TREND MICRO™

InterScan™ Web Security As A Service

Getting Started Guide

Total Web Protection - Everywhere and All the Time

Protected Cloud

Web Security

Trend Micro Incorporated reserves the right to make changes to this document and to the service described herein without notice. Before installing and using the service, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

http://docs.trendmicro.com

Document Part No.: APEM16354/140318

Release Date: March 2014

Protected by U.S. Patent No.: Patents pending.

This documentation introduces the main features of the service and/or provides installation instructions for a production environment. Read through the documentation before installing or using the service.

Detailed information about how to use specific features within the service may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp

Welcome to the Trend Micro™ InterScan Web Security as a Service Getting Start Guide. This guide describes how to perform basic product operations, test product configurations, and resolve issues.

About InterScan Web Security as a Service

InterScan Web Security as a Service (IWSaaS) is a security application that runs in a cloud environment. There is no capital expenditure as investments are not required for either hardware or software. By using IWSaaS, you can focus on strategic security, such as policy and architecture, rather than on the operational tasks of managing network infrastructure.

IWSaaS can protect a computer or mobile device. Using Mobile VPN, IWSaaS can protect iOS- and Android-based mobile devices.

Features:

- Anti-Malware Protection is highly configurable and detects viruses or other security risks in file uploads and downloads. IWSaaS also scans for many types of spyware, grayware, and other risks.
- Application Control automates the discovery of popular Internet applications and allows administrators to control them using policies.
- Approved/Blocked lists can also be used to control access to any specific site.
- URL Filtering offers policy-based traffic scans organized by URL categories, such as “Adult” or “Gambling” to filter traffic. When a user requests a URL, IWSaaS first looks up the category for that URL and then allows, denies, or monitors access based on the policies set up.

The figure below illustrates how IWSaaS manages your network traffic in the cloud. When a user sends an HTTP request - whether inside or outside your firewall - that user's traffic is routed through the cloud. IWSaaS inspects the request, analyzes it, and filters it based on policies set by administrators. If the request is allowed, and the user logs on IWSaaS, then IWSaaS sends the secure content back to the user. If the request is not allowed, for example a request to a forbidden URL category, then IWSaaS blocks the request and notifies the user.

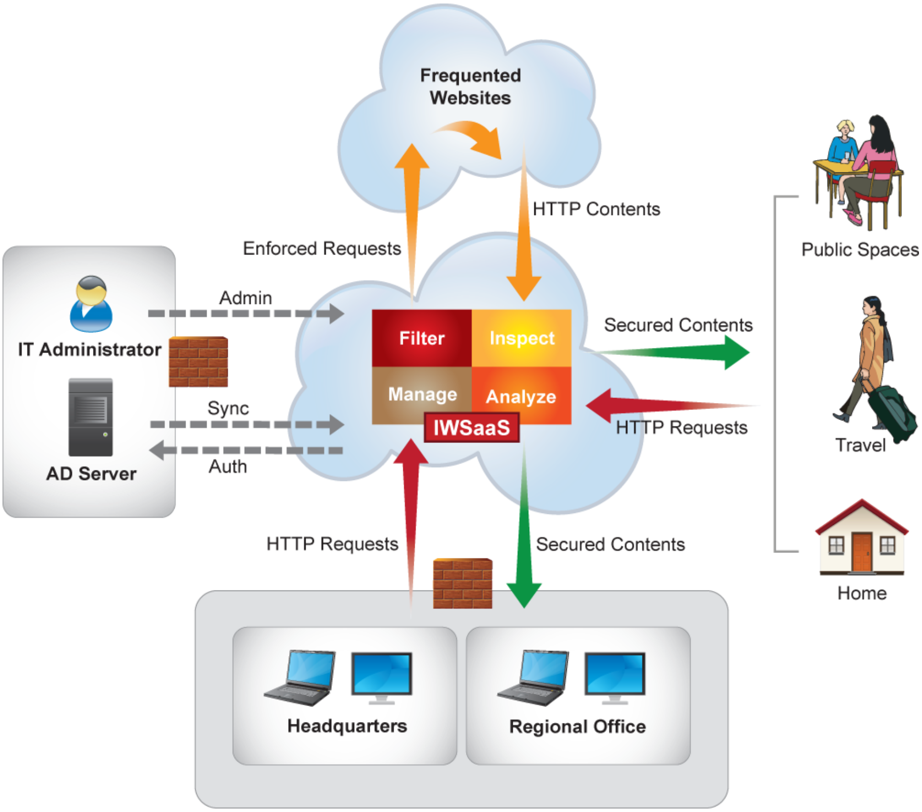


FIGURE 1. High-level Architecture Flow Diagram

For users wanting IWSaaS protection on their iOS or Android mobile devices, Mobile VPN connects each mobile user to IWSaaS and establishes an Internet Protocol Security (IPsec)-based VPN tunnel to send and receive traffic. Mobile VPN uses certificate-based authentication coupled with the mobile user's username and password to authenticate the user when establishing the VPN tunnel.

Audience

This guide is written for IT managers and system administrators. The reader should have in-depth knowledge of networks schemas, including:

- HTTP, HTTPS, FTP and other Internet protocols
- Antivirus and web security technology

Requirements

TABLE 1. Browser Requirements

BROWSER	VERSION	MANAGEMENT CONSOLE	CLIENT CONSOLE
Internet Explorer	8.x, 9.0, 10.0	Yes	Yes
Firefox	13.x - 22.x	Yes	Yes
Chrome	20.x - 28.x	Yes	Yes
Safari	5.x - 6.x	No	Yes

IWSaaS supports the following operating systems for the Authentication Agent and Synchronization Agent:

- Windows Server 2003
- Windows Server 2008 R2

IWSaaS supports the following platforms for Mobile VPN:

- iOS 6.x
- Android 3.x and greater

Summary of Operations

The following are the basic steps necessary to implement IWSaaS and establish protection that is best for your environment.

Procedure

1. Choose how to manage traffic.

   Forward traffic from your organization to IWSaaS using either port forwarding, proxy PAC, or proxy chaining.

   See *Provisioning Traffic Flow on page 5*.

2. Create a Customer Licensing Portal (CLP) account and log in for the first time.

   Logging on IWSaaS requires a CLP account.

   See *Creating an Account and Logging On on page 12*

3. Create all user accounts that will use IWSaaS.

   Adding a new user requires basic login information, as well as group and department affiliation.
   See *Adding New Users, Groups, and Departments on page 13*

   - If you have users in an Active Directory, you can authenticate these users for use in IWSaaS.

     See *Authenticating Active Directory Users on page 30*.

   - Instruct any users who desire to receive IWSaaS protection on their mobile devices. Download the installation and setup file(s) in order to connect a mobile device with the IWSaaS Service.

     See *Setting Up IWSaaS on a Mobile Device on page 15*.

4. Control traffic with policies for different user groups.

   Security and access policies can be customized for different needs, such as handling potentially malicious code or viewing certain categories of web content.
   See *Implementing Policies on page 49*.

To enforce traffic to IWSaaS, configure your network or client computers with the proper configuration. See *Enforcing Traffic to IWSaaS on page 56*.

5. Run reports based on network activities.

   Reports are generated from log information in the database.
   See *Analysis and Reporting on page 67*

6. Test the configuration.

   To test connectivity, set up the end-user account, specify the forwarding method and then connect to IWSaaS.

   See *Testing Connectivity and Performance on page 68*.

Provisioning Traffic Flow

Traffic forwarding requires no special hardware configurations because IWSaaS forwards traffic using existing infrastructure. Choosing a traffic-forwarding option depends on your existing architecture, budget, and organizational needs.

- Proxy Auto Configuration (PAC) file is best when the organization already has proxy configured and when supporting clients that often work outside of the network is required.
- Proxy chaining is best when you already have a proxy. PAC files and proxy chaining can be used concurrently.
- Only use port forwarding when necessary because it requires additional configuration.

Traffic Forwarding Options

TABLE 2. Pros and Cons of Traffic-forwarding Options

OPTION	PROS	CONS
Proxy PAC	• Supported by all major browsers • Easy to deploy using Active Directory • Users are protected whether on or off the network	Users with admin rights can bypass IWSaaS by installing a non-standard browser
Proxy Chaining	• Easy setup • Multiple rules offer full redundancy • Supported by most web proxies • Users cannot bypass	Users off corporate network are unprotected
Port Forwarding	• Easy setup • Supported by every major firewall • Users cannot bypass	• Only supports HTTP traffic, not HTTPS • Requires manual change if primary gateway is unavailable • Users off corporate network are unprotected
Mobile VPN	• Supports the iOS and Android platforms • Support both Wifi and 3G networks, with encryption further enhancing the user privacy over Wifi	

PAC File

Configure and specify a PAC file on the client browser to control which proxies are allowed. This requires no network changes and each PAC file can be customized for different users. If needed, use Active Directory Group Policies to simplify scaling the implementation.

Before deciding to use a PAC file, consider the following:

- PAC files are required for clients who may not always have network connectivity.
- Internet Explorer changes may be locked if the PAC file is implemented using Active Directory Group Policies.

Downloading the Default PAC File

IWSaaS provides a default PAC file that administrators can use or customize.

Location: **Administration** > **Service Deployment** > **PAC Files**

Procedure

1. Do one of the following:
   - Locate `proxy.pac` in the list, click the link in the **PAC File Location** column, and then save the file to the local device.
   - Click the `proxy.pac` file in the **PAC File Name** column and copy the contents from the **PAC file contents** field.
2. Import the default proxy.pac file into client browsers or modify the contents and then follow the instructions in *Adding a PAC File to IWSaaS on page 7*.

Adding a PAC File to IWSaaS

You can add a maximum of 10 PAC files.

Location: **Administration** > **Service Deployment** > **PAC Files**

Procedure

1. Click **Add**.
2. Provide the name, description, and the PAC file content.

> **Note**
>
> Trend Micro recommends authoring the PAC file in a text editor and then pasting the content into the dialog box.

3. Click **OK**.

Changing, Duplicating or Deleting a PAC File

Location: **Administration** > **Service Deployment** > **PAC Files**

- To modify an existing PAC file, open the desired file from the list.
- To duplicate an existing PAC file, select the desired file and then click **Duplicate**.
- To delete an existing PAC file, select the desired file and then click **Delete**.

PAC File Syntax

The below reference is the default PAC file that IWSaaS provides. For instructions about downloading the file to customize or import into client browsers, see *Downloading the Default PAC File on page 7*.

```
function islocalip(ip)  {
     return isInNet(ip, "127.0.0.0", "255.0.0.0") ||
            isInNet(ip, "169.254.0.0", "255.255.0.0") ||
            isInNet(ip, "10.0.0.0", "255.0.0.0") ||
            isInNet(ip, "192.168.0.0", "255.255.0.0") ||
            isInNet(ip, "172.16.0.0", "255.240.0.0");
}
function FindProxyForURL(url, host) {
     var DefaultScanner =
        "PROXY proxy.iws.trendmicro.com:80; DIRECT";
var HTTPSScanner   =
   "PROXY proxy.iws.trendmicro.com:80; DIRECT";
var FTPScanner     = "DIRECT";
var DNSNeedResolve = false;
var SkipHosts = [];
     if (isPlainHostName(host)) {
        return "DIRECT";
     }
     for (var i in SkipHosts) {
          if (shExpMatch(host, SkipHosts[i])) {
             return 'DIRECT';
          }
     }
     if (/\d+\.\d+\.\d+\.\d+/.test(host)) {
                if (islocalip(host)) {
                return 'DIRECT';
   }
     } else if (DNSNeedResolve) {
                  if (islocalip(dnsResolve(host))) {
                           return 'DIRECT';
              }
     }
     // ftp URL
     if (url.substring(0, 3) == "ftp") {
        return FTPScanner;
     }
     // https URL
     else if (url.substring(0, 5) == "https") {
          return HTTPSScanner;
     }
     // others URL
     else {
        return DefaultScanner;
     }
}
```

Note

- IWSaaS supports ports 80 and 8080.
- The default PAC file cannot be modified or deleted. Administrators can duplicate the default PAC file and update the new one according to their network firewall policies.
- The default PAC file is not configured to allow users inside the company network to access company's internal web servers. For information about setting the PAC file to allow internal sites, see *Accessing Internal Sites on page 70*.

