Web Security Service

Authentication Guide

Revision: NOV.07.2020

Symantec™
A Division of Broadcom

Copyrights

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

Symantec WSS: Authentication Deployment Guide

The Symantec Web Security Service solutions provide real-time protection against web-borne threats. As a cloud-based product, the Web Security Service leverages Symantec's proven security technology, including the WebPulse™ cloud community.

With extensive web application controls and detailed reporting features, IT administrators can use the Web Security Service to create and enforce granular policies that are applied to all covered users, including fixed locations and roaming users.

Most connectivity methods require an authentication solution, which provides the user and group affiliation information required for reporting and pre-traffic policy creation.

- One main option is the integration of the Symantec Auth Connector with your Active Directory (AD) deployment;
- The second method is integration of your existing Security Assertion Markup Language (SAML) deployment.

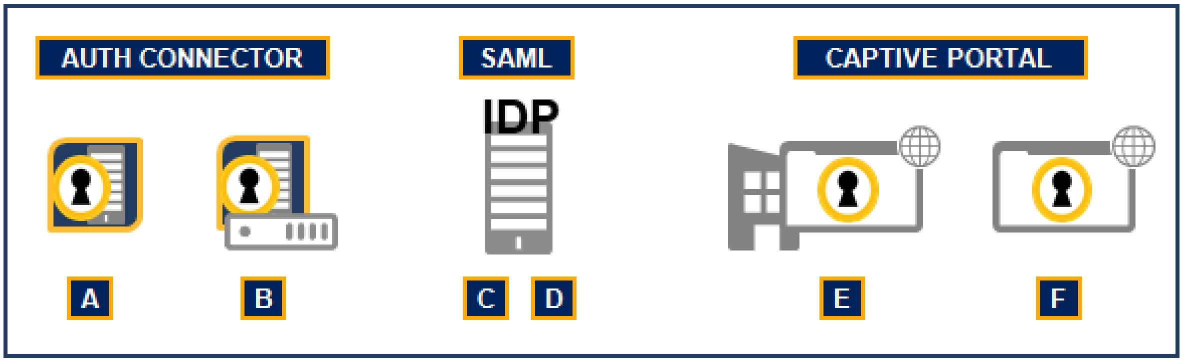
Table Of Contents

About User Authentication

User identification is a core component for all security policies. After obtaining the identity, the Web Security Service knows how to authorize who can do what from where to where.

Authentication Method Summaries

The WSS supports multiple connectivity methods (how employees have traffic routed to the WSS); likewise, it supports multiple authentication methods. The connectivity method can dictate which auth method is best or supported.



A—Auth Connector–A WSS-specific agent that you obtain from your WSS portal and install on an Active Directory member server. The Domain Controller Query (DCQ) instructs the Auth Connector to query all the domain controllers in your AD to identify users by their IP address when they log on. Also required for mobile device enrollments.

B—Auth Connector with ACLogon–An option for Firewall/VPN connectivity methods only. For very large enterprises with many domain controllers spread out across locations, the DCQ method might create scalability issues; some user logons might be missed because the domain controllers cannot respond fast enough. The alternative is the ACLogon App made available to each client system.

C—SAML with AD FS–The WSS provides native support with Microsoft® Active Directory Federation Services (AD FS) 2.0.

D—SAML with Third-Party–If you already have a SAML authorization method deployed, the WSS is compatible with several major third-party Identity Providers (IdP). You can also use the Auth Connector as an IdP, which allows for Symantec Single Sign On (SSO).

E—Captive Portal–Enforces a challenge-based authentication credential dialog to users each time they open a web browser.

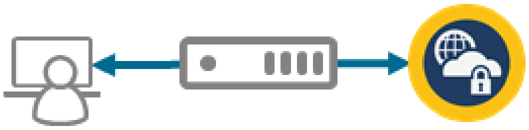
F—Roaming Captive Portal–A captive portal method for roaming/mobile users.

Depending on the how many WSS connectivity methods your enterprise employs, you might require multiple methods.

Authentication Methods by Connectivity

The methods used to route employee web traffic to the WSS dictates which authentication methods are available.

