
Perform Manual Hardening for Versa Branches, Controllers, and Hubs

 For supported software information, click [here](#).

This article describes the Versa recommended procedure for performing manual hardening on Versa Operating System™ (VOS™) branch, controller, and hub devices. System hardening ensures that Versa products are secure when running in customer networks.

The hardening procedures described in this article are common for all types of devices, unless specified otherwise.

Disable the eth0 Interface

For branch devices only.

After you perform initial provisioning, the eth0 out-of-band management interface on a branch device is not required for normal operation.

To disable the eth0 interface:

1. Log in to the device CLI.
2. Disable the interface:

```
[admin@Branch-3: ~] $ sudo sed -i 's/auto eth0/manual eth0/g' /etc/network/interfaces
```

Use Signed SSL Certificates

By default, Versa devices have a self-signed and autogenerated certificate bound to a process on the eth0 out-of-band interface. In normal branch, controller, or hub device operation, this certificate is not used. However, because of normal security requirements, a production equipment requires a valid and signed certificate if the eth0 interface is enabled.

Note: Enabling secure mode has consequences for the procedures described in this article. It is advisable that you verify the working condition of all system functions before you enable secure mode.

To enable SSL certificates:

1. Generate a certificate signing request (CSR) by issuing the **openssl** command:

```
[admin@Hub-1: ~] $ mkdir /home/admin/certs
[admin@Hub-1: ~] $ chmod 700 /home/admin/certs
[admin@Hub-1: ~] $ cd /home/admin/certs
[admin@Hub-1: certs] $ openssl req -new -newkey rsa:2048 -nodes -keyout controller.key -out
controller.csr
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:IL
Locality Name (eg, city) []:Downers Grove
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Versa Networks
Organizational Unit Name (eg, section) []:Lab
Common Name (e.g. server FQDN or YOUR name) []:Controller1.lab.versa-networks.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:versa123
An optional company name []:
```

2. Copy the server.csr file to the Certificate Authority (CA) and sign it. Note that the signed certificate must be in PEM file format.
3. Copy the signed certificate and CA certificate to the /var/tmp directory. Note that you must use this directory.
4. Install the SSL certificate:

```
$ sudo mv /home/admin/certs/signed-certificate /opt/versa/var/cert/vshost.crt
$ sudo mv /home/admin/certs/private-key /opt/versa/var/cert/vshost.key
$ sudo mv /home/admin/certs/CA-certificate /opt/versa/var/cert/ca.crt
```

5. Change the permissions of the certificates:

```
$ sudo chmod 644 /opt/versa/var/cert/vshost.crt
$ sudo chmod 644 /opt/versa/var/cert/vshost.key
$ sudo chmod 644 /opt/versa/var/cert/ca.crt
```

6. Restart Versa services:

```
$ vsh restart
```

7. Securely back up and store the certificate and private key files generated in Steps 1 and 3 to a secure location using the scp command.
8. Delete the certificate and private key files generated in Steps 1 and 3 so that the private key is not left for anyone to read.

Enable SSH Banners

1. Copy the banner text to the `/opt/versa/etc/banner.net` file.
2. Change the file ownership to `versa:versa`:

```
versa@analytics1:~$ sudo chown versa:versa /opt/versa/etc/banner.net
```

3. Replace the SSH banner with the text in the `banner.net` file:

```
admin@director1$ sudo sed -i -e 's/#Banner.*/Banner Vopt/versa/etc/banner.net/' /etc/ssh/sshd_config
```

4. Restart the SSH service:

```
admin@director1$ sudo service ssh restart
```

Update OS Security Pack

To harden the branch, controller, or hub device security, regularly update the Director nodes to the latest OS SPack. For more information, see [Use OS Security Packages](#).



Configure NTP

You configure the Network Time Protocol (NTP) and the timezone to use in the network so that all devices in the network operate on the same time. Time synchronization is important so that the timestamps in log files match across all devices. Also, there are cryptographic requirements for time synchronization.

To configure an NTP server for a device:

1. Restart Versa services:

```
$ vsh restart
```

2. In the Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Templates > Device Templates in the horizontal menu bar.
 - c. Select an organization in the left navigation panel.
 - d. Select a device from the main pane. The view changes to Appliance view.
3. Select the Configuration tab in the top menu bar.
4. Select Others  > System > Time & Date > Time Settings in the left menu bar
5. Click the  Edit icon. The Edit Time Settings window displays.