Configuring Browsers with a Proxy or PAC File

Different browsers store proxy settings in a different locations.

Internet Explorer

Location: **Tools** > **Internet Options** > **Connections**

1. Click **LAN Settings**.
2. Do one of the following:
   - Select **Use automatic configuration script** and provide the file path of the proxy PAC file (stored locally or on a network share).
   - Select **Use a proxy server for your LAN** and provide the following address:

     ```
     proxy.iws.trendmicro.com:80
     ```
3. Click **OK** to close the **Local Area Network (LAN) Settings** window, and then click **OK** again to close **Internet Options**.

Google Chrome

1. Click the wrench icon located at the top-right.
2. Go to **Settings** > **Show advanced settings...** > **Change proxy settings...**.

   The **Internet Properties** window appears.
3. Click **LAN Settings**.

4. Do one of the following:

   - Select **Use automatic configuration script** and provide the file path of the proxy PAC file (stored locally or on a network share).

   - Select **Use a proxy server for your LAN** and provide the following address:

     ```
     proxy.iws.trendmicro.com:80
     ```

5. Click **OK** to close the **Local Area Network (LAN) Settings** window.

6. Click **OK** again to close **Internet Properties**.

Mozilla Firefox

Location: **Tools** > **Options** > **Advanced** > **Network Tab** > **Settings...**

1. Do one of the following:

   - Select **Manual proxy configuration** and provide the following address:

     ```
     proxy.iws.trendmicro.com:80
     ```

     Note

     To have IWSaaS scan HTTPS traffic, select **Use this proxy server for all protocols**.

   - Select **Automatic proxy configuration URL** and provide the file path of the proxy PAC file (stored locally or on a network share).

2. Click **OK** to close the **Connection Settings** window, and then click **OK** again to close **Options**.

Apple Safari (Mac)

Location: **System Preferences** > **Network**

1. Choose the method that the computer uses to connect to the Internet and then click **Advanced**.

2. Click the **Proxies** tab

3. Select **Automatic Proxy Configuration** and do one of the following:

    - In the **Proxy Configuration File** field, type `proxy.iws.trendmicro.com:80`.

    - Click **Choose File...** and select the file path of the proxy PAC file (stored locally or on a network share).

4. Click **OK**.

5. Click **Apply.**

Creating an Account and Logging On

Create a Trend Micro Customer Licensing Portal (CLP) account to log on to IWSaaS. If you already have a CLP account, log on with your current credentials.

Procedure

1. To obtain an account, visit https://tm.login.trendmicro.com and then click **Sign up now**.

2. Select **No, I am a first time user**, type the product key, and then click **Continue**.

3. Register your CLP account with Trend Micro.

    Provide your account information, such as user name, email, company name, address, timezone, and language.

4. Once logged on to CLP, click **Get Started**.

5. From the IWSaaS management console, verify company and license information:

    a. Go to **Administration** > **License Information**.

    b. Verify the company name and the license information.

        If this is incorrect, contact Trend Micro Support.

6. Specify domain configuration:

    The domain is predefined at the time of setup.

a. Go to **Administration** > **Users & Authentication** > **Domains** and then click **Add**.

b. Specify the domain name, and then click **Save**.

Repeat for all domains in your organization.

Note

Only register the public domain that is associated with email addresses. These domains are used to create hosted accounts (the account is an email address).

Managing IWSaaS with IWSH

If you are using InterScan Web Security Hybrid (IWSH) and would like this application to manage IWSaaS, then complete the following steps:

Procedure

1. Generate a Registration Token from the IWSH console.

   See the IWSH documentation for details.

2. From the **Web Security Hybrid** screen, enter the Registration Token.

3. Click **Register**.

Adding New Users, Groups, and Departments

Adding a new user requires basic logon information, as well as group and department affiliation. Use a group to implement policies and use a department for reporting.

Note

To ensure access to the IWSaaS Management Console, create at least one Administrator account in case the Customer Licensing Portal is under maintenance.

Location: **Administration** > **Users & Authentication** > **Hosted Users**

Procedure

1. Click **Add**.
2. From the **User Accounts** screen, specify the user account details.
   - The email address is the user name for new users.
   - The domain is specified at **Administration > Users & Authentication > Domains**
3. Specify your password.
4. Select a group membership or create a new one.
5. Select department membership or create a new one.
6. Click **Save**.

   IWSaaS sends the new hosted user a welcome email containing a link used to setup a password on the product. Using the text field in the "User Notifications" screen, you can append a customized message to the email.

IWSaaS Mobile Service

Mobile VPN supports the iOS and Android platforms. With Mobile VPN, each mobile user connects to InterScan Web Security as a Service (IWSaaS) and establishes an Internet Protocol Security (IPsec)-based VPN tunnel to send and receive traffic. Mobile VPN uses certificate-based authentication coupled with the mobile user's username and password to authenticate the user when establishing the VPN tunnel.

The mobile devices are IPsec clients of the IWSaaS Mobile VPN Server. As IPsec clients, IWSaaS secures IP communications by authenticating the user when establishing the tunnel and encrypting each IP packet of a communication session.

For mobile users leaving an organization, all that is needed to disable the Mobile VPN service for them is to disable their authentication credentials (either in Active Directory or hosted environment). There is no need for the system administrator to proactively uninstall the profile or certificates as the user authentication will prevent the user from using IWSaaS.

Setting Up IWSaaS on a Mobile Device

Location: Administration > Service Deployment > Mobile VPN

Download the installation and setup file(s) in order to connect a mobile device with the IWSaaS Service.

For an iOS mobile device:

1. Click the appropriate link to download the profile.

2. Pass this file to mobile users who want protection from the IWSaaS Service using a VPN.

3. Instruct the mobile users on how to connect their mobile devices with the IWSaaS Service.

   See *Preparing an iOS Mobile Device for IWSaaS Protection on page 16*.

For an Android mobile device:

1. Click the appropriate links to download the Certificate Authority (CA) and Android Certificate.

2. Pass these files to mobile users who want protection from the IWSaaS Service using a VPN.

3. Instruct the mobile users on how to connect their mobile devices with the IWSaaS Service.

   See *Preparing an Android Mobile Device for IWSaaS Protection on page 19*

4. Instruct the mobile users on how to scan their mobile devices.

   See *Scanning a Mobile Device with IWSaaS on page 26*.

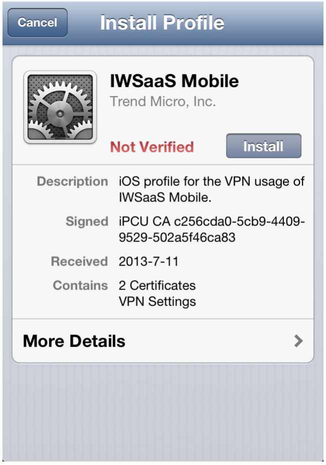
Preparing an iOS Mobile Device for IWSaaS Protection

Use this procedure to instruct users on how to receive IWSaaS protection on their iOS mobile devices.

Procedure

1. From the email sent by the system administrator, tap the iOS mobile profile or the network link to this file.

2. From the "Install Profile" dialog box, tap **Install**.

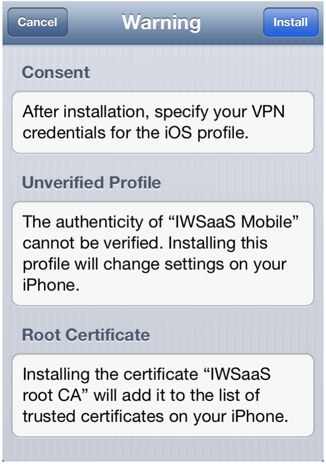


Description: iOS profile for the VPN usage of IWSaaS Mobile.
Signed: iPCU CA c256cda0-5cb9-4409-9529-502a5f46ca83
Received: 2013-7-11
Contains: 2 Certificates
VPN Settings

Since this is a self-signed certificate, a warning message appears stating that this profile is unverified. There is no reason to be concerned about this.

3. Tap **Install**.

The warning message stating that this profile is unverified is nothing to be concerned about and requires no action from you. The "Profile Installed" screen appears displaying two certificates – the VPN CA certificate and the mobile client certificate – as well as the various VPN settings such as VPN server name and proxy information.



Consent

After installation, specify your VPN credentials for the iOS profile.

Unverified Profile

The authenticity of “IWSaaS Mobile” cannot be verified. Installing this profile will change settings on your iPhone.

Root Certificate

Installing the certificate “IWSaaS root CA” will add it to the list of trusted certificates on your iPhone.

4. Tap **Install**.

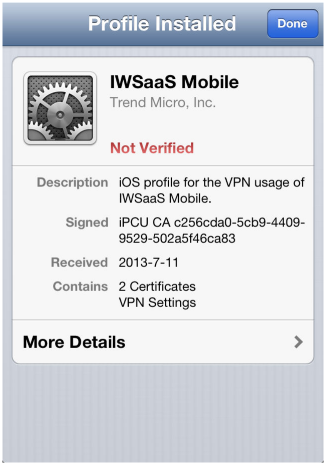
   If the mobile device is PIN-protected, supply the necessary information.

5. Tap **Done**.

Note

Once the certificates are installed and signed by a Certificate Authority, the Unverified Profile warning message leaves and the installed profile appears in the “Profiles” screen.

To view the newly installed profile, go to **Settings > General > Profiles**.



Profile Installed

Done

IWSaaS Mobile

Trend Micro, Inc.

Not Verified

Description iOS profile for the VPN usage of IWSaaS Mobile.

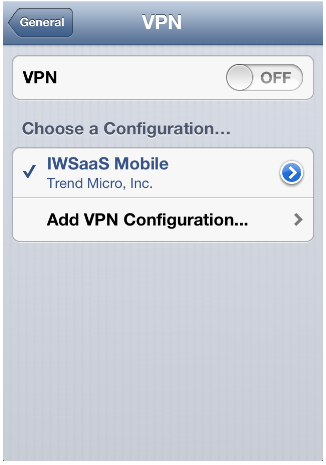
Signed iPCU CA c256cda0-5cb9-4409-9529-502a5f46ca83

Received 2013-7-11

Contains 2 Certificates
VPN Settings

More Details

6. Go to **Settings > VPN > IWSaaS Mobile**.



General

VPN

VPN OFF

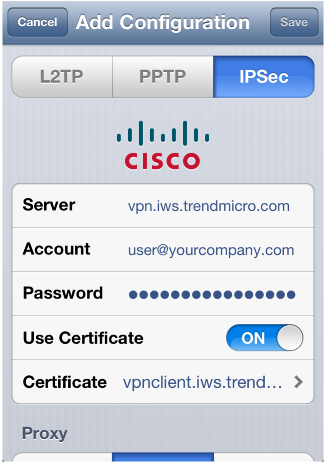
Choose a Configuration...

✓ IWSaaS Mobile
Trend Micro, Inc.

Add VPN Configuration...

7. Tap on the small, blue arrow button.

The "Add Configuration" dialog box appears for that VPN Profile (with the “IPSec” tab enabled).



Server vpn.iws.trendmicro.com

Account user@yourcompany.com

Password ●●●●●●●●●●●●●●●●

Use Certificate ON

Certificate vpnclient.iws.trend…

8. From the “Add Configuration” dialog box, enter the account and password information and then tap **Save**.

Preparing an Android Mobile Device for IWSaaS Protection

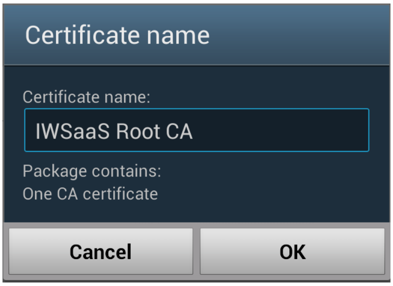
Use this procedure to instruct users on how to receive IWSaaS protection on their Android mobile devices.