Firewall/VPN/IPsec



Supported Authentication Methods

- Auth Connector and DCQ
- Auth Connector and ACLogon

  The WSS returns web-form challenge and credentials pass through the Auth Connector for validation.

- SAML (IP or Surrogate Cookie)

  The WSS redirects to the SAML IdP for authentication; the returned assertion provides group-membership.

- Captive Portal (forms-based)

Deployment Notes

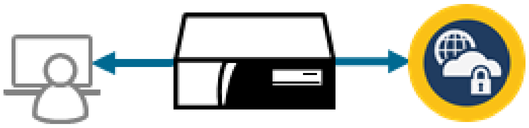
The Firewall/VPN/IPsec connectivity method requires an authentication method.

- You can deploy the Auth Connector, integrate with your existing SAML implementation, or use a hybrid (SAML with Auth Connector as the IdP).
- If you deploy a third-party SAML solution, Symantec recommends that you consider deploying the Auth Connector as a backup method or as a method to support roaming (SEP/WSS Agent) connections.
- These methods also provide the option to enable Captive Portal, which adds a form-based authentication challenge and the ability to set surrogate types and refresh times per location.
- This authentication method also applies to the Explicit Over IPsec connectivity method.

Is the original client source IP available?

- Yes.

Proxy Forwarding



Authentication is managed from the premises proxy, which communicates user and group affiliations in HTTP headers to the WSS.

Supported Authentication Methods

- Auth Connector and DCQ
- Auth Connector and ACLogon

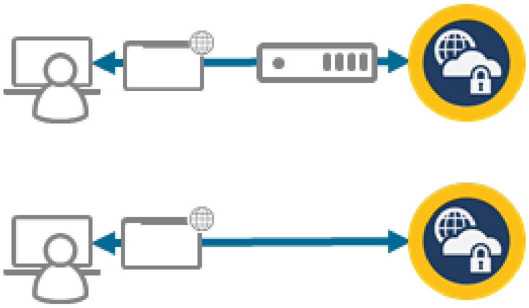
Deployment Notes

- Authentication occurs through supported authentication realms on the local proxy appliance.
- The WSS supports proxy-based authentication methods. The proxy validates groups of interest, which are required for access to the WSS. The gateway proxy adds user (BC_AUTH_USER) and group (BC_AUTH_GROUP) information to the forwarded request.
- The Auth Connector is required to obtain the user and groups from Active Directory to allow for policy creation.
- If you do not deploy the Auth Connector, you can define policy per-user after the WSS receives traffic from that user. However, Symantec does not recommend this security strategy.

Is the original client source IP available?

- Yes (XFF).

Explicit Proxy



There are multiple ways to configure explicit proxy connectivity to the WSS Agent.

Supported Authentication Methods–Fixed Location

You can configure a Fixed Location; for example, all client systems at a small branch have a PAC file that routes internet-bound traffic through an egress device with a static IP address. User logs in; however, the WSS believes the IP address of the gateway device, routed to by the PAC file, is the requester. As the designated explicit proxy location configured in the service, this IP address is granted access to the service. Without the Captive Portal (known locations) or Roaming Captive Portal (unknown locations) option enabled, no user/group names are available for reporting or policy creation.

- Captive Portal
- Auth Connector and DCQ
- Auth Connector and ACLogon

  The WSS returns web-form challenge and credentials pass through the Auth Connector for validation.

- SAML (Cookie Surrogate)

  The WSS redirects to the SAML IdP for authentication; the returned assertion provides group-membership.

Supported Authentication Methods–Unknown Location

You can distribute PAC files to clients; the PAC file forces the browser to send traffic to the WSS.

- Roaming Captive Portal
- Auth Connector and DCQ
- Auth Connector and ACLogon

Deployment Notes

- A user logs in; however, the WSS believes the IP address of the gateway device, routed by the PAC file, is the requester. As the designated explicit proxy location configured in the service, this IP address is granted access to the service. Without the Captive Portal (fixed locations) or Roaming Captive Portal (unknown locations) option enabled, no user/group names are available for reporting or policy creation.