Edit Time Settings

Current Time: Mon, Sep 07 2020, 01:57

Time Zone*: America/Los_Angeles

Set Date/time at: Mon, Sep 07 2020, 01:57

☒ NTP ☐ Manual

NTP Servers

	Server IP Address/Host N...	Key ID	Routing Insta...	Source Netw...	Source Interf...	Version
<input type="checkbox"/>	192.168.0.100		Analytics-VR			4

OK Cancel

6. In the Timezone field, select the timezone.
7. Click NTP and enter information for the NTP server.
8. Click OK.

For more information, see [Configure Time Settings](#).

Configure DNS Servers

Many security exploits rely on injecting invalid Domain Name System (DNS) servers into the device to redirect resolution queries to a foreign DNS server. The DNS configuration described here forces a DNS server to be input to the device template to reduce DNS-based attacks.

To configure a DNS server:


1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Templates > Device Templates in the horizontal menu bar.
 - c. Select an organization in the left navigation bar.
 - d. Select a device from the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Others > System > Domain Name Servers in the left menu bar. The main pane displays the configured

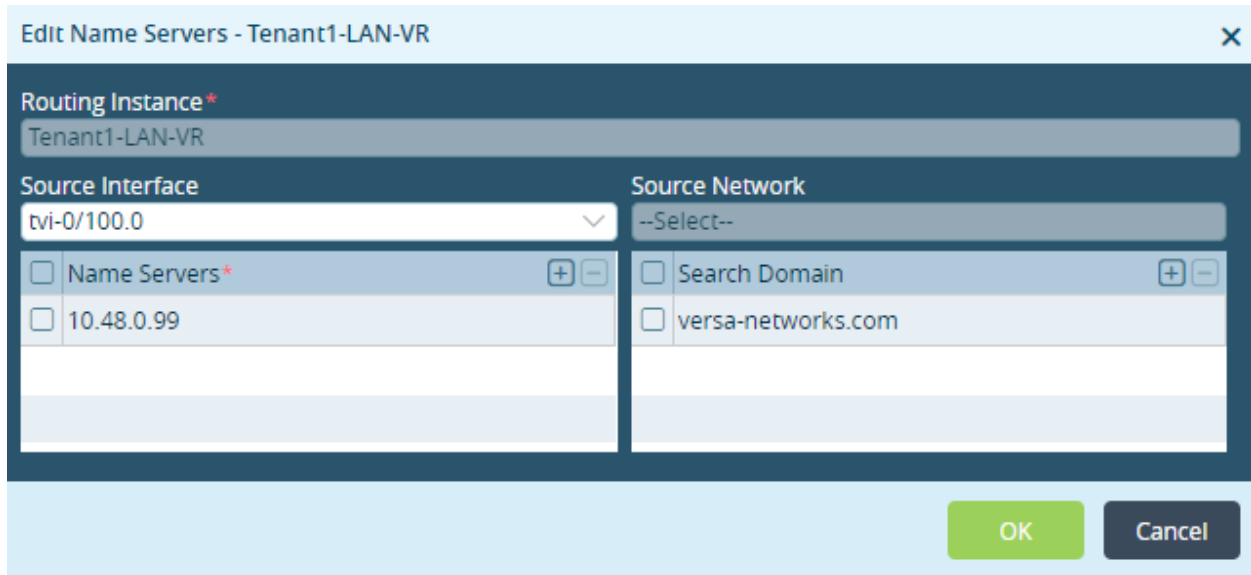
https://docs.versa-networks.com/Solutions/System_Hardening/Perform_Manual_Hardening_for_Versa_Branches%2C_Contr...

Updated: Thu, 24 Oct 2024 10:51:44 GMT

Copyright © 2024, Versa Networks, Inc.

DNS servers.

4. Click the  Edit icon to configure a DNS server.



5. Enter information in the Edit DNS window. For more information, see [Configure DNS Servers](#).
6. Click OK.

Verify the Software Version

For the best performance of all SD-WAN components, Versa Networks recommends that all components run the same software version. For more information, see [Perform Manual Hardening for Versa Director](#).

