 Mb/s

300v	20-100Mb/s
500	100 Mb/s

Note: You may want to set these limits lower, depending on your network bandwidth, particularly if your network connection is metered, as with a cellular provider.

When setting rate limits, also consider the performance of the Mirror Destination Airwall Gateway, the packet analyzer, and network connection between these Airwall Gateways.

BPF Filters

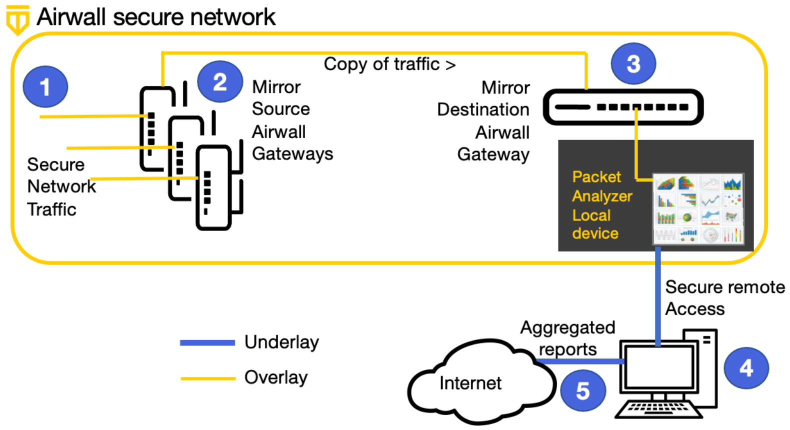
You can select which traffic is mirrored by specifying a BPF filter. If no filter is specified, all traffic is mirrored. By default, Mirror Source Airwall Gateways use the BPF filters specified on the Mirror Destination Airwall Gateway. You can override this default by setting different filters on any of the Mirror Source Airwall Gateways. BPF filters will filter mirrored traffic to specific protocols using BPF filter expressions. For information on the BPF filters most helpful for port mirroring, see BPF Settings for Port Mirroring on page 464.

Set up security for mirrored traffic

Protect your mirrored traffic.

Because your packet analyzer can be a back door to sensitive information about your network (impacting your Airwall secure network invisibility), you need to set up security policies to limit access to your packet analyzer and mirrored traffic so that only trusted devices can access it.

CAUTION: It is a best practice to keep all of the information being sent to your packet analyzer within the Airwall secure network. Since you are essentially making a copy of potentially-sensitive overlay traffic and decrypting it for the packet analyzer, there is a risk of exposure if your packet analyzer is compromised, not secured, or if the network information you are capturing is sent over an unsecured network. You can secure the packet analyzer management interface within the Airwall secure network, with access to the interface limited to authorized personnel.



Configure your packet analyzer tool

Make sure your packet analyzer tool is set up to receive the mirrored network traffic data.

You should now be getting traffic to your packet analyzer tool (protocol analyzer, packet broker, or other tool that consumes network traffic information) and can configure your packet analyzer software to consume the data being received from the Mirror Destination Airwall Gateway. For assistance, see the documentation for your packet analyzer software.

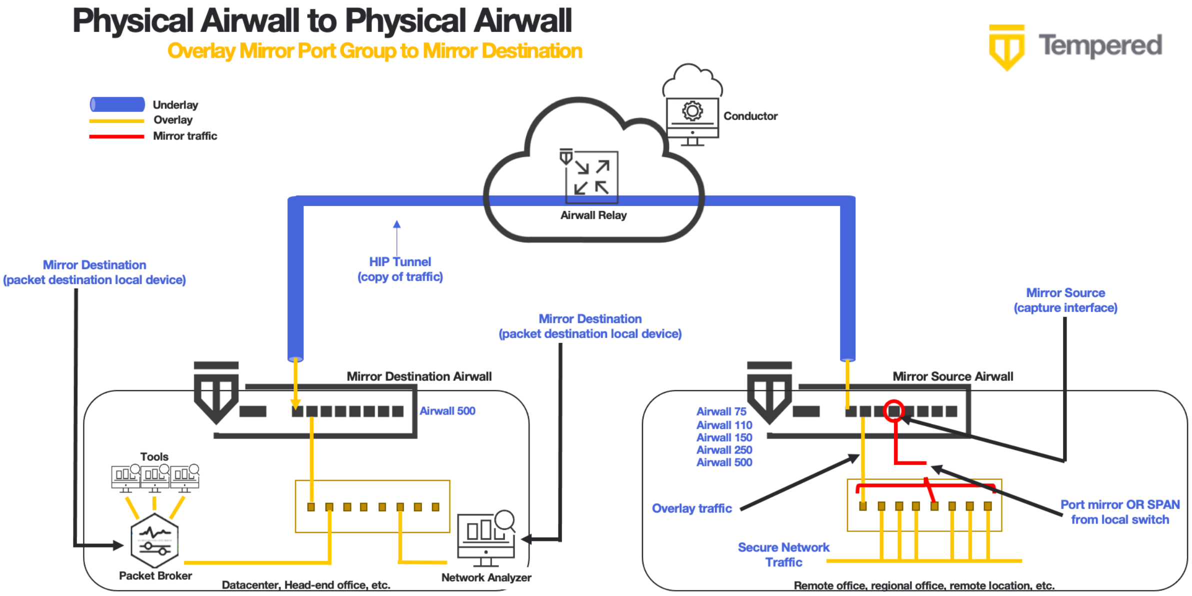
Mirror non-Airwall network traffic

Use this mirrored traffic scenario if you want to capture network traffic that isn't currently going through an Airwall Gateway. This method uses:

- **Mirror Destination** – A local device

- **Mirror Source** – A dedicated port and overlay port group on an Airwall Gateway that collects non-Airwall network traffic and sends to the Mirror Destination

This diagram shows how the traffic is mirrored and accessed, with mirrored traffic sent to a Mirror Source Airwall Gateway, then to the Mirror Destination Airwall Gateway over encrypted HIP Tunnels on the Underlay.



NOTE: THIS IS GRE/ ERSPAN TO PACKET BROKER OR NETWORK ANALYZER LOCAL DEVICE

NOTE: THIS IS A NEW OVERLAY INTERFACE USED ONLY FOR THE SOURCE CAPTURE INTERFACE

Set up this Mirrored Traffic Scenario

To configure this scenario, you need to:

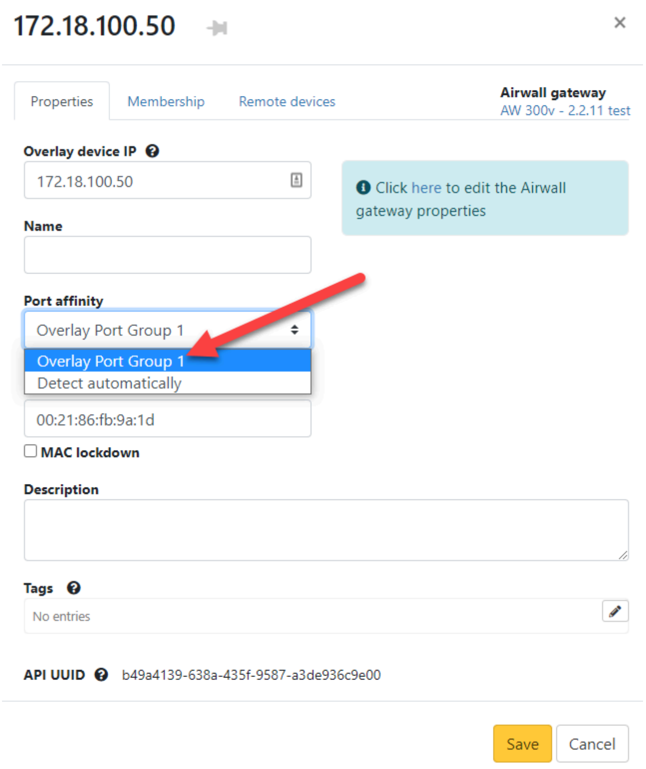
1. Create a local device for your packet analyzer tool.
2. Configure a Mirror Destination to a Local Device.
3. Mirror non-Airwall traffic to an Overlay port group.
   a) Add an Overlay Port group to capture non-Airwall traffic.
   b) Add a Port Mirroring Configuration.
4. Adjust Performance for Mirrored Traffic.
5. Configure your network to send traffic to the Overlay Port group.
6. Connect your packet analyzer.

Create a local device for your packet analyzer tool

Create a local device on a dedicated overlay port group for your packet analyzer tool (protocol analyzer, packet broker, or other tool that consumes network traffic information).

The destination for your mirrored traffic can be your packet analyzer set up as a local device on your Mirror Destination Airwall Gateway.

1. Add the packet analyzer tool as a local device to the Airwall Gateway that you're going to use as your Mirror Destination (the one that receives the mirrored traffic and sends it to the destination, which is your analyzer).
2. When you're adding the device (either manually or through auto-discovery), you must set Port affinity (it cannot be left on auto).



172.18.100.50

Airwall gateway
AW 300v - 2.2.11 test

Overlay device IP: 172.18.100.50

Click here to edit the Airwall gateway properties

Name:

Port affinity: Overlay Port Group 1

Overlay Port Group 1
Detect automatically

00:21:86:fb:9a:1d

□ MAC lockdown

Description:

Tags: No entries

API UUID: b49a4139-638a-435f-9587-a3de936c9e00

For more information, see Add devices to the Conductor on page 414.

If you are using this method to connect your packet analyzer tool, you need to configure your mirror destination as described on this page: Configure a Mirror Destination to send to a Local Device on page 460

Configure a Mirror Destination to send to a Local Device

The Mirror Destination Airwall Gateway receives the mirrored traffic and sends it to your packet analyzer (or network analyzer or packet broker).

If your packet analyzer supports receiving packets encapsulated in GRE or ERSPAN, this is the preferred configuration. It avoids the possibly of mirrored traffic being recirculated on your network and the MAC address table issues with switches. It also provides additional fields to your packet analyzer that allow it to distinguish between traffic captured by multiple Airwall Gateways (using GRE key/ERSPAN session ID) and detect lost or reordered packets (using ERSPAN sequence number).

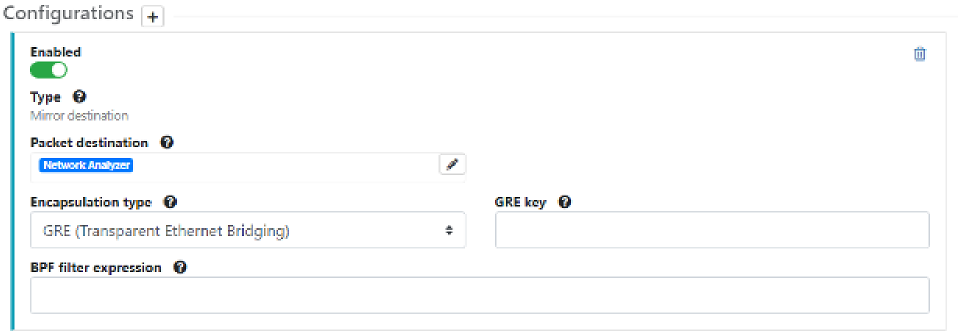
1. On the Airwall Gateway page, go to **Ports** > **Port mirroring**.
2. Select **Edit Settings**.
3. Next to **Configurations**, select the + to add a mirroring configuration.
4. In your new configuration:
   a) Set the **Enabled** toggle to On.

      Note: After configuration, use this toggle to turn mirroring on and off.

   b) Under **Type**, select `Mirror Destination`.
   c) Under **Packet destination**, select the local device for your packet analyzer you set up earlier.

      Note: The device will not show up as destination when you're selecting the Mirror Destination Airwall Gateway unless you've set a specific port group affinity (not `Auto`). See Create a local device for your packet analyzer tool on page 459.

   d) Under **Encapsulation type**, select the encapsulation (`GRE` or `ERSPAN Type I, II, or III`) supported by your packet analyzer. For example, for Nozomi, pick ERSPAN type II. Refer to documentation of your packet analyzer to determine which encapsulations it supports.



Configurations +

Enabled

Type: Mirror destination

Packet destination: Network Analyzer

Encapsulation type: GRE (Transparent Ethernet Bridging)

GRE key

BPF filter expression

e) *Optional* – Enter any information allowed for the type you selected (for example, GRE key or session ID).

f) *Optional* – Under BPF filter, add any BPF filters you would like to use to filter the traffic that is mirrored to this Mirror Destination. See BPF Settings for Port Mirroring on page 464.

> **Note:** If you use a BPF expression on the Mirror Destination, that's the default for all of the Mirror Sources, unless you set a BPF expression on the source, which overrides this default.

5. Select **Update Settings**.

You should be able to see some traffic from the Mirror Destination to the packet analyzer local device.

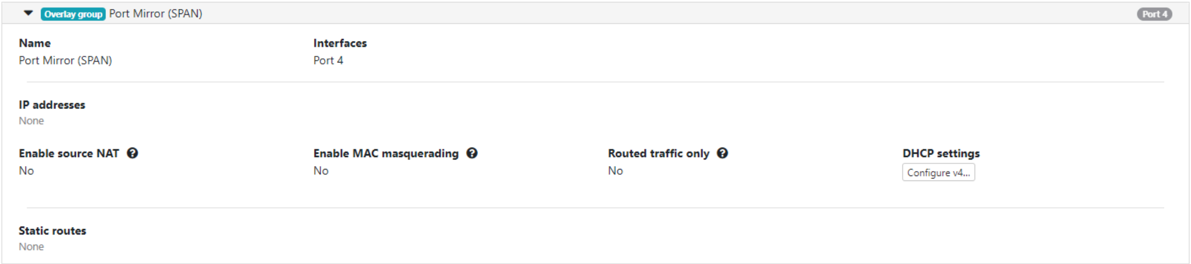
Mirror non-Airwall traffic to an Overlay port group

To capture mirrored non-Airwall traffic, you can configure an Overlay Port Group on a Mirror Source Airwall Gateway, which then sends network information to the Mirror Destination Airwall Gateway.

For this scenario, you need to add an overlay port group to capture non-Airwall traffic and a Mirror Source port mirroring configuration that captures the mirrored traffic on that port.

If you use GRE Transparent Ethernet Bridging, ERSPAN type II or ERSPAN type III – You can use GRE key or Session ID to identify which source the packets arrived on.

1. Set up an Overlay port group on a Mirror Source Airwall Gateway to capture the non-Airwall traffic being collected by your network:



Overlay group Port Mirror (SPAN) Port 4

Name: Port Mirror (SPAN)

Interfaces: Port 4

IP addresses: None

Enable source NAT: No

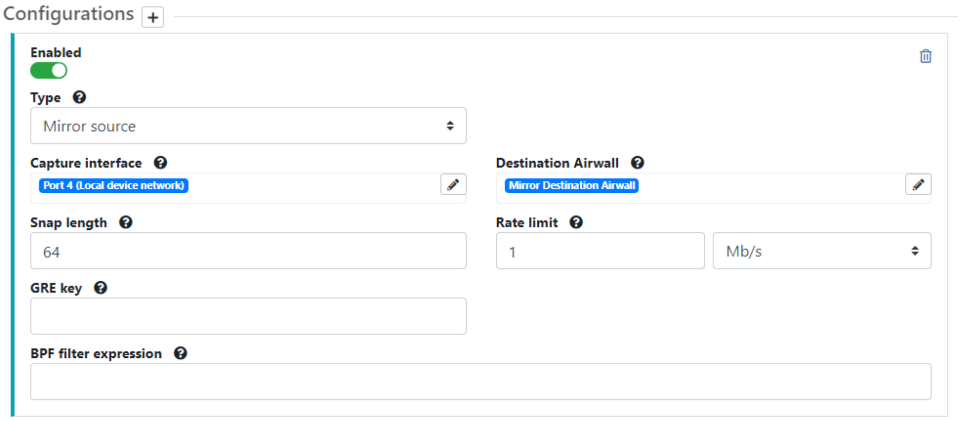
Enable MAC masquerading: No

Routed traffic only: No

DHCP settings: Configure v4...

Static routes: None

2. Add a Port Mirroring Configuration on the same Airwall Gateway, selecting the port you configured as your Port Mirror (SPAN) Overlay group above as the Capture interface, and the Mirror Destination:



Configurations +

Enabled

Type: Mirror source

Capture interface: Port 4 (Local device network)

Destination Airwall: Mirror Destination Airwall

Snap length: 64

Rate limit: 1 Mb/s

GRE key

BPF filter expression

For details on how, see Configure Airwall Gateways to act as the Mirror Sources on page 461

Adjust performance for mirrored traffic

Because mirroring traffic can impact your network performance, it is best practice to set one or all of the following performance adjustments on the Mirror Destination and Source Airwall Gateways to mitigate the performance impact.

Here are the performance adjustments you can make:

Snap length

Specify that when mirroring traffic, a Mirror Source Airwall Gateway should only copy this many bytes of the original packet. You can use this setting to get "headers only" with a small value (~64 bytes), and/or avoid fragmentation with a larger value (~1000 bytes). Specifying a full Ethernet frame size of 1514 bytes will avoid truncating packets (if you are using 802.1q VLAN tags or jumbo frames you will need to increase this value), but results in fragmenting every full-size mirrored packet, doubling the number of packets which must be processed.

Rate limits

Set a rate limit for mirrored traffic. This limit is only applied to the mirrored copy of the traffic. It is a best practice to configure a rate limit to limit the performance impact of using mirroring so you do not negatively impact other traffic secured by the Airwall Gateway. This limit also protects against misconfigurations where the mirrored traffic itself is mirrored, resulting in infinitely mirroring the same packet.

As a starting point, here are some recommended values to not significantly impact existing traffic, based on the relative performance for specific Airwall Gateway models:

Airwall Gateway model	Suggested Rate Limit
100	1 Mb/s
110	3 Mb/s
75	5 Mb/s
150	10 Mb/s
250	15 Mb/s
300v	20-100Mb/s
500	100 Mb/s

Note: You may want to set these limits lower, depending on your network bandwidth, particularly if your network connection is metered, as with a cellular provider.

When setting rate limits, also consider the performance of the Mirror Destination Airwall Gateway, the packet analyzer, and network connection between these Airwall Gateways.

BPF Filters

You can select which traffic is mirrored by specifying a BPF filter. If no filter is specified, all traffic is mirrored. By default, Mirror Source Airwall Gateways use the BPF filters specified on the Mirror Destination Airwall Gateway. You can override this default by setting different filters on any of the Mirror Source Airwall Gateways. BPF filters will filter mirrored traffic to specific protocols using BPF filter expressions. For information on the BPF filters most helpful for port mirroring, see BPF Settings for Port Mirroring on page 464.

Configure your network to send traffic to the Overlay port group

Send your non-Airwall traffic to the Mirror source Airwall Gateway.

Connect your network to the port for the Overlay port group created on the Mirror Source Airwall Gateway, and follow the instructions for your network to gather and send traffic to that port.

Configure your packet analyzer tool

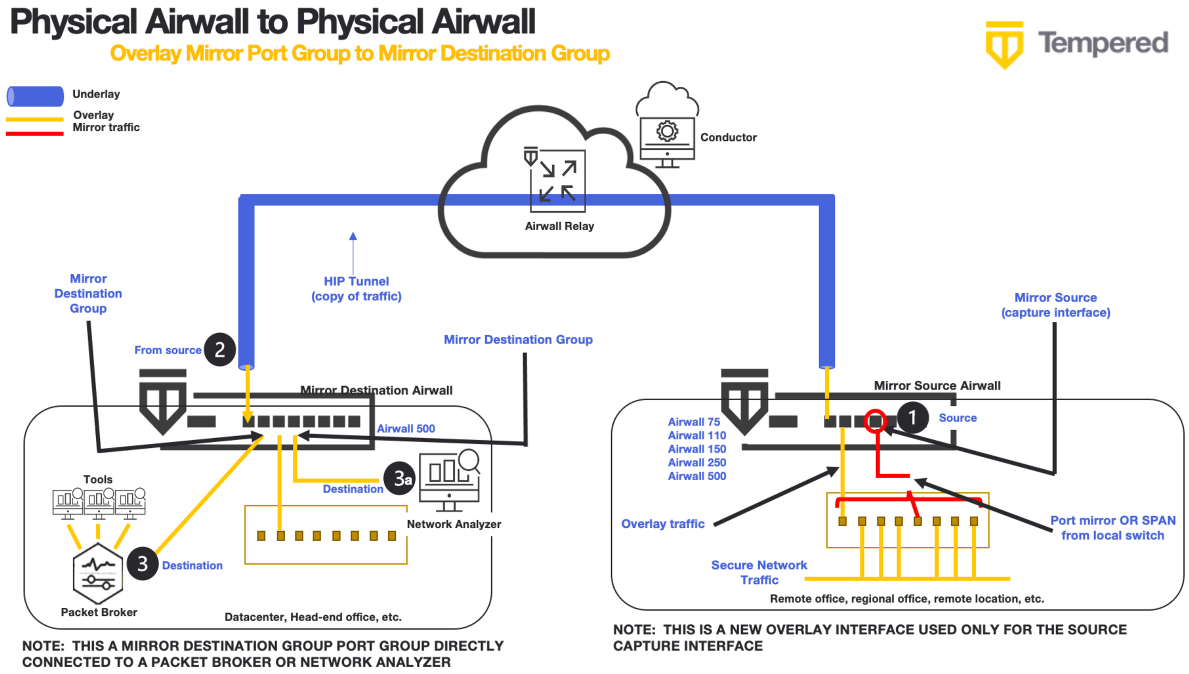
Make sure your packet analyzer tool is set up to receive the mirrored network traffic data.

You should now be getting traffic to your packet analyzer tool (protocol analyzer, packet broker, or other tool that consumes network traffic information) and can configure your packet analyzer software to consume the data being received from the Mirror Destination Airwall Gateway. For assistance, see the documentation for your packet analyzer software.

Diagrams for Port Mirroring

More supported configurations to mirror traffic.

Overlay Mirror Port Group to Mirror Destination Group



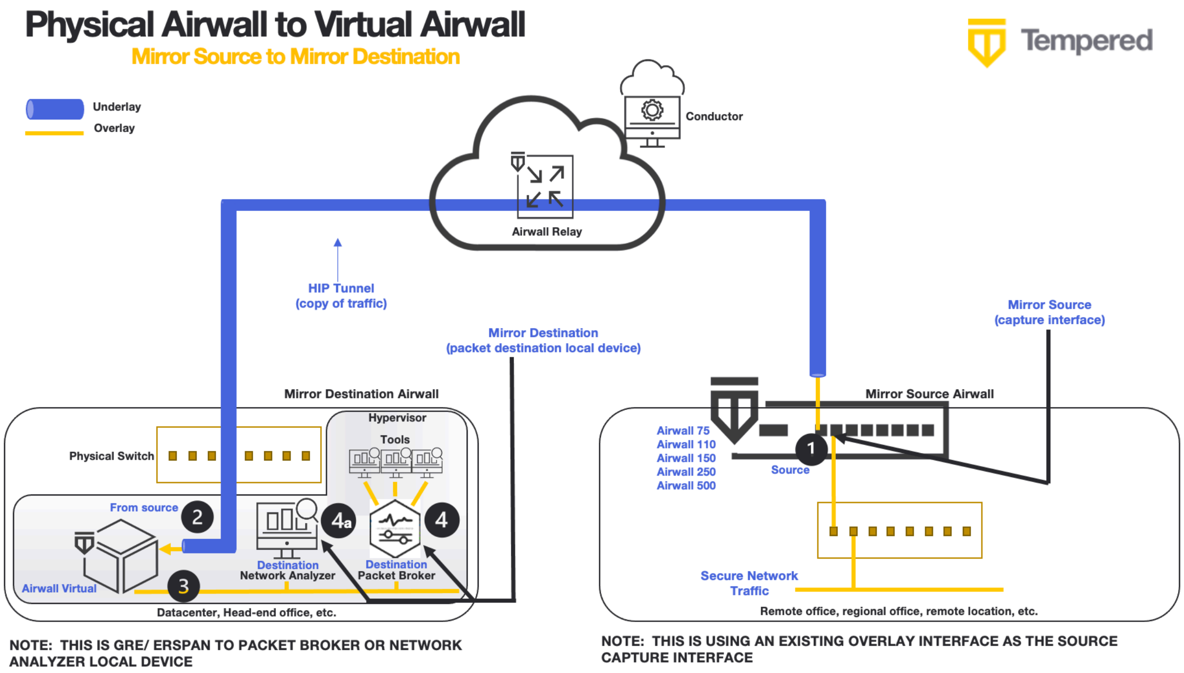
NOTE: THIS A MIRROR DESTINATION GROUP PORT GROUP DIRECTLY CONNECTED TO A PACKET BROKER OR NETWORK ANALYZER

NOTE: THIS IS A NEW OVERLAY INTERFACE USED ONLY FOR THE SOURCE CAPTURE INTERFACE

To set up this configuration:

1. Connect your packet analyzer tool to a dedicated port on page 468
2. Configure a Mirror Destination to send to a Mirror Destination Group on page 469
3. Mirror non-Airwall traffic to an Overlay port group on page 474
4. Adjust performance for mirrored traffic on page 462
5. Configure your network to send traffic to the Overlay port group on page 475
6. Configure your packet analyzer tool on page 463
7. Verify Port Mirroring on page 463

Physical Mirror Source to Virtual Mirror Destination



NOTE: THIS IS GRE/ ERSPAN TO PACKET BROKER OR NETWORK ANALYZER LOCAL DEVICE

NOTE: THIS IS USING AN EXISTING OVERLAY INTERFACE AS THE SOURCE CAPTURE INTERFACE

To set up this configuration:

1. Connect your packet analyzer tool to a dedicated port on page 468
2. Configure a Mirror Destination to send to a Mirror Destination Group on page 469
3. Configure Airwall Gateways to act as the Mirror Sources on page 461
4. Adjust performance for mirrored traffic on page 462
5. Set up security for mirrored traffic on page 463
6. Configure your packet analyzer tool on page 463
7. Verify Port Mirroring on page 463

Diagnostics and Troubleshooting

Diagnostic Tools

Put the Conductor into diagnostic mode

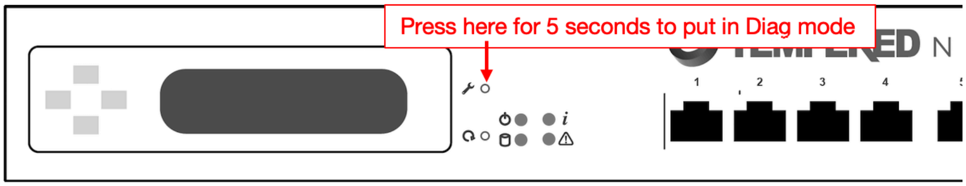
To place the Conductor into diagnostic mode, you will need a laptop connected to port 2 that is configured to receive a DHCP IP Address.

When the Conductor is in diagnostic mode, you can:

- Download a Conductor support bundle. You can also download a support bundle from the Conductor if it is running. See Create a support bundle for a Conductor on page 481.
- Display system status. You can also see system status on the Conductor Dashboard. See The Conductor Dashboard on page 32.
- Perform firmware updates. You can also easily apply firmware updates in the Conductor. See Update your Conductor and Airwall Edge Services on page 126.
- Enable and disable SSH (SSH is disabled by default). See Set up Remote Access to Airshell via SSH on page 374.

To put the Conductor into diagnostic mode

1. For a hardware Conductor, press the wrench pinhole on the front of the Conductor for 5 seconds should put it into diagnostic mode.



Press here for 5 seconds to put in Diag mode

2. Connect your laptop to port 2 of the Conductor, and configure your laptop adapter to use DHCP.
3. Once your laptop obtains an IP address, open a web browser and navigate to http://192.168.56.2 and the Conductor diagnostic page loads.

Once the Conductor is in diagnostic mode, Overlay network communications from the Conductor are disabled and device network is reconfigured with a static IP address.

For more information on console commands, see Airshell (airsh) Command Reference on page 362.

Put an Airwall Gateway into diagnostic mode

With an Airwall Gateway in diagnostic mode, you can troubleshoot it by collecting diagnostic information and you can also manage a variety of settings such as IP addresses, logs, and firmware.

After placing an Airwall Gateway in diagnostic mode, you must restart it to return it to normal operating mode. After restarting, the Airwall Gateway may require up to three minutes to return to operating mode.

There are many Airwall Gateway diagnostic tasks you can do in the Conductor if it has access. See Diagnostics and Troubleshooting on page 477.

Note: See the platform guide that came with your Airwall Gateway for specific instructions for your model. If you are using versions before 2.2.3, please see the 2.2.3 help.

1. Follow the instructions for your model:
   - **Airwall Gateway 75 / ESPRESSObin** - Place into diagnostic mode by connecting your computer to the micro-USB console port and using airsh to enter `diag`.
   - **Airwall Gateway 100, 110, 150, 200, and 250 series** - Place into diagnostic mode by pressing and holding the multi-purpose or reset button for only three seconds. Immediately release the button.

     Important: Do not continue pressing the multi-purpose or reset button after three seconds as this will reset the Airwall Gateway to factory settings.

     After three seconds, the status LED blinks to indicate the Airwall Gateway is in diagnostic mode. For more information about LED blink patterns, Status LED Blink Codes on page 480.
   - **Airwall Gateway 300, 400, and 500 series** - Place into diagnostic mode by connecting a VGA monitor and a USB keyboard to port 2 of the Airwall Gateway, and at the login prompt:
     - 2.2.3 and later: Enter `airsh` to enter the console, and then enter `diag`.

       Note: If you're asked for a password, enter the default password `airsh`, or the password you set.
     - Earlier than 2.2.3: Enter `diag` then enter the password `diag`.

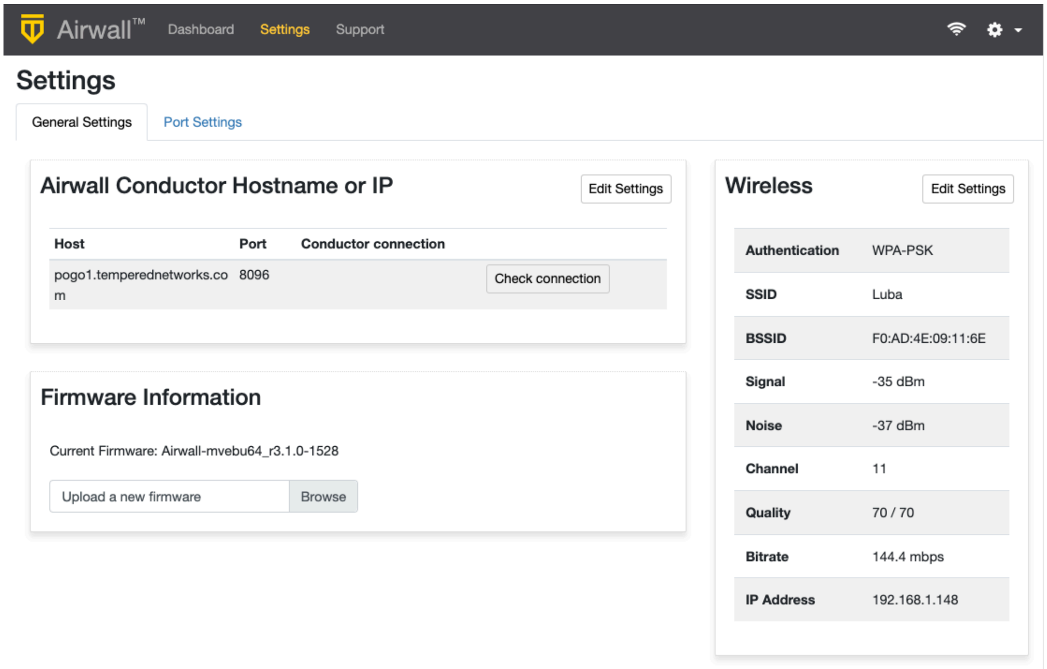
       Once the Airwall Gateway is in diagnostic mode, Overlay network communications from the Airwall Gateway are disabled and device network is reconfigured with a static IP address.
   - **Airwall AV3200g** - Place into diagnostic mode by pressing and holding the Reset button for 6 seconds.

     Immediately release the button when all the LED lights blink off. The status LED blinks to indicate the Airwall is in diagnostic mode.

Important: Do not hold the reset button for longer than 8 seconds as this will reset the default factory configuration.

- **Airwall AV3033** - Place into diagnostic mode with the Airwall's LCD screen and buttons.

2. Connect a computer to one of the device network ports (typically port 2 and above).
3. Open a web browser and go to `http://192.168.56.3` to access the Airwall Gateway diagnostic page.



Settings

Airwall Conductor Hostname or IP

Host	Port	Conductor connection
pogo1.temperednetworks.com	8096	

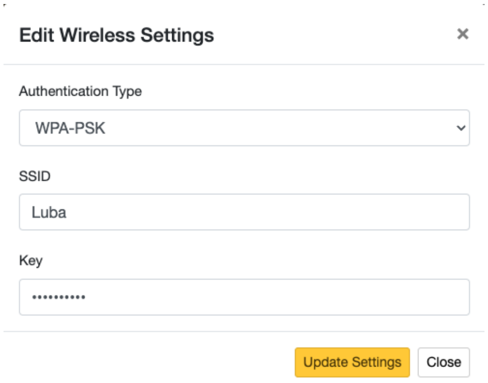
Firmware Information

Current Firmware: Airwall-mvebu64_r3.1.0-1528

Wireless

Authentication	WPA-PSK
SSID	Luba
BSSID	F0:AD:4E:09:11:6E
Signal	-35 dBm
Noise	-37 dBm
Channel	11
Quality	70 / 70
Bitrate	144.4 mbps
IP Address	192.168.1.148

4. To edit the Conductor, next to Airwall Conductor Hostname or IP, select **Edit Settings**. Make your selections and select **Update Settings**
5. To edit Wireless (Wi-Fi) settings, next to Wireless, select **Edit Settings**. Make your selections and select **Update Settings**.



Edit Wireless Settings

Authentication Type: WPA-PSK

SSID: Luba

Key: ••••••••••

Note: To exit diagnostic mode, select **Reboot** in the Diagnostic mode interface, or turn the Airwall Gateway off and back on again.

For more information on console commands, see Airshell (airsh) Command Reference on page 362. See also Connect an Airwall Gateway with Diag mode on page 292.

Create a Conductor database backup

A Conductor database backup can provide a measure of security when you are working on system-wide changes. Before you update firmware or replace hardware, we strongly recommend that you create, download and archive a Conductor database backup.

CAUTION: Do not attempt to restore a Conductor from a database backup that was running a previous firmware revision.

To create a database backup:

1. Log in to Conductor as a system administrator
2. Go to **Settings** and open the **Diagnostics** tab.
3. Under **Diagnostics**, select **Download database backup**.
4. Click **Create**.
5. Once the backup is complete, select **Download the backup archive** and save the backup file.

Restore or replace a Conductor database backup

Note: The Conductor database can be restored using a backup file; however, all changes to the Conductor configuration made after database backup creation will be lost.

To restore a Conductor from a previously created database backup, go to **Settings**, and select **Restore a database backup**. Choose the database backup file and click **Upload**.

Important: A Conductor cannot be restored using a database backup taken while running a previous firmware version.

Upgrade or replace a Conductor

If you are upgrading or replacing your Conductor, we strongly recommend that you first create a database backup as described above and download to your desktop or similar. Once the Conductor database backup has been created and downloaded, do not make any configuration changes. When the replacement Conductor is online, navigate to 192.168.56.2 and login as the System Administrator. Go to **Settings**, select **Restore a database backup**, choose the database backup file and click **Upload**. Next, take the existing Conductor offline and set the network configuration of the replacement Conductor so it is identical to the network configuration of the existing Conductor. Your Airwall Edge Services will begin communicating with the new Conductor. You can verify status in the **Dashboard** of the Conductor.

Identify a Physical Airwall Gateway

If you need to identify a particular physical Airwall Gateway from the Conductor, you can use Conductor Blink.

1. In the Conductor, open the page for a specific physical Airwall Gateway.
2. Open the **Actions** menu for the Airwall Gateway and select **Blink**.

Results:

- **Status LED** – On Airwall Gateway models with a status LED, the Airwall Gateway will do the Conductor Blink sequence for 5 minutes, then go back to its normal display.
- **LCD screen** – On Airwall Gateway models with an LCD screen, the LCD screen displays “Here I am.”

See also: Status LED Blink Codes on page 480

Status LED Blink Codes

Physical Airwall Gateways equipped with a Status LED use blink codes to indicate their status.

Status LED Codes

State	LED Pattern	State	LED Pattern
Normal Operation	On Steady	No Conductor Connection	**O O O O = = O O = =**
Conductor Blink	**O O = =**	System Error	**O O O O = = O O O = =**
Missing Identity	**O O O = = O = =**	Secure Network Error	**O O O O = = =**
Factory Reset	**O O = = O = =**	No Shared Network	**O O O O = = O = =**

State	LED Pattern	State	LED Pattern
Diagnostic Mode	**O** = **O** = (fast blink)	Firmware Download	**O O O** = = **O O** = =
		Firmware Update	**O O O** = = =
Key: **O** is on, = is off			

Here are more details on a couple of the blink codes:

Conductor Blink O O = =	This LED blink pattern is a Conductor-initiated blink code used to help identify a specific physical Airwall Gateway. See Identify a Physical Airwall Gateway on page 480.
No Shared Network O O O O = = O = =	The ping to the default router is failing.

Collect troubleshooting data for Airwall Gateways, Conductors, or Airwall Agents and Servers

How to capture information to assist in troubleshooting different parts of an Airwall secure network.

Sometimes Tempered Customer Success asks you to gather information as part of the troubleshooting process. The Customer Success team primarily needs the following items:

- Support Bundles
- Packet Captures
- Diagnostic reports
- Related logs and errata
- Advanced diagnostics

See the following sections for how to gather this information.

Create a support bundle for an Airwall Gateway

Creating a support bundle is one of several diagnostic tools that you can use to help our support staff assist in troubleshooting an Airwall Gateway. The Conductor offers several diagnostic capabilities and you can learn about the others by using the links near the bottom of this article.

Support bundles are encrypted files. For security purposes, only Tempered can open them.

Here's what's in support bundles:

- **Airwall Gateway Support Bundles** contain full system logs from the machine, along with configuration files and cached information.
- **Airwall Agent or Server Support Bundles** contain all software logs and configurations, cached data, and a snapshot of your system's network settings.

To create a support bundle:

1. Log in to the Conductor with a system administrator or network administrator role account.
2. Go to **Airwall edge services**, open one from the list, and then open **Diagnostics**.

   Note: If an Airwall Gateway is offline, you can put it into diagnostic mode and download a support bundle. See Put an Airwall Gateway into diagnostic mode on page 478 for more information.
3. Create your Airwall Gateway support bundle by clicking **Request a support bundle**.

   Once the support bundle `.pkg` file has been created, you will be provided a download link to the file. A support bundle `.pkg` file is an encrypted archive that facilitates technical support by Tempered only.
4. Send the support bundle as an email attachment to Customer Success. A Tempered support engineer will contact you when it is received.

Create a support bundle for a Conductor

To facilitate customer troubleshooting, Customer Success may request a Conductor support bundle

Conductor Support Bundles contain full system logs from the machine, along with a full copy of the database. These bundles can be used to replicate your Conductor in a lab for the purposes of reproducing problems.

To create a Conductor support bundle

1. Go to **Settings**, click **Diagnostics**, and select **Download a support bundle**. The Conductor creates a support bundle and provides it as a downloadable file.
2. Download the support bundle file and send to Customer Success Customer Success.

Customer Success can then analyze this encrypted support bundle.

Note: You can also download the most recent Conductor support bundle from the following URL: `https://<conductor-ip-address>/support/support_bundles/sc-support-bundle`.

Do a packet capture for an Airwall Gateway

Packet capture is one of several diagnostic tools that you can use to facilitate troubleshooting a Conductor or Airwall Gateway. The Conductor offers several diagnostic capabilities and you can learn about the others by using the links near the bottom of this article.

What's in a packet capture

Packet Captures show how traffic is flowing within your network. You can request packet captures from the Conductor for any Airwall Edge Service that is online.

Depending on the nature of your issue, Customer Success may require captures from the underlay network, the overlay (protected) network, or both.

- **Underlay network** captures show the HIP packets exchanged between Airwall Edge Services, MAP packets exchanged between the Airwall Edge Services and the Conductor, any other traffic to and from the Airwall, and ARP and Multicast messages.
- **Overlay network** captures show everything traversing the HIP tunnel to and from your protected devices.

You select which to capture by setting the Capture interface when requesting a packet capture.

How to get a packet capture

1. In the Conductor, go to **Airwall edge services**, open one from the list, and go to **Diagnostics**.
2. Select **Start Packet Capture**.
3. Select any needed options.

   Here are the options you might have. Options may vary based on Conductor or Airwall Edge Service versions.

   - **Capture interface** – Select which interface you want to capture.
   - **Protocol** – You can limit the capture to only a specific protocol, as needed.
   - **IP address** – Limit the capture to only a specific IP address. You can match either source or destination address to filter for only a specific device or remote destination on a busy Airwall Edge Service.
   - **Port** – Select a TCP/UDP or L4 port to capture on.
   - **Snap length** – Controls how much of each packet to capture. The default is 64 (headers only). Set to zero for unlimited, or to 1514 (standard size Ethernet packets) to not truncate each packet in the capture.
   - **BPF filter expression** – Set a filter using BPF filter expressions. See BPF Settings for Port Mirroring on page 464.
   - **Max capture filesize** – Limit how large the pcap file can be.
   - **Max capture time** – Set how long to capture.
   - **Limit upload bandwidth** – Slow down the upload of the resulting pcap for limited bandwidth environments (e.g. you pay for higher than a given throughput or you have a slow link (maybe shared with other devices) and the bulk upload of the pcap at the end could negatively impact other traffic.
4. Select **OK** to start the packet capture.
5. Do what you were doing when your issue occurred.
6. Stop the packet capture by selecting **Stop Packet Capture**.

The Conductor creates a packet capture `.pcap` file. When it is finished, you get a download link to the file. The `.pcap` file is a standard format file that can be viewed with an application such as **Wireshark**.

Do a packet capture for a Conductor

Packet capture is one of several diagnostic tools that you can use to facilitate troubleshooting an Conductor.

How to get a packet capture

1. In the Conductor, go to **Settings** > **Diagnostics** > **Network troubleshooting tools**.
2. Begin packet capture by selecting **Start Packet Capture**.
3. Do what you were doing when your issue occurred.
4. Stop the packet capture by selecting **Stop Packet Capture**.

   The Conductor creates a packet capture `.pcap` file. When it is finished, you get a download link to the file. The `.pcap` file is a standard format file that can be viewed with an application such as **Wireshark**.

Create a diagnostic report for an Airwall Gateway

Creating a diagnostic report is one of several diagnostic tools that you can use to get a general overview of the health of an Airwall Gateway. The Conductor offers several diagnostic capabilities and you can learn about the others by using the links near the bottom of this article.

To create a diagnostic report:

1. Go to **Airwall edge services**, open one from the list, and then go to **Diagnostics**.

   If an Airwall Gateway is offline, you can put it into diagnostic mode and download a support bundle. For more information, see Put an Airwall Gateway into diagnostic mode on page 478.
2. Create your report by clicking **Request a diagnostic report**.

   Once the report `.txt` file has been created, you will be provided a download link to it. The diagnostic report is a text file that you can examine to see a high-level look at the overall health of the Airwall Gateway.

Create a diagnostic report for a Conductor

Creating a diagnostic report is one of several diagnostic tools that you can use to get a general overview of the health of a Conductor.

To create a diagnostic report for your Conductor:

1. In the Conductor, go to **Settings** > **Diagnostics**.
2. Under **Diagnostics** select **View diagnostic report**.
3. Select all of the text and copy it into a .txt file.

Examine the diagnostic report text file to get a high-level view of the overall health of the Conductor.

Related logs and errata

There are always a dynamic set of data points that Tempered Customer Success may need to solve a problem outside of what the Conductor can capture. The most common items they may ask for are listed here:

General

- Network Diagrams
- Network Device Configs (Firewalls/Routers/Switches)
- Device lists

Windows

- Windows System Event Logs
- Windows Application Event Logs
- setupAPI logs:
- Tempered Program Files

Gather advanced diagnostics

The Tempered Customer Success team has a set of internal tools used to analyze the data you provide. With these tools, the team has created some ways you can collect data that will assist the Customer Success team in troubleshooting your issues.

These procedures often require you to run multiple concurrent packet captures. The easiest way to do this is to open the **Diagnostics** page for different Airwall Edge Services in multiple tabs to queue up captures quickly (use CTRL +TAB to switch between tabs).

Full-Mesh network connectivity test:

This test allows the Customer Success team to map out all connectivity on your entire online network.

1. Add all of your Airwall Edge Services to an Airwall group called `Diagnostic`.
2. In web browser tabs, queue up – but do not start – Shared Network packet captures for every online Airwall Gateway (see Do a packet capture for an Airwall Gateway on page 482) , as well as your Conductor (see Do a packet capture for a Conductor on page 483).
3. In additional browser tabs, queue up all online Airwall Agent or Server diagnostic pages. You need these later in this process.
4. For all online Airwall Edge Services from step 2, and for your Conductor, select **Start packet capture**.
5. (Optional) Start Shared Network packet captures on all online Airwall Agents and Servers. This cannot be done from the Conductor, so it is not required. Consider using *Wireshark* to do this.
6. On the **Airwall groups** tab, on the line for the Diagnostic Airwall group you created, from the **Actions** menu, select **Check Online**.
7. On **ALL online Airwalls**, go to the **Secure tunnels** tab, and check **Build new tunnels if none exist**, and then select **Check Secure Tunnels**.
8. Wait until all the diagnostic tests complete and then stop all packet captures.
9. Download all packet captures and collect them into one ZIP archive. Ensure that it is easy to identify which capture is which.
10. Send that data to Customer Success .

This data provides captures of all MAP packets between Airwall Edge Services and your Conductor, HIP packets between Airwall Edge Services, and all background traffic on your collective Shared Network.

In addition, Customer Success may also need:

1. Support bundles from all Airwall Gateways and Airwall Agents and Servers.
2. Lists of other network devices on your Shared Network (CSV preferred).
3. Any network diagrams you have.

Update the MAC address (OUI) (Manufacturer) List

The OUI (organizationally unique identifier) list is used to map device MACs to manufacturer names in your **Devices** list. If the list has changed since you installed your Conductor, you can now update it.

1. Log in to Conductor as a system administrator.
2. Go to **Settings** and open the **Diagnostics** tab.
3. Under **Actions**, select **Update OUI list**.

You now see updated OUI information on Device pages, and in the **OUI** column of the **Devices** list. See See MAC address OUI (Manufacturer) Information for Devices on page 115.

Connection Troubleshooting

Help if you're having trouble connecting Airwall Edge Services to your Airwall secure network.

Airwall Connectivity Tools

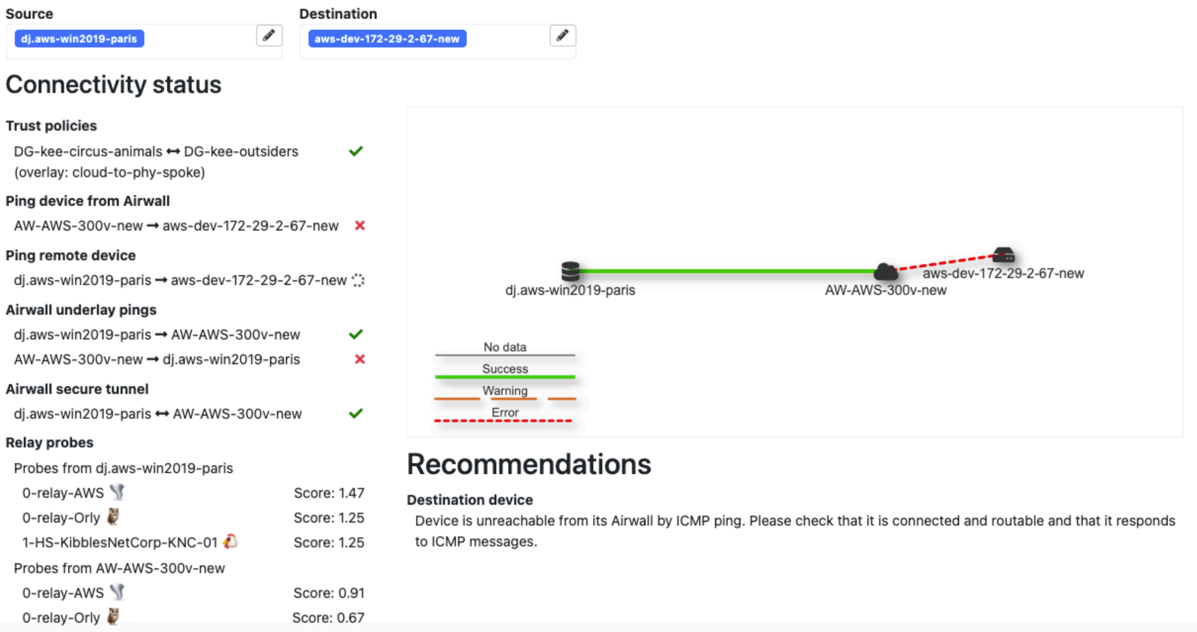
Conductor diagnostics include several tools for checking and troubleshooting connectivity.

Connectivity checker

Checks device to device connectivity.

Go to: **Visibility** > **Connectivity checker**

For more information, see Connectivity checker on page 486



Source: dj.aws-win2019-paris

Destination: aws-dev-172-29-2-67-new

Connectivity status

Trust policies

DG-kee-circus-animals ↔ DG-kee-outsiders (overlay: cloud-to-phy-spoke) ✓

Ping device from Airwall

AW-AWS-300v-new → aws-dev-172-29-2-67-new ✗

Ping remote device

dj.aws-win2019-paris → aws-dev-172-29-2-67-new

Airwall underlay pings

dj.aws-win2019-paris → AW-AWS-300v-new ✓

AW-AWS-300v-new → dj.aws-win2019-paris ✗

Airwall secure tunnel

dj.aws-win2019-paris ↔ AW-AWS-300v-new ✓

Relay probes

Probes from dj.aws-win2019-paris

0-relay-AWS	Score: 1.47
0-relay-Orly	Score: 1.25
1-HS-KibblesNetCorp-KNC-01	Score: 1.25

Probes from AW-AWS-300v-new

0-relay-AWS	Score: 0.91
0-relay-Orly	Score: 0.67

Recommendations

Destination device

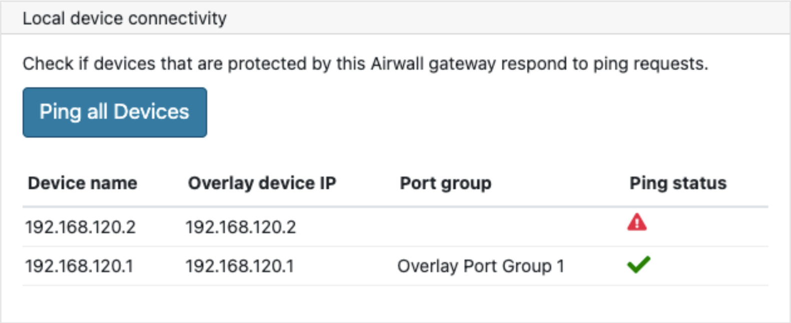
Device is unreachable from its Airwall by ICMP ping. Please check that it is connected and routable and that it responds to ICMP messages.

Local device connectivity

Checks that the devices protected by an Airwall Gateway can be reached from the Airwall Gateway.

Go to: **Airwalls** > **Diagnostics** > **Check connectivity** > **Local device connectivity**

This tool checks that the devices protected by an



Local device connectivity

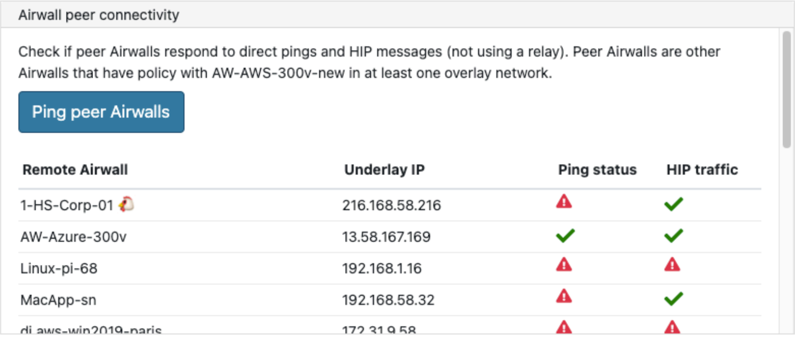
Check if devices that are protected by this Airwall gateway respond to ping requests.

Device name	Overlay device IP	Port group	Ping status
192.168.120.2	192.168.120.2		⚠
192.168.120.1	192.168.120.1	Overlay Port Group 1	✓

Airwall peer connectivity

Checks if peer Airwalls (Airwall Edge Services that have trust with this Airwall Edge Services) respond to direct pings and HIP messages (not using a relay).

Go to: **Airwalls** > **Diagnostics** > **Check connectivity** > **Airwall peer connectivity**



Airwall peer connectivity

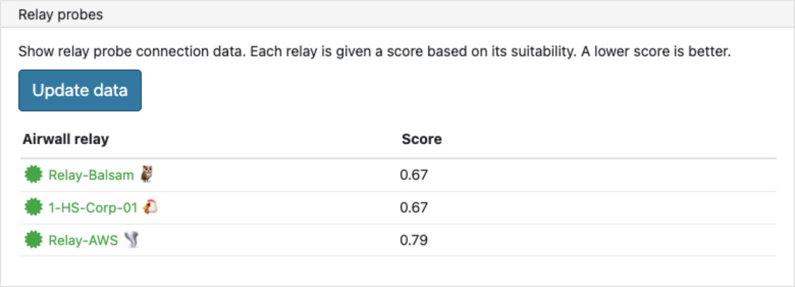
Check if peer Airwalls respond to direct pings and HIP messages (not using a relay). Peer Airwalls are other Airwalls that have policy with AW-AWS-300v-new in at least one overlay network.

Remote Airwall	Underlay IP	Ping status	HIP traffic
1-HS-Corp-01	216.168.58.216	⚠	✓
AW-Azure-300v	13.58.167.169	✓	✓
Linux-pi-68	192.168.1.16	⚠	⚠
MacApp-sn	192.168.58.32	⚠	✓
dj aws-win2019-paris	172.31.9.58	⚠	⚠

Relay probes

Checks the suitability of the relays that an Airwall Gateway has access to, using relay probe connection data. The score indicates each relay's suitability, with lower scores indicating more suitable relays.

Go to: **Airwalls** > **Diagnostics** > **Check connectivity** > **Relay probes**



Relay probes

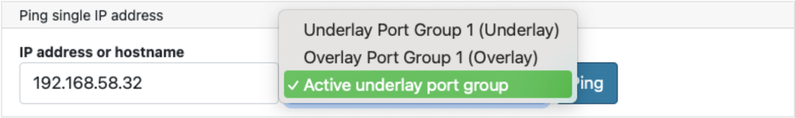
Show relay probe connection data. Each relay is given a score based on its suitability. A lower score is better.

Airwall relay	Score
Relay-Balsam	0.67
1-HS-Corp-01	0.67
Relay-AWS	0.79

Ping Single IP Address

Pings a specific IP address or hostname over a specific overlay or underlay port group, helping you determine where connectivity issues are happening.

Go to: **Airwalls** > **Diagnostics** > **Check connectivity** > **Ping single IP address**



Ping single IP address

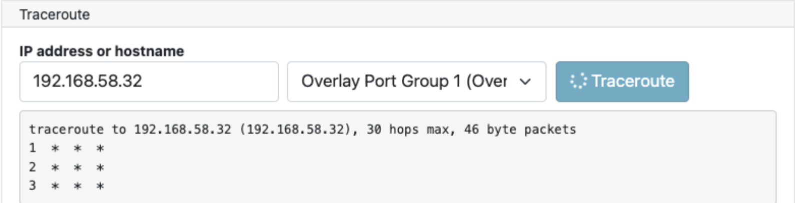
IP address or hostname: 192.168.58.32

Underlay Port Group 1 (Underlay)
Overlay Port Group 1 (Overlay)
✓ Active underlay port group
ing

Traceroute

Gives the traceroute to a specific IP address or hostname over a specific overlay or underlay port group. The traceroute maps the paths data packets take to their destination, and can show you where a failure is occurring.

Go to: **Airwalls** > **Diagnostics** > **Check connectivity** > **Traceroute**



Traceroute

IP address or hostname: 192.168.58.32

Overlay Port Group 1 (Over

```
traceroute to 192.168.58.32 (192.168.58.32), 30 hops max, 46 byte packets
1  *  *  *
2  *  *  *
3  *  *  *
```

Connectivity checker

The **Connectivity checker** does a full analysis of the connectivity between two devices in your Airwall secure network.

Note: For connectivity diagnostic tools for Airwall Edge Services, go to **Airwalls** > **Diagnostics** > **Check connectivity**. For more information, see Check Airwall Edge Service Connectivity on page 488.

Supported Versions	v3.1 and later Conductor, and Airwall Edge Services at any version, though results are enhanced with v3.1.
Required Role	• System or network administrators • Permissions to use the Airwall Edge Services that protect the devices between which you are checking connectivity.

Note: If you want to check an Airwall Agent or Server device that is operating in Disconnected mode, temporarily suspend Disconnected mode while you are running tests. See Disconnected Mode – Reduce Conductor traffic from Airwall Agents and Servers on page 99.

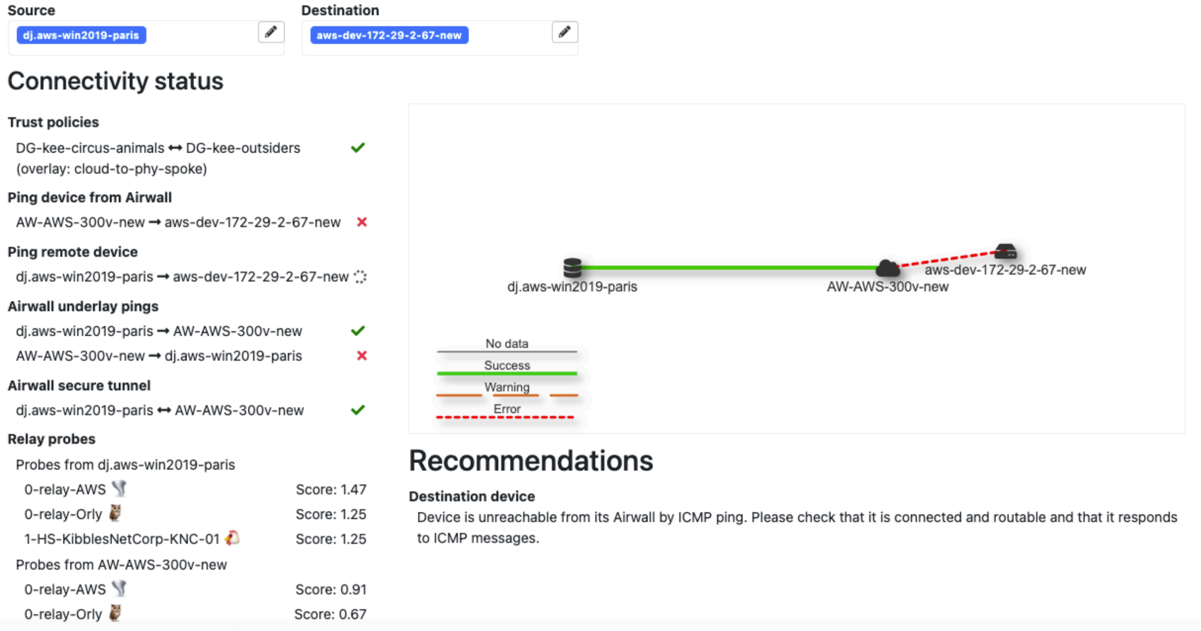
Note: If the Airwall Edge Service that the device is connected to is offline, see Troubleshoot Connection issues for offline Airwall Edge Services on page 489.

1. There are several ways to get to the **Connectivity checker** to check connectivity for a device in the network:
   - From the page for the device, select **Actions** > **Check connectivity**.
   - From an overlay network diagram, right-click a device or the connection line between two devices, and select **Check connectivity**.
   - Go to **Visibility** > **Connectivity tool**.
2. Under **Source**, select the device you want to check connectivity from.
3. Under **Destination**, select the device you want to check connectivity to.
4. Start a ping, or attempt to pass traffic, between the devices. Doing this provides the **Connectivity checker** with more information on device connectivity.
5. Select **Check connectivity**.
6. Once the checks are complete, see the **Recommendations** section for troubleshooting steps for any issues.

If both source and destination are online, the Conductor starts checking connectivity, and displays the results as they come in:

- ◌ (spinning circle) – Connectivity check in progress.
- ✓ (green check) – Connectivity check passed.
- ✕ (red x) – Connectivity check failed.
- Score: 1.25 (Score) – Relay probe suitability score. Lower scores mean more suitable to be used as a relay.

If there are connectivity issues, the Conductor shows recommendations for fixing the issues.



Source
dj.aws-win2019-paris

Destination
aws-dev-172-29-2-67-new

Connectivity status

Trust policies
DG-kee-circus-animals ↔ DG-kee-outsiders (overlay: cloud-to-phy-spoke) ✓

Ping device from Airwall
AW-AWS-300v-new → aws-dev-172-29-2-67-new ✗

Ping remote device
dj.aws-win2019-paris → aws-dev-172-29-2-67-new

Airwall underlay pings
dj.aws-win2019-paris → AW-AWS-300v-new ✓
AW-AWS-300v-new → dj.aws-win2019-paris ✗

Airwall secure tunnel
dj.aws-win2019-paris ↔ AW-AWS-300v-new ✓

Relay probes
Probes from dj.aws-win2019-paris
0-relay-AWS Score: 1.47
0-relay-Orly Score: 1.25
1-HS-KibblesNetCorp-KNC-01 Score: 1.25
Probes from AW-AWS-300v-new
0-relay-AWS Score: 0.91
0-relay-Orly Score: 0.67

Recommendations

Destination device
Device is unreachable from its Airwall by ICMP ping. Please check that it is connected and routable and that it responds to ICMP messages.

For more help in troubleshooting connectivity, see more Airwall Connectivity Tools on page 484. If the source or destination device is offline, see Troubleshoot Connection issues for offline Airwall Edge Services on page 489.

Check Airwall Edge Service Connectivity

Conductor diagnostics for Airwall Edge Services includes several tools for checking and troubleshooting connectivity.

Note: There is also a **Connectivity checker** that does a deeper analysis of device connections at **Visibility** > **Connectivity**. For more information, see Connectivity checker on page 486.

Supported Versions	v2.2.8 and later Conductor and Airwall Gateways
Required Role	System administrators, and network administrators with permissions to the edit the Airwall Gateways.

Note: If the Airwall Edge Service is offline, see Troubleshoot Connection issues for offline Airwall Edge Services on page 489.

Note: If you want to check a device that is operating in Disconnected mode, temporarily suspend it while running tests. See Disconnected Mode – Reduce Conductor traffic from Airwall Agents and Servers on page 99.

1. Go to **Airwalls** and open the Airwall Edge Service you want to check.
2. On the Airwall page, go to **Diagnostics** > **Check Connectivity**.
3. Select the tool you need and follow the suggestions for remedies in each tool. For more information on each tool, see Airwall Connectivity Tools on page 484.

You can also create packet capture and diagnostic reports, or a support bundle to send to Tempered Customer Success (Customer Success):

- Do a packet capture for an Airwall Gateway on page 482
- Create a diagnostic report for an Airwall Gateway on page 483
- Create a support bundle for an Airwall Gateway on page 481
- How to get support on page 181

Related concepts

Troubleshoot Connection issues for offline Airwall Edge Services on page 489

Related tasks

Connectivity checker on page 486

The **Connectivity checker** does a full analysis of the connectivity between two devices in your Airwall secure network.

Troubleshoot Connection issues for offline Airwall Edge Services

Here are the most common reasons an Airwall Edge Service is offline:

- **No power** – The Airwall Edge Service or device (for example, laptop or cell phone) is off. **Solution** – Make sure power is on and the device is booted up.
- **Port is blocked** – Port mapping is blocking traffic. **Solution** – Check that the following ports are open in your network firewall:

  - UDP 10500 - Check that both inbound and outbound connections are allowed.
  - TCP 8096 - Check that inbound connections are allowed.

  To verify that TCP 8096 is working through any firewall connections:

  ```
  netcat: nc -vz <Conductor-IP> port 8096
  ```
- **No network connection** – There is no connection between the Conductor and the Airwall Edge Service. **Solution** – Check that they are both connected to a network with routes to each other.
- **Device is in Disconnected mode** – An Airwall Agent or Server is in Disconnected mode. **Solution** – Temporarily suspend Disconnected mode while you troubleshoot.

If none of these suggestions help, see the additional troubleshooting topics below.

Device Connections

- Connectivity checker on page 486

Airwall Gateway Connections

- Check Airwall Edge Service Connectivity on page 488
- Troubleshoot Initial Airwall Gateway connections on page 491
- Airwall Agent or Server or Airwall Gateway using IPv6 has trouble connecting on page 489
- Bypass warning when connecting to the Conductor on page 491
- Capture network traffic on an Airwall Gateway on page 490

Airwall Agent or Server Connections

- Airwall Agent or Server or Airwall Gateway using IPv6 has trouble connecting on page 489

Conductor Connections

- Bypass warning when connecting to the Conductor on page 491

Airwall Agent or Server or Airwall Gateway using IPv6 has trouble connecting

If you have Airwall Edge Services that are using only an IPv6 address, they will only be able to connect to Airwall Edge Services that are using IPv4 addresses through a dual stack (IPv4 + IPv6) Airwall Relay. They also need to have relay policy with each other. Dual stack means the relay needs both IPv4 and IPv6 underlay addresses with global Internet connectivity.

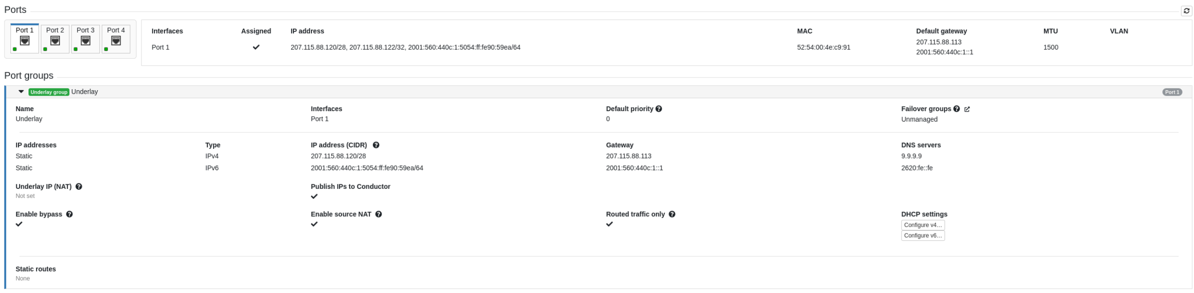
Requirement

You must have a dual-stack (IPv4 and IPv6) Internet connection and public IPv4 and IPv6 addresses for your Airwall Relay.

Set up a dual-stack Airwall Relay

1. Go to or create an Airwall Relay that has a dual-stack Internet connection.
2. Set up or open an underlay port group on the Airwall Relay.
3. Add both an IPv4 and an IPv6 address:

   Note: Select static or DHCP for the IP addresses, depending on your internet provider's configuration.



Interfaces	Assigned	IP address	MAC	Default gateway	MTU	VLAN
Port 1	✓	207.115.88.120/28, 207.115.88.122/32, 2001:560:440c:1:5054:ff:fe90:59ea/64	52:54:00:4e:c9:91	207.115.88.113 2001:560:440c:1::1	1500	

Name: Underlay

Interfaces: Port 1

Default priority: 0

Failover groups: Unmanaged

IP addresses	Type	IP address (CIDR)	Gateway	DNS servers
Static	IPv4	207.115.88.120/28	207.115.88.113	9.9.9.9
Static	IPv6	2001:560:440c:1:5054:ff:fe90:59ea/64	2001:560:440c:1::1	2620:fe::fe

Underlay IP (NAT): Not set

Publish IPs to Conductor: ✓

Enable bypass: ✓

Enable source NAT: ✓

Routed traffic only: ✓

DHCP settings

Static routes: None

4. Make sure the IPv4 and IPv6 devices that you want to communicate have trust between them on an overlay. See Configure Device Trust on page 427.

Capture network traffic on an Airwall Gateway

As part of the troubleshooting process, it is sometimes necessary to capture network traffic. The Airwall Gateway can capture traffic on the local interfaces as well as on the HIP tunnel from the Airwall Gateway to other Airwall Gateways.

All of these steps are done from a Conductor and require administrator permissions.

- Navigate to the Airwall Gateway you wish to capture from
- Select **Diagnostics**
- In Data capture, select **Start Packet Capture**
- Select the appropriate interface, if needed

Interface	Role	Usage
HIP tunnel	HIP Traffic	Use the HIP tunnel for protected traffic.
Internal	Internal Traffic	This captures the traffic that occurs within the local network.
Port 0	Underlay	This is the Port 2 (underlay) for traffic to/from the local network of the Airwall Gateway.
Port 1	Overlay	Use the Port 1 (overlay), for traffic to/from the protected device.

- Set any other options needed for the capture
- Click **Ok** to start the capture

CAUTION: The maximum file size is one quarter (1/4) of the available free space, so it is recommended that you set limits on the capture. In some models, such as the Airwall Gateway/HIPswitch 100, this can take up enough space to cause issues with upgrades.

Airwall Gateway link monitoring

Airwall Gateways have a utility to monitor its underlay network interfaces and determine if one is available for use.

Internet Control Message Protocol (ICMP) is a prerequisite for link monitoring to validate a link.

By default, an Airwall Gateway will prefer wired underlay interfaces to cellular or Wi-Fi.

2.1.x and later

Starting in v2.1.x, the Airwall Gateway has a link monitor that is fully configurable, allowing the following tunable options:

- Custom ping destinations (Conductor enabled by default)
- Ping rate (frequency), timeout, time to live (TTL), and failure count

- Disable ping monitors on active link

Troubleshoot Initial Airwall Gateway connections

Here are some things to check if you are having trouble connecting your Airwall Gateway to your Conductor or underlay network.

- Check that the information you've entered for your WiFi or cellular service are correct.
- If you have a wired connection, check that it is connected to correct port for your Airwall Gateway. See your platform guide for instructions.
- Try pinging:
  - Ping the Conductor in Airshell:

    ```
    airsh>> ping Conductor_IP_address
    ```
  - Ping a well-known service (such as Google DNS 8.8.8.8) to check for Internet connectivity:

    ```
    airsh>> ping 8.8.8.8
    ```
  - Ping the default gateway for your network.

  If pinging fails, get a packet capture from the Airwall Gateway and see where the ping is failing. For more information, see Do a packet capture for an Airwall Gateway on page 482.
- Check that the interface has IP. You can get the IP address using the Airshell status command:

  ```
  airsh>> status network

  airsh>> status cell

  airsh>> status wifi
  ```
- Check that the default route and link are up.
- Check that the following ports are open in your network firewall:
  - UDP 10500 - Check that both inbound and outbound connections are allowed.
  - TCP 8096 - Check that inbound connections are allowed.

  To verify that TCP 8096 is working through any firewall connections:

  ```
  netcat: nc -vz <Conductor-IP> port 8096
  ```

Conductor connectivity

Help for Conductor connectivity issues.

Bypass warning when connecting to the Conductor

Many browsers see the self-signed certificate on a new Conductor as a security risk. Here's how to proceed past the warning to the Conductor on several browsers. Sometimes after provisioning the Conductor, you will be able to bypass this warning. To prevent this error, Install a Custom CA Certificate Chain on page 239.

Google Chrome "Your connect is not private"	You may need to type `thisisunsafe` in the browser window to proceed past the warning. After you provision the Conductor, you will be able to bypass this warning by selecting Advanced and bypass.
Firefox	Select Advanced and then proceed to bypass.

Cloud Airwall Gateways and Conductor Troubleshooting

Links to topics for common issues on cloud Airwall Gateways and Conductor.

Enable ENA for an AWS Network Adapter	See https://www.claudiokuenzler.com/blog/882/cannot-start-aws-ec2-instance-ensure-enabled-ena

Get an AWS Airwall Gateway to pull the correct route table

If you've added a route table to a subnet in Amazon Web Services (AWS), but the Conductor isn't pulling the correct route table, here are some tips on troubleshooting.

This issue most commonly occurs when you've attached another interface (for example, port 3) and then rebooted the Airwall Gateway before you've associated the route table. In this case, the Conductor sees the new interface and checks the route table. When it doesn't find a specific one, it tries to find one, and it may not find the correct one. It doesn't recheck the route table once it's found one.

To avoid this issue, see Add an interface with an associated route table on a cloud Airwall Gateway on page 339.

1. Go to the AWS console, and detach your added interface from your Airwall Gateway.
2. Reboot the Airwall Gateway and wait until it comes back online in the Conductor.
3. Back in the AWS console, re-attach your 3rd interface to the Airwall Gateway.
4. Again, reboot the Airwall and wait until it comes back online on the Conductor.

You should get the correct route table now.

Add an interface with an associated route table on a cloud Airwall Gateway

If you need to attach a route table to an interface you're adding in AWS or Azure, you'll need to add the interface and attach the route table before you reboot the Airwall Gateway.

Supported versions	• v3.0.0 Conductors • AWS and Azure Cloud Airwall Gateways
Supported Roles	AWS or Azure cloud administrator, and Conductor system administrator , or network administrator with permissions to create cloud Airwall Gateways

CAUTION: If you reboot the Airwall Gateway before you've associated the route table, the Conductor sees the new interface and checks the route table. When it doesn't find a specific one, it tries to find one, and it may not find the correct one. It doesn't recheck the route table once it's found one.

For the most up-to-date information, see the documentation for your respective cloud provider.

If you've already rebooted, see Get an AWS Airwall Gateway to pull the correct route table on page 492.

1. Associate the route table to your new interface (for example, Port 3) subnet.
2. Create a new interface (for example, Port 3).
3. Attach the new interface to the Airwall Gateway.
4. Reboot the Airwall Gateway.

Here are some suggested resources for AWS and Azure documentation on multiple NICs:

AWS:

- **Associate a protected subnet with a protected route table first**: https://docs.aws.amazon.com/vpc/latest/userguide/WorkWithRouteTables.html#AssociateSubnet
- **Attach an interface to an instance**: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#working-with-enis

Azure:

- **Associate a protected subnet with a protected route table first**:https://docs.microsoft.com/en-us/azure/virtual-network/manage-route-table#associate-a-route-table-to-a-subnet
- **Attach an interface to an instance**:https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface-vm

Handle IP Conflicts

Learn how to identify and manage IP conflicts in your Airwall secure network.

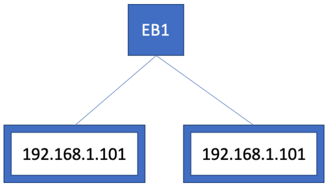
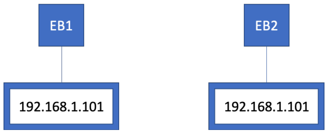
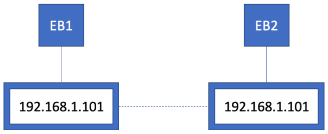
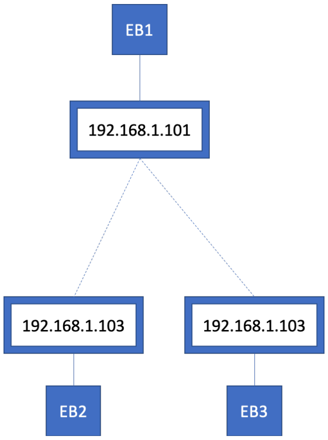
Your Airwall secure network can manage devices with the same IP as long as these duplicate IPs:

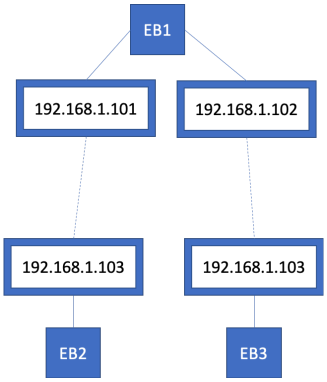
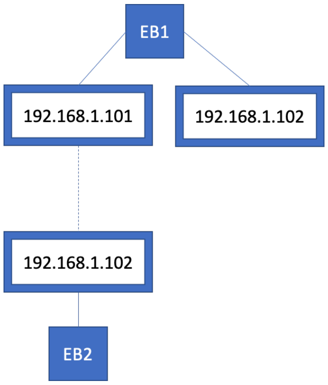
- Are not on the same Airwall Gateway, AND
- Do not have direct, indirect, or implicit policy between them in an overlay.

You can have duplicate IPs on the same overlay, as long as there is no policy between them.

If you are making a change that causes an IP conflict, the Conductor gives you an error message with information on the conflict.

The following diagrams show examples of IP conflicts, with suggestions for removing the conflict besides changing one of the IPs. If you want to have policy between the two, you have to change on of the IP addresses:

Conflict	No Conflict
Duplicate IPs on an Airwall Gateway  	Duplicate IPs on different Airwall Gateways, in the same overlay, but with no policy between them. 
Duplicate IPs (in the same or different overlays) with policy to each other  	Give devices with the same IP a NAT overlay device IP. See Resolve IP conflicts by giving duplicate devices a NAT IP address on page 494.
Duplicate IPs in an overlay with policy to a shared IP  EB1 192.168.1.101 192.168.1.103 192.168.1.103 EB2 EB3	Duplicate IPs in an overlay with policy to IPs on different Airwall Gateways, or give one of the devices a NAT overlay device IP. See Resolve IP conflicts by giving duplicate devices a NAT IP address on page 494.

Conflict	No Conflict
Indirect conflict – Duplicate IPs in an overlay with policy to IPs on a shared Airwall Gateway.  EB1 192.168.1.101 192.168.1.102 192.168.1.103 192.168.1.103 EB2 EB3	Give devices with the same IP a NAT overlay device IP. See Resolve IP conflicts by giving duplicate devices a NAT IP address on page 494
Implicit conflict – IP in an overlay with policy to an IP that shares an Airwall Gateway with the same IP.  EB1 192.168.1.101 192.168.1.102 192.168.1.102 EB2	Give devices with the same IP a NAT overlay device IP. See Resolve IP conflicts by giving duplicate devices a NAT IP address on page 494

Resolve IP conflicts by giving duplicate devices a NAT IP address

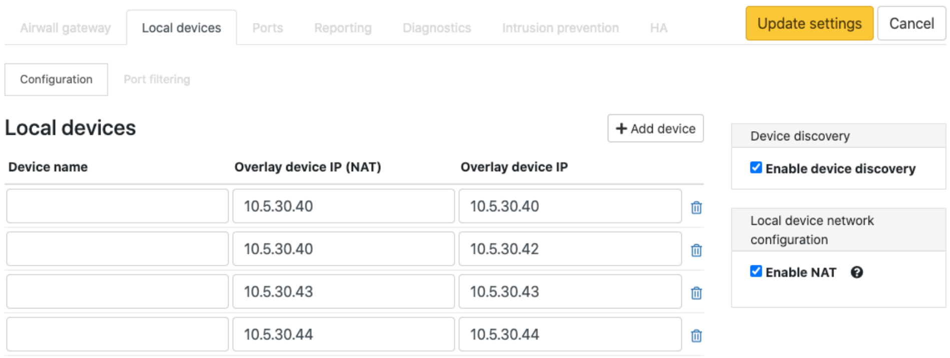
If you have an IP conflict, and want to have policy (set trust) between the conflicting IPs, you can often resolve the issue by giving any devices with duplicate IP addresses a NAT IP address.

It is important to understand the difference between the two IPs: overlay device IP and overlay device IP (NAT). The overlay device IP is both the local and overlay IP unless NAT is turned on. If NAT is on, then the overlay device IP is only the local IP and the NAT IP is the overlay IP. Other Airwall Gateways only see the overlay IP, so the local IP cannot cause a conflict on them.

It is possible to change the local IP, but you have to be able to change it on the device itself. It is often easier to just NAT the IP if your conflict falls into one of the categories where NAT will fix it (see Handle IP Conflicts on page 492). Changing the device's actual IP and updating its overlay device IP should be reserved for situations that cannot otherwise be solved.

To give a device a NAT IP:

1. On the device's host Airwall Gateway, open the **Local devices** tab, **Configuration** subtab, and select **Edit Settings**.
2. On the right, under **Local device network configuration**, check **Enable NAT** .
3. In the **Local devices** table, enter a unique **Overlay device IP (NAT)** address for any devices that will conflict with another device that you want to create policy to (direct, indirect, or implicit – see Handle IP Conflicts on page 492).



Local devices

Device name	Overlay device IP (NAT)	Overlay device IP
	10.5.30.40	10.5.30.40
	10.5.30.40	10.5.30.42
	10.5.30.43	10.5.30.43
	10.5.30.44	10.5.30.44

Device discovery

☑ Enable device discovery

Local device network configuration

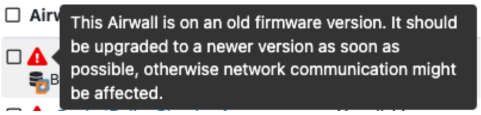
☑ Enable NAT

4. Select **Update Settings**.

Update v2.1.x Airwall Edge Services for the v3.0.0 Conductor

With this release, any Airwall Edge Services running v2.1.x releases will show an error recommending you update them. After updating Conductor to v3.0.0 or later, you won't be able to configure v2.1.x devices from the Conductor until you update them.

The red exclamation point next to the Airwall Edge Service indicates one that needs to be updated.



This Airwall is on an old firmware version. It should be upgraded to a newer version as soon as possible, otherwise network communication might be affected.

Updatev2.1.x Airwall Edge Services

1. Update any Airwall Edge Services running v2.1.x firmware to a v2.2.x firmware version first.
2. If desired, then update to v3.0 or later.

Configure v2.1.x Airwall Edge Services in a v3.0.0 or later Conductor

To configure v2.1.x Airwall Edge Services after updating the Conductor to v3.0.0 or later, you must update those services to v2.2.x or later as described above.

Factory Reset a Conductor

Reset a Conductor to return it to the original factory settings. If an Airwall Edge Service is not online at the time of a factory reset, and an SRV record is configured for the MAP server in DNS, the Conductor performs these actions when the Airwall Edge Service next comes online.

Note: Factory resetting a Conductor requires console access with a VGA monitor and USB keyboard.

To reset the Conductor:

1. In the console at the login prompt, enter the username `<factoryreset>`.
2. At the password prompt, enter the password `<factoryreset>`.
   Conductor will be factory reset.

Once a Conductor is factory reset, all Airwall Edge Services must be factory reset to re-connect to the Conductor, unless the Conductor configuration is restored from a Conductor database backup. To avoid this, download a Conductor database backup prior to doing a factory reset.

Factory Reset a Virtual Conductor

You can reset a virtual Conductor to return it to the original settings.

Once a Conductor is factory reset, all Airwall Edge Services must be factory reset to reconnect to the Conductor, unless the Conductor configuration is restored from a Conductor database backup. To avoid this, download a Conductor database backup prior to factory resetting a Conductor.

1. Display the console for the Conductor instance you would like to reset.
2. Enter `factoryreset` for user name and `factoryreset` for the password.

The Conductor will now revert to its factory default settings.

Reboot an Airwall Gateway

Rebooting an Airwall Gateway is one of several diagnostic techniques that you can use to help troubleshoot. How you reboot and Airwall Gateway varies depending on the model. Be careful with the reset button, because for some models, pressing for an extended time factory resets the Airwall Gateway.

For instructions on rebooting your Airwall Gateway, refer to the platform guide that came with your Airwall Gateway, or see Documentation Downloads on page 810.

Factory Reset an Airwall Gateway

You can reset Airwall Gateways to return them to the original factory settings. If an Airwall Gateway is not online at the time of a factory reset, and an SRV record is configured for the MAP server in DNS, the Conductor performs these actions when the Airwall Gateway next comes online.

To factory reset your Airwall Gateway, use the `factoryreset` command. This command reverts the Airwall Gateway to factory settings, erasing all configuration settings, so use it with caution.

```
login: factoryreset
password: factoryreset
```

Once an Airwall Gateway is in the factory-reset state, it is placed into the unmanaged mode and one of the following scenarios will occur:

- The Airwall Gateway page in the Conductor shows a status as offline. Once the Airwall Gateway is factory reset, all devices attached to the Airwall Gateway are removed along with any additional user-provided information, such as name, location, overlay network and wireless configurations. To re-deploy a factory-reset Airwall Gateway, you must reconfigure the Airwall Gateway to point to the Conductor. Once configured, the Airwall Gateway appears in the Conductor with "factory reset" appended to its name.
- If you've configured a DNS SRV record for your Conductor, the Airwall Gateway automatically re-connects. After the Airwall Gateway connects, the Conductor removes it from any existing overlay networks, and appends (factory reset) to its name. The Conductor also removes all devices attached to the Airwall Gateway, as well as any additional user-provided information, such as human-friendly name or location. Cached overlay network and wireless configurations are also removed.

Revoke and Reactivate an Airwall Edge Service

If an Airwall Gateway, Airwall Agent, or Airwall Server is lost, stolen or damaged, you can revoke it to remove its access to your Airwall secure network. You must be a manager of all overlay networks to which the Airwall Edge Service belongs. Once revoked, the Airwall Edge Service will not be able to establish or receive communications on your Airwall secure network.

To revoke an Airwall Edge Service:

1. Log in as an administrator with manager access rights to the overlays the Airwall Edge Service belongs to.
2. Go to the **Airwalls** page, and find the Airwall Edge Service you want to revoke.
3. Open the actions menu with the arrow to the to the right of the Airwall Edge Service, and select **Revoke**.
4. In the confirmation dialog, click **Apply**.

The Airwall Edge Service is revoked and "revoked" is added to its name. By default, revoked Airwall Edge Services are not displayed in the Conductor. You can display them again by choosing **Revoked** in the **Show All Airwalls** box.

To re-activate a revoked Airwall Edge Service:

1. Log in as an administrator with manager access rights to the overlays the Airwall Edge Service belongs to.
2. Go to the **Airwalls** page.
3. In the **Show all Airwalls** box, select **Revoked**, and find the revoked Airwall Edge Service.
4. Select the arrow to the to the right of the Airwall Edge Service you want to re-activate.
5. Select **Re-activate** and in the confirmation dialog, click **Apply**.
   The Airwall Edge Service is re-activated, and **"(revoked)"** is removed from its name.

Note: Only System Administrators have permission to re-activate revoked Airwall Edge Services.

Troubleshoot MAP2 Protocol Issues

Conductors and Airwall Gateways running versions 2.0.0 or greater use a new metadata protocol (MAP2). MAP2 allows for better scalability and performance than the previously implemented IF-MAP protocol.

Note: A Conductor running 2.0.x and 2.1.x can also run the legacy IF-MAP protocol to support any Airwall Edge Services running version 1.x.

To help verify the Conductor and Airwall Edge Service are communicating, the Airwall Edge Service maintains the following data:

1. Signature of the Conductor identity
2. The Conductor's shared Airwall Edge Service key

The shared Airwall Edge Service key can be viewed and changed in the Conductor from **Settings** > **Advanced** > **Shared HIPservice key**.

If neither of those values match, an Airwall Edge Service will not connect to the Conductor. A factory reset will be required for an Airwall Gateway to connect to a different Conductor.

Note: Beginning in version 2.1.0, the shared key provided to the Airwall Edge Service is now encrypted. If an Airwall Edge Service was previously connected to a 2.0.x Conductor and refuses to connect to a 2.1.x Conductor that has the correct shared key, disabling shared key encryption might help.

You can disable shared key encryption from the Conductor by going to **Settings** > **Advanced** > **Disable shared key encryption**.

Note: If you disable shared key encryption, enable it again after all Airwall Edge Services have successfully connected.

Measure wireless signal strength - WiFi and cellular

There are two methods to determine the signal strength of a WiFi-enabled Airwall Gateway.

1. Go to **Airwalls** and select an Airwall Edge Service from the list. Click **Reporting**, where the signal strength is reported every five minutes.
2. Place the Airwall Gateway in diagnostic mode. See Put an Airwall Gateway into diagnostic mode on page 478 for more information.
3. Once the Airwall Gateway is in diagnostic mode, select **Status** on the diagnostic page.
4. The wireless signal strength is displayed. Refresh the diagnostic mode page to update the signal strength. Signal strength is updated every 5 seconds.

Security Notices, Advisory Notices, and Product Bulletins

This section contains important information such as security vulnerabilities, end-of-life notices, and other product updates.

Recent notices and bulletins

- Software end of life for Windows 7 and 32-bit Windows Airwall Agents on page 504
- T-Mobile – Required Cellular Firmware Update for 110g on page 498

Security Notices

Check this page for the latest security updates for Tempered products. They are listed by year.

2021	
Log4j Java Vulnerability - Not affected	**Tempered Products are not impacted by Apache log4j Vulnerability (CVE-2021-44228)** – Tempered is aware of the vulnerability and has completed verification that **this issue does not affect Tempered's products** including Conductor, Airwall Gateways, and Airwall Agents and Servers.
2020	
Urgent/11 - Not affected	Urgent/11, a security vulnerability which resides in VxWorks' TCP/IP stack, does not affect the Tempered Airwall solution. Urgent/11 is limited to the VxWorks real-time operating system.

Advisory Notices

The following is a complete list of our active advisory notices.

AWS and Azure Linux OS Versions End of Support

Amazon Web Services and Azure cloud providers have announced that they will no longer support Ubuntu16 and Centos7 Linux servers that are reaching the end of support by their providers.

Affected Linux OS Versions	• Ubuntu16 • Centos7
End of Support Date	Mar 31, 2022

Tempered also will no longer support these versions on these cloud platforms after the end of support date. Tempered may continue to support these platforms for non-cloud deployments and for cloud providers that still support them.

For more information, see the announcements from the Linux OS providers.

T-Mobile – Required Cellular Firmware Update for 110g

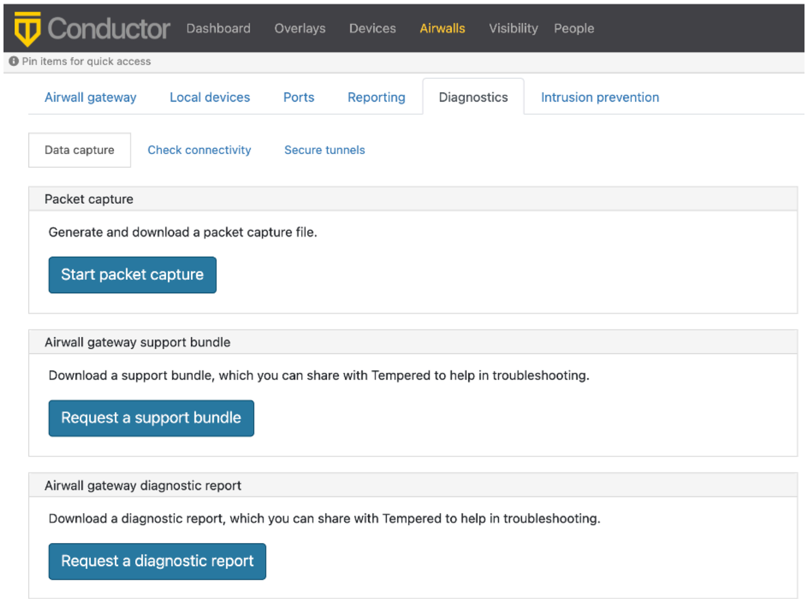
Quectel released guidance indicating T-Mobile IPv4 settings needed to be updated. This cellular firmware update applies the required changes per Quectel guidance.

Supported Versions	v2.2.0 and later 110g Airwall Gateways and Conductor
Supported Cellular Services	• **T-Mobile on 110g** - Required.

Check if you need the update

1. In the Conductor, go to **Airwalls**, and open the page for the Airwall Gateway 110g or Advantech ICR-32xx that you want to check.
2. Open **Diagnostics**.

3. Select **Request a diagnostic report**.



Packet capture

Generate and download a packet capture file.

Airwall gateway support bundle

Download a support bundle, which you can share with Tempered to help in troubleshooting.

Airwall gateway diagnostic report

Download a diagnostic report, which you can share with Tempered to help in troubleshooting.

4. Wait for it to build the report, and then download it.
5. Open the report and search for `Cellular Firmware package revision`. Check that it shows 923f147.

If you are checking several Airwall Gateways, tag the ones that are not updated so you can easily search for them when applying the update.

Update your Cellular Firmware

1. Check that your Conductor has the cellular firmware update, or download the "Hotfix for T-Mobile IPv4 settings Airwall Gateway 110 (filename is `Airwall-110_cellfw-923f147-130_package`) from Hotfixes on page 548 or Cellular modem firmware on page 538.
2. If you downloaded the file, in the Conductor, upload the cellular firmware packages:
   a) Go to **Settings** > **General Settings**.
   b) Under **Firmware updates**, select **Upload firmware**.
   c) Select **Choose file**, and select the firmware package you downloaded.
   d) Select **Upload**.
3. Go to **Airwalls**, and select all of your 110g Airwall Gateways.
4. Select **Airwall actions** > **Install Hotfix**.
5. Under **Update available**, select `cellfw-923f147` for each Airwall Gateway.
6. Select **Apply**. The new firmware will be installed as each Airwall Gateway connects to the Conductor.

Note: You can also find the firmware update under **Settings** > **Firmware updates** and select **Install**.

Tip: After you've updated these Airwall Gateways, use **Airwall actions** > **Edit tags** and tag them (with something like "Ready for IPv4 T-Mobile update") to indicate they've been updated.

3G Sunset – Required Cellular Firmware Update for 110g

AT&T Turned off their 3G network on Feb 22, 2022, and T-Mobile is turning off their 3G network on Jul 1, 2022. This change affects the Quectel modems on the 110g Airwall Gateway, and any AV3200g/u Airwall Gateways installed before Dec 12, 2021. If you are operating one of these Airwall Gateways using an AT&T or TMobile cellular connection, you should install new cellular firmware on them before the respective shutoff date.