- Captive Portal is required for pre-traffic policy; if enabled you must also deploy the Auth Connector.

- See SEP section for more information.

Is the original client source IP available?

- No.

SEP

As with Explicit Proxy, clients with Symantec Endpoint Protection (SEP) installed are routed to the WSS through a PAC file configuration.

Supported Authentication Methods—Fixed Location

- Auth Connector and DCQ
- Auth Connector and ACLogon
- SAML
- Captive Portal

Supported Authentication Methods—Unknown Location

- Auth Connector and DCQ
- Auth Connector and ACLogon
- WSS-SEP-WTR and WSS-SEP-NTR with Seamless Identification (recommended)
- SEP with Seamless Identification and Roaming SAML (recommended)
- Captive Portal

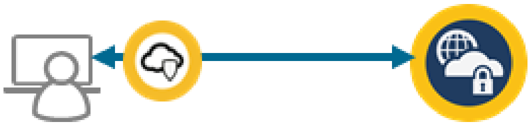
Deployment Notes

- The SEP solution has various authentication considerations.
- Identification: SEP returns the logged-in username. If the SEP agent is configured to use the WSS integration token, the agent adds a new header (`X-WSS-CLIENT-INFO`) to the HTTP Connect requests. The new header has the token that points the WSS to your tenant.
- AD and SAML: If identification fails, the WSS authenticates the user per authentication policy and it returns a unique *super cookie* value per user. SEP uses the new cookie value in a all HTTP Connect requests (`X-Bluecoat-Authorization`).

Is the original client source IP available?

- No.

WSS Agent



Supported Authentication Methods

- Auth Connector and DCQ
- Auth Connector and ACLogon
- Captive Portal in some versions.

Deployment Notes

- The WSS Agent sends cached user credentials (login) and the WSS user identification to the service. The access credential pop-up originates from the service. To have true challenge-based auth, enable the Captive Portal option.
- The Auth Connector is required if you plan to create custom policy based on your AD group names.
- When a client that has WSS Agent installed connects to corporate network, the agent goes into passive mode and the authentication occurs per the method configured on-premises.

Is the original client source IP available?

- No.

Mobile/Apps

The WSS supports connections from various mobile and app-based solutions.

Mobile Devices

SEP-Mobile (iOS) and Android (app store)

- Auth Connector and DCQ
- Auth Connector and ACLogon
- Roaming Captive Portal

Cloud Connect Defense

An app for Windows 10 endpoints.

- Auth Connector and DCQ
- Auth Connector and ACLogon

ChromeOS

Protect Chromebooks and any client running ChromeOS

- Auth Connector and DCQ
- Auth Connector and ACLogon
- Roaming Captive Portal

Deployment Notes

- The Auth Connector is required for mobile enrollment. When users enroll their mobile devices, they must enter their network credentials. The user identity must be validated for device enrollment, and the Auth Connector verifies the user credentials (username and password) in Active Directory.
- After enrollment, the user authentication and identity is provided by the certificate that is installed on the device following a successful enrollment.
- Furthermore, the Auth Connector is required if you plan to create custom policy based on your AD group names.

Is the original client source IP available?

- No.

Learn More About Authentication Methods

With the knowledge of how authentication is associated with each connectivity method, learn more about each authentication method.

- "About the Auth Connector Integration" on page 19
- "About SAML Authentication" on page 36
- "About Captive Portal Authentication" on page 99
- "About Roaming Captive Portal" on page 102

About the Auth Connector Integration

The Auth Connector is an authentication agent specific to the Web Security Service. Installed on an Active Directory member server (Windows Server 2008 R2 is the minimum), it performs the following.

- Forwards user and group information to the WSS to allow custom policy based on group and/or user names before they begin generating traffic; without it, you must wait until users/groups generate traffic and then re-actively create policy.
- Monitors log in and log out activity of domain users to build an IP-to-username-matrix.
- Informs the WSS of user log in and log out activities to keep the IP-to-user-matrix updated; or maintains this matrix itself on the Domain Controller and pushes the updated matrix regularly to the Cloud.
- Trust relationships between all Active Directories (AD) means that users spread across different domains remain susceptible to WSS policies.