Enable TACACS+ or RADIUS Authentication


It is recommended that you enable centralized authentication using TACACS+ or RADIUS, and you can enable them at the device level.

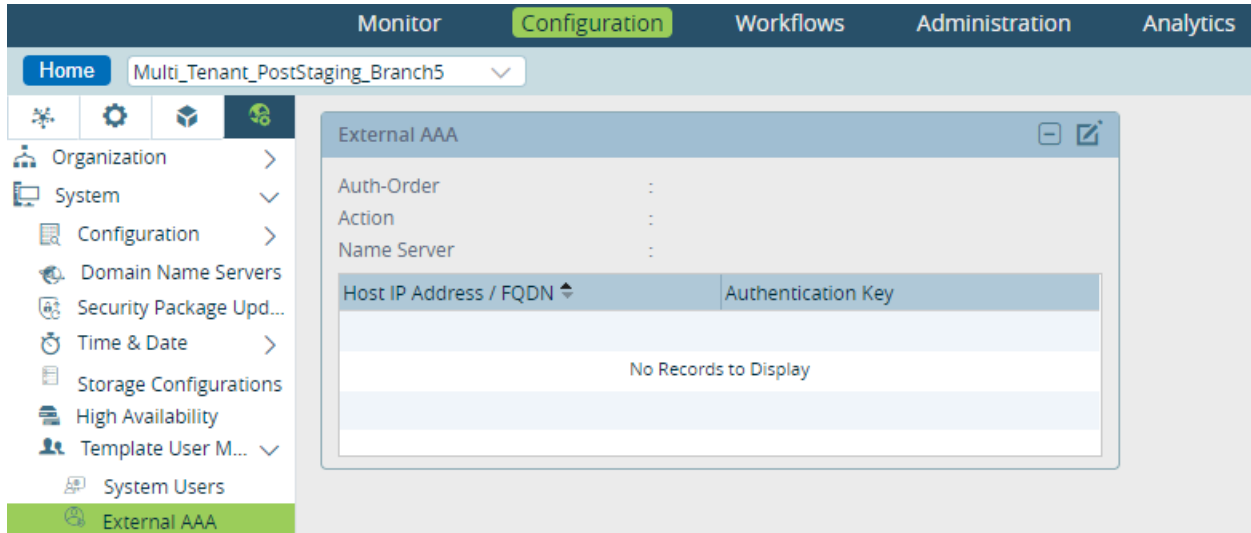
Enable Centralized Authentication

It is recommended that you enable centralized authentication on all Versa devices, using either TACACS+ or RADIUS for authentication.

To enable centralized authentication:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.

- b. Select Templates > Device Templates in the horizontal menu bar.
 - c. Select a device template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Others  > System > Appliance User Management > External AAA in the left menu bar.