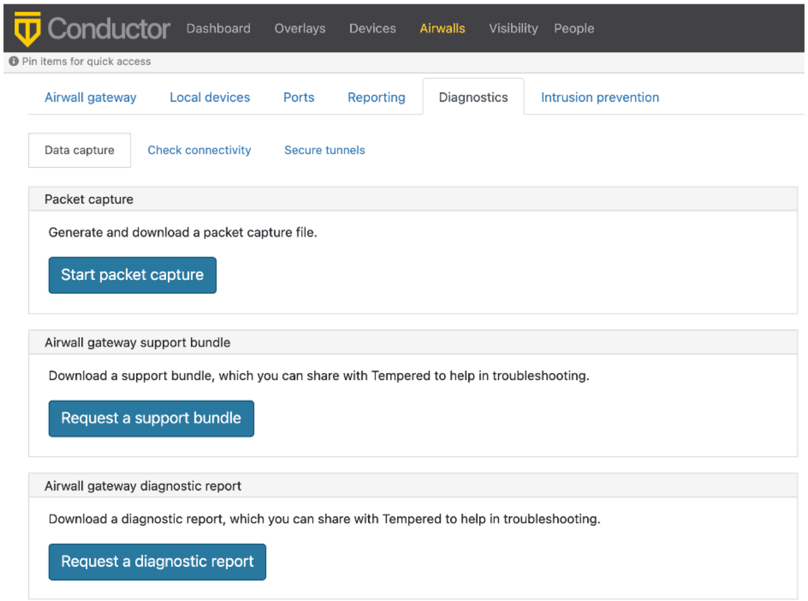
Warning: To avoid disruptions in your AT&T or T-Mobile cellular service, you must update your cellular firmware on 110g Airwall Gateways before 2/22/22 (AT&T) or 07/01/22 (T-Mobile). If you do not, you will have to have an ethernet connection or perform on-site diagnostics for all impacted Airwall Gateways to restore reliable cell connectivity.

Attention: If you already updated Airwall Gateways that are using T-Mobile cellular – Install the latest (build 125) update to correct any issues.

Supported Versions	v2.2.0 and later Airwall Gateways and Conductor
Supported Cellular Services	• **AT&T** - Required • **T-Mobile on 110g** - Required. • **T-Mobile on Advantech ICR-32xx** – Not certified by Advantech. • **All others** - Optional

Check if you need the update

1. In the Conductor, go to **Airwalls**, and open the page for the Airwall Gateway 110g or Advantech ICR-32xx that you want to check.
2. Open **Diagnostics**.
3. Select **Request a diagnostic report**.

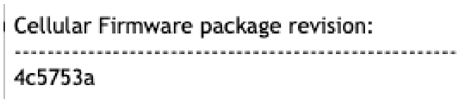


Generate and download a packet capture file.

Download a support bundle, which you can share with Tempered to help in troubleshooting.

Download a diagnostic report, which you can share with Tempered to help in troubleshooting.

4. Wait for it to build the report, and then download it.
5. Open the report and search for `Cellular Firmware package revision`. Check that it shows 4c5753a:



```
Cellular Firmware package revision:
----------------------------------------------------------
4c5753a
```

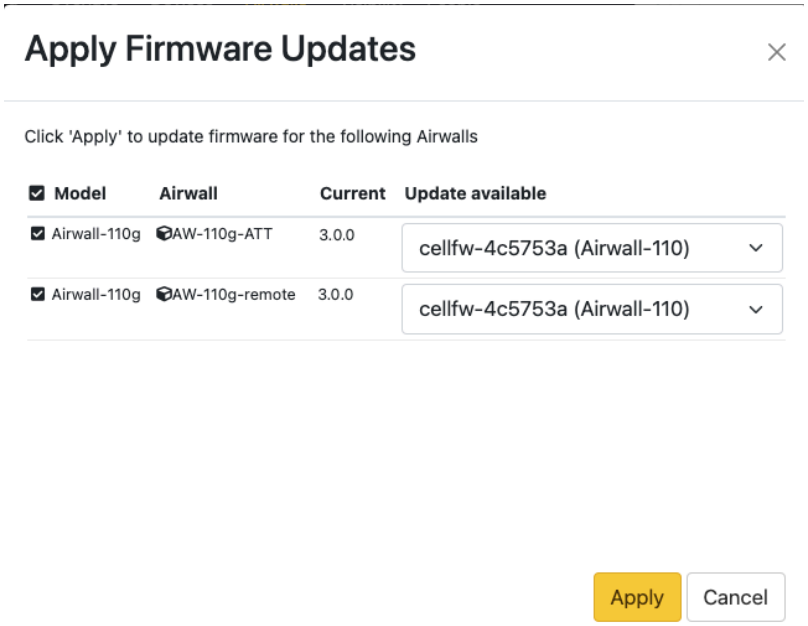
If you are checking several Airwall Gateways, tag the ones that are not updated so you can easily search for them when applying the update.

Update your Cellular Firmware

1. Check that your Conductor has the cellular firmware update, or download the "Hotfix for 3G Sunset Airwall Gateway 110" (filename is `Airwall-110_cellfw-4c5753a-125_package`) or Advantech 32xx (filename is `Airwall-112_cellfw-4c5753a-125_package`) from Hotfixes on page 548 or Cellular modem firmware on page 538.
2. If you downloaded the file, in the Conductor, upload the cellular firmware packages:
   a) Go to **Settings** > **General Settings**.
   b) Under **Firmware updates**, select **Upload firmware**.
   c) Select **Choose file**, and select the firmware package you downloaded.

   d) Select **Upload**.

3. Go to **Airwalls**, and select all of your 110g (or Advantech, if needed) Airwall Gateways.
4. Select **Airwall actions** > **Install Hotfix**. These images show updating 110g Airwall Gateways.



Apply Firmware Updates

Click 'Apply' to update firmware for the following Airwalls

☑ Model	Airwall	Current	Update available
☑ Airwall-110g	AW-110g-ATT	3.0.0	cellfw-4c5753a (Airwall-110)
☑ Airwall-110g	AW-110g-remote	3.0.0	cellfw-4c5753a (Airwall-110)

5. Under **Update available**, select `cellfw-1dfe737` for each Airwall Gateway.
6. Select **Apply**. The new firmware will be installed as each Airwall Gateway connects to the Conductor.

Note: You can also find the firmware update under **Settings** > **Firmware updates** and select **Install**.

Tip: After you've updated these Airwall Gateways, use **Airwall actions** > **Edit tags** and tag them (with something like "Ready for 3G Sunset") to indicate they've been updated.

Auth0 Update does not affect OpenID Connect Integration

The Auth0 update deprecating fixed length authorization codes and access tokens should have no effect on Auth0 authentication integration with an Airwall secure network.

Airwall integrated Auth0 in a way that is not affected by this update.

AT&T 3G Sunset – Required Cellular Firmware Update for 110g

AT&T is turning off their 3G network on 2/22/22, which affects the Quectel modems on the 110g Airwall Gateway, and any AV3200g/u Airwall Gateways installed before Dec 12, 2021. If you are operating one of these Airwall Gateways using an AT&T cellular connection, you should install new cellular firmware on them before the AT&T shutoff date.

Warning: To avoid disruptions in your AT&T cellular service, you must update your cellular firmware on 110g Airwall Gateways before 2/22/22. If you do not, you will have to have an ethernet connection or perform on-site diagnostics for all impacted Airwall Gateways to restore reliable cell connectivity.

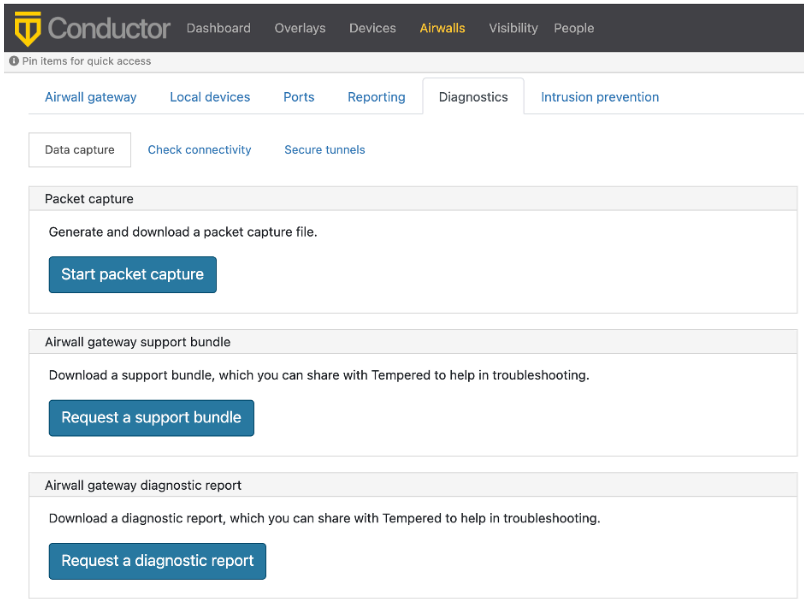
Attention: If you already updated Airwall Gateways that are using T-Mobile cellular – Install the latest (build 125) update to correct any issues.

Supported Versions	v2.2.0 and later Airwall Gateways and Conductor
Supported Cellular Services	• **AT&T** - Required • **T-Mobile on 110g** - Supported. • **T-Mobile on Advantech ICR-32xx** – Not certified by Advantech.

- **All others** - Optional

Check if you need the update

1. In the Conductor, go to **Airwalls**, and open the page for the Airwall Gateway 110g or Advantech ICR-32xx that you want to check.
2. Open **Diagnostics**.
3. Select **Request a diagnostic report**.



Packet capture

Generate and download a packet capture file.

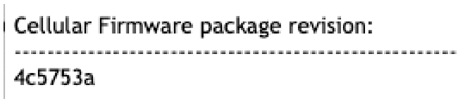
Airwall gateway support bundle

Download a support bundle, which you can share with Tempered to help in troubleshooting.

Airwall gateway diagnostic report

Download a diagnostic report, which you can share with Tempered to help in troubleshooting.

4. Wait for it to build the report, and then download it.
5. Open the report and search for `Cellular Firmware package revision`. Check that it shows 4c5753a:

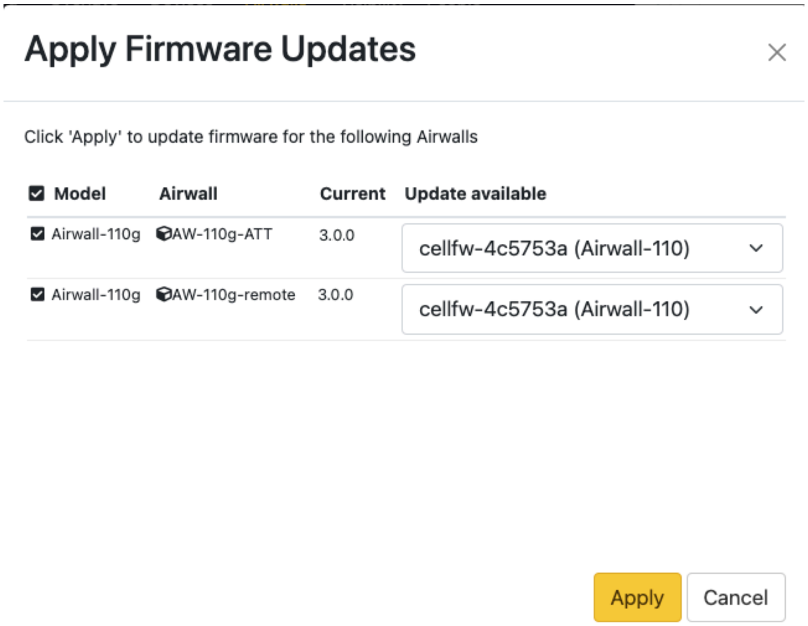


```
Cellular Firmware package revision:
------------------------------------------------------------
4c5753a
```

If you are checking several Airwall Gateways, tag the ones that are not updated so you can easily search for them when applying the update.

Update your Cellular Firmware

1. Check that your Conductor has the cellular firmware update, or download the "Hotfix for AT&T 3G Sunset Airwall Gateway 110" (filename is `Airwall-110_cellfw-4c5753a-125_package`) or Advantech 32xx (filename is `Airwall-112_cellfw-4c5753a-125_package`) from Hotfixes on page 548 or Cellular modem firmware on page 538.
2. If you downloaded the file, in the Conductor, upload the cellular firmware packages:
   a) Go to **Settings** > **General Settings**.
   b) Under **Firmware updates**, select **Upload firmware**.
   c) Select **Choose file**, and select the firmware package you downloaded.
   d) Select **Upload**.
3. Go to **Airwalls**, and select all of your 110g (or Advantech, if needed) Airwall Gateways.
4. Select **Airwall actions** > **Install Hotfix**. These images show updating 110g Airwall Gateways.



Apply Firmware Updates

Click 'Apply' to update firmware for the following Airwalls

☑ Model	Airwall	Current	Update available
☑ Airwall-110g	AW-110g-ATT	3.0.0	cellfw-4c5753a (Airwall-110)
☑ Airwall-110g	AW-110g-remote	3.0.0	cellfw-4c5753a (Airwall-110)

5. Under **Update available**, select `cellfw-1dfe737` for each Airwall Gateway.

6. Select **Apply**. The new firmware will be installed as each Airwall Gateway connects to the Conductor.

Note: You can also find the firmware update under **Settings** > **Firmware updates** and select **Install**.

Tip: After you've updated these Airwall Gateways, use **Airwall actions** > **Edit tags** and tag them (with something like "Ready for AT&T Sunset") to indicate they've been updated.

Upgrade Airwall Gateway 100e or Airwall Gateway 100g to newer firmware

Upgrade Airwall Gateway 100 to version 2.2 may result in a non-functional unit due to drive space issues.

Advisory ID:	Tempered-201910A-001
Version:	2.2
Updated:	10/01/2019

Description

When a Airwall Gateway 100e or 100g unit has been running for an extended period of time, the unit may run out of space on the temporary drive. Before performing an upgrade to the latest firmware, you must reboot the Airwall Gateway prior to installing the firmware update. If this is not done, the Airwall Gateway will not complete the upgrade properly and may result in a non-functional Airwall Gateway.

Affected Products

- Airwall Gateway 100e
- Airwall Gateway 100g

Processor Speculative Execution and Indirect Branch Prediction Vulnerabilities

The Spectre and Meltdown vulnerabilities in modern processor architecture optimizations, allow unprivileged local attackers to read arbitrary memory without restrictions.

Advisory ID:	Tempered-201801A-001
CVEs:	CVE-2017-5715, CVE-2017-5753, CVE-2017-5754
Version:	2.0

Updated:	2/21/2018
Status:	Interim

Overview

Impact

Successful vulnerability exploitation requires the attacker's ability to run code on the targeted machine.

Airwall Gateway & Conductor

Airwall Gateway and Conductor are purpose-built systems that do not allow remote or local system login, execution/installation of arbitrary code, nor the addition of operating system users. This design does not expose them to Spectre and Meltdown attacks.

HIPApps

Airwall Agent and Airwall Server are exposed to Spectre and Meltdown vulnerabilities through the hardware they are installed on. Work with your operating system and hardware vendors to receive the appropriate mitigation software and/or microcode.

Virtual Airwall Gateways & Conductor

Virtualized Airwall Gateway, Virtualized Conductor, and Cloud Airwall Gateway are vulnerable to Spectre and Meltdown through the hypervisor hardware which hosts them. Work with your hypervisor, cloud, and/or hardware vendors to receive the appropriate mitigation software and microcode.

Affected Products

- None directly
- Airwall Agents and Servers and Virtuals via the host hardware

Remediation

- Airwall Gateway and Conductor – none
- Airwall Agents and Servers and Virutals: Mitigation updates for the host operating system and/or hardware microcode

References

- https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html
- http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5715
- http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5753
- http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5754
- https://spectreattack.com/

Product Bulletins

The following is a complete list of our active product bulletins.

For pre-2.1.x advisories and bulletins, please see pre-2.2.3 Advisory Notices and Product Bulletins.

Software end of life for Windows 7 and 32-bit Windows Airwall Agents

Tempered is announcing the end of Airwall Agent updates for older Windows versions, including Windows 7 and all 32-bit versions.

Product versions:	Airwall Agents for Windows 7 and all 32-bit Windows operating systems
Effective date:	Jul 29, 2022

Tempered will no longer provide updates for Windows 7 or 32-bit Windows Airwall Agents.

You can continue using and getting support for current Windows 7 and 32-bit Windows Airwall Agents. If you choose to update your Windows operating systems to a version that supports 64-bit Windows Airwall Agents, see the recommended update path at Manage Versions of Airwall Agents and Servers on page 126. If you require additional planning assistance, please contact your solution architect or Tempered Customer Success at https://tempered.force.com/TemperedSupportCenter/s/ or email Customer Success.

Software support end of life for versions 2.1.x and earlier

Tempered is announcing our intent to end support for software versions 2.1.x and earlier on March 31, 2022.

Platforms:	All platforms
Product versions:	v2.1.x and earlier
Effective date:	March 31, 2022

After the effective date, Tempered will no longer provide troubleshooting services nor develop hot fixes for deployments running v2.1.x or earlier software.

Start planning to update your deployments to the latest Airwall software and firmware releases as soon as possible. For information about update planning, including a recommend update path, see Manage Versions of Airwall Agents and Servers on page 126. If you require additional planning assistance, please contact your solution architect or Tempered Customer Success at https://tempered.force.com/TemperedSupportCenter/s/ or email Customer Success.

Platform end-of-life for Airwall Gateway/ HIPswitch 100 series

Tempered announces the End of Life schedule for the Airwall Gateway/HIPswitch 100 series platforms.

End of life schedule for the 100 series

Date	Milestone	Description
10/30/2019	End of Sale	Last date on which the platform may be purchased
5/24/2021	Last supported Software version	The 100 series support v2.2.x software versions. Attempts to install 3.x or later versions will fail.
10/30/2021	Last Full Term MSMU Renewal	Last date a MSMU contract may be renewed for a full 12-month term. MSMU contracts apply only to 300 appliance products with perpetual software licenses. Contracts renewed after this date are required to end no later than 01/01/2022.
10/1/2022	Platform End of Life	Date on which the platform is no longer supported by Tempered.

Multiple-spoke HIPswitch Deployment Tunnel Issues

Hotfix available for tunnel issues in multiple-spoke (over 16) Hub-and-Spoke deployments.

Affected platforms:	HS-150 HS-250 HS-300 HS-400 HS-500
Affected product versions:	2.2.2

Note:

This affects physical, virtual, and cloud Airwall Gateways.

Issue – There is a bug in the HIP tunnel update that can be triggered when you are using Autoconnect and more than 16 spokes on a Hub-and-Spoke deployment. The symptom of this bug is the short-term drop of a HIP tunnel (from 2-3 minutes). This affects a random tunnel or tunnels once every hour.

Solution - Upgrade to 2.2.2, and then download hotfix HF-12219 and apply it to the hub Airwall Gateway of your network.

Download - https://temperedsoftware.s3.amazonaws.com/release/hotfixes/HIPswitch_hotfix-12219

Platform end-of-life for Airwall Gateway 300 series hardware appliance

Tempered announces the End of Life schedule for the 300 series Airwall Gateway hardware platforms.

Note: This only applies to the 300 series hardware appliance. The 300v cloud and virtual Airwall Gateway is still supported.

End of life schedule for the 300 series

Date	Milestone	Definition
01/01/2019	End of Sale	Last date on which the platform may be purchased
11/13/2019	Last supported Software version	The 300 series support software versions up to v2.1.7. Attempts to install v2.1.8 or later will fail.
01/01/2020	Last Full Term MSMU Renewal	Last date a MSMU contract may be renewed for a full 12 month term. MSMU contracts apply only to the 300 appliance products with perpetual software licenses. Contracts renewed after this date are required to end no later than 01/01/2020.
01/01/2021	Platform End of Life	The date on which the platform is no longer supported by Tempered.

Tempered Networks harmonized tariff codes and country of origin

Affected platforms:	All Platforms

Details

Platform Series	HTS Code	Country of Origin
Conductor 500 Series	8517620020	Taiwan
HIPswitch 75 Series	8517620020	China
HIPswitch 100 Series	8517620020	Taiwan
HIPswitch 150 Series (base platform only)	8517620020	China
HIPswitch 150 Series cellular expansion modules	8517620010	China
HIPswitch 250 Series	8517620020	China

Platform Series	HTS Code	Country of Origin
HIPswitch 500 Series	8517620020	Taiwan

Pre-Airwall Bulletins

Product bulletins for earlier products.

Software support end of life for versions 1.12.6 and earlier

Affected platforms:	All platforms
Affected product versions:	1.12.x and earlier
Date effective:	September 16, 2019

Tempered Networks is providing six-month advance notice of our intent to end support for software versions 1.12.6 and earlier on September 16, 2019, the **Effective Date** noted above. After the effective date, Tempered Networks will no longer provide troubleshooting services or develop hot fixes for deployments running 1.12.6 or earlier software. See below for customer resolution.

We strongly recommend that customers start planning to upgrade their deployments to the latest software release as soon as possible. For information about upgrade planning, including a recommend upgrade path, please visit the Tempered Networks Online Documentation here: temperednetworks.com/webhelp. If you require additional planning assistance, please contact your solution architect or Tempered Networks Customer Support at https://tempered.force.com/TemperedSupportCenter/s/.

IF-MAP protocol deprecated in IDN 2.2

Affected platforms:	Conductor 400 Conductor 500 Conductor, all cloud platforms Conductor, all virtual platforms
Affected product versions:	1.x and earlier

Conductor software versions 2.1.x and earlier use the IF-MAP protocol to facilitate communication between Conductor and HIP Services running software versions 1.x.x. However, as of Conductor software version 2.2.0, the IF-MAP protocol is no longer supported. Customers applying a version 2.2.0 upgrade to Conductor will experience loss of connectivity with HIP Services running versions earlier than 2.0.0, and need to plan their upgrade path accordingly.

When planning an upgrade of Conductor to version 2.2.0, we strongly recommend that customers verify all HIP Services are running software version 2.1.x or later. For information about upgrade planning, including a recommended upgrade path, please visit the Tempered Networks Online Documentation here: temperednetworks.com/webhelp. If you require additional planning assistance, please contact your solution architect or Tempered Customer Support at https://tempered.force.com/TemperedSupportCenter/s/.

Important Patch for HIPswitch-100 and HIPswitch-250 running version 2.1.3

An issue was recently discovered in 2.1.3 when a HIPswitch is in service for a long period of time. When a network interface reaches a total of 2.1GB of traffic, an internal management daemon starts experiencing errors and restarts repeatedly. These restarts appear in the Conductor UI as HIPswitch connects and disconnects. No HIP traffic issues occur when this happens, and secure tunnels will remain intact. The noticeable behavior is the periodic loss of connection to the Conductor.

A hotfix for 2.1.3 is available for the affected platforms. Tempered Networks strongly recommends this hotfix to all customers who have affected platforms running version 2.1.3.

If you are unable to install the hotfix, disable traffic stats reporting for the affected platforms. This action can be performed from the Conductor.

You can download the hotfixes for your platform here or from the Hotfixes on page 548 page:

- **HIPswitch 100 Series:** Hotfix 8543
- **HIPswitch 250 Series:** Hotfix 8551

Important HIPswitch 250 Verizon modem firmware update

Verizon is rolling out an upgrade to their towers that has a known issue with the modem used in the HIPswitch 250.

Our vendor has issued a firmware update for this issue, customers with a HIPswitch 250g or HIPswitch 250gd need to apply this firmware update for compatibility with the Verizon update.

Issue

In rare cases, the module may not be able to attach to an LTE cell in a particular network condition because the module is unable to decode some SIB messages and skip additional information element introduced in higher than 3GPP versions 9.13.0. The module will fallback to 3G if the corresponding cell is available.

Resolution

Update to the newest firmware for the modem.

This firmware is released for Tempered Networks HIPswitch 250g and HIPswitch 250gd connecting to Verizon.

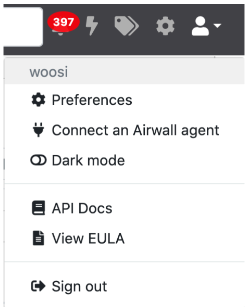
The firmware is available at:

https://app.box.com/shared/static/7coj9v4ychhel3rlpl8lvzjho2qs6b7y.package

Airwall API

You can access the Airwall API Reference from your Conductor.

1. In the Airwall Conductor, open your profile menu:



2. Select **API Docs**. The Tempered Simple Connect API docs open in a new tab.
3. When you are finished, close the tab.

Script Repository

Device Failover

The Conductor API allows for collecting and modifying attributes in Conductor. The following script is an example of how to perform device failover within an overlay network.

Select a device in an overlay and replace it with a different device or device group.

Prerequisites

- Experience with Python and install Python packages
- RESTful API experience
- Conductor user account with API access enabled

Note: ICMP is used to monitor a host to determine when to failover. This requires a sudoer or Administrator account to run.

Required Python Packages

- `multiping`
- `requests`

Note: Other imports in this script should be covered by Python's default packages. If not included, you may have to install them manually.

Sample Script

```
#!/usr/bin/python3

from ipaddress import ip_address
import json
from multiping import MultiPing
import os
import requests
from requests.packages.urllib3.exceptions import InsecureRequestWarning
import sys
import time

# Suppress cert warning
requests.packages.urllib3.disable_warnings(InsecureRequestWarning)

url = "https://<Conductor IP>/api/v1/"

# pre-2.1.3 API headers
# headers = {
#     'x-person-token': '1234',
#     'x-person-email': 'api@temperednetworks.com',
#     'content-type': 'application/json'
# }

headers = {
    'x-api-client-id': 'KWFCITL4VX_B-ZSdywD0Eg',
    'x-api-token': 'grui5TWLvvic8mZ7fgglbA',
    'content-type': 'application/json'
}


def generate_menu_select(cont, msg):
    """
    Generate a menu structure from a list of dictionaries

    :param cont: content to be processed
    :param msg: message to be asked

    :returns: selected object from list
    """

    data = sorted(cont, key=lambda k: k['name'])
    for d in data:

        print('{0}) {1}'.format(data.index(d) + 1, d['name']))

    i = input(msg)

    try:
        return(data[int(i) - 1])
    except (IndexError, ValueError):
        print('Selected input {0} not found or invalid'.format(i))
        sys.exit()
```

```
def get_overlay():
    """
    Get all overlays in Conductor

    :returns: selected overlay network
    """

    r = requests.get(url + "overlay_networks", headers=headers,
 verify=False)

    if r.status_code == requests.codes.ok:
        print('Collected overlays:')
        return generate_menu_select(r.json(),
                                    "Select overlay network to failover: ")
    else:
        print('Error getting overlay networks')
        print(r.json())
        sys.exit()


def get_object_in_overlay(devs, dgs, ovl_gps):
    """
    Get all devices/device groups in the overlay. Move to own list.

    :param devs: all devices
    :param dgs: all device groups
    :param ovl_gps: all devices/device groups in overlay

    :returns: selected device/device group
    """

    # devices and device groups
    grps = [d for d in devs for o in ovl_gps if o == d['uuid']]
    grps.extend([d for d in dgs for o in ovl_gps if o == d['uuid']])

    print('Collected devices and device groups in overlay network:')
    return generate_menu_select(grps, 'Select device/device group to
 replace: ')


def get_device_groups():
    """
    Get all device groups in Conductor

    :returns: all Conductor device groups
    """

    r = requests.get(url + "device_groups", headers=headers, verify=False)

    if r.status_code == requests.codes.ok:
        return r.json()
    else:
        print('Error getting device groups')
        print(r.json())
        sys.exit()


def get_devices():
    """
    Get all devices in Conductor

    :returns: all Conductor devices
    """
    r = requests.get(url + "devices", headers=headers, verify=False)

    if r.status_code == requests.codes.ok:
        return r.json()
    else:
        print('Error getting devices')
        print(r.json())
        sys.exit()


def add_device_to_overlay(ovl_uuid, d_uuid):
    """
    Add a device to an overlay network

    :param ovl_uuid: overlay network UUID
    :param d_uuid: device UUID
    """

    payload = {'network_id': ovl_uuid,
               'device_group_ids': [d_uuid]}

    r = requests.post(url + "overlay_network_devices", headers=headers,
                      data=json.dumps(payload), verify=False)

    if not r.status_code == requests.codes.ok:
        print('Error adding to overlay')
        print(r.json())
        sys.exit()


def remove_device_from_overlay(ovl_uuid, d_uuid):
    """
    Remove a device from an overlay network

    :param ovl_uuid: overlay network UUID
    :param d_uuid: device UUID
    """

    payload = {'network_id': ovl_uuid,
               'device_group_ids': [d_uuid]}

    r = requests.delete(url + "overlay_network_devices", headers=headers,
                        data=json.dumps(payload), verify=False)

    if not r.status_code == requests.codes.ok:
        print('Error removing from overlay')
        print(r.json())
        sys.exit()


def build_overlay_policy(ovl_uuid, d_uuid, ds_uuid):
    """
    Build the overlay policy

    :param ovl_uuid: overlay network UUID
    :param d_uuid: device UUID
    :param ds_uuid: UUIDs of devices in policy with previous device (target)
    """

    for uuid in ds_uuid:
        payload = {'network_id': ovl_uuid,
                   'device_group_1': d_uuid,
                   'device_group_2': uuid}
        r = requests.post(url + "overlay_network_devices/trust",
 headers=headers,
                          data=json.dumps(payload), verify=False)

        if not r.status_code == requests.codes.ok:
            print('Error adding policy in overlay')
            print(r.json())


def get_replacement_object(devs, dgs):
    """
    Select which object to use as a replacement

    :param devs: all devices
    :param dgs: all device groups

    :returns: device/device group JSON data
    """

    selection = [{'name': 'Device'}, {'name': 'Device Group'}]

    sel = generate_menu_select(selection, 'Type to replace with: ')

    if sel['name'] == 'Device':
        return generate_menu_select(devs, 'Select replacement device: ')
    elif sel['name'] == 'Device Group':
        return generate_menu_select(dgs, 'Select replacement device group:
 ')


def replace_overlay_object(ovl, target, replacement):
    """
    Replace a given target with a replacement device/device group object

    :param ovl: overlay JSON data
    :param target: target device JSON data
    :param replacement: replacement device JSON data
    """

    policies = [p for p in [t['from'] for t in ovl['policy'] if t['to'] ==
 target['uuid']]]

    remove_device_from_overlay(ovl['uuid'], target['uuid'])
    print('Removing device from overlay')
    add_device_to_overlay(ovl['uuid'], replacement['uuid'])
    print('Adding replacement device to overlay')
    build_overlay_policy(ovl['uuid'], replacement['uuid'], policies)
    print('Build overlay policy with replacement device')


def select_mon_target():
    """
    Input an IP to monitor

    :returns: IP address to monitor
    """

    selection = True
    mon_target = None

    while selection:
        mon_target = input('Enter IP target to monitor: ')
        try:
            ip_address(mon_target)
            selection = False
        except ValueError:
            print('Invalid IP address.')
            continue

    return mon_target


def monitor_target(mon_target):
    """
    Monitor the given target import ip

    :param mon_target: IP address to monitor
    """

    active = True
    while active:
        if mon_target:
            mp = MultiPing([mon_target])
            mp.send()
            resp, no_resp = mp.receive(.1)
            stamp = time.strftime('%Y-%m-%d %H:%M:%S')

            if no_resp:
                print('{0}: Monitor failed'.format(stamp))
                break
            else:
                print('{0}: Ping monitor successful'.format(stamp))
                time.sleep(1)


def main():

    if not os.geteuid() == 0:
        print('Must run as root or Administrator. Exiting...')

    else:

        # get content
        ovl = get_overlay()
        devs = get_devices()
        dgs = get_device_groups()

        # ask questions
        target = get_object_in_overlay(devs, dgs, ovl['device_groups'])
        replacement = get_replacement_object(devs, dgs)

        # monitor ip
        mon_target = select_mon_target()
        monitor_target(mon_target)

        # do work
        replace_overlay_object(ovl, target, replacement)
        print('Device failover completed')


if __name__ == "__main__":
    try:
        main()
    except KeyboardInterrupt:
        sys.exit()
```

Software Downloads and Release Notes

Download Tempered's Airwall software and firmware for your version and platform here, and get the release notes for those versions.

For help applying updates, see the following topics:

- Update Conductor Firmware on page 127
- Update Airwall Gateway firmware on page 129
- Update firmware for a group of Airwall Edge Services on page 131

Latest firmware and software

This topic is linked from the Conductor. Talk to dev before renaming or removing.

Follow the links below to download the latest firmware and software. For release notes, see Latest Release Notes (v3.2.4) on page 551:

⚠ **CAUTION:** When you update your firmware from older versions to a much more recent one, you may need to update to another, earlier version first. See How to Update from Older Versions on page 515.

Conductor firmware

Conductor	Version	Download
Conductor - Physical, Cloud, or Virtual	v3.2.3	Conductor_r3.2.3-2219_package

Airwall Gateway firmware

Model	Version	Download
75 (mvebu64)	v3.2.4	Airwall-mvebu64_r3.2.4-1816_package
110, 150, and 250 (mvebu)	v3.2.4	Airwall-mvebu_r3.2.4-1938_package
300v, 400, and 500 (x86_64)	v3.2.4	Airwall-x86_64_r3.2.4-2185_package
ESXi virtual (x86_64 OVA)	v3.2.4	Airwall-x86_64_r3.2.4-2185-combined-ext4.ova
Hyper-V virtual (x86_64 Hyper-V image)	v3.2.4	Airwall-x86_64_r3.2.4-2185-combined-ext4.vhdx

Airwall Agent and Airwall Server Software

For the latest iOS and Android Airwall Agents, search for "Airwall Agent" in the store for your device.

Laptop or Mobile Device	Version	Download
Airwall Agents		
macOS, OSX	v3.2.3	Airwall-Mac_3.2.3.2628.pkg
iOS	v2.2.12	Download from the Apple AppStore (says 2.2.13, but it is an update to 2.2.12)
Android	v3.0.0	Download from the Google Play Store

Laptop or Mobile Device	Version	Download
Windows PC 64-bit	v2.2.13	**Installer** – AirwallAgent64-bit_2.2.13.427_Installer.exe **Express Installer** – AirwallAgent64-bit_2.2.13.427_ExpressInstaller.exe **Unattended Installer** – AirwallAgent64-bit_UnattendedInstaller_2.2.13.427.msi
Airwall Servers		
Linux/Ubuntu v16	v3.0.0	airwall-ubuntu16_3.0.0-1206_amd64.deb
Linux/Ubuntu v18 and v20	v3.1.0	airwall-ubuntu18_3.1.0-1459_amd64.deb
Linux/CentOS 8	v3.1.0	airwall-3.1.0-1177.el8.x86_64.rpm
Linux/CentOS 7	v3.0.0	airwall-3.0.0-1173.el7.x86_64.rpm
Linux/Fedora	v3.1.0	airwall-3.1.0-1185.fc34.x86_64.rpm
Windows Server 64-bit	v2.2.13	**Install** – AirwallServer64-bit_2.2.13.427_Installer.exe **Express Installer** – AirwallServer64-bit_2.2.13.427_ExpressInstaller.exe **Unattended Installer** – AirwallServer64-bit_UnattendedInstaller_2.2.13.427.msi

Cellular Modem Firmware Updates

Airwall Gateway Model	Download
110 – See note	Airwall-110_cellfw-2e8314c-129_package
110 – Hotfix for AT&T 3G Sunset	Airwall-110_cellfw-4c5753a-125_package
Advantech – See note	Airwall-112_cellfw-2e8314c-129_package
Advantech – Hotfix for AT&T 3G Sunset	Airwall-112_cellfw-4c5753a-125_package
150 – See note	Airwall-150_cellfw-2e8314c-129_package
250 – See note	Airwall-250_cellfw-2e8314c-129_package

Note: Contains an updated map of Mobile County Code and Mobile Network Code values, most notably a change of some codes that formerly identified T-Mobile that now identify AT&T.

Windows Serial Port Drivers

Serial Port Driver for:	Version	Download
Pre-2.2.3 Airwall Gateway 150 only	Windows, 32-bit	HIPswitch150Driver_x86.msi
Windows, 64-bit Airwall Gateway 100, 110, and 150	Dec 2020	Airwall1XXSerialDriver_x64.msi

How to Update from Older Versions

When you update your firmware from older versions to a much more recent one, you may need to update to another, earlier version first. Check the **Version Compatibility** table below to see which versions you can update to.

For example, if you want to update from v2.1.2 to v3.0.0, you need to update from v2.1.2 to v2.1.7, then to v2.2.13, and then you can update to v3.0.0.

Table 1: Version Compatibility

Starting Firmware Version	Highest Compatible version
2.1.0	2.1.7
2.1.1	2.1.7
2.1.2	2.1.7
2.1.3	2.1.7
2.1.4	2.1.7
2.1.5	2.1.7
2.1.6	2.1.7
2.1.7	2.2.12 / 2.2.13
2.2.0	2.2.12 / 2.2.13
2.2.1	2.2.12 / 2.2.13
2.2.3	2.2.12 / 2.2.13
2.2.5	2.2.12 / 2.2.13
2.2.8	2.2.12 / 2.2.13
2.2.10	2.2.12 / 2.2.13
2.2.11	2.2.12 / 2.2.13
2.2.12 / 2.2.13	Any 3.0.x version
3.0.0	Any 3.0.x version
3.0.1	Any 3.0.x version
3.0.2	Any 3.0.x version
3.0.3	Any 3.0.x version
3.1.0	Any 3.1.x version
3.1.2	Any 3.1.x version
3.2.4	Any 3.2.x version

3.3.0 firmware and software

Follow the links below to download the v3.3.0 firmware and software. This release contains new firmware for Airwall Conductors and Airwall Gateways. For release notes, see Release Notes v3.3.0 on page 551.

Note: Also review Hotfixes on page 548 for any hotfix releases.

Checksums	MD5 SHA1

Conductor firmware

Conductor	Version	Download
Conductor - Physical, Cloud, or Virtual	v3.2.3	Conductor_r3.2.3-2219_package

Airwall Gateway firmware

Model	Version	Download
75 (mvebu64)	v3.2.4	Airwall-mvebu64_r3.2.4-1816_package
110, 150, and 250 (mvebu)	v3.2.4	Airwall-mvebu_r3.2.4-1938_package
300v, 400, and 500 (x86_64)	v3.2.4	Airwall-x86_64_r3.2.4-2185_package
ESXi virtual (x86_64 OVA)	v3.2.4	Airwall-x86_64_r3.2.4-2185-combined-ext4.ova
Hyper-V virtual (x86_64 Hyper-V image)	v3.2.4	Airwall-x86_64_r3.2.4-2185-combined-ext4.vhdx

Airwall Agent and Airwall Server Software

For the latest iOS and Android Airwall Agents, search for "Airwall Agent" in the store for your device.

Laptop or Mobile Device	Version	Download
Airwall Agents		
macOS, OSX	v3.2.3	Airwall-Mac_3.2.3.2628.pkg

Cellular Modem Firmware Updates

Cellular Modem Firmware for:	Download
Airwall Gateway 110	Airwall-110_cellfw-9224c85-106_package
Airwall Gateway 150	Airwall-150_cellfw-9224c85-106_package
Airwall Gateway 250	Airwall-250_cellfw-9224c85-106_package

Windows Serial Port Drivers

Serial Port Driver for:	Version	Download
Pre-2.2.3 Airwall Gateway 150 only	Windows, 32-bit	HIPswitch150Driver_x86.msi
Windows, 64-bit Airwall Gateway 100, 110, and 150	Dec 2020	Airwall1XXSerialDriver_x64.msi

3.2.4 firmware and software

Note: This release is a combination of 3.2.3 and 3.2.4.

Follow the links below to download the v3.2.4 firmware and software. This release contains new firmware for Airwall Conductors and Airwall Gateways. For release notes, see Release Notes v3.2.4 on page 558.

Note: Also review Hotfixes on page 548 for any hotfix releases.

Checksums	MD5 SHA1

Conductor firmware

Conductor	Version	Download
Conductor - Physical, Cloud, or Virtual	v3.2.3	Conductor_r3.2.3-2219_package

Airwall Gateway firmware

Model	Version	Download
75 (mvebu64)	v3.2.4	Airwall-mvebu64_r3.2.4-1816_package
110, 150, and 250 (mvebu)	v3.2.4	Airwall-mvebu_r3.2.4-1938_package
300v, 400, and 500 (x86_64)	v3.2.4	Airwall-x86_64_r3.2.4-2185_package
ESXi virtual (x86_64 OVA)	v3.2.4	Airwall-x86_64_r3.2.4-2185-combined-ext4.ova
Hyper-V virtual (x86_64 Hyper-V image)	v3.2.4	Airwall-x86_64_r3.2.4-2185-combined-ext4.vhdx

Airwall Agent and Airwall Server Software

For the latest iOS and Android Airwall Agents, search for "Airwall Agent" in the store for your device.

Laptop or Mobile Device	Version	Download
Airwall Agents		
macOS, OSX	v3.2.3	Airwall-Mac_3.2.3.2628.pkg

Cellular Modem Firmware Updates

Cellular Modem Firmware for:	Download
Airwall Gateway 110	Airwall-110_cellfw-9224c85-106_package
Airwall Gateway 150	Airwall-150_cellfw-9224c85-106_package
Airwall Gateway 250	Airwall-250_cellfw-9224c85-106_package

Windows Serial Port Drivers

Serial Port Driver for:	Version	Download
Pre-2.2.3 Airwall Gateway 150 only	Windows, 32-bit	HIPswitch150Driver_x86.msi
Windows, 64-bit Airwall Gateway 100, 110, and 150	Dec 2020	Airwall1XXSerialDriver_x64.msi

3.1.2 firmware and software

Follow the links below to download the v3.1.2 firmware and software. This release contains new firmware for Airwall Conductors and Airwall Gateways. For release notes, see Release Notes v3.1.2 on page 566.

Note: Also review Hotfixes on page 548 for any hotfix releases.

Checksums	MD5 SHA1

Conductor firmware

Conductor	Version	Download
Conductor - Physical, Cloud, or Virtual	v3.1.2	Conductor_r3.1.2-2063_package

Airwall Gateway firmware

Model	Version	Download
75 (mvebu64)	v3.1.2	Airwall-mvebu64_r3.1.2-1644_package
110, 150, and 250 (mvebu)	v3.1.2	Airwall-mvebu_r3.1.2-1777_package
300v, 400, and 500 (x86_64)	v3.1.2	Airwall-x86_64_r3.1.2-2020_package
ESXi virtual (x86_64 OVA)	v3.1.2	Airwall-x86_64_r3.1.2-2020-combined-ext4.ova

Airwall Agent and Airwall Server Software

For the latest iOS and Android Airwall Agents, search for "Airwall Agent" in the store for your device.

Note: **For** Airwall Agents and Servers that are not part of this release, see the latest version available at Latest firmware and software on page 514.

Laptop or Mobile Device	Version	Download
Airwall Agents		
macOS, OSX	v3.0	Airwall-Mac_3.0.0.2065.pkg
Android	v3.0	Download from the Google Play Store
iOS	v2.2.12	Download from the Apple AppStore (says 2.2.13, but it is an update to 2.2.12)
Windows PC 64-bit	v2.2.13	**Installer** – AirwallAgent64-bit_2.2.13.427_Installer.exe **Express Installer** – AirwallAgent64-bit_2.2.13.427_ExpressInstaller.exe **Unattended Installer** – AirwallAgent64-bit_UnattendedInstaller_2.2.13.427.msi
Airwall Servers		
Linux/Ubuntu v16	v3.0	airwall-ubuntu16_3.0.0-1206_amd64.deb

Laptop or Mobile Device	Version	Download
Linux/Ubuntu v18 and v20	v3.0	airwall-ubuntu18_3.0.0-1094_amd64.deb
Linux/CentOS 8	v3.0	airwall-3.0.0-819.el8.x86_64.rpm
Linux/CentOS 7	v3.0	airwall-3.0.0-1173.el7.x86_64.rpm
Linux/Fedora	v3.0	airwall-3.0.0-877.fc33.x86_64.rpm
Windows Server 64-bit	v2.2.13	**Install** – AirwallServer64-bit_2.2.13.427_Installer.exe **Express Installer** – AirwallServer64-bit_2.2.13.427_ExpressInstaller.exe **Unattended Installer** – AirwallServer64-bit_UnattendedInstaller_2.2.13.427.msi

Cellular Modem Firmware Updates

Cellular Modem Firmware for:	Download
Airwall Gateway 110	Airwall-110_cellfw-9224c85-106_package
Airwall Gateway 150	Airwall-150_cellfw-9224c85-106_package
Airwall Gateway 250	Airwall-250_cellfw-9224c85-106_package

Windows Serial Port Drivers

Serial Port Driver for:	Version	Download
Pre-2.2.3 Airwall Gateway 150 only	Windows, 32-bit	HIPswitch150Driver_x86.msi
Windows, 64-bit Airwall Gateway 100, 110, and 150	Dec 2020	Airwall1XXSerialDriver_x64.msi

3.1.0 firmware and software

Follow the links below to download the v3.1.0 firmware and software. For release notes, see Release Notes v3.1.0 on page 573.

Note: Also review Hotfixes on page 548 for any hotfix releases.

Checksums	MD5 SHA1

Conductor firmware

Conductor	Version	Download
Conductor - Physical, Cloud, or Virtual	v3.1.0	Conductor_r3.1.0-1991_package

Airwall Gateway firmware

Model	Version	Download
75 (mvebu64)	v3.1.0	Airwall-mvebu64_r3.1.0-1569_package
110, 150, and 250 (mvebu)	v3.1.0	Airwall-mvebu_r3.1.0-1704_package
300v, 400, and 500 (x86_64)	v3.1.0	Airwall-x86_64_r3.1.0-1951_package
ESXi virtual (x86_64 OVA)	v3.1.0	Airwall-x86_64_r3.1.0-1951-combined-ext4.ova
Hyper-V virtual (x86_64 Hyper-V image)	v3.1.0	Airwall-x86_64_r3.1.0-1951-combined-ext4.vhdx

Airwall Agent and Airwall Server Software

For the latest iOS and Android Airwall Agents, search for "Airwall Agent" in the store for your device.

Note: For Airwall Agents and Servers that are not part of this release, see the latest version available at Latest firmware and software on page 514.

Laptop or Mobile Device	Version	Download
Airwall Agents		
macOS, OSX	v3.1.0	Airwall-Mac_3.1.0.2444.pkg
iOS	v2.2.13	Download from the Apple AppStore (says 2.2.13, but it is an update to 2.2.12)
Windows PC 64-bit	v2.2.13	**Installer** – AirwallAgent64-bit_2.2.13.427_Installer.exe **Express Installer** – AirwallAgent64-bit_2.2.13.427_ExpressInstaller.exe **Unattended Installer** – AirwallAgent64-bit_UnattendedInstaller_2.2.13.427.msi
Airwall Servers		
Linux/Ubuntu v18 and v20	v3.1.0	airwall-ubuntu18_3.1.0-1459_amd64.deb
Linux/CentOS 8	v3.1.0	airwall-3.1.0-1177.el8.x86_64.rpm
Linux/Fedora	v3.1.0	airwall-3.1.0-1185.fc34.x86_64.rpm
Windows Server 64-bit	v2.2.13	**Install** – AirwallServer64-bit_2.2.13.427_Installer.exe **Express Installer** – AirwallServer64-bit_2.2.13.427_ExpressInstaller.exe **Unattended Installer** – AirwallServer64-bit_UnattendedInstaller_2.2.13.427.msi

Cellular Modem Firmware Updates

Cellular Modem Firmware for:	Download
Airwall Gateway 110	Airwall-110_cellfw-9224c85-106_package
Airwall Gateway 150	Airwall-150_cellfw-9224c85-106_package
Airwall Gateway 250	Airwall-250_cellfw-9224c85-106_package

Windows Serial Port Drivers

Serial Port Driver for:	Version	Download
Pre-2.2.3 Airwall Gateway 150 only	Windows, 32-bit	HIPswitch150Driver_x86.msi
Windows, 64-bit Airwall Gateway 100, 110, and 150	Dec 2020	Airwall1XXSerialDriver_x64.msi

3.0.3 firmware and software

Follow the links below to download the v3.0.3 firmware and software. This release contains new firmware for Airwall Conductors and Airwall Gateways. For release notes, see Release Notes v3.0.3 on page 587.

Note: Also review Hotfixes on page 548 for any hotfix releases.

Checksums	MD5 SHA1

Conductor firmware

Conductor	Version	Download
Conductor - Physical, Cloud, or Virtual	v3.0.3	Conductor_r3.0.3-1791_package

Airwall Gateway firmware

Model	Version	Download
Advantech AV3200g installer	v3.0.3	temperedfw-r3.0.3-1526.tgz
75 (mvebu64)	v3.0.3	Airwall-mvebu64_r3.0.3-1391_package
110, 150, and 250 (mvebu)	v3.0.3	Airwall-mvebu_r3.0.3-1526_package
300v, 400, and 500 (x86_64)	v3.0.3	Airwall-x86_64_r3.0.3-1770_package
ESXi virtual (x86_64 OVA)	v3.0.3	Airwall-x86_64_r3.0.3-1770-combined-ext4.ova
Hyper-V virtual (x86_64 Hyper-V image)	v3.0.3	Airwall-x86_64_r3.0.3-1770-combined-ext4.vhdx

Airwall Agent and Airwall Server Software

For the latest iOS and Android Airwall Agents, search for "Airwall Agent" in the store for your device.

Note: For Airwall Agents and Servers that are not part of this release, see the latest version available at Latest firmware and software on page 514.

Laptop or Mobile Device	Version	Download
Airwall Agents		
macOS, OSX	v3.0	Airwall-Mac_3.0.0.2065.pkg
Android	v3.0	Download from the Google Play Store
iOS	v2.2.12	Download from the Apple AppStore (says 2.2.13, but it is an update to 2.2.12)
Windows PC 64-bit	v2.2.13	**Installer** – AirwallAgent64-bit_2.2.13.427_Installer.exe **Express Installer** – AirwallAgent64-bit_2.2.13.427_ExpressInstaller.exe **Unattended Installer** – AirwallAgent64-bit_UnattendedInstaller_2.2.13.427.msi
Airwall Servers		
Linux/Ubuntu v16	v3.0	airwall-ubuntu16_3.0.0-1206_amd64.deb
Linux/Ubuntu v18 and v20	v3.0	airwall-ubuntu18_3.0.0-1094_amd64.deb
Linux/CentOS 8	v3.0	airwall-3.0.0-819.el8.x86_64.rpm
Linux/CentOS 7	v3.0	airwall-3.0.0-1173.el7.x86_64.rpm
Linux/Fedora	v3.0	airwall-3.0.0-877.fc33.x86_64.rpm
Windows Server 64-bit	v2.2.13	**Install** – AirwallServer64-bit_2.2.13.427_Installer.exe **Express Installer** – AirwallServer64-bit_2.2.13.427_ExpressInstaller.exe **Unattended Installer** – AirwallServer64-bit_UnattendedInstaller_2.2.13.427.msi

Cellular Modem Firmware Updates

Cellular Modem Firmware for:	Download
Airwall Gateway 110	Airwall-110_cellfw-9224c85-106_package
Airwall Gateway 150	Airwall-150_cellfw-9224c85-106_package
Airwall Gateway 250	Airwall-250_cellfw-9224c85-106_package

Windows Serial Port Drivers

Serial Port Driver for:	Version	Download
Pre-2.2.3 Airwall Gateway 150 only	Windows, 32-bit	HIPswitch150Driver_x86.msi

Serial Port Driver for:	Version	Download
Windows, 64-bit Airwall Gateway 100, 110, and 150	Dec 2020	Airwall1XXSerialDriver_x64.msi

3.0.2 firmware and software

Please follow the links below to download the v3.0.2 firmware and software. This release contains new firmware for Airwall Conductors and Airwall Gateways. For release notes, see Release Notes v3.0.2 on page 593.

Note: Also review Hotfixes on page 548 for any hotfix releases.

Checksums	MD5 SHA

Conductor firmware

Conductor	Version	Download
Conductor - Physical, Cloud, or Virtual	v3.0.2	Conductor_r3.0.2-1787_package

Airwall Gateway firmware

Model	Version	Download
Advantech AV3200g installer	v3.0.2	temperedfw-r3.0.2-1522.tgz
75 (mvebu64)	v3.0.2	Airwall-mvebu64_r3.0.2-1387_package
110, 150, and 250 (mvebu)	v3.0.2	Airwall-mvebu_r3.0.2-1522_package
300v, 400, and 500 (x86_64)	v3.0.2	Airwall-x86_64_r3.0.2-1765_package
ESXi virtual (x86_64 OVA)	v3.0.2	Airwall-x86_64_r3.0.2-1765-combined-ext4.ova
Hyper-V virtual (x86_64 Hyper-V image)	v3.0.2	Airwall-x86_64_r3.0.2-1765-combined-ext4.vhdx

Airwall Agent and Airwall Server Software

For the latest iOS and Android Airwall Agents, search for "Airwall Agent" in the store for your device.

Note: **For** Airwall Agents and Servers that are not part of this release, see the latest version available at Latest firmware and software on page 514.

Laptop or Mobile Device	Version	Download
Airwall Agents		
macOS, OSX	v3.0	Airwall-Mac_3.0.0.2065.pkg
Android	v3.0	Download from the Google Play Store
iOS	v2.2.12	Download from the Apple AppStore (says 2.2.13, but it is an update to 2.2.12)

Laptop or Mobile Device	Version	Download
Windows PC 64-bit	v2.2.13	**Installer** – AirwallAgent64-bit_2.2.13.427_Installer.exe **Express Installer** – AirwallAgent64-bit_2.2.13.427_ExpressInstaller.exe **Unattended Installer** – AirwallAgent64-bit_UnattendedInstaller_2.2.13.427.msi
Airwall Servers		
Linux/Ubuntu v16	v3.0	airwall-ubuntu16_3.0.0-1206_amd64.deb
Linux/Ubuntu v18 and v20	v3.0	airwall-ubuntu18_3.0.0-1094_amd64.deb
Linux/CentOS 8	v3.0	airwall-3.0.0-819.el8.x86_64.rpm
Linux/CentOS 7	v3.0	airwall-3.0.0-1173.el7.x86_64.rpm
Linux/Fedora	v3.0	airwall-3.0.0-877.fc33.x86_64.rpm
Windows Server 64-bit	v2.2.13	**Install** – AirwallServer64-bit_2.2.13.427_Installer.exe **Express Installer** – AirwallServer64-bit_2.2.13.427_ExpressInstaller.exe **Unattended Installer** – AirwallServer64-bit_UnattendedInstaller_2.2.13.427.msi

Cellular Modem Firmware Updates

Cellular Modem Firmware for:	Download
Airwall Gateway 110	Airwall-110_cellfw-9224c85-106_package
Airwall Gateway 150	Airwall-150_cellfw-9224c85-106_package
Airwall Gateway 250	Airwall-250_cellfw-9224c85-106_package

Windows Serial Port Drivers

Serial Port Driver for:	Version	Download
Pre-2.2.3 Airwall Gateway 150 only	Windows, 32-bit	HIPswitch150Driver_x86.msi
Windows, 64-bit Airwall Gateway 100, 110, and 150	Dec 2020	Airwall1XXSerialDriver_x64.msi

3.0.1 firmware and software

Please follow the links below to download the v3.0.1 firmware and software. This release contains new firmware for Airwall Conductors and Airwall Gateways. For release notes, see Release Notes v3.0.1 on page 600.

Note: Also review Hotfixes on page 548 for any hotfix releases.

Checksums	MD5 SHA1

Conductor firmware

Conductor	Version	Download
Conductor - Physical, Cloud, or Virtual	v3.0.1	Conductor_r3.0.1-1777_package

Airwall Gateway firmware

Model	Version	Download
Advantech AV3200g installer	v3.0.1	temperedfw-r3.0.1-1511.tgz
75 (mvebu64)	v3.0.1	Airwall-mvebu64_r3.0.1-1376_package
110, 150, and 250 (mvebu)	v3.0.1	Airwall-mvebu_r3.0.1-1511_package
300v, 400, and 500 (x86_64)	v3.0.1	Airwall-x86_64_r3.0.1-1751_package
ESXi virtual (x86_64 OVA)	v3.0.1	Airwall-x86_64_r3.0.1-1751-combined-ext4.ova
Hyper-V virtual (x86_64 Hyper-V image)	v3.0.1	Airwall-x86_64_r3.0.1-1751-combined-ext4.vhdx

Airwall Agent and Airwall Server Software

For the latest iOS and Android Airwall Agents, search for "Airwall Agent" in the store for your device.

Note: For Airwall Agents and Servers that are not part of this release, see the latest version available at Latest firmware and software on page 514.

Laptop or Mobile Device	Version	Download
Airwall Agents		
macOS, OSX	v3.0	Airwall-Mac_3.0.0.2065.pkg
Android	v3.0	Download from the Google Play Store
iOS	v2.2.12	Download from the Apple AppStore (says 2.2.13, but it is an update to 2.2.12)
Windows PC 64-bit	v2.2.13	**Installer** – AirwallAgent64-bit_2.2.13.427_Installer.exe **Express Installer** – AirwallAgent64-bit_2.2.13.427_ExpressInstaller.exe **Unattended Installer** – AirwallAgent64-bit_UnattendedInstaller_2.2.13.427.msi
Airwall Servers		

Laptop or Mobile Device	Version	Download
Linux/Ubuntu v16	v3.0	airwall-ubuntu16_3.0.0-1206_amd64.deb
Linux/Ubuntu v18 and v20	v3.0	airwall-ubuntu18_3.0.0-1094_amd64.deb
Linux/CentOS 8	v3.0	airwall-3.0.0-819.el8.x86_64.rpm
Linux/CentOS 7	v3.0	airwall-3.0.0-1173.el7.x86_64.rpm
Linux/Fedora	v3.0	airwall-3.0.0-877.fc33.x86_64.rpm
Windows Server 64-bit	v2.2.13	**Install** – AirwallServer64-bit_2.2.13.427_Installer.exe **Express Installer** – AirwallServer64-bit_2.2.13.427_ExpressInstaller.exe **Unattended Installer** – AirwallServer64-bit_UnattendedInstaller_2.2.13.427.msi

Cellular Modem Firmware Updates

Cellular Modem Firmware for:	Download
Airwall Gateway 110	Airwall-110_cellfw-9224c85-106_package
Airwall Gateway 150	Airwall-150_cellfw-9224c85-106_package
Airwall Gateway 250	Airwall-250_cellfw-9224c85-106_package

Windows Serial Port Drivers

Serial Port Driver for:	Version	Download
Pre-2.2.3 Airwall Gateway 150 only	Windows, 32-bit	HIPswitch150Driver_x86.msi
Windows, 64-bit Airwall Gateway 100, 110, and 150	Dec 2020	Airwall1XXSerialDriver_x64.msi

3.0.0 firmware and software

Please follow the links below to download the v3.0.0 firmware and software. For release notes, see Release Notes v3.0.0 on page 609.

Note: Also review Hotfixes on page 548 for any hotfix releases.

Checksums	MD5 SHA1

Conductor firmware

Conductor	Version	Download
Conductor - Physical, Cloud, or Virtual	v3.0.0	Conductor_r3.0.0-1721_package

Airwall Gateway firmware

Model	Version	Download
Advantech AV3200g installer	v3.0.0	temperedfw-r3.0.0-1456.tgz
75 (mvebu64)	v3.0.0	Airwall-mvebu64_r3.0.0-1319_package
110, 150, and 250 (mvebu)	v3.0.0	Airwall-mvebu_r3.0.0-1456_package
300v, 400, and 500 (x86_64)	v3.0.0	Airwall-x86_64_r3.0.0-1689_package
ESXi virtual (x86_64 OVA)	v3.0.0	Airwall-x86_64_r3.0.0-1689-combined-ext4.ova
Hyper-V virtual (x86_64 Hyper-V image)	v3.0.0	Airwall-x86_64_r3.0.0-1689-combined-ext4.vhdx

Airwall Agent and Airwall Server Software

For the latest iOS and Android Airwall Agents, search for "Airwall Agent" in the store for your device.

Note: For Airwall Agents and Servers that are not part of this release, see the latest version available at Latest firmware and software on page 514.

Laptop or Mobile Device	Version	Download
Airwall Agents		
macOS, OSX	v3.0.0	Airwall-Mac_3.0.0.2065.pkg
Android	v3.0.0	Download from the Google Play Store
iOS	v2.2.12	Download from the Apple AppStore (says 2.2.13, but it is an update to 2.2.12)
Windows PC 64-bit	v2.2.13	**Installer** – AirwallAgent64-bit_2.2.13.427_Installer.exe **Express Installer** – AirwallAgent64-bit_2.2.13.427_ExpressInstaller.exe **Unattended Installer** – AirwallAgent64-bit_UnattendedInstaller_2.2.13.427.msi
Airwall Servers		
Linux/Ubuntu v16	v3.0.0	airwall-ubuntu16_3.0.0-1206_amd64.deb
Linux/Ubuntu v18 and v20	v3.0.0	airwall-ubuntu18_3.0.0-1094_amd64.deb
Linux/CentOS 8	v3.0.0	airwall-3.0.0-819.el8.x86_64.rpm
Linux/CentOS 7	v3.0.0	airwall-3.0.0-1173.el7.x86_64.rpm

Laptop or Mobile Device	Version	Download
Linux/Fedora	v3.0.0	airwall-3.0.0-877.fc33.x86_64.rpm
Windows Server 64-bit	v2.2.13	**Install** – AirwallServer64-bit_2.2.13.427_Installer.exe **Express Installer** – AirwallServer64-bit_2.2.13.427_ExpressInstaller.exe **Unattended Installer** – AirwallServer64-bit_UnattendedInstaller_2.2.13.427.msi

Cellular Modem Firmware Updates

Cellular Modem Firmware for:	Download
Airwall Gateway 110	Airwall-110_cellfw-9224c85-106_package
Airwall Gateway 150	Airwall-150_cellfw-9224c85-106_package
Airwall Gateway 250	Airwall-250_cellfw-9224c85-106_package

Windows Serial Port Drivers

Serial Port Driver for:	Version	Download
Pre-2.2.3 Airwall Gateway 150 only	Windows, 32-bit	HIPswitch150Driver_x86.msi
Windows, 64-bit Airwall Gateway 100, 110, and 150	Dec 2020	Airwall1XXSerialDriver_x64.msi

2.2.13 firmware and software

Please follow the links below to download the 2.2.13 firmware and software. For release notes, see Release Notes 2.2.13 on page 620.

Note: Also review Hotfixes on page 548 for any hotfix releases.

Conductor firmware

Conductor	Version	Download
Conductor - All Platforms	v2.2.13	Conductor_r2.2.13-1575_package

Airwall Gateway firmware

Model	Version	Download
Advantech Airwall Gateway AV3200g installer	v2.2.13	**v3.0 recommended** – Download from 3.0.0 firmware and software on page 527

Airwall Agent and Airwall Server Software

For the latest iOS and Android Airwall Agents, search for "Airwall Agent" in the store for your device.

Laptop or Mobile Device	Version	Download
Airwall Agents		
Windows 64-bit PC	v2.2.13	**Installer** – AirwallAgent64-bit_2.2.13.427_Installer.exe **Express Installer** – AirwallAgent64-bit_2.2.13.427_ExpressInstaller.exe **Unattended Installer** – AirwallAgent64-bit_UnattendedInstaller_2.2.13.427.msi
Airwall Servers		
Windows 64-bit Server	Windows Server 64 Airwall Server Install	**Installer** – AirwallServer64-bit_2.2.13.427_Installer.exe **Express Installer** – AirwallServer64-bit_2.2.13.427_ExpressInstaller.exe **Unattended Installer** – AirwallServer64-bit_UnattendedInstaller_2.2.13.427.msi

2.2.12 firmware and software

Please follow the links below to download the 2.2.12 firmware and software. For release notes, see Release Notes 2.2.12 on page 628.

Note: This release may not have firmware and software for all platforms. See the latest version for each platform available at Latest firmware and software on page 514.

Note: Also review Hotfixes on page 548 for any hotfix releases.

Conductor firmware

Conductor	Version	Download
Conductor - All Platforms	v2.2.12	Conductor_r2.2.12-1506_package

Airwall Gateway firmware

Airwall Gateway Model	Version	Download
75 (mvebu64)	v2.2.12	Airwall-mvebu64_r2.2.12-1143_package
100g and 100e (ramips)	v2.2.12	Airwall-ramips_r2.2.12-1218_package
110, 150, and 250 (mvebu)	v2.2.12	Airwall-mvebu_r2.2.12-1272_package
100rc, 300v, 400, and 500 (x86_64)	v2.2.12	Airwall-x86_64_r2.2.12-1482_package
ESXi (x86_64 OVA)	v2.2.12	Airwall-x86_64_r2.2.12-1482-combined-ext4.ova
Hyper-V (x86_64 Hyper-V image)	v2.2.12	Airwall-x86_64_r2.2.12-1482-combined-ext4.vhdx

Airwall Agent and Airwall Server Software

For the latest iOS and Android Airwall Agents, search for "Airwall Agent" in the store for your device.

Note: **For** Airwall Agents and Servers that are not part of this release, see the latest version available at Latest firmware and software on page 514.

Laptop or Mobile Device	Version	Download
Airwall Agents		
macOS, OSX	v2.2.12	Airwall-Mac_2.2.12.1977.pkg
Windows 64-bit PC	v2.2.12	**Installer** – AirwallAgent64-bit_2.2.12.353_Installer.exe **Express Installer** – AirwallAgent64-bit_2.2.12.353_ExpressInstaller.exe **Unattended Installer** – AirwallAgent64-bit_UnattendedInstaller_2.2.12.353.msi
Airwall Servers		
Windows 64-bit Server	v2.2.12	**Installer** –AirwallServer64-bit_2.2.12.353_Installer.exe **Express Installer** – AirwallServer64-bit_2.2.12.353_ExpressInstaller.exe **Unattended Installer** – AirwallServer64-bit_UnattendedInstaller_2.2.12.353.msi

2.2.11 firmware and software

Please follow the links below to download the 2.2.11 firmware and software. For release notes, see Release Notes 2.2.11 on page 639.

Note: Also review Hotfixes on page 548 for any hotfix releases.

Conductor firmware

Conductor	Version	Download
Conductor – All platforms	v2.2.11	Conductor_r2.2.11-1432_package

Airwall Gateway firmware

Airwall Gateway model	Version	Download
75 (mvebu64)	v2.2.11	Airwall-mvebu64_r2.2.11-1053_package
100g and 100e (ramips)	v2.2.11	Airwall-ramips_r2.2.11-1126_package
mvebu (All 110-, 150-, and 250-series)	v2.2.11	Airwall-mvebu_r2.2.11-1179_package
x86_64 (100rc, virtual 300-series, 400-series, and 500-series)	v2.2.11	Airwall-x86_64_r2.2.11-1390_package
x86_64 OVA (ESXi)	v2.2.11	Airwall-x86_64_r2.2.11-1390-combined-ext4.ova
x86_64 Hyper-V image	v2.2.11	Airwall-x86_64_r2.2.11-1390-combined-ext4.vhdx

Airwall Agents and Servers Software

For the latest iOS and Android Airwall Agents, search for "Airwall Agent" in the store for your device.

Link	Applies To	File Name
Airwall Agents		
Download 2.2.11	macOS, OSX Airwall Agent	Airwall-Mac_2.2.11.1775.pkg
Download 2.2.11	Windows 64 Airwall Agent Install	AirwallAgent64-bit_2.2.11.333_Installer.exe
Download 2.2.11	Windows 64 Airwall Agent Express Install	AirwallAgent64-bit_2.2.11.333_ExpressInstaller.exe
Download 2.2.11	Windows 64 Unattended Install	AirwallAgent64-bit_UnattendedInstaller_2.2.11.333.msi
Airwall Servers		
Download 2.2.11	Linux/Ubuntu v16 Airwall Server	airwall-2.2.11.Ubuntu16.amd64.deb
Download 2.2.11	Linux/Ubuntu v18 and v20 Airwall Server	airwall-2.2.11.Ubuntu18.amd64.deb
Download 2.2.11	Linux/CentOS 8 Airwall Server	airwall-2.2.11.Centos8.x86_64.rpm
Download 2.2.11	Linux/CentOS 7 Airwall Server	airwall-2.2.11.Centos7.x86_64.rpm
Download 2.2.11	Linux/Fedora Airwall Server	airwall-2.2.11.Fedora33.x86_64.rpm
Download 2.2.11	Windows Server 64 Airwall Server Install	AirwallServer64-bit_2.2.11.333_Installer.exe
Download 2.2.11	Windows Server 64 Airwall Server Express Install	AirwallServer64-bit_2.2.11.333_ExpressInstaller.exe
Download 2.2.11	Windows Server 64 Airwall Server Unattended Install	AirwallServer64-bit_UnattendedInstaller_2.2.11.333.msi

Cellular Modem Firmware Updates

Link	Applies To	File Name
Download	Airwall Gateway 110	Airwall-110_cellfw-9224c85-106_package
Download	Airwall Gateway 150	Airwall-150_cellfw-9224c85-106_package
Download	Airwall Gateway 250	Airwall-250_cellfw-9224c85-106_package

Windows Serial Port Drivers

Link	Applies To	File Name
Download	Windows, 64-bit Airwall 100, 110, and 150	Airwall1XXSerialDriver_x64.msi

2.2.10 firmware and software

Please follow the links below to download the 2.2.10 firmware and software. For release notes, see Release Notes 2.2.10 on page 652.

Note: Also review Hotfixes on page 548 for any hotfix releases.

Conductor firmware

Link	Applies To	File Name
Download	Conductor - All Platforms	Conductor_r2.2.10-1286_package

Airwall Gateway firmware

Link	Applies To	File Name
Download	Airwall mvebu64 (All 75-series)	Airwall-mvebu64_r2.2.10-921_package
Download	Airwall ramips (100g and 100e Airwall Gateways)	Airwall-ramips_r2.2.10-999_package
Download	Airwall mvebu (All 110-, 150-, and 250-series Airwall Gateways)	Airwall-mvebu_r2.2.10-1065_package
Download	Airwall x86_64 (100rc, virtual 300-series, 400-series, and 500-series Airwall Gateways)	Airwall-x86_64_r2.2.10-1251_package
Download	Airwall x86_64 OVA (ESXi)	Airwall-x86_64_r2.2.10-1251-combined-ext4.ova

Airwall Agents and Servers Software

For the latest iOS and Android Airwall Agents, search for "Airwall Agent" in the store for your device.

Link	Applies To	File Name
Airwall Agents		
Download 2.2.10	macOS, OSX Airwall Agent	Airwall-Mac-2.2.10-1594-signed.pkg
Download 2.2.10	Windows 64 Airwall Agent Install	AirwallAgent64-bit_2.2.10_Installer.exe
Download 2.2.10	Windows 64 Airwall Agent Express Install	AirwallAgent64-bit_2.2.10_ExpressInstaller.exe
Download 2.2.10	Windows 64 Unattended Install	AirwallAgent64-bit_UnattendedInstaller_2.2.10.msi
Airwall Servers		
Download 2.2.10	Linux/Ubuntu v16 Airwall Server	airwall-2.2.10.Ubuntu16.amd64.deb
Download 2.2.10	Linux/Ubuntu v18 and v20 Airwall Server	airwall-2.2.10.Ubuntu18.amd64.deb
Download 2.2.10	Linux/CentOS 8 Airwall Server	airwall-2.2.10.Centos8.x86_64.rpm
Download 2.2.10	Linux/CentOS 7 Airwall Server	airwall-2.2.10.Centos7.x86_64.rpm
Download 2.2.10	Linux/Fedora 2.7 Airwall Server	airwall-2.2.10.Fedora27.x86_64.rpm
Download 2.2.10	Windows Server 64 Airwall Server Install	AirwallServer64-bit_2.2.10_Installer.exe

Link	Applies To	File Name
Download 2.2.10	Windows Server 64 Airwall Server Express Install	AirwallServer64-bit_2.2.10_ExpressInstaller.exe
Download 2.2.10	Windows Server 64 Airwall Server Unattended Install	AirwallServer64-bit_UnattendedInstaller_2.2.10.msi

Cellular Modem Firmware Updates

Link	Applies To	File Name
Download	Airwall Gateway 110	Airwall-110_cellfw-9224c85-106_package
Download	Airwall Gateway 150	Airwall-150_cellfw-9224c85-106_package
Download	Airwall Gateway 250	Airwall-250_cellfw-9224c85-106_package

Windows Serial Port Drivers

Link	Applies To	File Name
Download	Windows, 64-bit Airwall 100, 110, and 150	Airwall1XXSerialDriver_x64.msi

2.2.8 firmware and software

Please follow the links below to download the 2.2.8 firmware and software. For release notes, see Release Notes 2.2.8 on page 673.

Note: Also review Hotfixes on page 548 for any hotfix releases.

Conductor firmware

Link	Applies To	File Name
Download	Conductor - All Platforms	Conductor_r2.2.8-1102_package

Airwall firmware

Link	Applies To	File Name
Download	Airwall mvebu64 (All 75-series)	Airwall-mvebu64_r2.2.8-767_package
Download	Airwall ramips (100g and 100e Airwall Gateways)	Airwall-ramips_r2.2.8-846_package
Download	Airwall mvebu (All 150-series and 250-series Airwall Gateways)	Airwall-mvebu_r2.2.8-863_package
Download	Airwall x86_64 (100rc, virtual 300-series, 400-series, and 500-series Airwall Gateways)	Airwall-x86_64_r2.2.8-1043_package
Download	Airwall x86_64 OVA (ESXi)	Airwall-x86_64_r2.2.8-1043-combined-ext4.ova

Airwall Agent and Airwall Server Software

For the latest iOS and Android Airwall Agents, search for "Airwall Agent" in the store for your device.

Link	Applies To	File Name
Airwall Agents		
Download 2.2.8 update	macOS, OSX Airwall Agent	Airwall-Mac-2.2.8-signed.pkg
Download 2.2.8 update	Windows 64 Airwall Agent Install	AirwallAgent64-bit_2.2.8_Installer.exe
Download 2.2.8 update	Windows 64 Airwall Agent Express Install	AirwallAgent64_ExpressInstaller_2.2.8.exe
Download 2.2.8 update	Windows 64 Unattended Install	AirwallAgent64-bit_UnattendedInstaller_2.2.8.msi
Airwall Servers		
Download 2.2.8 update	Linux/Ubuntu v16 Airwall Server	airwall-ubuntu16_2.2.8_amd64.deb
Download 2.2.8 update	Linux/Ubuntu v18 and v20 Airwall Server	airwall-ubuntu18_2.2.8_amd64.deb
Download 2.2.8 update	Linux/CentOS 8 Airwall Server	airwall-Centos8_2.2.8_x86_64.rpm
Download 2.2.8 update	Linux/CentOS 7 Airwall Server	airwall-Centos7_2.2.8_x86_64.rpm
Download 2.2.8 update	Linux/Fedora 2.7 Airwall Server	airwall-Fedora27_2.2.8_x86_64.rpm
Download 2.2.8 update	Windows Server 64 Airwall Server Install	AirwallServer64-bit_2.2.8_Installer.exe
Download 2.2.8 update	Windows Server 64 Airwall Server Express Install	AirwallServer64_2.2.8_ExpressInstaller.exe
Download 2.2.8 update	Windows Server 64 Airwall Server Unattended Install	AirwallServer64-bit_UnattendedInstaller_2.2.8.msi

Cellular Modem Firmware Upgrades

Link	Applies To	File Name
Download		HIPswitch-150_cellfw-12ddb86-r12_package
Download		HIPswitch-250_cellfw-12ddb86-r2_package
Download		HIPswitch-250_cellfw-12ddb86-r1_package

Windows Serial Port Drivers

Link	Applies To	File Name
Download	Windows, 32-bit Airwall 150	HIPswitch150Driver_x86.msi
Download	Windows, 64-bit Airwall 150	HIPswitch150Driver_x64.msi

2.2.5 firmware and software

Please follow the links below to download the 2.2.5 firmware and software. For release notes, see Release Notes 2.2.5 on page 685:

Conductor firmware

Link	Applies To	File Name
Download	Conductor - All Platforms	Conductor_r2.2.5-907_package

Airwall firmware

Link	Applies To	File Name
Download	Airwall mvebu64 (All 75-series)	Airwall-mvebu64_r2.2.5-630_package
Download	Airwall ramips (100g and 100e Airwall Gateways)	Airwall-ramips_r2.2.5-711_package
Download	Airwall mvebu (All 150-series and 250-series Airwall Gateways)	Airwall-mvebu_r2.2.5-731_package
Download	Airwall x86_64 (100rc, virtual 300-series, 400-series, and 500-series Airwall Gateways)	Airwall-x86_64_r2.2.5-890_package
Download	Airwall x86_64 OVA (ESXi)	Airwall-x86_64_r2.2.5-890-combined-ext4.ova

Airwall Agent and Airwall Server Software

Link	Applies To	File Name
Airwall Agents		
Download	macOS, OSX Airwall Agent	Airwall-Mac-2.2.3-1270-signed.pkg
Download	Windows 64 Airwall Agent Install	AirwallClient64_2.2.3.620_20200218_Installer.exe
Download	Windows 64 Airwall Agent Express Install	AirwallClient64_2.2.3.648_ExpressInstaller.exe
Download	Windows 64 Unattended Install	AirwallClient64_UnattendedInstaller_2.2.3.msi
Download	Windows 64 Airwall Agent Upgrade Package (2.2.2 to 2.2.3 only)	Airwall-Winclient_64_r2.2.3-620_package
Airwall Servers		
Download	Linux/Ubuntu v16 Airwall Server	airwall-ubuntu16_2.2.3-469_amd64.deb
Download	Linux/Ubuntu v18 Airwall Server	airwall-ubuntu18_2.2.3-377_amd64.deb
Download	Linux/CentOS 8 Airwall Server	airwall-2.2.3-124.el8.x86_64.rpm
Download	Linux/CentOS 7 Airwall Server	airwall-2.2.3-449.el7.x86_64.rpm
Download	Linux/Fedora 2.7 Airwall Server	airwall-2.2.3-151.fc27.x86_64.rpm
Download	Windows Server 64 Airwall Server Install	AirwallServer64_2.2.3.623_20200218_Installer.exe

Link	Applies To	File Name
Download	Windows Server 64 Airwall Server Express Install	AirwallServer64_2.2.3.651_ExpressInstaller.exe
Download	Windows Server 64 Airwall Server Unattended Install	AirwallServer64_UnattendedInstaller_2.2.3.msi
Download	Windows 64 Airwall Server Upgrade Package (2.2.2 to 2.2.3 only)	Airwall-Winserver_64_r2.2.3-623_package

Cellular Modem Firmware Upgrades

Link	Applies To	File Name
Download		HIPswitch-150_cellfw-12ddb86-r12_package
Download		HIPswitch-250_cellfw-12ddb86-r2_package
Download		HIPswitch-250_cellfw-12ddb86-r1_package

Windows Serial Port Drivers

Link	Applies To	File Name
Download	Windows, 32-bit Airwall 150	HIPswitch150Driver_x86.msi
Download	Windows, 64-bit Airwall 150	HIPswitch150Driver_x64.msi

2.2.3 firmware and software

Please follow the links below to download the 2.2.3 firmware and software. For release notes, see Release Notes 2.2.3 on page 688:

Conductor firmware

Link	Applies To	File Name
Download	Conductor - All Platforms	Conductor_r2.2.3-805_package

Airwall firmware

Link	Applies To	File Name
Download	Airwall mvebu64 (All 75-series)	Airwall-mvebu64_r2.2.3-546_package
Download	Airwall ramips (100g and 100e Airwall Gateways)	Airwall-ramips_r2.2.3-629_package
Download	Airwall mvebu (All 150-series and 250-series Airwall Gateways)	Airwall-mvebu_r2.2.3-648_package
Download	Airwall x86_64 (100rc, virtual 300-series, 400-series, and 500-series Airwall Gateways)	Airwall-x86_64_r2.2.3-802_package

Link	Applies To	File Name
Download	Airwall x86_64 OVA (ESXi)	Airwall-x86_64_r2.2.3-802-combined-ext4.ova

Airwall Agent and Airwall Server Software

Link	Applies To	File Name
Airwall Agents		
Download	macOS, OSX Airwall Agent	Airwall-Mac-2.2.3-signed.pkg
Download	Windows 64 Airwall Agent Install	AirwallClient64_2.2.3_Installer.exe
Download	Windows 64 Airwall Agent Express Install	AirwallClient64_ExpressInstaller_2.2.3.exe
Download	Windows 64 Unattended Install	AirwallClient64_UnattendedInstaller_2.2.3.msi
Download	Windows 64 Airwall Agent Upgrade Package (2.2.2 to 2.2.3 only)	Airwall-Winclient_64_r2.2.3_package
Airwall Servers		
Download	Linux/Ubuntu v16 Airwall Server	airwall-ubuntu16_2.2.3_amd64.deb
Download	Linux/Ubuntu v18 Airwall Server	airwall-ubuntu18_2.2.3_amd64.deb
Download	Linux/CentOS 8 Airwall Server	airwall-2.2.3.el8.x86_64.rpm
Download	Linux/CentOS 7 Airwall Server	airwall-2.2.3.el7.x86_64.rpm
Download	Linux/Fedora 2.7 Airwall Server	airwall-2.2.3.fc27.x86_64.rpm
Download	Windows Server 64 Airwall Server Install	AirwallServer64_2.2.3_Installer.exe
Download	Windows Server 64 Airwall Server Express Install	AirwallServer64_2.2.3_ExpressInstaller.exe
Download	Windows Server 64 Airwall Server Unattended Install	AirwallServer64_UnattendedInstaller_2.2.3.msi
Download	Windows 64 Airwall Server Upgrade Package (2.2.2 to 2.2.3 only)	Airwall-Winserver_64_r2.2.3_package

Cellular modem firmware

Firmware updated May 19, 2022

Please follow the links below to download firmware:

Checksums:	MD5 SHA-1

Cellular Modem Firmware Updates

Airwall Gateway Model	Download
110g – Hotfix for T-Mobile IPv4 settings	Airwall-110_cellfw-923f147-130_package
110 – See note	Airwall-110_cellfw-2e8314c-129_package
110 – Hotfix for AT&T and T-Mobile 3G Sunset	Airwall-110_cellfw-4c5753a-125_package

Airwall Gateway Model	Download
Advantech – See note	Airwall-112_cellfw-2e8314c-129_package
Advantech – Hotfix for AT&T 3G Sunset	Airwall-112_cellfw-4c5753a-125_package
150 – See note	Airwall-150_cellfw-2e8314c-129_package
250 – See note	Airwall-250_cellfw-2e8314c-129_package

Note: Contains an updated map of Mobile County Code and Mobile Network Code values, most notably a change of some codes that formerly identified T-Mobile that now identify AT&T.

Serial drivers

64-bit drivers updated Dec 16, 2020

Please follow the links below to download serial drivers for your Airwall Gateway. If you need instructions for accessing the Airwall Gateway via the console port, see Connecting to the console port on an Airwall Gateway on page 297.

Checksums: MD5 SHA-1

Airwall 75

The PL2303 Chip is built into the Airwall 75 to provide serial connectivity to the console. However, the driver is not included out-of-the-box with Windows or macOS, so you need to download it from the manufacturer's site and install it before you connect.

Download: Windows | macOS

Airwall 110 and 150

A custom chip built into these Airwall Gateways to provides serial connectivity to the console. This chip has drivers for Linux and macOS built-in, but Windows requires you to download and install a driver before you can connect.

Download:

- Windows, 32-bit – Available on request (contact Customer Success at Customer Success).
- Windows, 64-bit – 110 or 150 (Dec 2020 update)

Airwall 250

The FT232RL chip is built into the Airwall 250 to provide serial connectivity to the console. However, this driver is not included out-of-the-box with Windows or OSX/macOS, so you need to download it before you connect.

Download: All platforms

Older downloads

Downloads for 2.1.x to 2.2.2 firmware and software versions. For firmware downloads for versions 1.12.1 through 2.0.x, see the pre-2.2.3 software downloads page.

2.2.2 firmware and software

Please follow the links below to download version 2.2.2 firmware:

Checksums:

Conductor firmware

Link	Applies To	File Name
Download	Conductor (All Platforms, Azure see below)	Conductor_r2.2.2-587_package
Download	Conductor, Azure	Conductor-azure_r2.2.2-587_package

HIPswitch firmware

Link	Applies To	File Name
Download	HIPswitch mvebu64 (All 75-series HIPswitches)	HIPswitch-mvebu64_r2.2.2-394_package
Download	HIPswitch ramips (100g and 100e HIPswitches)	HIPswitch-ramips_r2.2.2-480_package
Download	HIPswitch mvebu (All 150-series and 250-series HIPswitches)	HIPswitch-mvebu_r2.2.2-483_package
Download	HIPswitch x86_64 (100rc, virtual 300-series, 400-series, and 500-series HIPswitches)	HIPswitch-x86_64_r2.2.2-594_package
Download	HIPswitch x86_64 OVA (ESXi)	HIPswitch-x86_64_r2.2.2-598-combined-ext4.ova
Download	HIPswitch x86_64 (Azure)	HIPswitch-x86_64-azure_r2.2.2-598_package

Software

Link	Applies To	File Name
Download	HIPclient (OSX, macOS)	HIPclient_2.2.1.924.pkg
Download	HIPclient (Windows 32) Express Install	HIPclient32_2.2.2.378_ExpressInstaller.exe
Download	HIPclient (Windows 64) Express Install	HIPclient64_2.2.2.432_ExpressInstaller.exe
Download	HIPserver (Linux/Ubuntu v16)	hipserver_2.2.2-307_amd64.deb
Download	HIPserver (Linux/Ubuntu v18)	hipserver_2.2.2-213_amd64.deb
Download	HIPserver (Linux/CentOS)	hipserver-2.2.2-291.el7.x86_64.rpm
Download	HIPserver (Windows Server 64) Express Install	HIPserver64_2.2.2.443_ExpressInstaller.exe

Cellular Modem Firmware Upgrades

Link	Applies To	File Name
Download		HIPswitch-150_cellfw-12ddb86-r12_package

Link	Applies To	File Name
Download		HIPswitch-250_cellfw-12ddb86-r2_package
Download		HIPswitch-250_cellfw-12ddb86-r1_package

Windows Serial Port Drivers

Link	Applies To	File Name
Download	HIPswitch 150 (Windows, 32-bit)	HIPswitch150Driver_x86.msi
Download	HIPswitch 150 (Windows, 64-bit)	HIPswitch150Driver_x64.msi

2.2.1 firmware and software

Please follow the links below to download version 2.2.1 firmware:

Checksums:

Conductor firmware

Link	Applies To	File Name
Download	Conductor (All Platforms, Azure see below)	Conductor_r2.2.1-466_package
Download	Conductor, Azure	Conductor-azure_r2.2.1-466_package

HIPswitch firmware

Link	Applies To	File Name
Download	HIPswitch mvebu64 (All 75-series HIPswitches)	HIPswitch-mvebu64_r2.2.1-294_package
Download	HIPswitch ramips (100g and 100e HIPswitches)	HIPswitch-ramips_r2.2.1-390_package
Download	HIPswitch mvebu (All 150-series and 250-series HIPswitches)	HIPswitch-mvebu_r2.2.1-391_package
Download	HIPswitch x86_64 (100rc, virtual 300-series, 400-series, and 500-series HIPswitches)	HIPswitch-x86_64_r2.2.1-479_package
Download	HIPswitch x86_64 OVA (ESXi)	HIPswitch-x86_64_r2.2.1-479-combined-ext4.ova
Download	HIPswitch x86_64 (Azure)	HIPswitch-x86_64-azure_r2.2.1-479_package
Download	HIPswitch x86_64 VHD (Hyper-V)	HIPswitch-x86_64_r2.2.1-479-combined-ext4.vhd

Software

Link	Applies To	File Name
Download	HIPclient (Windows, 32-bit)	HIPclient32_2.2.1_Installer.exe
Download	HIPclient (Windows, 32-bit), Unattended Install	HIPclient32_UnattendedInstaller_2.2.1.msi
Download	HIPclient (Windows, 32-bit), Express Install	HIPclient32_2.2.1_ExpressInstaller.exe
Download	HIPclient (Windows, 64-bit)	HIPclient64_2.2.1_Installer.exe
Download	HIPclient (Windows, 64-bit), Unattended Install	HIPclient64_UnattendedInstaller_2.2.1.msi
Download	HIPclient (Windows, 64-bit), Express Install	HIPclient64_2.2.1_ExpressInstaller.exe
Download	HIPserver (Windows, 64-bit)	HIPserver64_2.2.1_Installer.exe
Download	HIPserver (Windows, 64-bit), Unattended Install	HIPserver64_UnattendedInstaller_2.2.1.msi
Download	HIPserver (Windows, 64-bit), Express Install	HIPserver64_2.2.1_ExpressInstaller.exe
Download	HIPclient (OSX, macOS)	HIPclient_2.2.1.pkg
Download	HIPserver (Linux/Ubuntu v16)	hipserver_Ubuntu16-2.2.1_amd64.deb
Download	HIPserver (Linux/Ubuntu v18)	hipserver_Ubuntu18-2.2.1_amd64.deb
Download	HIPserver (Linux/CentOS)	hipserver_Centos7-2.2.1_x86_64.rpm

Cellular Modem Firmware Upgrades

Link	Applies To	File Name
Download		HIPswitch-150_cellfw-12ddb86-r12_package
Download		HIPswitch-250_cellfw-12ddb86-r2_package
Download		HIPswitch-250_cellfw-12ddb86-r1_package

Windows Serial Port Drivers

Link	Applies To	File Name
Download	HIPswitch 150 (Windows, 32-bit)	HIPswitch150Driver_x86.msi
Download	HIPswitch 150 (Windows, 64-bit)	HIPswitch150Driver_x64.msi

2.1.7 firmware and software

Please follow the links below to download version 2.1.7 firmware:

Checksums:	MD5 SHA-1

Conductor firmware

Link	Applies To	File Name
Download	Conductor (All Platforms, Azure see below)	Conductor_r2.1.7-1308_package

HIPswitch firmware

Link	Applies To	File Name
Download	HIPswitch mvebu64 (All 75-series HIPswitches)	HIPswitch-mvebu64_r2.1.7-628_package
Download	HIPswitch ramips (100g and 100e HIPswitches)	HIPswitch-ramips_r2.1.7-1095_package
Download	HIPswitch mvebu (All 150-series and 250-series HIPswitches)	HIPswitch-mvebu_r2.1.7-1250_package
Download	HIPswitch x86_64 (100rc, all 300-series, 400-series, and 500-series HIPswitches)	HIPswitch-x86_64_r2.1.7-1512_package
Download	HIPswitch x86_64 OVA (ESXi)	HIPswitch-x86_64_r2.1.7-1523-combined-ext4.ova
Download	HIPswitch x86_64 VHD (Hyper-V)	HIPswitch-x86_64_r2.1.7-1523-combined-ext4.vhdx

Software

Note: In this maintainence release, our HIP clients and HIP servers remain unchanged from version 2.1.6.