Procedure

1. From the email sent by the system administrator, import the certificates.

   a. Tap the CA certificate link to import this certificate.

   b. Specify the name tag for the CA certificate, such as “IWSaaS Root CA”.



Certificate name

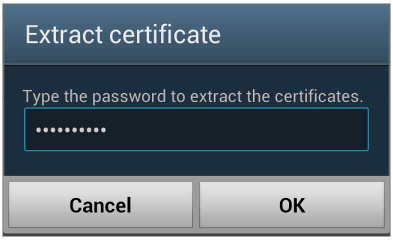
Certificate name:

IWSaaS Root CA

Package contains:
One CA certificate

c. Tap the mobile certificate link to import this certificate.

When prompted, specify the `trendmicro` password in order to extract the certificate.

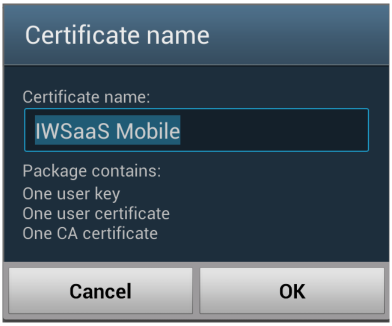


Extract certificate

Type the password to extract the certificates.

••••••••••

d. Specify the name tag for the mobile certificate, such as “IWSaaS Mobile”.



Certificate name

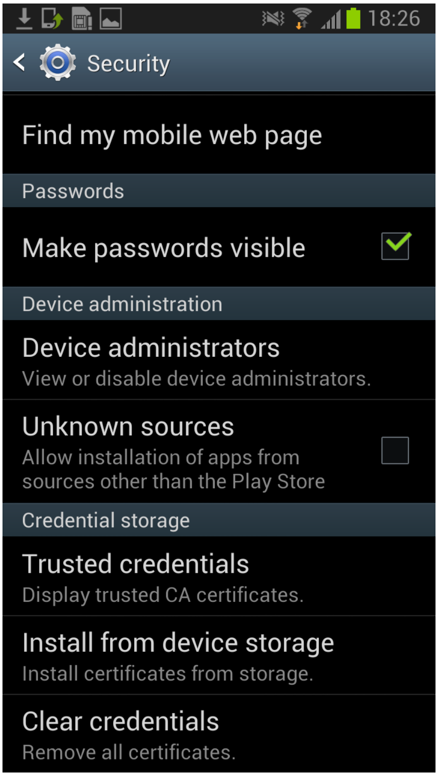
Certificate name:

IWSaaS Mobile

Package contains:
One user key
One user certificate
One CA certificate

2. To view your certificates, go to **Settings > Security > Trusted Credentials**.

The “System” tab is displayed by default.



18:26

Security

Find my mobile web page

Passwords

Make passwords visible ☑

Device administration

Device administrators
View or disable device administrators.

Unknown sources ☐
Allow installation of apps from sources other than the Play Store

Credential storage

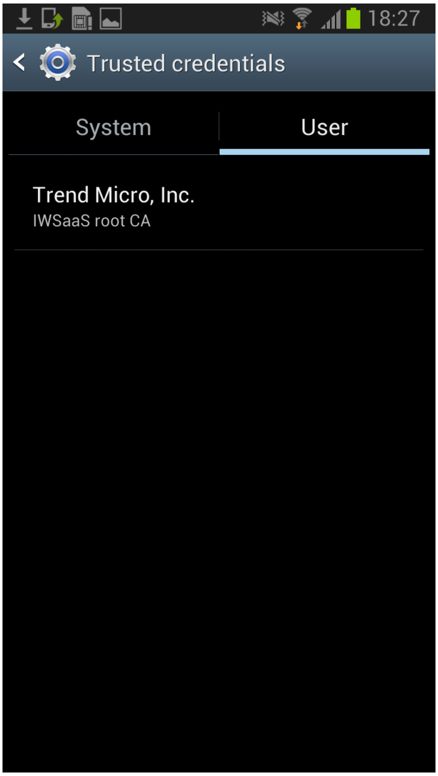
Trusted credentials
Display trusted CA certificates.

Install from device storage
Install certificates from storage.

Clear credentials
Remove all certificates.

3. Click on the “User” tab.

The CA certificates you installed appears.

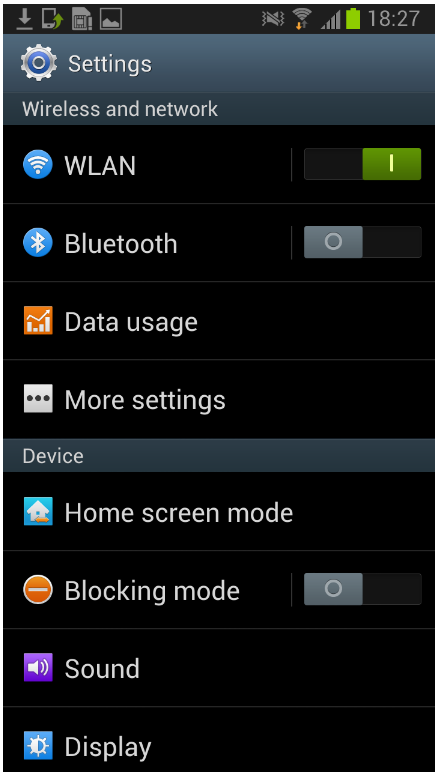


18:27

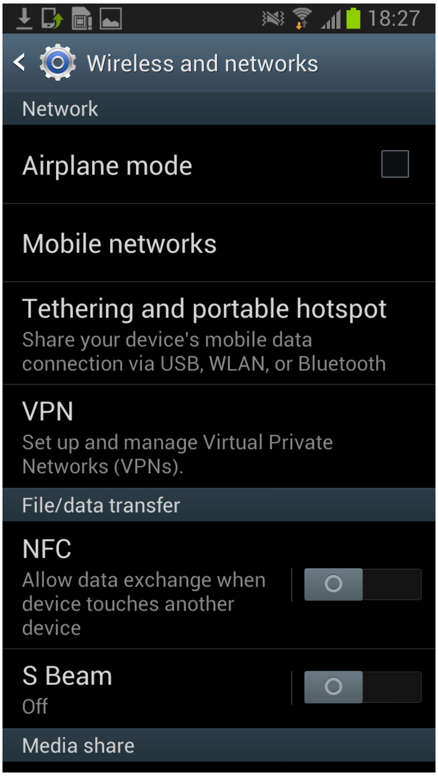
Trusted credentials

Trend Micro, Inc.
IWSaaS root CA

4. To configure the Android VPN profile, select **Settings > Wireless & Networks > More Settings > VPN**.



18:27
Settings
Wireless and network
WLAN
I
Bluetooth
O
Data usage
More settings
Device
Home screen mode
Blocking mode
O
Sound
Display



18:27

Wireless and networks

Network

Airplane mode □

Mobile networks

Tethering and portable hotspot
Share your device's mobile data connection via USB, WLAN, or Bluetooth

VPN
Set up and manage Virtual Private Networks (VPNs).

File/data transfer

NFC
Allow data exchange when device touches another device

S Beam
Off

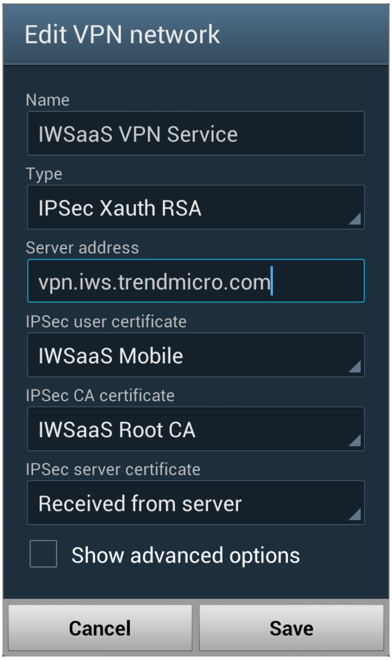
Media share

5. If you have the option of basic VPN or advance VPN, choose basic VPN.

6. Enter the details of the VPN profile, with particular note to the following:

    - Enter the profile name (such as "IWSaaS VPN Service") in the **Name** field. This can be any ASCII string that describes your profile.
    - Change the default **Type** field from **PPTP** to **IPSec XAuth RSA**.
    - In the **Server Address** field, enter the VPN service name "vpn.iws.trendmicro.com".
    - Select the client certificate (for example, "IWSaaS Mobile") you have just installed for the **IPSec User Certificate** field.

- Select the CA certificate (for example, "IWSaaS Root CA") you have just installed for the **IPSec CA Certificate** field.



Edit VPN network

Name: IWSaaS VPN Service

Type: IPSec Xauth RSA

Server address: vpn.iws.trendmicro.com

IPSec user certificate: IWSaaS Mobile

IPSec CA certificate: IWSaaS Root CA

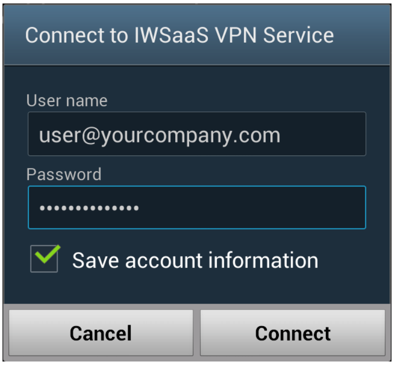
IPSec server certificate: Received from server

□ Show advanced options

7. Click **Save**.

8. From the list of configured VPN profiles, tap and hold on the profile name.

9. Enter your IWSaaS account information in the **Username** and **Password** fields.



Connect to IWSaaS VPN Service

User name: user@yourcompany.com

Password: ••••••••••••••

☑ Save account information

You can save the information to avoid re-specifying it for each session of IWSaaS VPN.

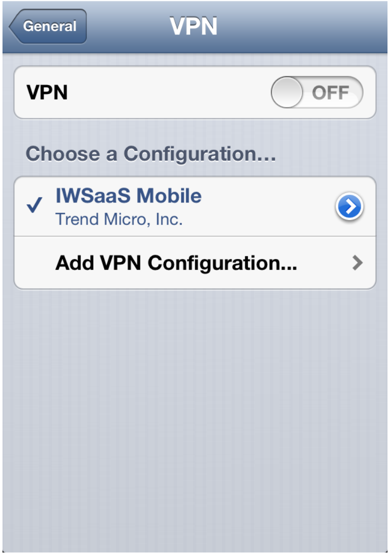
Scanning a Mobile Device with IWSaaS

After Mobile VPN connects, IWSaaS directs all traffic through the VPN tunnel to the VPN Service. The first time you browse to a website, IWSaaS redirects you to the login page where you enter your user login and password information. Next, IWSaaS redirects you to your website.

IWSaaS stores a cookie on the iOS and Android device so you will not be asked for your login information for the next 2 weeks (14 days).

For an iOS mobile device:

1. Go to **Settings > VPN** and then slide the **VPN** button to **On**.



VPN OFF

Choose a Configuration...

✓ IWSaaS Mobile
Trend Micro, Inc.

Add VPN Configuration...

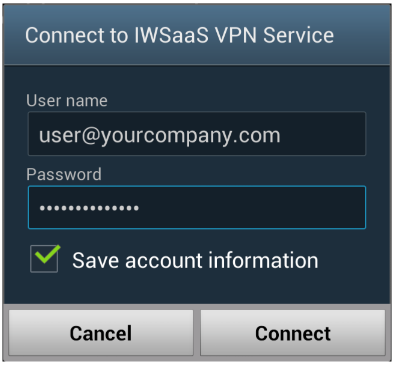
After mobile VPN connects, access any HTTP website with your default browser to authenticate IWSaaS. Otherwise, IWSaaS VPN Service cannot protect the traffic from a mobile application.

Note

The IWSaaS VPN Service disconnects after an iOS mobile device auto-locks.