4. Click the  Edit icon. In the Edit External AAA popup window, enter information for the following fields.

Edit External AAA

Protocol*

TACACS

Auth-Order*

local-then-remote

Action

☐ Authentication

☐ Accounting

☐ Both

☒ Use Remote Group

Server


Key*	IP Address	Routing Instance	
		Global	+
1	10.10.4.5	global	

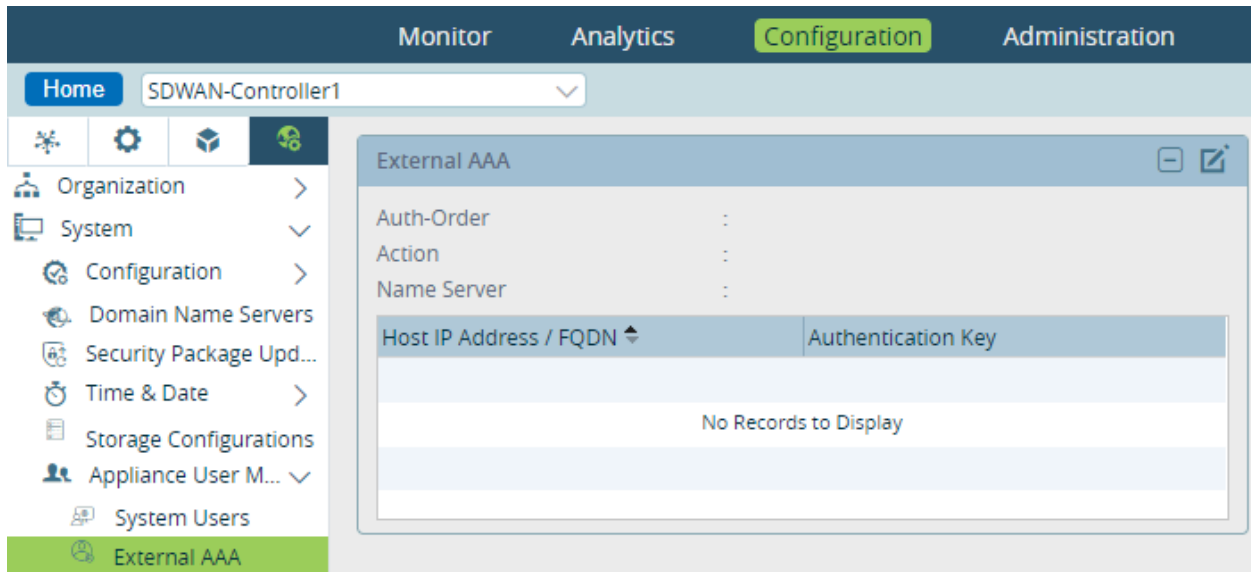
OK

Cancel

Field	Description
Protocol	Select the protocol: <ul style="list-style-type: none"> ◦ RADIUS ◦ TACACS+
Authentication Order	Select the order of authorization: <ul style="list-style-type: none"> ◦ local-then-remote ◦ remote-then-local
Action	Click to select the AAA action: <ul style="list-style-type: none"> ◦ Accounting ◦ Authentication ◦ Both
Server (Group of Fields)	
◦ Key	Enter the password to use to access the server.
◦ IP Address	Enter the IP address of the server.
◦ Routing Instance	Select the routing instance to use to reach the AAA server.

Enable TACACS+ or RADIUS Authentication at the Device Level

- In Director view:
 - Select the Configuration tab in the top menu bar.
 - Select Devices > Devices in the horizontal menu bar.
 - Select a Controller in the main pane. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select Others  > System > Appliance User Management > External AAA in the left menu bar.



4. Click the  Edit icon. The Edit External AAA popup window displays.

The 'Edit External AAA' popup window is shown. It has a title bar with a close button. The form contains the following fields and options:

- Protocol***: A dropdown menu currently set to 'TACACS'.
- Auth-Order***: A dropdown menu currently set to 'local-then-remote'.
- Action***: A group of radio buttons with options 'Authentication' (selected), 'Accounting', and 'Both'.
- Server**: A section containing a table with columns 'IP Address/FQDN*' and 'Authentication Key*'. The table is empty, showing 'No Records to Display'. A green '+' button is located to the right of the table header.

At the bottom of the window are two buttons: 'OK' (green) and 'Cancel' (dark blue).

5. In the Protocol field, select TACACS+ or RADIUS, and enter information for the other fields.
6. Click OK.

Authentication Attributes for SSH Access

To retain SSH access to a Director node, the following attributes must be returned as part of the TACACS+ or RADIUS accept message:

Attribute	Access Level
Versa-User-Group = admin	CLI read/write access
Versa-User-Group = oper	CLI read only access