Link	Applies To	File Name
Download	HIPclient (Windows, 32-bit)	HIPclient32_2.1.6.326_20190222_Installer.exe
Download	HIPclient (Windows, 64-bit)	HIPclient64_2.1.6.636_20190222_Installer.exe
Download	HIPserver (Windows, 32-bit)	HIPserver32_2.1.6.250_20190301_Installer.exe
Download	HIPserver (Windows, 64-bit)	HIPserver64_2.1.6.804_20190301_Installer.exe
Download	HIPclient (OSX, macOS)	HIPclient_2.1.6.1209.pkg
Download	HIPserver (Linux/Ubuntu)	hipserver_2.1.6-1007_amd64.deb
Download	HIPserver (Linux/CentOS)	hipserver-2.1.6-805.el7.x86_64.rpm

Cellular Modem Firmware Upgrades

Link	Applies To	File Name
Download		HIPswitch-150_cellfw-12ddb86-r12_package
Download		HIPswitch-250_cellfw-12ddb86-r2_package
Download		HIPswitch-250_cellfw-12ddb86-r1_package

Windows Serial Port Drivers

Link	Applies To	File Name
Download	HIPswitch 150 (Windows, 32-bit)	HIPswitch150Driver_x86.msi
Download	HIPswitch 150 (Windows, 64-bit)	HIPswitch150Driver_x64.msi

2.1.6 firmware and software

Please follow the links below to download version 2.1.6 firmware:

Checksums:	MD5 SHA-1

Conductor firmware

Link	Applies To	File Name
Download	Conductor (All Platforms, Azure see below)	Conductor_r2.1.6-1144_package
Download	Conductor, Azure	Conductor_r2.1.6-752-azure_package

HIPswitch firmware

Link	Applies To	File Name
Download	HIPswitch mvebu64 (All 75-series HIPswitches)	HIPswitch-mvebu64_r2.1.6-472_package
Download	HIPswitch ramips (100g and 100e HIPswitches)	HIPswitch-ramips_r2.1.6-941_package
Download	HIPswitch mvebu (All 150-series and 250-series HIPswitches)	HIPswitch-mvebu_r2.1.6-1070_package
Download	HIPswitch x86_64 (100rc, all 300-series, 400-series, and 500-series HIPswitches)	HIPswitch-x86_64_r2.1.6-1357_package
Download	HIPswitch x86_64 OVA (ESXi)	HIPswitch-x86_64_r2.1.6-1357-combined-ext4.ova
Download	HIPswitch x86_64 (Azure)	HIPswitch-x86_64_r2.1.6-781-azure_package
Download	HIPswitch x86_64 VHD (Hyper-V)	HIPswitch-x86_64_r2.1.6-1357-combined-ext4.vhd

Software

Link	Applies To	File Name
Download	HIPclient (Windows, 32-bit)	HIPclient32_2.1.6_Installer.exe
Download	HIPclient (Windows, 64-bit)	HIPclient64_2.1.6_Installer.exe
Download	HIPserver (Windows, 32-bit)	HIPserver32_2.1.6_Installer.exe
Download	HIPserver (Windows, 64-bit)	HIPserver64_2.1.6_Installer.exe
Download	HIPclient (OSX, macOS)	HIPclient_2.1.6.pkg

Link	Applies To	File Name
Download	HIPserver (Linux/Ubuntu)	hipserver_2.1.6_amd64.deb
Download	HIPserver (Linux/CentOS)	hipserver-2.1.6-805.el7.x86_64.rpm

Cellular Modem Firmware Upgrades

Link	Applies To	File Name
Download		HIPswitch-150_cellfw-12ddb86-r12_package
Download		HIPswitch-250_cellfw-12ddb86-r2_package
Download		HIPswitch-250_cellfw-12ddb86-r1_package

Windows Serial Port Drivers

Link	Applies To	File Name
Download	HIPswitch 150 (Windows, 32-bit)	HIPswitch150Driver_x86.msi
Download	HIPswitch 150 (Windows, 64-bit)	HIPswitch150Driver_x64.msi

2.1.5 firmware and software

Please follow the links below to download version 2.1.5 firmware:

Checksums:	MD5 SHA-1

Conductor firmware

Link	Applies To	File Name
Download	Conductor (All Platforms)	Conductor_r2.1.5-1035_package
Download	Conductor, Azure	Conductor_r2.1.5-660-azure_package

Airwall Gateway firmware

Link	Applies To	File Name
Download	Airwall mvebu64 (All 75-series Airwall Gateways)	HIPswitch-mvebu64_r2.1.5-372_package
Download	Airwall ramips (100g and 100e Airwall Gateways)	HIPswitch-ramips_r2.1.5-840_package
Download	Airwall mvebu (All 150-series and 250-series Airwall Gateways)	HIPswitch-mvebu_r2.1.5-972_package
Download	Airwall x86_64 (100rc, all 300-series, 400-series, and 500-series Airwall Gateways)	HIPswitch-x86_64_r2.1.5-1249_package
Download	Airwall x86_64 (Azure)	HIPswitch-x86_64_r2.1.5-687-azure_package

Link	Applies To	File Name
Download	Airwall x86_64 OVA (ESXi)	HIPswitch-x86_64_r2.1.5-1249-combined-ext4.ova
Download	Airwall x86_64 VHD (Hyper-V)	HIPswitch-x86_64_r2.1.5-1249-combined-ext4.vhd

Software

Link	Applies To	File Name
Download	HIPclient (Windows, 64-bit)	HIPclient64_2.1.5.537_20181212_Installer.exe
Download	HIPclient (Windows, 32-bit)	HIPclient32_2.1.5.240_20181212_Installer.exe
Download	HIPserver (Windows, 64-bit)	HIPserver64_2.1.5.706_20181212_Installer.exe
Download	HIPserver (Windows, 32-bit)	HIPserver32_2.1.5.154_20181212_Installer.exe
Download	HIPclient (OSX, macOS)	HIPclient_2.1.5.1119.pkg
Download	HIPserver (Linux/Ubuntu)	hipserver_2.1.5-922_amd64.deb
Download	HIPserver (Linux/CentOS)	hipserver-2.1.5-720.el7.x86_64.rpm

2.1.4 firmware and software

Please follow the links below to download version 2.1.4 firmware:

Conductor firmware

Link	Applies To	File Name	File Size	Checksum
Download	Conductor (All Platforms, Azure see below)	Conductor_r2.1.4-954_package	108612787	**MD5:** 7a6e0c14fc3b68ff5f2291 **SHA 1:** f938cb958ab7d2bb2d68d
Download	Conductor, Azure	Conductor_r2.1.4-585-azure_package	113228503	**MD5:** 846221fbecccb8021bab9 **SHA-1:** 6ebe7af9b51a076c90e08

Airwall Gateway firmware

Link	Applies To	File Name	File Size	Checksum
Download	Airwall mvebu64 (All 75-series Airwall Gateways)	HIPswitch-mvebu64_r2.1.4-305_package	27864195	**MD5:** 6c0c2ef1ffb64c66b641cf **SHA-1:** b37df06dab38c08c4ad9a
Download	Airwall ramips (100g and 100e Airwall Gateways)	HIPswitch-ramips_r2.1.4-777_package	12840142	**MD5:** e14c89e5b47b303ef8f60 **SHA-1:** c138075c7b6427fb99b2a
Download	Airwall mvebu (All 250-series Airwall Gateways)	HIPswitch-mvebu_r2.1.4-891_package	22979484	**MD5:** 6c2c2e9a5e2ddb03dc9da **SHA-1:** 58bdeabc3c404676bc43d

Link	Applies To	File Name	File Size	Checksum
Download	Airwall x86_64 (100rc, all 300-series, 400-series, and 500-series Airwall Gateways)	HIPswitch-x86_64_r2.1.4-1182_package	18311139	**MD5:** ec430c60e0e7f36e19f2a6 **SHA-1:** 3a67079f798d1b6b3f682
Download	Airwall x86_64 OVA (ESXi)	HIPswitch-x86_64_r2.1.4-1182-combined-ext4.ova	20084736	**MD5:** 3cd09a8a879c6ed734b78 **SHA-1:** 64298c83d9f9e530df9aa3
Download	Airwall x86_64 VHD (Hyper-V)	HIPswitch-x86_64_r2.1.4-1182-combined-ext4.vhd	139461120	**MD5:** 44febc8e50d44ea6362e0 **SHA-1:** 5ef4dc6ffa08f0c0153d98

Software

Link	Applies To	File Name	File Size	Checksum
Download	Airwall Agent (Windows)	HIPclient64_2.1.4.457_20161014_Installer.exe	18262545	**MD5:** e4b21604879c2dd7acc67 **SHA-1:** 220f6f9f99514619b1913
Download	Airwall Server (Windows)	HIPserver64_2.1.4.631_20161015_Installer.exe	18265504	**MD5:** 3aa38ed65aa812fd5f865a **SHA-1:** b8a495810624a5afcbbd3
Download	Airwall Agent (OSX, macOS)	HIPclient_2.1.4.1046.pkg	6940415	**MD5:** a9ac9996a9623bd79d8b5 **SHA-1:** 517b031d2f96db3063faf
Download	Airwall Server (Linux/Ubuntu)	hipserver_2.1.4-858_amd64.deb	3364166	**MD5:** 98691f27c5b98d4ad1994 **SHA-1:** bebfe567c10c992198182
Download	Airwall Server (Linux/CentOS)	hipserver-2.1.4-655.el7.x86_64.rpm	3269241	**MD5:** 9f3d8dd6f56e8ef92d9a78 **SHA-1:** 4542be30ae588a11d2a25

2.1.3 firmware and software

Please follow the links below to download version 2.1.3 firmware:

Conductor firmware:

- Conductor (All platforms)

Airwall firmware:

- HIPswitch ramips (100g and 100e HIPswitches)
- Airwall Gateway Cns3xxx (All 200-series Airwall Gateways)

  Important: The HIPswitch 200 Series is not supported on software versions later than 2.1.2. Please see product bulletin End of Life for HIPswitch 200 Series for more information.
- Airwall mvebu (All 250-series Airwall Gateways)
- HIPswitch x86_64 (100rc, all 300-series, 400-series, and 500-series HIPswitches)

Software:

- Airwall Agent (Windows)
- Airwall Server (Windows)
- Airwall Agent (MacOS)
- Airwall Server (Linux/Ubuntu)
- Airwall Server (Linux/CentOS)

Note: The iOSAirwall Agent is available in the App Store.

Virtual Images:

- HIPswitch x86_64 OVA (ESXi)
- HIPswitch x86_64 VHD (Hyper-V)

2.1.2 firmware and software

Please follow the links below to download version 2.1.2 firmware:

Conductor firmware:

- Conductor (All platforms)

HIPswitch firmware:

- HIPswitch ramips (100g and 100e Airwall Gateways)
- HIPswitch Cns3xxx (All 200-series Airwall Gateways)
- HIPswitch_mvebu (All 250-series Airwall Gateways)
- HIPswitch x86_64 (100rc, all 300-series and 400-series Airwall Gateways)

Software:

- Airwall Agent (Windows)
- Airwall Server (Windows)
- Airwall Agent (MacOS)

Virtual Images:

- HIPswitch x86_64 OVA (ESXi)
- HIPswitch x86_64 VHD (Hyper-V)

Hotfixes

Updated May 19, 2022

Please follow the links below to download the hotfix for your platform. For hotfixes before 2.1.x, see pre-Airwall Hotfixes.

Cellular Hotfixes

Cellular Modem Firmware for:	Download
110g – Hotfix for T-Mobile IPv4 settings	Airwall-110_cellfw-923f147-130_package
Hotfix for 3G Sunset (AT&T and T-Mobile) – 110 Airwall Gateway	Airwall-110_cellfw-4c5753a-125_package

Cellular Modem Firmware for:	Download
Hotfix for 3G Sunset (AT&T and T-Mobile) – Advantech Airwall Gateway	Airwall-112_cellfw-4c5753a-125_package

2.2.12 Hotfixes

Download	Applies to:	Date	Behavior
2.2.12 Conductor Hotfix HF-15748	2.2.12 Conductors	May 28, 2021	See Release Notes 2.2.12 Hotfix – Conductor HF-15748 on page 628.

2.2.11 Hotfixes

Download	Applies to:	Date	Behavior
2.2.11 Conductor Hotfix HF-1	2.2.11 Conductors	Apr 13, 2021	See Release Notes 2.2.11 Hotfix – Conductor HF-1 on page 637.
2.2.11 Airwall Gateway Hotfix HF-2	2.2.11 Airwall Gateways	Mar 30, 2021	See Release Notes 2.2.11 Hotfix – Airwall Gateway HF-2 on page 638.
2.2.11 Airwall Gateway Hotfix HF-1	2.2.11 Airwall Gateways	Mar 17, 2021	See Release Notes 2.2.11 Hotfix – Airwall Gateway HF-1 on page 639.

2.2.10 Hotfixes

Download	Applies to:	Date	Behavior
2.2.10 Airwall Gateway Hotfix HF-1	2.2.10 Airwall Gateways	Dec 16, 2020	See Release Notes 2.2.10 Hotfix – Airwall Gateway HF-1 on page 650.
2.2.10 Conductor Hotfix HF-1	2.2.10 Conductor	Dec 16, 2020	See Release Notes 2.2.10 Hotfix – Conductor HF-1 on page 651

2.2.8 Hotfixes

Download	Applies to:	Date	Behavior	Notes
Conductor HF-5 Includes Conductor HF-1 through HF-4	2.2.8	Dec 18, 2020	Short password reset timeout for new users.	See Release Notes 2.2.8 Hotfix – Conductor HF-5 on page 666.

Download	Applies to:	Date	Behavior	Notes
TPM keystore Airwall Gateway Hotfix-14558	2.2.8	Nov 18, 2020	Airwall Gateways using a TPM keystore fail to upgrade to 2.2.10.	For v2.2.8 Airwall Gateways that use a TPM keystore, install this hotfix before upgrading to v2.2.10.
Airwall Gateway Hotfix HF-3 Includes HF-1 and 2	2.2.8 Airwall Gateways	Oct 19, 2020	See Release Notes 2.2.8 Hotfix – Airwall Gateway HF-3 on page 669	Install the hotfix to resolve issues fixed in this hotfix, or in retired Airwall Gateway hotfixes HF-2 or HF-1.
2.2.8 Conductor Hotfix HF-4 Includes HF-1, 2, and 3	2.2.8 Conductor	Oct 19, 2020	Release Notes 2.2.8 Hotfix – Conductor HF-4 on page 670	Install the hotfix to resolve issues fixed in this hotfix, or in retired Conductor hotfixes HF-3, HF-2, or HF-1.
2.2.8 Airwall Gateway Hotfix-13955	2.2.8 Airwall Gateways	Aug 4, 2020	See Release Notes 2.2.8 Hotfix – Airwall Gateway Hotfix-13955 on page 673.	Install this hotfix before upgrading Airwall Gateways to 2.2.8.
Retired 2.2.8 Hotfixes				
Airwall Gateway Hotfix HF-2 (Retired)	2.2.8 Airwall Gateway	Sep 15, 2020	See Release Notes 2.2.8 Hotfix – Airwall Gateway HF-2 (Retired) on page 770.	Retired
Conductor Hotfix HF-3 (Retired)	2.2.8 Conductor	Sep 3, 2020	See Release Notes 2.2.8 Hotfix – Conductor HF-3 (Retired) on page 773	Retired
Airwall Gateway Hotfix HF-1 (Retired)	2.2.8 Airwall Gateways	Sep 3, 2020	See Release Notes 2.2.8 Hotfix – Airwall Gateway HF-1 (Retired) on page 772.	Retired
2.2.8 Conductor Hotfix HF-2 (Retired)	2.2.8 Conductor	Aug 19, 2020	See Release Notes 2.2.8 Hotfix – Conductor HF-2 (Retired) on page 775	Retired
2.2.8 Conductor Hotfix HF-1 (Retired)	2.2.8 Conductor	July 30, 2020	See Release Notes 2.2.8 Hotfix – Conductor HF-1 (Retired) on page 776.	Retired

2.1.x Series Hotfixes

Download	Applies to:	Date	Behavior	Resolution
Hotfix 8551	HIPswitch 250 Series running version 2.1.3	August 23, 2018	HIPswitch repeatedly connects and disconnects. See Product Bulletin 201808B-001 for more information.	Apply Hotfix 8551 to resolve the issue.
Hotfix 8543	HIPswitch 100 Series running version 2.1.3	August 23, 2018	HIPswitch repeatedly connects and disconnects. See Product Bulletin 201808B-001 for more information.	Apply Hotfix 8543 to resolve the issue.
Hotfix 7414	2.1.2 virtual HIPswitches running in VMware ESXi	March 15, 2018	VMware reports 100% CPU usage when running a 2.1.2 virtual HIPswitch	Apply Hotfix 7414 to resolve the issue.

Release Notes

Release notes track incremental improvements and major releases for the Airwall solution, software applications, and our physical, virtual, and cloud platforms. For older Release Notes, see pre-2.2.3 help.

Latest Release Notes (v3.2.4)

This topic is linked from the Conductor. Talk to dev before renaming or removing.

Release Notes v3.3.0

Release Date: August, 2023

Update Considerations

You may want to update to this version to use the following features:

- Updated Windows Airwall Agent
- Airwall support for Kubernetes (on Dell 5300 running RedHat)
- Airwall WSS proxy traversal
- Conductor scalability improvements
- Airwall support for HA in the Cloud
- Bypass performance and scalability improvements
- Security improvements

This update addresses the following issues:

- Security update for an OpenSSL vulnerability (CVE-2023-2650) - OpenSSL version has been updated to 1.1.1u (for OpenWRT).

What's New in 3.3.0

This version of the Airwall Solution includes several usability and functionality improvements that can simplify and streamline the setup and diagnostics for an Airwall secure network.

Device group shows overlay networks

In the Conductor, the device groups page now shows overlay membership.

New and Improved Conductor Features

Learn more –

-
-

New and Updated Help

In addition to the content added for new features linked above, here's the new and updated content published since our last major release:

New –

- Set Up Intrusion Prevention on page 138
- Enable HIP on Conductor on page 274

Updated –

- Set up Microsoft Azure as a cloud provider on page 434
- Set up Google Cloud as a cloud provider on page 438
- Set up Amazon Web Services (AWS) as a cloud provider on page 433
- Manually deploy a Conductor on the Google Cloud Platform (GCP) on page 219
- Google Cloud (GCP) – Set up an Airwall Gateway on page 334
- Create an Event Monitor on page 119
- Local Bypass on page 394
- Backhaul Bypass on page 395
- Run the Conductor as an Airwall Relay on page 354
- Configure Airwall Relay rules on page 353

Downloads

For firmware and software downloads for this version, see 3.3.0 firmware and software on page 516.

Deprecations

Fixes

ID	Applies to	Description
AWDEV-393	Airwall Agent	Updated Linux Agent OpenSSL to 3.0.9
AWDEV-389	Airwall Gateway	Fixed an issue where bypass gateways cannot be HA paired using UDP heartbeat.
AWDEV-369	General	Updated c-ares to 1.19.1.
AWDEV-260	General	Updated Dropbear to 2022.82.
AWDEV-218	General	Updated Snort rule sets to latest.

ID	Applies to	Description
AWDEV-204	Conductor	Fixed an issue where Connectivity Checker shows null rather than specific IP range.
AWDEV-189	Conductor	Fixed an issue that causes iptables load error on bypass port.
AWDEV-129	Conductor	Fixed an issue where network admins could not successfully upgrade Airwall firmware in the Conductor.
AWDEV-107	Conductor	Updated Libwebsockets from 3.1.0 to 4.3.2.

Known Issues

ID	Applies to	Description
DEV-18144	Conductor	The Connectivity Checker.
DEV-17887	Cloud, Conductor	If you use unrecognized credentials when calling jobs on a cloud Airwall Gateway, the Conductor sends multiple error messages when it tries to call route injection and validate cloud attributes. Workaround -- Make sure your cloud credentials are correct and update the credentials on the "Cloud providers" page under Conductor settings.
DEV-17648	Linux Airwall Servers	Many Airshell functions (including changing log level) are non-functional until you have configured and licensed your Conductor.
DEV-17263	Conductor	If you fix a conflict in a smart device group by changing the IP of one of the conflicted devices, sometimes the change in IP does not result in the device being removed from the group and the change is not propagated to the Airwall Gateway. **Workaround** – Fully remove the device from the smart device group and then add it back again.
DEV-16503	macOS Airwall Agent	Deleting a profile does not immediately delete the associated private key. **Workaround** - After deleting a profile, switch to a different profile before creating a new profile. If you've already created the new profile, delete it, switch, and then re-create it.
DEV-16431	Conductor	When specifying a port mirror destination IP address, ensure that it doesn't conflict with any of the Airwall Gateway's local device IPs
DEV-16397	Conductor	If you change the LSI prefix and have port mirroring configured, you need to either reboot the Conductor, or go to **Settings** > **Diagnostics** and select **Restart metadata cache** to update the LSI prefix.
DEV-16068	Amazon Web Services Conductor	To enable enhanced networking for a cloud Amazon Web Services Airwall Gateway or Conductor, use the custom images instead of the marketplace image.
DEV-16067	Cloud, Conductor, Airwall Gateways	If you are adding a new interface to an existing cloud Airwall Gateway, you must set the source and destination check to false (see your cloud provider for the terminology they use for source and destination checks).

ID	Applies to	Description
DEV-16059	Airwall Gateways	When HA-pairing two Airwall Gateways that do not have the HA link plugged in correctly, the Conductor displays no actionable error message and the HA setup never completes.
DEV-15982	Conductor	Traffic stats reporting graphs generally show a smooth curve between data points. However, over time the graph can show up with sharper angles. The data is still correct, but this is a known issue with the graphing library used by the Conductor.
DEV-15945	Airwall Gateways	If you configure port mirroring using a remote destination local device, GRE/ERSPAN traffic from remote Airwall Gateways will arrive with a source IP in the LSI prefix (defaults to 1.0.0.0/8).
DEV-15923	Airwall Gateways	When you run **Check secure tunnels** on a v3.0 Airwall Gateway, the check falsely reports a bad tunnel status for any peer airwall running a firmware version that is v2.2.8 or lower.
DEV-15887	Airwall Gateways	You cannot currently add VLAN interfaces to the Ruggedcom platform.
DEV-15808	Google Cloud Airwall Gateways	Google Cloud Airwall Gateways with the same VM name have the same device serial number, which can result in a failure when you make a license request in the Conductor. **Workaround** – In Google Cloud, use unique deployment names (VM names) for Airwall Gateways.
DEV-15791	AIrwall Gateway	On the Airwall Gateway 100, Port 2 might be inactive after a factory-reset. **Workaround** - After a factory reset, manually reboot the Airwall Gateway 100.
DEV-15705	iOS, Android Airwall Agent	Establishing a tunnel TO a mobile Airwall Agent (iOS or Android) fails when there is no Airwall Relay involved. **Workaround** - Establish the tunnel FROM the mobile Airwall Agent.
DEV-15787	macOS Airwall Agents	If a person who already has a profile makes a Request to Connect from the Remote Access User portal on the same Conductor, no profile is created. **Workaround** – If the user wants a second profile, they can use an invite code or enter the Conductor information manually.

ID	Applies to	Description
DEV-15572	Airwall Gateways	If you do not specify a gateway in the DHCP server configuration, the DHCP client cannot configure a default gateway. **Workaround** – Unless you want to configure a single isolated subnet, always specify a gateway. For example, a subnet for networked PDUs that should not have any outside connectivity aside from remote access through an Airwall Gateway, and used in conjunction with SNAT over the overlay port group. See DHCP server is not serving as a gateway on page 802
DEV-15489	Windows Airwall Agent	Windows 7 sends an extra Windows system popup when the Windows Airwall Agent UserAuth prompt appears. You can safely ignore this popup.
DEV-15357	macOS Airwall Agent	If you update the macOS Airwall Agent to a release later than v2.2.11 on macOS Mojave using a Conductor-based update package, it may not report the updated version to the Conductor. **Workaround** - Restart the Airwall Agent or reapply the update.
DEV-15302	macOS Airwall Agent	The profile for a macOS Airwall Agent does not work correctly when restored to a new computer using Time Machine. **Workaround** - Create a new profile on the Airwall Agent, and then on the Conductor, replace the old profile with the new one.
DEV-15219	Cellular 110g Airwall Gateways	The Airwall Gateway 110g does not work on the Bell Mobility (Canada) cellular provider because they require the use of a http/https proxy.
DEV-15031	Airwall Gateways	Remote syslog over TLS doesn't work when using keys stored in TPM.
DEV-14860	Conductor	Airwall Gateways on older firmware (pre v2.2.0) may send passively-discovered device events to the Conductor even when the feature is off.
DEV-14835	Conductor	Airwall Gateway 150 serial numbers look like exponentiated numbers to Windows Excel, so the column displaying the Serial number shows xxxEyyy instead of the full serial number.
DEV-14739	Airwall Gateways	If you set IPv4 to DHCPv4 and set a static IP address for IPv6, the setting that you set second doesn't get saved. **Workaround** – If you need both IPv4 and IPv6, set static IP addresses for both.

ID	Applies to	Description
DEV-14736	Cellular Airwall Gateways	Cellular details may display as "unavailable" on the first boot after you update anAirwall Gateway. The cellular connections are not affected. **Workaround** – Reboot the Airwall Gateway again to correctly display the cellular details.
DEV-14726	Conductor	If you are viewing an Android Airwall Agent **Ports** tab and the Airwall Agent changes how it is connected to the Conductor (for example, from WiFi to cellular), the display does not update correctly. **Workaround** – Refresh the page.
DEV-14610	Conductor	After changing the Reporting traffic stats reporting time, the CPU graph does not display. **Workaround** – Refresh your browser page.
DEV-14584	Cellular Airwall Gateways	Hot-swapping the SIM on an Airwall Gateway 110 with firmware version v2.2.11 may not work. **Workaround** – Reboot the Airwall Gateway after installing a new SIM card.
DEV-14551	Conductor	The Android Airwall Agent lets you press the **Edit Settings** button on the **Ports** page; however, submitting any changes to the page results in an error message.
DEV-14426	Conductor, Airwall Gateways	Bypass destinations with a hostname do not show device activity in the Conductor.
DEV-14308	OpenHIP	Initial packets are dropped while building a new tunnel to a new peer Airwall Gateway.
DEV-14223	Google Cloud	Add an overlay IP to agent in order to talk to device behind Google 300v.
DEV-14218	Airwall Gateways	NAT broadcast applied to traffic between ports within a single port group. Use an external switch if you need to connect multiple devices to a single port group and use the NAT broadcast feature and require IP broadcast un-NATed between those local devices.
DEV-14015	OpenHIP	If an Airwall Relay is also used as a bypass gateway, Airwall Edge Services behind the relay are not able to use that relay. **Workaround** – Deploy multiple relays so at least one relay is usable by each pair of Airwall Edge Services that need to communicate.
DEV-13775	Azure Cloud Airwall Gateways	The Conductor might rarely give a "Net::ReadTimeout" error when you try to deploy an Azure Airwall Gateway 300v or server. This error doesn't indicate that the deployment has failed. If you get this error message, go to Azure portal and check the actual deployment result.
DEV-13650	Conductor	SoIP device activity is not being reported on an Airwall Gateway **Local Devices** tab.

ID	Applies to	Description
DEV-13640	Conductor	Airwall Relay diagnostics do not work on a Standby Conductor.
DEV-13633	Conductor	A standby Conductor shows available firmware downloads, but they cannot be downloaded. **Workaround** – Download firmware from the active Conductor.
DEV-13620	Conductor	In **Airwall** > **Ports** > **Failover settings**, the failover ping occurs only every "ping rate" + "ping timeout" seconds, somewhat unexpectedly.
DEV-13607	Conductor, Airwall Gateways	Creating a link failover group (**Airwall** > **Ports** > **Failover settings**) does not apply the settings to any port groups. You must also assign the failover group to port groups on the **Ports** page.
DEV-13588	Conductor	Opening the Conductor on Internet Explorer 11 can be very slow for medium to large deployments. **Workaround** – Use the latest version of Chrome, Firefox, or Edge instead.
DEV-13536	Windows Airwall Agent	When you uninstall the Windows Airwall Agent, it does not remove the tun-tap driver. **Workaround** - Delete the driver from C:\Windows \System32\drivers\tnw-tap.sys.
DEV-13531	Cloud Conductor	Automatically creating Cloud HA Conductors only works if you use the same cloud provider for both active and standby Conductors. For example, AWS HA Active and AWS HA Standby. **Workaround** – You can manually set up different cloud providers as HA pair Conductors.
DEV-13474	Airwall Gateways	If you configure multiple overlay port groups with the same overlay IP subnet (same or different IP addresses) and then create a local device equal to the entire subnet with port affinity set, it may not lead to the expected result.
DEV-13331	Alibaba Cloud Airwall Gateways	The Alibaba Cloud Conductor system time is incorrect. **Workaround** – Change the Conductor system time to browser time: In Conductor **Settings**, under **System time**, select **Edit Settings**, select **Set browser time**, and then select **Update Settings**.
DEV-13195	Conductor, Airwall Gateways	When you upgrade a Cellular Airwall Gateway-150 from 2.2.3 to 2.2.5, the cellular details all become "Unavailable." **Workaround** – Reboot and the details return.

ID	Applies to	Description
DEV-13194	Conductor	**Check Connectivity** > **Ping Local Devices** for an Airwall Gateway fails in Internet Explorer 11 if one of the devices is defined as a CIDR. **Workaround** – Use one of the latest versions of Chrome, Firefox, Safari or Edge.
DEV-11710	macOS Airwall Agents	If you change the LSI prefix on the Conductor, the macOS Airwall Agent doesn't update the routes correctly. **Workaround** – Close and reopen the macOS Airwall Agent.
12852	Windows Airwall Agent	Windows by default doesn't allow multiple 'active' interfaces. It prefers ethernet over cellular whenever possible. **Workaround** - Set Windows to keep multiple interfaces open by editing the fMinimizeConnections registry value: **1.** Hold the Windows Key and Press R. **2.** In the run dialog, type regedit and click OK. **3.** Navigate to the following path in Registry Editor: HKEY_LOCAL_MACHINE\SOFTWARE\Policies \Microsoft\Windows\WcmSvc\4 **4.** See if the GroupPolicy subkey exists. If not with, WcmSvc highlighted, right click on WcmSvc and Choose New > Key and name it GroupPolicy. **5.** Right-click GroupPolicy and choose New > DWORD (32-bit) > Create value. **6.** Name the value "fMinimizeConnections," and select OK. (The value should be 0, or false). **7.** Reboot and test.
DEV-10590	Cloud Airwall Gateways	The Conductor does not display an error when adding a route that would exceed the maximum number of allowed routes in the cloud provider.
DEV-10039	Airwall Gateways	An Airwall Gateway-150 can show "could not detect attached switch" intermittently.
DEV-9546	Airwall Gateways, Airwall Gateways 150	The Airwall Gateway-150 serial connection has an intermittent issue when large amounts of data are sent over the console.
DEV-9429	Windows Airwall Agent	When you update the Overlay Device IP address for a Windows Airwall Server in the Conductor, it doesn't always update the first time. **Workaround** - Open and update the address a second time.

Release Notes v3.2.4

Release Date: May, 2023

Update Considerations

Important: This release is a combination of 3.2.3 and 3.2.4.

You may want to update to this version to use the following features:

- Use region bypass, see Region bypass on page 397.
- Switch between Conductors from the Airwall Agent (macOS) dropdown menu, see Connect with an Apple (OSX and macOS) Airwall Agent on page 19.

This update addresses the following issues:

- API bypass device creation
- incorrect connectivity checker graph display
- traffic disruption from multiple hostnames with same IP
- Airsh ssh-key add command cloud failure

What's New in 3.2.4

This version of the Airwall Solution includes several usability and functionality improvements that can simplify and streamline the setup and diagnostics for an Airwall secure network.

Region Bypass

Use bypass regions to group and load-balance bypass gateways by region. A bypass region is configured by creating a region tag. Add the region tag (or tags) to one or more bypass egress gateways and to the Airwalls you want to use with the region bypass egress gateways. See Region bypass on page 397 and Create a Tag on page 100.

Airwall Agent Conductor toggle

You can now toggle between Conductors in the Airwall Agent (macOS) without opening Configure box, see Connect with an Apple (OSX and macOS) Airwall Agent on page 19.

Airwall AV3200g Installation Guide

There is now a specific installation guide for Airwall AV3200g, see Airwall Gateway AV3200g Hardware Installation Guide on page 281.

Airwall AV3033 Installation Guide

There is now a specific installation guide for Airwall AV3033, see Airwall Gateway AV3033 Hardware Installation Guide on page 284

New and Improved Conductor Features

Learn more –

-
-

New and Updated Help

In addition to the content added for new features linked above, here’s the new and updated content published since our last major release:

New –

- Region bypass on page 397
- Airwall Gateway AV3200g Hardware Installation Guide on page 281
- Airwall Gateway AV3033 Hardware Installation Guide on page 284

Updated –

- Airwall Gateway Hardware Installation Guide on page 276
- Airshell (airsh) Command Reference on page 362
- Create a Tag on page 100
- Add Interfaces to a Port on page 389

Downloads

For firmware and software downloads for this version, see 3.2.4 firmware and software on page 517.

Deprecations

Deprecating system setting for Preferred Airwall agent version. This setting indicated what version of the Airwall Agent would be linked from the remote user access portal. Beginning in v3.2, only the most recent version of each Airwall Agent will be available. Customers that want to distribute older versions of the Airwall Agent can still make those available to their users.

Fixes

ID	Applies to	Description
DEV-18688	Conductor	Fixed an issue where agile devices did not show their identifier in the device discovery dialog.
DEV-18616	TMSTAT	Fixed interger overflow in displayed timer values in tmstat / airsh table output on 32 bit platforms.
DEV-18536	API, Conductor	Fixed an issue that prevented creaing bypass devices via the API.
DEV-18496	Conductor	Fixed an issue where using the connectivity checker swap button would display an incorrect graph.
DEV-18484	Common	Upgraded zlib to 1.2.13
DEV-18478	Airwall Gateway	Improve reliability with complex overlay configurations and multiple port groups, added additional heartbeats when applying policy changes after applying configuration to each port group.
DEV-18477	Airwall Gateway	We fixed a bug that could disrupt traffic to DNS bypass hosts if multiple hostnames resolve to the same IP.
DEV-18405	Conductor	Fixed an issue where devices might not be added to or removed from a tag-based smart device group when Airwalls are added to or removed from an Airwall group with the specified tag.
DEV-18402	Conductor	Fixed a bug that could cause Airwalls to appear offline while connected to the Conductor.
DEV-18394	Conductor	Fixed an issue where a user would get a misleading set of recommendations from the connectivity checker if their Airwalls could not talk directly, were in a relay rule and the relay rule contained no relays.
DEV-18385	Conductor, Airwall Gateway	Fixed an issue where the ping all devices diagnostic tool did not work with agile devices.
DEV-18379	Conductor	Fixed an issue where updating the global API token expiration would extend the API token expiration of users that have a more specific expiration.
DEV-18218	Conductor	Fixed a bug that caused the Airsh ssh-key add command to fail on cloud Airwalls.
DEV-18113	Conductor	Fixed an issue where references to revoked or factory reset Airwalls could be left in bypass gateway configuration when they shouldn't be.

Known Issues

ID	Applies to	Description
DEV-18144	Conductor	The Connectivity Checker.
DEV-17887	Cloud, Conductor	If you use unrecognized credentials when calling jobs on a cloud Airwall Gateway, the Conductor sends multiple error messages when it tries to call route injection and validate cloud attributes. Workaround -- Make sure your cloud credentials are correct and update the credentials on the "Cloud providers" page under Conductor settings.
DEV-17648	Linux Airwall Servers	Many Airshell functions (including changing log level) are non-functional until you have configured and licensed your Conductor.
DEV-17263	Conductor	If you fix a conflict in a smart device group by changing the IP of one of the conflicted devices, sometimes the change in IP does not result in the device being removed from the group and the change is not propagated to the Airwall Gateway. **Workaround** – Fully remove the device from the smart device group and then add it back again.
DEV-16503	macOS Airwall Agent	Deleting a profile does not immediately delete the associated private key. **Workaround** - After deleting a profile, switch to a different profile before creating a new profile. If you've already created the new profile, delete it, switch, and then re-create it.
DEV-16431	Conductor	When specifying a port mirror destination IP address, ensure that it doesn't conflict with any of the Airwall Gateway's local device IPs
DEV-16397	Conductor	If you change the LSI prefix and have port mirroring configured, you need to either reboot the Conductor, or go to **Settings** > **Diagnostics** and select **Restart metadata cache** to update the LSI prefix.
DEV-16068	Amazon Web Services Conductor	To enable enhanced networking for a cloud Amazon Web Services Airwall Gateway or Conductor, use the custom images instead of the marketplace image.
DEV-16067	Cloud, Conductor, Airwall Gateways	If you are adding a new interface to an existing cloud Airwall Gateway, you must set the source and destination check to false (see your cloud provider for the terminology they use for source and destination checks).
DEV-16059	Airwall Gateways	When HA-pairing two Airwall Gateways that do not have the HA link plugged in correctly, the Conductor displays no actionable error message and the HA setup never completes.
DEV-15982	Conductor	Traffic stats reporting graphs generally show a smooth curve between data points. However, over time the graph can show up with sharper angles. The data is still correct, but this is a known issue with the graphing library used by the Conductor.

ID	Applies to	Description
DEV-15945	Airwall Gateways	If you configure port mirroring using a remote destination local device, GRE/ERSPAN traffic from remote Airwall Gateways will arrive with a source IP in the LSI prefix (defaults to 1.0.0.0/8).
DEV-15923	Airwall Gateways	When you run **Check secure tunnels** on a v3.0 Airwall Gateway, the check falsely reports a bad tunnel status for any peer airwall running a firmware version that is v2.2.8 or lower.
DEV-15887	Airwall Gateways	You cannot currently add VLAN interfaces to the Ruggedcom platform.
DEV-15808	Google Cloud Airwall Gateways	Google Cloud Airwall Gateways with the same VM name have the same device serial number, which can result in a failure when you make a license request in the Conductor. **Workaround** – In Google Cloud, use unique deployment names (VM names) for Airwall Gateways.
DEV-15791	AIrwall Gateway	On the Airwall Gateway 100, Port 2 might be inactive after a factory-reset. **Workaround** - After a factory reset, manually reboot the Airwall Gateway 100.
DEV-15705	iOS, Android Airwall Agent	Establishing a tunnel TO a mobile Airwall Agent (iOS or Android) fails when there is no Airwall Relay involved. **Workaround** - Establish the tunnel FROM the mobile Airwall Agent.
DEV-15787	macOS Airwall Agents	If a person who already has a profile makes a Request to Connect from the Remote Access User portal on the same Conductor, no profile is created. **Workaround** – If the user wants a second profile, they can use an invite code or enter the Conductor information manually.
DEV-15572	Airwall Gateways	If you do not specify a gateway in the DHCP server configuration, the DHCP client cannot configure a default gateway. **Workaround** – Unless you want to configure a single isolated subnet, always specify a gateway. For example, a subnet for networked PDUs that should not have any outside connectivity aside from remote access through an Airwall Gateway, and used in conjunction with SNAT over the overlay port group. See DHCP server is not serving as a gateway on page 802.
DEV-15489	Windows Airwall Agent	Windows 7 sends an extra Windows system popup when the Windows Airwall Agent UserAuth prompt appears. You can safely ignore this popup.

ID	Applies to	Description
DEV-15357	macOS Airwall Agent	If you update the macOS Airwall Agent to a release later than v2.2.11 on macOS Mojave using a Conductor-based update package, it may not report the updated version to the Conductor. **Workaround** - Restart the Airwall Agent or reapply the update.
DEV-15302	macOS Airwall Agent	The profile for a macOS Airwall Agent does not work correctly when restored to a new computer using Time Machine. **Workaround** - Create a new profile on the Airwall Agent, and then on the Conductor, replace the old profile with the new one.
DEV-15219	Cellular 110g Airwall Gateways	The Airwall Gateway 110g does not work on the Bell Mobility (Canada) cellular provider because they require the use of a http/https proxy.
DEV-15031	Airwall Gateways	Remote syslog over TLS doesn't work when using keys stored in TPM.
DEV-14860	Conductor	Airwall Gateways on older firmware (pre v2.2.0) may send passively-discovered device events to the Conductor even when the feature is off.
DEV-14835	Conductor	Airwall Gateway 150 serial numbers look like exponentiated numbers to Windows Excel, so the column displaying the Serial number shows xxxEyyy instead of the full serial number.
DEV-14739	Airwall Gateways	If you set IPv4 to DHCPv4 and set a static IP address for IPv6, the setting that you set second doesn't get saved. **Workaround** – If you need both IPv4 and IPv6, set static IP addresses for both.
DEV-14736	Cellular Airwall Gateways	Cellular details may display as "unavailable" on the first boot after you update anAirwall Gateway. The cellular connections are not affected. **Workaround** – Reboot the Airwall Gateway again to correctly display the cellular details.
DEV-14726	Conductor	If you are viewing an Android Airwall Agent **Ports** tab and the Airwall Agent changes how it is connected to the Conductor (for example, from WiFi to cellular), the display does not update correctly. **Workaround** – Refresh the page.
DEV-14610	Conductor	After changing the Reporting traffic stats reporting time, the CPU graph does not display. **Workaround** – Refresh your browser page.

ID	Applies to	Description
DEV-14584	Cellular Airwall Gateways	Hot-swapping the SIM on an Airwall Gateway 110 with firmware version v2.2.11 may not work. **Workaround** – Reboot the Airwall Gateway after installing a new SIM card.
DEV-14551	Conductor	The Android Airwall Agent lets you press the **Edit Settings** button on the **Ports** page; however, submitting any changes to the page results in an error message.
DEV-14426	Conductor, Airwall Gateways	Bypass destinations with a hostname do not show device activity in the Conductor.
DEV-14308	OpenHIP	Initial packets are dropped while building a new tunnel to a new peer Airwall Gateway.
DEV-14223	Google Cloud	Add an overlay IP to agent in order to talk to device behind Google 300v.
DEV-14218	Airwall Gateways	NAT broadcast applied to traffic between ports within a single port group. Use an external switch if you need to connect multiple devices to a single port group and use the NAT broadcast feature and require IP broadcast un-NATed between those local devices.
DEV-14015	OpenHIP	If an Airwall Relay is also used as a bypass gateway, Airwall Edge Services behind the relay are not able to use that relay. **Workaround** – Deploy multiple relays so at least one relay is usable by each pair of Airwall Edge Services that need to communicate.
DEV-13775	Azure Cloud Airwall Gateways	The Conductor might rarely give a "Net::ReadTimeout" error when you try to deploy an Azure Airwall Gateway 300v or server. This error doesn't indicate that the deployment has failed. If you get this error message, go to Azure portal and check the actual deployment result.
DEV-13650	Conductor	SoIP device activity is not being reported on an Airwall Gateway **Local Devices** tab.
DEV-13640	Conductor	Airwall Relay diagnostics do not work on a Standby Conductor.
DEV-13633	Conductor	A standby Conductor shows available firmware downloads, but they cannot be downloaded. **Workaround** – Download firmware from the active Conductor.
DEV-13620	Conductor	In **Airwall** > **Ports** > **Failover settings**, the failover ping occurs only every "ping rate" + "ping timeout" seconds, somewhat unexpectedly.
DEV-13607	Conductor, Airwall Gateways	Creating a link failover group (**Airwall** > **Ports** > **Failover settings**) does not apply the settings to any port groups. You must also assign the failover group to port groups on the **Ports** page.

ID	Applies to	Description
DEV-13588	Conductor	Opening the Conductor on Internet Explorer 11 can be very slow for medium to large deployments. **Workaround** – Use the latest version of Chrome, Firefox, or Edge instead.
DEV-13536	Windows Airwall Agent	When you uninstall the Windows Airwall Agent, it does not remove the tun-tap driver. **Workaround** - Delete the driver from C:\Windows \System32\drivers\tnw-tap.sys.
DEV-13531	Cloud Conductor	Automatically creating Cloud HA Conductors only works if you use the same cloud provider for both active and standby Conductors. For example, AWS HA Active and AWS HA Standby. **Workaround** – You can manually set up different cloud providers as HA pair Conductors.
DEV-13474	Airwall Gateways	If you configure multiple overlay port groups with the same overlay IP subnet (same or different IP addresses) and then create a local device equal to the entire subnet with port affinity set, it may not lead to the expected result.
DEV-13331	Alibaba Cloud Airwall Gateways	The Alibaba Cloud Conductor system time is incorrect. **Workaround** – Change the Conductor system time to browser time: In Conductor **Settings**, under **System time**, select **Edit Settings**, select **Set browser time**, and then select **Update Settings**.
DEV-13195	Conductor, Airwall Gateways	When you upgrade a Cellular Airwall Gateway-150 from 2.2.3 to 2.2.5, the cellular details all become "Unavailable." **Workaround** – Reboot and the details return.
DEV-13194	Conductor	**Check Connectivity** > **Ping Local Devices** for an Airwall Gateway fails in Internet Explorer 11 if one of the devices is defined as a CIDR. **Workaround** – Use one of the latest versions of Chrome, Firefox, Safari or Edge.
DEV-11710	macOS Airwall Agents	If you change the LSI prefix on the Conductor, the macOS Airwall Agent doesn't update the routes correctly. **Workaround** – Close and reopen the macOS Airwall Agent.

ID	Applies to	Description
12852	Windows Airwall Agent	Windows by default doesn't allow multiple 'active' interfaces. It prefers ethernet over cellular whenever possible. **Workaround** - Set Windows to keep multiple interfaces open by editing the fMinimizeConnections registry value: **1.** Hold the Windows Key and Press R. **2.** In the run dialog, type regedit and click OK. **3.** Navigate to the following path in Registry Editor: HKEY_LOCAL_MACHINE\SOFTWARE\Policies \Microsoft\Windows\WcmSvc\4 **4.** See if the GroupPolicy subkey exists. If not with, WcmSvc highlighted, right click on WcmSvc and Choose New > Key and name it GroupPolicy. **5.** Right-click GroupPolicy and choose New > DWORD (32-bit) > Create value. **6.** Name the value "fMinimizeConnections," and select OK. (The value should be 0, or false). **7.** Reboot and test.
DEV-10590	Cloud Airwall Gateways	The Conductor does not display an error when adding a route that would exceed the maximum number of allowed routes in the cloud provider.
DEV-10039	Airwall Gateways	An Airwall Gateway-150 can show "could not detect attached switch" intermittently.
DEV-9546	Airwall Gateways, Airwall Gateways 150	The Airwall Gateway-150 serial connection has an intermittent issue when large amounts of data are sent over the console.
DEV-9429	Windows Airwall Agent	When you update the Overlay Device IP address for a Windows Airwall Server in the Conductor, it doesn't always update the first time. **Workaround** - Open and update the address a second time.

Release Notes v3.1.2

Release Date: November 30, 2022

Update Considerations

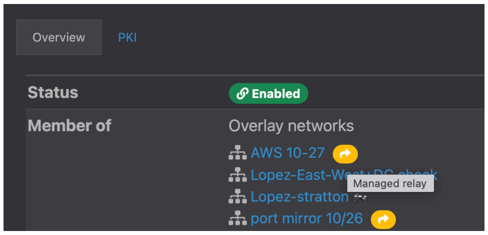
Important: Update downtime – When you update a Conductor, there may be database and configuration changes related to the new release that require Airwall Edge Services to update their configuration data, resulting in downtime while secure tunnels are re-established. Downtime is typically up to, and in most cases is much less than, two minutes.

This update addresses the following issues:

- Map server deadlock.
- Remote logging failure.
- M2 chatter reduction.
- JsonRPC server deadlock.
- MAC address validation.

New Features

- New airsh command allows a user to see the port group IDs using `conf net list`, see Airshell (airsh) Command Reference on page 362.
- On an Airwall details view you can now see which overlay networks use managed relay rules.



Status: Enabled

Member of: Overlay networks
- AWS 10-27
- Lopez-East-West+DC check
- Lopez-stratton
- port mirror 10/26

Downloads

For firmware and software downloads for this version, see 3.1.2 firmware and software on page 518.

Deprecations

Deprecating system setting for Preferred Airwall agent version. This setting indicated what version of the Airwall agent would be linked from the remote user access portal. Beginning in v3.2, only the most recent version of each Airwall agent will be available. Customers that want to distribute older versions of the Airwall agent can still make those available to their users.

Fixes

ID	Applies to	Description
DEV-18305	Conductor	Fixed an issue where Conductor could not verify the certificate of some OpenID Connect providers.
DEV-18291	Conductor	Fixed an issue where a custom MAP port would revert back to the original 8096 port on upgrade.
DEV-18273	Conductor	Fixed an issue where both IPs of NATed devices may not display correctly when navigating directly to the device.
DEV-18254	Conductor	Fixed a bug that could cause a deadlock in the map server.
DEV-18252	Conductor	Large custom logos should be properly resized on the login screen.
DEV-18251	Common	zlib upgraded to 1.2.12.
DEV-18250	Common	util-linux upgraded to 2.38.
DEV-18249	Conductor	Fixed an issue where the managed Airwall name would sometimes be blank for Airwall invites.
DEV-18239	BaseOS	Upgrade lib c-ares to 1.18.1.
DEV-18235	Conductor	Fixed an issue that caused remote logging to fail for the Conductor.
DEV-18220	Conductor	Fixed an issue where overlay managed relay rules might not include needed bypass gateways.
DEV-18216	Conductor	Fixed an issue causing a JS exception when a user tried to access a context menu in the overlay graph after deleting a device from the table on the right.
DEV-18199	Conductor	Reduced m2 chatter when enabling intrusion prevention

ID	Applies to	Description
DEV-18179	Conductor	Fixed an issue where some details about deleted objects were not serialized when using bulk delete.
DEV-18176	Conductor	Fixed coloring issue with diagnostic report in dark mode.
DEV-18173	Conductor	Fixed an issue where a new user that is invited to Conductor and sets their password cannot request an API token without logging out and logging back in.
DEV-18167	Conductor	Fixed issue where device MAC addresses were not properly validated.
DEV-18160	Conductor	Network devices are no longer included in the source or destination options as they are not supported.
DEV-18157	Conductor	Fixed coloring issue with traceroute results in dark mode.
DEV-18156	Conductor	Fixed an issue where the same tag could be added and removed in the "edit tags" dialog resulting in the tag being added.
DEV-18153	Conductor	Fixed an issue where using the quick switcher to switch between overlays would cause the overlay graph layout to be lost.
DEV-18142	Conductor	Fixed an issue where the default values for date range access windows were not being used.
DEV-18137	Conductor	Fixed an issue where the network membership dialog for a people group could be entirely blank when the Conductor contains no overlays.
DEV-18134	Hipswitch	Fixed deadlock in JsonRPC Server.
DEV-18113	Conductor	Fixed an issue where references to revoked or factory reset Airwalls could be left in bypass gateway configuration when they should not be.
DEV-18106	API, Conductor	Fixed the API documentation for api/v1/hipservices/revoke (bulk revoke).
DEV-18102	HIPswitch	Fixed an issue that caused the IDS not to start or reboot in certain configurations.
DEV-18044	airsh	Fixed issue with airsh status dnscache command when a unhandled DNS record type is present in the cache.
DEV-18021	Conductor	Fixed an issue where version numbers and model names were out of order in the Airwall Status report.
DEV-17998	Conductor	Fixed an issue where reports that start in the future could be run.
DEV-17853	Conductor	Fixed an issue that required a refresh for the UI to display that an Airwall's ability to be a bypass gateway has been disabled. The change still took effect, but the browser needed to be refreshed for it to display properly to the user.

ID	Applies to	Description
DEV-16525	Cloud, Conductor	Fixed an issue where, with individual route injection for cloud Airwalls enabled, devices added to groups that already have policy with a cloud Airwall did not correctly update the cloud provider's routing tables.

Known Issues

ID	Applies to	Description
DEV-18144	Conductor	The Connectivity Checker.
DEV-17648	Cloud, Conductor	If you use unrecognized credentials when calling jobs on a cloud Airwall Gateway, the Conductor sends multiple error messages when it tries to call route injection and validate cloud attributes. Workaround -- Make sure your cloud credentials are correct and update the credentials on the "Cloud providers" page under Conductor settings.
DEV-17648	HIPapp-Linux	Many Airshell functions (including changing log level) are non-functional until you have configured and licensed your Conductor.
DEV-17582	HIPswitch	Currently DNS bypass is not HA aware, on a HA failover the contents of the DNS cache are lost and traffic will be blocked until the protected device queries for the DNS name again.
DEV-17263	Conductor	If you fix a conflict in a smart device group by changing the IP of one of the conflicted devices, sometimes the change in IP does not result in the device being removed from the group and the change is not propagated to the Airwall Gateway. Workaround – Fully remove the device from the smart device group and then add it back again.
DEV-16431	Conductor	When specifying a port mirror destination IP address, ensure that it doesn't conflict with any of the Airwall Gateway's local device IPs
DEV-16397	Conductor	If you change the LSI prefix and have port mirroring configured, you need to either reboot the Conductor, or go to **Settings** > **Diagnostics** and select **Restart metadata cache** to update the LSI prefix.
DEV-16068	Amazon Web Services Conductor	To enable enhanced networking for a cloud Amazon Web Services Airwall Gateway or Conductor, use the custom images instead of the marketplace image.
DEV-16067	Cloud, Conductor, Airwall Gateways	If you are adding a new interface to an existing cloud Airwall Gateway, you must set the source and destination check to false (see your cloud provider for the terminology they use for source and destination checks).
DEV-16059	Airwall Gateways	When HA-pairing two Airwall Gateways that do not have the HA link plugged in correctly, the Conductor displays no actionable error message and the HA setup never completes.

ID	Applies to	Description
DEV-15982	Conductor	Traffic stats reporting graphs generally show a smooth curve between data points. However, over time the graph can show up with sharper angles. The data is still correct, but this is a known issue with the graphing library used by the Conductor.
DEV-15945	Airwall Gateways	If you configure port mirroring using a remote destination local device, GRE/ERSPAN traffic from remote Airwall Gateways will arrive with a source IP in the LSI prefix (defaults to 1.0.0.0/8).
DEV-15923	Airwall Gateways	When you run **Check secure tunnels** on a v3.0 Airwall Gateway, the check falsely reports a bad tunnel status for any peer airwall running a firmware version that is v2.2.8 or lower.
DEV-15887	Airwall Gateways	You cannot currently add VLAN interfaces to the Ruggedcom platform.
DEV-15808	Google Cloud Airwall Gateways	Google Cloud Airwall Gateways with the same VM name have the same device serial number, which can result in a failure when you make a license request in the Conductor. **Workaround** – In Google Cloud, use unique deployment names (VM names) for Airwall Gateways.
DEV-15787	macOS Airwall Agents	If a person who already has a profile makes a Request to Connect from the Remote Access User portal on the same Conductor, no profile is created. **Workaround** – If the user wants a second profile, they can use an invite code or enter the Conductor information manually.
DEV-15572	Airwall Gateways	If you do not specify a gateway in the DHCP server configuration, the DHCP client cannot configure a default gateway. **Workaround** – Unless you want to configure a single isolated subnet, always specify a gateway. For example, a subnet for networked PDUs that should not have any outside connectivity aside from remote access through an Airwall Gateway, and used in conjunction with SNAT over the overlay port group. See https://tempered.force.com/TemperedSupportCenter/s/article/DHCP-server-isn-t-serving-as-a-gateway.
DEV-15219	Cellular 110g Airwall Gateways	The Airwall Gateway 110g does not work on the Bell Mobility (Canada) cellular provider because they require the use of a http/https proxy.
DEV-15031	Airwall Gateways	Remote syslog over TLS doesn't work when using keys stored in TPM.
DEV-14860	Conductor	Airwall Gateways on older firmware (pre v2.2.0) may send passively-discovered device events to the Conductor even when the feature is off.

ID	Applies to	Description
DEV-14835	Conductor	Airwall Gateway 150 serial numbers look like exponentiated numbers to Windows Excel, so the column displaying the Serial number shows xxxEyyy instead of the full serial number.
DEV-14739	Airwall Gateways	If you set IPv4 to DHCPv4 and set a static IP address for IPv6, the setting that you set second doesn't get saved. **Workaround** – If you need both IPv4 and IPv6, set static IP addresses for both.
DEV-14736	Cellular Airwall Gateways	Cellular details may display as "unavailable" on the first boot after you update anAirwall Gateway. The cellular connections are not affected. **Workaround** – Reboot the Airwall Gateway again to correctly display the cellular details.
DEV-14726	Conductor	If you are viewing an Android Airwall Agent **Ports** tab and the Airwall Agent changes how it is connected to the Conductor (for example, from WiFi to cellular), the display does not update correctly. **Workaround** – Refresh the page.
DEV-14610	Conductor	After changing the Reporting traffic stats reporting time, the CPU graph does not display. **Workaround** – Refresh your browser page.
DEV-14584	Cellular Airwall Gateways	Hot-swapping the SIM on an Airwall Gateway 110 with firmware version v2.2.11 may not work. **Workaround** – Reboot the Airwall Gateway after installing a new SIM card.
DEV-14551	Conductor	The Android Airwall Agent lets you press the **Edit Settings** button on the **Ports** page; however, submitting any changes to the page results in an error message.
DEV-14426	Conductor, Airwall Gateways	Bypass destinations with a hostname do not show device activity in the Conductor.
DEV-14308	OpenHIP	Initial packets are dropped while building a new tunnel to a new peer Airwall Gateway.
DEV-14223	Google Cloud	Add an overlay IP to agent in order to talk to device behind Google 300v.
DEV-14218	Airwall Gateways	NAT broadcast applied to traffic between ports within a single port group. Use an external switch if you need to connect multiple devices to a single port group and use the NAT broadcast feature and require IP broadcast un-NATed between those local devices.

ID	Applies to	Description
DEV-14015	OpenHIP	If an Airwall Relay is also used as a bypass gateway, Airwall Edge Services behind the relay are not able to use that relay. **Workaround** – Deploy multiple relays so at least one relay is usable by each pair of Airwall Edge Services that need to communicate.
DEV-13775	Azure Cloud Airwall Gateways	The Conductor might rarely give a "Net::ReadTimeout" error when you try to deploy an Azure Airwall Gateway 300v or server. This error doesn't indicate that the deployment has failed. If you get this error message, go to Azure portal and check the actual deployment result.
DEV-13650	Conductor	SoIP device activity is not being reported on an Airwall Gateway **Local Devices** tab.
DEV-13640	Conductor	Airwall Relay diagnostics do not work on a Standby Conductor.
DEV-13633	Conductor	A standby Conductor shows available firmware downloads, but they cannot be downloaded. **Workaround** – Download firmware from the active Conductor.
DEV-13620	Conductor	In **Airwall** > **Ports** > **Failover settings**, the failover ping occurs only every "ping rate" + "ping timeout" seconds, somewhat unexpectedly.
DEV-13607	Conductor, Airwall Gateways	Creating a link failover group (**Airwall** > **Ports** > **Failover settings**) does not apply the settings to any port groups. You must also assign the failover group to port groups on the **Ports** page.
DEV-13588	Conductor	Opening the Conductor on Internet Explorer 11 can be very slow for medium to large deployments. **Workaround** – Use the latest version of Chrome, Firefox, or Edge instead.
DEV-13531	Cloud Conductor	Automatically creating Cloud HA Conductors only works if you use the same cloud provider for both active and standby Conductors. For example, AWS HA Active and AWS HA Standby. **Workaround** – You can manually set up different cloud providers as HA pair Conductors.
DEV-13474	Airwall Gateways	If you configure multiple overlay port groups with the same overlay IP subnet (same or different IP addresses) and then create a local device equal to the entire subnet with port affinity set, it may not lead to the expected result.
DEV-13331	Alibaba Cloud Airwall Gateways	The Alibaba Cloud Conductor system time is incorrect. **Workaround** – Change the Conductor system time to browser time: In Conductor **Settings**, under **System time**, select **Edit Settings**, select **Set browser time**, and then select **Update Settings**.

ID	Applies to	Description
DEV-13195	Conductor, Airwall Gateways	When you upgrade a Cellular Airwall Gateway-150 from 2.2.3 to 2.2.5, the cellular details all become "Unavailable." **Workaround** – Reboot and the details return.
DEV-13194	Conductor	**Check Connectivity** > **Ping Local Devices** for an Airwall Gateway fails in Internet Explorer 11 if one of the devices is defined as a CIDR. **Workaround** – Use one of the latest versions of Chrome, Firefox, Safari or Edge.
DEV-11710	macOS Airwall Agents	If you change the LSI prefix on the Conductor, the macOS Airwall Agent doesn't update the routes correctly. **Workaround** – Close and reopen the macOS Airwall Agent.
DEV-10590	Cloud Airwall Gateways	The Conductor does not display an error when adding a route that would exceed the maximum number of allowed routes in the cloud provider.
DEV-10039	Airwall Gateways	An Airwall Gateway-150 can show "could not detect attached switch" intermittently.
DEV-9546	Airwall Gateways, Airwall Gateways 150	The Airwall Gateway-150 serial connection has an intermittent issue when large amounts of data are sent over the console.

Release Notes v3.1.0

Release Date: Oct 13, 2022

Important Notes

- **Update all v2.1.x Airwall Edge Services** – Update all v2.1.x and earlier Airwall Edge Services with v2.2.x or later before installing v3.0.0. With this release, any Airwall Edge Services running v2.1.x firmware show an error in the Conductor. For more information, see Update v2.1.x Airwall Edge Services for the v3.0.0 Conductor on page 495.
- **If you are updating a virtual Conductor to v3.0.0 or v3.1.0** – You may need to expand the disk size for the virtual machine to 1GB. For instructions, see your virtual machine documentation, or the suggested VMware and Hyper-V instructions at Expand the Disk Size for a virtual Airwall Gateway on page 311.

Advisory Notices and Product Bulletins

Here are advisory notices and product bulletins since the last major update.

- Software end of life for Windows 7 and 32-bit Windows Airwall Agents on page 504
- T-Mobile – Required Cellular Firmware Update for 110g on page 498
- 3G Sunset – Required Cellular Firmware Update for 110g on page 499
- Auth0 Update does not affect OpenID Connect Integration on page 501
- AT&T 3G Sunset – Required Cellular Firmware Update for 110g on page 501

Update Considerations

You may want to update to this version to use the following features:

- Check connectivity with the Connectivity checker on page 486

- Do network discovery and security audits in Airshell (nmap) on page 377
- Set up Airwall Gateway High-availability Heartbeat options. For how to, see Configure High Availability Airwall Gateways (v2.2.8 and later) on page 399
- Run the Conductor as an Airwall Relay on page 354
- Customize People's Access to your Airwall secure network with People Groups on page 86
- Run Airshell remotely from the Conductor on page 374
- Use expressions to Search in the Conductor on page 44

Downloads

For firmware and software downloads for this version, see 3.1.0 firmware and software on page 520.

What's New in 3.1.0

This version of the Airwall Solution includes several usability and functionality improvements that can simplify and streamline the setup and diagnostics for an Airwall secure network.

Tutorial and Help Improvements

- **What's new Tutorial** – You can now see what’s new by running the **Dashboard** tutorial from the Conductor Dashboard.
- **Help links for a page** – In addition to tutorials, you can now access more specific Airwall help content for a page from the ? menu on most pages.
- **Video overviews and demos** – For video overviews and demos of the Airwall Solution, see Video Overview and Demos on page 6.

New tools to troubleshoot connectivity issues

The Conductor **Connectivity checker** does a full analysis of the connectivity between two devices in your Airwall secure network.

Learn more – Connectivity checker on page 486

Run Conductor as a Relay

For small- to moderate-sized Airwall secure networks, you can run your Conductor as a relay, rather than having a separate Airwall Relay. Since Airwall Edge Services must all be able to reach the Conductor, using it as an Airwall Relay simplifies your deployment. You must have both a Conductor and an Airwall Relay license to run your Conductor as a relay.

Learn more – Run the Conductor as an Airwall Relay on page 354

Control Access with People Groups

Using people groups, you can control what the people in the group can see and use on the Conductor, including cloud providers, Airwall Gateways, and Overlay networks and resources. You can also now see to which overlay networks the people group has permissions.

Learn more – Customize People's Access to your Airwall secure network with People Groups on page 86

Airwall Gateway High Availability (HA) Heartbeat options

You now have a choice on how the Airwall Gateway HA heartbeat functions. When setting up an Airwall Gateway HA pair, you can choose how to do the heartbeat between the two HA units. There are two options: LAN mode or routed mode.

Learn more – Configure High Availability Airwall Gateways (v2.2.8 and later) on page 399

Remote Airshell

For remote administration of Airwall Gateways, you can use Airshell to run diagnostic and configuration commands from the Conductor.

Learn more – Run Airshell remotely from the Conductor on page 374

Airshell Additions and Improvements

The following commands and functionality have been added to Airshell:

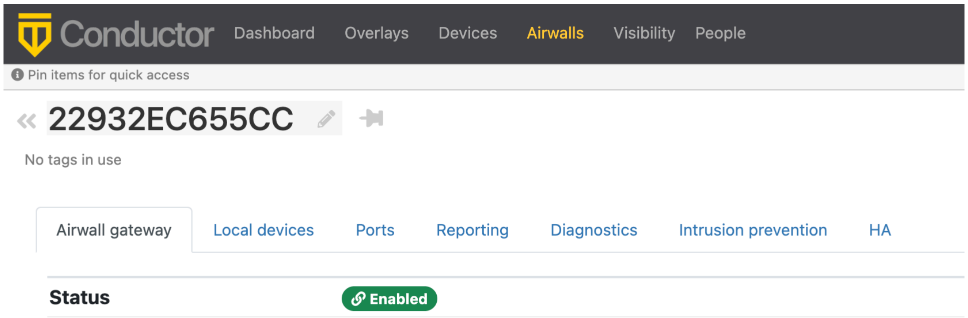
- `nmap` – (Network mapping support) Maps your network for discovery or security audits. **Learn more:** Do network discovery and security audits in Airshell (nmap) on page 377
- `table` – See the table command at Airshell (airsh) Command Reference on page 362.
- `conductor ping` – New `conductor ping` Airshell command for Airwall Gateways, Linux Airwall Servers, and macOS Airwall Agents checks name resolution and performs TLS connection attempt with every configured Conductor URI.
- `status dnscache` and `status dnscache flush` – For Airwall Gateways, dumps or flushes the DNS cache.
- `status threads` – Reports CPU and memory usage of threads of major services running on an Airwall secure network.
- `status` – Results now show information (revision hash and date) for the installed cellular firmware package.

Learn more – Airshell (airsh) Command Reference on page 362

Conductor and Airwall Edge Services Improvements

Navigation and Search

- **Back Navigation** – On most pages, you now have a link back to the original page. For example, from an Airwall Edge Service page, you can select the back icon « to get back to the list of Airwall Edge Services.



22932EC655CC

No tags in use

Status Enabled

- **Search by Expression** – The Conductor now supports an alternative to full text search, searching by expressions using the Conductor Query Language. Searching by expression is available in the search boxes on the **Overlays**, **Airwalls**, **Devices**, **People**, and **Dashboard** pages. **Learn more:** Search by Expression with the Conductor Query Language on page 45
- **Device quick filter** – The quick filter for devices is now also available on the **Dashboard Devices** list.

Overlay network graph

- **Multi-select** – Select more than one item on the network graph by holding down the meta key for your platform (`Ctrl` on Windows, or `cmd` on macOS) and clicking on multiple items. You can then use the context menu to create a device group or remove the items from the network.
- **Overlay Edit options** – The network graph also now has **Edit layout** and **Edit trust** options.
- **Create device group** – You can now create a device group by using multi-select to select devices, then right-click to create a device group.
- **Airwall model information** – When you hover over an Airwall Edge Service in the Airwall Edge Service network graph, the graph now shows the Airwall Edge Service model.

Learn more: Add and remove device trust on page 427

Set a preference for your overlay networks view

Go to **[your account]** > **Preferences** and scroll down to the bottom. Toggle the **Default overlay networks to advanced view** to show or hide the advanced view by default.

Learn more: Change My Conductor Preferences on page 30

Diagnostics and Monitoring Improvements

- **Email failure alerts** – When emails fail to send, the Conductor now shows alerts and records system events.
- **Summary for check secure tunnels** – There is now a summary for the **Check secure tunnels** Airwall Edge Service diagnostic tool indicating the number of remote Airwall Edge Services and the number of active tunnels.
- **Firmware Revision information** – In the Conductor, on an Airwall Edge Service page, revision information is shown on the main page below the Airwall Edge Service's firmware revision.
- **Ping peer Airwalls** – This diagnostic tool now indicates if traffic was conducted over a relay and which relay it used.
- **Airwall Relay diagnostics** – **Diagnostics** > **Airwall relay diagnostics** on an Airwall Relay now shows the IP addresses of the communicating Airwall Edge Services, as seen from the viewpoint of the relay.
- **HIP tunnel stats** – HIP tunnel stats now default to **On**, and are sent every 5 minutes for newly-connected Airwall Edge Services that support the feature. Go to **Airwall** > **Reporting** > **HIP tunnel stats** to see how much traffic you have over each tunnel.
- **HIP tunnel event monitors** – You can now configure a delay for actions on HIP tunnel event monitors, allowing you to reduce noise for transient events (for example, an Airwall Edge Service that goes offline briefly). There is also improved tracking and messaging around why a tunnel has closed. You can filter on the reasons a tunnel closed so that event actions are not performed for certain reasons. For example, you may not want to alert when a tunnel goes down due to an idle timeout (no traffic passed).
- **More fields for Templated values in Event monitor actions** - You can now use any data that is part of the monitored object by adding it as a templated value. For example, in the HTTP call action, you could use the Airwall Edge Service's name with "${monitored_object.name}", or get a device's overlay IP with "${monitored_object.overlay_device_ip}".
- **PCI user activities** – Now indicate if an action was performed via API.

Airwall Agents and Servers Improvements

- **Linux** – The Linux Airwall Server now supports traceroute from the Conductor diagnostic page when installed and available. Looks for the presence of traceroute or tracepath. It also now remembers its state when you update the firmware, and return to that state after the update (either active or inactive).
- **Android** – The Android Airwall Agent now restarts when you update the app, or if you restart the device while the app service is running. You can also now ping devices on the **Network** page.

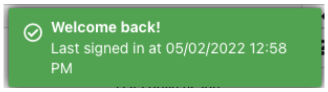
Deployment Improvements

- **Cloud accounts** – The Airwall Gateway detects the cloud `accountid` used during deployment and sends that provider-specific value to the Conductor.
- **Google Cloud** – There is now a standalone Airwall Gateway deployment for Google Cloud.
- **Device discovery** – The Conductor now shows the time a device was discovered.
- **Easier OpenID Connect integration troubleshooting** – It is now easier to troubleshoot integrating your Conductor with an OpenID Connect provider using Conductor Airshell and log following. **Learn more**: Integrate Third-party Authentication with OpenID Connect on page 247

Security and Privacy Updates

- **New overlay network role for Network Administrators** – The roles available for overlay permissions now are viewer, user, or manager. For more information, see Edit people who can access an overlay network on page 419.

- **New `conductor ping` airsh command** for Airwall Gateways, and macOS and Linux Airwall Agents and Servers – Checks name resolution and performs TLS connection attempt with every configured Conductor URI. **Learn more:** Diagnostic commands on page 366
- **Tag Ownership** – With v3.1.0, the tag ownership rules have changed to be more restrictive by default. If a system administrator creates a tag, by default, only system administrators can see or use them. If a network administrator creates a tag, ownership defaults to only them or their people group, and system administrators. This change allows you to have department or customer-specific tags that only members of specific people groups can see and use. **Learn more:** Manage Tag Ownership on page 104
- **Airwall Diagnostic permissions** – Diagnostics now require a network admin to have edit permissions on the Airwall Edge Service.
- **Lock Airwall Edge Services** – You can lock an Airwall Edge Service so only system administrators can edit it. **Learn more:** Lock an Airwall Edge Service on page 94
- **Login notifications** – The Conductor notifies admins the first time a user logs in, and the Conductor also shows a user's last log in when they log in, including through OpenID Connect Third-party integrations.



Welcome back!
Last signed in at 05/02/2022 12:58 PM

Onboarding Improvements

- **Delete Airwall Invitations** – You can now delete **Airwall Invitations**, both in the Conductor, and from the API.
- **Replace an Airwall Agent or Server** – You can now send an **Airwall Invitation** from a specific Airwall Agent or Server, and when the user activates the invitation, the Conductor automatically revokes and replaces the Airwall Agent or Server from which you sent the **Airwall Invitation**.
- **Device detection improvements** – The device detection workflow (and the related dialog) have been updated to streamline the onboarding process. The dialog now allows the user to detect devices and then, as they are detected, update their names and IP, apply an overlay IP NAT from a NAT pool and add them directly to an overlay.
- **Set an Airwall Gateway name using Airshell before provisioning** – You can now check the **Allow Airshell to set name** option when sending **Airwall Invitations**. When checked, you can use Airshell to set an Airwall Gateway's name before using the activation code to provision and manage it. If you use the invitation for other Airwall Edge Services, it is ignored.
- **New options for user onboarding** – When you onboard people using activation codes using either **Airwall Invitations** or People group user onboarding, you can now set up these new options:
  - User auth for remote sessions
  - Airwall Agent's or Server's overlay device IP netmask
  - Bypass Airwall Gateway

Logging Updates

- **Per-Airwall logging** – You can now configure remote syslog and overlay traffic logging per Airwall Edge Service. **Learn more:** Set overlay traffic logging for an Airwall Gateway on page 422.
- **Set global overlay traffic logging** – Tech Preview You can now set overlay traffic logging globally for your Airwall secure network on the page for an Airwall Gateway that supports it.
- **Log rate limiting** – The Conductor now rate limits log messages to 100 messages per second. You can examine rate limiting details using the Airshell command: `log status <hip|ebm2>`. **Learn more:** Status Commands on page 368.

Airwall Relay Updates

Message rate limiting – An Airwall Relay now rate-limits "Relay missing client address" messages to once every 15 minutes per client.

New and Improved Conductor Features

Learn more –

-
-

New and Updated Help

In addition to the content added for new features linked above, here's the new and updated content published since our last major release:

New –

- Move an Airwall Gateway to a Different Conductor on page 132
- Deploy a Conductor in Microsoft Hyper-V on page 231
- How to Update from Older Versions on page 515
- Airwall Agent or Server or Airwall Gateway using IPv6 has trouble connecting on page 489
- Event Monitors and Alerts Reference on page 120
- Auth0 Update does not affect OpenID Connect Integration on page 501
- U.S. Cellular Carrier Certifications on page 377
- 3G Sunset – Required Cellular Firmware Update for 110g on page 499
- Manage Airwall Edge Services from an Overlay on page 427
- Overlay Timelines on page 427
- Device page on page 417
- Set a Proxy Server on page 238
- Configure an authenticated Airwall Agent or Server session on page 384
- Knowledge Base (KB) Articles on page 778 - 90 KB articles are now available in Airwall Help

Updated –

- Step 1: Add Alibaba Cloud as a provider to your Conductor on page 315
- Microsoft Azure – Set up an Airwall Gateway on page 324 – Create Application
- Airshell (airsh) Command Reference on page 362
- Install a Custom CA Certificate Chain on page 239
- Put an Airwall Gateway into diagnostic mode on page 478
- Put the Conductor into diagnostic mode on page 477
- Backhaul Bypass on page 395
- Search in the Conductor on page 44
- Edit people who can access an overlay network on page 419
- See Airwall Edge Service Information and Status on page 95
- Security Notices on page 498

Fixes

ID	Applies to	Description
DEV-18102	Airwall Gateways	Fixed an issue that caused the IDS not to start or reboot in certain configurations.
DEV-18001	Airwall Gateways	Fixed an issue where HA secondary Airwall Gateways didn't share the bypass gateway settings of the HA primary Airwall Gateway.
DEV-17973	Airwall Gateways	When a lock is contended, bypass now retries applying underlay/bypass firewall rules.
DEV-17905	Linux Airwall Servers	Fixed an instability in the Linux Airwall Server running on Fedora.

ID	Applies to	Description
DEV-17881	OpenHIP	Fixed a crash handling JsonRPC requests.
DEV-17878	Conductor	Fixed an issue where bypass gateway settings could be misleading when an Airwall Edge Service was set up to use local bypass.
DEV-17847	Airshell	Improved usability of Airshell results: Now show "Provisioned: yes/no" and "Device key: (keystore type)(file present/missing if file keystore type)"
DEV-17839	Airwall Gateways	Fixed an issue where health data "Relay sessions" (sadb_relay) were not shown in the UI. Fixed an additional issue where the value reported by the Airwall Gateway was doubled (one for each side of a relay session).
DEV-17818	Airwall Gateways	Fixed an issue where port group ID was conflated with index. Now "PGID" in "airsh policy" shows the actual port group ID. Also added "pg_id" to the io_channel tmstat table.
DEV-17784	Conductor	An unmanaged or revoked Airwall page now hides information that is not relevant.
DEV-17761	macOS Airwall Agents	Fixed two minor issues with new Path MTU TLV.
DEV-17750	Conductor	Fixed an issue where users would sometimes not receive an email after receiving an activation code from a people group.
DEV-17716	Conductor	Fixed an issue where the Airwall Gateway page showed an erroneous bypass IP conflict.
DEV-17637	Conductor	Fixed an issue where the incomplete edge would disappear if the network received an update during new edge dragging in policy edit mode for the network graph.
DEV-17605	Conductor	Fixed an issue where adding a device to a device group as a result of using an activation code would not trigger recalculation of any smart device groups that rely on that device group.
DEV-17593	Linux Airwall Servers	Fixed an issue where the Linux Airwall Servers had an "Operation unsupported" error during interface discovery.
DEV-17580	AWS, Conductor	Fixed an issue with Conductor formatting the nvme drive on Amazon Web Services.
DEV-17562	Conductor	Fixed a formatting issue where remote device overlays would be on multiple lines causing them to be misaligned with the devices they refer to.
DEV-17549	Airwall Gateways	Improved local device (and remote device for backhaul bypass egress gateways) scalability.
DEV-17498	Conductor	The network graph has been updated to be more efficient with very large node counts.
DEV-17439	Conductor	Fixed overflow issues with ipv6 addresses in dialogs.
DEV-17434	Conductor	Fixed terminology around Airwall Gateway High-Availability (HA).

ID	Applies to	Description
DEV-17427	Common	Route summarization improved to process large routing tables faster.
DEV-17405	Conductor	Fixed an issue where bypass gateways with local devices may not be configured properly in overlay networks that have bypass devices.
DEV-17370		Fixed an issue that could cause a crash of the metadata service on the Conductor.
DEV-17323	OpenHIP	Added improved logging for an unlikely case when attempting to establish a tunnel to a peer Airwall Gateway that has "publish IP address to Conductor" disabled on all underlays and doesn't have relay. In this configuration, initiating a tunnel to that peer is not possible.
DEV-17319	Airwall Gateways	Fixed an issue that could prevent bypass traffic from Airwall Agents and Servers if the bypass gateway is HA configured.
DEV-17317	Airwall Agents and Servers	Fixed an issue that caused Airwall Agents and Servers to allow traffic to blocked bypass destinations when those could be reached directly on the underlay network.
DEV-17311	macOS Airwall Agents	Fixed an issue that could cause Airwall Agents and Servers tunnel traffic problems under rare circumstances.
DEV-17300	Conductor	Fixed an issue where Airwall Edge Services using the default bypass gateway may have not been given the correct configuration to fully access it.
DEV-17270	Airwall Gateways	Airshell policy output is now aligned in columns
DEV-17264	Airwall Gateways	Fixed an issue with overlay route summarization when local device doesn't match any connected or overlay routes and has port affinity or there is only a single overlay port group and no bypass.
DEV-17238	DataPlane	Fixed excessive packet buffer allocations and encrypt_engine rx_pkts counter.
DEV-17231	tnw-basic	Fixed a crash on service shutdown.
DEV-17207	Conductor	Fixed an issue that was breaking the OUI list.
DEV-17175	Conductor	System admins can now use all tags.
DEV-17171	Conductor	Fixed an issue causing all new devices added to a network to be placed in the same spot on the network graph.
DEV-17140	Conductor	Fixed issue where Airwall Agents would not display as disabled in the network graph
DEV-17135	OpenHIP	Fixed an issue with tunnel keepalives that results in an OpenHIP error message (openhip: [WARNING] encrypt_engine_rx_pkts: received packet without HIT: ...) and Airwall Edge Services fall back to HIP UPDATE keepalives.
DEV-17129	Conductor	Fixed an issue where changes to password requirements would sometimes not take effect until the Conductor was rebooted.

ID	Applies to	Description
DEV-17123	Conductor	Fixed an issue where generated passwords would always be 10 characters long rather than honoring the minimum password length set by the user.
DEV-17122	Airwall Gateways	Fixed a service hang when reconfiguring overlay port groups.
DEV-17115	Conductor	Fixed an issue where network admins might not be able to view the relays in an overlay managed relay rule.
DEV-17048	Common	Fixed tmstat: BUG: tmsegment_free invoked on a handle with rows outstanding
DEV-17008	Conductor	Fixed a usability issue where device match rules could use system managed Airwall groups.
DEV-16994	Conductor	Fixed an issue where it is unclear as to why the relay probes diagnostic shows "Unknown" for relays that a network admin does not have permissions to view.
DEV-16986	Azure Cloud Airwall Gateways	Fixed an issue where some cloud attributes were not retained during firmware upgrades and, in some cases, after a reboot.
DEV-16983	Conductor	Truncated names now have their full name displayed as hover text.
DEV-16924	Conductor	Network admins now only see events that pertain to them and their permissions.
DEV-16913	Conductor	Fixed an issue where some overlays might not be found when using filtering via the API index endpoint
DEV-16907	Conductor	Fixed an issue where cellular Airwall Gateways on versions prior to 3.1.0 would have a /0 prefix erroneously report 'invalid' for the gateway.
DEV-16874	Common	Fixed a duplicate timestamp in Airwall Gateway and Conductor logs.
DEV-16868	Conductor	Fixed an issue where the result for ping device was misaligned
DEV-16814	Conductor	Network admins that only have access to the simplified UI will now have the ability to create device groups from the dashboard tab.
DEV-16746	Conductor	The Conductor now validates that overlay and underlay addresses on Airwall Gateways are not unspecified, loopback, or multicast addresses.
DEV-16713	Linux Airwall Servers	Fixed an issue where firmware installation times were incorrect, and now sort times by the most recent to the oldest.
DEV-16692	Airwall Agents and Servers	Fixed an issue where no Health Data was reported while an Airwall Edge Service was in Disconnected Mode.
DEV-16646	Linux Airwall Servers	Fixed an issue that prevented Linux Airwall Servers from generating cloud attributes when deployed to a cloud provider.
DEV-16644	Linux Airwall Servers	Fixed an issue where the Linux Airwall Server ping single IP from the overlay wasn't working.
DEV-16533	Conductor	Fixed an issue where name and description lengths were not validated when importing people.

ID	Applies to	Description
DEV-16532	Conductor	Improved layout in the Person import dialog.
DEV-16530	Conductor	Fixed a dark mode styling issue with the errors table when importing people.
DEV-16527	Conductor	Fixed a redirect loop that occurred when a logged in user is set to inactive. The user should now be returned to the login screen
DEV-16525	Cloud Airwall Gateways, Conductor	Fixed an issue where, with individual route injection for cloud Airwall Gateways enabled, devices added to groups that already have policy with a cloud Airwall Gateway did not correctly update the cloud provider's routing tables.
DEV-16497	OpenHIP	Fixed an issue that caused a brief packet drop and/or forgetting tunnel MTU with an SA rekey.
DEV-16496	Airwall Gateways	Updating the Overlay MTU in the Conductor now updates existing tunnels using a larger tunnel MTU. Existing tunnels using a smaller MTU will continue to use the smaller MTU until the tunnel is rebuilt.
DEV-16483	OpenHIP	Updating Airwall tunnel stats reporting interval no longer requires restarting the dataplane, but disabling or enabling this feature still requires a restart impacting traffic flowing through the Airwall. Fixed benign error message: "Invalid sa_stats window".
DEV-16425	Conductor	When setting trust on an overlay network graph, you can now select something from the context menu by clicking anywhere in row rather than just on the text.
DEV-16412	Airwall Gateways	You can no longer add duplicate VLAN tags to a single port.
DEV-16407	Diagnostic mode	Improved the reliability of **Check Conductor URL** in Airwall Gateway Diag mode.
DEV-16382	Conductor	Network admins who do not have the "Can view full user interface" permission but do have permission for Airwall groups and relay rules can now create both from the dashboard.
DEV-16313	Conductor	Customization settings for email colors are now hidden until email settings are configured.
DEV-16220	Android and macOS Airwall Agents	Fixed an issue where Airwall Agents could connect sooner than configured in Disconnected Mode.
DEV-16116	Conductor	Fixed some irregularities with the user experience of reports for non-system administrators.
DEV-15976	Conductor	Fixed an issue where certificate expiration notifications were showing the **View** button for its HA partner.
DEV-15338	Linux Airwall Agents	Linux Airwall Servers now use a predictable MAC address (derived from identity and platform configuration) so systemd-network shouldn't attempt to change it.
DEV-14739	Airwall Gateways	Fixed configuring Airwall Gateway underlay with DHCP for both IPv4 and IPv6.

ID	Applies to	Description
DEV-14211	Airwall Gateways	Added support for configuring automatic IPv6 addresses using DHCPv6 stateless.
DEV-13591	Conductor	Fixed an issue with long words in invitation email "Note from the administrator" causing the email to display incorrectly.

Known Issues

ID	Applies to	Description
DEV-17887	Cloud, Conductor	If you use unrecognized credentials when calling jobs on a cloud Airwall Gateway, the Conductor sends multiple error messages when it tries to call route injection and validate cloud attributes. **Workaround** -- Make sure your cloud credentials are correct on the **Cloud Providers** page under Conductor Settings..
DEV-17648	Linux Airwall Servers	Many Airshell functions (including changing log level) are non-functional until you have configured and licensed your Conductor.
DEV-17263	Conductor	If you fix a conflict in a smart device group by changing the IP of one of the conflicted devices, sometimes the change in IP does not result in the device being removed from the group and the change is not propagated to the Airwall Gateway. **Workaround** – Fully remove the device from the smart device group and then add it back again.
DEV-16999	150 Airwall Gateways	On some 150 Airwall Gateways, the port 5 SFP LEDs may not light up when the port is actually linked and active.
DEV-16503	macOS Airwall Agents	Deleting a profile does not immediately delete the associated private key. **Workaround** – Switch to a different profile before creating a profile after deleting one.
DEV-16431	Conductor	When you specify a port mirror destination IP address for an Airwall Gateway, make sure it doesn't conflict with any of the local device IPs on that Airwall Gateway.
DEV-16397	Conductor	If you change the LSI prefix and have port mirroring configured, you need to either reboot the Conductor, or go to **Settings** > **Diagnostics** and select **Restart metadata cache** to update the LSI prefix.
DEV-16068	Amazon Web Services Conductor	To enable enhanced networking for a cloud Amazon Web Services Airwall Gateway or Conductor, use the custom images instead of the marketplace image.
DEV-16067	Cloud, Conductor, Airwall Gateways	If you are adding a new interface to an existing cloud Airwall Gateway, you must set the source and destination check to false (see your cloud provider for the terminology they use for source and destination checks).

ID	Applies to	Description
DEV-16059	Airwall Gateways	When HA-pairing two Airwall Gateways that do not have the HA link plugged in correctly, the Conductor displays no actionable error message and the HA setup never completes.
DEV-15982	Conductor	Traffic stats reporting graphs generally show a smooth curve between data points. However, over time the graph can show up with sharper angles. The data is still correct, but this is a known issue with the graphing library used by the Conductor.
DEV-15945	Airwall Gateways	If you configure port mirroring using a remote destination local device, GRE/ERSPAN traffic from remote Airwalls will arrive with a source IP in the LSI prefix (defaults to 1.0.0.0/8).
DEV-15923	Airwall Gateways	When you run **Check secure tunnels** on a v3.0 Airwall Gateway, the check falsely reports a bad tunnel status for any peer Airwall Gateway running a firmware version that is v2.2.8 or earlier.
DEV-15887	Airwall Gateways	You cannot currently add VLAN interfaces to the Ruggedcom platform.
DEV-15808	Google Cloud Airwall Gateways	Google Cloud Airwall Gateways with the same VM name have the same device serial number, which can result in a failure when you make a license request in the Conductor. **Workaround** – In Google Cloud, use unique deployment names (VM names) for Airwall Gateways.
DEV-15791	Airwall Gateways	On the Airwall Gateway 100, Port 2 might be inactive after a factory-reset. **Workaround** – After a factory reset, manually reboot the Airwall Gateway 100.
DEV-15705	macOS Airwall Agents	Establishing a tunnel TO a mobile Airwall Agent (iOS or Android) fails when there is no Airwall Relay involved. **Workaround** – Establish the tunnel FROM the mobile Airwall Agent.
DEV-15572	Airwall Gateways	If you do not specify a gateway in the DHCP server configuration, the DHCP client cannot configure a default gateway. **Workaround** – Unless you want to configure a single isolated subnet, always specify a gateway. For example, a subnet for networked PDUs that should not have any outside connectivity aside from remote access through an Airwall Gateway, and used in conjunction with SNAT over the overlay port group. See https://tempered.force.com/TemperedSupportCenter/s/article/DHCP-server-isn-t-serving-as-a-gateway.

ID	Applies to	Description
DEV-15357	macOS Airwall Agents	If you update the macOS Airwall Agent to a release later than v2.2.11 on macOS Mojave using a Conductor-based update package, it may not report the updated version to the Conductor. **Workaround** – Restart the Airwall Agent or reapply the update.
DEV-15302	macOS Airwall Agents	The profile for a macOS Airwall Agent does not work correctly when restored to a new computer using Time Machine. **Workaround** – Create a new profile on the Airwall Agent, and then on the Conductor, replace the old profile with the new one.
DEV-15219	Cellular 110g Airwall Gateways	The Airwall Gateway 110g does not on the Bell Mobility (Canada) cellular provider because they require the use of a http/https proxy.
DEV-15031	Airwall Gateways	Remote syslog over TLS doesn't work when using keys stored in TPM.
DEV-14860	Conductor	Airwall Gateways on older firmware (pre v2.2.0) may send passively-discovered device events to the Conductor even when the feature is off.
DEV-14835	Conductor	Airwall Gateway 150 serial numbers look like exponentiated numbers to Windows Excel, so the column displaying the Serial number shows xxxEyyy instead of the full serial number.
DEV-14736	Cellular Airwall Gateways	Cellular details may display as "unavailable" on the first boot after you update an Airwall Gateway. The cellular connections are not affected. **Workaround** – Reboot the Airwall Gateway again to correctly display the cellular details.
DEV-14726	Conductor	If you're viewing an Android Airwall Agent **Ports** tab and the Airwall Agent changes how it is connected to the Conductor (for example, from WiFi to cellular), the display does not update correctly. **Workaround** – Refresh the page.
DEV-14715	macOS Airwall Agents	Big Sur ARM64 Macs are not supported in this release
DEV-14610	Conductor	After changing the Reporting traffic stats reporting time, the CPU graph does not display. **Workaround** – Refresh your browser page.
DEV-14584	Cellular Airwall Gateways	Hot swapping the SIM on an Airwall Gateway 110 with firmware version v2.2.11 may not work. **Workaround** – Reboot the Airwall Gateway after installing a new SIM card.

ID	Applies to	Description
DEV-14551	Conductor	The Android Airwall Agent lets you press the **Edit Settings** button on the **Ports** page; however, submitting any changes to the page results in an error message.
DEV-14426	Conductor, Airwall Gateways	Bypass destinations with a hostname do not show device activity in the Conductor.
DEV-14308	OpenHIP	Initial packets are dropped while building a new tunnel to a new peer Airwall Gateway.
DEV-14223	Google Cloud	To talk to a device behind a 300v Airwall Gateway running on Google cloud, add an overlay IP to an Airwall Agent or Server.
DEV-14218	Airwall Gateways	NAT broadcast applied to traffic between ports within a single port group. Use an external switch if you need to connect multiple devices to a single port group and use the NAT broadcast feature and require IP broadcast un-NATed between those local devices.
DEV-14015	OpenHIP	If an Airwall Relay is also used as a bypass gateway, Airwall Edge Services behind the relay are not able to use that relay. **Workaround** – Deploy multiple relays so at least one relay is usable by each pair of Airwall Edge Services that need to communicate.
DEV-13775	Azure Cloud Airwall Gateways	The Conductor might rarely give a "Net::ReadTimeout" error when you try to deploy an Azure Airwall Gateway 300v or server. This error doesn't indicate that the deployment has failed. If you get this error message, go to Azure portal and check the actual deployment result.
DEV-13650	Conductor	SoIP device activity is not being reported on an Airwall Gateway **Local Devices** tab.
DEV-13640	Conductor	Airwall Relay diagnostics do not work on a Standby Conductor.
DEV-13633	Conductor	A standby Conductor shows available firmware downloads, but they cannot be downloaded. **Workaround** – Download firmware from the active Conductor.
DEV-13620	Conductor	In **Airwall** > **Ports** > **Failover settings**, the failover ping occurs only every "ping rate" + "ping timeout" seconds, somewhat unexpectedly.
DEV-13607	Conductor, Airwall Gateways	Creating a link failover group (**Airwall** > **Ports** > **Failover settings**) does not apply the settings to any port groups. You must also assign the failover group to port groups on the **Ports** page.
DEV-13588	Conductor	Opening the Conductor on Internet Explorer 11 can be very slow for medium to large deployments. **Workaround** – Use the latest version of Chrome, Firefox, or Edge instead.

ID	Applies to	Description
DEV-13531	Cloud Conductor	Automatically creating Cloud HA Conductors only works if you use the same cloud provider for both active and standby Conductors. For example, AWS HA Active and AWS HA Standby. **Workaround** – You can manually set up different cloud providers as HA pair Conductors.
DEV-13474	Airwall Gateways	If you configure multiple overlay port groups with the same overlay IP subnet (same or different IP addresses) and then create a local device equal to the entire subnet with port affinity set, it may not lead to the expected result.
DEV-13331	Alibaba Cloud Airwall Gateways	The Alibaba Cloud Conductor system time is incorrect. **Workaround** – Change the Conductor system time to browser time: In Conductor **Settings**, under **System time**, select **Edit Settings**, select **Set browser time**, and then select **Update Settings**.
DEV-13195	Conductor, Airwall Gateways	When you upgrade a Cellular Airwall Gateway-150 from 2.2.3 to 2.2.5, the cellular details all become "Unavailable." **Workaround** – Reboot and the details return.
DEV-13194	Conductor	**Check Connectivity** > **Ping Local Devices** for an Airwall Gateway fails in Internet Explorer 11 if one of the devices is defined as a CIDR. **Workaround** – Use one of the latest versions of Chrome, Firefox, Safari or Edge.
DEV-10590	Cloud Airwall Gateways	The Conductor does not display an error when adding a route that would exceed the maximum number of allowed routes in the cloud provider.
DEV-10039	Airwall Gateways	An Airwall Gateway-150 can show "could not detect attached switch" intermittently.
DEV-9546	Airwall Gateways, Airwall Gateways 150	The Airwall Gateway-150 serial connection has an intermittent issue when large amounts of data are sent over the console.

Release Notes v3.0.3

Release Date: May 10, 2022

Update Considerations

❗ **Important: Update downtime** – When you update a Conductor or Airwall Edge Services, there may be database and configuration changes related to the new release that require Airwall Edge Services to update their configuration data, resulting in downtime while secure tunnels are re-established. Downtime is typically up to, and in most cases is much less than, two minutes.

This update addresses the following issues:

- Relay performance
- DNS bypass fixes and optimizations

Downloads

For firmware and software downloads for this version, see 3.0.3 firmware and software on page 522.

Fixes

ID	Applies to	Description
DEV-17529	Airwall Gateways	Fixed an issue with DNS bypass where subsequent DNS queries for a DNS bypass destination triggered updating policy causing high CPU usage.
DEV-17521	Airwall Relays	Fixed an issue that caused failures that limited tunnel or relayed tunnel scalability.
DEV-17519	Conductor	Fixed an issue where updating and then demoting a standby HA Conductor could result in 500 errors being returned.
DEV-17505	Conductor	Fixed an issue where updating the name of an overlay network would clear Airwall Relays from the managed relay settings.

Known Issues

ID	Applies to	Description
DEV-17178	Cellular Airwall Gateways	Cellular details show "unavailable" on the Conductor **Ports** tab after you update the Airwall Gateway to v3.0.1. **Workaround** -- Reboot the Airwall Gateway.
DEV-16999	Airwall Gateways	AW-150 port 5 SFP LEDs are non-functional when the port may be actually linked and active.
DEV-16503	macOS Airwall Agents	Deleting a profile does not immediately delete the associated private key. **Workaround** – Switch to a different profile before creating a profile after deleting one.
DEV-16431	Conductor	When specifying a port mirror destination IP address, ensure that it doesn't conflict with any of the Airwall Gateway's local device IPs
DEV-16397	Conductor	If you change the LSI prefix and have port mirroring configured, you need to either reboot the Conductor, or go to **Settings** > **Diagnostics** and select **Restart metadata cache** to update the LSI prefix.
DEV-16068	Amazon Web Services Conductor	To enable enhanced networking for a cloud Amazon Web Services Airwall Gateway or Conductor, use the custom images instead of the marketplace image.
DEV-16067	Cloud, Conductor, Airwall Gateways	If you are adding a new interface to an existing cloud Airwall Gateway, you must set the source and destination check to false (see your cloud provider for the terminology they use for source and destination checks).
DEV-16059	Airwall Gateways	When HA-pairing two Airwall Gateways that do not have the HA link plugged in correctly, the Conductor displays no actionable error message and the HA setup never completes.