For an Android mobile device:

1. Go to **Wireless Networks > More Settings > VPN** and then tap your IWSaaS VPN profile.



Connect to IWSaaS VPN Service

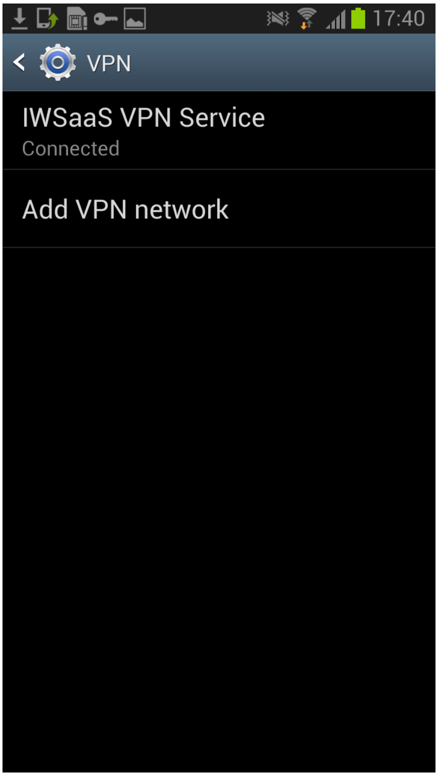
User name: user@yourcompany.com

Password: ••••••••••••••

☑ Save account information

2. Tap **Connect** in the dialog box.

   An image of a key appears in the menu bar and the "Connected" status appears under the profile name.



17:40

VPN

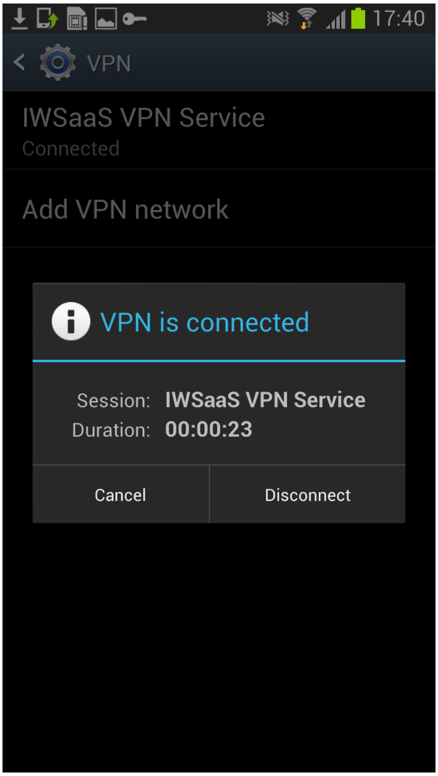
IWSaaS VPN Service

Connected

Add VPN network

After mobile VPN connects, access any HTTP website with your default browser to authenticate IWSaaS. Otherwise, IWSaaS VPN Service cannot protect the traffic from a mobile application.

To disconnect, tap the profile name and then tap **Disconnect** in the dialog box.


17:40

VPN

IWSaaS VPN Service
Connected

Add VPN network

VPN is connected

Session: IWSaaS VPN Service
Duration: 00:00:23

Authenticating Active Directory Users

You can authenticate Active Directory users using either the Direct, SAML, or Agent authentication method, in conjunction with the default authentication method, Hosted Users.

TABLE 3. Choosing an Active Directory Authentication Method

METHOD	ABOUT	BENEFIT
Direct Authentication	Direct Authentication is an agentless solution that authenticates users by connecting directly to your Active Directory and synchronizing Active Directory users and groups having limited attributes, which are configured in IWSaaS.	Requires no extra tool or agent installation in your network.
SAML Authentication	SAML Authentication uses the Synchronization Agent and your SAML server to synchronize and authenticate users. The Synchronization Agent provides the Active Directory synchronization.	Provides a secure solution for those with a SAML server, such as ADFS. With this authentication method, the Active Directory account and password do not go through IWSaaS, which adds to your privacy.
Agent Authentication	Agent Authentication uses the Synchronization Agent and Authentication Agent to synchronize and authenticate users. This authentication method functions the same as the SAML IDP server.	Provides the same level of security that SAML Authentication provides, for those not using a SAML server. It helps you setup SAML service which integrates with IWSaaS simply and quickly.

Specifying the Primary Domain and Active Directory User Account Format

Regardless of the authentication method, you need to select a primary Active Directory domain from your approved domain list. If you do not have an approved domain, there will be no primary domain available for selection in the **Active Directory** screen.

Location: **Administration** > **Users and Authentication** > **Domains**

Procedure

1. Register your organization's domain and wait for approval.

2. Select your primary domain from the **Active Directory** screen.

   It is necessary to select a primary domain in order to specify the Active Directory account format for end users. The Active Directory account format is as follows: `<sAM Account Name>@<primary domain>`.

   For example, an organization's domain could be `example.com` and a user could have an email address of `john_doe@example.com`. When this user logs on to the organization’s domain, the account format is `example\johnd`. When the organization joined IWSaaS and registered `example.com` as the primary domain, `johnd@example.com` was the account format used for user, John Doe.

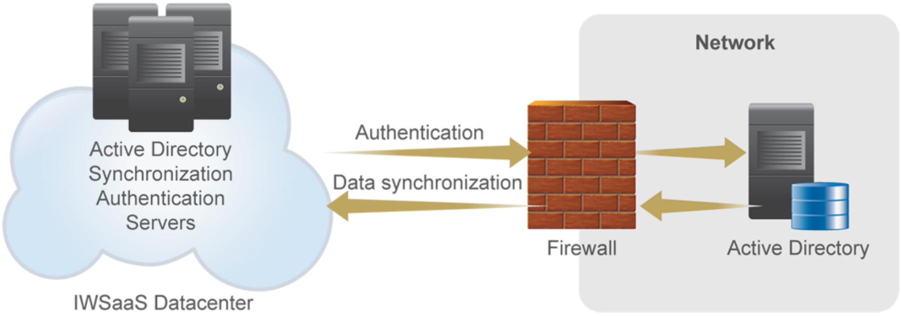
   Note

   The Active Directory account format is different from that of hosted accounts. When the administrator tries to create a hosted account for a user, he will use his email address format `john_doe@example.com` so all of the hosted account related emails, such as welcome emails and reset password emails, can be delivered to this mail address.

   IWSaaS also enables Active Directory users to log on using their email address, once the email attribute is correctly configured.

Authenticating Users Directly

Use this method of user authentication if you want a simplified solution that provides adequate security.



This method is an agentless solution which does not require you to install any agent-supporting software on your network. IWSaaS servers running in the cloud connect directly to your Active Directory servers to synchronize and authenticate users and groups when they logon to IWSaaS.

Note

When there is a firewall protecting the network, open incoming port 389 to allow IWSaaS servers to connect to the Active Directory. If the Active Directory is set to transmit Active Directory traffic over SSL, then open incoming port 636 instead.

Note

To enhance the firewall security level setting, only allow the IWSaaS server's IP to connect to the Active Directory using either port 389 or 636. Request the IP list from Trend Micro (http://esupport.trendmicro.com/SRFMain.aspx).

Note

Access http://support.microsoft.com/kb/321051/en-us to learn how to enable your Active Directory to transmit Active Directory traffic over SSL.

Location: Administration > Users and Authentication > Active Directory

Procedure

1. Click the **Direct** Active Directory authentication method.

2. From the **Cloud Settings** section, specify all the necessary information.

   - **Enable secondary Active Directory** ensures the continuation of service in case the primary Active Directory server becomes unavailable.

   - **Enable anonymous authentication** allows the administrator to be authenticated without providing an Active Directory administrator's account.

     > **Note**
     >
     > **Enable anonymous authentication** on the Active Directory server in order for it to work in IWSaaS.

   - The **Base Distinguished Name** is used by the Active Directory server as a reference point when querying the Active Directory.

   - From the **User settings** section, configure all the user's attributes.

     > **Note**
     >
     > If **User Email Attribute** is correctly configured, then Active Directory users are able to log on using their email address as their account name.

   - From the **Group Settings** section, configure all the user group attributes.

   - **Synchronization Frequency** is where you can either initiate Active Directory synchronization manually, or specify automatic synchronization (daily, weekly, or monthly). If you choose **Manually**, click **Sync Now** to complete the operation.

3. From the **Attributes** section, specify all the necessary information.

   - **Username attribute** is the Active Directory user ID attribute name, with "sAMAcountName" as the default. This name is unique over the whole domain and can be up to 20 characters. Typically, this name is the user's Windows user name and does not include the user's domain name.

- **Email attribute** is the Active Directory user email address. Configuring this field enables Active Directory users to log on using their email address as their account name.
- **User full name attribute** the name of the Active Directory user.
- **Department name attribute** is the attribute name of the department to which the Active Directory user belongs.
- **Group attribute** is the Active Directory group attribute that is used in the relationship between a user and a group or a group and a group.
- **Group name attribute** is the name of the Active Directory group attribute.

Note

The values in the **Attributes** section are the default values from the Active Directory. You can change any of these values and specify information for any empty fields.

4. From the **Filters** section, specify all the necessary information.

Note

The values in the **Filters** section are the default values from the Active Directory. You can change any of these values and specify information for any empty fields.

5. Click **Save**.

Authenticating Users Using a SAML Server

Use this method of user authentication if you want a very secure solution and you have a SAML server. The Active Directory account and password do not go through IWSaaS.

Specifying Ports for the SAML Server

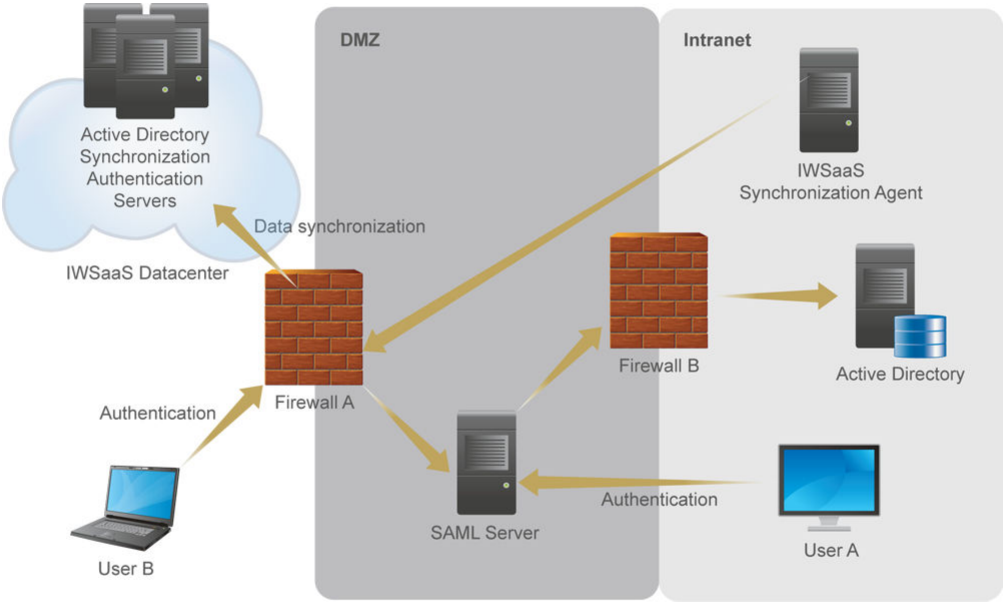


FIGURE 2. SAML Server Deployment

Procedure

1. Install the IWSaaS Synchronization Agent in your Intranet.

   The Synchronization Agent connects to your Active Directory to synchronize user and group data with IWSaaS. The data transmits over the HTTPS protocol on port 443 and this outgoing port is usually open on Firewall A by default, as depicted in the graphic above.

2. Deploy the SAML server in the DMZ.

3. On Firewall A, open incoming port 443 to allow any IP to connect to your SAML server.

4. On Firewall B, open incoming port 389 (or 636 when SSL is enabled in the Active Directory) to allow SAML server connect to the Active Directory.

Note

Putting the SAML server in the DMZ allows user authentication regardless if they are inside the corporate network (User A) or outside of it (User B). But if you deploy the SAML server in the Intranet, only User A--who is inside the corporate network, can authenticate and login to IWSaaS.