This section describes the Auth Connector agent network footprint.

When Is The Auth Connector Required?

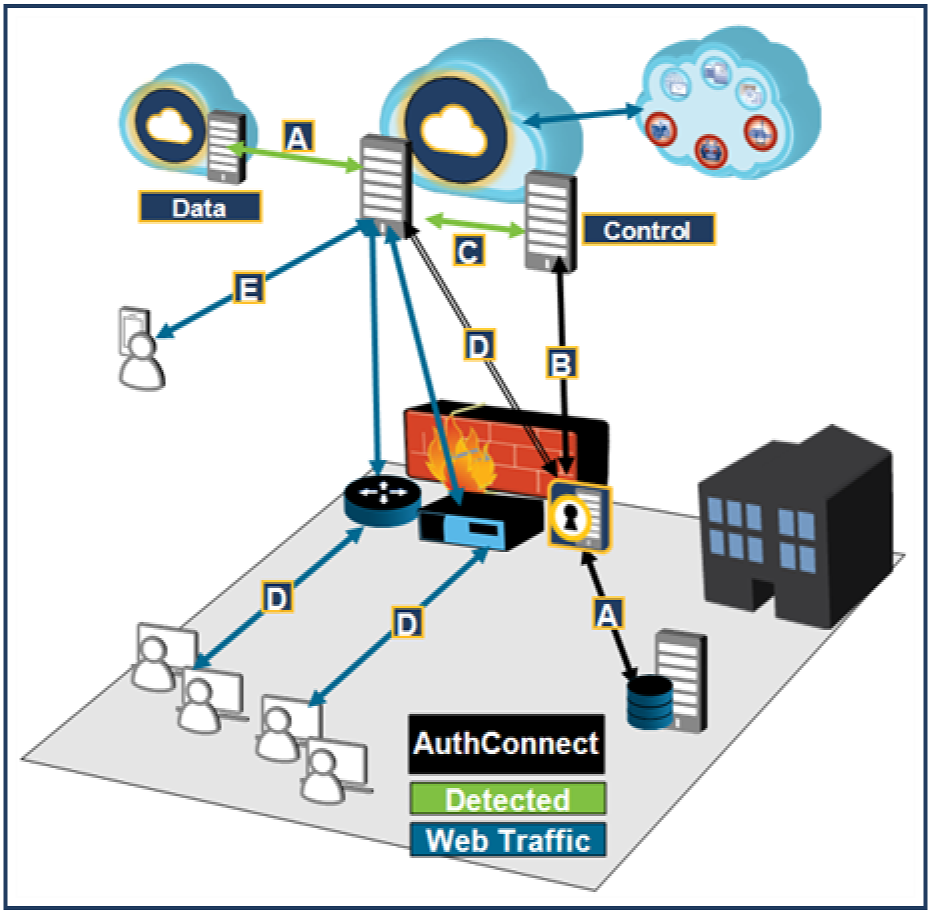
The Auth Connector is not always required for all connectivity methods. However, it is often required if you plan to create custom *pre-traffic* policy based on user and group names. This means you want policies in place before employees begin to perform internet requests. You might also deploy the Auth Connector as a backup method to a SAML implementation. To learn more about what methods support the Auth Connector, see "About User Authentication" on page 10.

The Auth Connector is *not* required for the following methods.

- SAML authentication method.
- SEP clients *unless* group-based policies are required.

With What Does the Auth Connector Communicate?

The Auth Connector comprises three communication footprints when completing a WSS transaction.



A—Active Directory Connection

When all Domain Controllers are discovered, the Auth Connector calls a Microsoft API that creates a NETBIOS connection to each Domain Controller. By default, the Auth Connector queries the following information to send to the WSS Control Pod.

- All Domain names that can be found
- All Users (SAM account names) from each domain
- All Security Groups from each domain
- All Members of each Security Group (for report filtering)

> **Tip:** You can modify a file to limit which users and groups are sent. This is described in the Auth Connector deployment procedure, which is linked at the end of this topic. Continue reading this section to obtain all of the important information.