ID	Applies to	Description
DEV-15982	Conductor	Traffic stats reporting graphs generally show a smooth curve between data points. However, over time the graph can show up with sharper angles. The data is still correct, but this is a known issue with the graphing library used by the Conductor.
DEV-15945	Airwall Gateways	If you configure port mirroring using a remote destination local device, GRE/ERSPAN traffic from remote Airwall Gateways will arrive with a source IP in the LSI prefix (defaults to 1.0.0.0/8).
DEV-15923	Airwall Gateways	When you run **Check secure tunnels** on a v3.0 Airwall Gateway, the check falsely reports a bad tunnel status for any peer airwall running a firmware version that is v2.2.8 or lower.
DEV-15887	Airwall Gateways	You cannot currently add VLAN interfaces to the Ruggedcom platform.
DEV-15808	Google Cloud Airwall Gateways	Google Cloud Airwall Gateways with the same VM name have the same device serial number, which can result in a failure when you make a license request in the Conductor. **Workaround** – In Google Cloud, use unique deployment names (VM names) for Airwall Gateways.
DEV-15791	Airwall Gateways	On the Airwall Gateway 100, Port 2 might be inactive after a factory-reset. **Workaround** – After a factory reset, manually reboot the Airwall Gateway 100.
DEV-15787	macOS Airwall Agents	If a person who already has a profile makes a Request to Connect from the Remote Access User portal on the same Conductor, no profile is created. **Workaround** – If the user wants a second profile, they can use an invite code or enter the Conductor information manually.
DEV-15705	macOS Airwall Agents	Establishing a tunnel TO a mobile Airwall Agent (iOS or Android) fails when there is no Airwall Relay involved. **Workaround** – Establish the tunnel FROM the mobile Airwall Agent.
DEV-15572	Airwall Gateways	If you do not specify a gateway in the DHCP server configuration, the DHCP client cannot configure a default gateway. **Workaround** – Unless you want to configure a single isolated subnet, always specify a gateway. For example, a subnet for networked PDUs that should not have any outside connectivity aside from remote access through an Airwall Gateway, and used in conjunction with SNAT over the overlay port group. See https://tempered.force.com/TemperedSupportCenter/s/article/DHCP-server-isn-t-serving-as-a-gateway.

ID	Applies to	Description
DEV-15489	Windows Airwall Agents and Servers	Windows 7 sends an extra Windows system popup when the Windows Airwall Agent UserAuth prompt appears. You can safely ignore this popup, or can disable the Windows 7 service as described in this article from Broadcom: https://knowledge.broadcom.com/external/article/153693/interactive-services-detection-a-progra.html
DEV-15357	macOS Airwall Agents	If you update the macOS Airwall Agent to a release later than v2.2.11 on macOS Mojave using a Conductor-based update package, it may not report the updated version to the Conductor. **Workaround** – Restart the Airwall Agent or reapply the update.
DEV-15338	Linux Airwall Servers	If using a recent systemd-based Linux distribution including Fedora 33 and Debian 11, disable systemd-networkd MAC address randomization of the hip1 interface.
DEV-15302	macOS Airwall Agents	The profile for a macOS Airwall Agent does not work correctly when restored to a new computer using Time Machine. **Workaround** – Create a new profile on the Airwall Agent, and then on the Conductor, replace the old profile with the new one.
DEV-15219	Cellular 110g Airwall Gateways	The Airwall Gateway 110g does not on the Bell Mobility (Canada) cellular provider because they require the use of a http/https proxy.
DEV-15031	Airwall Gateways	Remote syslog over TLS doesn't work when using keys stored in TPM.
DEV-14860	Conductor	Airwall Gateways on older firmware (pre v2.2.0) may send passively-discovered device events to the Conductor even when the feature is off.
DEV-14835	Conductor	Airwall Gateway 150 serial numbers look like exponentiated numbers to Windows Excel, so the column displaying the Serial number shows xxxEyyy instead of the full serial number.
DEV-14739	Airwall Gateways	If you set IPv4 to DHCPv4 and set a static IP address for IPv6, the setting that you set second doesn't get saved. **Workaround** – If you need both IPv4 and IPv6, set static IP addresses for both.
DEV-14736	Cellular Airwall Gateways	Cellular details may display as "unavailable" on the first boot after you update anAirwall Gateway. The cellular connections are not affected. **Workaround** – Reboot the Airwall Gateway again to correctly display the cellular details.

ID	Applies to	Description
DEV-14726	Conductor	If you are viewing an Android Airwall Agent **Ports** tab and the Airwall Agent changes how it is connected to the Conductor (for example, from WiFi to cellular), the display does not update correctly. **Workaround** – Refresh the page.
DEV-14715	macOS Airwall Agents	Big Sur ARM64 Macs are not supported in this release
DEV-14610	Conductor	After changing the Reporting traffic stats reporting time, the CPU graph does not display. **Workaround** – Refresh your browser page.
DEV-14584	Cellular Airwall Gateways	Hot-swapping the SIM on an Airwall Gateway 110 with firmware version v2.2.11 may not work. **Workaround** – Reboot the Airwall Gateway after installing a new SIM card.
DEV-14551	Conductor	The Android Airwall Agent lets you press the **Edit Settings** button on the **Ports** page; however, submitting any changes to the page results in an error message.
DEV-14426	Conductor, Airwall Gateways	Bypass destinations with a hostname do not show device activity in the Conductor.
DEV-14308	OpenHIP	Initial packets are dropped while building a new tunnel to a new peer Airwall Gateway.
DEV-14249	iOS Airwall Agents	**Check Secure TunnelsTunnel Status** may show as unavailable on iOS. **Workaround** – You can determine tunnel status by checking packets sent or received.
DEV-14223	Google Cloud	Add an overlay IP to agent in order to talk to device behind Google 300v.
DEV-14218	Airwall Gateways	NAT broadcast applied to traffic between ports within a single port group. Use an external switch if you need to connect multiple devices to a single port group and use the NAT broadcast feature and require IP broadcast un-NATed between those local devices.
DEV-14045	Android and iOS Airwall Agents	iOS does not currently support overlay ping.
DEV-14015	OpenHIP	If an Airwall Relay is also used as a bypass gateway, Airwall Edge Services behind the relay are not able to use that relay. **Workaround** – Deploy multiple relays so at least one relay is usable by each pair of Airwall Edge Services that need to communicate.
DEV-13775	Azure Cloud Airwall Gateways	The Conductor might rarely give a "Net::ReadTimeout" error when you try to deploy an Azure Airwall Gateway 300v or server. This error doesn't indicate that the deployment has failed. If you get this error message, go to Azure portal and check the actual deployment result.

ID	Applies to	Description
DEV-13699	Windows Airwall Agents and Servers	The initial ping from the Windows Airwall Agent can be misleading since it currently includes the time to initially set up the connection. **Workaround** – Ping a second time to see actual ping time.
DEV-13650	Conductor	SoIP device activity is not being reported on an Airwall Gateway **Local Devices** tab.
DEV-13640	Conductor	Airwall Relay diagnostics do not work on a Standby Conductor.
DEV-13633	Conductor	A standby Conductor shows available firmware downloads, but they cannot be downloaded. **Workaround** – Download firmware from the active Conductor.
DEV-13620	Conductor	In **Airwall** > **Ports** > **Failover settings**, the failover ping occurs only every "ping rate" + "ping timeout" seconds, somewhat unexpectedly.
DEV-13607	Conductor, Airwall Gateways	Creating a link failover group (**Airwall** > **Ports** > **Failover settings**) does not apply the settings to any port groups. You must also assign the failover group to port groups on the **Ports** page.
DEV-13588	Conductor	Opening the Conductor on Internet Explorer 11 can be very slow for medium to large deployments. **Workaround** – Use the latest version of Chrome, Firefox, or Edge instead.
DEV-13536	Windows Airwall Agents and Servers	When you uninstall the Windows Airwall Agent, it does not remove the tun-tap driver. **Workaround** – Delete the driver from C:\Windows \System32\drivers\tnw-tap.sys.
DEV-13531	Cloud Conductor	Automatically creating Cloud HA Conductors only works if you use the same cloud provider for both active and standby Conductors. For example, AWS HA Active and AWS HA Standby. **Workaround** – You can manually set up different cloud providers as HA pair Conductors.
DEV-13474	Airwall Gateways	If you configure multiple overlay port groups with the same overlay IP subnet (same or different IP addresses) and then create a local device equal to the entire subnet with port affinity set, it may not lead to the expected result.
DEV-13331	Alibaba Cloud Airwall Gateways	The Alibaba Cloud Conductor system time is incorrect. **Workaround** – Change the Conductor system time to browser time: In Conductor **Settings**, under **System time**, select **Edit Settings**, select **Set browser time**, and then select **Update Settings**.

ID	Applies to	Description
DEV-13195	Conductor, Airwall Gateways	When you upgrade a Cellular Airwall Gateway-150 from 2.2.3 to 2.2.5, the cellular details all become "Unavailable." **Workaround** – Reboot and the details return.
DEV-13194	Conductor	**Check Connectivity** > **Ping Local Devices** for an Airwall Gateway fails in Internet Explorer 11 if one of the devices is defined as a CIDR. **Workaround** – Use one of the latest versions of Chrome, Firefox, Safari or Edge.
DEV-12852	Windows Airwall Agents	Windows by default doesn't allow multiple 'active' interfaces. It prefers ethernet over cellular whenever possible. **Workaround** – Set Windows to keep multiple interfaces open by editing the fMinimizeConnections registry value: **1.** Hold the Windows Key and press `R`. **2.** On the **Run** page, type `regedit` and click **OK**. **3.** Navigate to the following path in Registry Editor: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WcmSvc\` **4.** See if the `GroupPolicy` subkey exists. If not, right-click on `WcmSvc` and select **New** > **Key** and name it `GroupPolicy`. **5.** Right-click `GroupPolicy` and choose **New** > **DWORD (32-bit)** > **Create value**. **6.** Name the value `fMinimizeConnections` and select **OK**. (The value should be 0, or false). **7.** Reboot and test.
DEV-11710	macOS Airwall Agents	If you change the LSI prefix on the Conductor, the macOS Airwall Agent doesn't update the routes correctly. **Workaround** – Close and reopen the macOS Airwall Agent.
DEV-10590	Cloud Airwall Gateways	The Conductor does not display an error when adding a route that would exceed the maximum number of allowed routes in the cloud provider.
DEV-10039	Airwall Gateways	An Airwall Gateway-150 can show "could not detect attached switch" intermittently.
DEV-9546	Airwall Gateways, Airwall Gateways 150	The Airwall Gateway-150 serial connection has an intermittent issue when large amounts of data are sent over the console.
DEV-9429	Windows Airwall Agents	When you update the Overlay Device IP address for a Windows Airwall Server in the Conductor, it doesn't always update the first time. Workaround -- Open and update the address a second time.

Release Notes v3.0.2

Release Date: Apr 8, 2022

Update Considerations

This update addresses the following issues:

- Service restarts on Conductor
- Service restarts on Airwall Gateway
- Cloud Airwall Gateway auto-config overriding custom settings
- Security update for an OpenSSL vulnerability (CVE-2022-0778) - OpenSSL version has been updated.

Downloads

For firmware and software downloads for this version, see 3.0.2 firmware and software on page 524.

Fixes

ID	Applies to	Description
DEV-17432	Conductors	Fixed an issue where bypass Airwall Gateways with local devices may not be configured properly in overlay networks that have bypass devices.
DEV-17398	Airwall Gateways	Fixed get_iface_mtu_by_name ioctl SIOCGIFMTU: No such device warning on Airwall relay.
DEV-17388	Cloud Airwall Gateways	Fixed an issue where the Conductor failed to properly provision older Airwall Gateways.
DEV-17376	Conductors	Fixed an issue that could crash the metadata service on the Conductor.
DEV-17375	Conductors	Fixed a race condition that could cause a crash of the Airwall control plane daemon.
DEV-17334	Airwall Gateways	Fixed a backhaul bypass warning: "PortGroupImpl::syncInterfaceRoutes unable to add route on backhaul bypass gateway and Agents without an overlay IP have bypass policy."
DEV-17327	Airwall Gateways	Fixed an issue that could cause Airwall Agents configured with a NAT IP to become unreachable on 3.0.0 and 3.0.1 Conductors.
DEV-17315	Conductors	Fixed an issue where Airwall Edge Services using the default bypass gateway may have not been given the correct configuration to fully access it.
DEV-17296	Airwall Gateways	Fixed an issue that could cause a service crash on the Conductor immediately after reboot.
DEV-17269	Airwall Gateways	Fixed an issue that could cause service interruption when executing several long-lasting diagnostic or device discovery requests.
DEV-17267	Airwall Gateways	Fixed an issue that could deadlock the Airwall control daemon causing service restarts and Conductor reconnects.
DEV-17255	Airwall Gateways	Fixed an issue that could cause control plane service restarts because of heartbeat starvation during the overlay route summation.
DEV-17082	OpenHIP	Fixed a bug where HIP continually exchanges UPDATE packets with a peer.

ID	Applies to	Description
DEV-17016	Cellular Airwall Gateways	Fixed an issue that may affect certain SIM swaps on cellular Airwall Gateways.
DEV-16963	Airwall Gateways	Fixed an issue where the AW-250 SFP (combo port) PHY settings were reset to default when you updated the firmware. The PHY mode settings will now be reset during factory reset. Use Diag Mode to change these settings.
DEV-16638	OpenHIP	Airwall Gateways acting as a Relay may now initiate tunnels to peers that are behind a NAT, using the address of that peer learned via received relay probes.
DEV-16374	Airwall Gateways	Diagnostic mode no longer prevents long hostnames in the "Airwall Conductor Hostname or IP" section

Known Issues

ID	Applies to	Description
DEV-17450	Airwall Gateways	If you are upgrading an AWS cloud **Airwall Gateway *with NVMe***, the update from v2.2.12 to v3.0.1 fails. **Workaround** -- Skip the v3.0.1 release and update to v3.0.2.
DEV-17178	Cellular Airwall Gateways	Cellular details show "unavailable" on the Conductor **Ports** tab after you update the Airwall Gateway to v3.0.1. **Workaround** -- Reboot the Airwall Gateway.
DEV-16999	Airwall Gateways	AW-150 port 5 SFP LEDs are non-functional when the port may be actually linked and active.
DEV-16503	macOS Airwall Agents	Deleting a profile does not immediately delete the associated private key. **Workaround** – Switch to a different profile before creating a profile after deleting one.
DEV-16431	Conductor	When specifying a port mirror destination IP address, ensure that it doesn't conflict with any of the Airwall Gateway's local device IPs
DEV-16397	Conductor	If you change the LSI prefix and have port mirroring configured, you need to either reboot the Conductor, or go to **Settings** > **Diagnostics** and select **Restart metadata cache** to update the LSI prefix.
DEV-16068	Amazon Web Services Conductor	To enable enhanced networking for a cloud Amazon Web Services Airwall Gateway or Conductor, use the custom images instead of the marketplace image.
DEV-16067	Cloud, Conductor, Airwall Gateways	If you are adding a new interface to an existing cloud Airwall Gateway, you must set the source and destination check to false (see your cloud provider for the terminology they use for source and destination checks).
DEV-16059	Airwall Gateways	When HA-pairing two Airwall Gateways that do not have the HA link plugged in correctly, the Conductor displays no actionable error message and the HA setup never completes.

ID	Applies to	Description
DEV-15982	Conductor	Traffic stats reporting graphs generally show a smooth curve between data points. However, over time the graph can show up with sharper angles. The data is still correct, but this is a known issue with the graphing library used by the Conductor.
DEV-15945	Airwall Gateways	If you configure port mirroring using a remote destination local device, GRE/ERSPAN traffic from remote Airwall Gateways will arrive with a source IP in the LSI prefix (defaults to 1.0.0.0/8).
DEV-15923	Airwall Gateways	When you run **Check secure tunnels** on a v3.0 Airwall Gateway, the check falsely reports a bad tunnel status for any peer airwall running a firmware version that is v2.2.8 or lower.
DEV-15887	Airwall Gateways	You cannot currently add VLAN interfaces to the Ruggedcom platform.
DEV-15808	Google Cloud Airwall Gateways	Google Cloud Airwall Gateways with the same VM name have the same device serial number, which can result in a failure when you make a license request in the Conductor. **Workaround** – In Google Cloud, use unique deployment names (VM names) for Airwall Gateways.
DEV-15791	Airwall Gateways	On the Airwall Gateway 100, Port 2 might be inactive after a factory-reset. **Workaround** – After a factory reset, manually reboot the Airwall Gateway 100.
DEV-15787	macOS Airwall Agents	If a person who already has a profile makes a Request to Connect from the Remote Access User portal on the same Conductor, no profile is created. **Workaround** – If the user wants a second profile, they can use an invite code or enter the Conductor information manually.
DEV-15705	macOS Airwall Agents	Establishing a tunnel TO a mobile Airwall Agent (iOS or Android) fails when there is no Airwall Relay involved. **Workaround** – Establish the tunnel FROM the mobile Airwall Agent.
DEV-15572	Airwall Gateways	If you do not specify a gateway in the DHCP server configuration, the DHCP client cannot configure a default gateway. **Workaround** – Unless you want to configure a single isolated subnet, always specify a gateway. For example, a subnet for networked PDUs that should not have any outside connectivity aside from remote access through an Airwall Gateway, and used in conjunction with SNAT over the overlay port group. See https://tempered.force.com/TemperedSupportCenter/s/article/DHCP-server-isn-t-serving-as-a-gateway.

ID	Applies to	Description
DEV-15489	Windows Airwall Agents and Servers	Windows 7 sends an extra Windows system popup when the Windows Airwall Agent UserAuth prompt appears. You can safely ignore this popup, or can disable the Windows 7 service as described in this article from Broadcom: https://knowledge.broadcom.com/external/article/153693/interactive-services-detection-a-progra.html
DEV-15357	macOS Airwall Agents	If you update the macOS Airwall Agent to a release later than v2.2.11 on macOS Mojave using a Conductor-based update package, it may not report the updated version to the Conductor. **Workaround** – Restart the Airwall Agent or reapply the update.
DEV-15338	Linux Airwall Servers	If using a recent systemd-based Linux distribution including Fedora 33 and Debian 11, disable systemd-networkd MAC address randomization of the hip1 interface.
DEV-15302	macOS Airwall Agents	The profile for a macOS Airwall Agent does not work correctly when restored to a new computer using Time Machine. **Workaround** – Create a new profile on the Airwall Agent, and then on the Conductor, replace the old profile with the new one.
DEV-15219	Cellular 110g Airwall Gateways	The Airwall Gateway 110g does not on the Bell Mobility (Canada) cellular provider because they require the use of a http/https proxy.
DEV-15031	Airwall Gateways	Remote syslog over TLS doesn't work when using keys stored in TPM.
DEV-14860	Conductor	Airwall Gateways on older firmware (pre v2.2.0) may send passively-discovered device events to the Conductor even when the feature is off.
DEV-14835	Conductor	Airwall Gateway 150 serial numbers look like exponentiated numbers to Windows Excel, so the column displaying the Serial number shows xxxEyyy instead of the full serial number.
DEV-14739	Airwall Gateways	If you set IPv4 to DHCPv4 and set a static IP address for IPv6, the setting that you set second doesn't get saved. **Workaround** – If you need both IPv4 and IPv6, set static IP addresses for both.
DEV-14736	Cellular Airwall Gateways	Cellular details may display as "unavailable" on the first boot after you update anAirwall Gateway. The cellular connections are not affected. **Workaround** – Reboot the Airwall Gateway again to correctly display the cellular details.

ID	Applies to	Description
DEV-14726	Conductor	If you're viewing an Android Airwall Agent **Ports** tab and the Airwall Agent changes how it is connected to the Conductor (for example, from WiFi to cellular), the display doesn't update correctly. **Workaround** – Refresh the page.
DEV-14715	macOS Airwall Agents	Big Sur ARM64 Macs are not supported in this release
DEV-14610	Conductor	After changing the Reporting traffic stats reporting time, the CPU graph does not display. **Workaround** – Refresh your browser page.
DEV-14584	Cellular Airwall Gateways	Hot-swapping the SIM on an Airwall Gateway 110 with firmware version v2.2.11 may not work. **Workaround** – Reboot the Airwall Gateway after installing a new SIM card.
DEV-14551	Conductor	The Android Airwall Agent lets you press the **Edit Settings** button on the **Ports** page; however, submitting any changes to the page results in an error message.
DEV-14426	Conductor, Airwall Gateways	Bypass destinations with a hostname do not show device activity in the Conductor.
DEV-14308	OpenHIP	Initial packets are dropped while building a new tunnel to a new peer Airwall Gateway.
DEV-14249	iOS Airwall Agents	**Check Secure TunnelsTunnel Status** may show as unavailable on iOS. **Workaround** – You can determine tunnel status by checking packets sent or received.
DEV-14223	Google Cloud	Add an overlay IP to agent in order to talk to device behind Google 300v.
DEV-14218	Airwall Gateways	NAT broadcast applied to traffic between ports within a single port group. Use an external switch if you need to connect multiple devices to a single port group and use the NAT broadcast feature and require IP broadcast un-NATed between those local devices.
DEV-14045	Android and iOS Airwall Agents	iOS does not currently support overlay ping.
DEV-14015	OpenHIP	If an Airwall Relay is also used as a bypass gateway, Airwall Edge Services behind the relay are not able to use that relay. **Workaround** – Deploy multiple relays so at least one relay is usable by each pair of Airwall Edge Services that need to communicate.
DEV-13775	Azure Cloud Airwall Gateways	The Conductor might rarely give a "Net::ReadTimeout" error when you try to deploy an Azure Airwall Gateway 300v or server. This error doesn't indicate that the deployment has failed. If you get this error message, go to Azure portal and check the actual deployment result.

ID	Applies to	Description
DEV-13699	Windows Airwall Agents and Servers	The initial ping from the Windows Airwall Agent can be misleading since it currently includes the time to initially set up the connection. **Workaround** – Ping a second time to see actual ping time.
DEV-13650	Conductor	SoIP device activity is not being reported on an Airwall Gateway **Local Devices** tab.
DEV-13640	Conductor	Airwall Relay diagnostics do not work on a Standby Conductor.
DEV-13633	Conductor	A standby Conductor shows available firmware downloads, but they cannot be downloaded. **Workaround** – Download firmware from the active Conductor.
DEV-13620	Conductor	In **Airwall** > **Ports** > **Failover settings**, the failover ping occurs only every "ping rate" + "ping timeout" seconds, somewhat unexpectedly.
DEV-13607	Conductor, Airwall Gateways	Creating a link failover group (**Airwall** > **Ports** > **Failover settings**) does not apply the settings to any port groups. You must also assign the failover group to port groups on the **Ports** page.
DEV-13588	Conductor	Opening the Conductor on Internet Explorer 11 can be very slow for medium to large deployments. **Workaround** – Use the latest version of Chrome, Firefox, or Edge instead.
DEV-13536	Windows Airwall Agents and Servers	When you uninstall the Windows Airwall Agent, it does not remove the tun-tap driver. **Workaround** – Delete the driver from C:\Windows \System32\drivers\tnw-tap.sys.
DEV-13531	Cloud Conductor	Automatically creating Cloud HA Conductors only works if you use the same cloud provider for both active and standby Conductors. For example, AWS HA Active and AWS HA Standby. **Workaround** – You can manually set up different cloud providers as HA pair Conductors.
DEV-13474	Airwall Gateways	If you configure multiple overlay port groups with the same overlay IP subnet (same or different IP addresses) and then create a local device equal to the entire subnet with port affinity set, it may not lead to the expected result.
DEV-13331	Alibaba Cloud Airwall Gateways	The Alibaba Cloud Conductor system time is incorrect. **Workaround** – Change the Conductor system time to browser time: In Conductor **Settings**, under **System time**, select **Edit Settings**, select **Set browser time**, and then select **Update Settings**.

ID	Applies to	Description
DEV-13195	Conductor, Airwall Gateways	When you upgrade a Cellular Airwall Gateway-150 from 2.2.3 to 2.2.5, the cellular details all become "Unavailable." **Workaround** – Reboot and the details return.
DEV-13194	Conductor	**Check Connectivity** > **Ping Local Devices** for an Airwall Gateway fails in Internet Explorer 11 if one of the devices is defined as a CIDR. **Workaround** – Use one of the latest versions of Chrome, Firefox, Safari or Edge.
DEV-12852	Windows Airwall Agents	Windows by default doesn't allow multiple 'active' interfaces. It prefers ethernet over cellular whenever possible. **Workaround** – Set Windows to keep multiple interfaces open by editing the fMinimizeConnections registry value: **1.** Hold the Windows Key and press `R`. **2.** On the **Run** page, type `regedit` and click **OK**. **3.** Navigate to the following path in Registry Editor: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WcmSvc\` **4.** See if the `GroupPolicy` subkey exists. If not, right-click on `WcmSvc` and select **New** > **Key** and name it `GroupPolicy`. **5.** Right-click `GroupPolicy` and choose **New** > **DWORD (32-bit)** > **Create value**. **6.** Name the value `fMinimizeConnections` and select **OK**. (The value should be 0, or false). **7.** Reboot and test.
DEV-11710	macOS Airwall Agents	If you change the LSI prefix on the Conductor, the macOS Airwall Agent doesn't update the routes correctly. **Workaround** – Close and reopen the macOS Airwall Agent.
DEV-10590	Cloud Airwall Gateways	The Conductor does not display an error when adding a route that would exceed the maximum number of allowed routes in the cloud provider.
DEV-10039	Airwall Gateways	An Airwall Gateway-150 can show "could not detect attached switch" intermittently.
DEV-9546	Airwall Gateways, Airwall Gateways 150	The Airwall Gateway-150 serial connection has an intermittent issue when large amounts of data are sent over the console.
DEV-9429	Windows Airwall Agents	When you update the Overlay Device IP address for a Windows Airwall Server in the Conductor, it doesn't always update the first time. Workaround -- Open and update the address a second time.

Release Notes v3.0.1

Release Date: Feb 3, 2022

Update Considerations

Update to this version if you've experienced the following issues:

- Issues configuring an Airwall Gateway using a DNSSRV record.
- High disk usage using Conductor high-availability.
- Airwall Relay not relaying traffic to HA-pairedAirwall Gateways.

Downloads

For firmware and software downloads for this version, see 3.0.1 firmware and software on page 525.

Fixes

ID	Applies to	Description
DEV-17147	Conductor	Fixed an issue where a device match rule in smart device groups could match against a device on another Airwall Gateway when there are duplicates of the same IP address.
DEV-17146	Airwall Gateways	Cellular Airwall Gateways continue to auto-repair the cellular ports even if the ports are not being assigned to a link manager failover group. They also auto-reboot if none of the ports are healthy.
DEV-16941	Airwall Gateways	Fixed an issue that caused Airwall Relays to reject relaying traffic to HA-paired Airwall Gateways.
DEV-16938	API, Conductor	Fixed an API issue where a system administrator could not add, update, or remove device match rules on a smart device group unless they were the rule editor.
DEV-16919	Conductor	Fixed an issue where membership device count shown on overlay network index could double count devices if they were included in the network multiple times via device groups.
DEV-16895	Conductor	Very long names no longer run off the screen.
DEV-16879	Conductor	Reduced the standard expiration of stored tunnel stats to 1 week to improve database performance. You can adjust the expiration using the settings API.
DEV-16848	BaseOS	Updated the mvebu64 firmware update description for clarity.
DEV-16832	Conductor	Many tables have been updated to handle truncating and wrapping of important information (names, descriptions, etc) better.
DEV-16827	Conductor	Fixed an issue where, on the device show page, an actions drop-down menu with no actions is available to users who cannot edit the device.
DEV-16826	API, Conductor	API -- Devices of Airwall Agents now display the tags from the parent Airwall Gateway when serialized in the API (like they show in the UI).
DEV-16825	API, Conductor	If an Airwall Agent is tagged, the device for that Airwall Agent is also tagged and returned when searching for tagged devices.
DEV-16824	API, Conductor	Tagged devices, device groups, Airwalls, Airwall groups, people, and networks index endpoints are now all paginated.

ID	Applies to	Description
DEV-16812	Conductor	Fixed an issue where, for network administrators, some of the overlay networks they are a member of were not shown on their person page in the overlay networks panel.
DEV-16807	Airwall Gateways	Fixed an issue affecting Airwall Gateways with a Conductor URL auto-configured using a DNS SRV record. The Airwall Gateway would appear for initial provisioning but failed to connect back to the Conductor to be managed.The Airshell command `status conductor` now displays 'Conductor DNS SRV:' along with any URL discovered from DNS, otherwise the text "(not used)".
DEV-16801	Conductor	You can now disable spanning tree (by clearing the **Enable spanning tree** checkbox) for underlay bypasses with one interface. This setting is automatically enabled on an underlay with multiple ports or bypass port group with **Routed_only** disabled.
DEV-16781	Conductor	Fixed an issue where tag names at the top of pages were being truncated, making them difficult to read.
DEV-16780	Conductor	Fixed an issue where if you selected a device while the Airwall network graph was displayed, it would cause a console error.
DEV-16767	Conductor	Device names in the Airwall local devices table no longer truncate unnecessarily.
DEV-16759	Conductor	Fixed an issue where network administrators could create tags, possibly attached to smart device groups, that could then be used by network administrators in a different overlay in the system. Network administrators can now only create tags for use by themself.
DEV-16758	Conductor	Fixed an issue where tags created by system administrators were defaulting to "anyone," which allowed network administrators access to resources they were not intended to have. Tags created by system administrators now default to only other system administrators.
DEV-16755	Conductor	Fixed an issue where the default link failover group of new or factory-reset wireless Airwall Gateways was missing the bypass traffic type.
DEV-16753	Airwall Gateways	Fixed an issue that allowed you to revoke HA-paired Airwall Gateways in the Conductor.
DEV-16752	Airwall Gateways	Factory reset now clears activation codes.
DEV-16751	Conductor	Fixed an issue where viewing the details of sent Airwall Invitations would show a name schema even if one wasn't set.
DEV-16667	Airwall Gateways	Fixed an issue where the Airshell command `conf password` returned an error "The password for airsh cannot be changed yet" due to clock skew issues.
DEV-16639	Conductor	Fixed an issue where device groups created in one browser window did not display in other Conductor browser windows without a refresh.

ID	Applies to	Description
DEV-16540	Conductor	Fixed graph performance issues.
DEV-16521	OpenHIP	Improved path MTU discovery.
DEV-16456	Airwall Gateways	Fixed an issue where when you specify a BPF expression on both a port mirroring source and its port mirroring destination, then clear the expression from the port mirroring source, the BPF expression from the port mirroring destination isn't used.
DEV-16455	Airwall Gateways	Fixed an issue where an ERSPAN session ID/GRE key specified on a port mirroring destination was ignored when not overridden on the port mirroring source.
DEV-16379	Airwall Gateways	During a factory reset, configured log levels are now reset.
DEV-16365	Conductor	Fixed an issue where the error message from a failed user authentication from an agent or server was not clear when LDAP was configured on the Conductor.
DEV-16327	Conductor	Fixed an issue where user onboarding activation codes from a person group were not using the specified hostname if it did not match the default.
DEV-16322	Conductor	Fixed an issue where if a person is in more than one person group that has access windows set, they can only authenticate for a remote session during times that are inside all of the access windows for those person groups.
DEV-16308	Airwall Gateways	Fixed an issue where SNAT was not applied to routed traffic bypass traffic when SNAT was enabled and L3 only was disabled on a bypass port group. SNAT is not applied to L2 traffic.
DEV-16204	Conductor	The overlay Add Devices page and the overlay search box should now return the same results
DEV-15984	Cellular Airwall Gateways	Fixed an issue that could block bypass traffic on cellular ports.
DEV-14570	Conductor	Fixed an issue where if you set an Airwall Agent owner to a user (LDAP, local, or OIDC) and someone attempted to authenticate as a different OIDC user, they could not authenticate (which is the correct behavior), but they got a 500 error instead of a helpful error message.

Known Issues

ID	Applies to	Description
DEV-17450	Airwall Gateways	If you are upgrading an AWS cloud **Airwall Gateway *with NVMe***, the update from v2.2.12 to v3.0.1 fails. **Workaround** -- Skip the v3.0.1 release and update to v3.0.2.
DEV-16999	Airwall Gateways	AW-150 port 5 SFP LEDs are non-functional when the port may be actually linked and active.

ID	Applies to	Description
DEV-16503	macOS Airwall Agents	Deleting a profile does not immediately delete the associated private key. **Workaround** – Switch to a different profile before creating a profile after deleting one.
DEV-16397	Conductor	If you change the LSI prefix and have port mirroring configured, you need to either reboot the Conductor, or go to **Settings** > **Diagnostics** and select **Restart metadata cache** to update the LSI prefix.
DEV-16068	Amazon Web Services Conductor	To enable enhanced networking for a cloud Amazon Web Services Airwall Gateway or Conductor, use the custom images instead of the marketplace image.
DEV-16067	Cloud, Conductor, Airwall Gateways	If you are adding a new interface to an existing cloud Airwall Gateway, you must set the source and destination check to false (see your cloud provider for the terminology they use for source and destination checks).
DEV-16059	Airwall Gateways	When HA-pairing two Airwall Gateways that do not have the HA link plugged in correctly, the Conductor displays no actionable error message and the HA setup never completes.
DEV-15982	Conductor	Traffic stats reporting graphs generally show a smooth curve between data points. However, over time the graph can show up with sharper angles. The data is still correct, but this is a known issue with the graphing library used by the Conductor.
DEV-15945	Airwall Gateways	If you configure port mirroring using a remote destination local device, GRE/ERSPAN traffic from remote Airwall Gateways will arrive with a source IP in the LSI prefix (defaults to 1.0.0.0/8).
DEV-15923	Airwall Gateways	When you run **Check secure tunnels** on a v3.0 Airwall Gateway, the check falsely reports a bad tunnel status for any peer airwall running a firmware version that is v2.2.8 or lower.
DEV-15887	Airwall Gateways	You cannot currently add VLAN interfaces to the Ruggedcom platform.
DEV-15808	Google Cloud Airwall Gateways	Google Cloud Airwall Gateways with the same VM name have the same device serial number, which can result in a failure when you make a license request in the Conductor. **Workaround** – In Google Cloud, use unique deployment names (VM names) for Airwall Gateways.
DEV-15791	Airwall Gateways	On the Airwall Gateway 100, Port 2 might be inactive after a factory-reset. **Workaround** – After a factory reset, manually reboot the Airwall Gateway 100.

ID	Applies to	Description
DEV-15787	macOS Airwall Agents	If a person who already has a profile makes a Request to Connect from the Remote Access User portal on the same Conductor, no profile is created. **Workaround** – If the user wants a second profile, they can use an invite code or enter the Conductor information manually.
DEV-15705	macOS Airwall Agents	Establishing a tunnel TO a mobile Airwall Agent (iOS or Android) fails when there is no Airwall Relay involved. **Workaround** – Establish the tunnel FROM the mobile Airwall Agent.
DEV-15572	Airwall Gateways	If you do not specify a gateway in the DHCP server configuration, the DHCP client cannot configure a default gateway. **Workaround** – Unless you want to configure a single isolated subnet, always specify a gateway. For example, a subnet for networked PDUs that should not have any outside connectivity aside from remote access through an Airwall Gateway, and used in conjunction with SNAT over the overlay port group. See https://tempered.force.com/TemperedSupportCenter/s/article/DHCP-server-isn-t-serving-as-a-gateway.
DEV-15489	Windows Airwall Agents and Servers	Windows 7 sends an extra Windows system popup when the Windows Airwall Agent UserAuth prompt appears. You can safely ignore this popup, or can disable the Windows 7 service as described in this article from Broadcom: https://knowledge.broadcom.com/external/article/153693/interactive-services-detection-a-progra.html
DEV-15357	macOS Airwall Agents	If you update the macOS Airwall Agent to a release later than v2.2.11 on macOS Mojave using a Conductor-based update package, it may not report the updated version to the Conductor. **Workaround** – Restart the Airwall Agent or reapply the update.
DEV-15338	Linux Airwall Servers	If using a recent systemd-based Linux distribution including Fedora 33 and Debian 11, disable systemd-networkd MAC address randomization of the hip1 interface.
DEV-15302	macOS Airwall Agents	The profile for a macOS Airwall Agent does not work correctly when restored to a new computer using Time Machine. **Workaround** – Create a new profile on the Airwall Agent, and then on the Conductor, replace the old profile with the new one.
DEV-15219	Cellular 110g Airwall Gateways	The Airwall Gateway 110g does not on the Bell Mobility (Canada) cellular provider because they require the use of a http/https proxy.

ID	Applies to	Description
DEV-15031	Airwall Gateways	Remote syslog over TLS doesn't work when using keys stored in TPM.
DEV-14860	Conductor	Airwall Gateways on older firmware (pre v2.2.0) may send passively-discovered device events to the Conductor even when the feature is off.
DEV-14835	Conductor	Airwall Gateway 150 serial numbers look like exponentiated numbers to Windows Excel, so the column displaying the Serial number shows xxxEyyy instead of the full serial number.
DEV-14739	Airwall Gateways	If you set IPv4 to DHCPv4 and set a static IP address for IPv6, the setting that you set second doesn't get saved. **Workaround** – If you need both IPv4 and IPv6, set static IP addresses for both.
DEV-14736	Cellular Airwall Gateways	Cellular details may display as "unavailable" on the first boot after you update anAirwall Gateway. The cellular connections are not affected. **Workaround** – Reboot the Airwall Gateway again to correctly display the cellular details.
DEV-14726	Conductor	If you're viewing an Android Airwall Agent **Ports** tab and the Airwall Agent changes how it is connected to the Conductor (for example, from WiFi to cellular), the display does not update correctly. **Workaround** – Refresh the page.
DEV-14715	macOS Airwall Agents	Big Sur ARM64 Macs are not supported in this release
DEV-14610	Conductor	After changing the Reporting traffic stats reporting time, the CPU graph does not display. **Workaround** – Refresh your browser page.
DEV-14584	Cellular Airwall Gateways	Hot-swapping the SIM on an Airwall Gateway 110 with firmware version v2.2.11 may not work. **Workaround** – Reboot the Airwall Gateway after installing a new SIM card.
DEV-14551	Conductor	The Android Airwall Agent lets you press the **Edit Settings** button on the **Ports** page; however, submitting any changes to the page results in an error message.
DEV-14426	Conductor, Airwall Gateways	Bypass destinations with a hostname do not show device activity in the Conductor.
DEV-14308	OpenHIP	Initial packets are dropped while building a new tunnel to a new peer Airwall Gateway.
DEV-14249	iOS Airwall Agents	**Check Secure TunnelsTunnel Status** may show as unavailable on iOS. **Workaround** – You can determine tunnel status by checking packets sent or received.

ID	Applies to	Description
DEV-14223	Google Cloud	Add an overlay IP to agent in order to talk to device behind Google 300v.
DEV-14218	Airwall Gateways	NAT broadcast applied to traffic between ports within a single port group. Use an external switch if you need to connect multiple devices to a single port group and use the NAT broadcast feature and require IP broadcast un-NATed between those local devices.
DEV-14045	Android and iOS Airwall Agents	iOS does not currently support overlay ping.
DEV-14015	OpenHIP	If an Airwall Relay is also used as a bypass gateway, Airwall Edge Services behind the relay are not able to use that relay. **Workaround** – Deploy multiple relays so at least one relay is usable by each pair of Airwall Edge Services that need to communicate.
DEV-13775	Azure Cloud Airwall Gateways	The Conductor might rarely give a "Net::ReadTimeout" error when you try to deploy an Azure Airwall Gateway 300v or server. This error doesn't indicate that the deployment has failed. If you get this error message, go to Azure portal and check the actual deployment result.
DEV-13699	Windows Airwall Agents and Servers	The initial ping from the Windows Airwall Agent can be misleading since it currently includes the time to initially set up the connection. **Workaround** – Ping a second time to see actual ping time.
DEV-13650	Conductor	SoIP device activity is not being reported on an Airwall Gateway **Local Devices** tab.
DEV-13640	Conductor	Airwall Relay diagnostics do not work on a Standby Conductor.
DEV-13633	Conductor	A standby Conductor shows available firmware downloads, but they cannot be downloaded. **Workaround** – Download firmware from the active Conductor.
DEV-13620	Conductor	In **Airwall** > **Ports** > **Failover settings**, the failover ping occurs only every "ping rate" + "ping timeout" seconds, somewhat unexpectedly.
DEV-13607	Conductor, Airwall Gateways	Creating a link failover group (**Airwall** > **Ports** > **Failover settings**) does not apply the settings to any port groups. You must also assign the failover group to port groups on the **Ports** page.
DEV-13588	Conductor	Opening the Conductor on Internet Explorer 11 can be very slow for medium to large deployments. **Workaround** – Use the latest version of Chrome, Firefox, or Edge instead.

ID	Applies to	Description
DEV-13536	Windows Airwall Agents and Servers	When you uninstall the Windows Airwall Agent, it does not remove the tun-tap driver. **Workaround** – Delete the driver from C:\Windows \System32\drivers\tnw-tap.sys.
DEV-13531	Cloud Conductor	Automatically creating Cloud HA Conductors only works if you use the same cloud provider for both active and standby Conductors. For example, AWS HA Active and AWS HA Standby. **Workaround** – You can manually set up different cloud providers as HA pair Conductors.
DEV-13474	Airwall Gateways	If you configure multiple overlay port groups with the same overlay IP subnet (same or different IP addresses) and then create a local device equal to the entire subnet with port affinity set, it may not lead to the expected result.
DEV-13331	Alibaba Cloud Airwall Gateways	The Alibaba Cloud Conductor system time is incorrect. **Workaround** – Change the Conductor system time to browser time: In Conductor **Settings**, under **System time**, select **Edit Settings**, select **Set browser time**, and then select **Update Settings**.
DEV-13195	Conductor, Airwall Gateways	When you upgrade a Cellular Airwall Gateway-150 from 2.2.3 to 2.2.5, the cellular details all become "Unavailable." **Workaround** – Reboot and the details return.
DEV-13194	Conductor	**Check Connectivity** > **Ping Local Devices** for an Airwall Gateway fails in Internet Explorer 11 if one of the devices is defined as a CIDR. **Workaround** – Use one of the latest versions of Chrome, Firefox, Safari or Edge.
DEV-12852	Windows Airwall Agents	Windows by default doesn't allow multiple 'active' interfaces. It prefers ethernet over cellular whenever possible. **Workaround** – Set Windows to keep multiple interfaces open by editing the fMinimizeConnections registry value: **1.** Hold the Windows Key and press `R`. **2.** On the **Run** page, type `regedit` and click **OK**. **3.** Navigate to the following path in Registry Editor: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies \Microsoft\Windows\WcmSvc\` **4.** See if the `GroupPolicy` subkey exists. If not, right-click on `WcmSvc` and select **New** > **Key** and name it `GroupPolicy`. **5.** Right-click `GroupPolicy` and choose **New** > **DWORD (32-bit)** > **Create value**. **6.** Name the value `fMinimizeConnections` and select **OK**. (The value should be 0, or false). **7.** Reboot and test.

ID	Applies to	Description
DEV-11710	macOS Airwall Agents	If you change the LSI prefix on the Conductor, the macOS Airwall Agent doesn't update the routes correctly. **Workaround** – Close and reopen the macOS Airwall Agent.
DEV-10590	Cloud Airwall Gateways	The Conductor does not display an error when adding a route that would exceed the maximum number of allowed routes in the cloud provider.
DEV-10039	Airwall Gateways	An Airwall Gateway-150 can show "could not detect attached switch" intermittently.
DEV-9546	Airwall Gateways, Airwall Gateways 150	The Airwall Gateway-150 serial connection has an intermittent issue when large amounts of data are sent over the console.
DEV-9429	Windows Airwall Agents	When you update the Overlay Device IP address for a Windows Airwall Server in the Conductor, it doesn't always update the first time. Workaround -- Open and update the address a second time.

Release Notes v3.0.0

Release Date: Nov 2, 2021

Important Notes

- **Update all v2.1.x Airwall Edge Services** – It is recommended that you update all v2.1.x and earlier Airwall Edge Services with v2.2.x or later before installing v3.0.0. With this release, any Airwall Edge Services running v2.1.x firmware show an error in the Conductor. For more information, see Update v2.1.x Airwall Edge Services for the v3.0.0 Conductor on page 495.
- **If you are updating a virtual Conductor to v3.0.0 or later** – You may need to expand the disk size for the virtual machine to 1GB. For instructions, see your virtual machine documentation, or the suggested VMware and Hyper-V instructions at Expand the Disk Size for a virtual Airwall Gateway on page 311.

End of Life/End of Support Bulletins

- **2.1.x End of Life** – See Software support end of life for versions 2.1.x and earlier on page 505. For update instructions, see Update v2.1.x Airwall Edge Services for the v3.0.0 Conductor on page 495.
- **Ubuntu16 and Centos7 End of Support** – See AWS and Azure Linux OS Versions End of Support on page 498

Update Considerations

You may want to update to this version to use the following features:

- Backhaul Bypass on page 395
- Import people using a CSV file on page 61
- Customize Permissions for System and Network Administrators on page 56
- Customize the Conductor Login page on page 40
- Customize Conductor emails on page 42
- Disconnected Mode – Reduce Conductor traffic from Airwall Agents and Servers on page 99
- Airwall Invitation improvements – Walkthrough - Onboard people to your Airwall secure network with User Authentication on page 83
- Linux Airwall Server Airshell commands on page 372

- Manage Failover between Underlay Port Groups on page 391
- Run Network Activity Reports on page 116

Downloads

For firmware and software downloads for this version, see 3.0.0 firmware and software on page 527.

What's New in 3.0.0

This version of the Airwall Solution includes several usability and functionality improvements that can simplify and streamline the setup and administration of an Airwall secure network.

Add Trust Policy using Drag-and-drop

You can now add and remove trust between devices on an overlay visually, or through context menus on a graph. Changes to trust on the graph are reflected on the **Devices** tab.

Learn more – Add and remove device trust on page 427

Backhaul Bypass

You can designate an Airwall Gateway as a bypass egress and then point other Airwall Gateways at it so they can reach bypass destinations through the designated bypass egress Airwall Gateway.

Learn more – Backhaul Bypass on page 395

Bulk Editing of People and People Groups

You can add many local users to the Conductor at one time by importing them in bulk. You export a .csv file as a template or with current users, and then import to add people to the Conductor in one step.

Learn more –

- Import people using a CSV file on page 61
- Remove people in bulk on page 63

Customized Permissions for System and Network Administrators

You can fine tune permissions for system and network administrators, giving you finer control over permissions on your network.

Learn more – Customize Permissions for System and Network Administrators on page 56

Streamlined Conductor View for Network Administrators

One of the custom permissions you can set for Network administrators provides them with a streamlined view that can simplify their workflow. Network administrators using the streamlined view can manage their overlays, and the devices, **Device groups**, and Airwall Edge Services in them.

Learn more – Set a Streamlined View for a Network Administrator on page 58

Reports

You can now run reports on different types of network activity on your Airwall secure network, including:

- Onboarding and offboarding of Airwall Edge Services or people
- Status of Airwall Edge Services or devices
- Conductor local or remote access

Learn more – Run Network Activity Reports on page 116

Monitors and Alerts

This version includes the following additions:

- **CPU Frequency** – The Airwall health data monitors can now monitor CPU frequency.
- **Details for Intrusion prevention** – Intrusion prevention alerts now indicate which devices are the source or destination of the alert where possible.

Conductor Customization

You can customize the Conductor login screen and emails sent from the Conductor for your business. Here's what you can customize:

- **Conductor login screen** – Add your company logo, and change the background colors and favicon.
- **Conductor emails** – Add your company logo and change the text color. You can also customize the subject line and add a note from the administrator when sending Airwall Invitations.

Learn more –

- Customize the Conductor on page 40
- Customize the Conductor Login page on page 40
- Customize Conductor emails on page 42

Disconnected Mode

Reduce the traffic from Airwall Agents and Servers connecting to your Conductor by setting up Disconnected mode. In Disconnected mode, Airwall Agents and Servers connect to your Conductor at intervals – between 10 minutes and 12 hours (720 minutes) – to get updates when people are not actively using the connection.

By reducing the traffic on your Conductor, Disconnected mode allows you to improve performance and scalability of your Airwall secure network. In v3.0, Disconnected mode is supported by the v3.0 Android, Linux, and macOS Airwall Agents and Servers.

Learn more –

- Disconnected Mode – Reduce Conductor traffic from Airwall Agents and Servers on page 99
- Sync an Airwall Agent or Server in Disconnected Mode on page 29

Airwall Invitations

This version includes several enhancements to Airwall Invitations:

- When you're creating **People groups** with user onboarding enabled, you now have the option to send email to users when they get an activation code in the system. The email provides instructions on how to download an Airwall Agent and connect it to the Conductor.
- The email sent with Airwall Invitations has more options for customization. See **Conductor Customization** above.
- Airwall Invitations can now be used to give activation codes to existing users in addition to sending them to an email address or bulk downloading them. See the **Airwalls** > **New Airwall invitations**.
- The naming schema for Airwall Invitations can now include the hostname of the connecting Airwall Edge Service.
- You can now include the hostname of the connecting Airwall Edge Service when naming devices connecting using Airwall Invitations.

Learn more – Walkthrough - Onboard people to your Airwall secure network with User Authentication on page 83

Linux Airwall Server

This version includes these additions to the Linux Airwall Server:

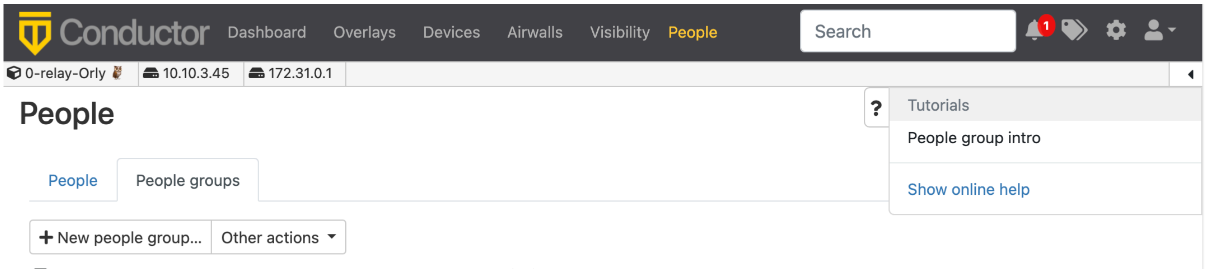
- **DockerHub deployment** – The Linux Airwall Server can now be deployed in a container from DockerHub using Ubuntu18 and CentOS8. For additional example Dockerfiles, contact Customer Success at Customer Success.
- **Supports Airshell** – The Linux Airwall Server now has the Airshell command-line utility. To start it, type `sudo airsh` (root user) or `sudo airwall -s`
- **Ping from port groups** – The ping function can now ping from the underlay or overlay port groups.
- **Firmware updates** – The Linux Airwall Server can now be updated from the Conductor.

Learn more –

- Connect with a Linux Airwall Server on page 26
- Linux Airwall Server Airshell commands on page 372

Conductor Tutorials and Help

The Conductor now contains several tutorials to help you set up and configure a new Conductor, as well as use and understand different features in the Conductor. You can also directly access Airwall help from the Conductor:



Learn more –

- Get Started using Conductor Help and Tutorials on page 140
- Show or Hide Conductor Setup progress on page 40

Licensing Updates

In v3.0, the following licenses have been changed:

- The Airwall Gateway 100V is no longer available
- You no longer need a separate license for port mirroring

Manage failover between underlay port groups

The Link Manager that Conductor uses to manage port failover groups has been improved. The following has been updated:

- You can now set port group link auto-repair globally per Airwall Gateway.
- You can now manage underlay links independently by traffic type.
- When you set up link failover groups, you can now require all pings to be successful if multiple ping destinations are assigned.

Learn more – Manage Failover between Underlay Port Groups on page 391

API Updates

The following updates and improvements have been made to the API:

- **Pagination** is turned on by default in 3.0 for all index endpoints, which may affect existing scripts. Enabling pagination helps scale Conductor capacity. If you need to preserve existing behavior, add a query parameter for `pagination=false` to any index API endpoints you are using.
- The API for **Airwall Invitations** now includes new invitation methods: email invites, download multiple activation codes, apply an invite to an existing person, or download a reusable invitation. The documentation has also been updated.

- **People reference** now includes `person_group_ids` and `overlay_network_ids`.
- **Person groups reference** now includes user onboarding configuration information.

Terraform Deployment Support

This version contains Terraform deployment support for Conductors, Airwall Gateways, and Linux Airwall Servers for all supported Cloud Providers. For example plans, please contact Customer Success at Customer Success.

New and Improved Conductor Features

Dashboard	The Dashboard now includes a **Provisioning** tab where you can see and manage all provisioning requests.
General	There is now infinite scrolling for lists on most pages, and streamlined inline editing, including direct editing of names and tags at the top on most pages.
Devices page	This page has been simplified, and provides more details on device conflicts to help you troubleshoot.
People page	Administrators can now view the Airwalls owned by a person from the person details page.
Settings	The Conductor Settings page has been streamlined and reorganized to make it easier to find the settings you want.
New Airwall Agent user authentication settings	New settings allow you to automate assigning an Airwall Agent owner: **Require owner for Airwall Agent authorization** and **Auto-assign Airwall agent owner on login**.
Replacing Airwalls	You now have the option to revoke, or both revoke and delete, a source Airwall Edge Service after replacing. Replaced Airwall Edge Services that are not deleted are named "<old name (Replaced by UID of replacement)>" to make them easier to find.
Diagnostic Tools on the Standby Conductor	You can now use diagnostic tools on a Standby Conductor.
Better CA certificate replacement and removal handling	When you replace your CA certificates, any Airwall Gateways with custom certs installed now check their cert against the new CA. If they cannot be verified, the cert is removed so the Airwall Gateway does not lose access to the Conductor. If the CA is removed entirely, all customer certs are also removed.

Learn more –

- The Conductor Dashboard on page 32
- Configure Authentication Options on page 242

New and Updated Help

In addition to the content added for new features linked above, here’s the new and updated content published since our last major release:

New –

- Expand the Disk Size for a virtual Airwall Gateway on page 311

- Airwall Gateway 75 Installation Guide (PDF)

Updated –

- Walkthrough - Onboard people to your Airwall secure network with User Authentication on page 83
- Configure Port Groups with Airshell on page 376
- Set up Conductor high availability on page 269
- Manage devices dynamically with Smart Device Groups on page 105
- Configuring a Conductor IP, Friendly URL, or Port on page 236
- Understand People Roles and Permissions on page 58
- Configure Conductor Remote Logging on page 273
- Enable DNS lookup for bypass destinations on page 398
- Monitor Activity and Connections on page 116
- Integrate Third-party Authentication with OpenID Connect on page 247
- Airwall Gateway Airshell Console Commands - airsh - New `conf model` command

Fixes

ID	Applies to	Description
DEV-16491	Cellular Airwall Gateways	Fixed an issue where underlay interface MTU was not considered in tunnel overlay MTU, and another where the path MTU didn't work correctly across local bypass configurations. **Known issue** – The path MTU doesn't work across backhaul bypass. Make sure any backhaul bypass egress Airwall Gateways have a full 1500 byte standard Ethernet MTU (that is, do not use a cell modem).
DEV-16233	Airwall Gateways	Fixed an issue where Ping <ip or hostname> (in Airwall Diagnostics) returned false negatives for hostnames longer than 46 bytes.
DEV-16102	Airshell, Airwall Gateways	The Airshell `firmware-fallback` command is now functional on Advantech (Airwall AV-3200 series).
DEV-15942	Airwall Gateways	Fixed a DNS resolver issue that could cause long delays for Airwall Gateways trying to reconnect to the Conductor when configured with a hostname.
DEV-15938	Airshell	The 'activate' command in Airshell now takes the activation code as an optional argument. For example, `activate 75820b33fa5a`.
DEV-15860	Hardware Conductor	Fixed an issue where the Conductor-500 LCD panel would display "Conductor unreachable".
DEV-15835	Conductor	Fixed an issue where the Traffic stats monitor alerts indicated traffic in kB/s when the correct value is Kb/s (kilobits per second).
DEV-15784	Diagnostic mode	Fixed an issue where bridging all overlay interfaces was causing problems when an Airwall Gateway was in Diag mode.
DEV-15762	Conductor	Fixed an issue where readonly users appeared to be able to edit some tag-related event actions.
DEV-15761	Conductor	Fixed an issue where readonly users appeared to be able to edit some person group user onboarding settings.

ID	Applies to	Description
DEV-15760	Conductor	Intrusion prevention controls are now disabled unless the user has edit permission for the Airwall Edge Service.
DEV-15759	Conductor	Fixed an issue where readonly users appeared to be able to create Airwall Invitations with a template.
DEV-15757	Conductor	Fixed an issue where readonly users appeared to be able to edit tags.
DEV-15736	Airwall Gateways	Fixed an issue where the Ping Peers diagnostic feature didn't support multiple peers with the same underlay IP address.
DEV-15707	Conductor	Fixed an issue where users could not remove all relays from an overlay-managed relay rule.
DEV-15679	Conductor	Your previous login selection is now saved regardless of provider (local, LDAP, or OpenID connect).
DEV-15653	Conductor	Instructions for setting up OpenID Connect on HA standby Conductors are now clearer.
DEV-15534	Cloud Airwall Gateways	Fixed an issue where detecting the underlay NAT IP of a cloud 300v Airwall Gateway wasn't being sent to peer Airwall Gateways
DEV-15525	Conductor	Fixed an issue during a device import where you could select **Next** even though there was an error.
DEV-15420	Conductor	Fixed an issue where you could enable passive device discovery before selecting an Overlay port group.
DEV-15393	Linux Airwall Servers	Fixed the invalid log level error message when starting up a Linux Airwall Server.
DEV-15203	Airwall Gateways	Fixed an issue that could cause passive device detection to ignore devices when traffic is seen immediately after reboot.
DEV-14908	Conductor	Display a warning when there is a mismatch in authentication providers for an Airwall Agent owner and the user auth allowed in the Conductor that would prevent a user from authenticating a remote session.
DEV-14608	Airwall Gateways	Fixed an issue that could prevent initialization of port groups with VLAN interfaces if the parent port was removed from another port group.
DEV-14471	Diagnostic mode	Port group numbers are no longer incremented by 2 in diag mode.
DEV-14318	Conductor, Linux Airwall Servers	Fixed an issue where the Linux Airwall Server wouldn't always get policy updates until it was rebooted.
DEV-13587	Conductor	Clarified language in the **Add / Remove tag** monitor action.
DEV-11607	Airwall Gateways	Fixed an issue in the health data capture for Airwall Gateways that showed all overlay ports as having no link.
DEV-11524	Android Airwall Agents	Fixed an issue where Android was reporting incorrect IPs for interfaces on its Ports tab in the Conductor.

Known Issues

ID	Applies to	Description
DEV-16807	Airwall Gateways	Airwall Gateways that used an auto-configured Conductor URL from a DNS SRV record appear for initial provisioning but fail to connect back to the Conductor to be managed. **Workaround** – Set the Conductor URL manually on the Airwall Gateway using `conductor set <conductor_url>`. For example, `conductor set conductor.example.com`.
DEV-16503	macOS Airwall Agents	Deleting a profile does not immediately delete the associated private key. **Workaround** – Switch to a different profile before creating a profile after deleting one.
DEV-16397	Conductor	If you change the LSI prefix and have port mirroring configured, you need to either reboot the Conductor, or go to **Settings** > **Diagnostics** and select **Restart metadata cache** to update the LSI prefix.
DEV-16322	Conductor	If a person is in more than one person group that has access windows set for the group, they can only authenticate for a remote session during times that are inside all of the access windows for those person groups.
DEV-16068	Amazon Web Services Conductor	To enable enhanced networking for a cloud Amazon Web Services Airwall Gateway or Conductor, use the custom images instead of the marketplace image.
DEV-16059	Airwall Gateways	When HA-pairing two Airwall Gateways that do not have the HA link plugged in correctly, the Conductor displays no actionable error message and the HA setup never completes.
DEV-15982	Conductor	Traffic stats reporting graphs generally show a smooth curve between data points. However, over time the graph can show up with sharper angles. The data is still correct, but this is a known issue with the graphing library used by the Conductor.
DEV-15887	Airwall Gateways	You cannot currently add VLAN interfaces to the Ruggedcom platform.
DEV-15808	Google Cloud Airwall Gateways	Google Cloud Airwall Gateways with the same VM name have the same device serial number, which can result in a failure when you make a license request in the Conductor. **Workaround** – In Google Cloud, use unique deployment names (VM names) for Airwall Gateways.
DEV-15791	Airwall Gateways	On the Airwall Gateway 100, Port 2 might be inactive after a factory-reset. **Workaround** – After a factory reset, manually reboot the Airwall Gateway 100.

ID	Applies to	Description
DEV-15787	macOS Airwall Agents	If a person who already has a profile makes a Request to Connect from the Remote Access User portal on the same Conductor, no profile is created. **Workaround** – If the user wants a second profile, they can use an invite code or enter the Conductor information manually.
DEV-15705	macOS Airwall Agents	Establishing a tunnel TO a mobile Airwall Agent (iOS or Android) fails when there is no Airwall Relay involved. **Workaround** – Establish the tunnel FROM the mobile Airwall Agent.
DEV-15572	Airwall Gateways	If you do not specify a gateway in the DHCP server configuration, the DHCP client cannot configure a default gateway. **Workaround** – Unless you want to configure a single isolated subnet, always specify a gateway. For example, a subnet for networked PDUs that should not have any outside connectivity aside from remote access through an Airwall Gateway, and used in conjunction with SNAT over the overlay port group. See https://tempered.force.com/TemperedSupportCenter/s/article/DHCP-server-isn-t-serving-as-a-gateway.
DEV-15357	macOS Airwall Agents	If you update the macOS Airwall Agent to a release later than v2.2.11 on macOS Mojave using a Conductor-based update package, it may not report the updated version to the Conductor. **Workaround** – Restart the Airwall Agent or reapply the update.
DEV-15338	Linux Airwall Servers	If using a recent systemd-based Linux distribution including Fedora 33 and Debian 11, disable systemd-networkd MAC address randomization of the hip1 interface.
DEV-15302	macOS Airwall Agents	The profile for a macOS Airwall Agent does not work correctly when restored to a new computer using Time Machine. **Workaround** – Create a new profile on the Airwall Agent, and then on the Conductor, replace the old profile with the new one.
DEV-15219	Cellular 110g Airwall Gateways	The Airwall Gateway 110g does not on the Bell Mobility (Canada) cellular provider because they require the use of a http/https proxy.
DEV-15031	Airwall Gateways	Remote syslog over TLS doesn't work when using keys stored in TPM.
DEV-14860	Conductor	Airwall Gateways on older firmware (pre v2.2.0) may send passively-discovered device events to the Conductor even when the feature is off.

ID	Applies to	Description
DEV-14835	Conductor	Airwall Gateway 150 serial numbers look like exponentiated numbers to Windows Excel, so the column displaying the Serial number shows xxxEyyy instead of the full serial number.
DEV-14739	Airwall Gateways	If you set IPv4 to DHCPv4 and set a static IP address for IPv6, the setting that you set second doesn't get saved. **Workaround** – If you need both IPv4 and IPv6, set static IP addresses for both.
DEV-14736	Cellular Airwall Gateways	Cellular details may display as "unavailable" on the first boot after you update anAirwall Gateway. The cellular connections are not affected. **Workaround** – Reboot the Airwall Gateway again to correctly display the cellular details.
DEV-14726	Conductor	If you're viewing an Android Airwall Agent **Ports** tab and the Airwall Agent changes how it is connected to the Conductor (for example, from WiFi to cellular), the display doesn't update correctly. **Workaround** – Refresh the page.
DEV-14715	macOS Airwall Agents	Big Sur ARM64 Macs are not supported in this release
DEV-14610	Conductor	After changing the Reporting traffic stats reporting time, the CPU graph does not display. **Workaround** – Refresh your browser page.
DEV-14584	Cellular Airwall Gateways	Hot-swapping the SIM on an Airwall Gateway 110 with firmware version v2.2.11 may not work. **Workaround** – Reboot the Airwall Gateway after installing a new SIM card.
DEV-14570	Conductor	If you set an Airwall Agent owner to a user (LDAP, local, or OIDC) and someone attempts to user authenticate with a different OIDC user, they will not be able to authenticate (which is the correct behavior), but they see a 500 instead of a helpful error message.
DEV-14551	Conductor	The Android Airwall Agent lets you press the **Edit Settings** button on the **Ports** page; however, submitting any changes to the page results in an error message.
DEV-14426	Conductor, Airwall Gateways	Bypass destinations with a hostname do not show device activity in the Conductor.
DEV-14308	OpenHIP	Initial packets are dropped while building a new tunnel to a new peer Airwall Gateway.
DEV-14249	iOS Airwall Agents	**Check Secure TunnelsTunnel Status** may show as unavailable on iOS. **Workaround** – You can determine tunnel status by checking packets sent or received.

ID	Applies to	Description
DEV-14218	Airwall Gateways	NAT broadcast applied to traffic between ports within a single port group. Use an external switch if you need to connect multiple devices to a single port group and use the NAT broadcast feature and require IP broadcast un-NATed between those local devices.
DEV-14045	Android and iOS Airwall Agents	iOS does not currently support overlay ping.
DEV-14015	OpenHIP	If an Airwall Relay is also used as a bypass gateway, Airwall Edge Services behind the relay are not able to use that relay. **Workaround** – Deploy multiple relays so at least one relay is usable by each pair of Airwall Edge Services that need to communicate.
DEV-13775	Azure Cloud Airwall Gateways	The Conductor might rarely give a "Net::ReadTimeout" error when you try to deploy an Azure Airwall Gateway 300v or server. This error doesn't indicate that the deployment has failed. If you get this error message, go to Azure portal and check the actual deployment result.
DEV-13650	Conductor	SoIP device activity is not being reported on an Airwall Gateway **Local Devices** tab.
DEV-13640	Conductor	Airwall Relay diagnostics do not work on a Standby Conductor.
DEV-13633	Conductor	A standby Conductor shows available firmware downloads, but they cannot be downloaded. **Workaround** – Download firmware from the active Conductor.
DEV-13620	Conductor	In **Airwall** > **Ports** > **Failover settings**, the failover ping occurs only every "ping rate" + "ping timeout" seconds, somewhat unexpectedly.
DEV-13607	Conductor, Airwall Gateways	Creating a link failover group (**Airwall** > **Ports** > **Failover settings**) does not apply the settings to any port groups. You must also assign the failover group to port groups on the **Ports** page.
DEV-13588	Conductor	Opening the Conductor on Internet Explorer 11 can be very slow for medium to large deployments. **Workaround** – Use the latest version of Chrome, Firefox, or Edge instead.
DEV-13531	Cloud Conductor	Automatically creating Cloud HA Conductors only works if you use the same cloud provider for both active and standby Conductors. For example, AWS HA Active and AWS HA Standby. **Workaround** – You can manually set up different cloud providers as HA pair Conductors.

ID	Applies to	Description
DEV-13474	Airwall Gateways	If you configure multiple overlay port groups with the same overlay IP subnet (same or different IP addresses) and then create a local device equal to the entire subnet with port affinity set, it may not lead to the expected result.
DEV-13331	Alibaba Cloud Airwall Gateways	The Alibaba Cloud Conductor system time is incorrect. **Workaround** – Change the Conductor system time to browser time: In Conductor **Settings**, under **System time**, select **Edit Settings**, select **Set browser time**, and then select **Update Settings**.
DEV-13195	Conductor, Airwall Gateways	When you upgrade a Cellular Airwall Gateway-150 from 2.2.3 to 2.2.5, the cellular details all become "Unavailable." **Workaround** – Reboot and the details return.
DEV-13194	Conductor	**Check Connectivity** > **Ping Local Devices** for an Airwall Gateway fails in Internet Explorer 11 if one of the devices is defined as a CIDR. **Workaround** – Use one of the latest versions of Chrome, Firefox, Safari or Edge.
DEV-11710	macOS Airwall Agents	If you change the LSI prefix on the Conductor, the macOS Airwall Agent doesn't update the routes correctly. **Workaround** – Close and reopen the macOS Airwall Agent.
DEV-10590	Cloud Airwall Gateways	The Conductor does not display an error when adding a route that would exceed the maximum number of allowed routes in the cloud provider.
DEV-10039	Airwall Gateways	An Airwall Gateway-150 can show "could not detect attached switch" intermittently.
DEV-9546	Airwall Gateways, Airwall Gateways 150	The Airwall Gateway-150 serial connection has an intermittent issue when large amounts of data are sent over the console.

Release Notes 2.2.13

Release Date: Jul 30, 2021

Update Considerations

Update to v2.2.13 if you want to use Advantech ICR-32xx model routers as Airwall Gateways.

You want to use any of the following features:	**You were impacted by any issues discovered in prior releases, especially if you have any of the following**:
•	Ran into these issues:

Downloads

For firmware and software downloads for this version, see 2.2.13 firmware and software on page 529.

What's New in 2.2.13

Here are the new features and enhancements in this version.

New and Improved Conductor Features

Port mirroring

Airwall Gateways configured with port mirroring now show mirrored status in list and status views.

DEV-15399

OpenID Connect

OpenID Connect tokens are now included in the webapp log at the debug level to assist with integration.

User Preferences

The Conductor now remembers user page size settings across sessions, browsers, and computers.

Underlay Network view

This view now visually separates the different underlay IPs to show their ping statuses, RTT, and count as they are being pinged.

Device name now shown on Overlay and Device pages

If you set a name for a device in an Airwall Agent or Server, it is now shown on the **Overlays** and **Devices** pages in the Conductor.

CPU Graph Changes

Starting with 2.2.12, the CPU graph on an Airwall Gateway Reporting page now shows CPU percentage, not the previously-shown CPU load average. The CPU percentage graph shows the percentage of CPU capacity being used on the Airwall Gateway over time.

New and Updated Help

In addition to the content added for new features linked above, here's the new and updated content published since our last major release:

New –

- Diagrams for Port Mirroring
- Virtual Airwall Edge Services

Updated –

- How Airwall Licensing Works on page 191
- Set up a virtual Airwall Gateway in VMware ESX/ESXi on page 306
- Set up a virtual Airwall Gateway in Microsoft Hyper-V on page 308
- Alibaba Cloud – Set up an Airwall Gateway on page 315
- Amazon Web Services – Set up an Airwall Gateway on page 320
- Microsoft Azure – Set up an Airwall Gateway on page 324
- Google Cloud (GCP) – Set up an Airwall Gateway on page 334
- Airwall Gateway Airshell Console Commands - airsh - New `conf model` command
- Mirror Traffic to a Dedicated Port

Fixes

ID	Applies to	Description
DEV-15984	Cellular Airwall Gateways	Fixed an issue that could block bypass traffic on cellular ports.
DEV-15948	Airwall Gateways	Fixed a DNS resolver issue that could cause long delays for Airwall Edge Services trying to reconnect to the Conductor that is configured with a hostname.

ID	Applies to	Description
DEV-15880	Conductors	When you replace an Airwall Gateway, the Conductor now replaces port configurations of different Airwall Gateway models.
DEV-15839	Airwall Gateways	Fixed an issue that could impact overlay device connectivity.

Known Issues

ID	Applies to	Description
DEV-15987	Cellular Airwall Gateways	Using the "Check Bandwidth" function on the Secure Tunnels tab may cause the Advantech Airwall Gateway to lose access to its cell modem until a reboot.
DEV-15982	Conductors	Traffic stats reporting graphs generally show a smooth curve between data points. Over time the graph can show up with sharper angles. The data is still correct, but this is a known cosmetic issue.
DEV-15808	Google Cloud Airwall Gateways	In Google Cloud, use a unique deployment name (vm name) for Airwall Gateways. Airwall Gateways with the same vm name will have the same device serial number and this can result in a failure when you make a license request.
DEV-15791	Airwall Gateways	On the Airwall Gateway-100, Port 2 might be inactive after a factory-reset. **Workaround** – Manually reboot the Airwall Gateway after a factory-reset.
DEV-15787	OSX Airwall Agents	Attempting to create a profile from the Remote Access User portal via the Request to connect to Conductor when a profile with that Conductor already exists will fail. **Workaround** -- Use an invite code or enter Conductor information manually.
DEV-15705	Android and iOS Airwall Agents	Establishing a tunnel TO a mobile agent (iOS / Android) will fail when there is no Airwall Relay involved. **Workaround** – Establish the tunnel FROM the mobile agent.
DEV-15572	Airwall Gateways	Not specifying a gateway in DHCP server config causes the Airwall DHCP server to not include the DHCP Router option, so the DHCP client cannot configure a default gateway. Not specifying a gateway is an unusual config, and should only be used when you want to configure a single isolated subnet. For example, a subnet for networked PDUs that should not have any outside connectivity aside from remote access through an Airwall Gateway used in conjunction with SNAT over the overlay port group.
DEV-15489	Windows Airwall Agents and Servers	Windows 7 Users will see an extra Windows system popup when the UserAuth prompt appears on screen. This message can be safely ignored or the service can be disabled.

ID	Applies to	Description
DEV-15381	Conductors	Sometimes, an Airwall Agent is not added to a Smart Device Group because the editor of the Smart Device Group rule does not have permissions to edit the Airwall Agent. This issue can happen, for example, when you add a tag to an Airwall Agent after it has been added to a single overlay network that the person who edited the rule is not a manager of. To avoid this issue, add tags relating to Smart Device Group actions to Airwall Agents and devices before adding them directly to any overlays.
DEV-15357	macOS Airwall Agents	If you update the macOS Airwall Agent to a release later than v2.2.11 on macOS Mojave using a Conductor-based update package, it may not report the updated version to the Conductor. **Workaround** – Restart the agent or reapply the update.
DEV-15302	macOS Airwall Agents	The macOS Airwall Agent profile will not work correctly when restored to a new machine via Timemachine. **Workaround** – Create a new profile on the Airwall Agent, and then on the Conductor, replace the old profile with the new one for that agent.
DEV-15219	MAP2-Client, OpenHIP	Airwall Gateways are not working on the Bell Mobility (Canada) cellular provider, due to the required use of a http/https proxy.
DEV-15031	Airwall Gateways	Remote syslog over TLS doesn't work when using keys stored in TPM.
DEV-14860	Conductors	Airwall Gateways on older firmware (pre 2.2.0) may send passively discovered device events to the Conductor even when the feature is off.
DEV-14835	Conductors	Airwall Gateway-150 serial numbers look like exponentiated numbers to Excel, so the column displaying the Serial number shows xxxEyyy instead of the full serial number.
DEV-14798	Conductors, Airwall Agents	Airwall Gateways with negative policy will still be able to talk to each other via their LSI. The peer will also still show up in the UI.
DEV-14772	macOS Airwall Agents	If the macOS Airwall Agent is set to "off on boot" and the computer is rebooted, DNS may not be correctly set at startup. **Workaround** – Restart the agent to regain access to DNS. Stop the agent, if desired, to return to the DNS servers as given by DHCP.
DEV-14739	Airwall Gateways	If you set IPv4 to DHCPv4 and set a static IP address for IPv6, the setting that you set second doesn't get saved. **Workaround** – If you need both IPv4 and IPv6, set static IP addresses for both.

ID	Applies to	Description
DEV-14736	Cellular Airwall Gateways	Cellular details may display as "unavailable" on the first boot after you update an Airwall Gateway. The cellular connections are not affected. **Workaround** – Reboot the Airwall Gateway again to correctly display the cellular details.
DEV-14726	Conductor	If you're viewing an Android Airwall Gateway **Ports** tab and the Airwall Agent changes how it is connected to the Conductor (for example, from WiFi to cellular), the display doesn't update correctly. **Workaround** – Refresh the page.
DEV-14715	macOS Airwall Agents	Big Sur ARM64 Macs are not supported in this release
DEV-14610	Conductor	After changing the Reporting traffic stats reporting time, the CPU graph will not display. **Workaround** – Refresh your browser page.
DEV-14584	Cellular Airwall Gateways	Hot-swapping the SIM on an Airwall Gateway 110 with firmware version 2.2.11 may not work. **Workaround** – Reboot the Airwall Gateway after installing a new SIM card.
DEV-14570	Conductors	If you set an Airwall Agent owner to a user (LDAP, local, or OIDC) and someone attempts to user authenticate with a different OIDC user, they will not be able to authenticate (which is the correct behavior), but they see a 500 instead of a helpful error message.
DEV-14551	Conductors	The Android Airwall Agent lets you press the **Edit Settings** button on the **Ports** page; however, submitting any changes to the page results in an error message.
DEV-14426	Conductors, Airwall Gateways	Bypass destinations with a hostname do not show device activity in the Conductor.
DEV-14361	Airwall Gateways	The **Build new tunnels if none exist** option doesn't build tunnels to peer Airwall Edge Services with IPv6-only policy. This feature currently depends on having IPv4 policy between peer Airwall Edge Services.
DEV-14308	OpenHIP	Initial packets dropped while building a new tunnel to a new peer Airwall Edge Service.
DEV-14249	iOS Airwall Agents	**Check Secure Tunnels** / **Tunnel Status** may show as unavailable on iOS. **Workaround** – You can determine tunnel status by checking packets sent or received.
DEV-14223	Cloud-Google	Add an overlay IP to agent to talk to device behind Google Cloud Airwall Gateway 300v.

ID	Applies to	Description
DEV-14218	Airwall Gateways	NAT broadcast applied to traffic between ports within a single port group. Use an external switch if you need to connect multiple devices to a single port group and use the NAT broadcast feature and require IP broadcast un-NATed between those local devices.
DEV-14045	Android and iOS Airwall Agents	iOS does not currently support overlay ping. This feature may be implemented in a future release.
DEV-14015	OpenHIP	If a relay is also used as a bypass gateway, Airwall Edge Services behind the relay are not able to use that relay. **Workaround** – Deploy multiple relays so at least one relay is usable by each pair of Airwall Edge Services that need to communicate.
DEV-13760	Conductors	Device export/import does not export or import Bypass Devices.
DEV-13754	Airwall Agents and Servers	The Conductor can falsely report that the Airwall Agent is offline in some cases.
DEV-13699	Windows Airwall Agents and Servers	The initial ping from the Windows Airwall Agent can be misleading since it currently includes the time to initially set up the connection. **Workaround** – Ping a second time to see actual ping time.
DEV-13650	Conductors	SoIP device activity is not being reported on an Airwall Gateway **Local Devices** tab.
DEV-13640	Conductors	Airwall Relay diagnostics doesn't work on a Standby Conductor.
DEV-13633	Conductors	A standby Conductor shows available firmware downloads, but cannot be downloaded. **Workaround** – Download firmware from the active Conductor.
DEV-13620	Conductors	In **Airwall** > **Ports** > **Failover settings**, the failover ping occurs only every "ping rate" + "ping timeout" seconds, somewhat unexpectedly.
DEV-13607	Conductors, Airwall Gateways	Creating a link failover group (**Airwall** > **Ports** > **Failover settings**) does not apply the settings to any port groups. This is easy to miss since you have to set the failover group on the ports page.
DEV-13588	Conductors	Opening the Conductor on Internet Explorer 11 can be very slow for medium to large deployments. **Workaround** – Use the latest version of Chrome, Firefox, or Edge instead.
DEV-13544	Linux Airwall Servers	If no relay is configured, checking Relay probe information on the Linux Airwall Server returns an error.

ID	Applies to	Description
DEV-13536	Windows Airwall Agents and Servers	Uninstalling the Windows Airwall Agent does not remove the tun-tap driver. **Workaround** – Delete the driver from C:\Windows \System32\drivers\tnw-tap.sys.
DEV-13531	Cloud	Automating creating Cloud HA Conductors only works with same cloud provider used for both active and standby. For example, having both your HA Active and HA Standby Conductors in AWS. **Workaround** -- You can manually set up different cloud providers as HA pair Conductors.
DEV-13474	Airwall Gateways	Configuring multiple overlay port groups with the same overlay IP subnet (same or different IP addresses) and then creating a local device equal to the entire subnet with port affinity set may not lead to the expected result.
DEV-13331	Cloud-Alibaba	Alibaba Cloud Conductor system time is incorrect. **Workaround** – Change the Conductor system time to browser time: **1.** In Conductor **Settings**, under **System time**, select **Edit settings**. **2.** Select **Set browser time**, and then select **Update**.
DEV-13195	Conductors, Airwall Gateways	When you upgrade a Cellular Airwall Gateway-150 from 2.2.3 to 2.2.5, the cellular details all become unavailable. **Workaround** – Reboot and the details return.
DEV-13194	Conductors	Check Connectivity / Ping Local Devices on an Airwall Gateway will fail in Internet Explorer 11 if one of the devices is defined as a CIDR. **Workaround** – use one of the latest versions of Chrome, Firefox, Safari or Edge.

ID	Applies to	Description
DEV-12852	Windows Airwall Agents and Servers	Windows by default doesn't allow multiple 'active' interfaces. It prefers ethernet over cellular whenever possible. **Workaround** – Set Windows to keep multiple interfaces open by editing the **fMinimizeConnections** registry value: **1.** Hold the Windows key and press **R**. **2.** In the **Run** dialog, type `regedit` and click **OK**. **3.** Navigate to the following path in Registry Editor: HKEY_LOCAL_MACHINE\SOFTWARE\Policies \Microsoft\Windows\WcmSvc\ **4.** See if the **GroupPolicy** subkey exists. If not with, **WcmSvc** highlighted, right-click on **WcmSvc** and select **New** > **Key**, and name it `GroupPolicy`. **5.** Right-click **GroupPolicy** and select **New** > **DWORD(32-bit)** > **Create value**. **6.** Name the value `fMinimizeConnections`, and select **OK**. **7.** Set the value to 0 (false). **8.** Save, reboot, and test.
DEV-11710	macOS Airwall Agents	If you change the LSI prefix on the Conductor, the macOS Airwall Agent doesn't update the routes correctly. **Workaround** – Close and reopen the macOS Airwall Agent.
DEV-10590	Cloud	The Conductor does not display an error when adding a route that would exceed the maximum number of allowed routes in the cloud provider.
DEV-10039	Airwall Gateways	An Airwall Gateway-150 can show a "Could not detect attached switch" message intermittently.
DEV-9546	Airwall Gateways, Airwall Gateway-150	The Airwall Gateway-150 serial connection has an intermittent issue when large amounts of data are sent over the console.
DEV-9429	Windows Airwall Agents and Servers	Updating the Overlay Device IP address for a Windows Airwall Server in the Conductor doesn't update the first time. **Workaround** – Open and update the address a second time.

Release Notes 2.2.12 Hotfix – Conductor HF-15849

Release Date: Jun 17, 2021

This is a hotfix to release v2.2.12 for Conductors. See Release Notes 2.2.12 on page 628 for more additions in this versions. Download 2.2.12 Conductor HF-1 from Hotfixes on page 548.

Update Considerations

Update to this v2.2.12 Conductor hotfix if you:

- .

Fixes

ID	Applies to	Description
DEV-	Conductor	

Known Issues

See Release Notes 2.2.12 on page 628 for known issues.

Release Notes 2.2.12 Hotfix – Conductor HF-15748

Release Date: May 28, 2021

This is a hotfix to release v2.2.12 for Conductors. See Release Notes 2.2.12 on page 628 for more additions in this versions. Download 2.2.12 Conductor HF-15748 from Hotfixes on page 548.

Update Considerations

Update to this v2.2.12 Conductor hotfix if you:

- Replace the port configuration of different Airwall Gateways.

Fixes

ID	Applies to	Description
DEV-15748	Conductor	Hotfix that allows replacing port configuration of different Airwall Gateways.

Known Issues

See Release Notes 2.2.12 on page 628 for known issues.

Release Notes 2.2.12

Release Date: May 24, 2021

Update Considerations

Important: Update downtime – When you update the Conductor or Airwall Edge Services, there may be database and configuration changes related to the new release that require Airwall Edge Services to update their configuration data, resulting in downtime while secure tunnels are re-established. Downtime is typically up to, and in most cases is much less than, two minutes.

Consider updating to v2.2.12 if:

You want to use any of the following features:	**You were impacted by any issues discovered in prior releases, especially if you have any of the following**:
• Use a Raspberry Pi as an Airwall Server • Plan on installing an 8-port module in an already in production Airwall Gateway-500	Ran into these issues: • Had issues with reconnecting previously revoked devices • Issues with Bypass in certain cases • Issues with port mirroring after deleting a destination • Have issues with Bypass and Device Discovery

Downloads

For firmware and software downloads for this version, see 2.2.12 firmware and software on page 530.

What's New in 2.2.12

Here are the new features and enhancements in this version.

Licensing Changes

- Port mirroring now requires an add-on license for any Airwall Gateway acting as a Mirror Source
- Licensing page changes:
  - Licenses are now paginated as needed.
  - Vouchers are automatically consolidated

Airwall Servers for Raspbian and Ubuntu ARM64

You can now get an Airwall Server that runs on Raspbian or Ubuntu ARM. For installation information, see Raspbian and RPi4/Ubuntu ARM64 – Install the Airwall Server on page 12.

Platform End of Life for 100 Series Appliances

Tempered announces the End of Life schedule for the HIPswitch 100 series platforms. For more information and a schedule, see Platform end-of-life for Airwall Gateway/ HIPswitch 100 series on page 505.

New and Improved Conductor Features

Port mirroring	Airwall Gateways configured with port mirroring now show mirrored status in list and status views. DEV-15399
OpenID Connect	OpenID Connect tokens are now included in the webapp log at the debug level to assist with integration.
User Preferences	The Conductor now remembers user page size settings across sessions, browsers, and computers.
Underlay Network view	This view now visually separates the different underlay IPs to show their ping statuses, RTT, and count as they are being pinged.
Device name now shown on Overlay and Device pages	If you set a name for a device in an Airwall Agent or Server, it is now shown on the **Overlays** and **Devices** pages in the Conductor.
CPU Graph Changes	Starting with 2.2.12, the CPU graph on an Airwall Gateway Reporting page now shows CPU percentage, not the previously-shown CPU load average. The CPU percentage graph shows the percentage of CPU capacity being used on the Airwall Gateway over time.

New and Updated Help

In addition to the content added for new features linked above, here's the new and updated content published since our last major release:

New –

- Diagrams for Port Mirroring
- Virtual Airwall Edge Services

Updated –

- How Airwall Licensing Works on page 191
- Set up a virtual Airwall Gateway in VMware ESX/ESXi on page 306
- Set up a virtual Airwall Gateway in Microsoft Hyper-V on page 308
- Alibaba Cloud – Set up an Airwall Gateway on page 315
- Amazon Web Services – Set up an Airwall Gateway on page 320
- Microsoft Azure – Set up an Airwall Gateway on page 324
- Google Cloud (GCP) – Set up an Airwall Gateway on page 334
- Airwall Gateway Airshell Console Commands - airsh - New `conf model` command
- Mirror Traffic to a Dedicated Port

Fixes

ID	Applies to	Description
DEV-16133	Windows Airwall Agents and Servers	Fixed an issue where Windows Airwall Agents and Servers sometimes lock up.
DEV-16101	Windows Airwall Agents and Servers	Fixed an issue where a Windows Airwall Agent or Server loses connectivity with the Conductor, or where the agent is still connected but cannot establish communications.
DEV-15680	Airwall Gateways	The Airwall Gateway CPU Load graph has been revised for Airwall Gateways running v2.2.12 and later. This graph now reports the percentage of CPU used rather than the load average reported by previous releases.
DEV-15635	Conductors	Fixed an issue where read-only system administrators were prevented from seeing license counts.
DEV-15579	Conductors	Fixed an issue where an incorrect packet capture interface may get selected when using Firefox browser.
DEV-15563	Conductors	Fixed an issue where the GRE key field wasn't being published for port mirror destinations.
DEV-15543	Conductors	Fixed an issue where group validation fails if there is a comma in the group name.
DEV-15541	macOS Airwall Agents	Fixed an issue where the macOS Airwall Agent wasn't cleaning up routes when shut down.
DEV-15538	Conductors	Fixed an issue where you could not add a device group with bypass destinations to an overlay.
DEV-15503	Airwall Gateways	Fixed an issue where Airwall Gateways were not always broadcasting all their monitor capabilities.
DEV-15467	Conductors	Swapping between Airwall Gateways should correctly reset the owner setting
DEV-15448	API, Conductors	API for port mirrors incorrectly used enumerable ID. It now uses a UUID.
DEV-15444	Conductors	Fixed an issue that could cause the Conductor to refuse policy creation involving bypass destinations in some situations.
DEV-15385	Airwall Gateways	Fixed an issue that could cause bad port and network configurations on Airwall Gateways with port expansion capabilities after inserting a network expansion module.

ID	Applies to	Description
DEV-15378	Airwall Gateways	Fixed an issue where you had to remove the Port Mirroring config before deleting a device.
DEV-15374	Android and iOS Airwall Agents	Airwall Agents now automatically restart when the port for HIP is changed on Conductor.
DEV-15370	Airwall Gateways	Fixed passive device discovery on routed traffic only port groups.
DEV-15367	Conductors	The user is now blocked from completing user auth if they are within a negative access window on any people group.
DEV-15360	Airwall Gateways	Fixed an issue where the port 1 and 2 labels were swapped on an AW-100 after it has been factory reset.
DEV-15352	Conductors	Fixed a UI issue that prevented changes to bypass settings on a standby Conductor.
DEV-15348	Conductors	The ping peer **Airwalls** diagnostic function in the UI should now enable/disable dynamically as the Airwall gains or loses peers.
DEV-15341	Airwall Gateways	Fixed an ebm2 crash on a rare race condition encountered when updating ports configuration when port mirroring is enabled.
DEV-15316	Airwall Gateways	Fixed an issue that caused **Ping peer Airwalls** to report a failure sending HIP traffic for HA-configured Airwall Gateways.
DEV-15314	Conductors	Fixed an issue where when using user auth tags and access windows, a user logging in could gain transient (< 5 minutes) access to a tag when they are outside the access window, and therefore gain access to a resource via smart device groups when they should not.Also fixed an issue where when a user gains a user auth tag that is in multiple people groups with access windows, the user might only gain access for the shorter window depending on group ordering.
DEV-15305	Conductors	The Conductor now validates the local device MAC address is a unicast address.
DEV-15179	HIP tunnel, Diagnostic mode	Fixed an issue where 'airsh conf cell roaming=1' did not match Diagnostic Mode settings. New syntax is 'airsh conf cell roaming=true' (or '... roaming=false').
DEV-15005	Conductors, Android Airwall Agents	Fixed an issue where overlay stats were not showing on the Android Airwall Agent.
DEV-14994	Android Airwall Agents	Fixed an issue where the cell port temporarily didn't show up on the **Ports** page in Conductor for an Android Airwall Agent.
DEV-14990	Airwall Gateways	Fixed an issue where bypass policy was applied to outbound but not inbound traffic.
DEV-14952	Airwall Agents and Servers	Fixed an issue where the Android Airwall Agent was not able to ping peer devices on Airwall Teams unless the communication was initiated from the peer devices.
DEV-14917	Android Airwall Agents	Fixed an issue where you couldn't stop the packet capture for Android Airwall Agents.

ID	Applies to	Description
DEV-14874	Android Airwall Agents	Fixed an issue where the Android Airwall Agent was reporting the underlay IP as 0.0.0.0 when on cellular.
DEV-14816	Conductors, Android and iOS Airwall Agents	The UI for the mobile agents need to be in either the background or foreground for the change to take effect without user interaction.
DEV-14806	Android Airwall Agents	Fixed an issue where Android 6 & 7 devices were unable to ping peer device without an Overlay device IP set.
DEV-14800	Android Airwall Agents	If an Android has multiple underlay IP addresses (like IPv4 and IPv6), the Conductor now pings them separately.
DEV-14795	Android Airwall Agents	Reduced the timeout length for **Check secure tunnel** on the Conductor for Android Airwall Agents.
DEV-14794	Android Airwall Agents	Fixed an issue where **Check secure tunnel** on the Conductor was not working on older Android devices.
DEV-14771	Android Airwall Agents	Note that if you scroll to the top while the log viewer is scrolling it will not force you to the bottom. It will only auto-scroll if you are scrolled to the last line and new log messages come in, which is how most auto-scrolling works.
DEV-14758	Conductors, Android Airwall Agents	Fixed an issue where the Conductor was sometimes not showing an IP for Android Airwall Agents.
DEV-14683	Airwall Gateways	Fixed an issue causing missing ports in the selection drop-down of the packet capture dialog of newly managed Airwall Edge Services.
DEV-14509	Airwall Gateways	**Ping peer Airwalls** (under Diagnostics > Check connectivity > Airwall peer connectivity) was fixed for Airwall Gateways and Linux Airwall Servers. Note that the other Airwall Agents and Servers (Windows, macOS, iOS, Android) may display a green checkboxes under HIP traffic when a HIP tunnel may not actually be available (false positives).

Known Issues

ID	Applies to	Description
DEV-16107	Windows Airwall Agents and Servers	There is an issue on Windows Airwall Agents and Servers where when you set the log level, the agent loses its connection to the Conductor, and no longer writes anything to the log. **Workaround**: Change the log level again, or close and restart the Airwall Agent or Server.
DEV-15808	Google Cloud Airwall Gateways	In Google Cloud, use a unique deployment name (vm name) for Airwall Gateways. Airwall Gateways with the same vm name will have the same device serial number and this can result in a failure when you make a license request.

ID	Applies to	Description
DEV-15803	Conductors	When you replace an Airwall Gateway in the Conductor, it transfers the **Underlay IP (NAT)** during the **Transfer port configuration** step, even if you have not checked **Transfer public IP addresses**. **Workaround** – Update the **Underlay IP (NAT)** after completing the Airwall replace.
DEV-15791	Airwall Gateways	On the Airwall Gateway-100, Port 2 might be inactive after a factory-reset. **Workaround** – Manually reboot the Airwall Gateway after a factory-reset.
DEV-15705	Android and iOS Airwall Agents	Establishing a tunnel TO a mobile agent (iOS / Android) will fail when there is no Airwall Relay involved. **Workaround** – Establish the tunnel FROM the mobile agent.
DEV-15489	Windows Airwall Agents and Servers	Windows 7 Users will see an extra Windows system popup when the UserAuth prompt appears on screen. This message can be safely ignored or the service can be disabled.
DEV-15357	macOS Airwall Agents	If you update the macOS Airwall Agent to a release later than v2.2.11 on macOS Mojave using a Conductor-based update package, it may not report the updated version to the Conductor. **Workaround** – Restart the agent or reapply the update.
DEV-15302	macOS Airwall Agents	The macOS Airwall Agent profile will not work correctly when restored to a new machine via Timemachine. **Workaround** – Create a new profile on the Airwall Agent, and then on the Conductor, replace the old profile with the new one for that agent.
DEV-15219	MAP2-Client, OpenHIP	Airwall Gateways are not working on the Bell Mobility (Canada) cellular provider, due to the required use of a http/https proxy.
DEV-15031	Airwall Gateways	Remote syslog over TLS doesn't work when using keys stored in TPM.
DEV-14892	Android Airwall Agents	Network order for Ethernet connections on an Android Airwall Agent doesn't work.
DEV-14835	Conductors	Airwall Gateway-150 serial numbers look like exponentiated numbers to Excel, so the column displaying the Serial number shows xxxEyyy instead of the full serial number.
DEV-14798	Conductors, Airwall Agents	Airwall Gateways with negative policy will still be able to talk to each other via their LSI. The peer will also still show up in the UI.