Source	Destination	Firewall settings
Intranet	IWSaaS services	Outbound port 443 on Firewall A (normally open)
Internet	SAML server in DMZ	Inbound port 443 on Firewall A
SAML Server in DMZ	Active Directory Server	Inbound port 389 on Firewall B (or 636 when SSL is enabled in the Active Directory)

Specifying SAML Active Directory Authentication

Location: Administration > Users and Authentication > Active Directory

Procedure

1. Enable Active Directory and then click **SAML**.
2. Click **Select** to select the desired SSL public certificate and then click **Upload** to upload it.

   You created the SSL public certificate in the **Certificate Export** wizard.
3. From the **SAML Identity Provider Settings** section, specify the following:
   - **URL of SAML SSO service**: https://<adfs_domain_name>/adfs/ls/
   - **Login name attribute**: sAMAccountName

- You can obtain the **URL of SAML SSO service** information from the XML metadata of the SAML Identity Provider.
- **Login name attribute** is used by IWSaaS to format Active Directory users based on the format, `userid@domain`. `userid` is synchronized from the Active Directory, using the **User Name Attribute** specified in the Active Directory synchronization settings. The **Login name attribute** should be the same value as the **User Name Attribute** of Active Directory synchronization setting, which is the default value of **sAMAccountName**.
- **SSL public certificate** is the public certificate of the SAML Identity Provider, used to verify a digital signature.

  You created the SSL public certificate in the **Certificate Export** wizard.

4. From the **SAML Service Provider Settings** section, specify all the necessary Service Provider information.

   Require signed SAML request is necessary if the SAML Service Provider expects the SAML request to be signed.

5. Click **Save**.

   The Synchronization Agent synchronizes users with IWSaaS.

Configuring for SAML Active Directory Authentication

The Synchronization Agent and SAML Server must be configured in order to use SAML Active Directory Authentication.

Configuring the Synchronization Agent

Location: Administration > Users and Authentication > Active Directory

Procedure

1. Enable Active Directory and then click **SAML**.
2. Click the **Download the Synchronization Agent** link.

3. Save the installation package to a server in the Intranet.

4. Launch the installation wizard and then follow the prompts.

5. From the "Trend Micro IWSaaS AD Sync Agent" dialog box, specify the necessary information and then click **Apply**.

   - **Enable secondary Active Directory** ensures the continuation of service in case the primary Active Directory server becomes unavailable.

   - **Enable anonymous authentication** allows the administrator to be authenticated without providing an Active Directory administrator's account.

   > **Note**
   >
   > **Enable anonymous authentication** on the Active Directory server in order for it to work in IWSaaS.

   - The **Base Distinguished Name** is used by the Active Directory server as a reference point when querying the Active Directory.

   - From the **User settings** section, configure all the user's attributes.

   > **Note**
   >
   > If **User Email Attribute** is correctly configured, then Active Directory users are able to log on using their email address as their account name.

   - From the **Group Settings** section, configure all the user group attributes.

   - **Synchronization Frequency** is where you can either initiate Active Directory synchronization manually, or specify automatic synchronization (daily, weekly, or monthly). If you choose **Manually**, click **Sync Now** to complete the operation.

   - From the "IWSaaS Credential" section, configure a IWSaaS hosted administrator's account and password here to allow this Synchronization Agent to connect to IWSaaS.

   - From the "Network" section, configure your proxy address if your Intranet network can only access the Internet through a proxy server.

Configuring the SAML Server

This section describes how to configure Active Directory Federation Service (AD FS) 2.0 as a SAML server in order to work with IWSaaS.

Location: IWSaaS web console > Administration > Users and Authentication > Active Directory

Procedure

1. Enable Active Directory and then select **SAML**.
2. From the "SAML Service Provider Settings" section, click the **View Service Provider Metadata** link.
3. Save the XML file as `iwsmetadata.xml`.
4. After installing AF DS 2.0 successfully, go to **Start > All Programs > Administrative Tools > AD FS 2.0 Management**.
5. On the AD FS 2.0 Management Console, go to **AD FS 2.0 > Trust Relationships** > , right click **Relying Party Trusts** and then choose **Add Relying Party Trust**.
6. Provide information for each screen in the Add Relying Party Trust wizard.
   - From the "Select Data Source" step, select **Import data about the relying party from a file** and then browse and select `iwsspmetadata.xml`
   - From the "Specify Display Name" step, specify your desired name, such as "IWSaaS".
   - From the "Choose Issuance Authorization Rules" step, select **Permit all users to access this relying party** and then click **Next**.
   - Continue clicking **Next** in the wizard and finally click **Close**.

     The "Edit Claim Rules for IWSaaS" window appears.
7. From the "Edit Claim Rules for IWSaaS" window, click **Add Rule** in the "Issuance Transform Rules" tab.
8. Provide information for each screen in the Add Transform Claim Rule wizard.

- From the "Choose Rule Type" step, specify "Claim rule template" for "Send LDAP Attributes as Claims" and then click **Next**.
- From the "Configure Claim Rule" step:
    - Specify the claim rule name and specify **Active Directory** for the attribute store.
    - Select **SAM-Account-Name** for the LDAP Attribute and select **sAMAccountName** for Outgoing Claim Type.

      Note

      The value for the **Outgoing Claim Type** column should be the same as the **Login name attribute** field in the “SAML Identity Provider Settings” section of SAML Authentication settings.

    - Click **Finish** to add the new rule.

9. From the "Edit Claim Rules for IWSaaS" dialog box, click **Add Rule** to add another rule with the following settings:
    - **Claim rule template:** Send Claims Using a Custom Rule
    - **Claim rule name:** Any desired name, such as “user-defined”.
    - **Custom rule:** Content of the customer rule.

```
c1:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
 && c2:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationinstant"]
 => add(store = "_OpaqueIdStore", types =
("http://mycompany/internal/sessionid"), query = "{0};{1};{2};{3};
{4}", param = "useEntropy", param = c1.Value, param =
c1.OriginalIssuer, param = "", param = c2.Value);
```

10. Click **Add Rule** to add a third rule with following settings:
    - **Claim rule template:** Transform an Incoming Claim
    - **Claim rule name:** Any desired name, such as “roamer”
    - **Incoming claim type:** http://mycompany/internal/sessionid
    - **Outgoing claim type:** Name ID

- **Outgoing name ID format:** Transient Identifier

11. Click **Apply** and then click **OK**.

12. From **AD FS 2.0 > Trust Relationships > Relying Party Trust**, double click the relying party trust file you created earlier.

13. From the "IWSaaS Properties" dialog box, click the "Advanced" tab.

14. For **Secure hash algorithm**, specify **SHA1** and then click **OK**.

15. Go to **AD FS 2.0 > Service > Certificates**

16. Open the certificate under "Token-signing".

17. From the "Certificate" dialog box, click **Copy to File** from the "Details" tab.

18. Provide information for each screen in the "Certificate Export" wizard.

    - From the "Export File Format" window, select **Base-64 encoded X.509 (.CER)** and then click **Next**.

    - From the "File to Export" window, locate the desired certificate file and then click **Next**.

    - At the "The export was successful" message, click **OK** to have the token signing certificate saved to the file.

19. Choose **Start > Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.

20. Go to **[Server] > Sites > Default Web Site > adfs > ls**.

21. From middle panel, double click the **Authentication** icon under "IIS".

22. From the "Authentication" panel, select **Windows Authentication** and then click **Advanced Settings** from the right panel.

23. From the "Advanced Settings" dialog box, select **Off** from **Extended Protection** and then click **OK**.

Note

Steps 18 - 22 resolve the issue Chrome has when running on Windows 7, which results in popups appearing for username and password input, and user authentication fails.

Testing SAML Active Directory Authentication

Once you successfully configured the Sychronization Agent and SAML Server, and specified SAML as the user authentication method, you can logon to an IWSaaS proxy server to verify your setup.

Procedure

1. Clear the browser of all cookies and then restart the browser.
2. Configure your browser to the IWSaaS proxy server.

   Either use the PAC file method (see *PAC File on page 7*), or specify in the browser `proxy.iws.trendmicro.com:80` as the proxy.
3. Visit any website and IWSaaS will direct you to the IWSaaS logon page.
4. Specify an Active Directory accounts (format: `sAMAccountName@primarydomain` or the user's email address) and then click **Login**.

   The system redirects you to the authentication page of the SAML Server.
5. Specify your `sAMAccountName` and password.

   Note

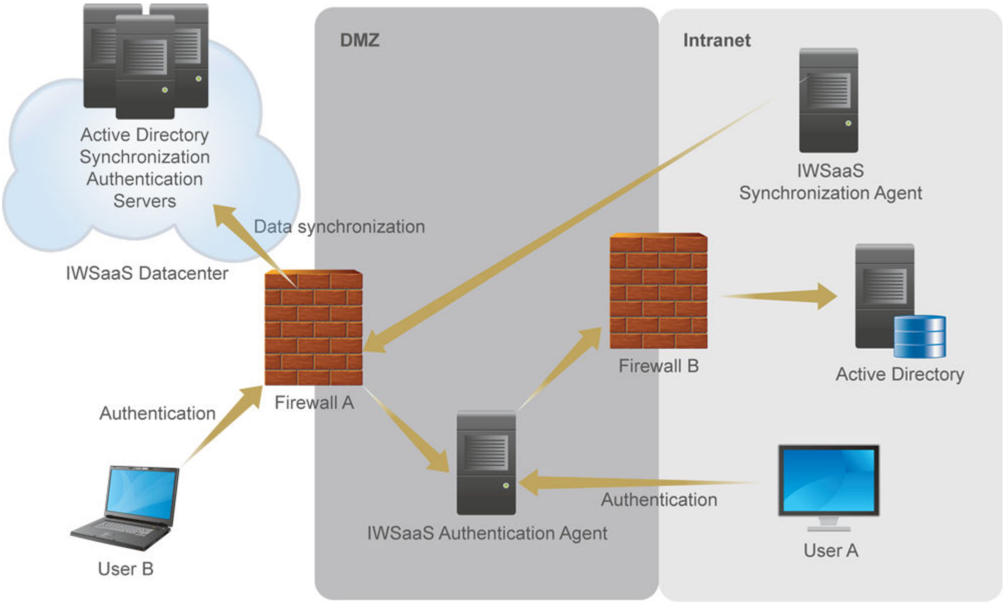
   If a user is using a computer that belongs to a domain configured in IWSaaS, then the user is not required to provide a password.

After the SAML Server verifies your account, you can visit the Internet safely.

Authenticating Users Using Agents

Use this method of user authentication if you do not have a SAML server, but still want the same level of security that SAML Authentication provides.

Specifying Ports for the Authentication Agent



Procedure

1. Install the IWSaaS Synchronization Agent in your Intranet.

   The Synchronization Agent connects to your Active Directory to sync user and group data with IWSaaS. The data transmits over the HTTPS protocol on port 443 and this outgoing port is usually open on Firewall A by default, as depicted in the graphic above.

2. Deploy the IWSaaS Authentication Agent in the DMZ.

3. On Firewall A, open incoming port 443 to allow any IP to connect to the IWSaaS Authentication Agent.

4. On Firewall B, open incoming port 389 (or 636 when SSL is enabled in the Active Directory) to allow IWSaaS Authentication Agent connect to the Active Directory.

Note

Putting the Authentication Agent in the DMZ allows user authentication regardless if they are inside the corporate network (User A) or outside of it (User B). But if you deploy the Authentication Agent in the Intranet, only User A--who is inside the corporate network, can authenticate and login to IWSaaS.

Source	Destination	Firewall settings
Intranet	IWSaaS services	Outbound port 443 on Firewall A (normally open)
Internet	IWSaaS Authentication Agent in DMZ	Inbound port 443 on Firewall A
IWSaaS Authentication Agent in DMZ	Active Directory Server	Inbound port 389 on Firewall B (or 636 when SSL is enabled in the Active Directory)

5. Deploy the IWSaaS Synchronization Agent to synchronize user and group data with IWSaaS.

   See *Configuring the Synchronization Agent on page 38*.

Specifying Agent Active Directory Authentication

Location: Administration > Users and Authentication > Active Directory

Procedure

1. Enable Active Directory and then click **Agent**.

2. Specify the **Authentication Agent URL address** so IWSaaS can locate and use the Authentication Agent to authenticate Active Directory users.