If you are employing the Firewall/VPN connectivity method, there are two methods that create and maintain the IP-to-User map; select the method from the Auth Connector setup wizard:

- Domain Controller Query–This is the default method for all connectivity methods. The Domain Controller Query (DCQ) instructs the Auth Connector to query all the domain controllers in your AD to identify users by their IP address when they log on. Each domain controller is contacted every 10 seconds to ensure detection of all logged on users. The Auth Connector contacts the WSS Control Pod through `auth.threatpulse.net` on port 443 and transfers the AD users and group names.

  The WSS returns IPsec endpoint information to the Auth Connector.

- ACLogon Application–For very large enterprises with many domain controllers spread out across locations, the DCQ method might create scalability issues; some user log ins might be missed because the domain controllers cannot respond fast enough. The alternative is to obtain the ACLogon App and make it available to each client system. See the **About the ACLogon App** section below.

B—Portal Connection

The Auth Connector contacts the WSS Control Pod through `auth.threatpulse.net` on port 443 and transfers the AD users and group names.

C—IPsec Connections

If the Auth Connector detects IPsec connections, it receives instructions from the Control Pod as to what Data Pods (including other locations) it must connect, then initiates and establishes the SSL connections when it must resolve an IP address to a user name. IPsec tunnels are determined by a network location defined in the portal as a Firewall/VPN location.

D—User Connections

User web requests connect to the Data Pod. WSS queries the Auth Connector for user, group name, or IP address verification, checks policy, and either proceeds with or denies the request.

E—Mobile/Remote Connections

If the Auth Connector detects connectivity from an iOS (SEP-Mobile), Android App, or the WSS Agent, the following occurs.

- The Auth Connector receives instructions to which Data Pods (including other locations) it must connect.
- When it must resolve group membership for the users that are passed to the data pod, it initiates and establishes the SSL connections.

Failure to allow the Auth Connector to connect to the Data Pod’s auth IP prevents proper group membership identification, which causes group-based policies to fail. See "Reference: Authentication IP Addresses" on page 129.

About User/Group Memberships

By default, the Auth Connector retrieves all users and groups. The configuration topic describes how to limit which groups are retreived.

WSS responds quickly to new AD integrations. After that, WSS automatically performs an AD refresh once a week to poll for newly added users.

However, group memberships are identified through a different process. WSS re-queries group membership every 15 minutes (for active log-ins and users who are already authenticated).

- If you add a user to a new AD group and the user is *not* yet connected and authenticated, WSS identifies their group membership when they connect.
- If you add a user to a new AD group and the user *is* already authenticated, it can take nearly 15 minutes for WSS to re-query group membership.

To perform an on-demand retrieval of all user and group names, return to the **Identity > Auth Connector** page and click **Sync with AD**. Be advised that it might take up to 24 hours for you see the information in your portal. Avoid re-clicking the button more than once in a 24-hour period; doing so might overly clog the sync queue, causing slower results.

Auth Connector Ciphers

The following ciphers apply only to the connection between the Auth Connector and the WSS portal. They do not impact end-user web filtering or administrator access to the portal.