The following is a sample of a TACACS+ server configuration file:

```
root@tacacs:/etc/tacacs+# more tac_plus.conf
# See man(5) tac_plus.conf for more details

# Define where to log accounting data; this is the default.

accounting file = /var/log/tac_plus.acct

# Dey that clients have to use to access TACACS+

key = versa123

# Use /etc/passwd file for authentication

# default authentication = file /etc/passwd

# Define a per-host key with different enable passwords
# host = 127.0.0.1 {
#     key = test
#     type = cisco
#     enable = <des|cleartext> enablepass
#     prompt = "Welcome XXX ISP Access Router \n\nUsername:"
#}

# Define local users and specify a file where data is stored.
# That file can be filled using tac_pwd
# user = test1 {
#     name = "Test User"
#     member = staff
#     login = file /etc/tacacs/tacacs_passwords
#}

# Specify rules valid per group of users.
# group = group1 {
#     cmd = conf {
#         deny
```

```

#    }
#}

# Another example: forbid configure command for some hosts
# for a defined range of clients
# group = group1 {
#     login = PAM
#     service = ppp
#     protocol = ip {
#         addr = 10.10.0.0/24
#     }
#     cmd = conf {
#         deny .*
#     }
#}

user = DEFAULT {
    login = PAM
    service = ppp protocol = ip {}
}

# Many more features are available, such as ACL, more service compatibilities,
# commands authorization, and scripting authorization.
# See the man page for more information.
#

group = TenantSuperAdminGroup {
    login = PAM
    service = test {
        Versa-Role = "TenantSuperAdmin"
        Versa-Tenant = "Galaxy-Foods"
        Versa-GUI-Idle-TimeOut = "300"
    }
}

group = TenantOperatorGroup {
    login = PAM
    service = test {
        Versa-Role = "TenantOperator"
        Versa-Tenant = "Galaxy-Foods"
        Versa-GUI-Idle-TimeOut = "300"
    }
}

group = TenantSecurityAdminGroup {
    login = PAM service = test {
        Versa-Role = "TenantSecurityAdmin"
        Versa-Tenant = "Galaxy-Foods"
        Versa-GUI-Idle-TimeOut = "300"
    }
}

group = TenantADCAdminGroup {
    login = PAM

```

```

    service = test {
        Versa-Role = "TenantADCAdmin"
        Versa-Tenant = "Galaxy-Foods"
        Versa-GUI-Idle-TimeOut = "300"
    }
}

group = ProviderDataCenterAdminGroup {
    login = PAM
    service = test {
        Versa-Role = "ProviderDataCenterAdmin"
        Versa-GUI-Idle-TimeOut = "300"
    }
}

group = ProviderDataCenterOperatorGroup {
    login = PAM service = test {
        Versa-Role = "ProviderDataCenterOperator"
        Versa-GUI-Idle-TimeOut = "300"
    }
}

group = ProviderDataCenterSystemAdminGroup {
    login = PAM service = test {
        Versa-Role = "ProviderDataCenterSystemAdmin"
        Versa-GUI-Idle-TimeOut = "300"
    }
}

group = flex_oper {
    default service = permit
    service = versa {
        Versa-User-Group = oper
    }
}

group = flex_admin {
    default service = permit
    service = versa {
        Versa-User-Group = admin
    }
}

group = uber_admin {
    default service = permit
    service = versa {
        Versa-User-Group = admin
    }
    login = PAM service = test {
        Versa-Role = "ProviderDataCenterSystemAdmin"
        Versa-GUI-Idle-TimeOut = "300"
    }
}

```

```

user = providersystemadmin {
    member = ProviderDataCenterSystemAdminGroup
    login = cleartext "versa123"
    pap = cleartext "versa123"
    # pap is needed for CLI access
    # # login is needed for GUI access
}

user = dave {
    default service = permit
    member = uber_admin
    login = des 1V4lf5pe4zRkE
    expires = "Sep 30 2099"
    pap = cleartext "versa123"
    # pap is needed for CLI access
    # # login is needed for GUI access
}

user = sultan {
    default service = permit
    member = ProviderDataCenterSystemAdminGroup
    login = des 1V4lf5pe4zRkE
    expires = "Sep 30 2099"
    pap = cleartext "versa123"
}

user = flexadmin {
    member = flex_admin
    login = cleartext "versa123"
    pap = cleartext "versa123"
}

```

Enable Secure Mode

You enable secure mode to harden the Linux core OS components to meet the Linux CIS benchmarks.

Before you enable secure mode, do the following:

- Download and install a full OS security package to the Versa Director so that the secure mode scripts are available. For more information, see [Use OS Security Packages](#).
- Enable centralized authentication. For more information, see [Enable Centralized Authentication](#), above.

To enable secure mode

1. From the CLI, execute the secure mode script:

```

| versa@Hub-a> request system secure-mode enable disable-nodejs

```

For example:

```
versa@Hub-1> request system secure-mode enable
Will enable secure mode. Are you sure? [no,yes] : yes
status success
result Enabling Versa OS secure mode
result Hardening SSH service
result Hardening password scheme
result Disabling USB storage
result Hardening permissions on system executables
result Hardening permissions on sensitive files
result Hardening: Disabling FileSystem knobs
result Hardening: Restricting the use of the job-scheduling privilege
result Hardening: System knobs and TCP settings
result Hardening console login permissions
result Hardening port permissions
```

2. Exit the CLI and restart Versa services for the changes to take effect:

```
$ vsh restart
```

3. Change the Linux user passwords on the local device so that they all meet the complexity criteria.

Update the IP Tables

You update the Linux IP tables to define IP packet filter rules for the Linux kernel firewall that allow or block traffic to the system. When a connection tries to establish itself on the system, iptables looks for a rule in its list to match it to. If no rule is found, the default action is taken.