3. Click **Save**.

Configuring for Agent Active Directory Authentication

The Synchronization Agent and Authentication Agent must be configured in order to use Agent Active Directory Authentication.

For the Synchronization Agent, configure this agent as described in *Configuring the Synchronization Agent on page 38*, except select **Agent** as your athentication method.

Configuring the Authentication Agent

Before you begin

Prepare a serever on which to install the Authentication Agent.

Location: Administration > Users and Authentication > Active Directory

Procedure

1. Enable Active Directory and then click **Agent**.

2. Click **Download the Authentication Agent** to download the Authentication Agent installation package.

3. Copy the installation package to the server in your fixed IP addresses that you prepared for the Authentication Agent.

4. Launch the installation wizard and then follow the prompts.

5. From the "Trend Micro Authentication Agent Config Tool" dialog box, specify all the necessary information.

    - **Auth Agent Web Port** is the port where the Authentication Agent operates. If you change the default 443 port, then also change the firewall setting to give incoming traffic access to the new port for the Authentication Agent.

- From the "LDAP Info" area, specify the Active Directory server information so that the IWSaaS Authentication Agent can connect to the Active Directory.

6. Click **Apply**.

Manually Deploying Customized Certificates for the Authentication Agent

You will need to manually deploy customized certificates for the Authentication Agent if you have your own URL and therefore your own SSL certificates.

Procedure

1. Stop the Trend Micro IWSaaS Apache service.

   a. Go to **Start > Control Panel > Administrative Tools > Services**

   b. Select the **Trend Micro IWSaaS Apache** service and then stop the service.

2. Copy the customized certificates.

   a. Open the IWSaaS Authentication Agent installation folder.

   `c:\Program Files\Trend Micro\InterScan Web Security as a Service\AuthenticationAgent`

   b. In the `AuthenticationAgent` sub-folder, `crt\`, copy the customized files.

   The certificate and private key are the customized files and have the following format:

   - Certificate file: `example.com.crt`
   - Certificate chain file: `example.com.chain.crt` (file is only needed if `example.com.crt` does not contain the certificate chain)
   - Private key: `example.com.key`

3. Modify the configuration.

   a. Go to the IWSaaS Authentication Agent installation folder, and open the `Apache-20\conf\extra` sub-folder.

b. Open the configuration file, `httpd-vhosts.conf`, and then update the following lines:

- `SSLCertificateFile ../crt/idpWebServer.crt` to `SSLCertificateFile ../crt/example.com.crt`
- Change `SSLCertificateChainFile ../crt/idpWebServer.crt` to `SSLCertificateChainFile ../crt/example.com.chain.crt` if `example.com.crt` does not contain the certificate chain. Otherwise, remove the following line from configuration file: `SSLCertificateChainFile ../crt/idpWebServer.crt`.
- `SSLCertificateKeyFile ../crt/idpWebServer.key` to `SSLCertificateKeyFile ../crt/example.com.key`

c. Save and close the configuration file.

4. Start the **Trend Micro IWSaaS Apache** service.

a. Go to **Start > Control Panel > Administrative Tools > Services**.

b. Start the **Trend Micro IWSaaS Apache** service.

Right click **Trend Micro IWSaaS Apache** and then select **Start** in the pop up menu.

Testing Agent Active Directory Authentication

Once you successfully configured the Sychronization Agent and Authentication Agent, and specified Authentication Agent as the user authentication method, you can logon to an IWSaaS proxy server to verify your setup.

Procedure

1. Clear the browser of all cookies and then restart the browser.

2. Configure your browser to the IWSaaS proxy server.

Either use the PAC file method (see *PAC File on page 7*), or specify in the browser `proxy.iws.trendmicro.com:80` as the proxy.

3. Visit any website and IWSaaS will direct you to the IWSaaS login page.

4. Specify an Active Directory account (format: `sAMAccountName@primarydomain` or user's email address) and then click **Login**.

The system redirects you to the authentication page of the Authentication Agent.

5. Specify your password.

Implementing Policies

Once account provisioning is complete, configure IWSaaS with different security settings for different users or groups on the network. In this way, security and access policies are customized for business needs, such as handling potentially malicious code or viewing certain categories of web content.

Policy Precedence

IWSaaS gives certain policies priority over others. The order of precedence is as follows:

1. Approved List

2. Blocked List

3. HTTPS Decryption

4. Application Control

5. URL Filtering

6. Advanced Threat (crimeware, malware, grayware)

7. Web Reputation Service (WRS)

8. Anti-Malware

Policy Precedence Rules

- IWSaaS applies security and access policies to HTTP requests and decrypted HTTPS traffic. IWSaaS treats HTTPS traffic as HTTP traffic when it is decrypted. If HTTPS traffic is not decrypted, IWSaaS does not apply policies to this traffic.
- If a policy blocks a URL, IWSaaS will not apply any policies that take precedence next.
- If a URL is included in the Approved List, IWSaaS applies no policies to this URL.
- If the HTTPS Decryption policy is disabled, IWSaaS tunnels all HTTPS traffic without applying the Application Control, URL Filtering, WRS, Advanced Threat, and Anti-Malware policies.
- If an HTTPS URL is part of the Exception List of the HTTPS Decryption policy, IWSaaS tunnels this URL without applying the Application Control, URL Filtering, WRS, Advanced Threat, and Anti-Malware policies.
- If the Application Control policy blocks an offending URL, then IWSaaS does not apply the URL Filtering policy.
- IWSaaS caches the WRS score of a URL. If the Anti-Malware policy blocks a URL, IWSaaS decreases the cached WRS score of the URL. Therefore, in the future the WRS policy could block this URL.

Roaming Users and the HTTPS Decryption Policy

When a roaming user (a person accessing IWSaaS from an unregistered gateway) makes an HTTPS request using IWSaaS for the first time, IWSaaS decrypts the traffic to authenticate the client. After authentication, IWSaaS retrieves and applies the client's policies.

Important

If the HTTPS policy is enabled, import the IWSaaS root certificate into client browsers. For details, see *Deploying Certificates on page 72*.

Note

- If the HTTPS domain is in the URL Exception List or global Approved URLs List, IWSaaS does not apply any policies to the client's traffic.
  - To modify the URL Exception List, go to **Administration** > **Service Deployment** > **HTTPS/SSL Policies** and then select a URL category or add a URL to exclude sites from scan.
  - To modify the Approved URLs, go to **Access Policies** > **Approved/Blocked URLs**.
- Any HTTPS domain in the Blocked URLs list will be blocked (as expected).
- Any HTTPS domain decrypted by IWSaaS that requests a client certificate will be blocked.
- To avoid traffic decryption when HTTPS decryption is disabled, the client IP and user credentials are mapped the first time that the roaming user makes an HTTP request and authenticates to IWSaaS.

Security Policies

Security policies protect against malware, web reputation, and other threats.

Changing Anti-Malware Policies

Location: **Security Policies** > **Anti-Malware Protection**

Procedure

1. Enable Anti-Malware Protection.
2. Under “File Extension Exceptions”, specify the file extensions to be excluded from scans.
3. Under “Action”, specify what action IWSaaS should take against certain file types.
4. Click **Save**.

Using Web Reputation

Location: **Security Policies** > **Advanced Web Protection** > **Web Reputation**

Procedure

1. Enable Web Reputation Protection.
2. Under "Sensitivity Level", specify the sensitivity level.
3. Under "Action", specify what action IWSaaS should take against sites with malicious content.
4. Click **Save**.

Setting Advanced Protection

Specify the settings for a variety of crimeware, malware, and grayware threats.

Note

Advanced Protection is only available with an Advanced Full license.

Location: **Security Policies** > **Advanced Web Protection** > **Advanced Protection**

Procedure

1. Enable Advanced Protection.
2. Under "Action", specify the action IWSaaS should take against crimeware, malware, and grayware threats.
3. Click **Save**.

Access Policies

Policies that control website access and application controls.

Configuring URL Filtering

Location: **Access Policies** > **Manage URL Filtering Policies**

Procedure

1. Enable URL filtering.
2. Click **Add**.
3. Specify the policy name and enable the policy.
4. Under "User/User Group", configure URL filtering for any user or a specific user group.
5. Under "Gateway Locations", select whether to filter any gateway or choose a gateway from the list.
6. Under "URL Categories", select the types of content to filter.
7. Under "Scheduling", set when the policy is used.
8. Under "Action", specify what action IWSaaS should take for filtered content.
9. Click **Save**.

Tip

Click any policy name from the list to make modifications or select the policy and click **Delete** to remove.

Creating Custom URL Categories

URL categories are used in URL filtering to monitor or block content that can be grouped together, such as lifestyle or business sites.

Location: **Access Policies** > **URL Filtering Policies** > **Custom URL Categories**

Procedure

1. Click **Add**.
2. Provide a name for the URL category.
3. Specify each URL and click **Add**.
4. Once all URLs are added, click **Save**.

   Tip

   Click any custom category name from the list to make modifications or click **Delete** to remove.

5. To use the new custom category, do the following:
   a. Open a URL filtering policy.
   b. Under “URL Categories,” select **Use the following categories**.
   c. Select **Custom Categories**.
   d. Select the new custom category.

Controlling Applications

Applications like file transfer, instant messaging, peer-to-peer or audio/video are disruptive because they slow down the network, are a security risk, and can be a distraction to employees. Administrators can use IWSaaS to control which applications are allowed on the network.

Note

Application Control is only available with an Advanced Full License.

Location: **Access Policies** > **Application Control**

Procedure

1. Enable Controlling Applications.
2. Click **Add**.
3. Specify the policy name and enable the policy.
4. Under "User/User Group", control applications for any user or a specific user group.
5. Under "Gateway Locations", select whether to filter any gateway or choose a gateway from the list.
6. Under "Application Categories", select the types of applications to control.
7. Under "Scheduling", set when the policy is used.
8. Under "Action", specify what action IWSaaS should take against selected applications.
9. Click **Save**.

Tip

Click any policy name from the list to make modifications or select the policy and click **Delete** to remove a control.

Using Approved and Blocked Lists

Location: **Access Policies** > **Approved/Blocked URLs**

Procedure

1. To add approved URLs:
   a. Specify the URL and click **Add**.
   b. Click **Delete** to delete a URL from the list.
2. To add blocked URLs:

a. Specify the URL and click **Add**.

b. Click **Delete** to delete a URL from the list.

3. Click **Save**.

Enforcing Traffic to IWSaaS

After implementing the policies (Security and Access), you can configure your network configuration or client computers to enforce traffic flow to the IWSaaS proxy server.

The following table describes the options to enforce traffic to IWSaaS.

Options	Description	Pros	Cons
Proxy Chaining	If your company enforces traffic using a company proxy server, then configure your proxy server to point upstream to IWSaaS.	• Easy setup • Supported by most Web proxies • If your network forbids ports 80 and 443, then only the proxy server can access the Internet. Users cannot bypass this. • Guest users are protected.	Users not on a corporate network are not protected

Options	Description	Pros	Cons
Enforce PAC	Use GPO (Group Policy Object) to enforce the system proxy to the IWSaaS PAC file.	• Easy to deploy. • Supported by all major browsers. • Users are protected whether on or off the network. • If your network forbids port 80 and 443, then open port 8080. You can enforce all of the users to use IWSaaS using port 8080 in the PAC file. Users cannot bypass this.	• Users can manually change the proxy setting to **no proxy**, in order to bypass it. • Guest users are not protected
IWSaaS Enforcement Agent	Install the Enforcement Agent on client computers to enforce the traffic to the IWSaaS proxy.	• Easy to deploy. • Users are protected whether on or off the network.	• Only supports the Windows platform. • Guest users are not protected

Proxy Chaining

If your company has an existing proxy server and Internet traffic passes through this proxy, you can configure IWSaaS as the upstream proxy on your proxy server. This proxy chaining enables all of the current http(s) traffic to move through IWSaaS smoothly.