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
```

No action is required. The Auth Connector uses the underlying Windows OS for cipher negotiation. As of time of the publication, all recent versions of the Windows OS support these ciphers.

The best practice is keeping the Windows Server up-to-date with the latest patches and updates on the systems running the Auth Connector.

About the ACLogon App

The Logon Application option is for very large enterprises with many domain controllers spread out across locations. When first executed, the Logon Application authenticates to the Auth Connector over TCP port `80`. The user log on name and IP address of the workstation are sent. The TCP connection then terminates. Upon a network change (such as WiFi enabled or IP address change), the ACLogon re-connects to the Auth Connector to regain the information. If only the ACLogon is used, the DCQ is disabled.

You must download the application and make it available to each client system. This is described in the Deployment topic.

Deploy the Auth Connector

To create custom policy based on user and group names before those groups generate traffic, you must download the Auth Connector to at least one member server. The Auth Connector connects to the Web Security Service and provides the user/group information from the Active Directory (AD). See "About the Auth Connector Integration" on page 19, which provides more detail about the Auth Connector agent footprint

Technical Requirements

- Direct Internet Requirement–The Auth Connector must have a direct connection to the internet. Do not allow the Auth Connector to connect through the same IPsec tunnel that goes to the WSS.
- For a list of required ports, see https://knowledge.broadcom.com/external/article?legacyId=tech245943.
- The Auth Connector communicates with devices in the geographically located data centers. The Symantec Operations team maintains the following Knowledge Base article.

  https://knowledge.broadcom.com/external/article?legacyId=TECH240889

Member Servers Installation Prerequisites

- The installation requires the following.
  - The user performing the install is a member of the Domain to which the Auth Connector is installed.
  - The user has local administrative privileges on that machine.
- The following specifications are a current Symantec-recommended bench line.
  - Windows Server 2012 R2 OS.
  - Windows Server 2019–This platform might require additional configurations as described in the procedural section.
  - 8V CPUs.
  - 32GB of memory.
  - 1TB of disk space, which allows for I/O operations and any required debugging logs.

  > **Tip:** Only install the Auth Connector on a *read-only* server that does not require protection provided by the WSS. Connections to the service will work, but all users connected to that datapod location display in reports as **unauthenticated user**.

- On the member server, verify that the Authenticated Users read access is appropriate. This is specific to Windows 2019 but is also applicable to the earlier versions where admins applied deeper security; the Auth Connector cannot retrieve all of the required information to validate users and groups.

- The installation prompts for a username and password. These are configured as the account under which Auth Connector runs. The user name must be in the form `ADDOMAIN\user` or `user@dns_domainname.com`, where `ADDOMAIN` is the NetBios name of the active directory to which the server the Auth Connector is installed on as a member. The installation grants this user account the **Log on as a service** privilege.