Create IP Tables Rules for Versa Network Components

1. Create the following iptables rules so that Director nodes can work properly by allowing traffic to the following host interfaces:
 - Primary and secondary Director northbound interface address
 - Primary and secondary Director southbound interface address
 - localhost loopback, 127.0.0.1

```
sudo iptables -A INPUT -s ip-address -j ACCEPT
```

2. Create the following iptables rules to block all outside traffic:

```
sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
sudo iptables -P OUTPUT ACCEPT
sudo iptables -P FORWARD DROP
sudo iptables -P INPUT DROP
```

3. Add rules for hosts requiring SSH access to the Analytics node:

```
sudo iptables -A INPUT -s ip-address-of-ssh-source -p tcp -m tcp --dport 22 -j ACCEPT
```

4. Save the iptables rules and set the startup script to execute them:

```
root@Controller-1:~# iptables-save > /opt/versa/etc/rules.v4
root@Controller-1:~# echo -e "#Restore iptables rules\niptables-restore < /opt/versa/etc/rules.v4"
>> /opt/versa/scripts/setup_versa_env.sh
```

Edit the Hub IP Tables Templates

To edit the IP tables template for a hub device:

1. Save the current IP tables template by issuing the **iptables-save** command.

```
root@device-name:~# iptables-save > /opt/versa/etc/rules.v4
```

2. Edit rules file, /etc/iptables/rules.v4 file, using the editor of your choice (nano or vi) to reflect template fields shown above. Define the rules for the chains associated with the filter table. Replace each line between “*filter” and “COMMIT” with the content shown below, specifying the appropriate IP addresses. Specify the DROP and ACCEPT actions as appropriate.

3. Activate the iptables rules:

```
root@Branch-device:~# iptables-restore < /opt/versa/etc/rules.v4
```

4. Make the rules permanent by editing the /opt/versa/scripts/setup_versa_env.sh file using the editor of your choice (nano or vi) and ensure that the following line is at the end of file:

```
# Restore iptables rules
iptables-restore < /opt/versa/etc/rules.v4
```

6. Ensure that the startup script is still configured to load the iptables rules.
7. Check the /opt/versa/etc/rules.v4 and /opt/versa/scripts/setup_versa_env.sh files.

The following lines in the IP tables file come from the services loaded in the device, and they are included to avoid a reboot or service restart after you apply the rules:

```
-A INPUT -p tcp -m multiport --dports 22 -j fail2ban-ssh <-- Block IP addresses of clients who had too many
SSH login attempts; from the fail2ban service
-A INPUT -p icmp -m icmp --icmp-type 13 -j DROP <-- Block ICMP timestamp replies
-A OUTPUT -p icmp -m icmp --icmp-type 3 -j DROP <-- Block ICMP destination unreachable messages
-A OUTPUT -p icmp -m icmp --icmp-type 14 -j DROP <-- Block ICMP timestamp requests
```

The default output chain target is ACCEPT. To handle this, include the following line:

```
-A INPUT -m comment --comment "ACCEPT (RELATED | ESTABLISHED)" -m state --state (RELATED |
ESTABLISHED) -j ACCEPT
```

In this line:

- ESTABLISHED—The state has established traffic in both directions and continuously matches these packets.
- RELATED—A connection in this state is related to an ESTABLISHED connection, for example, an FTP connection.

Change the Default Device Linux Passwords

As part of the security hardening process, you must change the default Linux passwords for the following Director predefined user accounts:

- **aaaadmin**—SSH is disabled; used to map a user from external AAA with admin role when trying to access the shell.
- **aaauser**—SSH is disabled; used to map a user from external AAA with the oper role.
- **admin**—SSH is enabled.
- **versa**—SSH is disabled.