Enforcing Traffic Through the PAC File Using GPO

Use the GPO (Group Policy Object) to enforce the proxy auto-config (PAC) file (see *PAC File on page 7*).

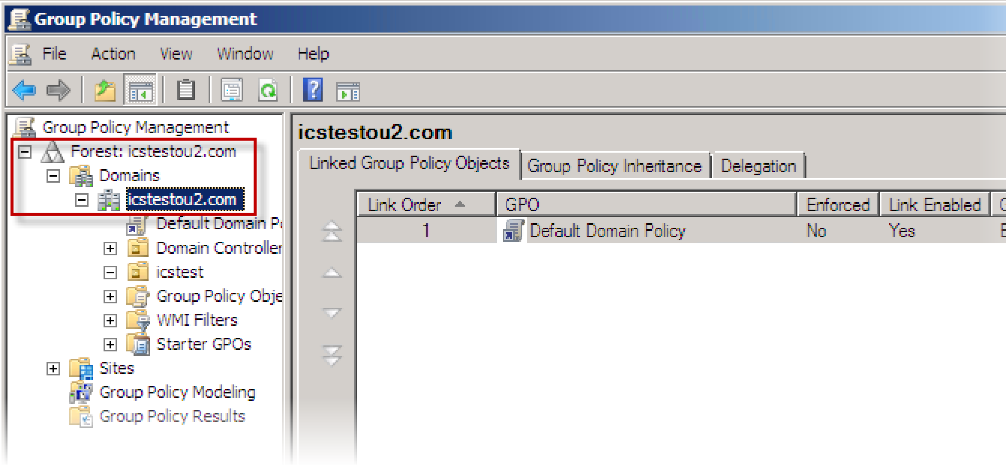
For Windows 2003:

1. Login to the Active Directory server as administrator.
2. Choose **Start > Administrative Tools > Active Directory Users and Computers** to open the **Active Directory Users and Computers** window and then click **Active Directory Users and Computers**.
3. From the center area, right click your domain and then select **Properties**.
4. From the **Properties** dialog box, click the **Group Policy** tab.
5. Click **New** to add a new GPO and then specify the GPO name.
6. Double click the newly created GPO.
7. From the **Group Policy Object Editor** window, choose **User Configuration > Windows Settings > Internet Explorer Maintenance > Connection**.
8. From the center area, double click **Automatic Browser Configuration**.
9. From the **Automatic Browser Configuration** dialog box, select the **Enable Automatic Configuration** check box.
10. Specify the frequency minutes and Auto-proxy URL.

    This URL can be the default PAC URL, the user created PAC URL on the IWSaaS web console, or the internal address of your PAC file.
11. Click **OK**.

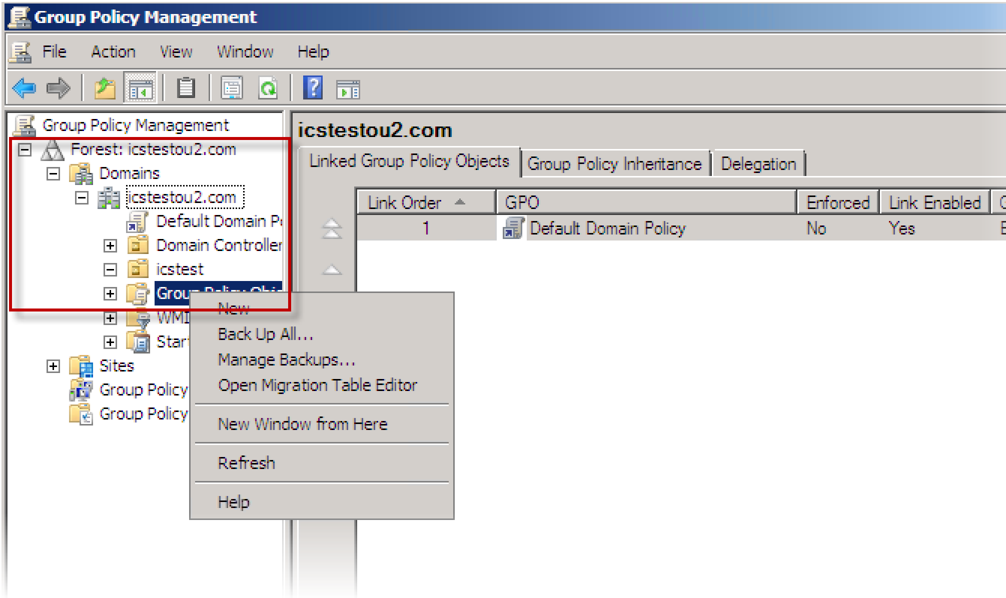
For Windows 2008:

1. Login to Active Directory as an administrator.
2. Choose **Start > Administrative Tools > Group Policy Management**.
3. From the **Group Policy Management** window, choose **Forest: [your forest] > Domains > [your domain]**..



Link Order	GPO	Enforced	Link Enabled
1	Default Domain Policy	No	Yes

4. Right click on **Group Policy Objects** of your domain to add a new GPO.

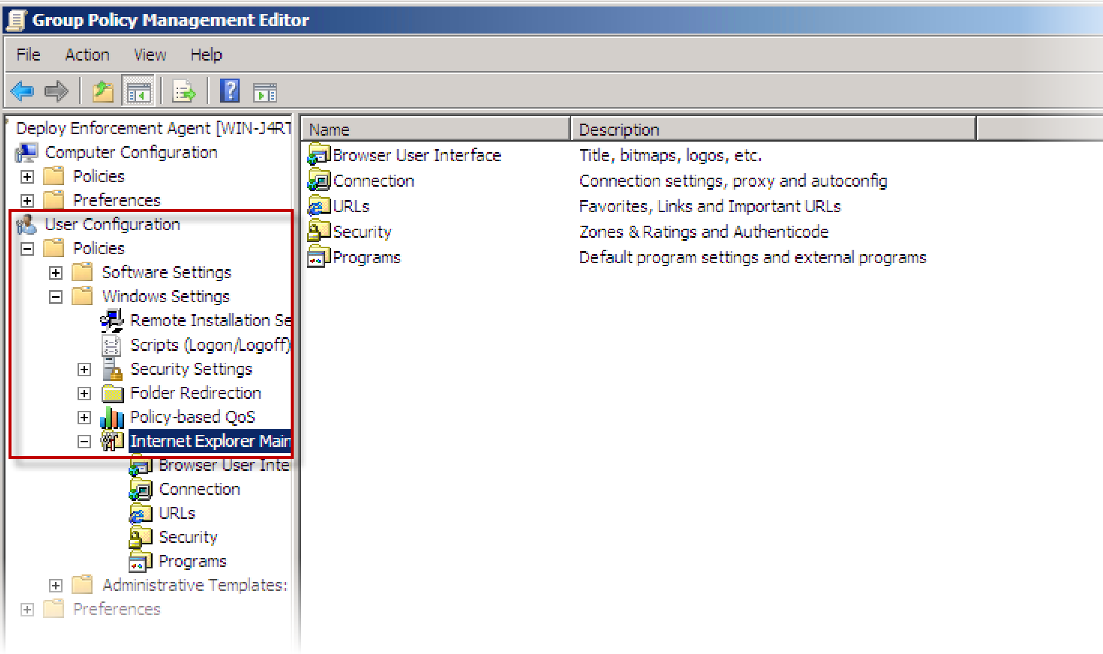


Link Order	GPO	Enforced	Link Enabled
1	Default Domain Policy	No	Yes

5. From the **New GPO** dialog box, specify the GPO name and then click **OK**.

6. Right click on the newly added GPO and then click **Edit**.

7. From the **Group Policy Management Editor** window, choose **User Configuration > Policies > Windows Settings > Internet Explorer Maintenance > Connection**.



Name	Description
Browser User Interface	Title, bitmaps, logos, etc.
Connection	Connection settings, proxy and autoconfig
URLs	Favorites, Links and Important URLs
Security	Zones & Ratings and Authenticode
Programs	Default program settings and external programs

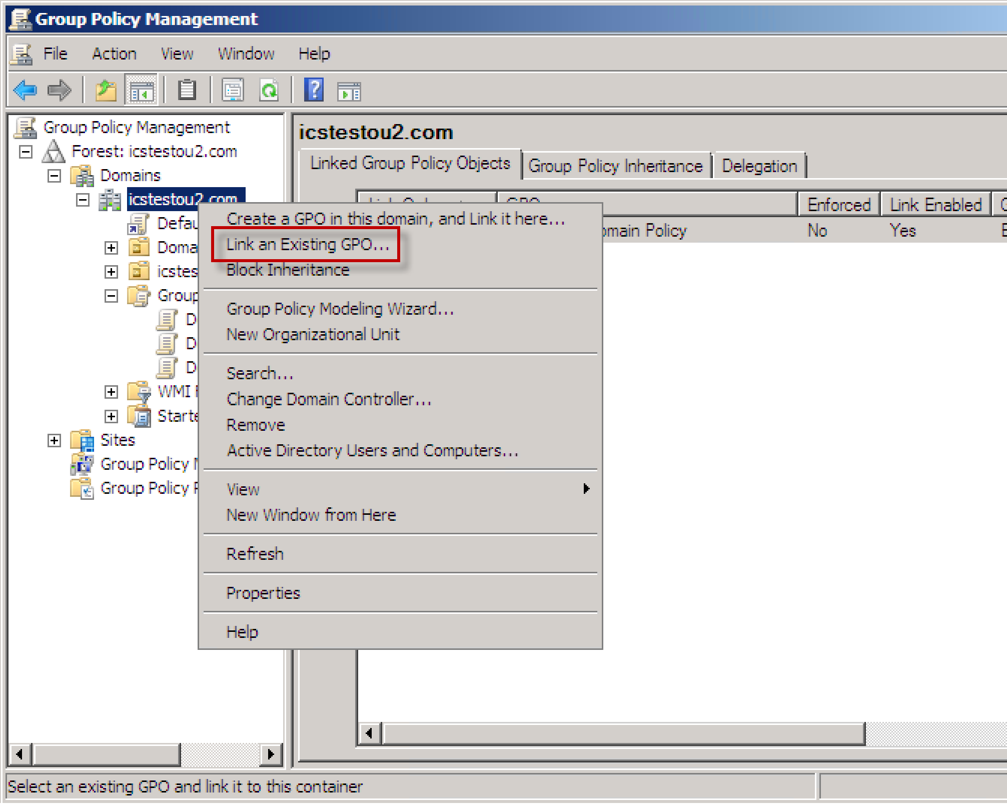
8. From the center area, double click **Automatic Browser Configuration**.

9. Specify the frequency minutes and Auto-proxy URL.

   This URL can be the default PAC URL, the user created PAC URL on the IWSaaS web console, or the internal address of your PAC file.

10. From the **Automatic Browser Configuration** dialog box, click **OK**.

11. Right click on your domain or organization unit and then click **Link an Existing GPO**.



Select an existing GPO and link it to this container

12. From the **Select GPO** dialog box, select the newly created GPO and then click **OK**.

Enforcing Traffic Through the Enforcement Agent

Besides the Proxy Chaining and Enforce PAC traffic enforcement options, IWSaaS traffic enforcement can also be achieved using the Enforcement Agent. This agent is installed to client machines (Windows XP, Windows7, Windows 8, Windows 8.1) to enforce the traffic to the IWSaaS server.

The Enforcement Agent does the following:

- Ensures that the system proxy is set to the specified PAC file. The Enforcement Agent will change the system proxy back if it is changed.
- Ensures that the Firefox proxy settings are not changed. (Keep the Connection Settings option, **Use system proxy settings** selected.). If these settings are changed, the Enforcement Agent notifies the user to change them back. If the settings are not changed back after five minutes, Firefox closes.
- Stops processes configured by an administrator. The Enforcement Agent by default will not close any processes.

Customizing and Downloading the Installation Package

Customize and download the Enforcement Agent installation package from the IWSaaS web console.

Procedure

1. Login to the IWSaaS web console.
2. Go to page **Administration > Enforcement Agent**.
3. Select **Customize** and then complete any necessary fields.
4. Click **Download**.
5. Unzip the installation file to a network location accessible to all domain computers.