  If the AD account password changes and the Auth Connector restarts, WSS cannot identify users until the password matches.

- The Auth Connector requires that a newer Entrust CA certificate `Entrust(2048)` be installed on the member server on which the Auth Connector runs. Verify this by browsing the Trusted Root Certification Authorities certificate list within the local machine store with `mmc.exe` and the certificates snap-in. If this Entrust certificated is not present in the list, you can update the CA certificates by downloading an update program from Microsoft at the following location: http://support.microsoft.com/kb/931125.

About Failover

To achieve failover, install Auth Connector on a second member server. If you install two Auth Connectors, you must designate one as the primary and one as the secondary; however, both must be installed on live systems as they both simultaneously connect to WSS. If the primary member server goes down, the backup immediately assumes the task.

About Proxy Aware Capability

The Auth Connector is proxy-aware. If you prefer to route Auth Connector traffic through a proxy, you can manually configure the `bcca.ini` file to include proxy connection information. This is described in **Step 7** in the following procedure.

Procedure

Prerequisite—Decide which User and Group names are forwarded to the service.

By default, the Auth Connector returns all group and usernames that are contained in your LDAP deployment to the WSS for use in custom policy creation. This might not be practical for an enterprise network that contains multiple user groups and large volumes of users.

- All domain names that can be seen.
- All users (`sam` account names) from each domain.
- All groups from each domain (security groups; *not* distribution groups).
- All members of each group - users (`sam` account names).

Sending that much information might cause Auth Connector resource constraints. For large LDAP deployments, Symantec recommends selecting all users, but decide which groups require policy and forward only those to the WSS. For example, you have domains named **HQ-QA**, **HQ-SALES**, and **HQ-OPERATIONS**; however, only users in the **HQ-SALES** domain require policy checks.

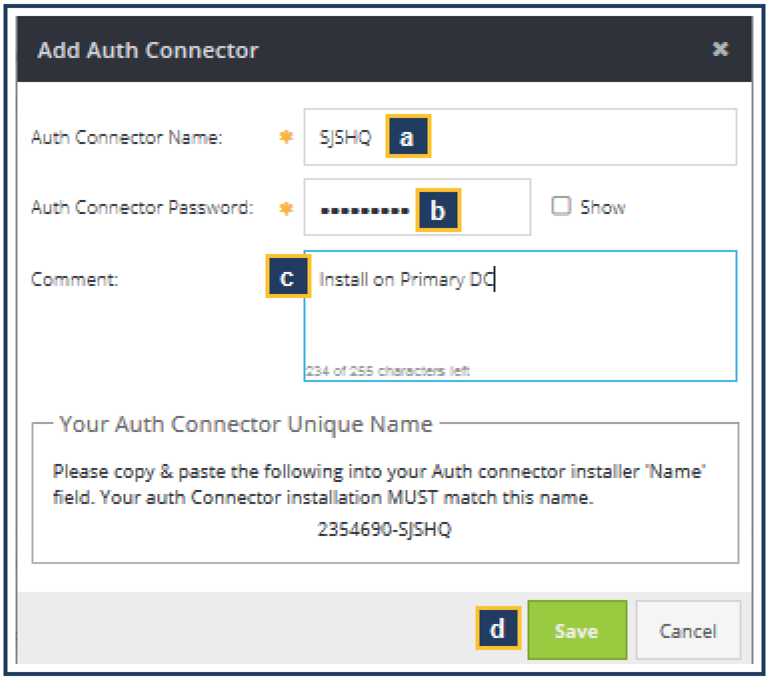
The **bcca.ini** file, which is part of the Auth Connector application (and described in the procedure in **Step 4**), contains `[Groups]` and `[Users]` sections. You can add entries to one, either, or both.

- If the `[Groups]` and `[Users]` sections are empty, WSS receives traffic from all domains and users.
- If the `[Groups]` section contains a domain entry (for example, `HQ-SALES\`), then all groups within that domain send traffic to the cloud service.
- To further narrow the scope with domains, add group names. For example: `HQ-SALES\RegionA`.
- The `Users` section functions in the same manner. Add specific users to even further limit whose traffic is sent to the cloud services. For example: `HQ-SALES\thomas.hardy`.

> **Note:** To prevent a full transmission of all user and group names, do not open the firewall for outbound `443/tcp` from the Auth Connector before you complete this procedure.

Step 1—Add an Auth Connector location to the WSS.

1. Navigate to **Identity > Auth Connector**.
2. Click **Add Auth Connector**.
3. Connect to the service.



Add Auth Connector

Auth Connector Name: * SJSHQ

Auth Connector Password: * •••••••••• ☐ Show

Comment: Install on Primary DC

234 of 255 characters left

Your Auth Connector Unique Name