ID	Applies to	Description
DEV-14772	macOS Airwall Agents	If the macOS Airwall Agent is set to "off on boot" and the computer is rebooted, DNS may not be correctly set at startup. **Workaround** – Restart the agent to regain access to DNS. Stop the agent, if desired, to return to the DNS servers as given by DHCP.
DEV-14739	Airwall Gateways	If you set IPv4 to DHCPv4 and set a static IP address for IPv6, the setting that you set second doesn't get saved. **Workaround** – If you need both IPv4 and IPv6, set static IP addresses for both.
DEV-14736	Cellular Airwall Gateways	Cellular details may display as "unavailable" on the first boot after you update an Airwall Gateway. The cellular connections are not affected. **Workaround** – Reboot the Airwall Gateway again to correctly display the cellular details.
DEV-14726	Conductor	If you're viewing an Android Airwall Gateway **Ports** tab and the Airwall Agent changes how it is connected to the Conductor (for example, from WiFi to cellular), the display doesn't update correctly. **Workaround** – Refresh the page.
DEV-14715	macOS Airwall Agents	Big Sur ARM64 Macs are not supported in this release
DEV-14610	Conductor	After changing the Reporting traffic stats reporting time, the CPU graph will not display. **Workaround** – Refresh your browser page.
DEV-14584	Cellular Airwall Gateways	Hot-swapping the SIM on an Airwall Gateway 110 with firmware version 2.2.11 may not work. **Workaround** – Reboot the Airwall Gateway after installing a new SIM card.
DEV-14570	Conductors	If you set an Airwall Agent owner to a user (LDAP, local, or OIDC) and someone attempts to user authenticate with a different OIDC user, they will not be able to authenticate (which is the correct behavior), but they see a 500 instead of a helpful error message.
DEV-14551	Conductors	The Android Airwall Agent lets you press the **Edit Settings** button on the **Ports** page; however, submitting any changes to the page results in an error message.
DEV-14426	Conductors, Airwall Gateways	Bypass destinations with a hostname do not show device activity in the Conductor.
DEV-14361	Airwall Gateways	The **Build new tunnels if none exist** option doesn't build tunnels to peer Airwall Edge Services with IPv6-only policy. This feature currently depends on having IPv4 policy between peer Airwall Edge Services.
DEV-14308	OpenHIP	Initial packets dropped while building a new tunnel to a new peer Airwall Edge Service.

ID	Applies to	Description
DEV-14249	iOS Airwall Agents	**Check Secure Tunnels** / **Tunnel Status** may show as unavailable on iOS. **Workaround** – You can determine tunnel status by checking packets sent or received.
DEV-14223	Cloud-Google	Add an overlay IP to agent to talk to device behind Google Cloud Airwall Gateway 300v.
DEV-14218	Airwall Gateways	NAT broadcast applied to traffic between ports within a single port group. Use an external switch if you need to connect multiple devices to a single port group and use the NAT broadcast feature and require IP broadcast un-NATed between those local devices.
DEV-14045	Android and iOS Airwall Agents	iOS does not currently support overlay ping. This feature may be implemented in a future release.
DEV-14015	OpenHIP	If a relay is also used as a bypass gateway, Airwall Edge Services behind the relay are not able to use that relay. **Workaround** – Deploy multiple relays so at least one relay is usable by each pair of Airwall Edge Services that need to communicate.
DEV-13970	Cloud-Alibaba, Conductors	When you upgrade a Conductor on Alibaba Cloud, the Conductor system time gets out of sync. **Workaround** – Go to **Settings** > **Other settings** > **System time and date**, click **Edit Settings**, then **Update** to resync.
DEV-13775	Cloud-Azure	The Conductor might rarely give a "Net::ReadTimeout" error when you try to deploy an Azure Airwall Gateway 300v or server. This error doesn't indicate that the deployment has failed. If you get this error message, go to Azure portal and check the actual deployment result.
DEV-13760	Conductors	Device export/import does not export or import Bypass Devices.
DEV-13754	Airwall Agents and Servers	The Conductor can falsely report that the Airwall Agent is offline in some cases.
DEV-13699	Windows Airwall Agents and Servers	The initial ping from the Windows Airwall Agent can be misleading since it currently includes the time to initially set up the connection. **Workaround** – Ping a second time to see actual ping time.
DEV-13650	Conductors	SoIP device activity is not being reported on an Airwall Gateway **Local Devices** tab.
DEV-13640	Conductors	Airwall Relay diagnostics doesn't work on a Standby Conductor.
DEV-13633	Conductors	A standby Conductor shows available firmware downloads, but cannot be downloaded. **Workaround** – Download firmware from the active Conductor.

ID	Applies to	Description
DEV-13620	Conductors	In **Airwall** > **Ports** > **Failover settings**, the failover ping occurs only every "ping rate" + "ping timeout" seconds, somewhat unexpectedly.
DEV-13607	Conductors, Airwall Gateways	Creating a link failover group (**Airwall** > **Ports** > **Failover settings**) does not apply the settings to any port groups. This is easy to miss since you have to set the failover group on the ports page.
DEV-13588	Conductors	Opening the Conductor on Internet Explorer 11 can be very slow for medium to large deployments. **Workaround** – Use the latest version of Chrome, Firefox, or Edge instead.
DEV-13544	Linux Airwall Servers	If no relay is configured, checking Relay probe information on the Linux Airwall Server returns an error.
DEV-13536	Windows Airwall Agents and Servers	Uninstalling the Windows Airwall Agent does not remove the tun-tap driver. **Workaround** – Delete the driver from C:\Windows \System32\drivers\tnw-tap.sys.
DEV-13531	Cloud	Automating creating Cloud HA Conductors only works with same cloud provider used for both active and standby. For example, having both your HA Active and HA Standby Conductors in AWS. **Workaround** -- You can manually set up different cloud providers as HA pair Conductors.
DEV-13474	Airwall Gateways	Configuring multiple overlay port groups with the same overlay IP subnet (same or different IP addresses) and then creating a local device equal to the entire subnet with port affinity set may not lead to the expected result.
DEV-13331	Cloud-Alibaba	Alibaba Cloud Conductor system time is incorrect. **Workaround** – Change the Conductor system time to browser time: **1.** In Conductor **Settings**, under **System time**, select **Edit settings**. **2.** Select **Set browser time**, and then select **Update**.
DEV-13195	Conductors, Airwall Gateways	When you upgrade a Cellular Airwall Gateway-150 from 2.2.3 to 2.2.5, the cellular details all become unavailable. **Workaround** – Reboot and the details return.
DEV-13194	Conductors	Check Connectivity / Ping Local Devices on an Airwall Gateway will fail in Internet Explorer 11 if one of the devices is defined as a CIDR. **Workaround** – use one of the latest versions of Chrome, Firefox, Safari or Edge.

ID	Applies to	Description
DEV-12852	Windows Airwall Agents and Servers	Windows by default doesn't allow multiple 'active' interfaces. It prefers ethernet over cellular whenever possible. **Workaround** – Set Windows to keep multiple interfaces open by editing the **fMinimizeConnections** registry value: **1.** Hold the Windows key and press **R**. **2.** In the **Run** dialog, type `regedit` and click **OK**. **3.** Navigate to the following path in Registry Editor: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WcmSvc\ **4.** See if the **GroupPolicy** subkey exists. If not with, **WcmSvc** highlighted, right-click on **WcmSvc** and select **New** > **Key**, and name it `GroupPolicy`. **5.** Right-click **GroupPolicy** and select **New** > **DWORD(32-bit)** > **Create value**. **6.** Name the value `fMinimizeConnections`, and select **OK**. **7.** Set the value to 0 (false). **8.** Save, reboot, and test.
DEV-11710	macOS Airwall Agents	If you change the LSI prefix on the Conductor, the macOS Airwall Agent doesn't update the routes correctly. **Workaround** – Close and reopen the macOS Airwall Agent.
DEV-10590	Cloud	The Conductor does not display an error when adding a route that would exceed the maximum number of allowed routes in the cloud provider.
DEV-10039	Airwall Gateways	An Airwall Gateway-150 can show a "Could not detect attached switch" message intermittently.
DEV-9546	Airwall Gateways, Airwall Gateway-150	The Airwall Gateway-150 serial connection has an intermittent issue when large amounts of data are sent over the console.
DEV-9429	Windows Airwall Agents and Servers	Updating the Overlay Device IP address for a Windows Airwall Server in the Conductor doesn't update the first time. **Workaround** – Open and update the address a second time.

Release Notes 2.2.11 Hotfix – Conductor HF-1

Release Date: Apr 13, 2021

This is a hotfix to release v2.2.11 for Conductors. See Release Notes 2.2.11 on page 639 for more additions in version 2.2.11. Download 2.2.11 Conductor HF-1 from Hotfixes on page 548.

Update Considerations

Update to this 2.2.11 Conductor hotfix if you:

- Want to use device groups for bypass devices
- Want to use GRE keys to disambiguate mirrored traffic
- Have an Airwall Gateway reporting bypass not enabled after enabling
- Cannot select all Airwall Gateways when creating link failover events

Fixes

ID	Applies to	Description
DEV-15577	Conductor	Fixed an issue where a Device Group with more than two DNS Bypass Destinations could not be added to an Overlay Network.
DEV-15564	Conductor	Fixed an issue where the GRE key field wasn't being published for port mirror destinations.
DEV-15552	Conductor	Full OpenID Connect tokens are printed in the webapp log at debug level to make it easier to integrate Conductor with OIDC providers.
DEV-15545	Conductor	LDAP and OpenID Connect groups containing commas are now supported. Commas in group names can now be escaped if used. For example,enter 123\,foo, 456\,bar to match groups 123,foo and 456,bar.
DEV-15542	Conductor	Fixed an issue that could cause the Conductor to reject policies with a bypass destination in some situations.
DEV-15524	Airwall Gateways	Fixed an issue where Airwall Gateways were sometimes not broadcasting all of their monitor capabilities.
DEV-15415	Conductor	If a user is blocked by any Access window in any people group, they are now blocked from completing user auth.
DEV-15380	Conductor	Fixed an issue where deleting a device that is being used as a port mirroring destination could prevent port mirroring config changes on that Airwall Gateway.

Known Issues

See Release Notes 2.2.11 on page 639 for known issues.

Release Notes 2.2.11 Hotfix – Airwall Gateway HF-2

Release Date: Mar 30, 2021

This is a hotfix to release v2.2.11 for Airwall Gateways. See Release Notes 2.2.11 on page 639 for more additions in version 2.2.11. Download HF-2 from Hotfixes on page 548.

Upgrade Considerations

Upgrade to this 2.2.11 Airwall Gateway hotfix if you ran into issues where traffic to bypass destinations did not work as expected.

Fixes

ID	Applies to	Description
DEV-15479	Airwall Gateway	Fixed an issue where devices with policy on an underlay bypass port did not create routes.

Known Issues

See Release Notes 2.2.11 on page 639 for known issues.

Release Notes 2.2.11 Hotfix – Airwall Gateway HF-1

Release Date: Mar 17, 2021

This is a hotfix to release v2.2.11 for Airwall Gateways. See Release Notes 2.2.11 on page 639 for more additions in version 2.2.11. Download HF-1 from Hotfixes on page 548.

Upgrade Considerations

Upgrade to this 2.2.11 Airwall Gateway hotfix if you were experiencing any of the following issues:

- Passive device discovery wasn't working on Routed traffic only port groups.
- Installing an expansion module mixed up ports.
- You had issues when using both Seamless bypass and port mirroring

Fixes

ID	Applies to	Description
DEV-15402	Airwall Gateway	Fixed using bypass and port mirroring port group destination concurrently.
DEV-15392	Airwall Gateway	Fixed passive device discovery on routed traffic only port groups.
DEV-15391	Airwall Gateway	Fixed rare crash when updating ports configuration while port mirroring is enabled.
DEV-15379	Airwall Gateway	Fixed an issue where an Airwall Gateway is unable to synchronize with the Conductor after port mirroring destination device is deleted followed by a reboot of the Airwall Gateway.
DEV-15324	Airwall Gateway	Fixed expansion module detection and issue where ports were mixed up after installing an expansion module.

Known Issues

See Release Notes 2.2.11 on page 639 for known issues.

Release Notes 2.2.11

Release Date: Mar 15, 2021

What's New in 2.2.11

Here are the new features and enhancements in this version.

Mirror network traffic for Packet Analyzers

You can now mirror network traffic to packet analyzer/visibility tools (like Nozomi or Wireshark) to see what's going on in your Airwall secure network.

See more: Mirror traffic from your Airwall Gateways to a packet analyzer tool on page 457

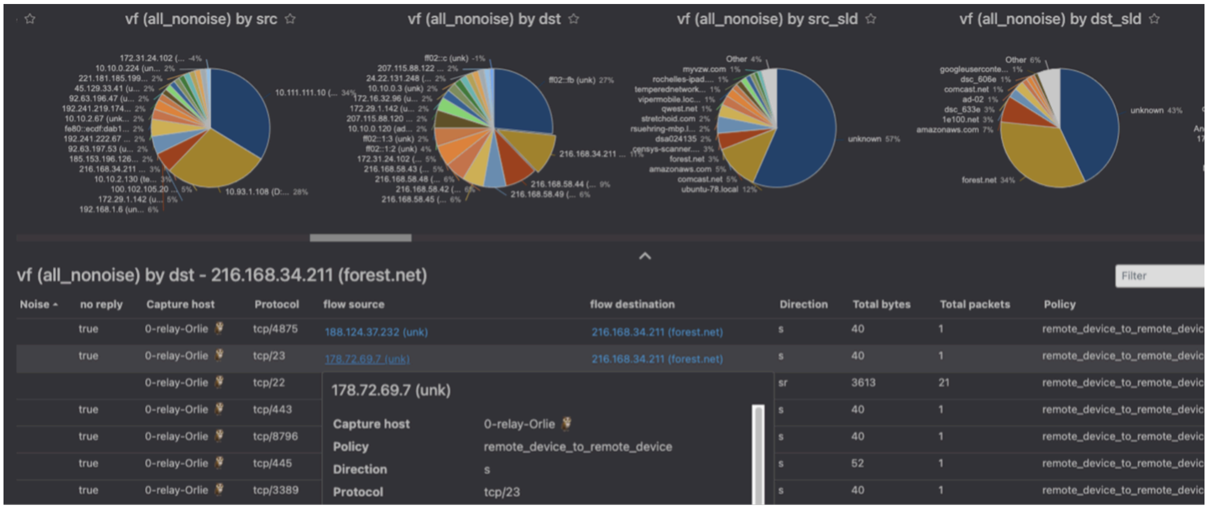
Assign Separate DNS Servers to Airwall Agents and Servers

If you need Airwall Agents and Servers to use different DNS servers, you can assign different DNS servers on an Overlay or individually for Airwall Agents and Servers that support it.

See more: Assign Separate DNS Servers to Airwall Agents and Servers on page 349

Preview - Airwall Visibility Connector

The Airwall Visibility Connector gives you a dynamic L4 view into the health and status of your Airwall secure network. You can explore many pre-computed reports in the Conductor, and can integrate other threat detection platforms. When configured, the Conductor continuously learns from these external systems, and can report or respond to threats as they are detected.



vf (all_nonoise) by dst - 216.168.34.211 (forest.net)

Noise	no reply	Capture host	Protocol	flow source	flow destination	Direction	Total bytes	Total packets	Policy
	true	0-relay-Orlie	tcp/4875	188.124.37.232 (unk)	216.168.34.211 (forest.net)	s	40	1	remote_device_to_remote_devic
	true	0-relay-Orlie	tcp/23	178.72.69.7 (unk)	216.168.34.211 (forest.net)	s	40	1	remote_device_to_remote_devic
		0-relay-Orlie	tcp/22			sr	3613	21	remote_device_to_remote_devic
	true	0-relay-Orlie	tcp/443			s	40	1	remote_device_to_remote_devic
	true	0-relay-Orlie	tcp/8796			s	40	1	remote_device_to_remote_devic
	true	0-relay-Orlie	tcp/445			s	52	1	remote_device_to_remote_devic
	true	0-relay-Orlie	tcp/3389			s	40	1	remote_device_to_remote_devic

178.72.69.7 (unk)

Capture host	0-relay-Orlie
Policy	remote_device_to_remote_device
Direction	s
Protocol	tcp/23

Contact Customer Success at Customer Success if you would like to preview this feature. A future version will expose the full feature with appropriate documentation, training, and platform options.

Raspberry Pi Airwall Agent

You can now get an Airwall Agent that runs on Raspberry Pi. For information, see .

Platform End of Life for 100 Series Appliances

Tempered announces the End of Life schedule for the HIPswitch 100 series platforms. For more information and a schedule, see Platform end-of-life for Airwall Gateway/ HIPswitch 100 series on page 505.

New Knowledge Base and Support Site

Tempered has a new site for our product Knowledge Base articles and support. Update your links!

- New Link to open a Support ticket: https://www.tempered.io/support/supportReq.html

New and Improved Conductor Features

Update macOS Airwall Agents from the Conductor

In v2.2.11, the macOS Airwall Agent introduces the ability to update from a Conductor package. For those running v2.2.10, upgrade one last time manually, with:

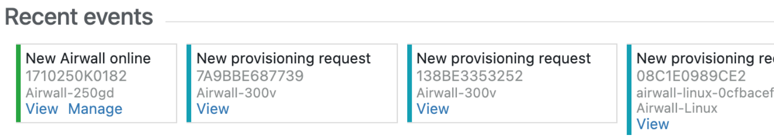
```
sudo installer -pkg /path/to/
Airwall-Mac_2.2.11.xxxx.pkg -
target /
```

You can then update future versions from a Conductor update package.

DEV-14804

Clear Recent events on the Dashboard

On the Dashboard System navigation, you can clear all events by selecting the Dismiss events icon 🔕: DEV-15157



Recent events

New Airwall online
1710250K0182
Airwall-250gd
View Manage

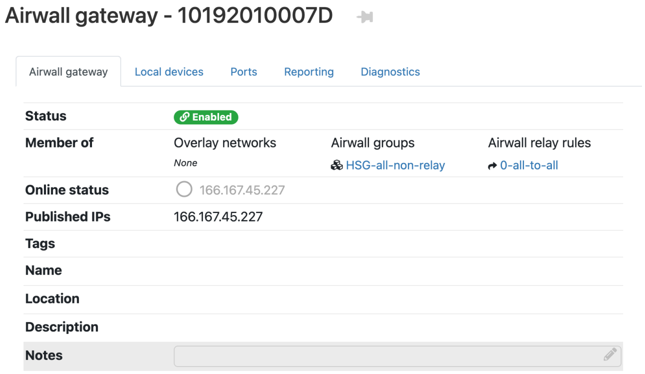
New provisioning request
7A9BBE687739
Airwall-300v
View

New provisioning request
138BE3353252
Airwall-300v
View

New provisioning re
08C1E0989CE2
airwall-linux-0cfbacef
Airwall-Linux
View

New Notes field on Airwall Edge Service pages

There is now a place where administrators can add notes on Airwall Edge Service pages: DEV-15111



Airwall gateway - 10192010007D

Status	Enabled		
Member of	Overlay networks None	Airwall groups HSG-all-non-relay	Airwall relay rules 0-all-to-all
Online status	○ 166.167.45.227		
Published IPs	166.167.45.227		
Tags			
Name			
Location			
Description			
Notes			

Conductor theme now follows you

Your Conductor theme is now saved across computers and browsers. DEV-15022

Failover groups improvement

Failover groups now start with an initial likely selection for underlay link failover configuration. DEV-14900

OpenID Connect improvement

OpenID Connect now supports Azure Active Directory (AD). DEV-14864

Conductor Certificate Expiration reminders

When a Conductor certificate is near expiration (1 month + 1 week), you get an event and a tag on the cert info that warns you of the upcoming expiration. On the day of expiration, you get an alert, event, and a tag telling you the certificate has expired. DEV-15160

Download a CSV with Licensing and Airwall Data

You can download all licensing and Airwall data in CSV format from **Settings** > **Licensing**. This data can be helpful in ensuring your Conductor vouchers are correctly renewed. DEV-14869

Access Windows Date Selection improvements

The way you choose dates for Access windows has been improved. DEV-14649

Airshell Improvements

You can now save your network configuration when doing a factory reset using the keep-networking option. See Airshell (airsh) Command Reference on page 362.

DEV-14465

Alert Improvements

Intrusion prevention alerts now indicate which devices are the source or destination of the alert where possible. These alerts are in Conductor alerts and indicated by the ID in the event data from the API DEV-14502, and snort metadata will be included in the API. DEV-14490

Diagnostic Mode Improvements	• Diagnostic Report Addition – The Diagnostic report now includes policy-based routing rules and IPv6 routes. DEV-14720 • Return to Diag mode after a hotfix – When applying a hotfix that does not require reboot, when the hotfix is complete you get an option to return to Diag mode. DEV-14582
API Improvements	• API tracks when changes happened – The Conductor API now serializes when many resources were created and updated, and includes These changes make it easier to see when resources were added or have changed from the API. DEV-14962 • New API endpoints – New API endpoints show history of Airwall Edge Services being managed and revoked DEV-15113, and returns a list of devices that each device has policy to and what overlays the policies are in DEV-14717. • Date time/NTP settings – The API now allows updating of Date time/NTP settings. DEV-14716

New and Updated Help

In addition to the content added for new features linked above, here's the new and updated content published since our last major release:

New –

- Configure an Underlay Port Failover Group
- Best Practices for Underlay Port Failover Groups

Updated –

- Seamless Bypass

Introducing our new free offering – Airwall Teams

Airwall Teams allows you to build truly private system-to-system networks—that span public, private, cloud, and mobile networks using an intuitive graphical interface - just draw lines between devices you want to connect. Airwall Teams replaces and expands on our Airnet platform.

Update Considerations

Consider updating to v2.2.11 if:

You want to use any of the following features:	You were impacted by any issues discovered in prior releases, especially if you have any of the following:
• Mirror network traffic to a packet analyzer • Assign different DNS servers to Airwall Agents and Servers	Ran into these issues: • **Syslog issues** – User Authentication was logging to Syslog, and external syslog over TLS • Seeing high CPU use from logwatch • **Airwall Invitations** were incorrectly using the US date format

Downloads

For firmware and software downloads for this version, see 2.2.11 firmware and software on page 531.

Fixes

ID	Applies to	Description
DEV-15317	Conductor	When using user authentication access windows, sessions now end at the end of the session timeout of the Airwall Edge Service if it is shorter than the access window.
DEV-15307	Linux Airwall Servers	Fixed some DNS issues in Linux Airwall Servers.
DEV-15265	Airwall Gateway	Fixed an issue where taking a packet capture didn't include hipbrN interfaces in **Routed only** overlay port groups.
DEV-15206	Conductor	When you attempt to disable a user who is the owner of any smart device groups, the Conductor now shows a warning advising you to transfer ownership to avoid their smart device groups being downgraded to regular device groups.
DEV-15152	Conductor	Fixed an issue where there could be unidentified device activity in the log.
DEV-15045	Windows Airwall Agents and Servers	Fixed an issue that caused the Windows Airwall Agents and Servers to close unexpectedly.
DEV-15001	macOS Airwall Agents	Fixed an issue where Okta user authentication was failing when you had assigned DNS servers globally on macOS Airwall Agents.
DEV-14996	macOS Airwall Agents	macOS Airwall Agents now correctly install on Big Sur (version 11.x) without excessive prompts to accept certificates.
DEV-14983	Conductor	When using the device discovered monitor with the tag action, tags are now correctly added to the discovered device, not the Airwall Gateway with the device.
DEV-14981	Linux Airwall Servers	Fixed an issue where occasionally ping results were not returned.
DEV-14980	Linux Airwall Servers	When attempting to connecting to the Conductor, if an error occurs, the Linux Airwall Servers now moves to the next network interface and tries again.
DEV-14976	Common	Fixed remote syslog to a TLS 1.3 endpoint.
DEV-14975	Windows Airwall Agents and Servers	Customers are unable to view Devices in the HIP Networks View portion of Windows Airwall Agents and Servers.
DEV-14972	Conductor	Resolved a display issue in the throughput shown on the Conductor Dashboard where bars would overlap with the legend.
DEV-14971	Cellular Airwall Gateways	Fixed a regression that sometimes caused long wait times when connecting an Airwall Gateway 110g to Verizon.
DEV-14958	Cloud-Azure, Conductor	Saving the Azure Conductor template with a new resource group name now appears correctly when you edit the template again.
DEV-14956	Airwall Gateways	Fixed a crash when using hostname based policy.
DEV-14951	Conductor, Airwall Gateways	Fixed an issue that could cause a database migration to fail on upgrade.

ID	Applies to	Description
DEV-14922	Conductor	Fixed an issue where people groups integration with authentication providers (LDAP or OpenID Connect) could run into problems if there were groups with the same name with different capitalization.
DEV-14893	Windows Airwall Agents and Servers	Fixed an issue where you had to disable lockdown mode on 2.2.10 Windows Airwall Agents and Servers before stopping it for traffic to properly pass.
DEV-14891	Conductor	Read-only administrators can now see e-mail addresses in user settings.
DEV-14888	Conductor	Syslog now includes remote session (login via agent / server) creation, failed attempts, and termination.
DEV-14887	Conductor	Fixed an issue where in some cases a failed OpenID Connect login could result in a 500 error.
DEV-14878	Linux Airwall Servers	Linux Airwall Servers now keep full firmware install logs.
DEV-14875	Cellular Airwall Gateways	Fixed an issue where Airwall Gateway 150s would sometimes experience 100% CPU usage when a remote syslog server was configured.
DEV-14872	Conductor	Fixed an issue where the link to set your password for a new user that is provided by email expired very quickly, and certain password error messages were not being displayed on the reset password page.
DEV-14863	Conductor	Licensing tab is now more clear about when your licenses will expire.
DEV-14854	Conductor	Fixed an issue where the remote access user portal's Linux Airwall Server connection string was missing the activation code.
DEV-14852	Linux Airwall Servers	Fixed a bug that could cause excessive numbers of Airwall interface status updates.
DEV-14848	Airwall Gateways	Fixed an issue that could cause the root file system to fill up with log messages on some virtual platforms.
DEV-14822	Conductor	**Airwall Invitations** now correctly honor local time and date format.
DEV-14820	Android, iOS, macOS, and Linux Airwall Agents and Servers	Airwall Agents and Servers now automatically restart when the port for HIP is changed on Conductor.
DEV-14803	Conductor	Fixed an issue that caused the logging settings for the Conductor to be ignored for the syslog output.
DEV-14766	Airwall Teams, Conductor	The Airwall Invitation API now returns the activation code in its response.
DEV-14725	Conductor	The Overlay network page where you manage devices and device groups now filters bypass destinations under their own heading.

ID	Applies to	Description
DEV-14723	Conductor	On the Detect devices page, the networks under **Network to scan** are now normalized. For example, '192.168.1.0/24' instead of '192.168.1.1/24'
DEV-14722	Conductor	When you delete a device from an overlay network that uses managed relay rules, if the Airwall Edge Service that device was on has no other devices in the overlay, then the Airwall Edge Service is now also removed from the managed relay rule.
DEV-14713	Conductor	The Conductor now correctly displays IPv6 addresses in Bypass settings.
DEV-14692	Airshell	In the new Airshell 'conf network' menu, when editing a port group, it is possible to enter invalid or duplicate interfaces, or interfaces already in use by another port group. When entering interface names, use `status network` output to see current settings and avoid invalid configurations.
DEV-14690	Airshell	The Airshell command, 'conf network', now lists available interfaces when assigning interfaces to a port group.
DEV-14689	Airshell	Fixed an issue where Airshell "conf network" would time out when applying changes, even though settings were saved.
DEV-14688	Cellular Airwall Gateways	The APN setting is now retained when you factory reset an Airwall Gateway 101g, instead of reverting to the default setting of "broadband."
DEV-14687	Cellular Airwall Gateways	Fixed an issue where the selected carrier was not showing up properly in Diag mode.
DEV-14686	Conductor	Fixed a few minor issues that could cause unsupported port group references in configuration data for an overlay DHCP and device port affinity.
DEV-14647	Cellular Airwall Gateways	Added a warning if you tried to select a carrier that wasn't compatible with the firmware installed on the Airwall Gateway 101g.
DEV-14636	Conductor	In people groups, if you add only blocking access windows, users can log in any time that access is not blocked. If you add both open and blocking access windows, then users can only log in during the open windows.
DEV-14629	Conductor	Clarified and fixed updating on Device Activity, Health Data, and Traffic Stats.
DEV-14608	Airwall Gateways	Fixed an issue that could prevent initialization of port groups with VLAN interfaces if the parent port was placed in a disabled port group.
DEV-14586	Conductor	Old tooltips no longer collect at the bottom of the screen
DEV-14577	Airwall Gateways	Fixed an issue where device activity wasn't reporting activity on bypass port groups with Routed only disabled.
DEV-14568	Airshell	Fixed issues with port group numbering when editing port groups in Airshell with 'conf network'.

ID	Applies to	Description
DEV-14560	Airwall Gateways	Setting a 0.0.0.0/0 Bypass and blocking by hostname now correctly blocks the named destinations.
DEV-14557	Conductor, Airwall Gateways	Fixed an issue where some device discovery notifications were missed by Conductor.
DEV-14504	Conductor	Filtering alerts with a search term in the Alerts list now filters incoming alerts as well.
DEV-14429	OpenHIP	HIP is now more responsive to failures.
DEV-14427	Conductor	Fixed an issue where IPv6 DHCP settings sometimes showed IPv4 options after choosing **Select one**.
DEV-14335	Linux Airwall Servers	Fixed an issue that caused file handle leakage on Airwall Servers after running packet captures.
DEV-14264	MAP2-Client	You can now choose whether to replace or augment Airwall Gateway-configured Conductor URLs with those configured on the Conductor.
DEV-14233	Virtual Airwall Gateways	Amazon EC2 Airwall Gateways using ENA network drivers will now start with the second interface disabled instead of defaulting to an overlay port group.
DEV-13951	Conductor	Conductor now provides an error message when attempting to pair with a Conductor that is already in Standby.
DEV-13763	Airwall Gateways	The Airwall Gateway 110 now detects the full 1GB of RAM rather than only 512MB.
DEV-11649	Airwall Gateways	**Ping peer Airwalls** now works for IPv6 peers on Linux-based platforms.

Known Issues

ID	Applies to	Description
New DEV-15302	macOS Airwall Agents	The macOS Airwall Agent profile will not work correctly when restored to a new machine via Timemachine. **Workaround** -- Create a new profile on the Airwall Agent, and then on the Conductor, replace the old profile with the new one for that agent.
DEV-15378 & DEV-15309	Airwall Gateways	Unable to synchronize MAP after deleting port mirroring destination local device. **Workaround** – Add back the device that you just deleted. Then remove the Port Mirroring config before deleting the device.
DEV-15370	Airwall Gateways	Passive device discovery doesn't work on port groups that have **Routed traffic only** checked.

ID	Applies to	Description
DEV-15367	Conductor	If you have two people groups with access windows, one giving a user access and another blocking access during the same time period, the user is allowed to complete user authentication when they should be blocked. **Workaround** – If possible, do not have allow and blocked access windows that overlap.
DEV-15357	macOS Airwall Agents	If you update the macOS Airwall Agent to a release later than v2.2.11 on macOS Mojave using a Conductor-based update package, it may not report the updated version to the Conductor. **Workaround** – Restart the agent or reapply the update.
DEV-15356	Conductor	Customer must "restart metadata cache" on conductor after attempting a replace.
DEV-15305	Conductor	Conductor does not validate the local device MAC address is a unicast address.
DEV-15219	MAP2-Client, OpenHIP	Airwall Gateways are not working on the Bell Mobility (Canada) cellular provider, due to the required use of a http/https proxy. (A major development effort would be required to support this.)
DEV-15031	Airwall Gateways	Remote syslog over TLS doesn't work when using keys stored in TPM
DEV-14957	iOS Airwall Agents	On iOS Airwall Agents, you must have Safari as your default browser to create a profile.
DEV-14835	Conductor	Airwall Gateway 150 serial numbers look like exponentiated numbers to Excel, so the column displaying the Serial number shows xxxEyyy instead of the full serial number.
DEV-14798	Conductor, Airwall Agents and Servers	Airwall Agents and Servers with negative policy will still be able to talk to each other via their LSI. The peer will also still show up in the UI.
DEV-14772	macOS Airwall Agents	If the macOS Airwall Agent is set to "off on boot" and the computer is rebooted, DNS may not be correctly set at startup. **Workaround** – Restart the agent to regain access to DNS. Stop the agent, if desired, to return to the DNS servers as given by DHCP.
DEV-14739	Airwall Gateways	If you set IPv4 to DHCPv4 and set a static IP address for IPv6, the setting that you set second doesn't get saved. **Workaround** – If you need both IPv4 and IPv6, set static IP addresses for both.
DEV-14736	Cellular Airwall Gateways	Cellular details may display as "unavailable" on the first boot after you update an Airwall Gateway. The cellular connections are not affected. **Workaround** – Reboot the Airwall Gateway again to correctly display the cellular details.

ID	Applies to	Description
DEV-14726	Conductor	If you're viewing an Android Airwall Agent **Ports** page and the Airwall Agent changes how it is connected to the Conductor (for example, from WiFi to cellular), the display doesn't update correctly. **Workaround** – Refresh the page.
DEV-14715	macOS Airwall Agents	Big Sur ARM64 Macs are not supported in this release
DEV-14610	Conductor	After changing the Reporting traffic stats reporting time, the CPU graph will not display. **Workaround** – Refresh your browser page.
DEV-14584	Cellular Airwall Gateways	Hot-swapping the SIM on an Airwall Gateway 110 with firmware version 2.2.11 may not work. **Workaround** – Reboot the Airwall Gateway after installing a new SIM card.
DEV-14570	Conductor	If you set an Airwall Agent owner to a user (LDAP, local, or OIDC) and someone attempts to user authenticate with a different OIDC user, they will not be able to authenticate (which is the correct behavior), but they see a 500 instead of a helpful error message.
DEV-14551	Conductor	The Android Airwall Agent lets you press the **Edit Settings** button on the **Ports** page; however, submitting any changes to the page results in an error message.
DEV-14509	Airwall Gateways	In Diagnostics, **Ping peer Airwalls** may return false negatives.
DEV-14426	Conductor, Airwall Gateways	Bypass destinations with a hostname do not show device activity in the Conductor.
DEV-14361	Airwall Gateways	The **Build new tunnels if none exist** option doesn't build tunnels to peer Airwall Edge Services with IPv6-only policy. This feature currently depends on having IPv4 policy between peer Airwall Edge Services.
DEV-14249	iOS Airwall Agents	Check Secure Tunnels / Tunnel Status may show as unavailable on iOS. **Workaround** – You can determine tunnel status by checking packets sent or received.
DEV-13970	Cloud-Alibaba, Conductor	When you upgrade a Conductor on Alibaba Cloud, the Conductor system time gets out of sync. **Workaround** – To resync the time, go to **Settings** > **Other settings** > **System time and date**, select **Edit Settings**, then **Update**.
DEV-13775	Cloud-Azure	The Conductor might rarely give a "Net::ReadTimeout" error when you try to deploy an Azure Airwall Gateway 300v or server. This error doesn't indicate that the deployment has failed. If you get this error message, go to Azure portal and check the actual deployment result.

ID	Applies to	Description
DEV-13760	Conductor	Device export/import does not export or import Bypass Devices.
DEV-13754	Android, Linux, and macOS Airwall Agents and Servers	The Conductor can falsely report that a macOS Airwall Agent is offline in some cases.
DEV-13620	Conductor	In **Airwall** > **Ports** > **Failover settings**, the failover ping occurs only every "ping rate" + "ping timeout" seconds, somewhat unexpectedly.
DEV-13588	Conductor	Opening the Conductor on Internet Explorer 11 can be very slow for medium to large deployments. **Workaround** – Use the latest version of Chrome, Firefox, or Edge instead.
DEV-13544	Linux Airwall Servers	If no relay is configured, checking Relay probe information on the Linux Airwall Servers returns an error.
DEV-13531	Cloud	Automating creating Cloud HA Conductors only works with same cloud provider used for both active and standby. For example, AWS HA Active and AWS HA Standby. **Workaround** – You can manually set up different cloud providers as HA pair Conductors.
DEV-13474	Airwall Gateways	Configuring multiple overlay port groups with the same overlay IP subnet (same or different IP addresses) and then creating a local device equal to the entire subnet with port affinity set may not lead to the expected result.
DEV-13331	Cloud-Alibaba	Alibaba Cloud Conductor system time is incorrect. **Workaround** – Change the Conductor system time to browser time: In Conductor **Settings**, under **System time**, select **Edit settings**, select **Set browser time**, and then select **Update**.
DEV-13195	Conductor, Airwall Gateways	When you upgrade a Cellular Airwall Gateway-150 from 2.2.3 to 2.2.5, the cellular details all become "Unavailable." **Workaround** – Reboot and the details return.

ID	Applies to	Description
DEV-12852	Windows Airwall Agents and Servers	Windows by default doesn't allow multiple 'active' interfaces. It prefers ethernet over cellular whenever possible. **Workaround** – Set Windows to keep multiple interfaces open by editing the fMinimizeConnections registry value: **1.** Hold the Windows Key and Press R. **2.** In the run dialog, type regedit and click OK. **3.** Navigate to the following path in Registry Editor: HKEY_LOCAL_MACHINE\SOFTWARE\Policies \Microsoft\Windows\WcmSvc\4. **4.** See if the GroupPolicy subkey exists. If not with, WcmSvc highlighted, right click on WcmSvc and Choose New > Key and name it GroupPolicy. **5.** Right-click GroupPolicy and choose New > DWORD (32-bit) > Create value. **6.** Name the value "fMinimizeConnections," and select OK. (The value should be 0, or false).Reboot and test.
DEV-11710	macOS Airwall Agents	If you change the LSI prefix on the Conductor, the macOS Airwall Agent doesn't update the routes correctly. **Workaround** – Close and reopen the macOS Airwall Agent.
DEV-10590	Cloud	The Conductor does not display an error when adding a route that would exceed the maximum number of allowed routes in the cloud provider.
DEV-10039	Airwall Gateways	An Airwall Gateway 150 can show "could not detect attached switch" intermittently.
DEV-9546	150 Airwall Gateways	The Airwall Gateway 150 serial connection has an intermittent issue when large amounts of data are sent over the console.
DEV-9429	Windows Airwall Agents and Servers	Updating the Overlay Device IP address for a Windows Airwall Server in the Conductor doesn't update the first time. **Workaround** – Open and update the address a second time.

Release Notes 2.2.10 Hotfix – Airwall Gateway HF-1

Release Date: Dec 16, 2020

This is a hotfix to release v2.2.10 for Airwall Gateways. See Release Notes 2.2.10 on page 652 for more additions in version 2.2.10. Download HF-1 from Hotfixes on page 548. See also Release Notes 2.2.10 Hotfix – Conductor HF-1 on page 651.

Note:

Also install Conductor HF-1, as it fixes some of these issues from the Conductor side. See Release Notes 2.2.10 Hotfix – Conductor HF-1 on page 651.

What’s New

IPv6 Support Added for Seamless Bypass

You can now use IPv6 with Seamless Bypass

See more:

- Set up a secure IPv6 overlay on page 380
- Local Bypass on page 394

Upgrade Considerations

Upgrade to this 2.2.10 hotfix if you were experiencing any of the following issues:

- An Airwall Gateway stops tunneling traffic after a reboot or a link fail-over.
- You want to access IPv6 bypass destinations.

Fixes

ID	Applies to	Description
DEV-14849	Airwall Gateway	Fixed a bug that could cause the root file system to fill up with log messages on some virtual platforms.
DEV-14817	Airwall Gateway	Fixed an issue that prevented using IPv6 with seamless bypass.
DEV-14815	Airwall Gateway	Fixed an issue that could cause Airwall Gateways to lose their policy configuration after reconnecting to the Conductor.
DEV-14814	Airwall Gateway	Include IPv6 policy-based routing rules or routing table in diagnostic report to help troubleshoot IPv6 connectivity issues.

Known Issues

See Release Notes 2.2.10 on page 652 for known issues.

Release Notes 2.2.10 Hotfix – Conductor HF-1

Release Date: Dec 16, 2020

What's New

2.2.10 Conductor Hotfix HF-1	This is a hotfix to release v2.2.10 for the Conductor. See Release Notes 2.2.10 on page 652 for more additions in version 2.2.10. Download HF-1 from Hotfixes on page 548.

Note:

Also install Airwall Gateway HF-1, as it fixes some of these issues from the Airwall Gateway side. See Release Notes 2.2.10 Hotfix – Airwall Gateway HF-1 on page 650.

Upgrade Considerations

Upgrade to this 2.2.10 hotfix if you:

- Ran into issues where an Airwall Gateway stops tunneling traffic after a reboot or link fail-over.
- Want to include in the syslog Agent logon/logoff information.
- Need **Airwall Invitations** to not expire in a short time
- Use localized time that is in dd/mm/yy and not US mm/dd/yy and use invites.

Or you were impacted by any of the other issues fixed in this hotfix.

Fixes

ID	Applies to	Description
DEV-14894	Conductor	The syslog now includes remote session (login via agent / server) creation, failed attempts, and termination.
DEV-14873	Conductor	Fixed an issue where the link to set your password for a new user that is provided by email expires very quickly. The expiration is now set to 2 weeks from the date of the invite. **Workarounds** – Go to the login page and reset your password to generate a new reset password token and then follow instructions in the email you receive. – Have your admin manually set the password. Additional issue that was fixed was an issue where error messages (e.g. from passwords that do not meet the necessary criteria) were not being displayed on the reset password page.
DEV-14870	Conductor	Fixed the OpenID Connect integration so that it works correctly with Azure AD platform.
DEV-14859	Airwall Gateway	Added a notification with the reason why a firmware update failed.
DEV-14846	Conductor	The expiration date in **Airwall Invitations** now displays in localized time formats.
DEV-14832	Conductor	Fixed an issue where revoking an Airwall Edge Service caused a deadlock and service restart on the Conductor.
DEV-14774	Conductor	**Airwall Invitations** created via the API did not include the activation code in the response.
DEV-14765	Conductor	Overlay network dialog to manage devices and device groups now filters bypass destinations under their own heading.
DEV-14763	Conductor	Bulk deleting checked alerts was causing an issue with real time Conductor notifications.

Known Issues

See Release Notes 2.2.10 on page 652 for known issues.

Release Notes 2.2.10

Release Date: Nov 18, 2020

What’s New

Access Windows for authenticated users

Specify or restrict what days and times authenticated users can log in to access resources on your secure network using Access Windows.

See more: Set Times Authenticated Users can Access the Secure Network on page 92

Automatic Relay Rules

Enable all connections in an overlay network to use a group of relays. This provides a less-granular, but simple way to manage relay rules.

See more: Set an Overlay to Automatically Manage Relay Rules on page 354

Airwall Gateway Custom Certificates

By default, Airwall Gateways come with a Tempered factory-installed certificate. You can now add your own custom CA certificate to use for Conductor communication.

See more: Add or Replace a Signed Certificate on an Airwall Gateway for Conductor Communication on page 384

Bulk Configuration of Airwall Gateways

Configure certain settings in bulk for Airwall Gateways or Airwall Gateway groups.

See more: Bulk Configuration of Airwall Edge Services on page 378

Enable DNS for Seamless Bypass

You can now enable DNS to use fully-qualified domain names (FQDN) for bypass destinations.

See more:

- Enable DNS lookup for bypass destinations on page 398
- Local Bypass on page 394

Setup Wizards for configuring Conductors and Airwall Gateways

2.2.10 has added two wizards to help you in deploying an Airwall secure network. The Conductor Deployment Wizard walks you through setting up, licensing, and provisioning a new Conductor, and the new Airshell (`airsh`) command `setup-ui` walks you through the most common Airwall Gateway setup options.

See more:

- Conductor Configuration Wizard Settings on page 197
- Configure an Airwall Gateway with the airsh Setup Wizard on page 274

Airwall Status Indicators

There are new ways to see information and status on the Airwall Edge Services connecting to your Airwall secure network

See more: See Airwall Edge Service Information and Status on page 95

Cloud Improvements

This release includes improvements that make it easier to deploy cloud Conductors and Airwall Gateways, and includes support for AWS GovCloud (see below):

- **ENA and SR-IOV support** – You can now deploy instances with enhanced networking configuration enabled with either ENA or SR-IOV, and see which machine types support or require ENA. Note that machine types marked as ENA may deploy as SR-IOV.
- **Disk IO has been improved** – Cloud deployments now include NVMe (memory) disk options.
- **Cloud HA deployment has been automated** – Simplified deployment for HA, eliminating many of the places where misconfiguration could happen.
- **New Azure cloud image names** – Image names now reflect their use, making it easier to choose the correct image.
- **Additional information as images are created** – More details are included in the status pane as the Conductor creates cloud images.

- **Can now choose resource groups** – You can now choose a new or existing resource group when you create cloud Airwall Gateways and Conductors.

  Note: If you choose an existing resource group, make sure no resource names in the existing resource group conflict with the new Airwall Gateway and Conductor deployment name that you are creating.
- **More information available in the Conductor** – New attributes are shown for cloud Airwall Gateways on the **Diagnostics** tab.

Preliminary IPv6 Support

If you have devices with IPv6 addresses, IPv6 is now supported for Airwall Gateways and Linux Airwall Servers. The control for source NAT is shared for both IPv4 and IPv6. Configurations sourcing NAT IPv4 but not IPv6 are not supported.

Airwall Gatewaysnow support static IPv6 addresses for both the underlay and overlay (some cellular carriers may not support it). You also need to assign a static IPv6 address to the Airwall Gateway.

Since IPv6 only supports routed configurations, you need to assign an IPv6 overlay address to the Airwall Gateway to use IPv6 overlay. L2/subnet extensions are not supported.

See more: Set up a secure IPv6 overlay on page 380

AWS GovCloud Support

Cloud Conductors and Airwall Gateways can be now be deployed in AWS GovCloud. Follow the instructions for deploying in AWS:

- Deploy a Conductor on Amazon Web Services (AWS) on page 205
- Set up Cloud Providers on page 433
- Deploy a cloud Airwall Server on page 355

Exponential Backoff

Added exponential backoff to the Airwall Gateway to/from Conductor management connection to comply with Verizon data retry requirements. This change means it could take up to 3 minutes to reconnect after an extended outage. *(DEV-14648)*

Upgrade Considerations

Consider upgrading to 2.2.10 if:

You want to use any of the following features:	You were impacted by any issues discovered in prior releases, especially if you have any of the following:

• Access windows for authenticated users • Automatic relay rules • Custom certificates for Airwall Gateways • Bulk configuration of Airwall Gateways • Enabling DNS for bypass destinations • Setup wizards for Airwall Gateways or the Conductor • Improved Airwall Status • Cloud deployment improvements • IPv6 support • AWS GovCloud deployment	Ran into the issues where: • Setting an Overlay default gateway breaks connected routes • Invites have incorrect links and configuration issues • Got errors on the Airwall Gateway 110g when running certain `airsh` commands You want to: • Access the Conductor firmware update server via a proxy • Disable individual devices in a bypass configuration • Allow network admins to manage new devices or agents • Use serial over IP on an Airwall Gateway 110e or 110g.

New and updated Airwall help content

In addition to help for new features, here are the changes to content published since our last release:

New Topics –

- Troubleshoot Initial Airwall Gateway connections on page 491

Updated –

- Create an overlay network on page 418
- Update Airwall Gateway firmware on page 128
- Update firmware for a group of Airwall Edge Services on page 131
- Download Airwall Edge Services firmware updates on page 129
- Replace an Airwall Gateway on page 132
- Monitor Activity and Connections on page 116
- Log in and Configure the Conductor on page 201
- License and Provision a Conductor (v2.2.8 and earlier) on page 191
- Deploy a Physical Conductor on page 199
- Conductor and Airwall Edge Service PCI Compliance on page 137
- Set up Microsoft Azure as a cloud provider on page 434

Fixes

ID	Applies to	Description
DEV-14703	OSX Airwall Agents	macOS Big Sur – Modified the OSX installer to correctly install on macOS Big Sur.
DEV-14675	Cellular Airwall Gateways	The Airwall 110g firmware now sets the DevInfo/Man and DevInfo/Mod OMA-DM strings when connected to Verizon.
DEV-14623	OpenHIP	v2.2.8 Mac Airwall Agents may form unusable tunnels with older 2.1.7 (and possible other versions) peer Airwall Edge Services, if traffic is being sent when the Airwall Agent is starting up.
DEV-14590	Conductor	Fixed an issue with JSON serialization of underlay and map IPs in the PCI Airwall reference.

ID	Applies to	Description
DEV-14581	Airwall Gateways	Fixed an issue where when failover groups were configured to not use the Conductor as a ping destination and with the Conductor address using a hostname, the Airwall Edge Service is unable to connect to the Conductor by hostname.
DEV-14558	Airwall Gateways	Due to a bug in firmware versions 2.2.2 - 2.2.8, Airwalls using a TPM-backed keystore cannot update directly to firmware version 2.2.10. Should you run into this bug, you will see the following message on the Reporting -> Health Data page of the Conductor: "firmware_verify: The currently selected keystore is not compatible with the target software version. Please factory reset theAirwall Gateway with the keystore=file argument to downgrade." To install firmware version 2.2.10 on a TPM-enabled Airwall Gateway, apply Airwall Gateway Hotfix-14558 first and then install 2.2.10 normally. See Hotfixes on page 548.
DEV-14521	Conductor	Fixed a health data setting for 2.2.8 Android and Windows Airwall Agents that may have had their health data inadvertently turned off.
DEV-14510	Airwall Gateways	Source UDP and TCP port are now randomized when passing through a bypass configuration with SNAT enabled. This change fixes a rare case where both the bypass gateway and another Airwall Gateway behind it are trying to communicate with the same peer (for example, a relay).
DEV-14506	Android and Windows Airwall Agents	Fixed an issue where modifying the reporting_interval for traffic stats via the Conductor would disable health data on the agents that supported it.
DEV-14461	Airwall Gateways	Fixed an issue where if overlay device NAT was configured on a port group with multiple ports, the overlay device NAT was incorrectly applied to traffic between the two ports in the same port group.
DEV-14447	Linux Airwall Servers	Fixed an issue where the support bundle for a Linux Airwall Server was missing attributes.
DEV-14434	Airwall Gateways	IPv6 bypass is now functional for cellular underlay links.
DEV-14424	Conductor	Rate limited how often the bypass destinations traffic timestamp is updated to prevent negative performance impact on the Conductor.
DEV-14406	Conductor	Disabling traffic stats and health data monitors now works.
DEV-14394	Conductor	Fixed an issue that could cause revoked and re-activated Airwall Edge Services to fail to reconnect to the Conductor.
DEV-14389	Conductor	Fixed an issue where unmanaged or revoked Airwall Edge Service attributes could be updated using the API.
DEV-14359	Android Airwall Agents	Fixed an issue where switching underlays would cause the old underlay to be reported as unknown in the Traffic stats tab under reporting on the Conductor.
DEV-14356	Airwall Gateways	Fixed an issue where you could enable STP on port groups that use only a single port interface.

ID	Applies to	Description
DEV-14312	Conductor	Fixed a broken download link in Linux Airwall Server setup.
DEV-14307	Airwall Gateways	Now allow Airwall Gateways and Linux Airwall ServerAirwall Servers to carry traffic within the LSI prefix (default to 1.0.0.0/8) across HIP tunnels, except for addresses that collide with peer Airwall Edge Service LSI addresses.
DEV-14291	Airwall Gateways	Fixed an issue that could cause a service crash on Airwall Edge Services when there was a network-related HA failover/ failback.
DEV-14278	Android Airwall Agents	Fixed an issue where replacing an Android Airwall Agent while the Android Airwall Agent service was running required the Airwall Agent to be restarted to get its new configuration and restore pings.
DEV-14266	Airshell	Fixed an issue preventing the 'diag-report' command from returning data under Airshell on the AW-110g. Diagnostic reports (system reports) take much longer to generate on cellular platforms.
DEV-14265	Airshell	Fixed Airshell 'status cell' command on the AW-110g, which sometimes repeatedly produced an error response.
DEV-14254	Conductor	Fixed an issue where Airwall Agents were showing up when creating a device discovery event monitor.
DEV-14251	Airwall Gateways	Fixed an issue introduced in Airwall Gateway HF-1 that could cause traffic to get blocked onAirwall Gateways with multiple overlay port groups.
DEV-14244	Azure Cloud Conductor	Fixed an issue where you were not able to select VNet when setting up a cloud Conductor.
DEV-14243	Airwall Gateways	Fixed an issue where broadcast and multicast received on an L2 bypass port group was consuming unnecessary bandwidth.
DEV-14228	Conductor	Fixed an issue where devices in smart device groups with tags may not have been removed correctly when the tags existed on both the devices and **Airwalls** or **Airwall groups**.
DEV-14222	OpenHIP	Fixed an issue where DHCP configuration wasn't being updated.
DEV-14220	Conductor	Fixed an issue where you could not update an existing rule order and create a new device match rule with the old order of the existing rule.
DEV-14209	Android Airwall Agents	Fixed an issue where the Airwall Agent crashed the first time the user tried to start the service for a new profile.
DEV-14195	Conductor	Conductor Firmware downloader and OUI updater will now use the Conductor proxy settings.
DEV-14194	Airshell	Fixed an issue where the 'policy' command in Airshell returns an error under certain (larger, busier) deployments.
DEV-14191	Airwall Gateways	Fixed an issue that could cause traffic problems in deployments with multiple overlay port groups on the same broadcast domain.

ID	Applies to	Description
DEV-14179	Conductor	Fixed an issue where the clock color indicating when a user last logged in was incorrect .
DEV-14172	Airwall Gateway 110g	Disabled IMS when using the Airwall Gateway 110g on T-Mobile.
DEV-14167	Windows Airwall Agents and Servers	Fixed an issue where the Conductor was showing Windows Airwall Agents had an update available when they already had that version installed. Note that you may still see updates available for x64 Windows if you have x32 firmware downloaded on the Conductor.
DEV-14166	Cellular Airwall Gateways	Fixed an issue when using customer-specific Verizon APNs on the Airwall Gateway 110g.
DEV-14159	Airwall Gateways	Fixed an issue where overlay traffic could flood out overlay ports.
DEV-14128	Conductor	The traffic stats monitor alert now more clearly indicates what is being measured, that is, kB/s, pkts/s
DEV-14123	Conductor	Notices on the login screen are now only displayed one time and disappear for your next visit to the page.
DEV-14119	Conductor	Fixed an issue where Airwall groups were not applying tags as the group was created.
DEV-14115	Conductor	Fixed an issue that could cause infrequent Conductor service issues resulting in all Airwall Edge Services needing to reconnect to the Conductor.
DEV-14113	Conductor	Fixed an issue where you could create policy to a bypass destination from a gateway's device even though the gateway has bypass disabled on its underlay.
DEV-14103	Conductor	Fixed an issue where disabling or re-enabling network communications for a device deleted any tags on it. This issue also was occurring when if you updated a device, device group, Airwall group, overlay network, or people group using the API.
DEV-14100	Conductor	Fixed an issue where if you added a device directly to a device group in an Airwall invitation or during user onboarding, some of the necessary information was not being sent to the Airwall Agents and Servers to fully enable Airwall policies.
DEV-14095	Android Airwall Agents	Fixed an issue where the Overlay networks page was showing inaccurate ping counts.
DEV-14073	Conductor	Underlay IPs for 2.2.8 Airwall Gateways are now in the "underlay_ips" key in the API. IPs used for the map connection are now in the "map_ips" key in the API.
DEV-14070	Conductor	Fixed an issue where Airwall Edge Services coming online were not being included in Recent Activity.
DEV-14068	Android Airwall Agents	Fixed an issue where rotating the screen cleared the username and password when attempting to log in using User Auth.
DEV-14062	Conductor	FIxed a display issue when changing the pagination size on the monitors page.

ID	Applies to	Description
DEV-14044	Android Airwall Agents	Fixed an issue where the ping status icon on the Overlay Networks/Edge Services page was always blue when pinging.
DEV-14032	Conductor	Fixed an issue where viewing an overlay's details page in timeline view could cause an error.
DEV-14013	Conductor	Standardized timestamps for Airwall Agents and Servers to display in the user’s locale.
DEV-14009	Conductor	Fixed an issue where you couldn't remove static routes from a Conductor.
DEV-13984	Airwall Gateways	Fixed an issue where specifying the gateway on an overlay IP prevented creating the local subnet/connected route.
DEV-13978	Conductor	Fixed an issue where a device with an unknown OUI didn't update when the OUI list was updated.
DEV-13963	Linux Airwall Servers	Fixed an issue where HIP was restarting on the Centos7 Airwall Server.
DEV-13948	Cellular Airwall Gateways	Fixed an issue where sometimes the IMEI is listed as "unavailable" in Airshell and diagnostic mode when the affected Airwall Gateway does not have a sim card installed.
DEV-13946	Conductor	Fixed an issue where when when you disabled an Airwall Agent or Server, it was not showing a disabled tag in the devices list.
DEV-13944	Conductor and Airwall Gateways	Fixed an issue that caused device traffic to local devices (east/west) or bypass destinations to continue after disabling the device. Traffic to remote devices was not affected.
DEV-13943	Conductor	Fixed an issue where the Tag actions did not list that devices would be impacted.
DEV-13942	Conductor	People groups can now be added as managers when creating new overlay networks in the network creation wizard.
DEV-13935	API	Fixed an issue where network admins were unable to get the job status of Airwall Edge Service support jobs that they started in the API.

ID	Applies to	Description
DEV-13930	Alibaba Cloud Conductor	If you have created a new Alibaba Cloud Airwall Gateway with v2.2.8, there is an issue with the protected subnet id on the Cloud tab actually being the public subnet. **Workaround**: You can avoid this issue by installing this hotfix on the Conductor before creating any Alibaba Cloud Airwall Gateways. **Workaround if you have already created an Alibaba Cloud Airwall Gateway**: **1.** Apply this hotfix to your Conductor. **2.** If you are not using an NTP for system time, on the **Settings** page, **General setting** tab, under **System time**, select **Edit Settings**, and then Under **Update date and time**, select **Set browser time** and then select **Update**. **3.** For any cloud Alibaba Airwall Gateways, on the **Cloud** tab, **Diagnostic** subtab, click **Refresh**.
DEV-13926	OpenHIP	Fixed a rare packet allocation failure issue on the Airwall Gateway 100.
DEV-13916	Airwall Gateways	Fixed an issue where using DNSSRV records for Airwall Gateway provisioning caused the Conductor configuration to be lost.
DEV-13914	Conductor	Fixed an issue where if you used multiple serial over IP devices on the same Airwall Gateway (only supported on some profiles), you could create an invalid configuration when both devices are configured with the same IP but different ports.
DEV-13910	Conductor	You now receive a warning when creating a monitor on a device or Airwall group when some members of the group do not support the monitor. Previously, you only received such a warning for remote monitors (monitors run on the Airwall Edge Service).
DEV-13904	Google Cloud Conductor	Fixed an issue in the Google Cloud images for 2.2.8 Conductor and Airwall Gateways.
DEV-13903	Airwall Gateways	Airwall Gateway 110 models now can use the link failover monitor.
DEV-13893	Conductor	Fixed an issue where you could select Airwall Edge Services that do not support health data for the health data monitor (for example, the Mac, Linux, or iOS platforms as of 2.2.8)
DEV-13860	Conductor	Fixed an issue where when creating a new device, the Port affinity drop-down menu showed the first overlay port group, but the value set was "Detect automatically."
DEV-13850	Conductor	Fixed an issue where network administrators couldn't manage an Airwall Edge Service from Recent events Dashboard notifications.
DEV-13844	Conductor	When replacing a high-availability paired Airwall Gateway, the Conductor now only lists Airwall Gateways that have an HA port configured.

ID	Applies to	Description
DEV-13817	Airwall Gateways	Fixed an issue where the DHCP server on an Airwall Gateway Overlay Port Group was not restarting after changing the 'LSI prefix' on the Conductor.
DEV-13813	Airwall Gateways	Fixed an issue with the serial ports of the Airwall Gateway 110 where RS232 with hardware flow control (RTS/CTS), RS422 (full duplex) and RS485 (half duplex) were not functional. Airwall Gateway firmware version 2.2.10 and later supports all three serial port modes.
DEV-13768	Airwall Gateways	Fixed an issue where the source NAT setting on a bypass underlay port group was not updating the setting.
DEV-13765	Airwall Gateways	Fixed an issue where bypass underlay port groups with source NAT enabled and routed mode disabled did not allow incoming connections from the underlay.
DEV-13759	Airwall Gateways	Fixed an issue where the Detect Devices button sometimes incorrectly included devices attached to other port groups or peer Airwall Gateways if policy permitted traffic from an Overlay IP to those destinations.
DEV-13755	Cellular Airwall Gateways	Disabled LWM2M reporting on the Airwall Gateway 110g when using the AT&T carrier configuration. AT&T ODIS requirements are met by using a product specific IMEI TAC.
DEV-13748	Conductor	Fixed an issue where if you disabled overlay MTU, the change was not immediately sent to Airwall Gateways.
DEV-13744	Conductor	Fixed an issue where the Airwall group dialog allowed you to attempt to modify it even if you didn't have permissions.
DEV-13689	Conductor	Overlays, Devices, Airwalls, and People pages now have a consistent scheme for button and filter placement, with actions on the left and filters on the right.
DEV-13682	Airshell	Fixed an issue where multiple MAP URIs were not correctly displayed within Airshell ('status conductor', 'conductor status', and 'conductor set').
DEV-13664	Conductor	Email colors have been adjusted to be more legible in more email applications.
DEV-13630	Cellular Airwall Gateways	Fixed a problem related to signal strength reporting from Airwall Gateways with a Quectel modem connected to a 3G network.
DEV-13621	Airwall Gateways	Improved the timing of link failure-related actions (like reboot or cellular session recycling) to reflect the configured timeouts more accurately.
DEV-13505	OpenHIP	Fixed high CPU usage by hipd thread.
DEV-13332	Cellular Airwall Gateways	Updated the Quectel EC25-AF firmware revision to EC25AFFDR07A09M4G_01.004.01.004, to address some AT&T related connection issues.

ID	Applies to	Description
DEV-13297	Airwall Gateways	Fixed an issue where when an Airwall Gateway with seamless bypass is configured as layer 2 "bump in the wire," traffic from the protected device to remote protected devices on different subnets was not working as expected.
DEV-13275	Airwall Gateways	Fixed an issue where a misconfigured local device was corrupting the ARP cache entries for peer Airwall Gateways.
DEV-13272	Airwall Gateways	Improved the reliability of firmware updates in very low bandwidth situations.
DEV-13109	Airwall Gateways	Fixed **Check secure tunnels** diagnostic function: relays and relay clients are not longer included in the list.
DEV-10936	Airwall Gateways	You no longer need to cable HA Airwall Gateways directly, and should no longer see situations where both Airwall Gateways are active.
DEV-6147	Conductor	Fixed an issue where the placeholder text for an Airwall invitation "Generated Airwall name" was incorrect.
DEV-3342	Conductor	Fixed an issue where the firewall settings become unresponsive when editing Airwall Gateway settings.

Known Issues

ID	Applies to	Description
New DEV-15302	macOS Airwall Agents	The macOS Airwall Agent profile will not work correctly when restored to a new machine via Timemachine. **Workaround** -- Create a new profile on the Airwall Agent, and then on the Conductor, replace the old profile with the new one for that agent.
DEV-15039	Linux Airwall Servers	There is a small memory leak in the Airwall Linux Agent Server that might require a restart over the course of a month.
DEV-14981	Linux Airwall Servers	The Linux Airwall Server crashes when trying to ping peer Airwall Edge Services from the Conductor, and the server has around 15+ peers.
DEV-14818	Airwall Gateways, Open HIP	DNS-based Bypass opens up a possible security hole by allowing dynamic policy creations based on results of name lookup over the Internet. Combined with disabling Source NAT (SNAT), this leaves the Overlay open to attack from a sufficiently-technical attacker. **Workaround** – Enable SNAT on the Underlay when using DNS-based bypass destinations to prevent potential inbound access from arbitrary sources.
DEV-14772	OSX Airwall Agents	If the Airwall Agent is set to "off on boot" and the mac is rebooted, DNS may not be correctly set at startup. **Workaround** – Restart the agent to regain access to DNS. Stop the agent, if desired, to return to the DNS servers as given by DHCP.

ID	Applies to	Description
DEV-14767	AWS Cloud Conductor	ENA required instance types won't be available in us-gov-east-1 region for GovCloud customers, and ap-east-1 & eu-north-1 regions for commercial cloud customers. ENA supported and unsupported instance types still work with these new regions.
DEV-14743	Conductor	The Airwall Gateway setting for DHCPv6 uses DHCPv4.
DEV-14739	Airwall Gateways	If you set IPv4 to DHCPv4 and set a static IP address for IPv6, the setting that you set second doesn't get saved. **Workaround** – If you need both IPv4 and IPv6, set static IP addresses for both.
DEV-14736	Cellular Airwall Gateway 150s	Cellular details may display as "unavailable" on the first boot after upgrade. Cellular connections are not affected. **Workaround** – Reboot the Airwall Gateway a 2nd time.
DEV-14692	Airshell	In the new Airshell 'conf network' menu system, when editing a port group, it is possible to enter unsupported or duplicate interfaces, or interfaces already in use by another port group. **Workaround** – Check the `status network` output to check for duplicates to avoid unsupported or conflicting configurations.
DEV-14688	Cellular Airwall Gateways	After factory resetting a Verizon 101g, you must change the APN to 'vzwinternet' in diagnostic mode.
DEV-14636	Conductor	When adding Access windows to a people group, if you add a blocked window, you also need to add an Access window for the times you do want to give access. Otherwise users will always be blocked.
DEV-14610	Conductor	After changing the Reporting traffic stats reporting time, the CPU graph will not display. **Workaround** – Refresh your browser.
DEV-14608	Airwall Gateways	If the parent port of a VLAN-tagged sub-port is placed in a disabled port group, the VLAN-tagged child-port will not be initialized correctly in all cases. **Workaround** – To work around this issue, do not place parent-ports that have VLAN sub-ports in a disabled port group. Instead, remove unneeded parent-ports from all port groups. This issue will be fixed in a future firmware revision.
DEV-14606	Airwall Gateways	When attempting to replace a HA member with a new Airwall Gateway, the Conductor allows you to select an Airwall Gateway that does not have an Overlay or HA port configured. **Workaround** – Make sure the Airwall Gateway you select has a workable HA port configuration.

ID	Applies to	Description
DEV-14595	Cellular Airwall Gateways	When an Airwall Gateway 110g is started without a SIM card installed and Verizon selected as the carrier, the cellular modem will restart every 2 minutes until a SIM card is installed.
DEV-14584	Cellular Airwall Gateways	SIM hot-swap functionality is not guaranteed on firmware version 2.2.10 with the Airwall Gateway 110. Please reboot the Airwall Gateway after installing a new SIM card.
DEV-14577	Airwall Gateways	Device activity doesn't report activity on bypass port groups with routed only disabled.
DEV-14570	Conductor	If an Airwall Agent owner is set as any user (LDAP, local, or OIDC) and someone attempts to user authenticate with a different OIDC user, they will not be able to authenticate (which is the correct behavior), but they see a 500 error message instead of a helpful error message.
DEV-14564	Conductor	The following log messages can be safely ignored: [ERROR] error parsing message: msg= [ERROR] JsonRpcDispatcher: received unknown method: method= msg=
DEV-14560	Airwall Gateways	Assigning block policies to bypass destinations has no effect. **Workaround** – Create a bypass destination using the resolved IP address of the hostname and create blocking policy for it.
DEV-14549	Android Airwall Agent	Cellular details are not currently available on the Ports tab for Android Airwall Agents.
DEV-14518	Android Airwall Agent	The Ports tab is now available for Android Airwall Agents with the following drawbacks: • The cellular interface data is not available. • You cannot change anything on the Agent Ports tab.
DEV-14509	Airwall Gateways	Diagnostics: Ping peer Airwall Gateways may return false negatives
DEV-14504	Conductor	Filtering alerts by name always includes new alerts, even if they do not match the filter keyword.
DEV-14483	Airwall Gateways	When you configure device NAT for devices on multi-port port groups, NAT is applied to the initial flow of intra-port group packets from those devices. Subsequent conversations will correctly omit the NAT.
DEV-14467	Airwall Gateways	Connecting an access port interface and a VLAN-tagged port interface within the same Airwall Gateway port group to an STP-enabled Cisco switch will trigger a Cisco port disable. **Workaround** – Set “no spanning-tree VLAN <#>” on the Cisco switch’s affected VLANs to prevent the port shutdown.
DEV-14427	Conductor	IPv6 DHCP settings sometimes show IPv4 options after choosing the 'Select one...' option. **Workaround** – Refresh the browser window and try again.

ID	Applies to	Description
DEV-14426	Conductor, Airwall Gateways	Bypass destinations with a hostname do not show device activity in the user interface.
DEV-14361	Airwall Gateways	The **Build new tunnels if none exist** setting doesn't trigger building tunnels on peer Airwall Edge Services with IPv6-only policy. **Workaround** – Add IPv4 policy between the peer Airwall Edge Services.
DEV-14336	AWS Cloud Conductor	If you choose an ENA machine type when creating a cloud Conductor on Amazon Web Services, you cannot downgrade or change it back to a non-ENA type. However, for a cloud Airwall Gateway, if you choose an ENA machine type, you can downgrade it if you first change it to a non-ENA machine type in Amazon Web Services.
DEV-14308	OpenHIP	Initial packets may be dropped while building a new tunnel to a new peer Airwall.
DEV-14249	iOS Airwall Agents	**Check Secure Tunnels** or **Tunnel Status** may be unavailable on iOS. **Workaround** – You can determine Tunnel status by checking packets sent/received.
DEV-14233	Virtual Airwall Gateways	Amazon EC2 Airwall Gateways using ENA network drivers will start with the second interface disabled instead of defaulting to an overlay port group.
DEV-14218	Airwall Gateways	NAT broadcast applies to traffic between ports within a single port group. Use an external switch if you need to connect multiple devices to a single port group and use the NAT broadcast feature and require IP broadcast un-NATed between those local devices.
DEV-14210	Conductor	Currently, when you set Source NAT, it configures it for both IPv4 and IPv6.
DEV-14208	Airwall Gateways	Bypass port groups do not currently support IPv6.
DEV-13970	Alibaba Cloud Conductor	When you upgrade a Conductor on Alibaba Cloud, the Conductor system time gets out of sync. **Workaround** – Go to **Settings** > **Other settings** > **System time and date**, click **Edit Settings**, then **Update** to resync.
DEV-13880	Diagnostic mode on Airwall Gateways	EAP-TLS does not work with current or previous WiFi Airwall Gateways (75w), so is now disabled. This setting will be reenabled once this feature is fixed.
DEV-13775	Azure Cloud Conductor	Conductor might rarely give "Net::ReadTimeout" error when user tries to deploy an Azure Airwall Gateway 300v or server. This doesn't indicate that the deployment has failed. If you get this error message, go to the Azure portal and check the actual deployment result.

ID	Applies to	Description
DEV-13753	Azure Cloud Conductor	During cloud Airwall Gateway deployment, you can now choose an existing resource group, as long as you make sure the name of the Airwall Gateway deployment does not conflict with any resources in the existing resource group.
DEV-13271	Airwall Gateways	The Airwall Gateway 110 has CPU frequency scaling enabled, which allows it to save power under low load conditions. This results in high load average / CPU usage figures in Conductor when the Airwall Gateway 110 CPU is in its lowest power state. Future releases may improve CPU utilization.
DEV-12852	Windows Airwall Agents and Servers	The Windows Airwall Agent may not connect when multiple interfaces are active This issue can be caused by a Windows default that doesn't allow multiple simultaneous active network interfaces, and prefers ethernet over cellular or WiFi. It can be bypassed by editing a registry value. See the troubleshooting steps in I am having trouble connecting on page 31.
DEV-8824	Android Airwall Agents	The implicit SNAT for Airwall Agents without an Overlay IP is not applied from a pre 2.2.10 Android Airwall Agent to a 2.2.10 Airwall Gateway with SNAT disabled: please upgrade the Android Airwall Agent to 2.2.10 or later.

Release Notes 2.2.8 Hotfix – Conductor HF-5

Release Date: Dec 18, 2020

This is a hotfix to release v2.2.8 for Conductors. See Release Notes 2.2.8 on page 673 for more additions in version 2.2.8. Download HF-5 from Hotfixes on page 548.

2.2.8 Conductor Hotfix HF-5 includes and replaces Conductor Hotfixes HF-1 through HF-4. Once installed, it will show all hotfixes (HF-1, HF-2, HF-3, HF-4, and HF-5) as installed.

What’s New

This hotfix is a replacement for Conductor HF-4 that fixes **Airwall Invitations** that were expiring too quickly.

Upgrade Considerations

Upgrade to this 2.2.8 hotfix if you were experiencing any of the following issues:

- Need **Airwall Invitations** to have a long expiration date.

Or if you were impacted by any of the other issues fixed in this or earlier hotfixes.

Fixes

ID	Applies to	Description
DEV-14901, DEV-14873	Conductor	Fixed an issue where the link to set your password for a new user that is provided by email expires very quickly. The expiration is now set to 2 weeks from the date of the invite. **Workarounds** – Go to the login page and reset your password to generate a new reset password token and then follow instructions in the email you receive. – Have your admin manually set the password. Also fixed an issue where error messages (e.g. from passwords that do not meet the necessary criteria) were not being displayed on the reset password page.
Includes HF-4 Fixes:		
DEV-14424	Conductor	Rate limit how often a bypass destinations traffic timestamp will be updated to prevent negative performance impact on the Conductor.
DEV-14332	Conductor	Fixed an issue where if you deleted a tag owner, the UI wouldn't show any tags on the page that would be displayed below it.
Includes HF-3 Fixes:		
DEV-14167	Windows Airwall Agent or Server	Fixed an issue where the Conductor was showing Windows Airwall Agents had an update available when they already had that version installed. Note that you may still see updates available for x64 Windows if you have x32 firmware downloaded on the Conductor.
Includes Conductor HF-2 Fixes:		
DEV-14103	Conductor	Fixed an issue where disabling or re-enabling network communications of a device would delete any tags on it. Updating a device, device group, Airwall group, overlay network, or people group via the API would delete any tags on the updated object.
DEV-14080	Conductor	Fixed an issue where when adding a device directly to a device group in an Airwall Invitation or during user onboarding, some of the necessary information was not being sent to the Airwall Agents and Servers to fully enable policies.
DEV-14077	Conductor	Fixed an issue where the dashboard number for upgradeable Airwalls was including Airwalls that could apply an earlier version.
DEV-14073	Conductor	Underlay IPs for 2.2.8 Airwall Gateways are now in the "underlay_ips" key in the API.

ID	Applies to	Description
DEV-14070	Conductor	Fixed an issue where Airwall Gateways coming online was not being included in an overlay network's Recent Activity.
DEV-14059	Conductor	Fixed an issue where you could apply HF-1 multiple times.
DEV-14032	Conductor	Fixed an issue where viewing an overlay's details page in timeline view could cause an error.
DEV-14009	Conductor	Fixed an issue where you sometimes couldn't remove static routes from an HA pair.
DEV-13944	Conductor, Airwall Gateway	Fixed an issue that caused device traffic to local devices (east/west) or bypass destinations to continue after disabling the device. Traffic to remote devices was not affected.
Includes Conductor HF-1 Fixes:		
DEV-13943	Conductor	Fixed an issue in the Tag Actions menu where devices with the tag were not included in the list of items that would be impacted by the action.
DEV-13942	Conductor	People groups can now be added as managers when creating new overlay networks.
DEV-13930	Cloud-Alibaba, Conductor	If you have created a new Alibaba Cloud Airwall Gateway with v2.2.8, there is an issue with the protected subnet id on the Cloud tab actually being the public subnet. **Workaround**: You can avoid this issue by installing this hotfix on the Conductor before creating any Alibaba Cloud Airwall Gateways. **Workaround if you have already created an Alibaba Cloud Airwall Gateway**: **1.** Apply this hotfix to your Conductor. **2.** If you are not using an NTP for system time, on the **Settings** page, **General setting** tab, under **System time**, select **Edit Settings**, and then Under **Update date and time**, select **Set browser time** and then select **Update**. **3.** For any cloud Alibaba Airwall Gateways, on the **Cloud** tab, **Diagnostic** subtab, click **Refresh**.
DEV-13912	Conductor	Fixed an issue where secure tunnel status was not accurately reporting tunnel status for HA-paired Airwall Gateway's.
DEV-13904	Cloud-Google, Conductor	To deploy a 2.2.8 Google Cloud 300v Airwall Gateway from the Conductor, apply this hotfix.
DEV-13893	Conductor	Fixed an issue where you could select Airwall Edge Services that do not support health data for the health data monitor (for example, you now cannot select the Mac, Linux, or iOS platforms)
DEV-13888	Conductor	Fixed an issue where when you attempted to manage items from a **New Airwall Online** notification on the new Dashboard, it could be lost if another notice is received.

ID	Applies to	Description
DEV-13870	Conductor	Fixed an issue where bandwidth would be reported multiple times, resulting in dashboard graphs reporting much higher throughput than the actual throughput.
DEV-13860	Conductor	Fixed an issue where when you were creating a new device, the **Port affinity** menu showed the first overlay port group, even though the value was set to **Detect automatically**.

Known Issues

See Release Notes 2.2.8 on page 673 for known issues.

Release Notes 2.2.8 Hotfix – Airwall Gateway HF-3

Release Date: Oct 19, 2020

This is a hotfix to release v2.2.8 for Airwall Gateways. See Release Notes 2.2.8 on page 673 for more additions in version 2.2.8. Download HF-3 from Hotfixes on page 548. See also Release Notes 2.2.8 Hotfix – Airwall Gateway Hotfix-13955 on page 673.

2.2.8 Airwall Gateway Hotfix HF-3 includes and replaces Airwall Gateway Hotfixes HF-1 and HF-2. Once installed, it will show all hotfixes (HF-1, HF-2, and HF-3) as installed.

Note:

Also install Conductor HF-4, as it fixes some of these issues from the Conductor side. See Release Notes 2.2.8 Hotfix – Conductor HF-4 on page 670.

What’s New

This hotfix is a replacement for Airwall Gateway HF-2 that fixes a bug in the HA failover logic causing invalid HA state information to be displayed in the Conductor when the failover was triggered by network availability. The hotfix also fixes an issue that could cause excessive device activity event reporting on bypass ports with large device network objects as well as a problem when using device NAT with bridged overlay port groups.

Upgrade Considerations

Upgrade to this 2.2.8 hotfix if you were experiencing any of the following issues:

- Conductor displaying an Invalid HA state for Airwall Gateways
- Excessive disk utilization on the Conductor and/or high network traffic between Airwall Gateways configured with a bypass port group and the Conductor
- Ping devices failures
- Airwall Gateways needing to reconnect to the Conductor
- Airwall Gateways failing a policy check on some overlay networks.

Or if you were impacted by any of the other issues fixed in this or earlier hotfixes.

Fixes

ID	Applies to	Description
Airwall Gateway HF-3:		
DEV-14452	Airwall Gateway	Rate-limited device activity events for network objects.
DEV-14451	Airwall Gateway	Fixed an HA issue after rebooting an Airwall Gateway

ID	Applies to	Description
DEV-14449	Airwall Gateway	Fixed an issue where the overlay NAT was being applied to traffic between ports in an Overlay port group.
Includes Airwall Gateway HF-2:		
DEV-14247	Airwall Gateway	Fixed a bug that was introduced in Airwall Gateway Hotfix rollup-1 that could cause traffic to get blocked on Airwall Gateways with multiple overlay port groups.
DEV-14190	Airwall Gateway	Fixed an issue that could cause traffic problems in deployments with multiple overlay port groups on the same broadcast domain.
DEV-14162	Airwall Gateway	Fixed an issue in Conductor HF-2 that was causing the "Ping devices" feature to fail for devices with plain IP addresses.
DEV-14115	Conductor	Fixed an issue that could cause infrequent Conductor service issues resulting in all Airwall Gateways needing to reconnect to the Conductor.
DEV-14067	Conductor, Airwall Gateway	Fixed an issue on 2.2.8 Airwall Edge Services that could cause false negatives in the policy check for some overlay network configurations.
DEV-13981	Airwall Gateway	Fixed an issue where setting an overlay default gateway prevented creating both the connected (local subnet) and default routes.
DEV-13974	OpenHIP	Fixed performance regression on multi-core platforms.
DEV-13926	OpenHIP	Fixed a rare packet allocation failure issue on Airwall Gateway-100.
DEV-13903	Airwall Gateway	Airwall Gateway-110 models now can use the link failover monitor.
DEV-13843	Airwall Gateway	Added firewall connection states to the diagnostic report.
DEV-13275	Airwall Gateway	Fixed an issue where a misconfigured local device was corrupting the ARP cache entries for peer Airwall Gateways.

Known Issues

See Release Notes 2.2.8 on page 673 for known issues.

Release Notes 2.2.8 Hotfix – Conductor HF-4

Release Date: Oct 19, 2020

What's New

2.2.8 Conductor Hotfix HF-4

This is a hotfix to release v2.2.8 for the Conductor. This hotfix rolls up the previous Conductor hotfixes HF-1 through 3, so you only need to install HF-4. See Release Notes 2.2.8 on page 673 for more additions in version 2.2.8. Download HF-4 from Hotfixes on page 548.

Note: Also install Airwall Gateway HF-3, as it fixes some of these issues from the Airwall

Gateway side. See Release Notes 2.2.8 Hotfix – Airwall Gateway HF-3 on page 669.

Upgrade Considerations

Upgrade to this 2.2.8 hotfix if you have a bypass destination configured and are experiencing Conductor performance issues, or were impacted by any of the other issues fixed in this hotfix.

Fixes

ID	Applies to	Description
HF-4 Fixes:		
DEV-14424	Conductor	Rate limit how often a bypass destinations traffic timestamp will be updated to prevent negative performance impact on the Conductor.
DEV-14332	Conductor	Fixed an issue where if you deleted a tag owner, the UI wouldn't show any tags on the page that would be displayed below it.
Includes HF-3 Fixes:		
DEV-14167	Windows Airwall Agent or Server	Fixed an issue where the Conductor was showing Windows Airwall Agents had an update available when they already had that version installed. Note that you may still see updates available for x64 Windows if you have x32 firmware downloaded on the Conductor.
Includes Conductor HF-2 Fixes:		
DEV-14103	Conductor	Fixed an issue where disabling or re-enabling network communications of a device would delete any tags on it. Updating a device, device group, Airwall group, overlay network, or people group via the API would delete any tags on the updated object.
DEV-14080	Conductor	Fixed an issue where when adding a device directly to a device group in an Airwall Invitation or during user onboarding, some of the necessary information was not being sent to the Airwall Agents and Servers to fully enable policies.
DEV-14077	Conductor	Fixed an issue where the dashboard number for upgradeable Airwalls was including Airwalls that could apply an earlier version.
DEV-14073	Conductor	Underlay IPs for 2.2.8 Airwall Gateways are now in the "underlay_ips" key in the API.
DEV-14070	Conductor	Fixed an issue where Airwall Gateways coming online was not being included in an overlay network's Recent Activity.
DEV-14059	Conductor	Fixed an issue where you could apply HF-1 multiple times.
DEV-14032	Conductor	Fixed an issue where viewing an overlay's details page in timeline view could cause an error.

ID	Applies to	Description
DEV-14009	Conductor	Fixed an issue where you sometimes couldn't remove static routes from an HA pair.
DEV-13944	Conductor, Airwall Gateway	Fixed an issue that caused device traffic to local devices (east/west) or bypass destinations to continue after disabling the device. Traffic to remote devices was not affected.
Includes Conductor HF-1 Fixes:		
DEV-13943	Conductor	Fixed an issue in the Tag Actions menu where devices with the tag were not included in the list of items that would be impacted by the action.
DEV-13942	Conductor	People groups can now be added as managers when creating new overlay networks.
DEV-13930	Cloud-Alibaba, Conductor	If you have created a new Alibaba Cloud Airwall Gateway with v2.2.8, there is an issue with the protected subnet id on the Cloud tab actually being the public subnet. **Workaround**: You can avoid this issue by installing this hotfix on the Conductor before creating any Alibaba Cloud Airwall Gateways. **Workaround if you have already created an Alibaba Cloud Airwall Gateway**: **1.** Apply this hotfix to your Conductor. **2.** If you are not using an NTP for system time, on the **Settings** page, **General setting** tab, under **System time**, select **Edit Settings**, and then Under **Update date and time**, select **Set browser time** and then select **Update**. **3.** For any cloud Alibaba Airwall Gateways, on the **Cloud** tab, **Diagnostic** subtab, click **Refresh**.
DEV-13912	Conductor	Fixed an issue where secure tunnel status was not accurately reporting tunnel status for HA-paired Airwall Gateway's.
DEV-13904	Cloud-Google, Conductor	To deploy a 2.2.8 Google Cloud 300v Airwall Gateway from the Conductor, apply this hotfix.
DEV-13893	Conductor	Fixed an issue where you could select Airwall Edge Services that do not support health data for the health data monitor (for example, you now cannot select the Mac, Linux, or iOS platforms)
DEV-13888	Conductor	Fixed an issue where when you attempted to manage items from a **New Airwall Online** notification on the new Dashboard, it could be lost if another notice is received.
DEV-13870	Conductor	Fixed an issue where bandwidth would be reported multiple times, resulting in dashboard graphs reporting much higher throughput than the actual throughput.
DEV-13860	Conductor	Fixed an issue where when you were creating a new device, the **Port affinity** menu showed the first overlay port group, even though the value was set to **Detect automatically**.

Known Issues

See Release Notes 2.2.8 on page 673 for known issues.

Release Notes 2.2.8 Hotfix – Airwall Gateway Hotfix-13955

Release Date: Aug 4, 2020

What's New

2.2.8 Airwall Gateway Hotfix	This is a hotfix to release v2.2.8 for Airwall Gateways. See the Release Notes 2.2.8 on page 673 for more additions in version 2.2.8. Download Hotfix-13955 from Hotfixes on page 548.

Upgrade Considerations

If you use DNSSRV to set the Conductor address on your Airwall Gateways, we recommend that you install this hotfix before upgrading them to 2.2.8 .

Fixes

ID	Applies to	Description
DEV-13916		Fixed the use of DNS SRV records for Airwall Gateway provisioning. Apply HF-13955 before upgrading Airwall Gateways to firmware version 2.2.8 or after provisioning new 2.2.8 Airwall Gateways via a DNS SRV record. You can then install 2.2.8 on the Airwall Gateways. If you have already installed 2.2.8 on Airwall Gateways and are experiencing this issue, please contact Customer Success for assistance, or you can manually configure the Conductor address in each Airwall Gateway using `airsh` or Diagnostic mode.

Known Issues

See Release Notes 2.2.8 on page 673 for known issues.

Release Notes 2.2.8

Release Date: Jul 17, 2020

What's New

Note: These release notes were updated Jul 31, 2020 to include the release of the v2.2.8 Windows Airwall Agents and Servers, and Sep 9, 2020, with an update for the all Airwall Agents and Servers. New versions are in the Latest firmware and software on page 514.

New Airwall Gateway Hardware – the Airwall-110

The Airwall-110 Series is a major upgrade for the 100-Series, with higher performance and global cellular connectivity – all in a smaller form factor that maximizes the v2.2.8 improvements. The Airwall-110 has more (4x) bandwidth performance and two serial ports, runs all Snort intrusion detection monitors, handles up to 6 HD video streams, and has more storage and memory (so it has higher capacity, quality, and scalability for production environments).

See more: Airwall Gateway 110 Series on page 144

New cellular modem support

Version 2.2.8 supports the upcoming North America and Global cellular expansion trays for our Airwall-150 appliance. These LTE Category 4 expansion modules come in two variants supporting North America and Rest of World. These expansion trays allow you to connect your Airwall 150 to more cellular carriers in more countries including the United States, Canada, Australia, New Zealand, Japan, the European Union, and other countries recognizing CE RED certificates.

Conductor Dashboard and Usability Improvements

The Conductor Dashboard has been improved to give you a broader look into the status of your Airwall secure network. New features include:

- Ability to pin pages you visit frequently
- See how many Airwall Edge Services are online, and how many authenticated users are logged in.
- Easily manage new provisioning requests
- See when new firmware and software is available, and easily update your network.
- Improved user onboarding workflow (see Improved User Management below)

See more:

- The Conductor Dashboard on page 32
- Create or Manage Dashboard Messages on page 38
- Conductor Icon Reference on page 35
- Monitor Connections to your Airwall secure network on page 124
- Download Airwall Edge Services firmware updates on page 129
- Update firmware for a group of Airwall Edge Services on page 131

Improved User Management and Remote Access User Features

Remote access user management has been expanded to scale for large organizations, with the Conductor doing most of the work that admins used to have to do to invite, onboard (especially installing and activating the Airwall Agents), orchestrate, and authenticate remote access users. Onboarded users can see what they can access through the overlay networks in Conductor, eliminating frequent support calls to Conductor admins for help getting server IP addresses.

See more:

Conductor Admin Topics

- Connect People's Devices to your Airwall secure network on page 64
- Connect People as Remote Access Users on page 74
- Connect People's Devices with Activation Codes on page 75
- Set up a People Group on page 89
- Manage Versions of Airwall Agents and Servers on page 126
- Provision Airwall Gateways using Activation Codes on page 193
- Walkthrough - Onboard people to your Airwall secure network with User Authentication on page 83

End user topics

- Change my Conductor password on page 30
- I have an Activation Code on page 15
- I want to request to connect on page 17
- I have a "Finish Setting up my account" email on page 15
- Create or Edit Airwall Agent or Server Profiles on page 29
- I am having trouble connecting on page 31

Enhanced Monitoring

You can now set monitor thresholds on health data and traffic stats to detect potential problems before they occur. We have redline stats for performance metrics of the Airwall Gateway, and for volumetric traffic stats.

Seamless Bypass (split tunnel)

Seamless bypass enables you to deploy without knowing all of the hosts to allow in an overlay policy. Seamless bypass replaces the need to create policy exceptions, and reduces the complexity, extra hardware, extra cabling, and reliance on configuration of your underlay infrastructure.

See more: Local Bypass on page 394

Alibaba Cloud Conductor and Airwall Gateways

You can now use Alibaba Cloud to deploy cloud Conductors and Airwall Gateways, and seamlessly connect cloud Conductors and Airwall Gateways with each other, as well as virtual and on-premises or physical environments. You can deploy an Airwall secure network on all of the major cloud providers.

See more:

- Deploy a Conductor on Alibaba Cloud on page 202
- Alibaba Cloud – Set up an Airwall Gateway on page 315

Routed Port Group Improvements

The ability to configure port groups can give you up to a 30% performance increase for common deployment cases using a single interface in the overlay port group (for example, cloud gateways, virtual gateways, and optionally on physical gateways). It is simpler to deploy and avoids multicast/broadcast chatter over the tunnel.

See more:

- Set up Port Groups on an Airwall Gateway on page 386
- Set up an Underlay Port Group on page 389
- Set up Overlay Port Groups on page 386

Custom signed Certificate Improvements

You can replace a signed certificate on the Conductor with the old certificate remaining active until the new certificate is activated.

See more: Add or Replace a Signed Certificate for the Conductor UI on page 239

Easier Deployment of High Availability Cloud Conductors

The Airwall Solution has automated the process of creating high availability Conductors in the cloud across different providers. You can now back up your Conductor and easily create an HA standby in the cloud using the Conductor's automated process and be guaranteed a successful cloud HA deployment.

See more: Automatically Create an Standby HA Conductor in the Cloud on page 265

Remote Airshell Access into Airwall Gateways

You can securely log in to the overlay IP address of an Airwall Gateway with key-based SSH, and run Airshell (airsh) commands remotely. Airsh has been enhanced to perform many of the functions of diagnostic mode. Remote access can help avoid in-person visits to perform diagnostics and troubleshooting. Status and statistics are available using airsh, which includes tab-completion and inline help.

See more:

- Set up Remote Access to Airshell via SSH on page 374
- Access an Airwall Gateway Remotely on page 375

Port configuration replication

You can now replicate the port configuration between two Airwall Gateways when setting up an Airwall Gateway HA pairing, or when replacing an Airwall Gateway.

See more:

- Configure High Availability Airwall Gateways (v2.2.8 and later) on page 399
- Replace an Airwall Gateway on page 132

Device Manufacturer (MAC address OUI) is now displayed

The **Devices** list now shows the manufacturer's name determined from the MAC address OUI (organizationally unique identifier), where available, in the **OUI** column. You can also now update the OUI list as needed.

See more:

- Update the MAC address (OUI) (Manufacturer) List on page 484
- See MAC address OUI (Manufacturer) Information for Devices on page 115
- Search for or Sort Devices by MAC Address OUI (Manufacturer) Name on page 115

Manage Airwall Agents through an MDM

Some MDM solutions now support managing Airwall Agents.

See more: Manage Airwall Agents through an MDM (Mobile Device Management) solution on page 82.

SD-WAN

An option was added to expose the Differentiated Services Code Point (DSCP) field of the inner IP header (plaintext) to the outer (encrypted) encapsulating header. This allows for classification of different types of network traffic for routing and prioritization purposes.