   Example: `\\GPO_controller_server\shared_folder\`

   Note

   The domain computers and domain users should be able to access the share folder.

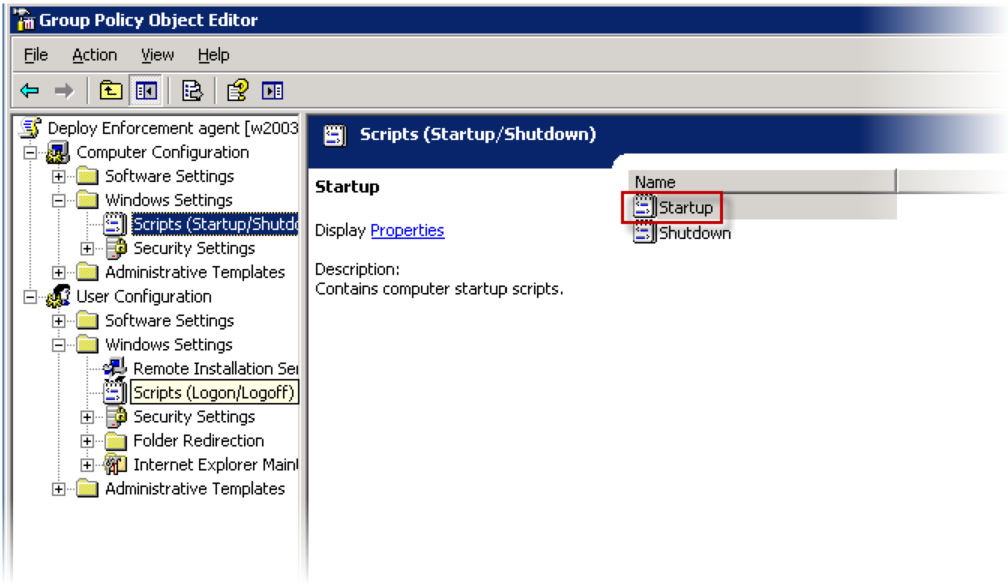
Deploying the Enforcement Agent to Client Computers

Deploying Using GPO

Deploy the Enforcement Agent installation package to multiple computers using GPO (Group Policy Object).

Procedure

1. Login to the Active Directory server as an administrator.
2. Choose **Start > Administrative Tools > Active Directory Users and Computers** to open the **Active Directory Users and Computers** window.
3. Click **Active Directory Users and Computers**.
4. From the **Active Directory Users and Computers** console tree, right click your domain, and then click **Properties**.
5. In the **Properties** window, click **Group Policy** and then click **New** to add a new GPO (Group Policy Object).
6. Enter the name of the new GPO.
7. Open the newly created GPO file for editing.
8. Choose **Computer Configuration > Windows Settings > Scripts (Startup/ Shutdown)** (for Windows 7 and Windows 8) or choose **User Configuration > Windows Settings > Scripts (Logon/Logoff)** (for Windows XP).
9. Double click **Startup** or **Logon**.



Startup

Display Properties

Description:
Contains computer startup scripts.

10. In **Startup Properties** or **Logon Properties**window, click **Add**.

11. Enter the path of the IWSaaS Enforcement Agent (`\\GPO_controller server\shared_folder\enforcement_agent\SlientSetup.bat`) and then click **OK**.

12. From the **Startup Properties** or **Logon Properties** window, click **Apply** and then **OK**.

    The Enforcement Agent installs when client computers restart or the domain users login to the client computers.

Deploying to Individual Computers

Procedure

1. Using the installation wizard, install the installation package on individual computers.

   a. Navigate to the `Trend Micro IWSaaS Enforce Agent.exe` and double click this file.

   b. Click **Next** in the **Welcome** dialog box.

   c. Accept the license agreement.

   d. Click **Next** to begin the installation.

   e. Click **Finish** after the installation completes.

2. Use `SilentSetup.bat` to automatically install the Enforcement Agent on a computer.

   a. Navigate to the **Trend Micro IWSaaS Enforce Agent** folder and run the `SilentSetup.bat` file.

Using the Enforcement Agent

After the Enforcement Agent is installed, the user is required to login to IWSaaS before accessing the Internet. The Enforcement Agent is represented in the system tray with an icon, which provides certain functions.

Logging in to IWSaaS

After the Enforcement Agent is installed on a computer, the user must login to IWSaaS as follows:

Procedure

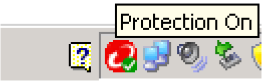
1. Browse to any external site.

2. Authenticate when prompted by the **Login** window.

3. Enter your user name and password and then click **Login**.

Using the Enforcement Agent Icon

After the Enforcement Agent is installed on a computer, the agent is represented by an icon in the system tray.



Users can right click the icon to disable the protection.

Select **Disable Protection** to temporarily bypass IWSaaS. Users must enter the password provided by their administrator.

To re-activate the Enforcement Agent, right click the icon and select **Enable Protection**. No password is required to re-enable the agent.

Note

If the option, **Display icon in system tray** is not selected when customizing the Enforcement Agent installation package, the icon will not appear in the system tray.

Upgrading the Enforcement Agent Package

Procedure

1. Use the new, downloaded and unzipped package to replace the original package.

   If you place the new package in a location other than the original location, you need to update the GPO to run the `SilentSetup.exe` of new package.

   The new package will be installed after you restart Windows 7 or Windows 8, or login as a domain user in Windows XP.

2. Upgrade the installation package on individual computers by either running the `Trend Micro IWSaaS Enforce Agent.exe` or `SilentSetup.bat`.

   Each of these files are located in the downloaded installation package.

Uninstalling the Enforcement Agent

Procedure

1. Choose **Start > Control Panel**.
2. In the **Control Panel** window, select the option for installing/uninstalling programs.

   For Windows XP, click **Add/Remove Programs**. In Windows 7, click **Programs and Features**.
3. From the program list, select **TrendMicro Enforcement Agent** and then click **Uninstall**.
4. When you are promoted for a password, enter the uninstall password that was specified when creating the installation package.

   If you are using the default package, enter **trendmicro**.

Analysis and Reporting

Reports are generated from log information in the database. For further analysis, export log data as a comma-separated value (CSV) file.

Log data is stored for three months.

Analyzing Logs

Location: **Analysis & Reports** > **Log Analysis**

Procedure

1. Select values in relevant fields to specify which log attributes to filter.

2. Click **Show Logs**.

Scheduling Reports

Location: **Analysis & Reports** > **Reports**

Procedure

1. Click **Add**.
2. Type a name and description for the report, and then click **On** to enable the report.
3. Under "Report Settings", specify a date range, gateway locations, frequency, format, and email recipients.
4. Under "Report Types", choose the type of report to run.
5. Click **Save**.

> **Note**
>
> To run an on-demand report, open Reports and click **Run** under the **Generated Frequency** column.

Testing Connectivity and Performance

Testing Connectivity with a Browser

Procedure

1. Set up the end user account.
2. Decide the traffic forwarding method, and use a test machine to connect to IWSaaS by this method.
3. Browse any website.

Connectivity with IWSaaS is working when the IWSaaS end-user portal logon displays.

4. Type the credentials used for this end user account to verify their account setup.

Testing Connectivity with the Diagnostic Tool

IWSaaS will not prompt a user to log on if the credentials have been provided within the last 2 weeks (14 days). In this case, the diagnostic tool is useful for testing. The user should already have an account and has already logged on successfully before.

Procedure

1. Open a web browser and go to http://diagnose.iws.trendmicro.com.

   IWSaaS is working properly when the connection status for IWSaaS is "Yes".

Testing Policies

It can take up to one (1) minute for a policy to take effect once it is set in the Management Console.

Procedure

1. Configure the policy (the action is blocked) and ensure that it is enabled.
2. Navigate to a URL or run an application that fits policy limitations.
3. When prompted by IWSaaS, log on with a user account that is managed by the policy.
   - If the policy is working, the browser will deny access and display event details.
   - If the policy is not working, return to the policy and check the configuration. Also, verify that the browser is connecting through a proxy to the cloud.

If the site is allowed or monitored by a policy, then the site loads; otherwise, a message appears notifying that the site is blocked.

Improving How Internet Explorer Displays Content

Internet Explorer has some security features that may block images or other content. By default, sites in the **Internet** and **Restricted sites** zones are restricted while sites in the **Local intranet** and **Trusted sites** zones are not. For security reasons, sites inside and outside of **Protected Mode** cannot share cookies, which causes some sites to display content incorrectly.

Modify the network zone settings and enable **Protected Mode** for all zones to improve how content is displayed when using IWSaaS.

Procedure

1. Go to **Tools** > **Internet Options** and open the **Security** tab.

   The **Security** tab appears.

2. For every zone, select **Enable Protected Mode** to enable **Protected Mode**.

   Sites in different zones can now share cookies.

Accessing Internal Sites

IWSaaS run outside the enterprise network in a cloud environment and may not have access to an enterprise's internal sites. Administrators can configure IWSaaS to allow end users access to internal sites.

Procedure

1. If using direct proxy server, modify the browser settings to include the restricted internal sites:

   - **Internet Explorer**

Location: **Tools** > **Internet Options** > **Connections**

a. Click **LAN Settings**.

b. Under "Proxy server," click **Advanced**.

c. Under "Exceptions," specify the local sites to access.

- **Google Chrome**

  a. Click on the wrench icon located at the top-right.

  b. Go to **Settings** > **Show advanced settings...** > **Change proxy settings...**.

  The **Internet Properties** window appears.

  c. Click **LAN Settings**.

  d. Under "Proxy server," click **Advanced**.

  e. Under "Exceptions," specify the local sites to access.

- **Mozilla Firefox**

  Location: **Tools** > **Options** > **Advanced**

  a. Click the **Network** tab.

  b. Under "No Proxy for:," specify the local sites to access.

2. If using a PAC file, open the IWSaaS Management Console and download the default PAC file. For instructions on downloading the default PAC file, see *Downloading the Default PAC File on page 7*.

a. Open the PAC file and make one of the following changes:

- Modify the PAC file to do DNS queries first and to judge whether the IP address is internal IP or external. If it is internal IP, do not forward the request to IWSaaS. To do this, change the value of `DNSNeedResolve` to `TRUE`. For example:

```
var DNSNeedResolve = true;
```

- Modify the PAC file and specify the URL of internal sites to allow using the SkipHosts variable with the following code:

```
var SkipHosts = ["<internal IP/hostname>",
                 "<internal IP/hostname>"];
for (var i in SkipHosts) {
     if (shExpMatch(host, SkipHosts[i])) {
        return 'DIRECT';
     }
}
```

Note

Do not change the order of variables or other content within the PAC file.

Deploying Certificates

Location: **Administration** > **Service Deployment** > **HTTPS/SSL policies**

Procedure

1. Scroll to the bottom of the screen and click **Download and install an SSL certificate for client devices**.
2. Select **Save File** and click **OK**.

   The file is saved in the browser's default download location with the file name `default_ca_cert.cer`.

Deploying to Internet Explorer and Chrome

Procedure

1. Open `default_ca_cert.cer`.

2. Click **Install Certificate**.

   The Certificate Import Wizard opens.

3. Click **Next**.

4. Select **Place all certificates in the following store** and click **Browse**.

5. Select **Trusted Root Certification Authorities** and click **OK**.

6. Click **Next**.

7. Click **Finish**.

Deploying to Firefox

Location: **Tools** > **Options** > **Advanced** > **Encryption**

Procedure

1. Click **View Certificates** and select **Authorities**.

   Note

   In Firefox, the CA cannot be imported to both the server and authorities. If the CA was imported to the server, delete it first.

2. Click **Import**.

3. Navigate to the download folder and select the `default_ca_cert.cer` file.

4. Select **Trust this CA to identify websites** and then click **OK**.

TREND MICRO INCORPORATED
10101 North De Anza Blvd. Cupertino, CA., 95014, USA
Tel:+1(408)257-1500/1-800 228-5651 Fax:+1(408)257-2003 info@trendmicro.com

www.trendmicro.com

Item Code: APEM16253/131223