To change the default passwords from the shell:

1. Log in to the Controller node using the shell.
2. Switch to the user using the **su** command.
3. Change the admin user account password:

```
admin@Branch-1:~$ passwd
Changing password for admin.
(current) UNIX password:
New password:
Retype new password:
passwd: password updated successfully
```

4. Change the versa user account password:

```
admin@Branch-1:~$ sudo su versa
versa@director1:/home/admin$ passwd
Changing password for versa.
(current) UNIX password:
New password:
Retype new password:
passwd: password updated successfully
versa@director1:/home/admin$ exit
```

5. Change the aaaadmin user account password:

```
admin@Branch-1:~$ sudo su aaaadmin
[aaaadmin@director1 admin] # passwd
Changing password for aaaadmin.
(current) UNIX password:
New password:
Retype new password:
passwd: password updated successfully
```

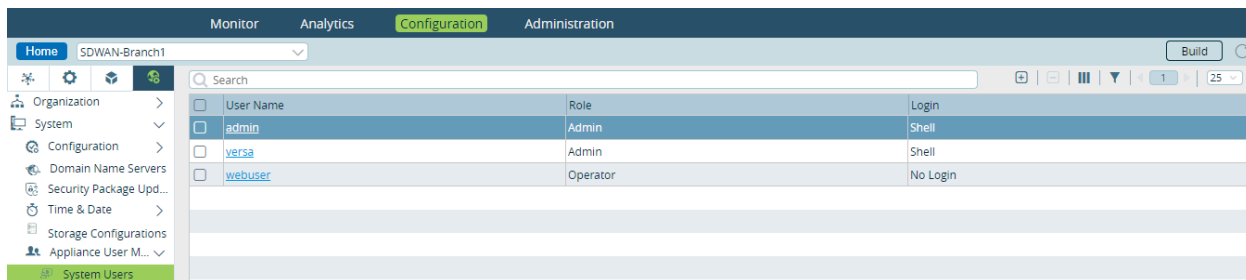
6. Change the aaauser user account password:

```
admin@Branch-1:~$ sudo su aaauser
[aaauser@Hub-1 admin] # passwd
Changing password for aaauser.
(current) UNIX password:
```


New password:
Retype new password:
passwd: password updated successfully

You can also change admin or versa user account passwords from the GUI:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Templates > Device Templates in the horizontal menu bar.
 - c. Select an organization in the left navigation bar.
 - d. Select a device from the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Others > System > Appliance User Management > System Users in the left menu bar.



4. Select the admin or versa user in the main pane. The Edit System User popup window displays.

The 'Edit System User - admin' popup window shows the following fields:

- User Name*: admin
- Login*: Shell
- Role*: Admin
- Password: [masked]
- Confirm Password: [masked]
- SSH-Public-Key: A table with columns 'Name' and 'Contents', currently empty with a 'No Records to Display' message.

At the bottom right are 'OK' and 'Cancel' buttons.

5. In the Password field, enter the password.
6. In the Confirm Password field, enter the same password.
7. Click OK.

Disable Promiscuous Mode

As part of branch, controller, or hub device hardening, you should disable promiscuous mode on the eth0 Ethernet interface.

To disable promiscuous mode on the eth0 interface:

1. Edit the `/etc/network/interfaces` file.

```
| $ sudo vi /etc/network/interfaces
```

2. Locate the line "iface ethx inet static", and replace x with the interface number.
3. Add the line "up ip link set ethx promisc off" to the file, replacing x with the interface number.
4. Save the file.
5. Switch off promiscuous mode:

```
| $ sudo ip link ethx promisc off
```

The following shows an example of the modified `/etc/network/interfaces` file for the eth0 interface:

```
auto eth0
iface eth0 inet static
up ip link set eth0 promisc off
address 192.168.0.10
netmask 255.255.255.0
mtu 1200
up route add -net 192.168.0.0 netmask 255.255.0.0 gw 192.168.0.239
up route add -net 10.0.0.0 netmask 255.255.0.0 gw 192.168.0.239
up route add -net 10.1.0.0 netmask 255.255.0.0 gw 192.168.0.239
up route add -net 10.2.0.0 netmask 255.255.0.0 gw 192.168.0.239
```

Harden SSH

Change the SSH Port

To change the default port on which the SSH daemon listens:

1. Change the default SSH port:

```
| $ sudo sed -i 's/22/1022/g' /etc/ssh/sshd_config
```

2. Restart the SSH service:

```
| $ sudo service ssh restart
```

Disable the SSH Server

As part of system hardening, you can optionally disable the SSH service on the branch device.