Upgrade Considerations

Consider upgrading to 2.2.8 if:

You want to use any of the following features:	You were impacted by any issues discovered in prior releases, especially if you have any of the following:
Seamless bypass (split tunnel)	
Alibaba Cloud Airwall Gateways	
Set up High-availability Cloud Conductors	

New and updated Airwall help content

In addition to help for new features, here are the changes to content published since our last release:

New Topics –

- Back up Azure Airwall Gateway 300v on page 133
- Restore an Azure Cloud Airwall Gateway on page 134
- Back up your Conductor on page 133
- Restore your Conductor from a database backup on page 133
- Set the Conductor system time
- Best Practices for Conductor Configuration on page 235
- Create an Event Monitor on page 119
- See and Manage Alerts on page 118
- Set who sees Event Monitors on page 119

- Set your Email Alert Level on page 118
- The Conductor Dashboard on page 32
- Conductor Icon Reference on page 35

Updated –

- Configure Authentication Options on page 242
- Limit Device Traffic on an Airwall Gateway with Port Filtering on page 411
- Set up Port Filtering on an Airwall Gateway on page 412
- What makes up an Airwall secure network? on page 141
- Deploy a Physical Conductor on page 199
- Configure a Conductor on page 235
- Create an Event Monitor on page 119
- Connect to the console port using Windows on page 298
- Set up physical Airwall Gateways on page 275
- Configure Advanced Airwall Edge Service Options on page 384
- Set up a virtual Airwall Gateway in Microsoft Hyper-V on page 308
- Allow an Airwall Agent or Server to access your Airwall secure network on page 82
- Airshell (airsh) Command Reference on page 362

Fixes

ID	Applies to	Description
DEV-14067	Airwall GatewaysConductor	Fixed an issue on 2.2.8 Airwall Edge Services that could cause false negatives in the policy check for some overlay network configurations.
DEV-13963	Linux Airwall Server	Fixed an issue where HIP was restarting on the Linux Centos7 Airwall Server.
DEV-13754	Airwall Agent	The agent now waits for DNS to be available if the Conductor MAP address is a fully qualified domain name (FQDN).
DEV-13720	Conductor	Setting "Disable pings on active link" no longer requires a reboot.
DEV-13683	Conductor	Fixed an issue where cloud attributes smart device group rules were broken due to internal database reconfigurations. You can match devices on cloud Airwall Gateways that match certain attributes: provider, region, VPC ID, and subnet ID. For instance, you can match on "aws" to find all devices inside AWS.
DEV-13643	Airwall Gateway	Peer auto-connect setting now must be done from the Conductor. It is no longer available in Diag mode.
DEV-13627	OpenHIP	Fixed a deadlock which may occur on a busy gateway which is also acting as a relay.
DEV-13569	Airwall Gateway	Fixed excessive CPU usage when using generic Serial over IP.
DEV-13566	OSX Airwall Agent	Fixed an issue in the installer.
DEV-13542	Linux Airwall Agent	The Conductor tunnel report is now working properly

ID	Applies to	Description
DEV-13535 DEV-13513	Conductor	Fixed an issue where Airwall agents and servers would publish transitory routing changes involving internal routing IP addresses as routing alerts in Conductor when there really was no problem. Any routing problems are still exposed via logging warnings.
DEV-13525	Airwall Gateway	Fixed an issue that caused disabling auto-repair in Linkmanager failover groups to be ignored.
DEV-13508	Conductor	Added PCI user activity entries for system level operations such as rebooting, restarting the metadata cache, and taking a database backup.
DEV-13439	Windows Airwall Agent	Fixed an issue when using Win update packages before v2.2.6 were not communicating whether they were 32- or 64-bit.
DEV-13405	Conductor	Fixed an issue where very large provisioning requests sync jobs to the licensing server were timing out.
DEV-13382	Conductor	Anonymous proxy servers are now allowed.
DEV-13353	Windows Airwall Agent	Fixed a cert error that prevented unattended installation of the Windows Airwall Agent.
DEV-13275	Airwall Gateway	Fixed an issue where a misconfigured local device can poison the ARP cache entries for peer Airwall Gateways.
DEV-13250	Airwall Gateway	You can now replace HA-paired Airwall Gateways after failure without first destroying the HA pairing.
DEV-13244	Conductor	Fixed an issue where Tag search device match rules (DMR - part of smart device groups) were not matching some matching device tags (e.g. query string of cell now matches cell1 or cellular). When adding a tag to a device that did not yet exist in the system, the DMR would miss adding the device to its group.
DEV-13217	Linux Airwall Agent	The default profile profile1 now cannot be deleted.
DEV-13213	Conductor	Fixed an issue where the Airwall Edge Service tunnel reporting data had Airwall Edge Service names truncated if they were too long. You can now see the full name by hovering over the clipped name.
DEV-13211	Windows Airwall Agent	Airwall Agent now re-enable Tempered TAP adapter on start up if it is disabled.
DEV-13209	Conductor	Ping peer Airwall Gateways now includes Airwall Gateways that are acting as both a gateway and a Relay.
DEV-13207	Airwall Gateway	Added the ability to specify PDP context IP type for cellular connections. In previous versions, the carrier-specific default was not overridden by the "ipv6" checkbox used in diag mode and airsh. This ipv6 checkbox has been replaced by an ip-type field, allowing customers to specify default (meaning carrier default), ipv4, ipv6, or dual-stack ipv4v6.

ID	Applies to	Description
DEV-13202	Conductor	Warning log on Airwall Edge Services that monitor is unsupported when the monitor is supported have been removed.
DEV-13147	OSX Airwall Agent	Fixed an issue with packet captures on the OSX Airwall Agent.
DEV-13134	Conductor	Fixed an issue where importing an Airwall Edge Service that doesn't exist silently fails the import.
DEV-13122	Android Airwall Agent	Fixed an issue where failover from cellular to Wifi didn't always work without a restart.
DEV-13121	Airwall Gateway	Fixed an issue that caused overlay network traffic to become blocked when using the Airwall Gateway's overlay IP for serial-over-IP.
DEV-13117	Conductor	Now all changes to Airwall Gateway port configurations are logged in the PCI user activities log.
DEV-13116	Conductor	It is no longer possible to add non-local users (that is, those created in LDAP or OIDC) to a people group during creation by using **Select all**. You manage these people group memberships via groups in their respective systems.
DEV-13107	Conductor	Added PCI logging for changes to Conductor web certificate and CA chains.
DEV-13101	Conductor	Fixed an issue that could cause the packet capture feature in the Conductor support tab to show no capture interfaces.
DEV-13100	Airwall Gateway 150	Fixed an issue where upon applying certain types of port configurations, the overlay ports fail to link up until the next reboot of the airwall.
DEV-13094	Airwall Gateway	Fixed an issue that caused link fail-over times to be delayed by up to 30 seconds.
DEV-13078	Airwall Gateway	Fixed an issue that caused the reboot setting in the underlay link manager to have no effect if any underlay port groups were configured as stand-alone.
DEV-13077	Serial-over-IP	Fixed an issue that could cause serial-over-IP to be come unresponsive after cellular outages.
DEV-13076	Conductor	Fixed a bug that could cause HIP tunnels to become stale after temporary cellular link failures.
DEV-13072	Conductor	Fixed Cellular signal strength timed out message.
DEV-13064	Conductor	Some event actions have a target box. Filtering the target box by name is now working.
DEV-13063	Conductor	Fixed a UI issue where button text wasn't visible on the HIP tunnel stats page when in Dark Mode.
DEV-13062	Conductor	Fixed a UI error when modifying the recipient list of an existing alert.
DEV-13061	Cloud	Updated paths for the 2.2.3 AW image ID in Google Cloud.

ID	Applies to	Description
DEV-13060	Conductor	Fixed an issue where Agent hostnames were not being correctly shown for provisioning requests.
DEV-13017	Linux Airwall Agent	Fixed a non-fatal error that occurred when installing Ubuntu package on Debian.
DEV-13007	Airwall Agent	Fixed an issue where we stop sending heartbeat traffic.
DEV-13001	Android Airwall Agent	Fixed an issue where the Android Airwall Agent was sending an incorrect hostname when provisioning.
DEV-12944	Conductor	Clarified routing conflict alerts
DEV-12939	Airwall Gateway	Fixed an issue where the noUnderlayNetwork status was not set properly. This resulted in the "No underlay network" status never being displayed on LCD screens of the Airwall Gateway-400 or -500.
DEV-12932	Conductor	Fixed an issue where an Airwall Gateway generates routing alerts for east-west policy across two overlay port groups having the same subnet and overlay IP.
DEV-12906	Conductor	Fixed an issue in device activity reporting.
DEV-12892	Conductor	When there are no relay probe diagnostic results, a message now indicates that it is because the Airwall Gateway is not a member of any relay rules. Furthermore, fixed an issue where a value in the diagnostic data was misidentified as latency. In reality, this value is a score used to determine which relay to use. A lower score is better.
DEV-12882	Conductor	Airwall Gateways that use stand-alone underlay port group configurations now reboot on link failure if the reboot feature is enabled.
DEV-12859	Airwall Gateway	Removed extra repeated log messages that occurred when Airwall Gateway-300v did not have a virtual serial port attached.
DEV-12858	Conductor	Fixed an issue where duplicate results in relay probe diagnostic data result from multiple interfaces attempting to connect to the relay. The Conductor now only shows the best results.
DEV-12855	Airwall Gateway	Fixed an issue where when reconfiguring overlay port groups the DHCP server / relay was not restarted.
DEV-12828	Windows Airwall Agent	Fixed an install issue with Windows 32-bit Airwall Agent.
DEV-12778	Windows Airwall Agent	Installation timestamp now fixed in Conductor.
DEV-12755	Conductor	Fixed an issue where User auth overlay membership was not correctly published in all cases when people were added and removed from people groups.
DEV-12731	Conductor	HA-paired relays are now correctly named in the relay probe diagnostic tool.
DEV-12727	Airwall Gateway	Fixed an issue where a relay was giving a “Relay could not find an IPv4 source address" error.

ID	Applies to	Description
DEV-12710	Airshell	Fixed an issue in Airshell where multiple cellular parameters could not be configured in one command.
DEV-12701	Airshell	When using Airshell, if the Airwall Gateway is in Diagnostic Mode, networking is not automatically restarted when configuring underlay address ('conf network') or modem settings ('conf cell').
DEV-12697	Airshell	Fixed an issue where the Airshell log command does not display the log file on virtual Airwall Gateways.
DEV-12684	Conductor	When looking at voucher details, license model names are now in the same format as those on the licensing page.
DEV-12662	Airwall Gateway	Fixed an issue where Airwall Gateways equipped with Quectel cellular modems did not properly report signal strength on the front-panel LEDs.
DEV-12648	Airwall Gateway	Fixed an issue where the Airwall Gateway-150 USB console port USB descriptor reported that the port is AT command capable, causing ModemManager on Debian to probe the port as if it were a modem.
DEV-12608	Airwall Gateway	Fixed an issue in firmware 2.2.3 and 2.2.5 where the SFP LEDs on the Airwall Gateway 150 remain on when the SFP port is not in use in some configurations.
DEV-12566	Conductor	People groups created as a result of logging in via an authentication provider are now part of the PCI log.
DEV-12559	Conductor	In the smart device group dialog, when "Ignore auto-discovered devices until accepted" is turned off, the group now picks up any existing discovered devices that match its rules.
DEV-12505	Conductor	New PCI logs for Airwall Edge Services reconnect support function, starting a PCAP, stopping a PCAP, requesting a support bundle, and requesting a diagnostic report.
DEV-12496	Conductor	Fixed an issue where event actions could have a text display error if you edit one action while editing another.
DEV-12434	Conductor, Airwall Gateway	Now have support for NATing subnet broadcasts on the device network.
DEV-12232	Airshell	The two logins available on both Airwall Gateways and Conductor are "airsh" and "diag". All previous logins have been removed.
DEV-11810	Conductor	The Conductor now displays a more helpful error page for Conductor session timeout.
DEV-11806	Cloud	Cloud Diagnostics page Refresh button now refreshes the Protected Route table.
DEV-11795	Linux Airwall Agent	Fixed an issue where the current profile is not changed as a result of an update.
DEV-11679	Airwall Gateway	Fixed an issue where HA configured Airwall Gateways did not support the overlay DHCP feature after a fail-over.

ID	Applies to	Description
DEV-11408	Android Airwall Agent	Fixed an issue where an Android Airwall Agent failed to connect with peers if it had policy to network objects.
DEV-10081	Conductor	Fixed an issue in the Create Conductor certificate dialog where hitting Enter didn't save the certificate.
DEV-8347	Windows Airwall Agent	Windows Support Bundles are now encrypted.

Known Issues

ID	Applies to	Description
DEV-14197	MacOS Airwall Agent	When you update the macOS Airwall Agent, you may be required to restart. If you do not see the tray icon after the update finishes, restart your Mac to restore operation of the Airwall Agent.
DEV-13944	Airwall Gateway	When a device is disabled it will only stop traffic to other devices on remote Airwall Gateway's. Traffic to bypass destinations will continue. Traffic to other devices on the same Airwall Gateway will not be stopped in some situations.
DEV-13930	Alibaba Cloud Airwall Gateway, Conductor	If you have created a new Alibaba Cloud Airwall Gateway with v2.2.8, there is an issue with the protected subnet id on the Cloud tab actually being the public subnet. **Workaround**: You can avoid this issue by waiting to install the upcoming 2.2.8 hotfix on the Conductor before creating any Alibaba Cloud Airwall Gateways. **Workaround if you have already created an Alibaba Cloud Airwall Gateway**: **1.** Apply this hotfix to your Conductor. **2.** If you are not using an NTP for system time, on the **Settings** page, **General setting** tab, under **System time**, select **Edit Settings**, and then Under **Update date and time**, select **Set browser time** and then select **Update**. **3.** For any cloud Alibaba Airwall Gateways, on the **Cloud** tab, **Diagnostic** subtab, click **Refresh**.

ID	Applies to	Description
DEV-13916	Airwall Gateway	Airwall Gateways running firmware version 2.2.8 will not use a Conductor URI that was previously learned from a DNS SRV record in v2.2.8 or a previous firmware revision. This leaves the Airwall Gateways unable to connect to the Conductor if the Airwall Gateway previously used a DNS SRV record for configuration and is later moved to a network without a Tempered DNS SRV record. Additionally, the Conductor setting that allows you to set the Conductor URI on all managed Airwall Gateways in **Advanced** Settings is not functional when used with DNS SRV record bootstrapping in firmware v2.2.8. **Workaround**: Prior to installing 2.2.8 on Airwall Gateways, install Hotfix-13955. You can then install 2.2.8 on the Airwall Gateways. If you have already installed 2.2.8 on Airwall Gateways and are experiencing this issue, please contact Customer Success for assistance, or you can manually configure the Conductor address in each Airwall Gateway using `airsh` or Diagnostic mode.
DEV-13913	Alibaba Cloud	The 2.2.5 Airwall Gateway image in Alibaba Cloud deploys a 2.2.3 image instead. **Workaround**: After you finish deploying, upgrade the Airwall Gateway to the version you want.
DEV-13887	Windows Airwall Agent or Server	There is a issue on some Windows machines where the Windows Airwall Agent or Server cannot connect, even though ipconfig shows an auto-configured IP address for the Tempered TAP adapter (169.254.*.*), and the Conductor shows the device as online but with no IP address. **Workaround**: Restart the service, or check your Airwall Agent or Server configuration in the Conductor.
DEV-13872	Conductor	When running **Ping all devices** on the Support tab for a HA standby Airwall Gateway, no results are being displayed and the busy status indicator never times out.
DEV-13860	Conductor	If you add a device when multiple port groups are already configured, the Port affinity list defaults to the first overlay port group, but the value set is "Detect automatically." **Workaround**: Edit the device again and change it to set port affinity.
DEV-13846	Conductor	Network admins cannot get the list of CAs and cannot add customer certificates to Airwalls through the UI, because the PKI button is not shown.
DEV-13813	Airwall Gateway 110g	RS-422 / RS-485 functionality is not guaranteed on the Airwall 110 for the 2.2.8 release.

ID	Applies to	Description
DEV-13811	Airwall Gateway	When using an Airwall Gateway to provide high availability across multiple underlay links, do not place multiple interfaces in the underlay port groups or use bypass with routed-only mode disabled.
DEV-13775	Cloud	The Conductor rarely gives a "Net::ReadTimeout" error when you try to deploy an Azure Airwall Gateway 300v or server. This error doesn't indicate that the deployment has failed – go to the Azure portal and check the actual deployment result.
DEV-13760	Conductor	Device page export/import does not export or import Bypass Devices in this release.
DEV-13759	Airwall Gateway	Detect Devices button may incorrectly report devices on attached to other port groups or peer Airwalls if policy permits traffic from an Overlay IP to those destinations.
DEV-13607	Conductor	Creating a link failover group (**Airwalls** -> **Ports** -> **Failover settings**) does not apply the settings to any port groups. This is easy to miss since you have to set the failover group on the ports page.
DEV-13297	Airwall Gateway	When deploying seamless bypass in a layer 2 "bump in the wire" configuration, traffic from the protected device to non-bypass destinations outside of the local subnet does not work as expected. The traffic egresses the remote Airwall Gateway or other port group with the destination MAC address of the local default gateway. Using seamless bypass in layer 2 "bump in the wire" mode to provide remote access to the protected device with and overlay IP and SNAT enabled works as expected.
DEV-13194	Conductor	An Airwall Edge Service's Check Connectivity / Ping Local Devices functionality can fail in Internet Explorer 11 if one of the devices is defined as a CIDR. To fix this, use one of the latest versions of Chrome, Firefox, Safari or Edge.
DEV-12852	Windows Airwall Agent	The Windows Airwall Agent may not connect when multiple interfaces are active This issue can be caused by a Windows default that doesn't allow multiple simultaneous active network interfaces, and prefers ethernet over cellular or WiFi. It can be bypassed by editing a registry value. See the troubleshooting steps in I am having trouble connecting on page 31.
DEV-12744	Airwall Gateway	Customers with Airwall Agents version 2.2.1 or earlier connecting to HA-paired Conductors might not be able to authenticate a user auth session. Recommendation: Upgrade Conductors and Airwall Agents to version 2.2.3 or above. Workaround: After upgrades, if you still see connectivity issues, restart the Airwall Agent.

ID	Applies to	Description
DEV-12692	API Documentation	The API docs navigation section does not work in chrome 80 though it worked on previous versions of chrome. It is still working in Firefox and Safari, so customers should use one of these browsers to view the docs.
DEV-12544	Conductor	If you restore a Conductor using a VM snapshot, and it is part of an HA pair, the Standby must be rebased as the standby. To do this, set the Standby Conductor to Active, and then back to Standby. This generates a new Standby Database.
DEV-12513	Cloud-Azure	Conductor rarely gives a "Net::ReadTimeout" error when user tries to deploy an Azure Airwall Gateway 300v or server. This doesn't indicate that the deployment has failed. If you get this error message, go to the Azure portal and check the actual deployment result.
DEV-12275	OSX Airwall Agent	DNS settings are seen and acted upon, but do not show up in resolver list.
DEV-12264	Airwall Agent	Revoking and then re-activating an Agent on a Conductor before v2.2.8 results in the Agent being unable to reconnect. Restarting the metadata cache on the Conductor resolves this issue.
DEV-11840	Conductor	Attempting to log into a Standby Conductor with an expired password cycles into a recycling change password prompt. If this occurs, log into the Active Conductor to change the password.
DEV-11523	Conductor	In rare cases, the Airwall Edge Services online/offline status graph on the Dashboard might be blank.
DEV-10977	Cloud	If one of the cloud attributes is missing, please reboot the Airwall Gateway by clicking the Airwall Gateway -> Actions -> Reboot.
DEV-10846	OSX Airwall Agent	On OSX Airwall Agents, it may not be possible to stop an ongoing packet capture. **Workaround**: Wait for the capture duration to expire.
DEV-10710	Conductor	Supported platforms for Upgrade are not listed in order in Conductor
DEV-10276	Windows Airwall Agent	Tray Application doesn't start on Server 2008 because .NET fails to install silently.
DEV-8486	Conductor	Clicking the Restart IF-MAP button will log the current user out.
DEV-8120	Conductor	Infrequently, an Azure Airwall Gateway may fail to reconnect to Conductor after firmware upgrade. This can be fixed by going to the Azure portal and restarting the VM the Airwall Gateway resides on. It can take up to 10 or 15 mins to come back online.

Release Notes 2.2.5

Release Date: Apr 17, 2020

What’s New

Support for NAT Subnet Broadcasts	The Airwall Solution now supports NATing subnet broadcasts on the device network.
New Airwall help content	• Airwall Invitations • Renew Expired Licenses • Integrate Third-party Authentication with OpenID Connect • Set up an Airwall Gateway in Microsoft Azure
Updated Airwall help content	• Configure a DHCP relay on an Airwall Gateway • Configure protected devices with DHCP • Route encrypted connections with Airwall Relay • Configure Airwall Relay rules • Install Airwall Server on Linux

Upgrade Considerations

Consider upgrading to 2.2.5 if:

You were impacted by any issues discovered in prior releases, especially if you have any of the following:
Heavy use of broadcast/multicast traffic.
Applying a new ports configuration resulted in overlay ports staying down until next reboot.
Tunnel failures after cellular outages.

Fixes

ID	**Applies to**	**Description**
DEV-13132	Conductor	Improved validation of Conductor device imports.
DEV-13087	Android Airwall Agent	Fixed an issue where user was unable to log in with user auth on Android.
DEV-13086	Conductor	Airwall port configuration changes made from the Conductor are now noted in the PCI user activities log
DEV-13067	Android Airwall Agent	Fixed Push-to-Talk not working on Android over Cellular.
DEV-13065	Android Airwall Agent	Fixed Android issue with sending User Auth credentials causing crashes.

ID	Applies to	Description
DEV-13031 DEV-12954	Conductor	Agent hostnames are now being shown correctly for provisioning requests.
DEV-13027	Conductor	Added new PCI logs for Airwall reconnect support function: Starting a PCAP, stopping a PCAP, requesting a support bundle, and requesting a diagnostic report.
DEV-13002 DEV-12938	Airwall Gateway	Fixed an issue that caused the reboot setting in the underlay Failover Settings tab to have no effect if any underlay port groups were configured as standalone.
DEV-12998 DEV-12930	Conductor	Fixed an issue that could cause the packet capture feature in the old Conductor support tab to show no capture interfaces.
DEV-12997	Conductor	Fixed an issue that could cause serial-over-IP to be come unresponsive after cellular outages.
DEV-12996	Conductor	Fixed an issue to allow users to request multiple support bundles at the same time.
DEV-12995 DEV-12871	Conductor	Fixed a bug that could cause HIP tunnels to become stale after temporary cellular outages.
DEV-12994 DEV-12866	Conductor	Some event actions have a target box. Filtering the target box by name is now working. Additionally you can select "+ more" to see more entries at the same time.
DEV-12992 DEV-12083	Conductor	Fixed a UI error when modifying the recipient list of an existing alert.
DEV-12991	Android Airwall Agent	Fixed Android Airwall Agent sending localhost as the hostname in its provisioning request.
DEV-12984	Airwall-75 Airwall-150 Airwall-250	Fixed an issue where applying certain types of port configurations caused the overlay ports fail to link up until the next reboot of the Airwall. Note: This issue may still occur in a configuration where only VLAN-tagged ports are assigned to overlay port groups. To work around this, ensure that at least one untagged port is assigned to an overlay port group.
DEV-12964	Airwall Gateway	Fixed a bug that caused the reporting interval settings to have no effect on device activity reporting.
DEV-12903	Conductor	Fixed an issue where syslog didn’t configure the first time on a new Conductor.
DEV-12748	Conductor	Fixed an issue where an Airwall may crash when processing a large amount of broadcast traffic with many tunnels.

Known Issues

ID	Applies to	Description
DEV-13028	Airwall Gateway	Airwall Gateway 150 has "could not detect attached switch" error. **Workaround**: Do a hard reboot.

Release Notes 2.2.3 Hotfix

Release Date: Mar 27, 2020

What's New

2.2.3 Hotfix	This is a hotfix to release v2.2.3. See the Release Notes 2.2.3 for more additions in version 2.2.3.

Upgrade Considerations

We recommend that you upgrade to this 2.2.3 hotfix if you were impacted by issues with the Windows or macOS Airwall Agents.

Note: If you're looking for the previous Tempered Networks Technical Documentation, most is included in the new Airwall Help. You can also click the link on the Airwall Help home page to get to the pre-2.2.3 Help.

Fixes

ID	Applies to	Formerly Known As	Description
DEV-12954	Conductor		Agent hostnames were not being correctly shown for provisioning requests.
DEV-12938	Airwall Gateway	HIPswitch	We fixed an issue that caused the reboot setting in the underlay link manager to have no effect if any underlay port groups were configured as stand-alone.
DEV-12930	Conductor		We fixed an issue that could cause the packet capture feature in the Conductor support tab to show no capture interfaces.
DEV-12871	Conductor		We fixed a bug that could cause HIP tunnels to become stale after temporary cellular link failures.
DEV-12866	Conductor		Some event actions have a target box. Filtering the target box by name is now working. Additionally you can select "+ more" to see more entries at the same time.
DEV-12852	Windows Airwall Agent	HIPclient-Windows	Windows Airwall Agent wasn't handling re-address during interface (for example, cell to wi-fi) changes
DEV-12803	Conductor		UI error when modifying the recipient list of an existing alert.
DEV-12755	Conductor		User auth overlay membership was not correctly published in all cases when people were added and removed from people groups.

Known Issues

See Release Notes 2.2.3 on page 688 for known issues.

Release Notes 2.2.3

Release Date: Feb 6, 2020

Introducing Tempered Airwall

Tempered's fully encrypted, virtual air-gap network security solution is now called Airwall. Our product offerings are also changing to match our brand and make their functions clearer.

What’s New

New Airwall help

If you're looking for the previous Tempered Networks Technical Documentation, most is included in the new Airwall Help. You can also click the link on the home page to get to the pre-Airwall Help.

OpenID Connect support for Airwall Agents

We have added OpenID Connect support for authenticating remote sessions on Android, iOS and macOS Airwall Agents (formerly Android, iOS, and OSx HIPclients). There is also now a global option to lock out clients that do not support user auth.

People groups as Overlay members/managers

People Groups are now able to be members of Overlay Networks as well as Managers of Overlay Networks. Now user permissions can be configured entirely in an authentication provider such as LDAP or OpenID Connect via people group membership.

Lockdown Mode

Lockdown Mode is now configurable from the Airwall Conductor for Airwall Agents (formerly HIPclients) that support this feature (currently supported by the Windows Airwall Agent).

Cloud Linux Airwall Servers

The Airwall Conductor can create and deploy Linux Airwall Servers directly in any cloud provider, such as Azure, AWS, or Google.

Upgrade Considerations

We recommend that you upgrade to 2.2.3 if:

You want to use any of the following features:	You were impacted by any issues discovered in prior releases, especially if you have any of the following:
Multifactor Authentication	• A large number of spokes causes network issues • Issues with NTPD (Network Time Protocol daemon) not running on Conductor • Broadcast traffic not forwarded across Overlay network

Important: If you are using SHA-1 for the ESP transform, you should convert to SHA-256 before upgrading to 2.2.x.

IMPORTANT: Migrating existing Deployments to 2.2.x

The 2.2.2 release brought a significant change to the base platform configuration and capabilities of an Airwall Gateway/HIPswitch. Conductors after 2.2.2 will not be able to manage Airwall Edge Services prior to version 2.0. See the note in the Release Notes 2.2.2 on page 697 for information on upgrading Airwall Edge Services prior to version 2.0.

Fixes

ID	Applies to	Formerly Known As	Description
DEV-12852	Windows Airwall Agent	HIPclient-Windows	Windows Airwall Agent wasn't handling re-address during interface (for example, cell to wi-fi) changes
DEV-12683	Airwall Gateway	HIPswitch	Fixed an issue where large firmware update packages would sometimes fail to be installed via Conductor, Diagnostic mode, and airsh (hipsh).
DEV-12613	Airwall Gateway-250	HIPswitch-250	Fixed an issue where port 8 (SFP portion) of the Airwall Gateway-250 does not get re-enabled after reconfiguring network interfaces. This issue affects firmware versions 2.2.0, 2.2.1, and 2.2.2.
DEV-12582	iOS Airwall Agent	HIPapp-iOS	iOS Airwall Agent - 2x 'Sign-in Failed' pop up for invalid username & password
DEV-12579	iOS Airwall Agent	HIPclient-iOS	iOS Airwall Agent not using 'DNS domain' from Conductor
DEV-12528	Android and iOS Airwall Agents	HIPclient-Android HIPclient-iOS	Android and iOS Airwall Agents user auth status pages are not getting updated on toggling policies
DEV-12510	Android Airwall Agent	HIPclient-Android	Android and iOS Airwall Agents user auth status pages are changing session expire time according to the current time of the phone.
DEV-12487	Android Airwall Agent	HIPclient-Android	Android Airwall Agent user auth Notification showing symbols instead of profile name
DEV-12468	Android Airwall Agent	HIPclient-Android	Android Airwall Agent crash on overlay networks page when you click refresh with no peers
DEV-12463	Conductor		Syslog setting appears disabled after upgrade while it is still enabled
DEV-12441	Linux, macOS, and Windows Airwall Agents OpenHIP	HIPclient-Linux, HIPclient-OSX HIPclient-Win	Mac, Linux and Windows Airwall Agents now use and select an optimal relay when the underlay interface is set to 'auto'.
DEV-12404	Airwall Gateway-150	HIPswitch-150	A new cellular modem firmware (version 02.33.03.00) is available for Airwall Gateway-150 with the SFF-MOD-MC7430 modem. Please see the downloads page.
DEV-12399	OpenHIP		Reject ARP responses for loopback, multicast, broadcast and 0.0.0.0
DEV-12382	Conductor		Airwall Edge Services online bar graph displays, then goes blank.
DEV-12376	Conductor		HTTP 422 error for some accounts after 2.2.1 > 2.2.2 Conductor upgrade.
DEV-12373	iOS Airwall Agent	HIPclient-iOS	iOS status page seems to not be updating

ID	Applies to	Formerly Known As	Description
DEV-12355	OpenHIP		Broadcast IP packets not traversing tunnel properly
DEV-12353	Airwall Gateway-150	HIPswitch-150	Some Airwall Gateway-150s with part numbers (PLF-) ending in -02 and -03 were shipped with non-functional SFP ports due to a firmware bug. This is fixed in firmware version 2.2.3. Additionally, a hotfix is available to address this issue in firmware versions 2.1.6, 2.1.7, 2.2.0, 2.2.1, and 2.2.2.
DEV-12339	Airwall Gateway-150	HIPswitch-150	A regression in firmware versions 2.2.0, 2.2.1, and 2.2.2 caused Airwall Gateway-150s to be unable to link with dual-speed or BiDi SFP/SFP + modules. Support for these SFPs is fixed in firmware 2.2.3.
DEV-12326	Conductor		Airwall Edge Services fail to reconnect to Conductor after re-provisioning
DEV-12318	Android Airwall Agent	HIPclient-Android	Android not using 'DNS domain' from Conductor
DEV-12311	Airwall Gateway	HIPswitch	Fixed an issue that was causing serial or modbus configured overlay ports to stop working after performing a reconnect.
DEV-12301	Airwall Gateway	HIPswitch	Fixed a bug that caused Airwall Gateways to lose their Conductor connection after installing a customer certificate requiring a reboot.
DEV-12293	Airwall Gateway	HIPswitch	Modbus-RTU times out when multiple sessions are connected from one host.
DEV-12287	Airwall Gateway-500	HIPswitch-500	Fixed a bug that caused some IP broadcasts on the overlay network to cross into different subnets.
DEV-12285	macOS Airwall Agent	HIPclient-OSX	Mac unable to log in via username and password after switching to a different profile
DEV-12276	Conductor		Do not allow a non-editor to be the rule editor of a Smart Device Group.
DEV-12241	iOS Airwall Agent	HIPclient-iOS	iOS needs to initiate pings for other side to reach it
DEV-12230	Airwall Gateway	HIPswitch	Do not remove port group configs during port detection
DEV-12219	OpenHIP		When processing concurrent traffic to or from multiple peers anAirwall Gateway may drop traffic for some tunnels.
DEV-12217	Airwall Invitations	HIPinvite	Poor messaging of license sync errors during invite activation
DEV-12214	Conductor		Monitor alert (flapping) settings do not result in an indication of frequent alerts
DEV-12205	Conductor		Not able to remove NTP on the Standby

ID	Applies to	Formerly Known As	Description
DEV-12187	Conductor		Airwall Edge Services uptime graph units scale incorrectly
DEV-12179	Conductor		Deleting SoIP/Modbus settings when a description is edited
DEV-12167	Conductor		Remove tags and end remote session on revoke
DEV-12159	Conductor		Doesn't log device traffic reported by High-Availability standby
DEV-12146	Windows Airwall Agent	HIPclient-Win	Windows Airwall Agent takes a very long time to appear in Conductor dashboard after license is granted
DEV-12127	OpenHIP		Detect unidirection traffic through tunnels which may indicate an extremely rare issue that causes tunneled traffic to be be lost and attempt to recovery tunnel by initiating a rekey
DEV-12104	Conductor		Change license pop up blocking functionality to a temporarily dismissible banner
DEV-12096	Airwall Gateway	HIPswitch	Address Marvell WiFi "mwifiex" driver CVEs: CVE-2019-3846, CVE-2019-14814, CVE-2019-14815, CVE-2019-14816, and CVE-2019-14895
DEV-12093	Android Airwall Agent	HIPclient-Android	Add DNS setting back to Android and iOS Airwall Agents
DEV-12092	Airwall Gateway-150	HIPswitch-150	Airwall Gateway-150 not maintaining HIP tunnels when configured with more than 10 peers
DEV-12090	OpenHIP		In previous versions, HIP would buffer packets during the base exchange. This has been removed to mitigate a potential DoS from a local protected device, almost all protocols will re-transmit making the buffering unnecessary. If you encounter issues with esoteric protocols, please turn on auto-connect so the tunnels are brought up automatically.
DEV-12077	Airwall Gateway	HIPswitch	If fail-safe reboot is enabled in the Failover settings, the Airwall Gateway reboots whenever the initial reboot timeout is expired (assuming all links failing) ignoring the timeout for recurring reboot.
DEV-12076	Conductor		Invalid license vouchers shouldn't prevent customers from loading new valid vouchers
DEV-12075	Licensing		Customer cannot remove invalid licenses due to license deficit
DEV-12024	Airwall Gateway-150	HIPswitch-150	Fixed a bug that was causing validation errors in the port configuration UI after factory-reseting and re-connecting an Airwall Gateway to the same Conductor.

ID	Applies to	Formerly Known As	Description
DEV-12005	Conductor		Device Match Rules rule "include Any Object without certain tag" does not include untagged devices
DEV-12004	Conductor		Device Match Rules "negative filter MAC_prefix" filters out devices without MAC address
DEV-12000	Conductor		Offline Airwall Agents are named incorrectly in Add Device to Network popup
DEV-11994	Conductor		Replacing Airwall Agent in Conductor doesn't update its capabilities
DEV-11992	Conductor	Conductor	Conductor breaks when upgrading to from 2.2.1 to 2.2.2 in a factory reset state.
DEV-11991	Airwall Gateway	HIPswitch	Fixed an issue that causes dropped packets when traffic from the same MAC address is received on multiple ports of the same Airwall Gateway (regardless of the port group membership of those ports).
DEV-11982	Conductor		The auto-generated Lockdown Mode Device Group doesn't appear to match new Airwall Gateways coming online.
DEV-11969	Conductor		NTPD terminates and won't come back.
DEV-11968	Cloud		Delay and fetch userdata causes slow Conductor refresh
DEV-11951	Conductor		Notifications Controller Validation failed: MTU must be greater than or equal to 100 when no MTU provided by 2.2.2 HIPapp
DEV-11900	Airwall Gateway	HIPswitch	Modbus-RTU does not work correctly when Overlay NAT is enabled.
DEV-11898	Android and iOS Airwall Agents	HIPclient-Android, HIPclient-iOS	Unable to establish any Overlay connections with Android and iOS Airwall Agent
DEV-11893	Android Airwall Agent	HIPclient-Android	Scale views on Overlay and Services page in Airwall Agent
DEV-11887	Android Airwall Agent	HIPclient-Android	In Add Profile, error remains after you correct the field
DEV-11881	Conductor		Keep user auth timeout within the range of 1 hour to 1 year
DEV-11867	Airwall Gateway	HIPswitch	Ruggedcom: Cannot enter diagnostic mode from hipsh (now airsh)
DEV-11864	Airwall Gateway-150	HIPswitch-150	Fixed an Airwall Gateway-150 issue where the cellular LED indicators did not function properly following the first reboot after inserting the AW-150 cellular module.
DEV-11858	Conductor		End Remote Session button activity is missing from PCI user activities

ID	Applies to	Formerly Known As	Description
DEV-11844	Conductor		Blank Provider name for OpenID connect leads to blank dropdown list item
DEV-11830	Conductor		Able to authenticate user auth using expired password
DEV-11829	Conductor		Unable to log in legacy users without email
DEV-11824	Conductor		Deleting the people group doesn't remove the tag from the Airwall Edge Services
DEV-11823	Android and iOS Airwall Agents	HIPclient-Android, HIPclient-iOS	Prevent users from clicking multiple times on Login and Sign in
DEV-11819	macOS Airwall Agent	HIPclient-OSX	Doing anything in the macOS Airwall Agent closes your user auth session
DEV-11815	Conductor		Add notice or block transparent mode when multiple overlay port groups are configured.
DEV-11807	Airwall Gateway	HIPswitch	Ping all devices on High-Availability Standby in failover mode
DEV-11804	Cloud		Route injection was not performed on Conductor reboot or upgrade
DEV-11794	Linux Airwall Agent	HIPclient-Linux	WiFi scanning is now available on the Linux Airwall Agent
DEV-11785	Conductor		Conductor should remove remote session button on disabling global user auth
DEV-11778	Airwall Gateway	HIPswitch	HTTP GET overlay monitor confused when multiple port groups
DEV-11772	iOS Airwall Agent	HIPclient-iOS	iOS Airwall Agent user auth alert icon on Dashboard doesn't work on click
DEV-11769	iOS Airwall Agent	HIPclient-iOS	iOS Airwall Agent not getting overlay device IP updates
DEV-11733	Conductor		Airwall Gateway High-Availability, you get incorrect status after failover: primary Airwall Gateway status reports OK (tunneling)
DEV-11732	Airwall Gateway-150	HIPswitch-150	Fixed an issue where Quectel cellular expansion modules would sometimes fail to connect to AT&T's LTE network and instead fall back to 3g / UMTS.
DEV-11727	Licensing		Denied license request not cleared after import of synced encrypted package
DEV-11698	Airwall Gateway-300v HA	HIPswitch-300v	Airwall Gateway-300v High-Availability member went offline after removing High Availability settings

ID	Applies to	Formerly Known As	Description
DEV-11684	Conductor		Starting concurrent packet captures on the same Airwall Gateway appears to work, then fails with "An error occurred communicating with the server"
DEV-11680	Android Airwall Agent	HIPapp-Android	Airwall Agent Invitations Decline and Conductor hidden in landscape view
DEV-11677	Conductor		Conductor ports config permits network address as overlay IP
DEV-11656	Airwall Gateway-150	HIPswitch-150	In firmware versions 2.2.0, 2.2.1, and 2.2.2, a regression caused the link LEDs for Airwall Gateway-150 port 5 (SFP) to not operate when port 5 is assigned to an Overlay port group. This is fixed in firmware version 2.2.3. Note: The SFP port LEDs turn on and stay solid when the Airwall Gateway has not been managed in a Conductor. This issue will be addressed in a future release.
DEV-11651	Conductor		Airwall Gateway Ports page doesn't display IP or MAC address after configuring
DEV-11645	Conductor		OpenID user auth login requires re-authentication
DEV-11516	Conductor		Device import allows device with arbitrary name/ description length
DEV-11499	iOS Airwall Agent	HIPclient-iOS	iOS Airwall Agent shows LSI for NAT'd devices on overlay networks page
DEV-11470	Airwall Agents Airwall Servers	HIPclients HIPservers	Changing overlay IP conf. back to NAT requires Airwall Agent restart
DEV-11459	Conductor		iOS Airwall Agent doesn't show up on Conductor
DEV-11343	Airwall Gateway	HIPswitch	The port detection part of hardware detection was made more reliable, for upgrades and during each boot on certain platforms.
DEV-11103	Conductor		A device's port group can now be seen and edited from the Airwall Gateway's "local devices" tab.
DEV-11013	macOS Airwall Agent	HIPclient-OSX	Switching profile doesn't forget about user auth sign-in
DEV-10960	macOS Airwall Agent	HIPclient-OSX	If you add wrong credentials for user auth on macOS, it won't ask you to enter again
DEV-10887	Linux Airwall Server	HIPserver-Linux	Linux Airwall Server DNS server settings do not seem to have any effect
DEV-10665	macOS Airwall Agent	HIPclient-OSX	macOS 10.15 requires app notarization by default
DEV-10592	Cloud-Azure		do not require reboot to get the route table ID
DEV-10555	Cloud-AWS		Better user error for auth failure due to time difference

ID	Applies to	Formerly Known As	Description
DEV-9927	Linux, macOS, and Windows Airwall Agents Airwall Gateways	HIPclient-Linux HIPclient-OSX HIPclient-Win HIPswitch	Mac Airwall Agent receives routes for disabled overlays
DEV-9857	iOS Airwall Agent	HIPclient-iOS	do not allow access to private key when phone is locked
DEV-9253	Conductor		Smart Device Groups will not add Airwall Agents and Airwall Servers using tag matches.
DEV-9204	Conductor		Airwall Gateway Underlay IP NAT field shouldn't accept CIDRs
DEV-9122	macOS Airwall Agent	HIPclient-OSX	macOS Airwall Agent publishes IP of random interface as an Underlay IP
DEV-8929	Windows Airwall Agent	HIPclient-Win	Tray app doesn't start after unattended install
DEV-8742	Conductor		Add better error messaging for the initial Conductor voucher failures

Known Issues

ID	Applies to	Formerly Known As	Description
DEV-12744	Airwall Gateways	HIPswitches	Customers with Conductor HA and Airwall Gateways version 2.2.1 or earlier might see connectivity issues when using User Authentication. Recommendation: Upgrade Conductors and Airwall Gateways to version 2.2.3 Workaround: After upgrades, if you still see connectivity issues, restart the primary Conductor.
DEV-12710	airsh	hipsh	Customers need to update each cell value individually when using airsh to configure the cell modems
DEV-12697	airsh	hipsh	The console command "airsh log" does not display the log file on a virtual Airwall Gateway. The 300v log file is now located at /etc/asguard/system/messages.
DEV-12692	API		The API docs navigation section does not work properly in Chrome v80. Use Firefox or Safari to view the API docs.
DEV-12645	Android Airwall Agent	HIPClient-Android	When creating a new profile and starting the app for the first time there is a chance the "Upgrade Needed" page will be displayed. This is an error and the user should simply click cancel and start the app again. This may only happen the first time you create the profile.

ID	Applies to	Formerly Known As	Description
DEV-12521	Airwall Gateway	HIPswitch	TPM usage is disabled by default for all Airwall Gateways due to the amount of time it takes to complete an RSA signature and frequency of RSA signatures when connected via a relay. This will be addressed in a future version.
DEV-12513	Cloud Azure		Conductor occasionally gives "Net::ReadTimeout" error when user tries to deploy an Azure Airwall Gateway 300v or server. This doesn't indicate that the deployment has failed. Go to the Azure portal and check the actual deployment result.
DEV-12303	macOS Airwall Agent	HIPclient-OSX	Upgrading macOS Airwall Agent from 2.2.1 to 2.2.3 requires uninstalling the 2.2.1 Airwall Agent, installing the 2.2.3 Airwall Agent, and replacing the old profile with new profile on Conductor.
DEV-12290	macOS Airwall Agent	HIPclient-OSX	User approval needed to complete macOSAirwall Agent installation. From macOS High Sierra onwards, you need to allow the system extension com.tempered.tuntaposx.tap, or simply tap.kext, required by the Airwall Agent. In the System Preferences, on the **Security and Privacy** page, open the **General** tab. Where it says system software was blocked from loading, click **Allow**. macOS only shows this allow message for a limited time (30mins). The installer will wait for you to allow the extension.
DEV-12268	Conductor		Firmware version on Conductor is not getting updated until macOS Airwall Agent is restarted
DEV-11578	Android Airwall Agent	HIPclient-Android	Do not change the LSI prefix to match a peer address.
DEV-9542	iOS Airwall Agent	HIPclient-iOS	Cannot generate a Support Bundle from the Conductor for an iOS Airwall Agent when the Conductor is in High Availability mode. You can instead generate a Support Bundle from the iOS Airwall Agent

Older Release Notes

Release Notes for versions 2.1.2 through 2.2.2.

Note: For v2.0.3 and earlier, see pre-2.2.3 Tempered Webhelp for release notes for earlier versions.

Release Notes 2.2.2

Release Date: October 18 , 2019

IMPORTANT: Customers using LDAP on Conductor 2.2.1

If you are using LDAP and running Conductor version 2.2.1, you must upgrade your Conductor to 2.2.2, to resolve an issue that could prevent you from logging in to the Conductor.

IMPORTANT: Migrating existing Deployments to 2.2.2

The 2.2.2 release brings a significant change to the base platform configuration and capabilities of a HIPswitch. HIPswitch versatility is dramatically increased. To achieve this, we had to give up some functional interoperability between version 2.2.2 and prior versions of HIPservices and Conductor. Also, Conductor 2.2.2 will no longer be able to manage HIPservices prior to version 2.0. While most things still work across versions 2.1.x and 2.2.2 during your upgrade, we recommend that 2.2.x deployments migrate completely as soon as possible using the following order:

1. If your Conductor is running a version earlier than 2.1.6, upgrade it to 2.1.6 or 2.1.7
2. If any HIP Services are running a version earlier than 2.1.6, upgrade them to 2.1.6 or 2.1.7
3. Verify that your Conductor and all HIP Services you updated in steps 1 and 2 are running 2.1.6 or later
4. Upgrade your Conductor to 2.2.2
5. Upgrade your HIP Services to 2.2.2

For more information on upgrading your Conductor to 2.1.6 from prior versions, log in to your account and select the **Documentation Center** link at the top-right of the page. You should review both the **Release Notes 2.1.6** and **Conductor and HIP Service Upgrades** pages.

What's New

Cloud Marketplace

You can now purchase a Tempered Networks cloud-based Conductor or HIPswitch directly from the Azure or Google marketplace. This greatly simplifies the purchase and deployment of Conductors and HIPswitches in your own cloud account and the setup of an independent license-ready environment.

User-Configurable LSI Prefix

You can now change the LSI prefix from 1 to another digit usage the Conductor's **Advanced Global HIPservice Settings**. This is useful if you have underlay network traffic that uses the 1.x.x.x range of addresses, which is routable on the Internet and prevalent in Asia-Pacific regions. You may choose any suitable prefix (routable or non-routable) given the distribution of your HIP Services globally. For details on routable traffic ranges, please see RFC 1918.

Android and iOS HIPclients Updated for 2.2

You can now manage Android and iOS HIPclients using the new 2.2 features, such as network objects.

Custom Overlay Policy with People Groups

People groups can be used with HIPclient and HIPserver authentication to create custom overlay network policies based on the user authenticating via the HIPclient or HIPserver. Tags specified in the people group will be added to a HIPclient or HIPserver, when a member of the people group authenticates and will be removed automatically once the session ends. The tags can be used in smart device groups to give the HIPclient or HIPserver custom overlay network policies.

Windows Client Multi-Factor Authentication (MFA)

OpenID Connect is now integrated into the Windows HIPclient and HIPserver authentication workflow. If enabled via an OpenID Connect provider, users will be required to use MFA to gain overlay access. Other HIPclient platforms will integrate client MFA for overlay access in future releases.

HIPclient and HIPserver Authentication Session Timeouts

Administrators can now configure how long a HIPclient or HIPserver authentication session will last, either globally or specific to a HIPclient or HIPserver.

Conductor Connection Failsafe

HIPswitches now have a watchdog monitor for the Conductor connection that will force a re-connect if it determines the current connection is unresponsive or missing. This should allow HIPswitches to reconnect in more cases without requiring human intervention (e.g. manual rebooting or other diagnostic activities that can require physical access to the HIPswitch).

More Resilient HIP Tunnels

HIP tunnel processes have been improved so that when a stale tunnel is detected, which may occur after reboots or carrier failures, it is rebuilt.

More Resilient Cellular Connectivity

Under certain circumstances (signal strength, cell-tower location, interruptions), Verizon based HIPswitches would experience frequent modem resets resulting in an occasional failure to recover. This release has safeguards to ensure that cellular connectivity is restored after these episodes.

OSX HIPclient no longer supports El Capitan with 2.2.x

If you are using the mac HIPclient on El Capitan, you should not upgrade to 2.2 until you upgrade the OS.

Upgrade Considerations

We recommend that you upgrade to 2.2.2 if:

You want to use any of the following features:	You were impacted by any issues discovered in prior releases, especially if you have any of the following:
• Multiple Overlays • Multiple Underlays • Port Groups • Network Objects • Automatic policy creation based on user type • Ability to change the LSI for regional compatibility • Windows User auth MFA	• Cellular carrier connection issues • Modbus GUI settings or connectivity • HS-100 connectivity issues • Use the 1.0.0.0/8 network address space • Network capture on Conductor 500

Important: If you are using SHA-1 for the ESP transform, you should convert to SHA-256 before upgrading to 2.2.1.

Fixes

ID	Applies to	Description
DEV-11660	HIPswitch	A second serial port is now available for use with the SoIP feature. The Serial over IP (SoIP) feature was previously not functional on the HIPswitch 400 Series and virtual HIPSwitches. Starting in version 2.2.2, the second serial port is available for use with the SoIP feature.

ID	Applies to	Description
DEV-11631	Conductor	Fixed a firewall problem causing blocked serial connections when configured to use the Modbus communications protocol
DEV-11623	Conductor	Fixed an issue causing HIPswitches upgraded from 2.1.x while in Transparent Mode to lose their underlay network configuration, preventing them from reconnecting to the Conductor.
DEV-11596	Conductor	HIP Service online/offline alert messages now report how long they have been offline/online.
DEV-11444	Conductor	Fixed an issue where IPv4 addresses in the **HIPswitch certificate conflict** dialog displayed incorrectly.
DEV-11397	HIPrelay	Fixed an issue specific to the Telstra mobile network that prevented a HIPservice from connecting to its peers via a HIPrelay.
DEV-11389	Conductor	Fixed an issue where setting a HIPservice attribute rule in a Smart Device Group could prevent you from modifying HIPservice fields.
DEV-11355	Conductor	Fixed an issue where Spanning Tree Protocol was automatically enabled regardless of the previous setting during a HIPswitch upgrade.
DEV-11347	Conductor	Fixed an issue where user authentication token validation could fail if a HIPservice failed over multiple times between HA-paired Conductors.
DEV-11324	HIPswitch, Cellular	Fixed an issue where a HIPSwitch-250, or HIPswitch 150 with an NL7588 type module, could take an extended period of time to register on the Verizon network.
DEV-11318	Diagnostic mode	Changing the IP address of the Conductor no longer causes diagnostic mode to lose connection with the Conductor, however settings are no longer applied immediately. **Note**: You are prompted to restart the Conductor to apply the new network settings.

ID	Applies to	Description
DEV-11317	Conductor	Fixed an issue where typing in a voucher code in lowercase when provisioning a Conductor could cause errors after re-syncing with the provisioning server.
DEV-11256	Conductor	Fixed an issue where the Snort frequency and port group setting would not be set when selected for the first time.
DEV-11218	HIPclient, Android	Fixed an issue where HIPclient profile data would not be updated when the Conductor initiates a configuration change.
DEV-11184	Conductor, Hyper-V	Conductor now correctly sets the primary interface IP address to the default 192.168.56.2 on first boot.
DEV-11169	HIPswitch, Virtual	Virtual machine host time synchronization on a HIPswitch no longer produces Conductor reconnects.
DEV-11150	Conductor	The HIPswitch the customer has access to is the only one that is disabled and not the one they can not edit.
DEV-11073	Diagnostic mode	Changed the Diagnostics Port tab to display Port # instead of ETH #.
DEV-11026	BaseOS	Updated BaseOS to OpenWrt 18.06.4. The CVEs addressed by this release are listed under **Security Fixes**at https://openwrt.org/releases/18.06/changelog-18.06.4
DEV-10985	Conductor	Device match rules are now correctly serialized in the PCI device groups reference.
DEV-10947	Conductor	EU-north-1 region is now supported in 2.2.2.
DEV-10940	OpenHIP	TCP maximum segment size (MSS) clamping is implemented to better support traffic from clients.
DEV-10866	Conductor	Fixed an issue where you could add non-relay HIPservices to a relay HIPservice group.
DEV-10804	Conductor, PCI	The PCI log will now show details of deleted policies by default.

ID	Applies to	Description
DEV-10803	Conductor	Fixed an issue where some PCI log entry details – including firmware updates to HIPservices -- were displayed incorrectly in the user activities report.
DEV-10796	Conductor	Improved the functionality of API index filtering and sorting.
DEV-10776	Conductor	Fixed an issue where checking if a HIPservice was online triggered a **HIPservice online** monitor event.
DEV-10743	Conductor	The session expired message on the login page now only displays when appropriate.
DEV-10737	Conductor	You can now toggle a users network membership off after toggling it on.
DEV-10719	Conductor	Fixed an issue where opening and closing the Conductor Proxy settings could save an empty value, causing the Conductor to fail to communicate with the license server.
DEV-10701	Conductor	The port group list in the **ping/ traceroute** drop-down will now contain each overlay port group and a single underlay option (since it is bridged) for 2.2.x HIPservices on pre 2.2 switches.

ID	Applies to	Description
DEV-10660	Conductor, Cloud	Improved the route injection option to eliminate additional user actions. The new behavior is as follows: Route injection deletes all routes if you: • Create a new credential provider with route injection disabled • Update the route injection option from enabled to disabled • Delete the existing credentials with route injection enabled Route injection adds all routes if you: • Create a new credential provider with route injection enabled • Update a route injection from disabled to enabled Route injection will not be performed if you: • Update credentials without changing the route injection option • Delete existing credentials with route injection disabled
DEV-10613	Conductor	Improved sorting of the **Device** and **Device Groups** pages.
DEV-10597	Conductor	Fixed an issue where cellular graphs displayed incorrect units.
DEV-10361	Diagnostic mode	Diagnostic mode should now display "None" if no part number file is found.
DEV-10186	HIPshell	The **Run mode** shown under the **hipsh** *status* command now shows major operating modes first. Minor operating modes are shown in parenthesis, in gray text.
DEV-9903	Conductor, 500 Series	The Conductor 500 is now able to run packet captures.
DEV-9577	HIPclient, iOS	Fixed an issue where you needed to deny VPN requests multiple times before the correct page appeared.
DEV-9470	HIPclient, Windows	Fixed an issue where **hipctl** *profile create* did not create profiles successfully.
DEV-9088	Conductor	LDAP groups are now case-insensitive.

ID	Applies to	Description
DEV-9043	Conductor	The Delete button no longer displays next to your own account on the **People** page.
DEV-8659	Conductor, 100 Series	Fixed an issue where the Conductor displayed an incorrect time for the HIPswitch 100g cellular.
DEV-5607	Conductor	Fixed bug where pushing large amounts of data through a HIPrelay caused the byte-count to appear as a negative number. The numbers now present as positive.

Known Issues

ID	Applies to	Description
DEV-11491	Conductor	Event Monitor of type *HIP tunnel* does not allow you to specify monitored peers. Workaround: None
DEV-10846	HIPclient, macOS	Currently, you cannot stop a packet capture once initiated from the Conductor UI for a macOS HIPclient. Workaround: Wait for the packet capture operation to terminate.
DEV-10764	HIPswitch, Cellular	When downgrading the HS-150 from 2.2.0 to 2.1.6, the cellular link LEDs may not be functional. Workaround: In order to restore LED functionality, in Conductor, change the "Underlay network" settings under the "Ports" tab. For example, adjust the priority. (Note that you may need to provide the "Access point name (APN)" since that field may appear blank, in order to successfully apply the settings.) After applying the settings, reboot the HS-150 for the Cellular LEDs to become functional again.
DEV-10703	Conductor	If a HIPswitch is factory reset, its details may not be removed from the Conductor UI. Workaround: none.

ID	Applies to	Description
DEV-10618	Conductor	When downloading a support bundle, the dialog box contains two buttons, **Download** and **Cancel**. **Cancel** has the same effect as closing the dialog. Workaround: None.
DEV-10602	HIPswitch 400, HIPswitch 500	The HIPswitch 400 and HIPswitch 500 LCD menus do not support setting Conductor host names longer than 16 characters. Workaround: Configure the corresponding IP address instead.
DEV-10577	HIPshell	Currently, the hipsh console will not timeout and may become locked. Workaround: Reboot or power-cycle the HIPswitch.
DEV-10492	HIPrelay	Once a HIPrelay learns an IPv4 / IPv6 address for a peer, it will continue to use that address indefinitely for forwarding peer packets). If the peer is offline and doesn't update its address with the HIPrelay, the old or invalid address will continue have HIP control packets forwarded to it. Workaround: None
DEV-10442	Conductor	In rare cases, the **Apply Firmware Updates** dialog will show duplicate entries in the **Upgrade Available** drop-down. Workaround: None.
DEV-10404	OpenHIP	Retransmitted HIP I1 packets are only sent using one source address/ destination pair. This differs from the initial I1 packets which attempt to use all source/destination address combinations. This issue occurs on multi-homed HIPswitches, with peer-auto connect turned on and relay probes off. Workaround: None.

ID	Applies to	Description
DEV-10276	HIPclient/HIPserver, Windows	The tray application crashes repeatedly and prevents the configuration of the HIPclient or HIPserver. Workaround: Reinstall .NET to resolve the issue.
DEV-10236	Conductor	If you log in to multiple software HIP Services as the same user, the remote session for the first HIP Service will be terminated. Workaround: None.
DEV-10200	Conductor UI	Currently, users with the Network Administrator role in the Conductor can see and grant provisioning requests but are unable to view license vouchers and make top level licensing changes. Workaround: None.
DEV-10109	HIPclient, Windows	When uninstalling the HIPclient or HIPserver, the tray icon may disappear, and the application will restart. This occurs without selecting **Yes** or **No** from the dialog. Workaround: None.
DEV-10081	Conductor	When creating a Conductor certificate using the **Create Conductor Certificate** dialog, you must click **Save**. Pressing *Enter* will result in an error and the operation will not complete successfully. Workaround: None.
DEV-10078	Conductor	Currently, HIPswitch reporting graphs do not indicate temperatures below freezing. Workaround: None.

ID	Applies to	Description
DEV-10047	HIPclient, macOS	he HIPclient may lose access to the macOS keychain following an update. Workaround: If this occurs, use the procedure below to resolve the issue. 1. Open the finder by pressing **Command-N** 2. Find the **TemperedNetworksHIP** application, right click it and select **Show Package Contents** 3. Double-click **Contents** 4. Double-click **MacOS** 5. Keep this window available, you will need it below 6. Start Keychain Access (**Applications > Utilities > Keychain Access**) 7. Navigate to the **System** keychain (on the upper left) 8. Click on **Keys** (on the lower left) 9. Click on the header named **Kind** to sort the keys 10. For each private key with the name **com.temperednetworks** do the following: a. Double-click the item to open it b. Click **Access Control** c. Enter your password d. Click the + e. Drag the tnw-hipd from the window opened earlier and drop it into the window you opened by tapping + f. Click tnw-hipd, then click **Add** - the window will close g. Click **Save Changes** h. Make a note of your username, you will need this in a moment. i. Enter your password and tap **Allow** j. You will be prompted to enter your username and password. Do so and close the **com.temperednetworks window.** Repeat step 10 for each private key named **com.temperednetworks**. You will have one key for each HIPclient profile you created.

ID	Applies to	Description
DEV-9877	Conductor, Azure, wireless HIPswitch	Link Manager default settings do not work between Conductors running on Azure using the Azure Network Security Group setting and wireless HIPswitches. Workaround: You must **Disable pings on active link** on each Wireless HIPswitch or set an alternate active ping target (e.g. 8.8.8.8).
DEV-9808	Conductor	You must be a manager of every overlay that contains any device associated with all HIPservices in a HIP Service group, otherwise you lose the ability to make edits to that HIP Service group. There is no error message or any explanation as to why you are not allowed to make edits. Workaround: None.
DEV-9688	Conductor	The HIPswitch **Limit Bandwidth**setting currently displays as bytes per second instead of bits per second. Workaround: None.
DEV-9606	HIPswitch 150 Series	When connected via serial console to a HIPswitch 150, pasting text ~35+ characters into the console requires the console to be disconnected and reconnected to restore functionality. Workaround: None.
DEV-9362	Conductor	In tag properties, if you enter a month value in the **Expire tag usage** field, such as 1M, it is converted to weeks and days when the change is applied. Workaround: None
DEV-8929	HIPclient, Windows	After installing a windows HIPclient using the unintended install method, the tray application does not start. Workaround: Start the application manually after installation is complete

ID	Applies to	Description
DEV-8810	HIPswitch, Cellular	Diagnostic mode displays a drop-down menu for selecting a preferred radio access technology, however the backend does not correctly handle this setting. Workaround: None.
DEV-8806	HIPclient, HIPserver	Client authentication does not display an error message when authentication fails due to the absence of a Conductor connection. Workaround: None
DEV-8805	HIPswitch	When enabling SNAT on a HIPswitch, new connections will begin to use the overlay gateway IP address of the HIPswitch, but existing connections will not use the SNAT address until the connection is idle for the specified connection TTL or if the HIPswitch is rebooted. Workaround: Reboot the HIPswitch after enabling SNAT.
DEV-8428	Conductor, HA	The time on a standby Conductor and master conductor can become out of sync and cause missing traffic stats and health data from HIPswitches. Workaround: When failing-over an HA-paired Conductor, verify that the timestamps are the same.
DEV-8120	Conductor, Azure	In rare cases, an HIPswitch running in Azure may fail to reconnect to the Conductor after a firmware upgrade. Workaround: Restart the HIPswitch VM. Please note it can take up to 10-15 minutes to come back online.
DEV-8106	Conductor	If a device stops communicating, the Conductor UI may not reset the activity display to gray, reporting online status incorrectly. Workaround: Reload the browser.
DEV-8060	Conductor	In rare cases, a Conductor HA pair may stop syncing. Workaround: If this occurs, promote the HA-secondary to primary, then re-pair them.

ID	Applies to	Description
DEV-7955	Conductor	Pinging an Azure-hosted HIPswitch from another HIPswitch will fail in the Conductor UI. This is due to ICMP being denied by Azure's security groups. Workaround: None
DEV-7769	HIPswitch, Google Cloud	Toggling policy too quickly on a HIPswitch running on Google Cloud can result in the route table becoming out of sync when using route injection. Workaround: After toggling policy, wait 10 seconds before toggling it again.
DEV-7735	HIPclient, HIPserver, All platforms	HIPclients and HIPservers are currently not compatible with 1.1.1.1 DNS service. Workaround: None
DEV-7499	Conductor	The bandwidth check in the HIPswitch **Diagnostics** tab may fail for HA-paired HIPswitches. Workaround: None.
DEV-6927	Conductor	If you place a Conductor in diagnostic mode and have a non-standard port configuration defined, it may not respond to ping commands. The diagnostic mode functionality should be otherwise unaffected. Workaround: None.
DEV-5866	HIPswitch	When configuring Wi-Fi settings in diagnostic mode, the HIPswitch may override the configuration on reboot if Wi-Fi configuration was configured in the Conductor previously. Workaround: Factory reset the HIPswitch before entering diagnostic mode.

Release Notes 2.2.1

Release Date: September 16 , 2019

IMPORTANT: Migrating existing Deployments to 2.2

The 2.2 release brings a significant change to the base platform configuration and capabilities of a HIPswitch. HIPswitch versatility is dramatically increased. To achieve this, we had to give up some functional interoperability between version 2.2 and prior versions of HIP Services and Conductor. Also, Conductor 2.2 will no longer be able to manage HIP Services prior to version 2.0. While most things still work across versions 2.1.x and 2.2 during your upgrade, we recommend that 2.2.x deployments migrate completely as soon as possible using the following order:

1. Upgrade your Conductor to 2.1.6
2. Upgrade all HIP Services to 2.1.6
3. Before proceeding, ensure you have no MAP1 clients
4. Upgrade HIP Services to 2.2.1

For more information on upgrading your Conductor to 2.2.1 from prior versions, review Conductor and HIP Service Upgrades.

What's New

HIP Tunnel Monitoring

New in this release is the ability to monitor HIP tunnel state changes directly. You can configure a monitor to watch the HIP tunnel to a particular remote HIP Service or to all trusted peer HIP Services. As with all monitors, you can create actions on events to alert, change policies, etc.

HIP tunnel stats graph

The tunnel stats introduced in 2.1.5 for HIP relays is now available for all HIP Services. You can see Tx and Rx bits between any pair of HIPswitches, allowing you to troubleshoot underlay and overlay connectivity issues.

OpenID Connect

Conductors now support OpenID Connect as an external authentication provider type. You can now use an Identity and Access Management tool such as Okta or OneLogin and integrate Single Sign-On (SSO) or Multi-Factor Authentication (MFA) support.

Multiple Underlay Networks

We now support active/standby multi-homed wired and wireless uplinks, even allowing communication between different ISPs. Multiple Underlay Networks give you more control over which link handles HIP tunnels and which link handles connection to the Conductor.

Multiple Overlay Networks

We now support isolation between port groups. Each overlay port group has its own overlay IP, static routes, and related network settings. Each overlay port group bridges its interfaces, but communication between port groups requires policy.

Portgroup Configuration

The **HIPswitch** > **Ports** user interface has been completely overhauled to enable the configuration of multiple underlay and overlay port groups. Several things that were configured in different places in 2.1.x are now consolidated in one location:

- Port group
- Port role
- Link Manager settings
- Wi-Fi
- Cellular

- 802.1q VLAN tags
- Overlay IP/Netmask

Interfaces appear on the screen with live status information from the HIP Service. Also, all configurations are committed only after the HIP Service validates and successfully implements the changes, eliminating disagreement between what is configured in the Conductor and what is actually implemented in the HIP Service.

Network Objects

You can now use a CIDR (like 10.3.5.0/24) instead of a /32 for a device address. The term **Network Objects** simply refers to a device that uses a CIDR, and this device can be used wherever you would use any other device, like in device groups and overlay networks. Using network objects, you can allowlist an entire IP network in one click. This should make policy migration from Firewalls and Routers during new deployments much easier. Site-to-site VPN becomes trivial. More specific policies are still supported, so you can create wide policies to open general site-to-site traffic and still segment traffic to HIP Services.

Negative policies are also supported so you can allow networks or individual IP addresses (like a router) and then create exceptions using a negative policy (like a firewall).

This makes it much easier to manage HIP Services. Configurations become simpler, shorter, and easier to maintain. For cloud-based HIP Services, route injection is much simpler because routes are summarized.

User Auth (Windows, Mac, Android; iOS to release shortly)

MacOS and Android now support the user authentication feature introduced in 2.1.3 Windows clients and HIPservers. OS will support this feature in a later release. This feature allows an admin to require client users to provide an additional factor of authentication, currently username and password, to access the overlay for a period of time. Since usernames and passwords are centrally managed, this mitigates concerns about stolen laptops or devices, giving an admin a centrally managed way to approve and deny overlay access.

New shell for HIPswitches (hipsh)

New in this release is **HIPshell**, a console that replaces the special login user accounts such as like *mapconfig*, *macinfo*, and *factory reset*. HIPshell provides tab-completion, inline help, and greatly expands your ability to deploy & configure a HIP Service directly without going into diagnostic mode.

Overlay Intrusion Prevention Monitor (snort)

Intrusion Prevention allows you to activate any number of pre-defined rule sets. Traffic on the overlay is inspected and if a rule matches, an event is created and sent to the Conductor. You can define event actions based on Snort events.

HIPswitch Latency improvements

On certain platforms with a single CPU core, the data plane latency has been reduced from 7ms to approximately 2ms. However, it is important to note that the reduction in latency can vary and depends on concurrency, packet sizes, and various other factors, but in general the latency through a HIP Service is reduced.

HIP relay Performance improvements

In version 2.2, we improved the speed of HIP relay traffic using XDP acceleration, allowing HIP traffic to scale even more on your existing hardware.

Full tunnel Windows clients and HIPservers

In prior releases, a client or HIPserver needs policies to opt-in to the overlay network, the default being *split tunnel*. In version 2.2, an administrator can check a box on the client or HIPserver in the Conductor to make the default *full tunnel and* capture all network traffic into the overlay, allowing for a few exceptions that may be in the underlay like DNS, AD, etc. Please note this is Windows only; macOS clients and Linux HIPservers will be available in a future release.

Multiple VLAN Tags per interface

We now support trunk ports, allowing you to have two or more VLANs configured on an interface. Each VLAN tag makes a new sub-interface. For example, VLAN tag 25 on eth0 creates a virtual interface named eth0.25. These interfaces can go into various port groups. East-West policies in the Conductor can be built between devices in different VLANs. Please note that you can still create bridges between VLANs as you did in version 2.1.x and earlier.

MAPv1 no longer supported

Conductor version 2.2 and beyond will no longer be able to manage HIP Services running 2.0 and earlier. Please note that this requires you to upgrade your HIP Services to version 2.0 or later your Conductor to version 2.2. Review the upgrade section at the beginning of this document for more information about the recommended upgrade process.

Dual-use port mode deprecated

Dual-use mode for interfaces is no longer available. Using multiple port groups and trunk ports, it is now much easier to implement split-tunnel with East-West policies. You can add the DNS, AD, and other servers as protected devices to a HIP Service and give them a separate overlay port group connected to the underlay network. In Conductor, you can then give your protected devices policy to the DNS, AD, etc., servers.

Upgrade Considerations

We recommend that you upgrade to 2.2.1 if:

You want to use any of the following features:	You were impacted by any issues discovered in prior releases, especially if you have any of the following:

• Multiple Overlays • Multiple Underlays • Port Groups • Network Objects	Note: Due to the large number of changes in this release, we recommend you continue to use 2.1.x unless you need one or more of the new features described above.

Important: If you are using SHA-1 for the ESP transform, you should convert to SHA-256 before upgrading to 2.2.1.

Note: You may upgrade HIPswitches to 2.2.1 provided you are running Conductor 2.2.1. Prior versions do not properly manage HIPswitch 2.2.1.

Fixes

ID	Applies to	Description
DEV-11194	Conductor	Fixed a bug where performing a Factory Reset on a HIPswitch keeps the event monitors targeted at device groups or HIP Service groups.
DEV-11144	Conductor	Fixed an issue where policy data would become out-of-sync for HIP Services that had multiple-policy connections when the remote HIP Service is revoked.
DEV-11080	Cloud	Fixed a bug where a Conductor-reboot now performs the route injection to sync the route table.
DEV-11028	Diagnostic mode	Fixed an issue where newer firmware silently failed to install from Diagnostic Mode.
DEV-10981	API	Fixed the paginated API endpoints.
DEV-10962	Conductor	Fix regression in 2.2.0 where smart device groups CIDR and IP range match rules with "only match overlay device IP" selected did not select the correct devices.
DEV-10955	Conductor	Fixed a bug that caused Access Point Name (APN) changes for Cellular Ports not to have any effect. Also APN settings from 2.1.x HIP Services will be set correctly when firmware-upgrading a HIPswitch to 2.2.
DEV-10953	Diagnostic Mode	The APN setting is now only configurable through the platform config under Port > Settings. This setting is available from both Diagnostic Mode and the Conductor UI.

ID	Applies to	Description
DEV-10931	HIPswitch	Included an output message informing the customer that Authentication failed.
DEV-10927	HIPswitch, Cellular	Fixed an issue that when the only active port groups are disabled, a customer will have to put the HIPswitch into Diagnostic Mode to recover it.
DEV-10913	HIPserver, Linux	Added Readme and License files and is now present on the disk.
DEV-10909	HIPswitch	Fixed a bug where the Conductor prevented the secondary HIPswitch in a HA pair from upgrading.
DEV-10905	HIPserver, Linux	A support URL was corrected for hip.service a systemd file.
DEV-10899	client/HIPserver, Windows	Fixed a bug where 'ipconfig /release', 'ipconfig /renew' - now works and NTP is able to synchronize system time DHCP broadcast is able to find DHCP server).
DEV-10898	HIPswitch-100	Fixed the ability for the HIPswitch to maintain Peers' File Information about the Peer involved in the policy.
DEV-10854	HIPswitch	When trying to configure a HS-500 and HS-400-202 in an HA pair, customers will no longer get an error the HA ports are moved to the HA portgroup. You no longer have to reboot the HIPswitch.
DEV-10847	Conductor	There was an inconsistency in connectivity when a HIP Service has a device deleted from a monitored device group. HIP Service now maintains connection to the Conductor.
DEV-10826	HIPswitch	HIPswitch-250 SFP Ports 1,2,7, and 8 work at 100 and 1000 mbps speeds in 2.2.1.
DEV-10823	HIPswitch	Fixed a bug that required customers to disable Transparent Mode before attempting to enter Diagnostic Mode.
DEV-10807	Diagnostic mode	Added the Media settings back in. It now exists in the Port Configuration section. This column should only show up on a HS 250.
DEV-10797	Conductor	Fixed non-functional bandwidth check button on the Secure Tunnels Diagnostics page.

ID	Applies to	Description
DEV-10792	HIPswitch	You are able to delete and add new DHCP server settings after configuring them.
DEV-10737	Conductor	A refresh of the browser restores proper functionality.
DEV-10726	HIPclient, macOS	Fixed the ability to uninstall the app from the **About** > **Uninstall** menu item. Additionally, you can continue to use a Command prompt: *sudo /Applications/TemperedNetworksHIP.app/Contents/Resources/uninstall.sh*
DEV-10720	Conductor, omapd	Fixed the ability to create a New Profile, a second time around, on the same Conductor.
DEV-10702	Conductor	The HIPswitch details page now displays the correct icon in the **Underlay IP** field, such as a Wi-Fi icon when the connection is wired.
DEV-10692	Conductor	On cell-connected HIP Services, cell details show on the Ports page as soon as they are available.
DEV-10640	HIPswitch	Able to set and maintain Conductor and Peers IP address to invisible when engaging 'Publish IPs to Conductor' to No.
DEV-10619	HIPswitch, Cellular	Fixed a USB driver issue that prevented reliable recovery from Cellular Modem Firmware crashes.
DEV-10575	Conductor	Fixed a bug that could prevent users from saving Overlay DHCP settings.
DEV-10548	Conductor	Fixed a bug where, in rare cases if a monitor is invalidated, it would never try running again.
DEV-10489	API	Fixed an issue where generating a token using basic authentication for a locally authenticated user required the username to be case sensitive. This is no longer the case.
DEV-10437	Conductor	Fixed an issue where the macOS HIPclient was missing packet statistics.
DEV-10435	Conductor	Fixed an issue where importing devices using a malformed *.CSV file would stop responding and provide an incorrect error message.

ID	Applies to	Description
DEV-10391	HIPswitch 150, Cellular	Fixed an issue where, when applying power to the HIPswitch 150, while the micro USB console port was connected to a computer, the HIPswitch would fail to enable power to the expansion bay.
DEV-10361	HIPswitch 100, HIPswitch 500	This issue is fixed for the HS 100. The diagnostic mode now display *None* if no part number file is found. This will be the case for the 100 and any other HS that does not write a part number.
DEV-10342	HIPswitch	Removed syslog-ng syntax check from init script, now syslog and udhcp start concurrently, this should allow entropy generation from network interrupts.
DEV-10356	Conductor	Fixed an issue where the **+ more entries** link in the **Edit Tags** dialog would not function correctly.
DEV-10210	HIPclient/HIPserver, Windows	Upgraded to the latest versions of openssl and curl used by the Windows HIPclient and HIPserver.
DEV-10163	HIPswitch	Fixed an issue where a broadcast storm occurred when multiple HIPswitches on same L2 broadcast domain received packets from a protected device.
DEV-10136	HIPclient, macOS	The HIPclient local device ID key file permissions have been adjusted to only allow user access.
DEV-10107	Conductor	Improved the error message to clearly indicate when the Conductor cannot access the licensing server.
DEV-10039	HIPswitch	Fixed an issue where HIPswitch-150 Ethernet ports would not enumerate correctly during the boot up sequence.

ID	Applies to	Description
DEV-10023	Conductor	If you have a virtual Conductor configured with a boot drive less than 1gb in size, you will need to increase the size to 1GB or larger before Conductor version 2.2 will install. The following links provide instructions for resizing a virtual disk: · VMware reference: https://kb.vmware.com/s/article/1004047 · Hyper-V reference: https://docs.microsoft.com/en-us/powershell/module/hyper-v/resize-vhd?view=win10-ps **Note**: Azure, AWS, and Google Cloud Conductors already have their boot drive set to 1GB. This issue will only affect those with EXSi or Hyper-V Conductors.
DEV-9994	Conductor	Improved the error messages the Conductor adds to syslog for HIPswitches.
DEV-9993	Cloud, Google	Fixed an issue when deploying a cloud HIP Service where the **Public network (VPC)** drop-down would display networks with no subnets.
DEV-9922	Conductor	Cellular information now displays correctly in **Ports** > **Underlay network**.
DEV-9880	OpenHIP	Fixed an issue where a HIP Service could not establish tunnels with other HIP Services if the Conductor time was adjusted to an earlier value. This could happen when enabling NTP on the Conductor for the first time.
DEV-9876	OpenHIP	Fixed an issue where HIP would crash and restart when broadcast/multicast packets were sent on a busy HIPswitch having a large number of tunnels.
DEV-9867	Conductor	Fixed an issue where HIPrelay tunnel stats were not stored in the database for HIPswitches while the tunnel was forming or disconnecting.
DEV-9845	Cloud, AWS	Fixed an issue where machine types other than t2.nano displayed incorrectly as a micro instance.

ID	Applies to	Description
DEV-9841	Conductor	Improved the error message when creating a Cloud HIP Service and no custom images exist for the account.
DEV-9772	HIPclient, Windows	Fixed an issue where the HIPclient would not prompt for credentials if the computer was restarted.
DEV-9715	Conductor, API	The API now displays a 403 response code rather than a 401 response code when permissions for the request are incorrect or missing.
DEV-9694	Conductor, API	The API now displays correct response codes when creating endpoints.
DEV-9673	Conductor, API	When destroying endpoints, invalid IDs are now ignored.
DEV-9665	HIPswitch	Fixed an issue where health data may not be properly disabled when changing the setting from the Conductor UI.
DEV-9531	Cloud, Azure	Fixed an issue where the **Image ID** field would not display the correct images when the region was changed
DEV-9511	Conductor	Fixed an issue where the **Forgot your password?** link would not send out an email if an LDAP username was provided.
DEV-9404	Conductor, API	Removed the 406 return code from the API documentation as it is not used.
DEV-9398	HIPclient, Windows	Reduced the possibility of the HIPclient tray icon remaining in the notification area when the client is terminated or uninstalled.
DEV-9392	Conductor	Fixed an issue where a HIP Service offline event may not be triggered if **Check Online** is used between the time a HIPswitch unexpectedly disconnects and a session timeout occurs.
DEV-9339	HIPswitch 75 Series	Resolved issues related to CPU frequency scaling on the HIPswitch 75.
DEV-9322	BaseOS	Fixed an issue where SFP ports 1 and 2 on the HIPswitch-250 did not link without 1000baseX auto-negotiation enabled on the connected switch.

ID	Applies to	Description
DEV-9300	HIPctl	Improved the error message received when requesting a log file and it does not exist.
DEV-9159	Conductor	Fixed an issue where dropping a user who is a rule editor of a Smart Device Groups caused the group to stop functioning. The Smart Device Group will now downgrade to a standard device group to prevent possible loss of service due to permissions violations.
DEV-9157	HIPclient, macOS	Agent GUI talks to the control daemon start-up to kill existing instances of the tnw-hipd daemon that it is supposed to control.
DEV-9123	HIPswitch 250	No longer dropping packets when both the fiber and copper ports of a combo port are connected.
DEV-9122	HIPclient, macOS	Fixed an issue where setting the HIPclient Network selector to **auto** could result in selecting the wrong interface, if more than one was available.
DEV-9085	HIPclient, macOS	Fixed an issue that caused the control daemon to crash on shutdown.
DEV-9078	HIPclient, macOS	Fixed an issue where a support bundle could not be created support bundle due to insufficient permissions.
DEV-9006	Conductor	Added more descriptive error messages due to incorrect credentials when creating cloud providers in the Conductor UI.
DEV-8804	HIPctl	Added more descriptive text to error messages received when trying to modify a profile that doesn't exist.
DEV-8633	Conductor	Regenerating an API token now requires the user to provide authentication credentials.
DEV-8561	Cloud	Added a warning message to **Cloud > Diagnostics** when there are no cloud provider credentials available for the HIP Service.

ID	Applies to	Description
DEV-8529	Conductor	Currently, you cannot remove email and syslog settings in the Conductor once they are configured. Workaround: You can work around this issue by entering invalid values in the settings fields, click the disable button, or delete the settings using the API.
DEV-8294	Conductor	Improved syslog **device_event** messages to provide more useful information.
DEV-8262	Cloud, AWS, Google	Fixed an issue when deploying a HIP Service on AWS or Google Cloud where the route table was unavailable if the default region in the cloud connector was different from the HIP Service's region.
DEV-8203	Conductor	Fixed an issue in the Conductor UI where pop-up information boxes would not disappear, resulting in multiple boxes on the screen.
DEV-8202	HIPserver, Linux	Fixed an issue where a newly created profile would not be set as the default profile after completing the HIPserver installation.
DEV-8105	HIPclient, Windows	Improved the **HIP Networks View** to display the Overlay name instead of the ID.
DEV-8085	HIPclient, HIPserver	HIPclients and HIPservers are now blocked from accepting inbound Overlay connections when an Overlay IP is not set.
DEV-8051	Conductor	Port addresses are displayed in 2.2.0.
DEV-8044	Conductor	Fixed an issue where selecting the refresh button for either cellular configurations on the **Ports > Underlay** network page would trigger both refresh buttons.
DEV-8012	Conductor	In rare circumstances, the traffic stat graph values can be off by a factor of 1000. If this occurs, refresh your browser.
DEV-7968	Conductor	Fixed an issue where authenticating with LDAP credentials logged the user out of the Conductor sessions.

ID	Applies to	Description
DEV-7956	Conductor	Fixed a display issue where deleting the primary port would result in the secondary cellular interface not displaying an IP address.
DEV-7955	Conductor, Azure	If you ping an HIPswitch running Azure from another HIPswitch, the ping will now connect to the Conductor UI. This is due to ICMP being allowed by Azure's security groups.
DEV-7919	Conductor	In previous versions of the product, if a discovered device was added to a smart device group and caused an IP conflict, the device was not detected. This behavior has been improved and device will now be detected but not added to the smart device group.
DEV-7774	HIPctl	The output from hipctl has been improved. On the command line the error and status messages are now simplified for clarity, and detailed output is sent to syslog.
DEV-7720	Conductor	Fixed an issue where the **+ more entries** link did not function correctly when selected.
DEV-7681	HIPclient, Windows	The HIPclient has been updated to improve protection against possible local threats.
DEV-7661	Conductor	Fixed an issue where after replacing a HIPswitch, it could take several minutes to reconnect and appear online in the Conductor.
DEV-7507	Conductor	Upgraded our current products to support OpenSSL, version 1.1.0.
DEV-7233	Conductor	Fixed an issue where the Conductor displayed an erroneous message if the login timed-out and the user attempted to log in again without refreshing the browser.
DEV-7063	HIPclient, Windows	Added a new HIPclient control window for easier access to the HIPclient features. You can access this window by left-clicking on the tray icon.
DEV-5607	Conductor	Fixed a cosmetic issue where when pushing large amounts of data through a HIPrelay can cause the byte-count to appear as a negative number.

ID	Applies to	Description
DEV-5713	Conductor	In rare cases, a shared network traffic graph may fail to draw data for the Conductor 400 if the 10G option card is installed. Reboot the Conductor to refresh.

Known Issues

ID	Applies to	Description
DEV-10887	HIPserver, Linux	Configuring DNS servers for a Linux HIPserver via the Conductor may not retain the settings once saved. Workaround: None.
DEV-10857	OpenHIP	Under certain conditions, a HIP Service may take up to 30 seconds to probe its active relays. This may result in longer initial connection delays. Workaround: None
DEV-10846	HIPclient, macOS	Currently, you cannot stop a packet capture once initiated from the Conductor UI for a macOS HIPclient. Workaround: Wait for the packet capture operation to terminate.
DEV-10764	HIPswitch, Cellular	When downgrading the HS-150 from 2.2.0 to 2.1.6, the cellular link LEDs may not be functional. Workaround: In order to restore LED functionality, in Conductor, change the "Underlay network" settings under the "Ports" tab. For example, adjust the priority. (Note that you may need to provide the "Access point name (APN)" since that field may appear blank, in order to successfully apply the settings.) After applying the settings, reboot the HS-150 for the Cellular LEDs to become functional again.
DEV-10703	Conductor	If a HIPswitch is factory reset, its details may not be removed from the Conductor UI. Workaround: none.

ID	Applies to	Description
DEV-10696	HIPswitch	A Conductor and multi-homed HIPrelay is incompatible with 2.1.x HIPswitches and HIPclients and will cause potential connectivity issues. Workaround: None.
DEV-10618	Conductor	When downloading a support bundle, the dialog box contains two buttons, **Download** and **Cancel**. **Cancel** has the same effect as closing the dialog. Workaround: None.
DEV-10602	HIPswitch 400, HIPswitch 500	The HIPswitch 400 and HIPswitch 500 LCD menus do not support setting Conductor host names longer than 16 characters. Workaround: Configure the corresponding IP address instead.
DEV-10592	HIPswitch, Azure	If you deploy a HIPswitch using a script instead of the Conductor UI and have not configured the user credentials for the cloud provider before granting a license, it is likely you will need to reboot the HIPswitch as the route table ID will be missing in the cloud attribute. Workaround: Deploy the HIPswitch using the Conductor UI.
DEV-10577	HIPshell	Currently, the hipsh console will not timeout and may become locked. Workaround: Reboot or power-cycle the HIPswitch.
DEV-10492	HIPrelay	Once a HIPrelay learns an IPv4 / IPv6 address for a peer, it will continue to use that address indefinitely for forwarding peer packets). If the peer is offline and doesn't update its address with the HIPrelay, the old or invalid address will continue have HIP control packets forwarded to it. Workaround: None
DEV-10442	Conductor	In rare cases, the **Apply Firmware Updates** dialog will show duplicate entries in the **Upgrade Available**drop-down. Workaround: None.

ID	Applies to	Description
DEV-10405	OpenHIP	When sending HIP I1 packets to all peer addresses, a HIPswitch will try all source/destination address combinations and does not query the routing table. This may cause I1 packets to be sent to the wrong interface, because the source address may not match the interface address. This issue occurs on multi-homed HIPswitches, with peer-auto connect turned on and relay probes off. Workaround: None.
DEV-10404	OpenHIP	Retransmitted HIP I1 packets are only sent using one source address/ destination pair. This differs from the initial I1 packets which attempt to use all source/destination address combinations. This issue occurs on multi-homed HIPswitches, with peer-auto connect turned on and relay probes off. Workaround: None.
DEV-10276	HIPclient/HIPserver, Windows	The tray application crashes repeatedly and prevents the configuration of the HIPclient or HIPserver. Workaround: Reinstall .NET to resolve the issue.
DEV-10236	Conductor	If you log in to multiple software HIP Services as the same user, the remote session for the first HIP Service will be terminated. Workaround: None.
DEV-10200	Conductor UI	Currently, users with the Network Administrator role in the Conductor can see and grant provisioning requests but are unable to view license vouchers and make top level licensing changes. Workaround: None.
DEV-10186	HIPshell	The **Run mode** shown when using the *hipsh status* command may contain multiple operating modes. This is normal and not indicative of any issue. Workaround: None.

ID	Applies to	Description
DEV-10109	HIPclient, Windows	When uninstalling the HIPclient or HIPserver, the tray icon may disappear, and the application will restart. This occurs without selecting **Yes** or **No** from the dialog. Workaround: None.
DEV-10081	Conductor	When creating a Conductor certificate using the **Create Conductor Certificate** dialog, you must click **Save**. Pressing *Enter* will result in an error and the operation will not complete successfully. Workaround: None.
DEV-10078	Conductor	Currently, HIPswitch reporting graphs do not indicate temperatures below freezing. Workaround: None.

ID	Applies to	Description
DEV-10047	HIPclient, macOS	The HIPclient may lose access to the macOS keychain following an update. Workaround: If this occurs, use the procedure below to resolve the issue. **1.** Open the finder by pressing **Command-N** **2.** Find the **TemperedNetworksHIP** application, right click it and select **Show Package Contents** **3.** Double-click **Contents** **4.** Double-click **MacOS** **5.** Keep this window available, you will need it below **6.** Start Keychain Access (**Applications > Utilities > Keychain Access**) **7.** Navigate to the **System** keychain (on the upper left) **8.** Click on **Keys** (on the lower left) **9.** Click on the header named **Kind** to sort the keys **10.** For each private key with the name **com.temperednetworks** do the following: **a.** Double-click the item to open it **b.** Click **Access Control** **c.** Enter your password **d.** Click the + **e.** Drag the tnw-hipd from the window opened earlier and drop it into the window you opened by tapping + **f.** Click tnw-hipd, then click **Add** - the window will close **g.** Click **Save Changes** **h.** Make a note of your username, you will need this in a moment **i.** Enter your password and tap **Allow** **j.** You will be prompted to enter your username and password. Do so and close the **com.temperednetworks window.** Repeat step 10 for each private key named **com.temperednetworks**. You will have one key for each HIPclient profile you created.

ID	Applies to	Description
DEV-9877	Conductor, Azure, wireless HIPswitch	Link Manager default settings do not work between Conductors running on Azure using the Azure Network Security Group setting and wireless HIPswitches. Workaround: You must **Disable pings on active link** on each Wireless HIPswitch or set an alternate active ping target (e.g. 8.8.8.8).
DEV-9853	Diagnostic mode	In diagnostic mode, if you set a static IP address using either the subnet ID or the broadcast address for a configured subnet there is no warning this setting is invalid. Workaround: None. (Replaced by the platform configuration).
DEV-9808	Conductor	You must be a manager of every overlay that contains any device associated with all HIP Services in a HIP Service group, otherwise you lose the ability to make edits to that HIP Service group. There is no error message or any explanation as to why you are not allowed to make edits. Workaround: None.
DEV-9688	Conductor	The HIPswitch **Limit Bandwidth**setting currently displays as bytes per second instead of bits per second. Workaround: None.
DEV-9606	HIPswitch 150 Series	When connected via serial console to a HIPswitch 150, pasting text ~35+ characters into the console requires the console to be disconnected and reconnected to restore functionality. Workaround: None.
DEV-9362	Conductor	In tag properties, if you enter a month value in the **Expire tag usage** field, such as 1M, it is converted to weeks and days when the change is applied. Workaround: None

ID	Applies to	Description
DEV-8929	HIPclient, Windows	After installing a windows HIPclient using the unintended install method, the tray application does not start. Workaround: Start the application manually after installation is complete
DEV-8810	HIPswitch, Cellular	Diagnostic mode displays a drop down menu for selecting a preferred radio access technology, however the backend does not correctly handle this setting. Workaround: None.
DEV-8805	HIPswitch	When enabling SNAT on a HIPswitch, new connections will begin to use the overlay gateway IP address of the HIPswitch, but existing connections will not use the SNAT address until the connection is idle for the specified connection TTL or if the HIPswitch is rebooted. Workaround: Reboot the HIPswitch after enabling SNAT.
DEV-8428	Conductor, HA	The time on a standby Conductor and master conductor can become out of sync and cause missing traffic stats and health data from HIPswitches. Workaround: When failing-over an HA-paired Conductor, verify that the timestamps are the same.
DEV-8120	Conductor, Azure	In rare cases, an HIPswitch running in Azure may fail to reconnect to the Conductor after a firmware upgrade. Workaround: Restart the HIPswitch VM. Please note it can take up to 10-15 minutes to come back online.
DEV-8106	Conductor	If a device stops communicating, the Conductor UI may not reset the activity display to gray, reporting online status incorrectly. Workaround: Reload the browser.
DEV-8060	Conductor	In rare cases, a Conductor HA pair may stop syncing. Workaround: If this occurs, promote the HA-secondary to primary, then re-pair them.

ID	Applies to	Description
DEV-7769	HIPswitch, Google Cloud	Toggling policy too quickly on a HIPswitch running on Google Cloud can result in the route table becoming out of sync when using route injection. Workaround: After toggling policy, wait 10 seconds before toggling it again.
DEV-7499	Conductor	The bandwidth check in the HIPswitch **Diagnostics** tab may fail for HA-paired HIPswitches. Workaround: None.
DEV-6927	Conductor	If you place a Conductor in diagnostic mode and have a non-standard port configuration defined, it may not respond to ping commands. The diagnostic mode functionality should be otherwise unaffected. Workaround: None.
DEV-5866	HIPswitch	When configuring Wi-Fi settings in diagnostic mode, the HIPswitch may override the configuration on reboot if Wi-Fi configuration was configured in the Conductor previously. Workaround: Factory reset the HIPswitch before entering diagnostic mode.

Release Notes 2.1.7

Release Date: November 11, 2019

Tempered Networks has released 2.1.7 which is intended to be the last of the 2.1.x releases. This release addresses, exclusively, maintenance and stability issues for the Conductor & HIPswitch and provides enhanced security.

What's New

New in this release:

Upgrade HIPswitch and Conductor to OpenSSL 1.1	OpenSSL 1.0 goes out of support at the end of 2019. This is a proactive upgrade to the new version of the library.
Conductor Connection Failsafe	HIPswitches now have a watchdog monitor for the Conductor connection that will force a re-connect if it determines the current connection is unresponsive or missing. This should allow HIPswitches to reconnect in more cases without requiring human intervention (e.g., manual rebooting or other diagnostic activities that can require physical access to the HIPswitch).

Conductor database consistency checker	Conductors now periodically check for and repair data consistency issues. This improves the reliability of the system and should allow more issues to be resolved without human intervention.

Upgrade Considerations

The 2.1.7 release includes all hotfixes from prior releases and addresses all known support cases at the time of release.

You may upgrade HIPswitches to 2.1.7 provided you are running Conductor 2.1.7.

We recommend you upgrade to 2.1.7 if:	
You want to take advantage of performance and stability increases in 2.1.7, or use any of the following features:	You were impacted by any issues discovered in prior releases, especially if you have any of the following:
• If you have a HS that must remain on 2.1.x but work through a multi-homed 2.2.x relay.	• HS-100 intermittently failing to execute diagnostic commands, or appearing to upgrade but not installing the upgrade. • Have intermittent issues with HS-150 cell modems • Need to use the HTTP GET monitor and point it at arbitrary IP addresses • Need HS-500 to not have ports 3/4, 5/6 go into hardware bypass when the unit is powered off

Note: You may upgrade Conductor directly to 2.1.7 from version 1.12.6 or later. You may upgrade HIPswitches to 2.1.7 provided you are running Conductor 2.1.7.

Extensive testing was conducted both in-house and with selected development partners, in lab and in production environments to ensure that performance is equivalent to 2.1.6. Additionally, 2.1.7 should be more stable than all prior releases.

Fixes

ID	Applies to	Description
DEV-11908	Conductor	Fixed an issue where viewing a HIPservice group in Diagnostic mode now refreshes the list of available HIPservices, correctly.
DEV-11863	HIPswitch-Cellular	A HIPswitch now connects via a newly installed Cell Module, when the new Cellular Module is installed after a firmware downgrade.
DEV-11182	Cloud-Azure	Microsoft Azure now supports ICMP. You are able to add ICMP rules to the Conductor and HIPswitch security groups.
DEV-11756	HIPswitch	For the HIPswitch-500 and Conductor-500 platforms: Fixed an issue where the hardware LAN bypass feature was turned on during power off. Ports 1-2, 3-4, 5-6, 7-8 were bypassed (physically connected together) when the system was powered off.
DEV-11478	HIPswitch	Fixed a bug with the Conductor-HIPswitch Time Synchronization and added a Watchdog functionality for the Conductor connection on HIPswitches.
DEV-11305	Cellular modem	Improved USB driver reliability, so Cellular Modems reliably recover from Modem Firmware crashes.
DEV-11194	Conductor	This issue is fixed where Factory resetting a HIPswitch would sometimes delete Event Monitors targeted at Device Groups or HIPservice Groups.

ID	Applies to	Description
DEV-11047	Conductor	Added a Warning Dialog to the Conductor upgrade process if the customer has HIPswitches which are not compatible with 2.2.x.
DEV-10822	HIPswitch	Fixed a bug where entering leading zeros, in the VLAN tag input fields on the Ports Configuration page, could the HIPswitch to be unable to function.
DEV-10770	HIPswitch-Cellular	When downgrading a HIPswitch-150 from 2.2.0 to 2.1.6 the cellular link, LEDs are now functional.
DEV-10723	Conductor	Fixed a bug where tags were removed from HIPswitches when performing Diagnostic actions.
DEV-10696	HIPswitch	Relay probes will now probe all published addresses for a Multi-homed 2.2.x Relay. The 2.1.7 HS itself still does not support multi-homing, so probes only originate from one preferred (IPv4 or IPv6) address.
DEV-10588	Conductor	When creating a Monitor action that is an HTTP Action (HTTP GET), the URL field now allows for both the Host names and IP address.
DEV-10560	Conductor	Fixed a bug that could prevent customers from saving Overlay DHCP settings.
DEV-10390	HIPswitch-Cellular	Improved the functionality on the HIPswitch-150 and correctly applies power to the Expansion Bay on boot-up, even when the USB console cable has been connected, prior to applying main system power.
DEV-10203	HIPswitch	Fixed an issue where the default Underlay Fail-safe (reboot) settings did not get applied correctly.
DEV-10159	HIPswitch	Updated the HS-150 platform to allow multiple Underlay Interfaces (wired and cellular) to HA-pair.
DEV-9953	Conductor	A check is in place to prevent a customer from adding a HIPSwitch’s Underlay IP address as a device IP for itself.
DEV-9949	HIPswitch-Cellular	Enabled modem statistics collection for HIPswitch-150 with an MC7430 modem installed.
DEV-9876	OpenHIP	Fixed an issue where broadcast/multicast packets being sent on a busy HIPswitch, having many tunnels (e.g., hub with many spokes), causes the HIPswitch to crash and restart.
DEV-9830	HS100	You can now reboot a HIPSwitch from both Diagnostic Mode and the Command Line.
DEV-9829	HIPswitch	Diagnostic Mode now displays **None,** when there is no Part Number file.
DEV-9800	Conductor	The HIPswitch displays the tags correctly, when you toggle between Transparent Mode and Protected Mode.
DEV-9524	HIPswitch	Fixed a bug that caused Diagnostic Device pings to fail on HIPservices after an HA fail-over.
DEV-9939	Conductor	Fixed a bug where opening and closing the Conductor Proxy settings will not save blank values.

Known Issues

ID	Applies to	Description
DEV-11350	HIPapp	UserAuth sometimes does not work with 2.1.6 HIPswitches. Workaround: None
DEV-11095	HIPapp-Android	Android HIPclient 2.1.6 is not able to pass traffic with another HIPclient with User Authentication feature enabled. Workaround: Upgrade Android HIPclient to 2.2.1 or later.
DEV-11196	HIPswitch	HTTP GET monitor does not work as expected.Workaround: HTTP GET monitor on a 2.1.6 HS with a 2.1.7 Conductor will not work. Please upgrade the HS to 2.1.7.
DEV-11047	Conductor	A 2.1.6 Conductor with map1 HS is not blocked from upgrading to 2.2. Workaround: None
DEV-10638	HIPswitch	CLONE (2.1.7) - Health data is sent when it is disabled in the Conductor. Workaround: None
DEV-9813	Conductor	The Route Notice check does bit check the currently configured routes. Workaround: The UI warns that you need an Overlay Gateway Address even though one is already configured.
DEV-9779	Conductor	Using the mvebu image as an example, it lists the 250 variants before the 150 variants. The x86 image is fine. Workaround: The list of platforms supported on a build image should list them in numerical order
DEV-9761	Conductor	The Conductor net/net utility incorrectly allows the setting of two (2) default routes. Workaround: Set only one (1) default route and then apply static routes via the **Setup** page, under **Conductor UI General Settings**,.
DEV-9782	HIPclient, all platforms	HIPclient chooses an incorrect interface and cannot establish a connection with devices behind a HIPswitch running on the Google Cloud Platform (GCP). It has to do with having multiple active interfaces. Workaround: In the HIPclient configuration, select your desired network interface instead of allowing the HIPclient to automatically choose an interface.

ID	Applies to	Description
DEV-9697	Conductor	Removing the Conductor HA does not remove the standby Conductor's address from the HIPswitch Conductor search list on HIPswitches running versions previous to 2.0. Workaround: De-configuring Conductor HA does not remove the Standby Conductor's address from the HIPswitch Conductor search list on HIPswitch versions older than v2.0. Customer should upgrade to 2.1x.
DEV-9397	Conductor	If you perform a factory reset on a Conductor that's in HA-mode, the database gets into a bad state and Postgres won't start. Note that a second factory reset fixes the issue. Workaround: Factory resetting a Conductor that's in an HA-pair doesn't work correctly the first time. To fix this, a second factory reset is required.
DEV-9200	HIPswitch	When attempting firmware upgrades get failure messages. Workaround: The first attempt to upgrade fails, reboot the HS and upgrade again. (this clears out old /tmp files)
DEV-9166	HIPswitch, Cloud	When route injection is enabled, a HIPswitch protected subnet must contain only one HIPswitch. Additionally, any custom routes added to the route table are deleted when route injection is enabled. Workaround: If you want to deploy multiple HIPswitches in the same protected subnet or keep your custom routes, disable route injection.
DEV-9125	HIPswitch	101g: Ping peer HIPswitches pings wrong Underlay IP. Workaround: On Mac and Linux HIPapp, if your computer has multiple active NICs and you select a specific NIC in HIPapp configuration, it instead lets the operating system chose the NIC for outbound traffic.
DEV-8097	HIPclient, macOS	If your computer has multiple active NICs and you select a specific NIC in your HIPclient configuration, the operating system will choose the NIC for outbound traffic. Workaround: None
DEV-8060	Conductor	In rare cases, the Conductor HA pair will stop syncing. Workaround: If this happens, promote the HA-secondary to a primary, then re-pair them.
DEV-8051	Conductor	The IP address field on associated with a HIPswitch may be blank on the **HIPservices** tab. Workaround: You can locate the IP address information under the **Reporting** tab.

ID	Applies to	Description
DEV-7769	Conductor	Toggling policy on and off too quickly on a HIPswitch hosted in Google Cloud can result in the Route Table becoming out of sync when using route injection. Workaround: After toggling policy, wait 10 seconds before toggling it again.
DEV-7058	HIPswitch	When reconfiguring your Underlay network from one physical port to another in the Conductor, the changes may not be applied successfully and the configuration will revert back to the original settings. Workaround: Make the configuration changes in diagnostic mode.
DEV-6590	Conductor	You can add a voucher code more then once from the Licensing tab. This does not create additional licenses, but is visually confusing. Workaround: None
DEV-6587	Conductor	The Licensing tab may display invalid entries. Workaround: Remove the invalid items manually.
DEV-6533	Conductor	When creating or editing a smart device group, rules can have the same ordinal values. This can cause unintended issues in the processing results. Workaround: When creating rules, verify each rule has a unique ordinal value.
DEV-6226	Conductor	A fully qualified Domain name cannot be used for local or peer replication addresses on an HA Conductor pair. Workaround: FQDN for Local or Peer Replication address on an HA Conductor pair can be used ONLY IF the reverse lookup yields the same FQDN
DEV-5832	HIPswitch	Device NAT functionality currently does not work with layer two (2) traffic. Workaround: None
DEV-5530	Conductor UI	In some cases, allow incoming pings (ICMP) and SYN Flood Protection on the **Firewall** page may be disabled and won't toggle. Workaround: Refresh your browser to resolve the issue.
DEV-5430	Conductor	After configuring the Conductor for the first time, you may receive a Lost Connection to the original server message if you select **Return to settings** too quickly. Workaround. Wait at least 20 seconds before selecting Return to settings.

ID	Applies to	Description
DEV-5008	PCI Reporting	PCI Reporting shows the UUID reference instead of the name when generating a PCI report from **Settings** > **Advanced** > **PCI Reporting** > **Downloads** > **User Activities Report**. Workaround: To view names, you can download object references from the same page where you generated the PCI report.

Release Notes 2.1.6

Release Date: March 1, 2019

What's New

New in this release:

Modbus TCP to RTU Gateway

We’ve enhanced our Serial over IP (SoIP) feature with a Modbus TCP to Modbus RTU gateway. After configuring Modbus via the HIPswitch SoIP settings in Conductor, the HIPswitch will accept Modbus TCP commands from servers, issue the commands to serially-connected Modbus RTU device(s), and return the responses via Modbus TCP back to the server. The HIPswitch accepts pipelined requests from the server(s). This provides optimal efficiency for Modbus traffic in terms of throughput, latency, and number of messages as compared to transparent Serial over IP.

DHCP Relay

HIPswitches can now relay DHCP requests to a central DHCP server as an alternative to your existing DHCP server. This allows additional deployment flexibility where extended DHCP options are needed, or an existing DHCP server integrates with other systems such as Active Directory and DNS.

> **Note:** When moving devices from one HIPswitch to a different one, the central DHCP server may issue the same IP address to the device, which could result in policy or routing conflicts depending on your network.

Wireless Underlay Failsafe

The HIPswitch Link Manager, introduced in version 2.1.0, intelligently monitors the health of the underlay connection, detecting when there are no options for the HIPswitch to connect to Conductor or peer HIPswitches. Link Manager is now enhanced to reboot the HIPswitch which may restore the wireless connection to a healthy state. Occasionally, changes made in the wireless provider network will drop or hang a cellular or WiFi HIPswitch uplink in such a way that the modem cannot recover. Rebooting the HS will force the modem and cell tower or access point to renegotiate their connection; sometimes this restores a healthy connection. This behavior is on by default for wireless models, and can be disabled and configured per HIPswitch in the Conductor UI. You can configure the amount of time Link Manager waits to reboot the HIPswitch after first detecting underlay failure, and a minimum amount of time to wait between reboot attempts. By default, all wireless models enable this feature with a wait-to-reboot value of 10 minutes, and min-wait-between-reboots value of 30 minutes.

Note: See known issue DEV-9877 for additional information in reference to running a HIPswitch on the Microsoft Azure platform.

APAC Modem Support

The HIPswitch cellular expansion module SFF-MOD-MC7430 (PLF-0118-01) is now available for the HIPswitch 150, which includes the Sierra Wireless MC7430 modem for operation in Hong Kong, Macau, and Japan.

Note: Firmware release 2.1.6 is required to use this expansion module.

HIPswitch 250 Series Revision 2 Support

The HIPswitch 250 Revision 2 is now available and includes the following SKUs:

- HIPswitch 250e (PLF-0062-02)
- HIPswitch 250g (PLF-0066-02)
- HIPswitch 250gd (PLF-0111-02)

Revision 2 provides improved SFP compatibility, modem watchdog support, and improved modem carrier compatibility.

Note: Firmware release 2.1.6 or higher is required to use Revision 2 of the HIPswitch 250.

Wired Interface Support for Android

The HIPclient for Android now supports wired ethernet connectivity.

Tag integration with HIP invitations

You can now specify tag(s) for HIP invitations, which apply to HIP services as they activate. This makes it easy to organize newly-activated HIP services and, when combined with smart device groups, automatically give them communications policy in overlay networks.

Longer HIPswitch UIDs

HIPswitches which are licensed with a 2.1.6 or higher firmware may generate a longer serial number portion of the UID (up to 20 characters), compared to the previous 12 characters. HIPswitches licensed from a previous release will not change their UID.

Upgrade Considerations

The 2.1.6 release includes all hotfixes from prior releases and addresses all known support cases at the time of release.

We recommend you upgrade to 2.1.6 if:	
You want to take advantage of performance and stability increases in 2.1.6, or use any of the following features:	You were impacted by any issues discovered in prior releases, especially if you have any of the following:

We recommend you upgrade to 2.1.6 if:	
• Modbus RTU to Modbus TCP proxy • HIPswitch DHCP relay • HIP invitation Tag integration • New hardware support	• HIPswitch 250 cellular instability • HIPswitch 150 cellular instability • Remote Linux HIPserver HIP tunnel instability • HIPswitch 75 memory instability

Note: You may upgrade Conductor directly to 2.1.6 from version 1.12.6 or later. You may upgrade HIPswitches to 2.1.6 provided you are running Conductor 2.1.6.

Extensive testing was conducted both in-house and with selected development partners, in lab and in production environments to ensure that performance is equivalent to 2.1.5. Additionally, 2.1.6 should be more stable than all prior releases.

Fixes

ID	Applies to	Description
DEV-9795	HIPclient, Windows	Fixed an issue in the Windows HIPclient where a MAP connection was required for the HIPclient t begin passing traffic.
DEV-9787	HIPswitch	Fixed an issue where incorrect health data was reported while a HIPswitch was in transparent mode
DEV-9771	HIPclient, Windows	Fixed an issue where the Windows HIPclient networks view would not report all available data.
DEV-9709	HIPclient, iOS	Fixed an issue where HIPclient profiles created from HIP invites on iOS devices using the same Apple ID were synced due to iOS clipboard behavior.
DEV-9639	OpenHIP	Fixed an issue where a HIPswitch sends update acknowledgements to the wrong address.
DEV-9601	HIPclient, Android	Fixed an issue where the 2.1.5 Android HIPclient was reported incorrectly in the Conductor as version 2.1.4
DEV-9595	HIPclient, Android	After an Android device running a HIPclient wakes, ping now correctly resumes.
DEV-9593	HIPclient, Android	It is no longer possible to delete the current active profile, which would cause unpredictable behavior with the HIPclient.
DEV-9574	Conductor	Fixed an issue where updating system settings after a proxy password has been entered may overwrite it with random data.
DEV-9560	HIPswitch	Fixed an issue that could cause packets on an overlay network to transmit on the underlay network under certain conditions.
DEV-9472	HIPclient, Windows	Fixed an issue with the Windows HIPclient where deleting a profile using the CLI would not update the HIPclient UI correctly, resulting in discrepancies in the profile list.
DEV-9477	Conductor	Fixed an issue in the **Health Data** tab where selecting **more...** would not display additional lines.
DEV-9389	API	POST /api/v1/people/{id}/tags in the Conductor API now presents clearer, more actionable error messages.

ID	Applies to	Description
DEV-9382	Conductor	Improved dialog information when attempting to update firmware with an image not compatible with the target platform. The dialog text now clearly states the firmware is incorrect, replacing the generic non-actionable error message.
DEV-9385	HIPclient, Android	Fixed an issue where profile selection is disabled after creating a new profile and restarting the Android HIPclient.
DEV-9382	Conductor	Fixed an issue where attempting to install a non-Azure firmware package in an Azure instance would produce an error message stating **<inserv form image>**.
DEV-9377	Diagnostic mode	Fixed an issue that would allow you to enter an invalid gateway address in diagnostic mode.
DEV-9366	Cellular	Raised the log level of cellular interface repair messages to provide information about when a cellular interface is being repaired.
DEV-9333	Conductor	The Standby Conductor in an HA pair will now correctly display the Diagnostics Tab in the UI.
DEV-9317	HIPswitch	Fixed an issue where a firmware upgrade may fail due to a timing issue, taking the HIPswitch offline until it is restarted.
DEV-9312	HIPclient, Windows	Fixed an issue where an overlay IP address displayed on the **Configuration** settings, but not in the **HIP Networks** view.
DEV-9269	HIPclient, Windows	Fixed an issue where the Windows HIPclient would display an incorrect underlay IP address.
DEV-9259	Conductor	HIPclient descriptions now correctly display in the **Devices Reference** file from the PCI downloads page.
DEV-9201	HIPswitch 75w	Fixed an issue where the HIPswitch 75w would not properly connect to WiFi after a factory reset.
DEV-9106	HIPclient, iOS	Fixed an issue where you were required to stop and start the HIPclient to resume traffic when failing over from cellular to WiFi.
DEV-9091	HIPclient, Android	Trailing spaces are now stripped when manually entering the Conductor URL on the configuration settings.
DEV-9013	HIPswitch 75w	The WiFi LED now correctly functions on the HIPswitch 75w.
DEV-7499	HIPswitch	The bandwidth check in the HIPswitch **Diagnostics** tab no longer fails for HA-paired HIPswitches.
DEV-6446	HIPclient, iOS	Fixed an issue where viewing traffic stats in the iOS app would display negative values instead of zero.

Known Issues

ID	Applies to	Description
DEV-9877	Conductor, Cellular HIPswitch	Link Manager default settings do not work with Conductors running on the Microsoft Azure platform when using Azure Network Security Group settings. Workaround: If you are using an Azure Conductor with Wireless (Cellular or WiFi) HIPswitches, disable pings on active link on each wireless HIPswitch or set an alternate active ping target (e.g. 8.8.8.8).
DEV-9830	HIPswitch 100	The HIPswitch 100g may sometimes fail to initiate a reboot when requested from the web interface in diagnostic mode. Workaround: Power cycle the HIPswitch.
DEV-9782	HIPclient, all platforms	HIPclient chooses an incorrect interface and cannot establish a connection with devices behind a HIPswitch running on the Google Cloud Platform (GCP). Workaround: In the HIPclient configuration, select your desired network interface instead of allowing the HIPclient to automatically choose an interface.
DEV-9697	Conductor	Removing Conductor HA does not remove the standby Conductor's address from the HIPswitch Conductor search list on HIPswitches running versions previous to 2.0. Workaround: None
DEV-9397	Conductor	Factory resetting a Conductor that's in an HA-pair doesn't work correctly the first time. Workaround: Factory reset the Conductor a second time to resolve the issue.
DEV-9166	HIPswitch, Cloud	When route injection is enabled, a HIPswitch protected subnet must contain only one HIPswitch. Additionally, any custom routes added to the route table are deleted when route injection is enabled. Workaround: If you want to deploy multiple HIPswitches in the same protected subnet or keep your custom routes, disable route injection.
DEV-9157	HIPclient, macOS	Killing the hipctl daemon (tnw-cltd) will result in the HIPclient not functioning properly. If you try and run any hipctl commands, the message Could not connect with Tempered Networks control process is displayed. No message is displayed when trying to make changes from the configuration UI. Workaround: Restart the process by entering sudo launchctl start com.temperednetworks.ctld from a terminal.
DEV-8097	HIPclient, macOS	If your computer has multiple active NICs and you select a specific NIC in your HIPclient configuration, the operating system will choose the NIC for outbound traffic.Workaround: None

ID	Applies to	Description
DEV-8060	Conductor	In rare cases, a Conductor HA pair will stop syncing. Workaround: If this happens, promote the HA-secondary to a primary, then re-pair them.
DEV-8051	Conductor	The IP address field on associated with a HIPswitch may be blank on the HIPservices tab.Workaround: You can locate the IP address information under the **Reporting** tab.
DEV-7955	Conductor	If you ping a HIPswitch running in Azure from another HIPswitch, it will fail in the Conductor UI. This is due to ICMP being denied by Azure's security groups. Workaround: None
DEV-7769	Conductor	Toggling policy on and off too quickly on a HIPswitch hosted in Google Cloud can result in the route table becoming out of sync when using route injection. Workaround: After toggling policy, wait 10 seconds before toggling it again.
DEV-7661	Conductor	When replacing a HIPswitch, the new HIPswitch may take a few minutes to reconnect and appear online in the Conductor. Workaround: Wait a few minutes after replacing the HIPswitch for it to display in the Conductor UI.
DEV-7125	Conductor, PCI	When exporting PCI data, HIPservices references may not display correctly when viewing the CSV file in Microsoft Excel. Workaround: None
DEV-7058	HIPswitch	When reconfiguring your underlay network from one physical port to another in the Conductor, the changes may not be applied successfully and the configuration will revert back to the original settings. Workaround: Make the configuration changes in diagnostic mode.
DEV-6590	Conductor	You can add a voucher code more then once from the Licensing tab. This does not create additional licenses, but is visually confusing.Workaround: None
DEV-6587	Conductor	The Licensing tab may display invalid entries.Workaround: Remove the invalid items manually.
DEV-6533	Conductor	When creating or editing a smart device group, rules can have the same ordinal values. This can cause unintended issues in the processing results. Workaround: When creating rules, verify each rule has a unique ordinal value.
DEV-6226	Conductor	A fully qualified domain name cannot be used for local or peer replication addresses on an HA Conductor pair. Workaround: None

ID	Applies to	Description
DEV-6195	Conductor	The Conductor incorrectly displays an option to check bandwidth for HIPclients in diagnostic view. This option is not supported for HIPclients and will not function correctly if selected. Workaround: None
DEV-5832	HIPswitch	Device NAT functionality currently does not work with layer 2 traffic. Workaround: None
DEV-5530	Conductor UI	In some cases, Allow incoming pings (ICMP) and SYN Flood Protection on the **Firewall** page may be disabled and won't toggle. Workaround: Refresh your browser to resolve the issue.
DEV-5430	Conductor	After configuring a Conductor for the first time, you may receive a Lost connection to the original server message if you select **Return to settings** too quickly. Workaround. Wait at least 20 seconds before selecting Return to settings.
DEV-5008	PCI Reporting	PCI Reporting shows the UUID reference instead of the name when generating a PCI report from **Settings** > **Advanced** > **PCI Reporting** > **Downloads** > **User Activities Report**. Workaround: To view names, you can download object references from the same page where you generated the PCI report.

Release Notes 2.1.5

Release Date: December 13, 2018

What's New

New in this release:

FIPS

Tempered Networks now offers FIPS 140-2, based on the HIPswitch 500 and Conductor 500 platforms. With FIPS, private keys are stored on the FIPS-certified HSM (hardware security module). The HSM performs all cryptographic operations. For this added key security, performance may be noticeably slower in terms of data plane throughput and firmware update processing. Redundant HA FIPS is not supported at this time.

Improved time management

NTP sync is now configurable from the Conductor. Various improvements have been made to ensure HIPswitch time is closely synchronized with the Conductor, eliminating time-drift.

Note: We recommend pointing your HIP-enabled servers and clients to the same NTP Time source to ensure proper synchronization.

HIPswitch 75w Series

We now offer the HIPswitch 75 Series with a built-in WiFi module. Software version 2.1.5 does not currently provide WiFi LED status on the outside of the unit, but the WiFi uplink functions correctly. This will be addressed in a future release.

HIPswitch 150e Series

We now offer the HIPswitch 150e base platform, suitable for ICS and SCADA environments and includes 4x Gig-E and 1x SFP port, 1x micro-USB console port, and can be powered by PoE or external single- or dual-power supply. The HIPswitch 150 can sustain 75 Mb/s, and burst up to 100 Mb/s. This new platform supports field-upgradeable expansion modules.

HIPswitch 150 Series cellular module

This release supports a cellular expansion module suitable for North American cell carriers, which accepts 3FF Micro SIM cards. ATT, Verizon, T-Mobile, Rogers, and Telus have been field-tested at the time of this release.

HIPswitch 250 Series single- and dual-modem automated recovery

We added an internal watchdog monitor for cell carrier uplink connections. If a HIPswitch cannot connect to Conductor via any means, then occasionally (approx. once per day) it will perform a full reset, which may re-establish the carrier connection in certain environments. This will only occur when the HIPswitch 250 has no means of reaching the Conductor or peer HIPswitches.

HIPrelay bandwidth reporting

It is now possible to view the bandwidth of relayed connections between HIP Services in Conductor! An extra tab will appear in Conductor at **HIPservice** > **Reporting** > **HIPrelay Stats** for each HIPrelay. These statistics provide visibility into your network utilization with full-color, layered bandwidth graphs. They are also useful for troubleshooting underlay network relayed connection issues.

Service-specific CPU and memory reporting

For 2.1.5 and above, your HIP Services will report resource utilization more granularly, and you will be able to see this diagnostic information in the **HIPservice** > **Reporting** > **Graphs**.

Headless install for Windows HIPclient and HIPserver

You can now perform non-interactive installations of the Windows 7 HIPclient or HIPserver using Microsoft's System Center Configuration Manager (SCCM). Previous releases required manual acknowledgment by an administrator to complete the installation of an unsigned network tap (TAP) driver on Windows. We have patched the driver and obtained Microsoft certification, so this step is no longer necessary.

Tags public API

All basic tagging capabilities released in software version 2.1.4 are exposed in the public API. This includes the ability to index the tags, set or unset tags on taggable objects, such as devices, device groups, HIP Services, HIPservice groups, networks, and people. You can manage tags, retrieve various objects by tag, manage tag expirations, and perform other tag-based actions on several taggable objects at once. Advanced tag management, such as using tags in smart device group rules, or managing monitor event-actions that manipulate tags, will be added in a future release.

Custom CA alerts & public API	Though technically possible, it was difficult to use a non-Tempered CA at scale with your Conductor and HIP Services. Prior releases required you to manually copy/paste each CSR and cert from the Conductor GUI. Now you can automate the process using new public API calls. This enables a scriptable, scalable Conductor-centric workflow. Also, an admin alert is created in Conductor when custom CA certs are near expiration.

Upgrade Considerations

The 2.1.5 release includes all hotfixes from prior releases and addresses all known support cases at the time of release.

We recommend you upgrade to 2.1.5 if:	
You want to take advantage of performance and stability increases in 2.1.5, or use any of the following features:	You were impacted by any issues discovered in prior releases, especially if you have any of the following:
• Relay bandwidth reporting • HIPswitch 75w • HIPswitch 150e • HIPswitch 250gd carrier monitoring • Windows SCCM HIPclient installs • Public API for Tags or Custom CA	• Time drift issues with Conductor or HIP Services • Cell carrier connection flapping • Issues switching cell carriers (e.g. changing SIM cards) on the HIPswitch 250 • Issues with SFP ports on the HIPswitch 250 • DHCP configuration on the overlay network • Problems setting one-arm mode on any multi-port HIPswitch • Event monitor permissions / usability problems • Difficult to detect misconfiguration problems pairing HA HIPswitches

Note: You may upgrade Conductor directly to 2.1.5 from version 1.12.6 or later. You may upgrade HIPswitches to 2.1.5 provided you are running Conductor 2.1.5.

Extensive testing was conducted both in-house and with selected development partners, in lab and in production environments to ensure that performance is equivalent to 2.1.4. Additionally, 2.1.5 should be more stable than all prior releases.

Fixes

ID	Applies to	Description
DEV-9462	HIPswitch	Fixed an issue with the HIPswitch 250g where ports 1, 2, and/or 7 are non-functional following an upgrade from 2.1.3 to 2.1.4, if the 100M SFP PHY setting is in use. (Otherwise it is reverting to the default of 1000M mode.)
DEV-9461	HIPswitch	Fixed an issue where port 8 on the HIPswitch 250 would not reestablish a link after a soft reboot.
DEV-9430	Conductor	The **PKI** tab now only displays on models that support the feature. Previously, the **PKI** tab was visible in the Conductor UI for HIPclients and HIPservers.
DEV-9378	HIPswitch-Cellular	Fixed an issue where cellular modems in the HIPswitch 150 and HIPswitch 250 were not properly initialized.
DEV-9370	Conductor	Fixed an issue where Conductor-initiated port configurations would fail.

ID	Applies to	Description
DEV-9353	Conductor	All users allowed to view an alert monitor can now receive alerts for that monitor.
DEV-9333	Conductor	Fixed an issue where a standby Conductor in an HA pair would not display the **Diagnostics** tab.
DEV-9287	Conductor	Fixed an issue where Conductors running software version 2.1.4 sent an incorrect DHCP server configuration data to HIPswitches running versions prior to 2.1.4.
DEV-9263	HIPswitch-Cellular	Fixed an issue where a HIPswitch 250 with a cellular modem may show abnormally high CPU usage.
DEV-9246	Conductor	Attempting to delete a HIPclient or HIPserver from the **Devices**page no longer returns a permission denied error.
DEV-9244	HIPclient, iOS	The Conductor now correctly reports the version of the connected iOS HIPclient.
DEV-9239	Conductor	The **Event Monitors** view no longer prevents the Conductor UI from timing out.
DEV-9152	HIPswitch	The Conductor now rejects configuration changes that would add a 0.0.0.0 wildcard device to an overlay network if the network also has a 0.0.0.0/0 route on one of the connected HIP Services.
DEV-9149	HIPclient, Windows	The Windows HIPclient and HIPserver now report errors in the correct format.
DEV-9136	HIPserver, Linux	Fixed an issue where hipctl on Linux would not report an error when trying to reset the active profile.
DEV-9120	Conductor API	Improved the API filter and sort parameters. Sending a parameter that is not supported results in a more actionable message.
DEV-9112	Conductor	Fixed an issue where a PCI user activity report would not contain firmware upload information.
DEV-9106	HIPclient, iOS	Mobile devices running iOS now failover from wireless to cellular correctly.
DEV-9053	HIPswitch	HIPswitch HA configurations now verify the HA floating IP address is in range of the shared network IP address, and will display an error in the Conductor UI if it is not.

Known Issues

ID	Applies to	Description
DEV-9887	HIPswitch 150	When applying power to a HIPswitch 150 while the microUSB console port is connected to a computer, the HIPSwitch-150 fails to enable power to the expansion bay. Workaround: Ensure your HIPswitch is connected to a power source prior to connecting to the console port.

ID	Applies to	Description
DEV-9875	OpenHIP	When the Conductor's time is changed backwards by a large amount, such as enabling NTP on the Conductor for the first time, all connected HIPswitches will adjust their time accordingly and result in HIPswitches being unable to establish tunnels with other HIPswitches. Workaround: Reboot your connected HIPswitches whenever you make large time adjustments to the Conductor.
DEV-9477	Conductor	The **Health Data** tab displays 28 lines with a link at the bottom stating **+438 more**. Clicking on the link does not expand the list Workaround: None
DEV-9397	Conductor	Factory resetting a Conductor that's in an HA-pair doesn't work correctly the first time. Workaround: Factory reset the Conductor a second time to resolve the issue.
DEV-9382	Conductor	Attempting to install a non-Azure firmware package in an Azure instance will produce an error message stating **<inserv form image>**. Workaround: None
DEV-9157	HIPclient, macOS	Killing the hipctl daemon (tnw-cltd) will result in the HIPclient not functioning properly. If you try and run any hipctl commands, the message Could not connect with Tempered Networks control process is displayed. No message is displayed when trying to make changes from the configuration UI. Workaround: Restart the process by entering sudo launchctl start com.temperednetworks.ctld from a terminal.
DEV-8097	HIPclient, macOS	If your computer has multiple active NICs and you select a specific NIC in your HIPclient configuration, the operating system will choose the NIC for outbound traffic.Workaround: None
DEV-8060	Conductor	In rare cases, a Conductor HA pair will stop syncing. Workaround: If this happens, promote the HA-secondary to a primary, then re-pair them.
DEV-8051	Conductor	The IP address field on associated with a HIPswitch may be blank on the HIP Services tab.Workaround: You can locate the IP address information under the **Reporting** tab.
DEV-7955	Conductor	If you ping a HIPswitch running in Azure from another HIPswitch, it will fail in the Conductor UI. This is due to ICMP being denied by Azure's security groups. Workaround: None

ID	Applies to	Description
DEV-7769	Conductor	Toggling policy on and off too quickly on a HIPswitch hosted in Google Cloud can result in the route table becoming out of sync when using route injection. Workaround: After toggling policy, wait 10 seconds before toggling it again.
DEV-7661	Conductor	When replacing a HIPswitch, the new HIPswitch may take a few minutes to reconnect and appear online in the Conductor. Workaround: Wait a few minutes after replacing the HIPswitch for it to display in the Conductor UI.
DEV-7499	HIPswitch	The bandwidth check in the HIPswitch **Diagnostics** tab might fail for HA-paired HIPswitches. Workaround: None
DEV-7125	Conductor, PCI	When exporting PCI data, HIP Services references may not display correctly when viewing the CSV file in Microsoft Excel. Workaround: None
DEV-7058	HIPswitch	When reconfiguring your underlay network from one physical port to another in the Conductor, the changes may not be applied successfully and the configuration will revert back to the original settings. Workaround: Make the configuration changes in diagnostic mode.
DEV-6590	Conductor	You can add a voucher code more then once from the Licensing tab. This does not create additional licenses, but is visually confusing.Workaround: None
DEV-6587	Conductor	The Licensing tab may display invalid entries.Workaround: Remove the invalid items manually.
DEV-6533	Conductor	When creating or editing a smart device group, rules can have the same ordinal values. This can cause unintended issues in the processing results. Workaround: When creating rules, verify each rule has a unique ordinal value.
DEV-6446	HIPclient, iOS	When viewing traffic stats in the iOS app, the chart may show negative values instead of zero. Workaround: None
DEV-6226	Conductor	A fully qualified domain name cannot be used for local or peer replication addresses on an HA Conductor pair. Workaround: None
DEV-6195	Conductor	The Conductor incorrectly displays an option to check bandwidth for HIPclients in diagnostic view. This option is not supported for HIPclients and will not function correctly if selected. Workaround: None

ID	Applies to	Description
DEV-5832	HIPswitch	Device NAT functionality currently does not work with layer 2 traffic. Workaround: None
DEV-5530	Conductor UI	In some cases, Allow incoming pings (ICMP)and SYN Flood Protection on the **Firewall** page may be disabled and won't toggle. Workaround: Refresh your browser to resolve the issue.
DEV-5430	Conductor	After configuring a Conductor for the first time, you may receive a Lost connection to the original server message if you select **Return to settings** too quickly. Workaround. Wait at least 20 seconds before selecting Return to settings.
DEV-5008	PCI Reporting	PCI Reporting shows the UUID reference instead of the name when generating a PCI report from **Settings** > **Advanced** > **PCI Reporting** > **Downloads** > **User Activities Report**. Workaround: To view names, you can download object references from the same page where you generated the PCI report.
DEV-1846	Conductor, HA	The standby Conductor UI in an HA pair will not timeout. This issue does not affect the master Conductor UI. Workaround: Log off manually when not using the standby Conductor UI.

Release Notes 2.1.4

Release Date: October 16, 2018

What's New

New in this release:

HIPclient for Android

With this release, the HIPclient is available for Android. Your Android devices can now natively connect to your IDN overlay, giving them a trusted and verifiable connection wherever you are. Multiple profiles allow you to easily switch between different IDN overlays as needed.

Improved Conductor UI Navigation

Several UI elements have been redone to improve navigation:

- Conductor settings are now accessed from the gear icon in the upper right corner of the UI.
- The logged in user profile, API docs, EULA, and sign-out are accessed from the user account icon in the upper right corner of the UI.
- Item names in many lists throughout the UI now actively link to properties pages and dialogs. This greatly simplifies navigation between related elements.

Tags

Tags provide flexible asset management in the Conductor. Devices, Device Groups, HIPswitches, HIPswitch Groups, Overlay Networks, and People can be tagged directly. The Tag information dialog allows you to **Navigate** directly to any tagged item, perform bulk **Actions** (Enable, Disable, or Untag tagged items), and edit **Properties**. Items can be tagged permanently or until you untag them. You can also set an expiration date, which will untag a component after a configurable period of time. You can create tags from the **Tags** page, access from the tag icon in the upper right corner of the UI.

You can also create tags inline while modifying an item’s tag members by entering a new tag name and select colors for easy classification. Tags have been integrated into searching and filtering throughout Conductor.

Tags can be used in matching rules to greatly simplify Smart Device Groups. They can also be added to or removed from taggable items in Event Monitor Actions, which allows monitor results to affect overlay network policies. By using tags with these features, you can optimize your workflows. For example, you can create temporary network policies for specific devices, easily revoke policy directly from devices or HIPswitches without having to navigate to a network, and allow multiple admins to keep track of their assets in a single Conductor.

Relay Probes

A HIPswitch with this option selected will periodically send probe packets to all of its relays, and use the closest relay when initiating secure tunnels. This reduces the amount of network traffic used to build new tunnels, and allows auto-connect to be turned off. You can find this option in the **Advanced settings** section of a HIPswitch's settings page.

Conductor Diagnostics

Similar to diagnostics offered for HIPswitches, the Conductor now has a set of maintenance and diagnostic functions consolidated under the Diagnostics tab of the Settings page. These include Creation or Restoration of a DB Backup, downloading a Conductor support bundle, and viewing a Conductor diagnostic report. Network diagnostics allow you to generate a packet capture on the Conductor interface, ping, and traceroute.

Upgrade Considerations

The 2.1.4 release includes all hotfixes from prior releases and addresses all known support cases at the time of release.

Note: The Tempered Networks TERMS OF PRODUCT SALE, LICENSE AND WARRANTY has changed. The most recent version of the HIPclient for all platforms require you to accept the updated licence agreement before using the product. This applies to updates as well as new installations. For more information, see https://www.temperednetworks.com/resources/terms-of-product-sale-license-and-warranty

We recommend you upgrade to 2.1.4 if:	
You want to take advantage of performance and stability increases in 2.1, especially for any of the following features: • Android HIPclient • Improved Conductor navigation • Tags • Conductor diagnostics • Relay probes	You were impacted by any issues discovered in prior releases, especially if you have any of the following: • If you experienced long UI start-up times in the browser (data management between the UI in the browser and the Conductor is more efficient). • Cellular connectivity and carrier selection on HIPswitch-250 models

Note: You may upgrade Conductor directly to 2.1.4 from version 1.12.6 or later. You may upgrade HIPswitches to 2.1.4 provided you are running Conductor 2.1.4.

Extensive testing was conducted both in-house and with selected development partners, in lab and in production environments to ensure that performance is equivalent to 2.1.3. Additionally, 2.1.4 should be more stable than all prior releases.

Enhancements

Applies to	Description
Conductor, API	Added a new node in the API, /api/v1/email_settings, containing methods for setting, updating, and retrieving Conductor email settings.
HIPclient, Windows	The HIPclient for Windows has received the following improvements: • Updated the HIPclient allow for express installations, which requires only the license code and a confirmation. • Updated the HIPclient to allow you to set the log level in the UI.
HIPclient, macOS	The HIPclient on macOS has received the following improvements: • Updated the HIPclient for to store the private key in the Keychain for newly created profiles. • Updated the HIPclient for macOS to include **tnw-ctld**, a launch daemon on macOS for running Tempered Networks CLI commands and monitoring**tnw-hipd**, the HIP service. • Updated the HIPclient to properly display activation code errors.
HIPclient, Windows and macOS	Updated the HIPclient UI to allow you to double-click a profile in the configuration dialog to make a profile active.
HIPswitch 500	Added support for the new 4-port 10GbE fiber-optic expansion module, available for the HIPswitch 500 Series hardware.

Fixes

ID	Applies to	Description
DEV-8849	HIPswitch	Fixed an issue on the HIPswitch 250 where using 100BASE-FX mode on port 8 could cause phantom link events.
DEV-8699	HIPclient, Linux	Fixed an issue where 32-bit platforms would drop MAP connections after a certain amount of network traffic.

ID	Applies to	Description
DEV-8221	OpenHIP	Fixed an issue where changing the default UDP port under **Settings** > **Advanced** > **Edit Settings** > **Host Identity Protocol Port** in the Conductor was not respected by 2.1.3 HIPswitches.
DEV-8142	Conductor	Fixed an issue where clicking **Finish** two times very quickly when upgrading Conductor firmware would cause the upgrade to fail.
DEV-8198	Licensing	Fixed an issue where some email clients would insert additional lines in the `encrypted_synced_package.json` file and prevent the file from uploading to the Conductor correctly.
DEV-8120	HIPswitch, Azure	Fixed an issue where in rare cases, an Azure HIPswitch may fail to reconnect to the Conductor after a firmware upgrade.
DEV-8119	Conductor	Fixed an issue where a reactivated HIPclient configured with an overlay IP was listed as two devices, and you were unable to remove the overlay IP.
DEV-8067	HIPswitch	Fixed an issue that caused overlay device NAT to fail if more than one device port was used, or if the port was configured as a VLAN.
DEV-8049	Conductor	Fixed an issue where a network administrator may be able to view a HIPswitch group while restricted from viewing some of the HIPswitches in the group.
DEV-7962	HIPclient, Windows	Fixed an issue where upon waking, a computer in sleep mode would cause the HIPservice to stop and start, taking 30-60 seconds to recover.
DEV-7959	HIPswitch 100	Fixed an issue where configuring a VLAN tag on a HIPswitch 100 would cause currently active tunnels to stop working.
DEV-7913	Conductor	Fixed a UI error when creating a new Cloud HIPservice where the dialog box message would display **Network create completed** incorrectly when the deployment creation failed.
DEV-7814	HIPclient, Windows	Fixed an issue where a user name was not retained between failed log in attempts.
DEV-6881	HIPswitch	Fixed an issue where the LCD panels on the HIPswitch 500 and Conductor 500 displayed messages incorrectly.
DEV-6507	Conductor	Fixed an issue where the throughput graph for a HIPservice would occasionally miss a data point and display it as a zero value.
DEV-6172	Conductor	Fixed an issue where a HIPclient would incorrectly show the underlay IP as the overlay IP when it did not have an overlay IP set. They now correctly display they are **NAT** devices in the overlay IP column.
DEV-5448	Conductor	Fixed an issue where navigating to an HA-paired secondary HIPswitch would allow you to select the **Swap Roles** option and cause the UI to stop responding.
DEV-5428	Conductor UI	Fixed an issue where creating a Smart Device Group with **Ignore auto-discovered devices until accepted** checked and then removing the setting would cause the Smart Device Group to continue ignoring unaccepted devices.
DEV-5343	Conductor UI	Fixed an issue where trying to log in after a session has timed out would generate the following error: **The change you wanted was rejected.**

ID	Applies to	Description
DEV-4548	HIPswitch	HIPswitches now support 802.1p tagged traffic when using VLAN-tagged traffic in overlay networks.
DEV-4537	Conductor	Fixed an issue where the UI would not update correctly when demoting a master Conductor to standby.

Known Issues

ID	Applies to	Description
DEV-9183		
DEV-9182		
DEV-9157	HIPclient, macOS	Killing the **hipctl** daemon (**tnw-cltd**) will result in the HIPclient not functioning properly. If you try and run any hipctl commands, the message **Could not connect with Tempered Networks control process** is displayed. No message is displayed when trying to make changes from the configuration UI. Workaround: Restart the process by entering `sudo launchctl start com.temperednetworks.ctld` from the terminal.
DEV-9081	HIPclient, macOS (El Capitan)	The HIPclient on macOS 10.11, El Capitan, does not provide the necessary cryptographic APIs to create and use a private key from the Keychain. Instead, the HIPclient for macOS will detect this case and store the private key in its own storage. Workaround: To take advantage of the added protection using the Keychain, upgrade to macOS 10.12 (Sierra) or higher and create a new HIPclient profile.
DEV-8188	HIPswitch	A HIPswitch in transparent mode will not update the version information reported in the Conductor UI. This causes upgrade issues from 1.12.x to 2.x. Workaround: Disable transparent mode for the HIPswitch. This updates the version information. You can then perform a firmware upgrade.
DEV-8122	Conductor	When creating o modifying a cloud HIPservice, the **Name** and **Network name** fields do not check for the presence of invalid characters. This will be fixed in a later release. Workaround: Do not include • Uppercase characters • Spaces • Special characters, except for a dash
DEV-8097	HIPclient, macOS	If your computer has multiple active NICs and you select a specific NIC in your HIPclient configuration, the operating system will choose the NIC for outbound traffic. Workaround: None

ID	Applies to	Description
DEV-8060	Conductor	In rare cases, a Conductor HA pair will stop syncing. Workaround: If this happens, promote the HA-secondary to a primary, then re-pair them.
DEV-8051	Conductor	The IP address field on associated with a HIPswitch may be blank on the **HIP Services** tab. Workaround: You can locate the IP address information under the **Reporting** tab.
DEV-7955	Conductor	If you ping a HIPswitch running in Azure from another HIPswitch, it will fail in the Conductor UI. This is due to ICMP being denied by Azure's security groups. Workaround: None
DEV-7814	HIPclient, Windows	If user authentication fails, your user name is not retained and you must re-enter it. Workaround: None
DEV-7769	Conductor	Toggling policy on and off too quickly on a HIPswitch hosted in Google Cloud can result in the route table becoming out of sync when using route injection. Workaround: After toggling policy, wait 10 seconds before toggling it again.
DEV-7661	Conductor	When replacing a HIPswitch, the new HIPswitch may take a few minutes to reconnect and appear online in the Conductor. Workaround: Wait a few minutes after replacing the HIPswitch for it to display in the Conductor UI.
DEV-7499	HIPswitch	The bandwidth check in the HIPswitch **Diagnostics** tab might fail for HA-paired HIPswitches. Workaround: None
DEV-7125	Conductor, PCI	When exporting PCI data, HIP Services references may not display correctly when viewing the CSV file in Microsoft Excel. Workaround: None
DEV-7058	HIPswitch	When reconfiguring your underlay network from one physical port to another in the Conductor, the changes may not be applied successfully and the configuration will revert back to the original settings. Workaround: Make the configuration changes in diagnostic mode.
DEV-6590	Conductor	You can add a voucher code more then once from the **Licensing** tab. This does not create additional licenses, but is visually confusing. This will be fixed in a later release. Workaround: None
DEV-6587	Conductor	The **Licensing** tab may display invalid entries. Workaround: Remove the invalid items manually.

ID	Applies to	Description
DEV-6533	Conductor	When creating or editing a smart device group, rules can have the same ordinal values. This can cause unintended issues in the processing results. Workaround: When creating rules, verify each rule has a unique ordinal value.
DEV-6446	HIPclient, iOS	When viewing traffic stats in the iOS app, the chart may show negative values instead of zero. Workaround: None
DEV-6226	Conductor	A fully qualified domain name cannot be used for local or peer replication addresses on an HA Conductor pair. Workaround: None
DEV-6195	Conductor	The Conductor incorrectly displays an option to check bandwidth for HIPclients in diagnostic view. This option is not supported for HIPclients and will not function correctly if selected. Workaround: None
DEV-6118	AWS	The **Forgot my password** link can send an invalid Conductor location. Workaround: Replace the location in the link with the correct Conductor address.
DEV-5832	HIPswitch	Device NAT functionality currently does not work with layer 2 traffic. Workaround: None
DEV-5530	Conductor UI	In some cases, **Allow incoming pings (ICMP)** and **SYN Flood Protection** on the **Firewall** page may be disabled and won't toggle. Workaround: Refresh your browser to resolve the issue.
DEV-5430	Conductor	After configuring a Conductor for the first time, you may receive a **Lost connection to the original server** message if you select **Return to settings** too quickly. Workaround. Wait at least 20 seconds before selecting **Return to settings**.
DEV-5008	PCI Reporting	PCI Reporting shows the UUID reference instead of the name when generating a PCI report from **Settings** > **Advanced** > **PCI Reporting** > **Downloads** > **User Activities Report**. Workaround: To view names, you can download object references from the same page where you generated the PCI report.
DEV-2417	Conductor UI	The password reset email link defaults to the first web enabled interface, and will be successful only if an administrator configures the first interface with a publicly-facing default route. Workaround: None.

ID	Applies to	Description
DEV-1846	Conductor, HA	The standby Conductor UI in an HA pair will not timeout. This issue does not affect the master Conductor UI. Workaround: Log off manually when not using the standby Conductor UI.

Release Notes 2.1.3

Release Date: May 24, 2018

What's New

New in this release:

The HIPswitch 75 Series	The HIPswitch 75, released with 2.1.3, is designed for medical devices, point of sale systems, and others like building automation controls. It securely connects and protects those endpoints across all networks with little to no change to existing infrastructure. The HIPswitch 75 plug and play design makes universal connectivity and segmentation simple, fast, and cost-effective.
HIPserver for Linux	With this release, the HIPclient is now available for Linux. Your Linux devices now can natively connect to your IDN overlay, giving them a trusted and verifiable connection wherever you are. Multiple profiles allow you to easily switch between different IDN overlays as needed.
New platform support for Microsoft Azure and Google Cloud	You can now create, manage, and retire Microsoft Azure and Google Cloud HIP Services directly from the Conductor UI.
Support for offline Conductor licensing	We have added support to allow Conductors without access to the public Internet to complete voucher and provisioning requests with our licensing and provisioning server. You can export a sync package, send it to Tempered Networks Support, and import a file containing your licenses back in to your Conductor from a drop-down on the **Settings** > **Licensing** tab.
New API token system and improved token management	We have updated the API to make tokens more secure. All API requests now require two headers: • **X-API-Client-ID** is unique by user and can be found on your user preferences page • **X-API-Token** is generated from your user preferences page. This token is secret, so if you lose it, you must generate a new one. Whenever you refresh your token, all previous tokens will be expired. The client ID and a refreshed secret token may also be acquired via the API using basic authorization at/ `api/v1/token/generate`. Please refer to the API documentation for details.

	Note: The **X-Person-Email** and **X-Person-Token** headers are deprecated and no longer function.
New network creation wizard	New in this release is the ability to quickly create a hub-and-spoke or full mesh network using a simple, wizard-driven UI.

Upgrade Considerations

The 2.1.3 release includes all hotfixes from prior releases and addresses all known support cases at the time of release.

Note: You can now upgrade a HIPswitch directly to 2.1.3 from either 1.12.6 or 2.0.x. If you are running an earlier version of 1.12.x, we recommend you upgrade to 1.12.6 before upgrading to 2.1.3. When upgrading a Conductor, we recommend you upgrade to the latest stable 2.0.x first before upgrading to 2.1.3.

We recommend you upgrade to 2.1.3 if:	
You want to take advantage of performance and stability increases in 2.1, especially for any of the following features: • High Availability • Simple Connect® API	You were impacted by any issues discovered in prior releases, especially if you have any of the following: • Windows HIPclient issues • macOS HIPclient issues • Cellular connectivity

Extensive testing was conducted both in-house and with selected development partners, in lab and in production environments to ensure that performance is equivalent to 2.1.2. Additionally, 2.1.3 should be more stable than all prior releases.

Enhancements

Applies to	**Description**
Conductor	You can now run the Conductor without opening port 443 for HIPswitch communications.
High Availability	We have made performance improvements to Conductor and HIPswitch failover. Additionally, we added a progress bar during database synchronization.
HIPswitch 250e	The HIPswitch 250e now supports high-availability mode.
HIP Services	HIPswitches now support the option of setting a default route on the overlay network. This can be set on a per HIPswitch basis under the **Local Devices** > **Overlay Routes** section.
HIP Services	It is now possible to perform bulk operations on HIP Services in the Conductor UI, such as: • Manage • Revoke • Reactivate • Delete/Move • Check Online
HIPclient, Windows	We added additional diagnostic information in the support bundle to properly troubleshoot the HIPclient.

Applies to	Description
HIPclient, Windows	The Windows HIPclient was updated to take advantage of the latest security patches. • openssl 1.0.2o • curl 7.59.0 • JSON 10.0.3

Fixes

ID	Applies to	Description
DEV-8172	HIPswitch, Cellular	Fixed an issue where a HIPswitch 100g Verizon static IP SIM could not aquire its cellular address.
DEV-8144	HIPswitch 100g	Fixed an issue where a HIPswitch 100g modem would not correctly restart if link manager monitors failed.
DEV-8042	HIPswitch 250	Fixed an issue with the HIPswitch 250 cellular modem interface where the modem would sometimes fail to connect to the cellular network.
DEV-8017	Conductor	Fixed an issue where the Local Devices page for a HIPswitch would not display correctly after updating the properties, requiring a page refresh.
DEV-7990	HIPswitch	Fixed an issue that, would cause a HIPswitch to lose connectivity to local devices after rebooting.
DEV-7935	Conductor	Network Administrators are now able to create smart device groups.
DEV-7918	Conductor	Fixed an issue with smart device groups where negating rules that apply to CIDR/Overlay device networks returned zero device matches.
DEV-7894	HIPclient, Windows	Fixed an issue where the Windows HIPclient health data was not consistently sent to the Conductor.
DEV-7845	HIPclient, macOS	Fixed an issue where a macOS HIPclient would attempt to readdress HIP tunnels with its own overlay device IP after an address change.
DEV-7832	HIPclient, Windows	Fixed an issue where the configuration panel would not display correctly if all profiles were removed.
DEV-7746, DEV-7698	HIPswitch	Fixed an issue that caused HIPswitches to reboot when placed into diagnostic mode after being factory-reset while offline.
DEV-7699	HIPswitch 100g	Fixed an issue where changing the priority of a link may not set in a timely manner, causing problems with default routes.
DEV-7682	Conductor	Fixed an issue where importing legacy devices to the Conductor would not import device names.
DEV-7665	HIPswitch	Fixed an issue where the IMEI, IMSI, ICCID, MSIDSN, and Operator ID sent to the Conductor and displayed in the HIPswitch diagnostic UI were sometimes out of date.
DEV-7608	HIPswitch	Fixed an issue where DHCP IP address changes on the underlay network could result in HIP tunnel failures.
DEV-7565	HIPswitch	Fixed an issue where a HIPswitch configured in one-armed mode could cause downstream routing to local devices behind a HIPswitch to fail.

ID	Applies to	Description
DEV-7555	HIPswitch	Fixed an issue where file transfers for support bundle requests and firmware updates would not respect the link priority after link failovers on HIPswitches.
DEV-7547	Conductor	Fixed an issue in the Conductor that prevented configuring source NAT for HIPswitches running in one-armed mode.
DEV-7531	HIPswitch	Fixed an issue where an HA pair configured to use one-arm mode could preventing it from functioning correctly.
DEV-7500	Conductor	Fixed an issue where under some circumstances device activity would not display properly in the Conductor.
DEV-7482	Conductor	Fixed an issue where the Conductor would not report a local device's MAC address or device activity if the device was configured to use NAT.
DEV-7476	Conductor	Fixed an issue where subscription licenses would not display correctly if both perpetual and subscription licenses were present for a given model.
DEV-7431	HIPclient, macOS	Fixed an issue where the configuration file for a macOS HIPclient could grow unnecessarily large after repeated configuration changes.
DEV-7379	HIPswitch	A spurious UDP packet is no longer broadcast by a HIPswitch on start-up.
DEV-7367	HIPclient, Windows	Fixed an issue where a HIPclient would fail to connect to the Conductor after being provisioned, requiring a restart.
DEV-7366	API	Fixed an issue where changes to the HIPservice settings **device_auto_detect** and **enabled** using the API would not change the settings.
DEV-7330	HIPclient, macOS	Fixed an issue where a macOS HIPclient would occasionally stop responding.
DEV-7302	HIPswitch	Fixed an issue where an upgrade of a HIPswitch in one-arm mode would rewrite port 1 MAC address to the port 2 MAC address.
DEV-7295	HIPclient, iOS	Fix an issue where an iOS HIPclient would intermittently fail to build secure connections for a newly-added device policy.
DEV-7157	Conductor	Fixed an issues where underlay traffic stats were not displayed in the Conductor if MTU was set to greater than 9000.
DEV-7153	HIPswitch 400,HIPswitch 500	Fixed the following issues when configuring expansion ports in diagnostic mode on the HIPswitch 500 and the HIPswitch 400 with an 8-port expansion module: • The priority field is no longer visible while the expansion port is disabled. • Changing an expansion port to an underlay port now allows editing of the priority field.
DEV-7145	HIPswitch 400, HIPswitch 500	Fixed and issue where the HIPswitch 400 and HIPswitch 500 would display **Manage in Conductor** on the LCD display panel before being configured with a Conductor URL.

ID	Applies to	Description
DEV-7143	HIPswitch 400, HIPswitch 500	Fixed an issue where the HIPswitch 400 and HIPswitch 500 LCD panel would continuously display **Firmware Updating** after applying a Hotfix from the Conductor.
DEV-7104	HIPswitch 400	Fixed an issue where placing a factory reset HIPswitch 400 in diagnostic mode before it has displayed the **Manage in Conductor** message on the LCD, would reboot the HIPswitch.
DEV-7092	Conductor	Fixed an issue where auto-discovered devices may display as protected devices on the **Check Connectivity** section of the **Diagnostic** tab for a HIPservice
DEV-7060	HIPswitch	Physical HIPswitch models with LCD now properly display **Restarting...** when rebooted from the Conductor UI, Diagnostic Mode, or the LCD.
DEV-7050	Conductor	Fixed an issue where you may receive an error accepting the EULA, when configuring a new Conductor.
DEV-7025	HIPclient, iOS	Fixed an issue where an iOS HIPclient would not allow Conductor addresses to be updated.
DEV-7014	HIPclient, Windows	HIPclient for Windows will now generate a crash dump.
DEV-6891	HIPswitch	Fixed an issue where the Conductor would not display underlay IPs in the Conductor UI if a HIPswitch was configured with multiple underlay ports.
DEV-6887	Conductor, PCI	Fixed an issue where a HIPrelay rule was not added in the PCI user activities report.
DEV-6868	HIPswitch	Fixed an issue where HA-paired HIPswitches older than version 1.12.x remained offline in the Conductor after firmware-upgrading to 2.1.x.
DEV-6794	HIPswitch	Fixed an issue where remote logging would not function on HIPswitches after link failover occurred between wired and wireless connections.
DEV-6670	HIPclient, Windows	Fixed an issue where the HIPclient for Windows would not display High Availability peers correctly in network diagnostics.
DEV-6563	Conductor	Fixed an issue where device group additions and removals were not captured in PCI logs.
DEV-6460	HIPclient, iOS	Fixed an issue where a HIPclient for iOS would not update its version correctly in the Conductor.
DEV-6459	Conductor	Fixed an issue where devices configured with serial-over-IP do not display in the **Add devices** list when attempting to add them to an overlay.
DEV-6196	HIPswitch	Fixed an issue where you were able to enter an invalid IP address without receiving an error message when configuring the Conductor URL in diagnostic mode.
DEV-6015	API	Fixed an issue in the API where the **ip** filter with **GET /api/v1/HIP Services** would return an **Invalid filter parameter** message.
DEV-5892	HIPswitch	Fixed an issue where a HIPswitch would go offline when using the **Replace** function for HIPswitches on the **HIP Services** tab in the Conductor UI.

ID	Applies to	Description
DEV-5470	HIPswitch	Fixed an issues where the cellular port is missing following a factory reset of the HIPswitch.
DEV-5434	HIPswitch	Fixed an issue where clicking **Detect Devices** repeatedly on a HIPswitch properties page would generate excess traffic.
DEV-5089	API	Fixed an issue where some API calls would return a `null` string.
DEV-4944	HIPswitch	Fixed an issue where a HIPswitch may report it entered a firmware update state after installing a hotfix.
DEV-4846	HIPswitch	Fixed an issue where a HIPswitch would report it is detecting a device with the same IP as the default gateway and not display it when the HIPswitch was in one-arm mode and device discovery was on.
DEV-4357	HIPswitch-Cellular	Fixed an issue where the IMEI and MSISDN fields of a cellular modem were not displayed correctly in the Conductor and HIPswitch diagnostic UI.
DEV-4074	Conductor-SimpleConnect	Fixed an issue where the Conductor would not check if the gateway IP address is a valid IP on the overlay network when setting up an overlay DHCP server on a HIPswitch.

Known Issues

ID	Applies to	Description
DEV-8142	Conductor	If you click **Finish** two times very quickly when upgrading Conductor firmware, it may attempt to upgrade the Conductor twice simultaneously, causing both to fail. Workaround: Do not repeatedly click **Finish**.
DEV-8122	Conductor	When creating o modifying a cloud HIPservice, the **Name** and **Network name** fields do not check for the presence of invalid characters. This will be fixed in a later release. Workaround: Do not include • Uppercase characters • Spaces • Special characters, except for a dash
DEV-8120	HIPswitch, Azure	In rare cases, an Azure HIPswitch may fail to reconnect to the Conductor after a firmware upgrade. Workaround: In the Azure portal, restart the VM hosting the HIPswitch. It can take up to 10 or 15 minutes to come back online.
DEV-8119	Conductor	A reactivated HIPclient configured with an overlay IP is listed as two devices, and you are unable to remove the overlay IP. Workaround: Completely delete a revoked HIPclient and allow it to come back as unmanaged in the Conductor. You can then manage it and configure as desired.

ID	Applies to	Description
DEV-8097	HIPclient, macOS	If your computer has multiple active NICs and you select a specific NIC in your HIPclient configuration, the operating system will choose the NIC for outbound traffic. Workaround: None
DEV-8067	HIPswitch	Combining NAT'd local devices and an overlay VLAN tag will block outbound overlay traffic.
DEV-8060	Conductor	In rare cases, a Conductor HA pair will stop syncing. Workaround: If this happens, promote the HA-secondary to a primary, then re-pair them.
DEV-8051	Conductor	The IP address field on associated with a HIPswitch may be blank on the **HIP Services** tab. Workaround: You can locate the IP address information under the **Reporting** tab.
DEV-8049	Conductor	A network administrator may be able to view a HIPswitch group while restricted from viewing some of the HIPswitches in the group. The UI indicates the HIPswitch group is editable, but will error if modified. As a result, the user is signed out. Workaround: None
DEV-7962	HIPclient, Windows	If your computer enters sleep mode, upon waking it may cause the HIPservice to stop and start, taking 30-60 seconds to recover. Workaround: None
DEV-7959	HIPswitch 100	If you configures a VLAN tag on a HIPswitch 100, your currently-active tunnels may stop working. Workaround: To resolve this issue, perform an action that causes a HIP restart, such as: • Reboot the HIPswitch • Change the default encryption type
DEV-7955	Conductor	If you ping a HIPswitch running in Azure from another HIPswitch, it will fail in the Conductor UI. This is due to ICMP being denied by Azure's security groups. Workaround: None
DEV-7814	HIPclient, Windows	If user authentication fails, your user name is not retained and you must re-enter it. Workaround: None
DEV-7769	Conductor	Toggling policy on and off too quickly on a HIPswitch hosted in Google Cloud can result in the route table becoming out of sync when using route injection. Workaround: After toggling policy, wait 10 seconds before toggling it again.

ID	Applies to	Description
DEV-7661	Conductor	When replacing a HIPswitch, the new HIPswitch may take a few minutes to reconnect and appear online in the Conductor. Workaround: Wait a few minutes after replacing the HIPswitch for it to display in the Conductor UI.
DEV-7499		The bandwidth check in the HIPswitch **Diagnostics** tab might fail for HA-paired HIPswitches.
DEV-7125	PCI	When exporting PCI data, HIP Services references may not display correctly when viewing the CSV file in Microsoft Excel. Workaround: None
DEV-7058	HIPswitch	When reconfiguring your underlay network from one physical port to another in the Conductor, the changes may not be applied successfully and the configuration will revert back to the original settings. Workaround: Make the configuration changes in diagnostic mode.
DEV-6881	HIPswitch	The LCD panels in the HIPswitch 500 and Conductor-500 are 16-characters wide. Messages are currently formatted for a 20-character LCD screen and may be truncated or display on more than one line. This will be fixed in a later release. Workaround: None
DEV-6590	Conductor	You can add a voucher code more then once from the **Licensing** tab. This does not create additional licenses, but is visually confusing. This will be fixed in a later release. Workaround: None
DEV-6587	Conductor	The **Licensing** tab may display invalid entries. Workaround: Remove the invalid items manually.
DEV-6533	Conductor	When creating or editing a smart device group, rules can have the same original values. This can cause unintended issues in the processing results. Workaround: When creating rules, verify each rule has a unique ordinal value.
DEV-6507	Conductor	The throughput graph for a HIPservice may occasionally miss a data point and draws it as a zero value. Workaround: Refresh the page to properly display the data point.
DEV-6446	HIPclient, iOS	When viewing traffic stats in the iOS app, the chart may show negative values instead of zero. Workaround: None
DEV-6226	Conductor	Currently a fully qualified domain name cannot be used for local or peer replication addresses on an HA Conductor pair. Workaround: None

ID	Applies to	Description
DEV-6195	Conductor	The Conductor incorrectly displays an option to check bandwidth for HIPclients in diagnostic view. This option is not supported for HIPclients and will not function correctly if selected. Workaround: None
DEV-6172	Conductor	When assigning a 1.x.x.x local device IP address to a HIPclient, the Conductor may continue to display the previous IP of the device. Workaround: None
DEV-5832	HIPswitch	Device NAT functionality currently does not work with layer 2 traffic. Workaround: None
DEV-5530, DEV-5441	Conductor UI	In some cases, **Allow incoming pings (ICMP)** and **SYN Flood Protection** on the **Firewall** page may be disabled and won't toggle. Workaround: Refresh your browser to resolve the issue.
DEV-5448	Conductor UI	Clicking the **Swap roles** button for a secondary HA-paired HIPswitch will cause the UI to stop responding. Workaround: Refresh your browser.
DEV-5430	Conductor	After configuring a Conductor for the first time, you may receive a **Lost connection to the original server** message if you select **Return to settings** too quickly. Workaround. Wait at least 20 seconds before selecting **Return to settings**.
DEV-5428	Conductor UI	When you create a Smart Device Group with **Ignore auto-discovered devices until accepted** checked and then remove the setting, the Smart Device Group will continue to ignore unaccepted devices. Workaround: None
DEV-5343	Conductor UI	If you try and log in after your session has timed out, you may receive the following error: **The change you wanted was rejected.** Workaround: Refresh your browser and log in.
DEV-5008	PCI Reporting	PCI Reporting shows the UUID reference instead of the name when generating a PCI report from **Settings** > **Advanced** > **PCI Reporting** > **Downloads** > **User Activities Report** > **.** Workaround: To view names, you can download object references from the same page where you generated the PCI report.
DEV-4537	Conductor	When demoting a master Conductor to standby, the processing screen might not correctly update. Workaround: Refresh your browser.

ID	Applies to	Description
DEV-2417	Conductor UI	The password reset email link defaults to the first web enabled interface, and will be successful only if an administrator configures the first interface with a publicly-facing default route. Workaround: None.
DEV-1846	Conductor, HA	Currently the standby Conductor UI in an HA pair will not timeout. This issue does not affect the master Conductor UI. Workaround: Log off manually when not using the standby Conductor UI.

Release Notes 2.1.2

Release Date: February 9, 2018

Important: If you are upgrading your hardware appliance to version 2.1.2 of our software, contact Tempered Networks Sales for updated licenses.

What's New

New in this release:

The HIPswitch 250 Series

The HIPswitch 250 Series is our newest hardware product and the industry’s first identity-based industrial IoT gateway for Industrial Control Systems, OT, SCADA, and critical infrastructure. The HIPswitch 250 includes highly available uplinks over ethernet and up to two different cellular carriers, all actively monitored using fast failover and the ability to prioritize across both cellular and wired links. It also provides 8 x 1 Gbps and 4 x SFP (fiber or copper) with PoE, eliminating the need for ethernet switches and additional power sources. The HIPswitch 250 can also act as a HIPrelay, a feature introduced in version 2.0 of our software.

HIPclient for macOS and iOS

With this release, the HIPclient is now available for macOS and iOS. Your devices now can natively connect to your IDN overlay, giving them a trusted and verifiable connection wherever you are. Multiple profiles allow you to easily switch between different IDN overlays as needed. Additionally, integration with HIPrelay gives you seamless and secure mobility for your computers running Apple's macOS and your devices running iOS.

Link Manager

Link Manager supports all cellular platforms, including our new HIPswitch 250 Series, providing uplink redundancy and intelligent monitoring for one wired and two cellular uplinks. Dynamic switching occurs based on which port provides the best performance. Default monitors can be customized with your own destinations.

Integration with AWS

You can now create, manage, and retire AWS HIP Services directly from the Conductor UI. After creating a template, you can easily create more HIP Services to function as HIPrelays or protect virtual machines in your VPCs.

HIP Invitations	HIP Invitations, a new feature in 2.1, allow you to add mobile phones, tablets, and computers running a HIPclient or HIPserver to your IDN solution by sending the user an email containing an invitation. When the user accepts the invitation, the Conductor automatically takes care of all the steps to provision, license, manage, name, group, and create policy for the new HIPapp without manual steps by the administrator. HIPinvitations can be sent in bulk to entire organizations, and the Conductor will handle the rest.
Improved alerts and monitoring	In this release we added additional monitors, such as the **HTTP GET** monitor that allows you to parse web responses from devices in an overlay. Monitors have been expanded to support device groups and HIPservice groups. The event history graphs will now display frequently or recently triggered monitors.
Improved performance	We made significant performance improvements across the board for all platforms, with virtual HIPswitches and the HIPswitch 400 roughly doubling in performance.

Upgrade Considerations

The 2.1.2 release includes all hotfixes from prior releases and addresses all known support cases at the time of release.

Note: You can now upgrade directly to 2.1.2 from either 1.12.6 or 2.0.x. If you are running an earlier version of 1.12.x, we recommend you upgrade to 1.12.6 before upgrading to 2.1.2.

Important: You must upgrade your Conductor to the latest 2.1.2 software if you plan on using the HIPswitch 250 in your environment.

We recommend you upgrade to 2.1.2 if:	
You want to take advantage of performance and stability increases in 2.1, especially for our recently added features: • Adding our HIPswitch 250 to your environment • Increased HIPservice performance • HIPclients for additional operating systems • Simplified AWS deployments • Improved alerts and monitors	You were impacted by any issues discovered in prior releases, especially if you have any of the following: • Stability and connectivity issues with HIP Services • Issues with the HIPswitch 200

Extensive testing was conducted both in-house and with selected development partners, in lab and in production environments to ensure that performance is equivalent to 2.1. Additionally, 2.1.2 should be more stable than all prior releases.

Enhancements

ID	Applies to	Description
DEV-5368	Conductor UI	An improved version of the import devices feature has been implemented in 2.1.
DEV-6509	Diagnostic mode	Shared network ports have been renamed to **underlay** ports and device ports have been renamed to **local device network** ports in diagnostic mode.

ID	Applies to	Description
DEV-3427	HIPclient, Windows	Several enhancements have been made to the HIPclient for Windows: • Added IP/NIC/routing info, disk usage, memory usage, operating system version, and client installation version/date to event logging • Improved titles and formatting to align with other HIPservice diagnostic reports • Improved reporting so the log targets an active profile
DEV-3074	HIPclient, HIPserver	Multiple profiles have been added to the HIPclient and HIPserver, allowing multiple Conductor configurations.

Fixes

ID	Applies to	Description
DEV-7070	HIPclient, iOS	Fixed an issue where an iOS HIPclient would stop passing traffic through a HIP relay after the relay was restarted.
DEV-7064	HIPswitch, 250 Series	Fixed an issue where configuration of multiple ethernet underlay ports in diagnostic mode did not work as expected.
DEV-7061	HIPswitch, 250 Series	Fixed an issue where port 7 on the HIPswitch 250 could not be set to 100 Mbps SFP mode.
DEV-7001		Fixed an issue where multiple tunnels to a HIPservice behind a NAT through a HIP relay would fail to pass traffic when the UDP source port changed.
DEV-6767	HIPserver, Windows	Fixed an issue that caused the HIP service process to stop responding, preventing the HIPserver from restarting properly and coming back online.
DEV-6726	HIPswitch	Fixed an issue where the ping tool did not work correctly from the **Tools** page in diagnostic mode.
DEV-6704	Conductor	Fixed an issue where you could no longer edit the underlay port of a HIPswitch in one-arm mode if one-armed mode removed and multiple underlay network ports were configured.
DEV-6653	Conductor	Fixed an issue where a deleted HIPswitch that comes back online does not report traffic stats.
DEV-6524	HIPswitch, 400 Series	Fixed an issue where a HIPswitch 400 loses connectivity to the Conductor when configuring the HIPswitch to use one-arm mode.
DEV-6523	HIPswitch, 400 Series	Fixed an issue where changing the port configuration on a HIPswitch 400 would not revert back to its previous configuration if it was unable to contact the Conductor.
DEV-6505	Conductor	Fixed an issue where PCI reporting logs may include some passwords in the output.
DEV-6460		
DEV-6376	HIPclient, Windows	Fixed an issue where HIPclients continue to report health data at five minute intervals, regardless of changes made in the Conductor.
DEV-6309	HIPswitch	Implemented a software fix to a hardware error affecting the HIPswitch 250 front panel LEDs.

ID	Applies to	Description
DEV-6268	Conductor	Fixed an issue where two devices in two different device groups with policy to each other would cause the connection between the HIP Services and Conductor connection to restart repeatedly.
DEV-6174	Conductor	Fixed an issue where a smart device group containing a HIPswitch group in its rules would prevent any device activated from a HIP invite to be added to the group automatically.
DEV-6073	Conductor	Fixed an issue where HIPswitch connections to Conductor would fail if network latency was greater than 500ms.
DEV-5965	Conductor	Fixed an issue where re-enabling a revoked HIPclient would not preserve its external IP address.
DEV-5891	HIPswitch	HIPswitches will now advertise their NAT underlay IP address, if set.
DEV-5857	HIPswitch	A HIPswitch 200 diagnostic report does not display CPU temperature.
DEV-5541	Conductor	Fixed an issue where the **Limit upload bandwidth** option would disallow a packet capture on a HIPswitch until the it reboots.
DEV-5529	HIPswitch	Fixed an issue where adding an invalid overlay route to a HIPswitch from the Conductor UI would not create a route on the HIPswitch.
DEV-5526	Conductor UI	Fixed an issue where the Conductor would show devices that became active in real-time, not when active devices became inactive.
DEV-5425	BaseOS	Fixed security vulnerability CVE-2017-8890 https://nvd.nist.gov/vuln/detail/CVE-2017-8890
DEV-4558	HIPswitch, 250 Series	Fixed an issue present in that caused the multi-purpose button to not function.
DEV-3989	Conductor	Fixed an issue where you could pair HIPswitches in HA if there was no HA interface.
DEV-3619	Conductor	Fixed an issue where a recent activity email would include notifications for offline HIPclients.

Known Issues

ID	Applies to	Description
DEV-7153	HIPswitch 400,HIPswitch 500	You may experience the following issues when configuring expansion ports in diagnostic mode on the HIPswitch 500 and the HIPswitch 400 with an 8-port expansion module: • The priority field is visible while the expansion port is disabled. • Changing an expansion port to an underlay port does not enable editing of the priority field. Apply the change and then refresh your browser to allow edits to the priority field. • Due to the issue above, multiple ports may temporarily have the same priority until you have finished changing the priority field, which is normally not allowed.
DEV-7157	HIPclient, Windows	Underlay traffic stats are not displayed in the Conductor if MTU is set to greater than 9000. Workaround: None

ID	Applies to	Description
DEV-7145	HIPswitch 400, HIPswitch 500	The HIPswitch 400 and HIPswitch 500 may display **Manage in Conductor** on the LCD display panel before being configured with a Conductor URL. Workaround: None
DEV-7143	HIPswitch 400	The HIPswitch 400 LCD panel may continuously display **Firmware Updating** after applying a Hotfix from the Conductor. Workaround: None
DEV-7125	PCI	When exporting PCI data, HIP Services references may not display correctly when viewing the CSV file in Microsoft Excel. Workaround: None
DEV-7092	Conductor	On the Check Connectivity section of the Diagnostic tab for a HIPservice, auto-discovered devices may display as protected devices. Workaround: None
DEV-7050	Conductor	When configuring a new Conductor, you may receive an error when trying to accept the EULA. Workaround: Change the URL in your browser to *<ConductorURL>*/ **app** to continue.
DEV-6590	Conductor	You can add a voucher code more then once from the **Licensing** tab. This does not create additional licenses, but is visually confusing. This will be fixed in a later release. Workaround: None
DEV-6587	Conductor	The **Licensing** tab may display invalid entries. Workaround: Remove the invalid items manually.
DEV-6533	Conductor	When creating or editing a smart device group, rules can have the same original values. This can cause unintended issues in the processing results. Workaround: When creating rules, verify each rule has a unique ordinal value.
DEV-6507	Conductor	The throughput graph for a HIPservice may occasionally miss a data point and draws it as a zero value. Workaround: Refresh the page to properly display the data point.

ID	Applies to	Description
DEV-6459	Conductor	Devices configured with serial-over-IP do not display in the **Add devices** list when attempting to add them to an overlay. Workaround: **1.** Create a new Smart Device Group (SDG) **2.** Add a **CIDR** rule to the SDG and set the argument to `deviceIP`/32 **3.** Check **only match overlay device IP** **4.** Click **Save** **5.** You chould now be able to sucessfully add the group containing the device to your overlay
DEV-6446	HIPclient, iOS	When viewing traffic stats in the iOS app, the chart may show negative values instead of zero. Workaround: None
DEV-6226	Conductor	Currently a fully qualified domain name cannot be used for local or peer replication addresses on an HA Conductor pair. Workaround: None
DEV-6196	Conductor	When configuring the Conductor URL in diagnostic mode, you are able to enter an invalid IP address without receiving an error message. Workaround: None
DEV-6195	Conductor	The Conductor incorrectly displays an option to check bandwidth for HIPclients in diagnostic view. This option is not supported for HIPclients and will not function correctly if selected. Workaround: None
DEV-6172	Conductor	When assigning a 1.x.x.x local device IP address to a HIPclient, the Conductor may continue to display the previous IP of the device. Workaround: None
DEV-6130	HIPclient, Windows	Setting or removing a Local Device IP on a Windows HIPclient may cause the client to report that the HIPservice is not running. Workaround: Restart the HIPclient to resolve the issue.
DEV-5832	HIPswitch	Device NAT functionality currently does not work with layer 2 traffic. Workaround: None
DEV-5530, DEV-5441	Conductor UI	In some cases, **Allow incoming pings (ICMP)** and **SYN Flood Protection** on the **Firewall** page may be disabled and won't toggle. Workaround: Refresh your browser to resolve the issue.
DEV-5448	Conductor UI	Clicking the **Swap roles** button for a secondary HA-paired HIPswitch will cause the UI to stop responding. Workaround: Refresh your browser.

ID	Applies to	Description
DEV-5434	Conductor UI	Clicking **Detect Devices** repeatedly on the HIPswitch properties page will generate excess traffic. Workaround: Give the Conductor time to complete the operation.
DEV-5430	Conductor	After configuring a Conductor for the first time, you may receive a **Lost connection to the original server** message if you select **Return to settings** too quickly. Workaround. Wait at least 20 seconds before selecting **Return to settings**.
DEV-5428	Conductor UI	When you create a Smart Device Group with **Ignore auto-discovered devices until accepted** checked and then remove the setting, the Smart Device Group will continue to ignore unaccepted devices. Workaround: None
DEV-5343	Conductor UI	If you try and log in after your session has timed out, you may receive the following error: **The change you wanted was rejected.** Workaround: Refresh your browser and log in.
DEV-5008	PCI Reporting	PCI Reporting shows the UUID reference instead of the name when generating a PCI report from **Settings** > **Advanced** > **PCI Reporting** > **Downloads** > **User Activities Report** > **.** Workaround: To view names, you can download object references from the same page where you generated the PCI report.
DEV-4846	HIPswitch	If a HIPswitch is in port one-arm mode and device discovery is enabled, the HIPswitch will report an error. Workaround: None
DEV-4537	Conductor	When demoting a master Conductor to standby, the processing screen might not correctly update. Workaround: Refresh your browser.
DEV-2417	Conductor UI	The password reset email link defaults to the first web enabled interface, and will be successful only if an administrator configures the first interface with a publicly-facing default route. Workaround: None.
DEV-1846	Conductor, HA	Currently the standby Conductor UI in an HA pair will not timeout. This issue does not affect the master Conductor UI. Workaround: Log off manually when not using the standby Conductor UI.

Release Notes for Retired Hotfixes

These hotfixes have been retired.

Release Notes 2.2.8 Hotfix – Airwall Gateway HF-2 (Retired)

Release Date: Sep 15, 2020

What's New

2.2.8 Airwall Gateway Hotfix HF-2 includes and replaces Airwall Gateway Hotfix HF-1. Once installed, it will show both HF-1 and HF-2 as installed.	This is a hotfix to release v2.2.8 for the Airwall Gateway. See Release Notes 2.2.8 on page 673 for more additions in version 2.2.8. Download Airwall Gateway HF-2 from Hotfixes on page 548.

Note:

Also install Conductor HF-3, as it fixes some of these issues from the Conductor side. See Release Notes 2.2.8 Hotfix – Conductor HF-3 (Retired) on page 773.

Upgrade Considerations

Upgrade to this 2.2.8 hotfix if you were experiencing any of the following issues:

- Blocked traffic on Airwall Gateways after installing Airwall Gateway HF-1.
- Ping devices failures.
- Airwall Gateways needing to reconnect to the Conductor.
- Airwall Gateways failing a policy check on some overlay networks

Or if you were impacted by any of the other issues fixed in this hotfix.

Fixes

ID	Applies to	Description
DEV-14247	Airwall Gateway	Fixed a bug that was introduced in Airwall Gateway Hotfix rollup-1 that could cause traffic to get blocked on Airwall Gateways with multiple overlay port groups.
DEV-14190	Airwall Gateway	Fixed an issue that could cause traffic problems in deployments with multiple overlay port groups on the same broadcast domain.
DEV-14162	Airwall Gateway	Fixed an issue in Conductor HF-2 that was causing the "Ping devices" feature to fail for devices with plain IP addresses.
DEV-14115	Conductor	Fixed an issue that could cause infrequent Conductor service issues resulting in all Airwall Gateways needing to reconnect to the Conductor.
DEV-14067	Conductor, Airwall Gateway	Fixed an issue on 2.2.8 Airwall Edge Services that could cause false negatives in the policy check for some overlay network configurations.
DEV-13981	Airwall Gateway	Fixed an issue where setting an overlay default gateway prevented creating both the connected (local subnet) and default routes.
DEV-13974	OpenHIP	Fixed performance regression on multi-core platforms.
DEV-13926	OpenHIP	Fixed a rare packet allocation failure issue on Airwall Gateway-100.
DEV-13903	Airwall Gateway	Airwall Gateway-110 models now can use the link failover monitor.
DEV-13843	Airwall Gateway	Added firewall connection states to the diagnostic report.
DEV-13275	Airwall Gateway	Fixed an issue where a misconfigured local device was corrupting the ARP cache entries for peer Airwall Gateways.

Known Issues

See Release Notes 2.2.8 on page 673 for known issues.

Release Notes 2.2.8 Hotfix – Airwall Gateway HF-1 (Retired)

Release Date: Sep 3, 2020

What's New

2.2.8 Airwall Gateway Hotfix HF-1	This hotfix has been retired. These fixes are included in Airwall Gateway HF-2. to release v2.2.8 for the Airwall Gateway. See Release Notes 2.2.8 on page 673 for more additions in version 2.2.8. Download Airwall Gateway HF-1 from Hotfixes on page 548.

Note:

Also install Conductor HF-3, as it fixes some of these issues from the Conductor side. See Release Notes 2.2.8 Hotfix – Conductor HF-3 (Retired) on page 773.

Upgrade Considerations

Upgrade to this 2.2.8 hotfix if you were experiencing any of the following issues:

- Ping devices failures.
- Airwall Gateways needing to reconnect to the Conductor.
- Airwall Gateways failing a policy check on some overlay networks

Or if you were impacted by any of the other issues fixed in this hotfix.

Fixes

ID	Applies to	Description
DEV-14190	Airwall Gateway	Fixed an issue that could cause traffic problems in deployments with multiple overlay port groups on the same broadcast domain.
DEV-14162	Airwall Gateway	Fixed an issue in Conductor HF-2 that was causing the "Ping devices" feature to fail for devices with plain IP addresses.
DEV-14115	Conductor	Fixed an issue that could cause infrequent Conductor service issues resulting in all Airwall Gateways needing to reconnect to the Conductor.
DEV-14067	Conductor, Airwall Gateway	Fixed an issue on 2.2.8 Airwall Edge Services that could cause false negatives in the policy check for some overlay network configurations.
DEV-13981	Airwall Gateway	Fixed an issue where setting an overlay default gateway prevented creating both the connected (local subnet) and default routes.
DEV-13974	OpenHIP	Fixed performance regression on multi-core platforms.
DEV-13926	OpenHIP	Fixed a rare packet allocation failure issue on Airwall Gateway-100.

ID	Applies to	Description
DEV-13903	Airwall Gateway	Airwall Gateway-110 models now can use the link failover monitor.
DEV-13843	Airwall Gateway	Added firewall connection states to the diagnostic report.
DEV-13275	Airwall Gateway	Fixed an issue where a misconfigured local device was corrupting the ARP cache entries for peer Airwall Gateways.

Known Issues

See Release Notes 2.2.8 on page 673 for known issues.

Release Notes 2.2.8 Hotfix – Conductor HF-3 (Retired)

Release Date: Sep 3, 2020

What's New

2.2.8 Conductor Hotfix HF-3

This is a hotfix to release v2.2.8 for the Conductor. This hotfix rolls up the previous Conductor hotfixes HF-1 and HF-2, so you only need to install HF-3. See Release Notes 2.2.8 on page 673 for more additions in version 2.2.8. Download HF-3 from Hotfixes on page 548.

Note: Also install Airwall Gateway HF-2, as it fixes some of these issues from the Airwall Gateway side. See Release Notes 2.2.8 Hotfix – Airwall Gateway HF-2 (Retired) on page 770.

Upgrade Considerations

Upgrade to this 2.2.8 hotfix if you deploy Google or Alibaba Cloud Airwall Gateways from the Conductor, if you were running into the policy issues with Airwall Gateways, or were impacted by any of the other issues fixed in this hotfix.

Fixes

ID	Applies to	Description
HF-3 Fixes:		
DEV-14167	Windows Airwall Agent or Server	Fixed an issue where the Conductor was showing Windows Airwall Agents had an update available when they already had that version installed. Note that you may still see updates available for x64 Windows if you have x32 firmware downloaded on the Conductor.
Includes Conductor HF-2 Fixes:		
DEV-14103	Conductor	Fixed an issue where disabling or re-enabling network communications of a device would delete any tags on it. Updating a device, device group, Airwall group, overlay network, or people group via the API would delete any tags on the updated object.

ID	Applies to	Description
DEV-14080	Conductor	Fixed an issue where when adding a device directly to a device group in an Airwall Invitation or during user onboarding, some of the necessary information was not being sent to the Airwall Agents and Servers to fully enable policies.
DEV-14077	Conductor	Fixed an issue where the dashboard number for upgradeable Airwalls was including Airwalls that could apply an earlier version.
DEV-14073	Conductor	Underlay IPs for 2.2.8 Airwall Gateways are now in the "underlay_ips" key in the API.
DEV-14070	Conductor	Fixed an issue where Airwall Gateways coming online was not being included in an overlay network's Recent Activity.
DEV-14059	Conductor	Fixed an issue where you could apply HF-1 multiple times.
DEV-14032	Conductor	Fixed an issue where viewing an overlay's details page in timeline view could cause an error.
DEV-14009	Conductor	Fixed an issue where you sometimes couldn't remove static routes from an HA pair.
DEV-13944	Conductor, Airwall Gateway	Fixed an issue that caused device traffic to local devices (east/west) or bypass destinations to continue after disabling the device. Traffic to remote devices was not affected.
Includes Conductor HF-1 Fixes:		
DEV-13943	Conductor	Fixed an issue in the Tag Actions menu where devices with the tag were not included in the list of items that would be impacted by the action.
DEV-13942	Conductor	People groups can now be added as managers when creating new overlay networks.
DEV-13930	Cloud-Alibaba, Conductor	If you have created a new Alibaba Cloud Airwall Gateway with v2.2.8, there is an issue with the protected subnet id on the Cloud tab actually being the public subnet. **Workaround**: You can avoid this issue by installing this hotfix on the Conductor before creating any Alibaba Cloud Airwall Gateways. **Workaround if you have already created an Alibaba Cloud Airwall Gateway**: **1.** Apply this hotfix to your Conductor. **2.** If you are not using an NTP for system time, on the **Settings** page, **General setting** tab, under **System time**, select **Edit Settings**, and then Under **Update date and time**, select **Set browser time** and then select **Update**. **3.** For any cloud Alibaba Airwall Gateways, on the **Cloud** tab, **Diagnostic** subtab, click **Refresh**.
DEV-13912	Conductor	Fixed an issue where secure tunnel status was not accurately reporting tunnel status for HA-paired Airwall Gateway's.

ID	Applies to	Description
DEV-13904	Cloud-Google, Conductor	To deploy a 2.2.8 Google Cloud 300v Airwall Gateway from the Conductor, apply this hotfix.
DEV-13893	Conductor	Fixed an issue where you could select Airwall Edge Services that do not support health data for the health data monitor (for example, you now cannot select the Mac, Linux, or iOS platforms)
DEV-13888	Conductor	Fixed an issue where when you attempted to manage items from a **New Airwall Online** notification on the new Dashboard, it could be lost if another notice is received.
DEV-13870	Conductor	Fixed an issue where bandwidth would be reported multiple times, resulting in dashboard graphs reporting much higher throughput than the actual throughput.
DEV-13860	Conductor	Fixed an issue where when you were creating a new device, the **Port affinity** menu showed the first overlay port group, even though the value was set to **Detect automatically**.

Known Issues

See Release Notes 2.2.8 on page 673 for known issues.

Release Notes 2.2.8 Hotfix – Conductor HF-2 (Retired)

Release Date: Aug 19, 2020. This hotfix is included in Conductor HF-3. See Release Notes 2.2.8 Hotfix – Conductor HF-3 (Retired) on page 773.

Upgrade Considerations

Note: This hotfix HF-2 is included in HF-3 (see Release Notes 2.2.8 Hotfix – Conductor HF-3 (Retired) on page 773) and has been retired.

Fixes

ID	Applies to	Description
DEV-14103	Conductor	Fixed an issue where disabling or re-enabling network communications of a device would delete any tags on it. Updating a device, device group, Airwall group, overlay network, or people group via the API would delete any tags on the updated object.
DEV-14080	Conductor	Fixed an issue where when adding a device directly to a device group in an Airwall Invitation or during user onboarding, some of the necessary information was not being sent to the Airwall Agents and Servers to fully enable policies.
DEV-14077	Conductor	Fixed an issue where the dashboard number for upgradeable Airwalls was including Airwalls that could apply an earlier version.
DEV-14073	Conductor	Underlay IPs for 2.2.8 Airwall Gateways are now in the "underlay_ips" key in the API.
DEV-14070	Conductor	Fixed an issue where Airwall Gateways coming online was not being included in an overlay network's Recent Activity.

ID	Applies to	Description
DEV-14067	Conductor, Airwall Gateway	Fixed an issue on 2.2.8 Airwall Gateways that could cause false negatives in the policy check for some overlay network configurations.
DEV-14059	Conductor	Fixed an issue where you could apply HF-1 multiple times.
DEV-14032	Conductor	Fixed an issue where viewing an overlay's details page in timeline view could cause an error.
DEV-14009	Conductor	Fixed an issue where you sometimes couldn't remove static routes from an HA pair.
DEV-13944	Conductor, Airwall Gateway	Fixed an issue that caused device traffic to local devices (east/west) or bypass destinations to continue after disabling the device. Traffic to remote devices was not affected.

Known Issues

See Release Notes 2.2.8 on page 673 for known issues.

Release Notes 2.2.8 Hotfix – Conductor HF-1 (Retired)

Release Date: Jul 29, 2020. This Hotfix has been retired and replaced by HF-3. See Release Notes 2.2.8 Hotfix – Conductor HF-3 (Retired) on page 773.

Upgrade Considerations

Note: This hotfix HF-1 is included in hotfix HF-2 (retired) and HF-3 (see Release Notes 2.2.8 Hotfix – Conductor HF-3 (Retired) on page 773) and has been retired.

Fixes

ID	Applies to	Description
DEV-13943	Conductor	Fixed an issue in the Tag Actions menu where devices with the tag were not included in the list of items that would be impacted by the action.
DEV-13942	Conductor	People groups can now be added as managers when creating new overlay networks.
DEV-13930	Cloud-Alibaba, Conductor	If you have created a new Alibaba Cloud Airwall Gateway with v2.2.8, there is an issue with the protected subnet id on the Cloud tab actually being the public subnet. **Workaround**: You can avoid this issue by installing this hotfix on the Conductor before creating any Alibaba Cloud Airwall Gateways. **Workaround if you have already created an Alibaba Cloud Airwall Gateway**: **1.** Apply this hotfix to your Conductor. **2.** If you are not using an NTP for system time, on the **Settings** page, **General setting** tab, under **System time**, select **Edit Settings**, and then Under **Update date and time**, select **Set browser time** and then select **Update**. **3.** For any cloud Alibaba Airwall Gateways, on the **Cloud** tab, **Diagnostic** subtab, click **Refresh**.