To disable the SSH service:

1. Stop the SSH daemon:

```
| $ sudo service ssh restart
```

2. Remove the SSH daemon from the init.d directory:

```
| $ sudo rm /etc/init.d/ssh
```

Harden the SSH Server Configuration

For branch devices only.

To have the SSH server on the branch device continue to run, set the following parameters:

1. Edit the `/etc/ssh/sshd_config` file, and set the following values for the following parameters:
 - `ClientAliveInterval`—300
 - `ClientAliveCountMax`—0
2. Save the file.
3. Restart the SSH daemon:

```
| $ sudo service ssh restart
```

Harden SSH Cryptographic Algorithms

This procedure is the follow up to [Harden the VOS confd Process](#) in the [Perform Manual Hardening for Versa Director](#) article.

To harden the SSH cryptographic algorithms:

1. Edit the `/etc/ssh/sshd_config` file
2. Verify that the following values are set for the Ciphers, MACs, and KexAlgorithms. Note that if other values are set, replace them with the values given below:
 - `Ciphers`—`aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr`
 - `MACs`—`hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512,hmac-sha2-256`
 - `KexAlgorithms`—`curve25519-sha256@libssh.org,diffie-hellman-exchange-sha256`
3. Save the file.
4. Restart the SSH daemon:

```
$ sudo service ssh restart
```

Harden File System Permissions

For Controller nodes only.

To harden the permissions on a Controller node:

1. Change the ownership of the /tmp and /var/tmp directories:

```
$ sudo chown root:versa_priv /tmp
$ sudo chown root:versa_priv /var/tmp
```

2. Change the permissions of the /tmp and /var/tmp directories:

```
$ sudo chmod 1770 /tmp
$ sudo chmod 1770 /var/tmp>
```

Secure ConfD SSH and SSL

As part of branch, Controller, and hub device hardening, you must perform additional hardening for port 8443, which is the Apache Tomcat port used for HTTPS and web GUI services. You can harden the channel between Versa Director and VOS devices, including Controller nodes, by using an encryption that is stronger than the default encryption for SSH and SSL transport.

To secure confd SSH and SSL:

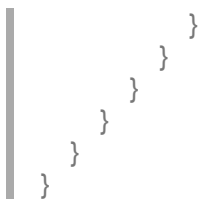
1. Log in to the device using the Director CLI.
2. Update the encryption for each Controller and VOS device:

```
devices {
  device SP01 {
    config {
      confdConfig {
        ssh {
          algorithms {
-           encryption aes128-ctr,aes192-ctr,aes256-ctr;
+           encryption aes256-ctr,aes256-cbc;
+           kex diffie-hellman-group-exchange-sha256;
          }
        }
      }
      webui {
        transport {
          ssl {
-           ciphers DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-
AES128-SHA256:DHE-RSA-AES256-SHA256;
+           ciphers DHE-DSS-AES256-SHA256,AES256-SHA256;
          }
        }
      }
    }
  }
}
```

https://docs.versa-networks.com/Solutions/System_Hardening/Perform_Manual_Hardening_for_Versa_Branches%2C_Contr...

Updated: Thu, 24 Oct 2024 10:51:44 GMT

Copyright © 2024, Versa Networks, Inc.



Perform System Upgrades

When you perform a system upgrade, for example, if you upgrade from Release 16.1R2S9 to Release 16.1R2S10, do the following to keep the system hardened

Before you upgrade a VOS device:

- Update to the latest OS Spack. For more information, see [Use OS Security Packages](#).
- Back up the iptables rules:

```
$ sudo iptables-save > iptables.rules
```

After you upgrade a VOS device:

- Reapply all the iptables rules

Supported Software Information

Releases 20.2 and later support all content described in this article.

Additional Information

[Configure AAA](#)

[Configure DNS Servers](#)

[Configure Systemwide Functions](#)

[Configure Time Settings](#)

[Perform Manual Hardening for Versa Analytics](#)

[Perform Manual Hardening for Versa Director](#)

[Use OS Security Packages](#)