ID	Applies to	Description
DEV-13912	Conductor	Fixed an issue where secure tunnel status was not accurately reporting tunnel status for HA-paired Airwall Gateway's.
DEV-13904	Cloud-Google, Conductor	To deploy a 2.2.8 Google Cloud 300v Airwall Gateway from the Conductor, apply this hotfix.
DEV-13893	Conductor	Fixed an issue where you could select Airwall Edge Services that do not support health data for the health data monitor (for example, you now cannot select the Mac, Linux, or iOS platforms)
DEV-13888	Conductor	Fixed an issue where when you attempted to manage items from a **New Airwall Online** notification on the new Dashboard, it could be lost if another notice is received.
DEV-13870	Conductor	Fixed an issue where bandwidth would be reported multiple times, resulting in dashboard graphs reporting much higher throughput than the actual throughput.
DEV-13860Th	Conductor	Fixed an issue where when you were creating a new device, the **Port affinity** menu showed the first overlay port group, even though the value was set to **Detect automatically**.

Known Issues

See Release Notes 2.2.8 on page 673 for known issues.

Get Support

You can often find answers to your questions in Airwall helpthe guide. If you still need help, check here for help getting support.

Here are your options for getting support:

- Browse the Knowledge Base (KB) Articles on page 778 to see if your issue is covered.
- Create a Support Request.
- Contact Customer Success at support@tempered.io. For what information to include, see How to get support on page 181.

How to get support

You can often find answers to your questions in Airwall helpthe guide, or by logging in to your **Support** account and searching the knowledge base articles. If you still cannot find what you are looking for, you can contact support for help.

Note: You must have a current support contract with Tempered to open a support ticket.

There are several ways to contact support.

Open a case on the Tempered Support Web Portal

1. Go to https://www.tempered.io/support/supportReq.html.
2. Sign in using your support account log in.
3. Click + or **New**.

4. Fill in the name and contact information.
5. Provide the **Information to Include** listed below.
6. Attach the support bundle from the affected devices.
7. For network issues, attach a packet capture.

Contact Tempered Support via email

1. Send an email message to Customer Success.
2. Provide the **Information to Include** listed below.
3. Attach your support bundle to the email.
4. For network issues, attach a packet capture.

Information to Include

Provide the following information when you open a case with Tempered Support:

- A full description of the issue, including the following details:
  - The symptoms of the issue, including a brief description of all systems applicable to the configuration.
  - The approximate time the issue first occurred.
  - The number of times the issue has recurred.
  - Any error output provided by the system.
  - Steps to reproduce the issue.
  - Any changes you made to the system close to when the issue first occurred.
  - Any steps you've taken to resolve the issue.
  - Whether this is a new implementation.
  - How many data centers and devices are applicable to the configuration.
  - Which devices are affected by the issue.
- A description of the impact the issue is having on your site.
- Days and times you are available to work on the issue, and any alternative contacts that can work on the issue if you are not available.

Get a Support Bundle

The Support Bundle is the technical information about the device. To best answer support issues, Tempered Support needs the Support Bundle from the Conductor and Support Bundles from any Airwall Gateway, Airwall Agent, and/or Airwall Server that is part of the issue you are reporting. For more assistance, see Create a support bundle for a Conductor on page 481.

Get a Packet capture

If the issue involves the network, perform a packet capture while the issue is occurring. Provide this packet capture when you open the case. For more assistance, see Do a packet capture for an Airwall Gateway on page 482.

Knowledge Base (KB) Articles

Check these Knowledge Base articles for solutions to common issues.

Connect KB Articles

Help with issues trying to connect or configure Airwall Agents and Servers.

Do I need to reinvite my Windows Airwall Agent after I update the software?

You do not need to reinvite a device to the network once you have upgraded your Airwall Agent or Server. When you update, it retains the previously-configured settings and profiles.

Set a Preferred Network to Cellular on an Android Airwall Agent

Most Android devices will not use Cellular if either Wifi or Ethernet is available. If you want to set your Preferred Network to Cellular, most devices require that you enable **Mobile data always active** in your device's Developer options.

To do this, on your Android device, you need to:

1. Enable Android **Developer Options**.
2. Enable **Mobile data always active**.

More details on how to do this are in the following sections.

Enable Developer Options

1. On your Android device, go to **Settings** > **About Phone** .
2. Tap **Software Info** > **Build Number**.
3. Tap **Build Number** seven times. After the first few taps, you should see the steps counting down until you unlock the developer options. You may also have to tap in your PIN for verification. Once developer options are activated, you see a message: `Developer mode is now turned on`.
4. Go back to the **Settings** page, where you will now find Developer options as a choice at the bottom.

To enable “Mobile data always active”

1. Go to **Settings** > **Developer Options**.
2. Enable **Developer Mode**, if needed.
3. Under **Networking**, scroll to find **Mobile data always active**, and tap to enable it.

Set your preferred network in the macOS Airwall Agent

The macOS Airwall Agent no longer uses the Network option, but instead automatically uses the network preferences on your macOS system settings. You can change the networks used by the Airwall Agent by changing your macOS system settings.

Note: This setting is a system-wide setting, and affects network preferences for your entire macOS system.

1. On your macOS computer, click the WiFi icon, and select **Network Preferences**.
2. Under the list of available networks, click the gear or ... icon, and select **Set Service Order**.
3. Drag the network options to set the network order you prefer, and then click **OK**.

Upgrade a macOS Airwall Agent key

The macOS Airwall Agent may lose access to the macOS keychain following an update to 2.2. If this occurs, use the procedure below to resolve the issue

1. Open the macOS finder by pressing `Command-N`.
2. Find the **Airwall** application, right-click it and select **Show Package Contents**.
3. Double-click **Contents**.
4. Double-click **MacOS**. Keep this window available, you will need it below.
5. Open the **Keychain Access** app (**Applications > Utilities > Keychain Access**).
6. Navigate to the **System** keychain (on the upper left).
7. Click on **Keys** (on the lower left).
8. Click on the header named **Name** to sort the keys.
9. For each private key with the name **com.temperednetworks** do the following:

   - Open the key (double-click on it).
   - Select **Access Control**.
   - Enter your password.
   - Select +.

- Drag the *tnw-hipd* from the window opened earlier and drop it into the window you opened by tapping +.
- Select **tnw-hipd**, then select **Add**.
- Select **Save Changes**.
- Make a note of your username, you will need this in a moment.
- Enter your password and select **Allow**.
- You will be prompted to enter your username and password. Do so and close the **temperednetworks** window.

10. Repeat step 9 for each private key named **com.temperednetworks**. You will have one key for each Airwall Agent profile you created.

Update Airwall Agents and Servers

How to update your Airwall Agent or Server by platform. For Windows, macOS, and Linux, download the latest version from Latest firmware and software on page 514.

Windows

Install the newest version of the Airwall Agent or Server on top of your previous version. The previous software is completely uninstalled and the latest software is installed in its place, with profiles retained.

macOS

Run the installer, and the existing software is replaced with the newest, with your profiles retained.

Linux

Install your DEB/RPM package on top of the existing package, and it is replaced with the newest, with your profiles retained.

Should you choose to uninstall first, your profiles are retained at /etc/tnw/. These profiles become available again after you reinstall the software.

iOS

Update from the Apple App Store. This is the only way to install or update the iOS Airwall Agent.

Android

Update from the Google Play store. You can also request an APK file if you wish to sideload it, or if you intend to install it on an Android device that does not include Google Play services.

The Android Airwall Agent is not available on any third-party app stores.

Manage KB Articles

Help with issues trying to manage an Airwall secure network.

Collect data from a Windows Airwall Agent or Server for advanced diagnostics

Sometimes Customer Success needs additional information to fully diagnose issues with Airwall Agent or Server software. Support bundles only contain logs regarding our software and limited information about your system, and sometimes these bundles cannot be collected at all in the event of an installation failure or a Conductor connectivity issue.

Below is a list of the additional data from your Windows system that you can provide us to fully diagnose issues with your Windows Airwall Agent or Server. Send all of these files to Tempered Customer Success at Customer Success:

1. A copy of C:\Windows\INF\setupapi.dev.log.
2. The zipped ..s of "C:\Program Files (x86)\TemperedNetworks\".
3. The output from the systeminfo command.

4. System and Application logs exported in EVTX format from the Windows Event Viewer.

More information on how to get this additional data is in the following sections.

setupapi.dev.log

This file records installation events from many installers, and records failures and warnings. It contains information regarding the installation of our product, and can sometimes provide information that complements Tempered software's internal logs. Warnings from other installers can also point us in the direction of a potential system problem.

1. In the Windows File Manager, open the C:\Windows\INF folder.
2. Copy the setupapi.dev.log file and send it to Customer Success.

C:\Program Files (x86)\TemperedNetworks\

This is where the Airwall Agent or Server installs the software and store profiles. Some sensitive information is stored here, so encrypt this data before transmitting it.

1. In the Windows file manager, go to C:\Program Files (x86)\.
2. Right-click on the TemperedNetworks folder, and select **Compress to ZIP file**.
3. Send the zip file to Customer Success using a secure method, or encrypt the file before sending it.

systeminfo

This file outlines the hardware and software configuration of the system, providing a more complete view of the environment in which the Airwall Agent or Server software is running.

1. Open a terminal window.
2. Run the `systeminfo` command and send the output to a text file:

```
systeminfo > systeminfo.txt
```

3. Send the systeminfo.txt file to Customer Success.

System & Application Logs

System logs are all events observed and recorded by the Windows operating system. Application Logs are all events observed and recorded by software installed on your Windows computer. These logs show everything else your system was doing at the time of a failure, and can help diagnose the cause of the problem you are reporting.

To export these logs

- Open the Windows **Event Viewer**.
- Expand **Windows Logs**, and select either **Application** or **System**.
- Under **Actions**, select **Save All Events As**.
- In the **Save As** window, make sure the **Save as type** is **Event files (*.evtx)**.
- Do these steps for the other logs, and Send these event files to Customer Success.

Conductor fails to import update packages

If your Conductor fails to import update packages, you may need to reboot the Conductor.

Solution

1. In the Conductor, go to **Settings** > **Diagnostics**.
2. Under **Actions**, select **Reboot Airwall Conductor**.
3. Try importing the update packages again.

How to filter with the Conductor API

For any filter of an API request, append `?filter=description::*filter_term*` to the end of the request.

Python Example

```
#!/usr/bin/python3
from pprint import pprint
import sys
import requests
from requests.packages.urllib3.exceptions import InsecureRequestWarning

# Suppress cert warning
requests.packages.urllib3.disable_warnings(InsecureRequestWarning)

URL = "https://<conductor>/api/v1/""
HEADERS = {
    'x-api-client-id': '<client_id>',
    'x-api-token': '<token>',
    'content-type': 'application/json'
}

def get_hipservices():
    """
    Get all hipservices in Conductor

    :returns: hipservices json
    """
    r = requests.get(URL + 'hipservices?filter=description::*Airwall*',
 headers=HEADERS, verify=False)

    if r.status_code == requests.codes.ok:
        return r.json()

    print('Error getting hipservices. HTTP error code:
 {}'.format(r.status_code))
    return {}

def main():
    hipservices = get_hipservices()
    pprint(hipservices)

if __name__ == "__main__":
    try:
        main()
    except KeyboardInterrupt:
        sys.exit()
```

API documentation

The most recent API documentation is available in your Conductor. See Airwall API on page 508.

How to turn on full-tunnel configuration for Windows Airwall Agents and Servers (v2.2.2 and v2.2.1)

How to configure Windows Airwall Agents and Servers for full-tunnel.

Full Tunnel on v2.2.2 Airwall Agents

1. Select an Airwall Gateway to be the gateway for ingress traffic for the Airwall Agent. (The Airwall Gateway you want to protect the device).
2. Add a fake 0.0.0.0 device to the Airwall Gateway on its **Local devices** page.

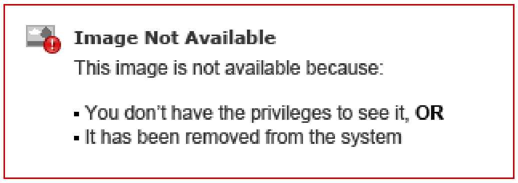


Image Not Available

This image is not available because:

- You don't have the privileges to see it, **OR**
- It has been removed from the system

3. Add the 0.0.0.0 device, the Airwall Agents, and the destination device to an Overlay network.
4. Whitelist "trust" the HIPclients to the 0.0.0.0 device. All HIPclients on that Overlay will turn into full-tunnel mode.

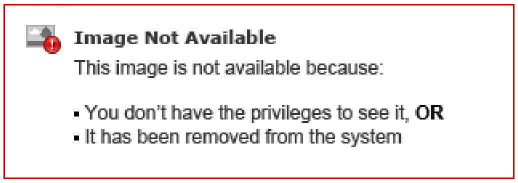


Image Not Available

This image is not available because:

- You don't have the privileges to see it, **OR**
- It has been removed from the system

5. Turn on **Source NAT** on Gateway HIPswitch. Step (3) above is crucial, while the rest depends on what exactly you want to achieve.

Full Tunnel on v2.2.1 Airwall Servers

For an Airwall Server: is just a "flip of the switch" firewall switch in the Airwall Server **Local Device** tab.

1. In the Conductor, open the page for the Airwall Server.
2. Go to **Local devices** > **Port filtering**.
3. Select **Edit Settings**.
4. Toggle the **Enable port filtering** Slider to **Enabled**"
5. Select **Update Settings**.

Is my Airwall Edge Service using the Airwall Relay?

How to tell if an Airwall Edge Service is using an Airwall Relay

There are two ways to check Airwall Relay connectivity:

- Run Airwall Relay diagnostics
- Analyze a Packet capture

Run Airwall Relay Diagnostics

While passing traffic over the HIP tunnel, check the Airwall Relay diagnostics on the page for the Airwall Relay.

1. Make sure there is traffic passing through the Airwall Relay.
2. On the page for the Airwall Relay, go to **Diagnostics** > **Airwall Relay diagnostics**.
3. Under **Active Connections**, select **Update data**.
4. The diagnostics show a table with traffic stats for Airwall Edge Services communicating over the Airwall Relay.

Analyze a Packet Capture

1. Start an Underlay packet capture from an Airwall Gateway:
   a) **On the Airwall page, go to the Diagnostics tab, and the Data capture subtab.**
   b) Under **Packet capture**, click **Start packet capture**.
   c) Under Capture interface, select HIP, and then select OK.
2. Run Secure Tunnel tests:
   a) **On the Airwall page, go to the Diagnostics tab and Secure Tunnels subtab.**
   b) **Check Build new tunnels if none exist.**
   c) Select **Check Secure Tunnel**.
3. Review the packet capture

a) **Go back to the Data capture subtab, and click Stop packet capture. Wait while the Conductor processes the file.**
b) **When the Conductor is finished, you will see a download link below the button. Download the PCAP file and review to see which Airwall Edge Services connected directly, vs. via the Airwall Relay.**

Return a hardware appliance

What to expect if you need to return a hardware appliance.

If you have a hardware malfunction, before you return it, you may need to request approval for a replacement, called an RMA (Return Manufacturing Approval).

The following events are likely reasons to assume hardware problems:

1. No Information/Status light or blink code.
2. No link lights on any interface.
3. Cannot enter Diagnostic mode.
4. Do not get the login shell when you connect via the console port.

Solutions

You can try a factory reset, or request troubleshooting help from Tempered Customer Success to try to resolve the issue. If those do not resolve the issue, you can request a replacement.

Factory Reset

Before you start a return, try a factory reset and see if that resolves the issue:

1. Factory Reset an Airwall Gateway on page 496.
2. Remove the Airwall Gateway entirely from Conductor, and then re-provision it.

Request Troubleshooting help from Tempered Customer Success

Tempered Customer Success needs to know what behavior you're observing to determine if there is an explanation for the issue you're seeing that can be resolved without replacing the hardware, or if the hardware needs to be replaced.

1. Send the following to Customer Success:
   - **Status** on information/status lights, diagnostic mode, and console access (if applicable).
   - A **Support bundle** from your Conductor, as well as from the affected device (if possible - older bundles work if you have one on file).
   - A **complete description** of the problem you are experiencing.
2. Tempered support will analyze the support bundle and the information you send and help you troubleshoot.

Request to Return and Replace the hardware

When you are troubleshooting the issue, Tempered Customer Success may let you know they've determined a replacement is necessary. Send the following information to Customer Success so they can send your replacement hardware:

- **Serial Number** printed on the sticker of the device.
- **A name and address** to send your replacement.

When your replacement unit arrives, use the provided shipping label to return your existing equipment in the same box.

Migrate a voucher

You can migrate a license voucher for Airwall Edge Services. You cannot migrate a Conductor voucher to another Conductor.

To migrate a license voucher for Airwall Edge Services, see Transfer a license to another Airwall Edge Service on page 196.

If you need assistance, contact Customer Success.

Deploy KB Articles

Help with issues trying to deploy an Airwall secure network.

Cellular management changes for 100g Airwall Gateway (v2.1.3 and later)

Starting in v2.1.3, the cellular management utility on the 100g Airwall Gateway (HIPswitch) no longer has an APN auto-connect feature enabled. It has been disabled on the cellular modem due to longevity and stability issues.

Prior to this change, the modem used the configured APN only as a suggestion. If it receives an alternative APN from its provisioning, or the APN is misconfigured, it will still connect without providing input to the user with some carriers and configurations. This can cause connection issues.

Solution

Enter the exact APN as what is provisioned for the SIM card as given by the cellular provider.

AES-256 CBC with HMAC SHA256

Given an MTU of 1500, the maximum plain text Overlay Ethernet frame size without fragmenting on the ciphertext underlay is 1421 bytes.

The Airwall Gateway HIP tunnel adds 79 bytes of overhead. For each frame (less than 1421 bytes), our overhead varies between 79-94 bytes.

AES-256 GCM

Given an MTU of 1500, the maximum plain text overlay Ethernet frame size without fragmenting on the ciphertext underlay is 1425 bytes.

The Airwall Gateway HIP tunnel adds 67 bytes of overhead. For each frame (less than 1425 bytes), our overhead varies between 67-78 bytes.

To allow for the HIP tunnel overhead due to encapsulation, use an MTU of 1500.

Configure overlay routes on an Airwall Gateway running in one-arm mode (v2.0.x and v2.1.x)

How to configure overlay routes on an Airwall Gateway running in one-arm mode.

Supported Versions	v2.0.x and v2.1.x Conductors

The overlay and underlay are considered the same when it is set up as a one-arm configuration.

1. Set a custom static route on the Airwall Gateway for devices using a different gateway.
2. Open the Airwall Gateway and go to **Local devices**.
3. Find **Overlay Routes**, and set an overlay route there. Do not use this route when you set it on the Airwall Gateway.

Connect a VLAN network across multiple Airwall Gateways

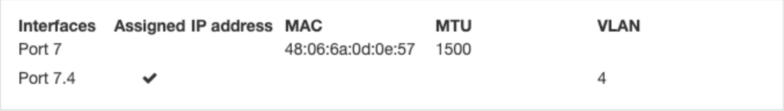
To connect multiple VLAN-tagged networks together, you do the following:

- Configure VLAN settings on both Airwall Gateways
- Add all devices to the Airwall Gateways
- Set trust betweem the devices in an overlay.

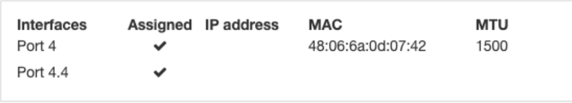
Airwall Gateways remove the VLAN tags from packets as they enter the overlay network, and add them back when they leave. Packets can jump from one VLAN to another seamlessly. You must configure VLANs explicitly on each Airwall Gateway.

In this tutorial, two locations are being connected with a 250 and a 150 Airwall Gateway.

1. Configure a port on each Airwall Gateway to have a VLAN tag available. This creates additional port objects in the format "Port NUM.VLAN"

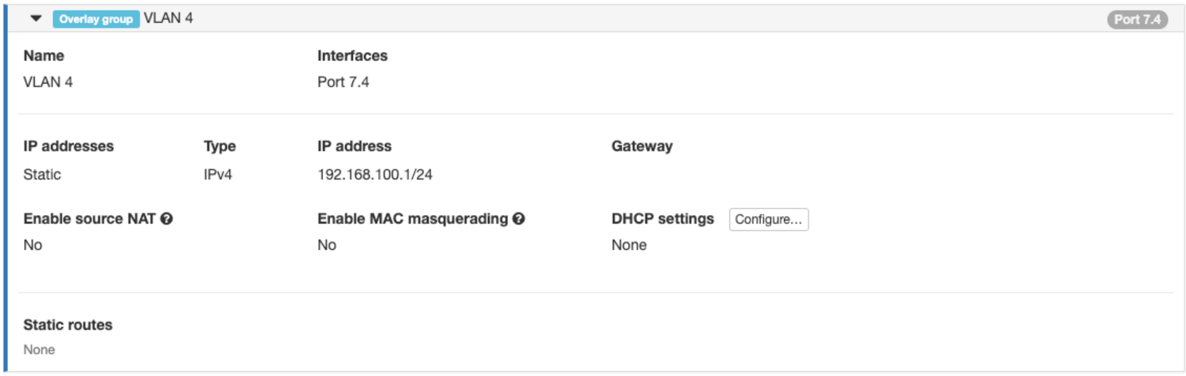


Interfaces	Assigned	IP address	MAC	MTU	VLAN
Port 7			48:06:6a:0d:0e:57	1500	
Port 7.4	✓				4



Interfaces	Assigned	IP address	MAC	MTU
Port 4	✓		48:06:6a:0d:07:42	1500
Port 4.4	✓			

2. Create an Overlay Port Group for this new VLAN (or add the VLAN to an existing Overlay Port Group).



VLAN 4

Name: VLAN 4

Interfaces: Port 7.4

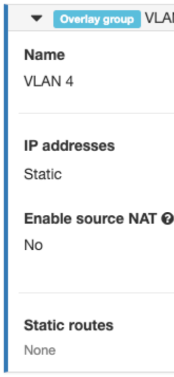
IP addresses	Type	IP address	Gateway
Static	IPv4	192.168.100.1/24	

Enable source NAT: No

Enable MAC masquerading: No

DHCP settings: None

Static routes: None



VLAI

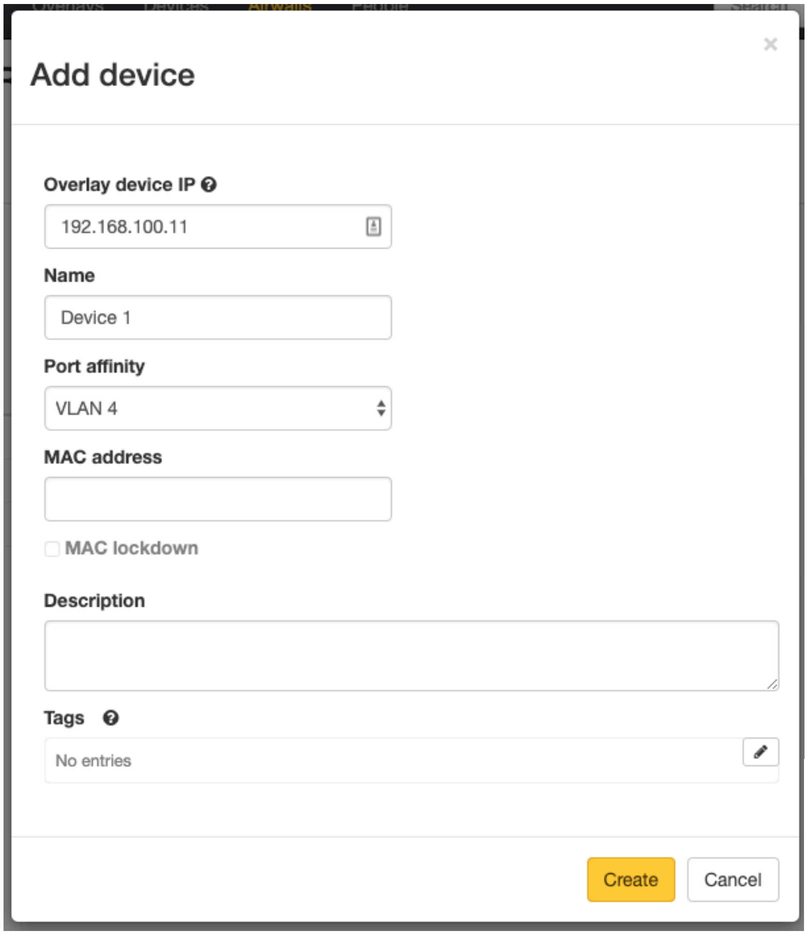
Name: VLAN 4

IP addresses: Static

Enable source NAT: No

Static routes: None

3. Add the devices that need to communicate with each other behind each Airwall Gateway, and make sure to set Port Affinity / Port Group to the Overlay Port Group that includes the desired VLAN tags.



Add device

Overlay device IP: 192.168.100.11

Name: Device 1

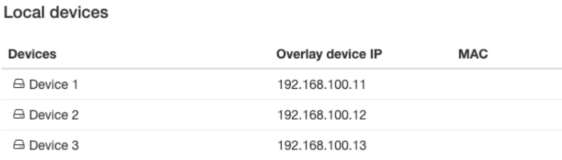
Port affinity: VLAN 4

MAC address:

□ MAC lockdown

Description:

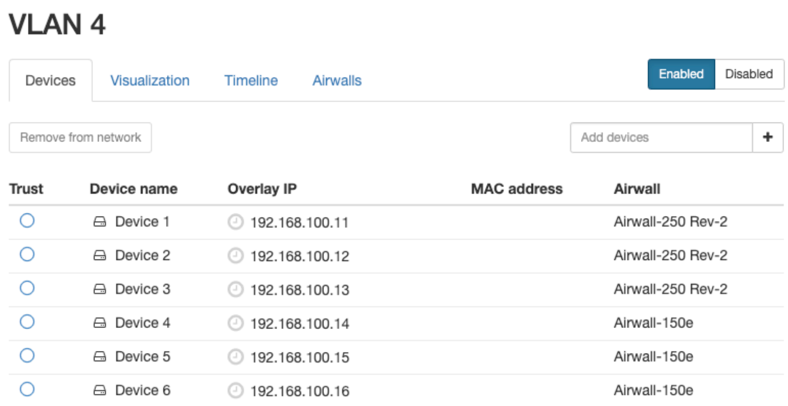
Tags: No entries



Local devices

Devices	Overlay device IP	MAC
Device 1	192.168.100.11	
Device 2	192.168.100.12	
Device 3	192.168.100.13	

4. Create a new overlay to add the devices to (or add them to an existing overlay) and give them policy with each other:



Trust	Device name	Overlay IP	MAC address	Airwall
○	Device 1	192.168.100.11		Airwall-250 Rev-2
○	Device 2	192.168.100.12		Airwall-250 Rev-2
○	Device 3	192.168.100.13		Airwall-250 Rev-2
○	Device 4	192.168.100.14		Airwall-150e
○	Device 5	192.168.100.15		Airwall-150e
○	Device 6	192.168.100.16		Airwall-150e

All of the devices should now be able to communicate with each other through the Airwall Gateways.

Deployment Tools for Hyper-V and Powershell

Deployment tools you can use to download Hyper-V images, create networks, and deploy a virtual Conductor and virtual Airwall Gateways.

Before you begin

These deployment tools instructions make the following assumptions:

- Image directory is C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\""
- Public network is named **vSwitchPublic**
- Protected network is name **vSwitchProtected**
- Your work directory hosts the script and the respective variables file. If you do not have a variable file, you can enter options interactively.

Download Hyper-V Powershell deployment tools

To download the deployment tools, enter the following commands:

```
cd C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\

wget https://temperedsoftware.s3.amazonaws.com/images/hyperv/tnw-hyperv-
deployment-tools-2.1.6-86.zip

unzip tnw-hyperv-deployment-tools-2.1.6-86.zip
```

Create public and private networks

To create networks named **vSwitchPublic** and **vSwitchProtected**, enter:

```
.\hyperv_deploy_network.ps1
```

Deploy a Conductor

To deploy a Conductor on the vSwitchPublic network, enter:

```
.\hyperv_deploy_conductor.ps1
```

Deploy an Airwall Gateway

To deploy an Airwall Gateway with a network adapter on each of the networks **vSwitchPublic** and **vSwitchProtected**, enter:

```
.\hyperv_deploy_hypswitch.ps1
```

Note: Deploy your protected virtual assets on the **vSwitchProtected** network.

Do cellular Airwall Gateways v2.2.3 and earlier work on the GCI cellular network?

No. The modems in the v2.2.3 and earlier 150 and 250 Airwall Gateways do not connect to the GCI network correctly when you insert a GCI SIM.

This may be addressed in future software updates from the cellular modem vendor.

Do I configure IPs for both HA Conductors on my Airwall Gateway?

No, you only need to configure Conductor (MAP) URL with the IP or DNS of the active Conductor. Once provisioned and connected to Conductor, AAirwall Gateways get the standby Conductor's IP configuration.

Do I need to use both cellular antennae?

Yes. The certification requirements for cellular modem require that both antenna be installed in operation. Tempered provides the correct number of antenna for each unit.

Does Airwall serial over IP support IEC-101?

IEC-101 is a fairly flat serial protocol, so it should work well with the Airwall Solution's serial-over-ip interface.

Please note, this interface simply encapsulates serial over a TCP connection. It does no processing, and does not respect framing. The software communicating with the IEC-101 devices needs to be able to reassemble the network frames.

As with any serial protocol and network software, test your exact combination to make sure it functions as expected.

Does Tempered support cellular Cat M1 service from Verizon?

No. Tempered does not have a Low Power (Cat M1) cellular modem currently available.

File proxies over Conductor MAP server (v2.1.3 and later)

As of Conductor version 2.1.3, Airwall Gateways running v2.1.3 and later use their established MAP connection (TLS 8096) to upload and download files from Conductor. This is useful when Airwall Gateways need to upload a packet capture or download a new firmware update.

Previously, Airwall Gateways relied on communication with the Conductor HTTPS web interface on TLS 443 for these downloads. Now, 443 does not need to be open to the Internet to allow Airwall Gateways to upload or download files.

Airwall Gateways prior to v2.1.3 use the older HTTPS/443 method for file transfers.

LSI Addresses in the 1.0.0.0/8 subnet

Airwall products use the 1.0.0.0/8 subnet by default to route packets between protected devices. It then translates those addresses to the addresses and subnets you configure in Conductor.

These addresses are called Local Scope Identifiers (LSI), and they are cryptographically derived from the Host Identity Tag (HIT).

You can change it if you are sure of your settings. If you cannot, here are some caveats:

- These APs cannot use Cloudflare DNS, and they badly interfere with Airwall Agents and Servers.
- You cannot connect to anything on the 1.0.0.0/8 subnet. This includes Cloudflare's 1.1.1.1 DNS service. On Airwall Agents and Servers, it stops routing traffic to that subnet, despite being a split-tunnel. On Airwall Gateways, it routes to the LSI gateway, rather than out of your Internet gateway (provided you have one configured).
- There is also a tiny chance that that two Airwall Edge Services might end up colliding. If this happens (extremely rare!), factory reset your Airwall Gateway or delete your profile on your Airwall Agent or Server to generate a new HIT.

Cause

This subnet was initially unused, and is not one covered under RFC-1918. It wasn't in use on the Internet when we (and other companies) first started using it; however, it is now fully allocated in Asia and the Pacific - and the 1.1.1.0/24 subnet has been famously purchased by CloudFlare for the 1.1.1.1 DNS service.

Related information

LSI conflict error on the Conductor on page 805

You cannot use any part of the 1.0.0.0/8 subnet privately. If your underlay subnet overlaps the 1/8 subnet, tunnels do not form between Airwall Edge Services. This issue includes over the Internet, so users who have real 1.0.0.0/8 WAN addresses would be unable to use Airwall Edge Services via these networks.

-

Provide access to the Internet with an Airwall Gateway in the DMZ

Provide Access to the Internet with an \ Airwall Gateway in the demilitarized zone (DMZ).

If you have protected devices that need access to the Internet (to get updates from Windows Update, or report to a cloud reporting service that is not protected by an Airwall Gateway, Agent, or Server, for example), you can provide that access by putting an Airwall Gateway in the DMZ (demilitarized zone, or perimeter network).

Note: It can be more practical to use a Microsoft WSUS server to provide a local copy of Windows and other Microsoft updates rather than allowing devices on the Overlay access to the Internet. For more information on this option, see Windows WSUS help.

How to Provide Access as Securely as Possible

When you put an Airwall Gateway in the DMZ, basically the entire world is a “Trusted Device” for the Overlay, so you need to tightly control the access into the Airwall Gateway Overlay. To do this, you must:

- Locate the Airwall Gateway in the DMZ adjacent to the firewall
- Configure strong firewall policies regarding traffic to and from the Overlay.
- Have a security policy on your firewall that doesn't open the HIP tunnel up to the entire world.

Use the following guidelines to provide access in the most secure way possible.

CAUTION: Potential Routing Issues with a Layer 3 (Routed) Overlay: When you are deploying the DMZ Airwall Gateway, and add the 0.0.0.0/0 local device to the DMZ Airwall Gateway, a 0.0.0.0/0 route appears on all of your Airwall Gateways that have policy with the DMZ Airwall Gateway. This route can cause routing issues if you have a Layer 3 (Routed) Overlay, and you may need to adjust local routes on the Airwall Gateways and Airwall Agents and Servers accordingly.

Warning: Windows and Mac Airwall Agents and Serverss: If you add the 0.0.0.0/0 route to policy with a Windows or Mac Airwall Agent or Server, it causes the Airwall Agent or Server to enter Full Tunnel mode and direct all network traffic through the HIP tunnel.

Before you Begin

This procedure requires the following:

- Conductor V2.2x or later
- A physical or virtual Airwall Gateway v2.2.x or later to use as the DMZ Airwall Gateway.

Before you configure a Airwall Gateway in the DMZ, you must:

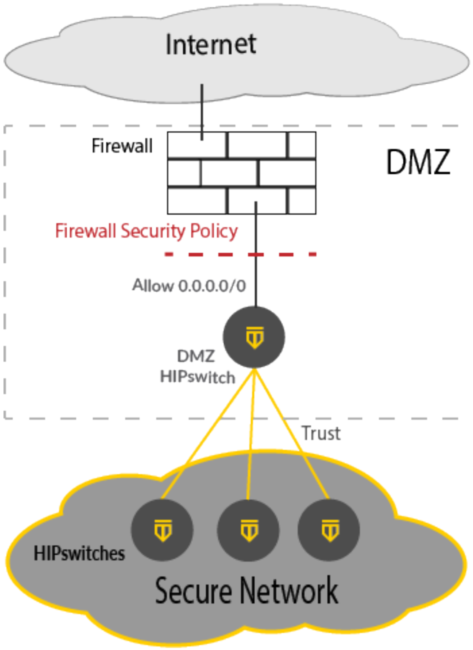
- Have a firewall or switch set up on your network and connected to the Internet.
- Have an open port on your firewall or switch to connect the Airwall Gateway.

Deploy the Airwall Gateway in the DMZ

To deploy an Airwall Gateway in the DMZ:

1. Install the Airwall Gateway in the DMZ

2. Configure the Firewall
3. Configure the DMZ Airwall Gateway
4. Test the DMZ Airwall Gateway and Firewall Configuration
5. Connect the DMZ Airwall Gateway to the Internet
6. Test the Deployment
   The following diagram gives an overview of how the Airwall Gateway is installed in the DMZ:



For more details, see the following sections.

Step 1: Install the Airwall Gateway in the DMZ

Install a Airwall Gateway in the DMZ with the Overlay Port plugged in to the Firewall (or the switch that is hosting the DMZ).

Step 2: Configure the Firewall

Configure your firewall to limit inbound traffic to the IP of the Airwall Gateway. You want to allow outbound traffic and inbound traffic for open connections. This configuration prevents hosts on the Internet from scanning the DMZ and the Airwall Gateway. For more information, see the instructions for your firewall.

Step 3: Configure the DMZ Airwall Gateway

Configure the Overlay port group on the DMZ Airwall Gateway as follows:

1. Add the **IP address** of the interface of the Firewall in the DMZ.
2. Set the **Default Route** to the interface of the Firewall.
3. Check **Enable source NAT** to force all overlay traffic to appear to come from the Airwall Gateway.

Step 4: Test the DMZ Airwall Gateway and firewall configuration

Test your configuration to make sure it is working as you expected.

Step 5: Connect the DMZ Airwall Gateway to the Internet

To connect the DMZ Airwall Gateway to the Internet, you set up the local device and Overlay.

1. On the DMZ Airwall Gateway, in **Local Devices**, click **Add Device**, and add the Local Device 0.0.0.0/0.
2. Create an overlay called Internet Access (or similar name, so you know what permissions it implies).
3. Add the Local Device 0.0.0.0/0 and all devices that require Internet access.

Note: As a best practice, configure overlays to limit connectivity to only those devices and servers that must communicate with each other.

4. Create trust from all other members of the Internet Access overlay to only to the 0.0.0.0/0 device (a Hub and Spoke arrangement, not a mesh).

Step 6: Test the deployment

1. In the Conductor, open the DMZ Airwall Gateway, and go to **Diagnostics** > **Check connectivity**.
2. In **Ping a single IP address**, under **IP address or hostname**, select **Overlay Port group**.
3. Enter the IP of a known host on the Internet, such as 8.8.8.8, and select **Ping**.
   If the ping succeeds, the deployment is working.

Replace a virtual Conductor with a fresh VM

Sometimes you may need to replace your virtual Conductor with a fresh VM.

This is normally only necessary if the Conductor has been updated through many different versions of our software, or if something happens to the VM that prevents the OS from running correctly.

In the worst case, you would need to restore from a DB backup. You should be doing DB backups and Conductor Support Bundles regularly.

If you need to replace your virtual Conductor, please create a support ticket and provide a DB Backup and/or a Support Bundle, if you have not already. Both are best, but Tempered Customer Success can work with one or the other if needed.

Before you begin

From Tempered Customer Success, you need:

- An open virtualization appliance (OVA) file
- A replacement license voucher for your replacement Conductor.
- Customer Success needs to un-bind your voucher in the license system so that your replacement voucher is valid

How to replace a Conductor

1. Keep your current Conductor running, if possible.
2. Create a new Conductor from the OVA file from Tempered Customer Success, and provision it with the new license voucher.
3. Complete the basic configuration steps, but do not configure it to match the IP of the current Conductor yet.
4. Once you get to the Conductor dashboard, go to **Settings (Gear Icon)** > **Diagnostics** > **Restore database backup**, and upload the most recent backup you have.
5. The Conductor will reboot, and come back online with all of your old settings.
6. Shut down your old Conductor, and re-IP the new Conductor to take its place.
7. Ensure that devices are coming back online.
8. Reach out to Customer Success and let us know that you have completed the replacement process. They will let you know when to re-sync your Conductor.
9. Re-sync your Conductor by going to **Settings** > **Licensing** > **Sync all**.

Replace a High-Availability (HA) Conductor

If you have two Conductors running as an HA pair, you can follow the same instructions above for your active only, and when everything is complete, you can spin up a new standby and HA-pair it with the active to replicate to it. There is no need to restore the standby from a DB backup.

Make sure to tell Customer Success if your Conductor is in HA so they can provide you with two replacement Conductor license vouchers.

Replace a physical Conductor

You can follow the steps above with a hardware 400 or 500 Conductor to migrate between physical Conductors, or to migrate from a hardware Conductor to a virtual/cloud Conductor.

Please reach out to Customer Success with information about your environment before doing this. There may be factors to take into account outside of a basic virtual-to-virtual migration.

Replace a cloud Conductor

If you are replacing a Conductor in the Cloud, re-IPing it to match the previous Conductor may not be possible. For this reason, it is best practice to use a DNS hostname rather than an IP address to connect your Airwall Edge Services to your Conductor, and simply change your DNS records once you have a new Conductor restored from backup.

What's the difference between an Underlay and an Overlay

Understand the difference between an Underlay and an Overlay.

There is a common misconception about our product that traffic can traverse an Airwall Gateway from the Underlay (your existing network) to the Overlay (a segment of your Airwall secure network). Unfortunately, this misconception can lead to incorrect network configurations, IP conflicts, and broadcast storms.

This article will describe the differences between these networks.

The Underlay network

On an Airwall Gateway, the Underlay network is what's behind behind Port 1. This is the interface where the Airwall Gateway acts as a MAP client and an Airwall client.

The Underlay network is your existing network and all networks in between (including the Internet). It can be:

- Your local LAN or corporate PtP network.
- A Cable, DSL or Fiber connection.
- A Cellular APN, or a long-range wireless network.

Basically, the Underlay network is where Airwall Gateways talk to each other over an existing network.

The Overlay network

The Overlay network is the protected device network created by the Airwall Solution. It can be the protected network behind an Airwall Gateway, or a Windows/Linux/macOS/iOS/Android computer running our Airwall Agent or Server software.

On an Airwall Gateway, the Overlay network is what's behind Ports 2 and up. These are the interfaces where the Airwall Gateway acts as a gateway.

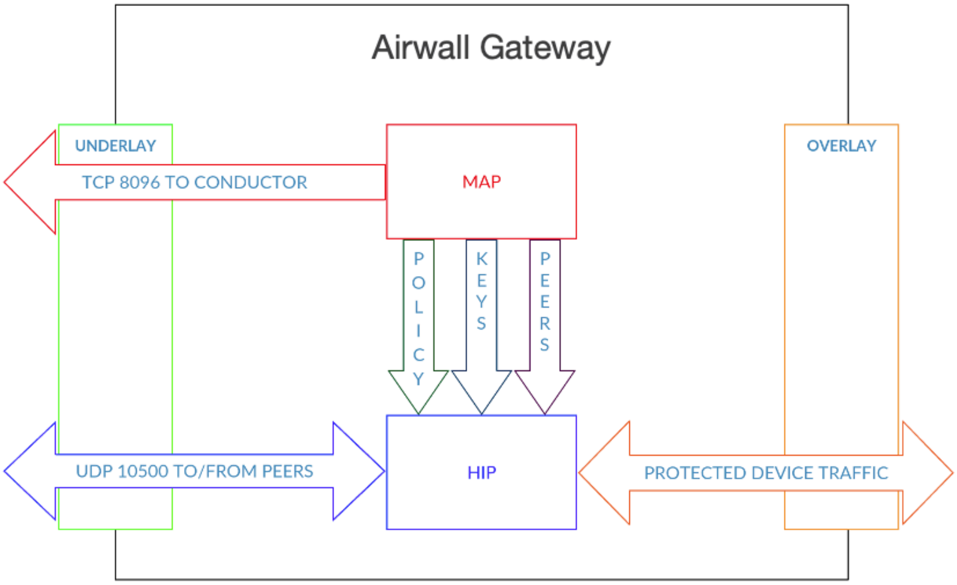
Getting data from the Overlay to the Underlay

These two networks may be different, but as you likely noticed, traffic still goes in one Airwall Gateway and comes out another. The Underlay is the only way they can communicate with each other, so that data must traverse the Underlay somehow.

And it does, but not without first getting processed by our HIP processing. This HIP process can see both the Overlay and the Underlay networks; however, it treats these networks completely differently.

On the Overlay (Protected Device) side, it captures all network traffic from connected devices, and according to trust policy it routes that data to its peers in encrypted HIP tunnels. No packet ever makes it through the HIP process without either being truncated, or encrypted and tunneled to a peer. No packet can ever make it through the Airwall Gateway from the Overlay to the Underlay, or vise versa, intact.

HIP is all configured via a MAP connection to the Conductor, where the Airwall Gateway is given information on trust policy, the addresses of their peers, and the cryptographic keys needed to exchange information with their peers.



Use a micro-SIM in an Airwall Gateway 100g (v2.1.x and v2.1.5)

Help if your Airwall Gateway fails to properly recognize the micro-SIM when inserted.

Solution

Use a SIM carrier to install the new micro-SIM in a Airwall Gateway 100g. The carrier allows the micro-SIM card to maintain better contact with the modem.

Cause

The punchdown micro-SIM is thinner than the old, full-sized SIM used to be.

Virtual Conductor -- Exchange a Conductor VM using scripts

Occasionally, you may want to swap out a Conductor. You can do this using scripts.

You add a new instance using CloudFormation and set it in place before you remove the existing Conductor.

With a full stack deployed (Conductor and Airwall Gateway), perform the following steps:

1. Copy `conductor.include` to `conductor.include.old`
2. Update the `conductor.include` file. Here are the parameters and what you must and can change:

```
stackName=my-conductor.  <=== Mandatory: this must be changed
netId=vpc-0638842e264e6f648                 <=== do not change
netSubnetPublicId=subnet-0bd40e059bb241cb3. <=== do not change
imageId=ami-0fcdcdb074d2bac5f                 <=== Can update
instanceType=t2.medium.                       <=== Can update
volumeType=io1                                <=== Can update
volumeSize=8                                  <=== Can update
iops=200                                      <=== Can update
region=us-west-1.                          <=== Do not change
```

3. Run

```
<component>-start.sh
```

   There should be two Conductors in the VPC.

4. Run

```
./delete-stack.sh <original stack-name>
```

There should now be only one Conductor.

What is the recommended MTU for protected devices?

What is the recommended maximum transmission unit (MTU) for protected devices?

Airwall Edge Services encapsulate and encrypt the full Layer 2 frame.

Depending on the cipher and size of the input frame, you may not want to have the outgoing encapsulated packet to end up fragmented. These recommendations should help avoid fragmented packets.

Solution

Enter the exact APN as what is provisioned for the SIM card as given by the cellular provider.

AES-256 CBC with HMAC SHA256

Given an MTU of 1500, the maximum plain text Overlay Ethernet frame size without fragmenting on the ciphertext underlay is 1421 bytes.

The Airwall Gateway HIP tunnel adds 79 bytes of overhead. For each frame (less than 1421 bytes), our overhead varies between 79-94 bytes.

AES-256 GCM

Given an MTU of 1500, the maximum plain text overlay Ethernet frame size without fragmenting on the ciphertext underlay is 1425 bytes.

The Airwall Gateway HIP tunnel adds 67 bytes of overhead. For each frame (less than 1425 bytes), our overhead varies between 67-78 bytes.

To allow for the HIP tunnel overhead due to encapsulation, use an MTU of 1500.

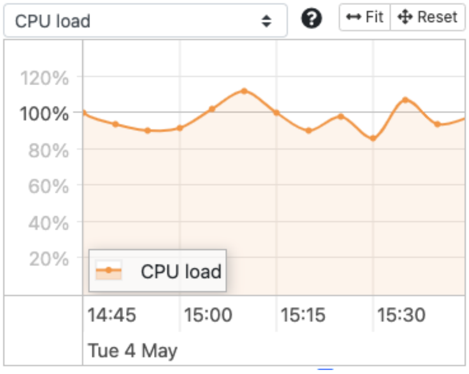
Troubleshoot KB Articles

Troubleshoot issues in an Airwall secure network.

High CPU load on a 110 Airwall Gateway

The CPU load graph on the Reporting tab for an Airwall Gateway shows a graph of the load average on the Airwall Gateway's CPU. This is an average of the number of processes waiting for the CPU, sampled every 5 minutes. It is not a percentage. This graph is fixed in v2.2.12 and will be the actual percentage of CPU used by running processes.

The 110 Airwall Gateway has an internal architecture that causes the CPU load to be higher than other units with the same configuration, often showing a CPU load average close to 1 (100% on the graph). While this does mean that most processes are waiting for the CPU, because HIPhh traffic is not CPU-bound, a load of 100% does not have a strong impact on traffic in the HIP tunnel.



HIPswitch 300v and VMware High Traffic Workaround

HIPswitch 300v

Date: April 28, 2016

Applies to: HIPswitch 300v in VMware vSphere

Behavior

If you are running a HIPswitch 300v on VMware with all six virtual adapters assigned to private network interfaces, unusually high activity may spike the CPU and cause traffic issues.

Workaround

To prevent traffic issues, do the following:

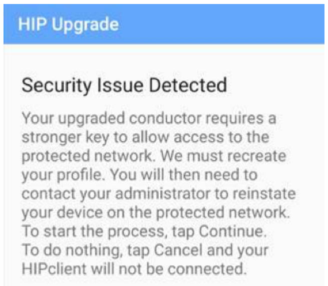
1. In the console, login with username `macinfo` and password `macinfo`.
2. A table of interfaces and corresponding MAC addresses is displayed. Record the results.
3. Edit your virtual machine settings:
    - Compare each MAC address with the corresponding interface
    - Match the MAC address for the shared interface with the network interface in settings (eth0 is always mapped to network interface 1).
    - Match the MAC address from the HA interface with the network interface in settings.
    - All other MAC addresses will be for the device network. Remove all but one of these interfaces.

The steps above should resolve any network traffic issues as well as CPU resource consumption.

Alternatively, you can reduce the chance of over consumption of CPU or memory resources by configuring resource constraints against the Virtual Machine, or placing the virtual machine in a configured vApp.

Security Issue detected when updating Android Airwall Agentfrom 2.1 to 2.2

If you have already connected to a Conductor on your Android device, and subsequently update your Android Airwall Agent from v2.1.x to 2.2.1 or 2.2.2, you receive the following message:



HIP Upgrade

Security Issue Detected

Your upgraded conductor requires a stronger key to allow access to the protected network. We must recreate your profile. You will then need to contact your administrator to reinstate your device on the protected network. To start the process, tap Continue. To do nothing, tap Cancel and your HIPclient will not be connected.

Solution

Ask your Conductor Administrator to revoke your Airwall Agent, and recreate your profile:

1. On your Android device, in the Airwall Agent menu, tap **Profiles**.
2. Tap your existing profile to open it and copy the URL from the **Conductor URL**
3. Still in **Profiles**, tap the plus (+) sign to create a new profile.
4. Name your new profile and paste the Conductor URL you copied earlier.
5. Tap **Add**.
6. Tap to open your old profile again, and tap **Delete**.
7. Return to the home page. Tap the profile selector at the top, and select your new profile. (You may need to toggle the switch to the left to disconnect from the Conductor before choosing your new profile.)
8. Toggle the switch next to the profile to reconnect to the Conductor.

Note: Your Conductor administrator may need to accept the new profile.

Airwall Edge Service disconnects from the Conductor every thirty seconds

Airwall Edge Services communicate to Conductor using the MAP2 protocol.

MAP2 provides the configuration policy for each Airwall Edge Service subscribed. Each Airwall Edge Service has a unique set of MAP2 data channels it is able to subscribe to.

In some situations, an Airwall Edge Service might try to subscribe to a channel it should have access to, but is unable to because the IF-MAP server doesn't believe it has access to that channel. The IF-MAP server will issue an error state forcing the Airwall Edge Service to disconnect.

Example log/syslog messages:

```
ignoring channel overlay:20:attributes (not allowed)
ignoring channel device_group:10:attributes (not allowed)ignoring channel
 endbox::attributes (not allowed)
ignoring channel endbox::notify (not allowed)
ignoring channel endbox::publish (not allowed)
subscription for device_group:10:attributes failed 4 times - re-connecting
 to server
MapClient error flag is set - will disconnect and try to reconnect
```

To fix this:

1. Restart the IF-MAP service in Conductor – Go to **Settings** > **Service Status** > **IF-MAP** > **Restart**.
2. Update to the latest Conductor firmware version.

Airwall Gateway has duplicate serial number (v2.1.5 and earlier)

How to handle an v2.1.5 or earlier Airwall Gateway with a duplicate serial number.

Prior to release v2.1.6, the serial number system used to calculate the UID Unique Identification (UID) of an Airwall Gateway did not use the entire length of the serial number.

This issue can result in a duplicate UID for an Airwall Gateway. If you install an Airwall Gateway of the same type as a one already on the network and the previous Airwall Gateway is removed from Conductor, check the displayed UID of each Airwall Gateway for duplicate serial numbers.

Solution

If the serial numbers are identical, return the newly-installed unit. This issue is resolved as of v2.1.6 by using a longer base to calculate the UID, as well as enhancements to the Conductor to warn of a collision of UID rather than dropping the old unit from Conductor.

110g Airwall Gateway - IMEI not displayed until SIM inserted

On the 110g Airwall Gateway v2.2.8, the IMEI (International Mobile Equipment Identify) is not displayed in the diagnostic report in Diagnostic Mode until there is a SIM inserted into the cellular modem.

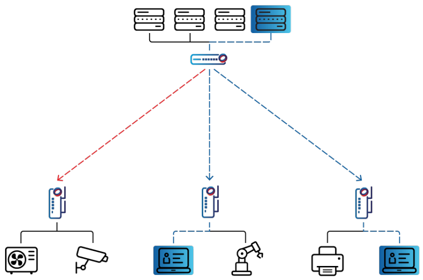
Workaround

Insert a SIM card to see the IMEI.

Airwall Gateway support for Multicast

Airwall Gateways will send multicast IP packets received on the protected network through the tunnel to all peers.

For example, an 224.0.0.1 (**IGMP**) Internet Group Management Protocol packet sent from Client-1 behind Airwall Gateway-1 will be seen by Client-2 behind Airwall Gateway-2 if they have trust set between them.



Note: There is no sparse PIM or other Multicast Routing protocol involved. These packets are sent to all peers without regard to whether or not local devices have subscribed to the multicast group.

Each peer receives a copy of the Multicast packet. In the case of Airwall Gateways to Airwall Agents and Servers, there is little bandwidth savings on the Shared Network side. From Airwall Gateway to Airwall Gateway, there could be some reduction in traffic.

200 Airwall Gateway is not responding and requires a manual reboot (v1.12.x)

Update to a later version if you are getting occasional lockups on a v1.10.x to v2.0 200 e or w Airwall Gateway.

If you are experiencing occasional lockups on a 200 Airwall Gateway running firmware version 1.10.1-1.12.4 or 2.0, update to at least v2.0.1.

Solution

Update the 200 Airwall Gateway to at least v2.0.1.

Troubleshoot an Airwall Gateway's connection to the Conductor

Some basic steps to troubleshoot basic connectivity issues between an online Airwall Gateway and the Conductor.

Requirements

For these troubleshooting steps, your Airwall Gateway must be:

- **Connected to the Conductor** – If you have not, see Configure an Airwall Gateway with the airsh Setup Wizard on page 274.
- **Online** – If the Airwall Gateway is offline, check that it is powered on, or see Troubleshoot Initial Airwall Gateway connections on page 491.

Check connectivity

1. On the page for the Airwall Gateway, go to **Diagnostics** > **Check connectivity**.
2. Select **Ping all devices**.
3. If the test fails, this could mean ICMP (Internet Control Message Protocol) packets are blocked by the firewall, or that there is not an active connection between the Airwall Gateway and devices connected to it.

   Note: Airwall Agents and Servers that are not currently running will not show up.

Run a trace route

1. On the page for the Airwall Gateway, go to **Diagnostics** > **Check connectivity**.
2. Scroll down to **Traceroute** and enter the IP address of the device you want to test.
3. Choose the interface, and select **Traceroute**.
4. Check the result to see whether UDP 10500 can traverse your network or is blocked by the firewall.
5. If it is blocked, unblock UDP 10500 on your firewall.

Check secure tunnels

1. On the page for the Airwall Gateway, go to **Diagnostics** > **Secure tunnels**.

2. Select **Check secure tunnels**.
3. Review the result to see if your tunnels are forming.

Capture networking data

Start a packet capture to see how traffic is traveling through your network.

1. On the page for the Airwall Gateway, go to **Diagnostics** > **Data capture**.
2. Select **Start a Packet capture**, and enter the options for the issue you're having.
3. Try to do what you are having issues with, then return and select **Stop packet capture**.
4. When the Conductor is finished processing the packet capture, select **Download** and view the packet capture (PCAP) file to analyze HIP and other relevant network traffic.

Create a diagnostic report

Diagnostic reports contain information on recent activity and model and firmware versions.

1. On the page for the Airwall Gateway, go to **Diagnostics** > **Data capture**.
2. Under **Airwall Gateway diagnostic report**, select **Request a diagnostic report**. The Conductor generates a report.
3. Click **Download** and review the report for information that can help with troubleshooting.

Cellular or wireless Airwall Gateway configured with a static IP does not work (v1.12.x and earlier)

If you have configured your Airwall Gateway (v1.12.x and earlier) with a static IP, failover between cellular or Wi-Fi to a wired connection does not work.

Solution - online Airwall Gateway

If the Airwall Gateway is showing online in the Conductor:

1. Go to the **Dashboard** and select the desired Airwall Gateway.
2. Go to **Ports** and click **Edit Settings**.
3. For **Protocols**, select **DHCP**.
4. Select **Save**.

Solution - offline Airwall Gateway

If the Airwall Gateway is not showing in the Conductor:

1. Connect a computer to Port 2 on the Airwall Gateway.
2. Place the Airwall Gateway in Diagnostic Mode.
3. Point your browser to `192.168.56.3`.
4. Go to **Configuration** > **IP address**.
5. For **Protocols**, select **DHCP**.
6. Select **Submit**.
7. From the **Actions** menu, select **Reboot**.

Cellular failover or intermittent connectivity on a 100g Airwall Gateway (before v1.12.5)

If you have configured your Airwall Gateway with DHCP, failover between cellular or WiFi to a wired connection in versions previous to v1.12.5 may not work correctly.

If you experience any of the following issues, you need to update your Airwall Gateway:

- Long latency when failing over between cellular or WiFi to a wired connection.
- An incorrect IP address is displayed for the Airwall Gateway after failing over.
- Intermittent packet loss between trusted endpoints after a successful failover.

Solution

Update the Airwall Gateway firmware to v1.12.5 or v2.0.1, available from the Firmware section of this site. If you want to update to a much later version, see How to Update from Older Versions on page 515 or contact Customer Success.

Cell provider refuses connection to a 110 Airwall Gateway

Early 110 Airwall Gateways had their RTC (Realtime Clock) set too far into the future. Having the date too far into the future causes the cell provider to refuse the connection. You can still provision and manage the 110 using Ethernet.

Note: This issue only applies to the early 110 Airwall Gateways that shipped before the issue was found. All units that are currently shipping have the correct date and time set in their RTC.

1. Provision the 110 Airwall Gateway using Ethernet
2. Apply Hotfix HF-15628.

   Note: The **Firmware Install Date** shown in the Conductor may still show the date from the future at this point. This issue is purely cosmetic. The Conductor date will update when you install the next firmware update. (This hotfix does not change this date stamp)

CentOS 7 Airwall Agent crashes after provisioning

Help if your Linux Airwall Agent running on CentOS 7 is crashing right after provisioning.

Issue

It has become common security practice in CentOS to disable IPv6 in the kernel.

This can causes the Airwall Agent to fail after it is provisioned. The error is similar to this:

```
Oct 14 07:18:52 corpkvm01 hip: Reading config file: /etc/tnw/profiles/
profile-123123/hip.conf
Oct 14 07:18:52 corpkvm01 systemd: hip.service: main process exited,
 code=exited, status=1/FAILURE
Oct 14 07:18:52 corpkvm01 systemd: Unit hip.service entered failed state.
Oct 14 07:18:52 corpkvm01 systemd: hip.service failed.
Oct 14 07:19:22 corpkvm01 systemd: hip.service holdoff time over, scheduling
 restart.
Oct 14 07:19:22 corpkvm01 systemd: Stopped Airwall Agent.
```

Workaround

Enable IPv6 on CentOS 7. The Airwall Agent uses IPv6 internally and requires the kernel to allow IPv6 addresses be present on the system.

API Try it now -- Unable to use in Conductor API (v2.1.4 and later)

The API documentation on Conductor contained a **Try It Now** button for testing the API. This was useful for validating requests and routes without having to craft a full HTTP request.

As of v2.1.4, this feature has been removed due to a security vulnerability in the underlying Ruby gem. This feature may return in a future release.

The most recent API documentation is available in your Conductor. See Airwall API on page 508.

Conductor Login error: "Your change was rejected" (v2.2.8 and earlier)

You may get this error if you log in to the Conductor from a different tab, or if your session has expired and you try to log in again.

Workaround

Refresh the page, or on the page URL, clear everything but the Conductor URL and press Enter.

For example: https://conductor.mydomain.com/

Both of these methods resets the token (see below) and allows you to log in.

Cause

This issue is caused by a feature in browsers intended to prevent cross-site attacks (called the cross-site request forgery (CSRF) Token – see https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)).

Can I downgrade my Conductor to a previous version?

Once you have upgraded the Conductor, you must continue with that version or higher and cannot roll it back to a previous version, as the Conductor does not have a downgrade path.

However, a Conductor of a higher release can manage Airwall Edge Services of previous releases, so an exact version match is not required.

If you need more help with this issue, contact Support.

Conductor MAP server using Tempered certificates

The Conductor MAP server uses the Tempered-provisioned certificate to establish TLS 1.2 connections with remote Airwall Edge Services over TCP 8096.

The TLS session is validated with both client and server-side certificate authentication. If a customer certificate is uploaded to the Conductor, this certificate is not used for MAP connections.

As the Tempered certificate (earlier versions may report Asguard Networks in the certificate) is not a common certificate chain, security scanners may report this as Untrusted Root.

Solution

To avoid the security error in your browser, you can Install a Custom CA Certificate Chain on page 239.

Enable message logging (syslog) on a Conductor

How to set up Syslog on a Conductor.

If you do not already have Syslog set up, this article walks you through setting up Syslog-ng with TLS.

1. Download and install the most recent Syslog-ng.
2. Generate a self-signed certificate and public key xx, using the openssl command:

```
Openssl req -x509 -sha256 -nodes -days 365 -newkey rsa:2048 -keyout
 privateKey.key -out certificate.crt
```

3. Move the certificate and key to /etc/syslong-ng/conf.d.
4. Modify the Syslog-ng configuration file (/etc/syslog-ng/syslog-ng.conf) to add a section for TLS. This example logs the Tempered device logs to /var/log/twn.log:

```
@version: 3.8
@include "scl.conf"
      options {
         time-reap(30);
         mark-freq(10);
         keep-hostname(yes);
       };
    source s_local { system(); internal(); };
    source s_tls {
              tcp(ip(0.0.0.0) port(993)
              tls( key-file("/etc/syslog-ng/conf.d/domain.key")
             cert-file("/etc/syslog-ng/conf.d/domain.crt")
             peer-verify(optional-untrusted)));
        };
    destination d_logs {
        file("/var/log/tnw.log"
            owner("root")
            group("root")
            perm(0777)
            ); };

    log { source(s_tls); destination(d_logs); };
```

Important: Add this line to the source you wish to use: - peer-verify(optional-untrusted))

5. Restart the **Syslog-ng** service.
6. In your Conductor, go to **Settings** > **General Settings**, and scroll down to the **Syslog Config**.
7. Select **Edit Settings**
8. Type in the Syslog server address and port that you wish to use and check Use TLS encryption
9. Select **Update Settings**.

Conductor displays information that appears to be out-of-date (v1.x to v2.00.x)

Refresh your browser to update information.

If you experience any of the issues below, refresh your browser to resolve the issue:

- After a session has timed out, you receive the following error when logging in:

  The change you wanted was rejected.
- After configuring a Conductor for the first time and selecting **Return to settings** too quickly, you may receive a **Lost connection to the original server** message.
- The Conductor is not displaying the recent activity of a local device correctly.
- Firewall enable/disable for ICMP and SYN protection buttons broken.
- Demoting an active Conductor to standby, the processing screen updates correctly.
- Selecting **Restore positions** in a network visualization freezes the nodes in place
- Selecting **Detect Devices** repeatedly on the **Airwalls** properties page will generate excess traffic
- Devices continue to appear in the Conductor user interface after an Airwall Gateway was factory reset
- After you configure two Conductors in an HA-pair, the Conductor does not return to the Dashboard.

CPU Load Graph# (v2.2.11 and earlier)

The CPU load graph on the Reporting tab for an Airwall Gateway shows a graph of the load average on the Airwall Gateway's CPU. This is an average of the number of processes waiting for the CPU, sampled every 5 minutes. It is not a percentage. This graph is fixed in v2.2.12 to be the actual percentage of CPU used by running processes.

The value reported is actually the Linux load average of the system which can be much higher than 1.00 (shown as 100% on the graph).

While a load average of 1.00 means that all processes were waiting for CPU at some time during the sample period, HIP traffic is not CPU-bound, and HIP traffic (traffic in the secure tunnel) will not be noticeably impacted.

For a discussion of Load Average, see: https://www.howtogeek.com/194642/understanding-the-load-average-on-linux-and-other-unix-like-systems/.

Device is not able to communicate with other devices (v1.10.x-v2.0.x)

Help if you have a device that cannot communicate with other devices in your Airwall secure network.

If a device in your overlay is having trouble connecting to other devices, follow the instructions below to troubleshoot the issue.

1. Ensure that the devices that must communicate with each other have trust to each other in at least one overlay.

2. Ensure that the devices have a route to each other through their respective Airwall Gateways. For example, the Airwall Gateways are connected to the same underlay network.
3. Ensure that the affected Airwall Gateways can establish tunnels:
   a) Open the Airwall Gateways for the devices, and go to **Diagnostics**.
   b) Check **Build new tunnels if none exist**, and run the **Secure Tunnels** test.
   c) If the Airwall Gateway does not show up, check your Protected Network policy.
   d) If the Airwall Gateway fails the test, check to ensure that at least one has UDP port 10500 open and accessible from the Airwall Gateway you are testing from. Or, implement an Airwall Relay as needed.
4. Ensure that the Conductor is accessible on the TCP port 8096 and that nothing is blocking/filtering the connection.

Disable SHA-256

If the above steps do not resolve your issue, follow these steps:

1. In the Conductor, go to **Settings**.
2. In the **Advanced** section, select **Edit Settings**.
3. For **ESP transform** , select **SHA-1**.
4. Select **Save**.

DHCP server is not serving as a gateway

If you provision an Airwall Gateway, but do not set the DHCP gateway or IP, the DHCP server won't serve as a Default gateway.

Not specifying a gateway in the DHCP server configuration causes the Airwall DHCP server not to include the DHCP Router option, so the DHCP client does not configure a default gateway.

Solution

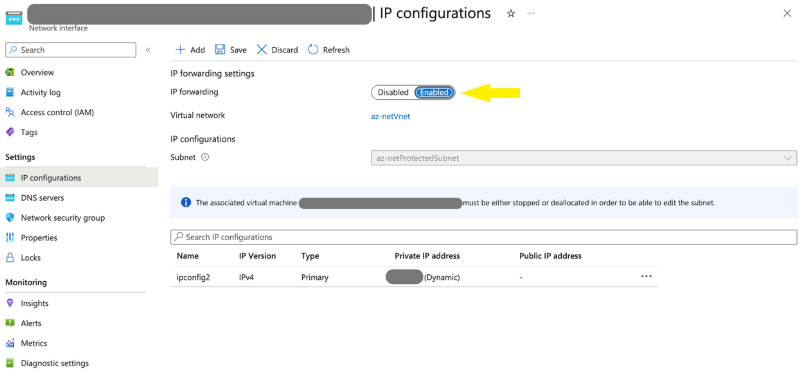
Configure the gateway or IP in the DHCP server configuration.:

Note: Not specifying a gateway is a possible, but unusual configuration, and should only be used when you want to configure a single isolated subnet. For example, a subnet for networked PDUs that should not have any outside connectivity aside from remote access through an Airwall Gateway used in conjunction with SNAT over the Overlay port group.

Ensure IP forwarding set to Enabled to avoid SNAT on Airwall

Complete the following steps to avoid SNAT on your Azure Airwall 300v.

1. In your Azure Airwall 300v virtual machine's Network interface, click **IP Configurations**.
2. Set **IP forwarding** to **Enabled**.



[redacted] | IP configurations

Network interface

IP forwarding settings

IP forwarding: Disabled [✓ Enabled]

Virtual network: az-netVnet

IP configurations

Subnet: az-netProtectedSubnet

The associated virtual machine [redacted] must be either stopped or deallocated in order to be able to edit the subnet.

Name	IP Version	Type	Private IP address	Public IP address
ipconfig2	IPv4	Primary	[redacted] (Dynamic)	-

East-West issue with Airwall-75, Airwall-150 (v2.2.1 and v2.2.2)

When using the East-West security feature of release v2.2.1 and v2.2.2, sometimes 75 and 150 Airwall Gateways stop responding to the Conductor after several minutes.

This issue is caused by a misconfiguration of the switch chip, where it hears its own traffic and shuts down the underlay port.

Apply Hotfix HF-11902 to fix the issue with East-West configuration where the switch chip

Solution

Apply Hotfix HF-11902 to fix the issue with East-West configuration where the switch chip

- For 75 Airwall Gateways: Apply this hotfix – https://temperedsoftware.s3.amazonaws.com/release/hotfixes/HIPswitch-mvebu64_hotfix-11902
- For 150 and 250 Airwall Gateways: Apply this hotfix – https://temperedsoftware.s3.amazonaws.com/release/hotfixes/HIPswitch-mvebu_hotfix-11902

Link Failover is not working on a fresh Conductor install

A new Conductor does not set the link failover settings until you access the page in the Conductor UI.

To resolve this issue:

1. Go to **Airwalls** > **Ports** > **Link Failover Settings**.
2. Without making any changes, select **Update**. This action saves the default settings and causes the Airwall Gateway to begin actively trying to recover if a failed connection over cellular occurs.

Invalid Gateway IP Address message (v2.1.3 and earlier)

What to do if you get an "Invalid gateway IP" message.

If you try to set both the Protected Network's Gateway IP and configure DHCP for the local devices at the same time you will get the error: "*Invalid Gateway IP address specified*."

Affected versions	Conductor v2.1.3 or earlier

Solution

Update to a later version of the Conductor to eliminate this bug. Newer versions apply Local Device network settings first so that the DHCP settings can be validated.

1. First set **Local Device** settings.
2. Save those settings.
3. Then set **DHCP** settings, and save again.

Cause

You cannot set DHCP without the Local Device network also being configured. When configuring them at the same time, the DHCP settings are rejected as the system still registers the Local Device network as unconfigured.

iOS Airwall Agent (v2.2.8 and v2.2.10) -- Error when creating a profile

You may get an error when creating a profile for the iOS Airwall Agent in v2.2.8 and v2.2.10. There is an error in iOS that assumes Safari is the default browser.

Workaround

1. Set Safari as your default browser.
2. Create your profile in the iOS Airwall Agent.

Key pair generation error on an Airwall Agent

If you get this error on an Airwall Agent, it could be one of the following:

- **Unrecognized Conductor URL** – Check the URL in your profile to make sure it is correct.
- **Profile issue** – If the URL is correct, do a profile reset:

    a) Delete any unused profiles.

b) Open and run the original profile.

c) Create and configure the profile you need and make it active.

This should reset your profiles and correct the issue.

Install Let's Encrypt Certificates on a Conductor

How to install a Let's Encrypt Conductor SSL certificate.

The Conductor uses a certificate for its web server issued by a Tempered Certificate Authority. As this certificate authority is not installed in browser trust stores, some web browsers may report that the Conductor is insecure. You can prevent this message by replacing the web server certificate with a publicly-trusted certificate. The following instructions outline how to install a Let's Encrypt Conductor SSL certificate.

Note: If you want to use a different certificate authority, see Add or Replace a Signed Certificate for the Conductor UI on page 239.

To install a Let's Encrypt certificate, you need to:

- Prepare the Let's Encrypt chain
- Upload the chain to the Conductor and get a certificate signing request (CSR)
- Use the CSR to get a signed certificate from Let's Encrypt
- Upload the signed certificate to the Conductor

Before you begin

Install the Let's Encrypt's certbot to get a certificate from Let's Encrypt. Their instructions on how install for your platform can be found on the Certbot site.

Prepare the Let's Encrypt chain

1. Collect the Let's Encrypt chain from https://letsencrypt.org/certificates/.
2. Download root and intermediate certificates. Use the ISRG Root X1 certificate and chain.
3. Concatenate the downloaded root and intermediate certificates into one file:

```
cat letsencryptauthorityx3.pem.txt isrgrootx1.pem.txt >
 letsencrypt_chain.pem
```

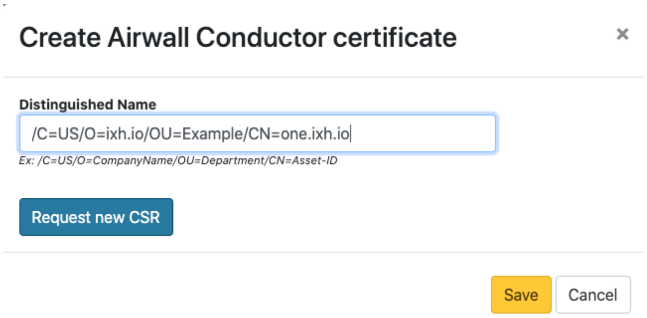
Upload the chain to the Conductor and get a certificate signing request (CSR)

1. Upload the prepared chain to the Conductor. For instructions, see Install a Custom CA Certificate Chain on page 239.
2. In Conductor **Settings**, under **Airwall Conductor Identity**, click **Actions**, and then select **Create certificate**.
3. Generate a new identity for the Conductor.

   For example:

```
/C=US/O=ixh.io/OU=Example/CN=one.ixh.io
```

4. Under **Distinguished Name**, enter the new Conductor identity, and select **Request new CSR**.



Create Airwall Conductor certificate

Distinguished Name

/C=US/O=ixh.io/OU=Example/CN=one.ixh.io

Ex: /C=US/O=CompanyName/OU=Department/CN=Asset-ID

5. Under **CSR**, select either **Copy** or **Download**, and copy the generated CSR to a machine with Let's Encrypt's **certbot** utility.
6. Select **Save**.

Use the CSR to get a signed certificate from Let's Encrypt

Certbot is Let's Encrypt's automated certificate command line tool. You need to use the manual option for certificate signing. More details from Let's Encrypt are here.

Typically, Let's Encrypt uses web server validation to verify you own the domain name for the certificate you're requesting. However, for a Conductor, you have to use their DNS verification steps.

1. Run the follow **certbot** command to process a CSR:

```
sudo certbot certonly --manual --preferred-challenges dns --csr <cert.csr>
```

2. The DNS validation for **certbot** typically relies on setting a TXT record for the domain you are issuing the certificate for. Follow the instructions **certbot** provides to validate this.

Upload the signed certificate to the Conductor

Once you have a signed certificate from Let's Encrypt, install the certificate into the Conductor. As the certificate is used in more places than just the web server, the Conductor may restart to activate the new certificate.

For additional help, see Install a Custom CA Certificate Chain on page 239.

What URLs and ports does Tempered use for provisioning and licensing?

Tempered uses its own licensing and provisioning service to bring up a new Airwall Edge Service.

- **URL**: https://licensing.temperednetworks.com
- **Ports**: HTTPS / 443

Linux Airwall Server not connecting via IPv6

Your router may not support IPv6

If you are having trouble with a Linux Airwall Server not connecting using IPv6, check to see if your router supports IPv6. If not, you may need to disable IPv6.

1. Run the *ip neighbors* tool. This tool is to identify how many domains are hosted by a particular server.
2. If you do not see a list of devices or at least your router, then your router doesn't support IPv6, and you won't be able to use IPv6 from this network. Please disable IPv6 using the instructions for your Linux OS. Here are instructions on IPv6 for Ubuntu/Red Hat:
   - **Ubuntu** - https://askubuntu.com/questions/440649/how-to-disable-ipv6-in-ubuntu-14-04
   - **RedHat** - https://access.redhat.com/solutions/8709

LSI conflict error on the Conductor

This error is extremely rare, and is the result of the Local Scope Identifier (LSI) or Host Identity Tag (HIT) being generated and conflicting with another device in your network.

Affected Airwall Edge Services	All Airwall Gateways and Airwall Agents and Servers

Solutions

For Airwall Agents and Servers

1. Create a new profile.
2. Point the new profile at the Conductor.
3. Delete the profile with the conflict.

For virtual Airwall Gateways

- Spin up a new virtual Airwall Gateway

For physical Airwall Gateways

1. Contact Customer Success for return merchandise authorization (RMA) of the hardware.
2. Install the replacement Airwall Gateway.

Understand LTE Signal Strength Values

Tempered LTE-capable Airwall Gateways offer three useful metrics for measuring LTE Signal Strength.

- RSRP: Signal Strength
- RSRQ: Sigla Quality
- RSSNR: Signal-to-Noise Ratio.

These values can be viewed under the **Reporting** tab, either as a graph, or as textual health data.

The values should be compared to this standard:

	RSRP (dBm)	RSRQ (dB)	RSSNR (dB)
Excellent	> -84	> -5	> 12.5dB
Good	-84 to -102	-5 to -9	10 to 12.5
Fair	-102 to -111	-9 to -12	7 to 10
Poor	< -111	<-12	<7

Migrate an existing deployment to v2.2

The 2.2 release brings a significant change to the base platform configuration and capabilities of the Airwall Gateway.

Airwall Gateway versatility is dramatically increased. To achieve this, this version gives up some functional interoperability between 2.2 and prior versions of Airwall Edge Services and the Conductor. A v2.2 Conductor cannot manage Airwall Edge Services on any version before v2.0. While most things still work across versions 2.0.x, 2.1.x and 2.2 during your upgrade, a best practice is to migrate 2.2.x deployments completely as soon as possible using the following order:

1. Upgrade your Conductor to 2.1.6
2. Upgrade all Airwall Edge Services to 2.1.6
3. Upgrade your Conductor to 2.2.0
4. Upgrade all Airwall Edge Services to 2.2.0

For more information on upgrading your Conductor to 2.1.6 from prior versions, contact Customer Success.

Port not showing after update from v2.1.x to v2.2.x

When you update an Airwall Gateway from v2.1.x to v2.2.x, there are significant changes in the way the Conductor displays the network configuration. Because of these changes, when you finish the update, the Airwall Gateway may still be converting the local configuration and may not have uploaded all of the details to the Conductor yet, and the **Ports** page may show no ports until it is refreshed.

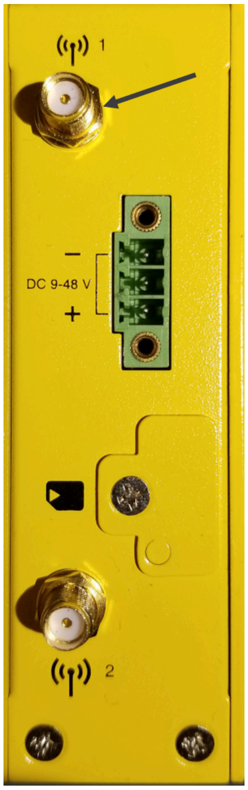
Solution

To update the ports information, on the **Ports** page, select **Click here to reload**, or refresh your browser window.

110g Airwall Gateway – Install Single Antenna in Port 1

If you install only one antenna in the 110g Airwall Gateway, you must install it in antenna port 1.

This is different than the 150 and 250 Airwall Gateways, where you can install a single antenna in either port.



Airwall Gateway is reporting filtered ports from a network scan (v2.1.0 and earlier)

In Airwall Gateways v2.1.0 and earlier REJECT packets on the underlay for services they are not listening on. This commonly shows up as a filtered port from network scanners.

In v2.1.0 and later, Airwall Gateways do not respond to (or drops) ports they do not actively use on the underlay.

There are no other listening services on the Airwall Gateway underlay.

On this version, the only listening service an Airwall Gateway has is the HIP process running on User Datagram Protocol (UDP) 10500 by default.

My SIM card doesn't work in my cellular Airwall Gateway

If you are trying to connect to a network over a cellular connection, and your Airwall Gateway won't connect to your service, try one or more of these troubleshooting steps:

Note: Not all of these troubleshooting tests are necessary for all cellular issues.

Check Settings

Note: If you are using a T-Mobile SIM, you must explicitly configure the Cellular Provider and APN for it to work. Manually configuring these settings may be necessary, as autoconfiguration over the network doesn't always work for M2M cellular devices.

- **Provider Settings** - In **Diagnostic** mode, under **Cellular Settings**, check the Provider settings are correct.
- **APN Settings** - In **Diagnostic** mode, under **Port Settings**, check the APN settings are correct.

Check the SIM card

- **SIM card orientation** - Check that the SIM card is inserted in the right orientation. Check your platform guide or Airwall help for assistance in correctly orienting the SIM card. If it is a 110 Airwall Gateway, see
- Insert the SIM card in a 110 on page 286.

- **SIM card fit** - Check that the SIM card is fully inserted into the Airwall Gateway, and if there is any wiggle, consider using a paper shim to ensure that the card is in tightly. Some cards come in varying thickness and might not fit perfectly into our trays.
- **SIM card activated** - Check that the SIM card is activated for your service.

Check connectivity

- **Signal quality** - Connect the Airwall Gateway to a wired underlay network and monitor the Cellular stats in the Conductor from the Health Data page. These stats will help you determine if you have a weak/bad-quality signal or too much noise.
- **Signal availability** - If your Airwall Gateway is being deployed in a remote location, consider testing it somewhere closer to a cell tower to determine whether or not the issue is environmental.

Check hardware

- **Antennas** - Check that your Airwall Gateway antennas are rated for cell networks and are firmly connected to the Airwall Gateway.
- **Power supply** - If you are using your own power supply, test it to ensure it delivers enough power to the Airwall Gateway. Operating below the listed power requirements can lead to modem instability.

Why is my Conductor slow? (v2.1.x)

If you have more than 20,000 local devices, the Conductor may lag in v2.1.x.

Workaround

Upgrade to a later version of the Conductor.

Snort: Large number of alerts from Snort for other protocols

The Other Protocols Snort rule captures traffic such as ICMP (ping) and other normal network traffic. Do not use this rule unless there is a specific reason, and even then, use it sparingly as it will constantly generate alerts.

Network monitoring triggers this rule, as will many other forms of network traffic that are considered normal day-to-day operations.

Use the **Other Protocols** rule only on a network that does not use ICMP for network monitoring and is typically extremely quiet.

Where do Airwall Gateways get time data from?

All Airwall Gateways sync the system clock with Conductor. The exception to this is virtual or cloud Airwall Gateways that use the host's clock.

When you restart an Airwall Gateway, it syncs its clock with the Conductor once a connection (specifically, a MAP connection) is established.

There may be a significant time sync if the Airwall Gateway has not synced with the Conductor time or has been powered off for a while.

An Airwall Gateway will also drift the clock to be in further sync with Conductor if the time difference is only by a few seconds.

Tpm0 warning on boot is cosmetic

You can safely ignore the Tpm0 warning when connected to a console on a 150 Airwall Gateway.

If you have a console connected to your 150 Airwall Gateway you might see a warning about tpm0:

```
"tpm tpm0: A TPM error (256) occurred continue selftest"
```

Solution

This is a benign error and does not indicate a problem with the unit.

Conflicting UIDs on 500 Airwall Gateway (before v2.1.6)

On Pre-v2.1.6 500 Airwall Gateways, it is possible for two Airwall Gateways to end up with the same Unique identifier (UID), preventing them from both being provisioned on the Conductor.

The UID is determined from the serial number, but the serial number scheme varies from model-to-model. The result is 500 Airwall Gateway could potentially have the same UID as its peers.

This scheme was updated for the 500 Airwall Gateway in v2.1.6 and only takes effect after a factory reset.

Solution

These steps should resolve the problem:

1. Place both conflicting 500 Airwall Gateways into Diagnostic Mode.
2. Update them to v2.1.6.
3. Apply HotFix HF-XXXX
4. Place both Airwall Gateways back into Diagnostic Mode.
5. Perform a Factory Reset.
6. Place both Airwall Gateways back into Diagnostic Mode.
7. Point them back at the Conductor.
8. Revoke and delete any leftover Airwall Gateways with invalid UIDs in your Conductor.
9. License and manage the new 500 Airwall Gateways provisioning requests with valid UIDs in your Conductor.

AWS Conductor– Unsupported partition used and now it won't start

If you are following the instructions from the AWS script to build the Conductor using the Readme First instructions, and you want to delete just the Conductor you can run.

```
aws --region $region cloudformation delete-stack --stack-name $stackName
```

Where the stack name is the name of the parameter that you used to create these resources when you ran the Create-stack command.

Using VPC Cloudformation

To back everything all the way back out, delete the VPC Cloudformation script as well as any other scripts previously run and not destroyed.

Unable to update an Airwall Gateway from v1.x to v2.x

To upgrade an Airwall Gateway running v1.x series, your Conductor must be on v2.x or later.

If you attempt to update, you may get an error message similar to the following:

```
Conductor must be version 2.0.0 or higher for this firmware to be installed.
```

A v1.x Conductor cannot configure or manage a v2.x Airwall Gateway.

Solution

To resolve this issue:

1. Upgrade your Conductor to the latest stable 2.x release.
2. If any of your Airwall Gateways are running in Transparent mode, set them to Protected mode.

   Note: Do not upgrade an Airwall Gateway while it is in Transparent mode. If a v1.x Airwall Gateway is running in Transparent mode, it might not correctly record the firmware version of its Conductor.
3. Update the Airwall Gateways to the 2.x release.
4. If needed, set any Airwall Gateways back to Transparent mode.

Cannot update my virtual Airwall Gateway from v1.12 to v2.0

If the Airwall Gateway does not have enough disk space, the firmware update fails with no indication it has failed.

In v2.0.0, the Airwall Gateway Virtual Disk image was resized to 138.5MB. Previously-deployed Airwall Gateways (from any launch prior to 2.0) have a virtual image size of 55MB.

Affected Versions	VMware ESXi and Hyper-V Airwall Gateways running v1.12.x

Solution

Resize the virtual disk on your Airwall Gateway to at least 150MB and try the update again. The following links provide instructions for resizing the virtual disk for the virtual machine running the Airwall Gateway:

- VMware reference: https://kb.vmware.com/s/article/1004047
- Hyper-V reference: https://docs.microsoft.com/en-us/powershell/module/hyper-v/resize-vhd?view=win10-ps

1. Power off the virtual machine (VM).
2. Resize the virtual disk using the guidance contained in the links at the top of this page.

   Note: You must resize the virtual disk while it is offline.
3. Power on the VM and perform the firmware update.

Update fails when updating a VMware Conductor to v2.2.x

Conductor update completes but does not update.

Affected versions	Conductor v2.2.x (2.2.1, 2.2.2, etc)

Solution

If you have a virtual Conductor configured with a boot drive less than 1gb in size, you need to increase the size to 1GB or larger before the Conductor version v2.2 will install.

The following links provide instructions for resizing a virtual disk:

- VMware reference: https://kb.vmware.com/s/article/1004047
- Hyper-V reference: https://docs.microsoft.com/en-us/powershell/module/hyper-v/resize-vhd?view=win10-ps

Note: Azure, AWS, and Google Cloud Conductors already have their boot drive set to 1GB. This issue only affects those with EXSi or Hyper-V Conductors.

Related Articles

See DEV-10023 in the Known Issues of Release Notes 2.2.1 on page 710.

Documentation Downloads

You can print PDF copies of any topic by clicking the print icon 🖶 at the top right of any topic.

Download the most recent PDF of Airwall help:

Airwall help	Download latest Includes v3.0 - created Nov 9, 2021

Go here for Pre-Airwall Documentation Downloads.

Tip: Select a Blue button below to download a manual in PDF format. Documentation downloads are organized by product version.

User Manuals

Conductor and Airwall Edge Services Administrator Guide	This document contains procedural information help you understand how to install, configure, and manage your Conductor, Airwall Edge Services, devices, and protected networks. Download for 2.1
Conductor andAirwall Edge Services Install Guide	This document outlines the steps required to deploy a Conductor, connect Airwall Edge Services, add devices, create and manage an overlay, and configure device trust. **Note:** The contents of the **Install Guide** are also included in the **Administrator Guide**. Use this guide if you need a shorter document consisting of basic instructions about installing and configuring your Conductor and Airwall Edge Services. Download for 2.1
Airwall Agent and Airwall Server Quick Start Guide	This document contains procedural information help you understand how to install, configure, and manage Airwall Agents and Airwall Servers. Download for 2.1

Documentation for Cloud Platforms

You can create and manage your Conductors and Airwall Edge Services in Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). The guides listed below provide end-to-end instructions on various aspects of your cloud deployment.

Deploy an Airwall Edge Service on the Amazon Web Services Platform	This document outlines the steps required to deploy an Airwall Edge Service on AWS. Download for 2.1
Deploy a Conductor on Microsoft Azure	This document outlines the steps required to deploy a Conductor on Azure. Download for 2.1
Deploy a Conductor on the Google Cloud Platform	This document outlines the steps required to deploy a Conductor on GCP. Download for 2.1

Hardware Specification Sheets and Platform Guides

If you no longer have access to the documentation included with your hardware, you can download a PDF here.

Tip: Search your model number in help for updated versions.

Airwall Gateway 75e	Airwall Gateway 75 Series Quick Start Guide

	Note: See Serial drivers on page 539 and install the serial driver if you want to use the serial port on the 75.
Airwall Gateway 110e and 110g	Airwall Gateway 110 Quick Start and Platform Guide
Airwall Gateway 150 and I-150	Airwall Gateway 150 Series Platform Guide Airwall Gateway 150 Series Hardware Specifications sheet
Airwall Gateway 150 Series - Expansion Modules (SFF-MOD-NL7588 and SFF-MOD-MC7430 cellular expansion modules)	Airwall Gateway 150 Expansion Module Manual
Airwall Gateway 250e, 250g, and 250gd	Airwall Gateway 250 Platform Guide **Note:** See Serial drivers on page 539 and install the serial driver if you want to use the serial port on the 250.
Conductor/Airwall Gateway 500	Conductor or Airwall Gateway 500 Platform Guide Airwall Gateway 500 Series Hardware Specifications sheet
Retired – Airwall Gateway/HIPswitch 100e and 100g	Airwall Gateway 100 Series Platform Guide

Terms and Definitions

Glossary of Airwall components.

Terms and Definitions

Glossary of Airwall components.

region bypass

Use the regional backhaul bypass pool to group bypass egress gateways.

Airshell

A command-line interface that allows you to deploy and configure Airwall Gateways. See Airshell Command Line on page 360.

allowlist

List of assets that are allowed access on your network.

Airwall Agent

Software that runs on a laptop or mobile device that allows that device to connect securely to resources on an Airwall secure network according to trust policies set up by an administrator of an Airwall Conductor.

Airwall Edge Service

A term that refers to all of the hardware and software that manages trust policies on an Airwall secure network, including Airwall Agents and Servers, Airwall Gateways, and Airwall Relays.

Airwall Gateway

A physical, virtual, or cloud gateway that protects the devices connected to it, and manages the devices' communication according to the trust policies set up by an administrator of an Airwall Conductor.

Physical Airwall Gateways, depending on the model, can have built-in Ethernet, Wi-Fi, and Cellular (2G, 3G, 4G LTE modems), as well as Serial-over IP for the flexible link connectivity options. You can also deploy virtual and cloud Airwall Gateways.

Airwall Invitation

Airwall Invitations provide a simpler way to add people’s mobile phones, tablets, and computers to your Airwall secure network. At a minimum, sending invitations automatically provisions and manages people as they connect. You can also set up the invitation to place people into overlays to define what resources they can reach on the network, access windows when they can connect, and other settings.

Airwall Relay

An Airwall Relay routes encrypted communications between resources and Airwall Edge Services. Relays reduce network complexity and enable complete connectivity between disparate systems. An Airwall Relay provides a private identity namespace that eliminates the need for public IP addresses and inbound firewall rules to connect devices.

Airwall secure network

A virtual air-gap solution that ensures your devices are completely invisible, where you can secure and micro-segment network communication and remote access between devices over your existing network.

Airwall Server

Software that runs on a server computer that allows that server to connect securely to resources on an Airwall secure network according to trust policies set up by an administrator of an Airwall Conductor.

backhaul bypass

Sending bypass traffic through a designated Airwall Gateway set up to handle traffic out of and into the Airwall secure network. The Airwall Gateway that is handling bypass traffic is called a bypass egress gateway.

bypass traffic

Traffic leaving the Airwall secure network (for example, traffic to and from the Google DNS servers or the Internet). See also *seamless bypass* or *backhaul bypass*.

cloak

Hiding or making invisible endpoints on an overlay (secure) network. Cloaking is a unique function of HIP and the Airwall Solution.

Conductor

The physical, virtual, or cloud service that centrally manages connections and trust for an Airwall secure network. The Conductor provides one centralized location for you to set up and manage Airwall Edge Services and trust policies between them to create, manage, and monitor your Airwall secure network. It is not involved in the data that is exchanged between Airwall Edge Services and the devices they protect.

isolated Conductor

An Airwall Conductor that's installed in an isolated (or "dark") environment, with no access outside of the private network. See License a Conductor and Airwall Edge Services in an Isolated Environment on page 196.

standby

The Conductor or Airwall Gateway that is standing by to take over if the active one fails in a high-availability configuration. Also called secondary.

denylist

List of assets that are denied access on your network.

full tunnel

A setting on an Airwall Agent or Server that forces all traffic on the device to go through the secure HIP tunnel.

HIP

Host Identity Protocol

HIP is the secure protocol used by the Airwall Solution to provide secure networks. HIP is an open standard that separates the role of an IP address as both host identity and location within a network, such that hosts are instead identified using cryptographic identities in the form of public keys. You can then define device-to-device trust relationships based on the host identity instead of the IP address.

lock down

A setting on an Airwall Agent or Server that only allows HIP traffic on the device.

MAP, MAP2, IF-MAP

The interface to Metadata Access Points. Airwall Edge Services use this client/server protocol to communicate with the Conductor, which provides authentication keys and communication policy to them.

micro-segmentation

Compartmentalizing your network into isolated segments in which devices are only exposed to each other when they have a need to communicate.

overlay

Overlays are virtual networks that make up your Airwall secure network that connect and establish trust between two or more Airwall Edge Services and the devices they protect.

The secured communications channels you create with an overlay are encrypted HIP tunnels that allow trusted devices to communicate securely with each other across the network. These communication channels are controlled by the Airwall Edge Services deployed throughout the underlay and administered by the Conductor.

seamless bypass

Local bypass allows you to separate traffic (split tunnel) going through your Airwall Gateway, where you selectively encrypt and tunnel some traffic, while allowing other traffic to pass through the Airwall Gateway unchanged. This ability also allows protected devices to securely communicate with devices or network locations that are not protected by Airwall Edge Services, such as software update servers on the Internet.

Configuring an Airwall Gateway for local bypass permits traffic between the secure overlay network and an insecure underlay network, where the Airwall Gateway acts similarly to an SNAT (Source Network Address Translation) gateway. Connections initiated from the underlay network are still blocked, but connections initiated from a protected device to a permitted bypass destination are allowed.

tunneling/tunnels

Encapuslating network traffic in an encrypted connection between two points (for example, similar to a VPN). A tunnel refers to the encrypted connection that is passing traffic.

region bypass

Use the regional backhaul bypass pool to group bypass egress gateways.

Additional Resources

Supplementary information that may be useful in managing or deploying the Airwall Solution.

Resource	Link to Download
Outdoor/External Cellular Antenna Reference Guide Suggestions on outdoor/external cellular antennas to use with Airwall Gateways.	Download PDF

Index