Please copy & paste the following into your Auth connector installer 'Name' field. Your auth Connector installation MUST match this name.

2354690-SJSHQ

   a. **Name** the service.
   b. Define a **Password**; record this password, as it is required during the Auth Connector application installation.
   c. **Comments** are optional.

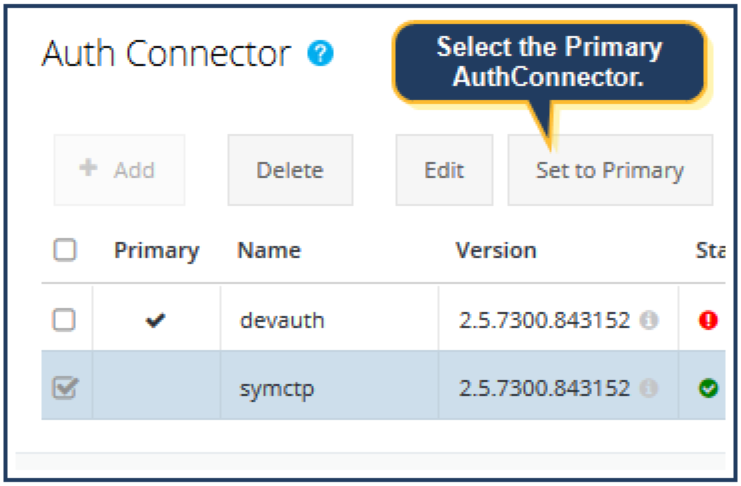
d. The WSS generates **Your Auth Connector Unique Name**, which is a unique customer identification. Record this value, as you must enter it during the Auth Connector application installation process. You can also see the name later by click **Edit** on the **Network > Authentication** page.

e. Click **Save**.

Step 2–(Optional) Add a Backup Auth Connector location.

For authentication failover, add a backup Auth Connector location that will receive data from a second, live domain controller. Repeat **Step 1**.

After configuring, verify that you have the correct Auth Connector **Set to Primary**.



Select the Primary AuthConnector.

☐	Primary	Name	Version	Sta
☐	✓	devauth	2.5.7300.843152	!
☑		symctp	2.5.7300.843152	✓

Step 3–Download Auth Connector.

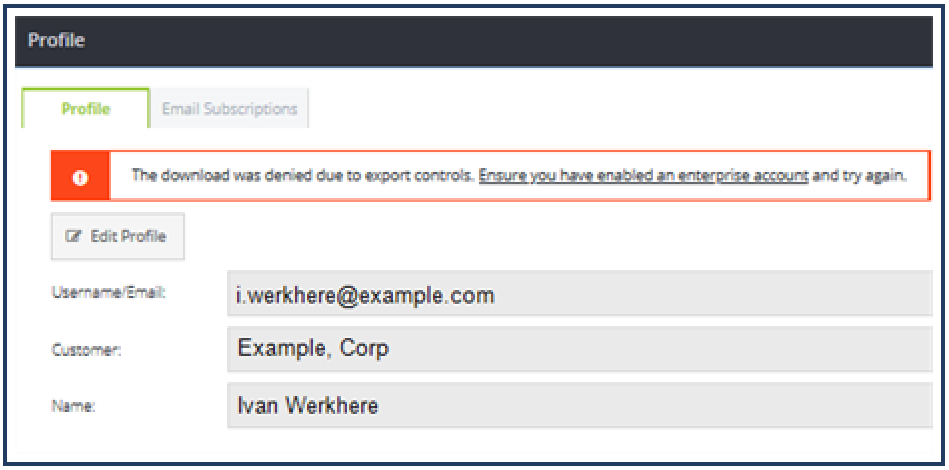
> **Note:** If you downloaded the Auth Connector agent during the Initial Configuration Wizard process, skip to **Step 4**.

1. Remaining on the **Identity > Auth Connector** page, expand the **Download Installer** area.

   On the **Latest Version** is the **Release Note** link. This pop-up provides the information for the most current Auth Connector build.

2. Click **Download**.

3. If this is the first time you are attempting to download the application, the service displays the Profile dialog.



The download was denied due to export controls. Ensure you have enabled an enterprise account and try again.

Username/Email: i.werkhere@example.com

Customer: Example, Corp

Name: Ivan Werkhere

As a company that provides security services across the globe, Symantec supports and complies with United States and local export controls. As an authorized member of your enterprise/organization, you must complete this form before downloading the Auth Connector.

a. Click the **Ensure...enterprise account** link, which opens your Broadcom profile page.

b. Complete your enterprise information and click **Next**.

c. Verify and click **Upgrade Account**. Broadcom sends you a confirmation email.

d. Return to the portal, log out, and log in again. If you do not, you still cannot download the agent.

4. If you have access from your workstation, save the application to a directory of your choice on the domain controller. If you do not, download the application locally and transfer it as necessary.

Step 4—Modify the .ini File to Include Specific Users/Groups.

As described in the **Prerequisite** step, this process to add domains, users, and groups is manual.

1. Access the server that has the Auth Connector application.
2. Using a text editor, open the `bcca.ini` file. If you installed the Auth Connector in the default directory, find it in: **C:\Program Files\Blue Coat Systems\BCCA\**.
3. Locate the `[Groups]` and `[Users]` sections and add entries. You must use the same letter cases that match what is in the Active Directory. Add one entry per line. For example:

```
[Groups]

HQ-SALES\NAWest

HQ-SALES\NANorthWest

[Users]

HQ-SALES\Administrator
```

4. Save the file.

Step 5—Install the Primary Auth Connector on a Member Server.

This installation process grants this account the **Log on as a service** and **Act as a part of the operating system** privileges.

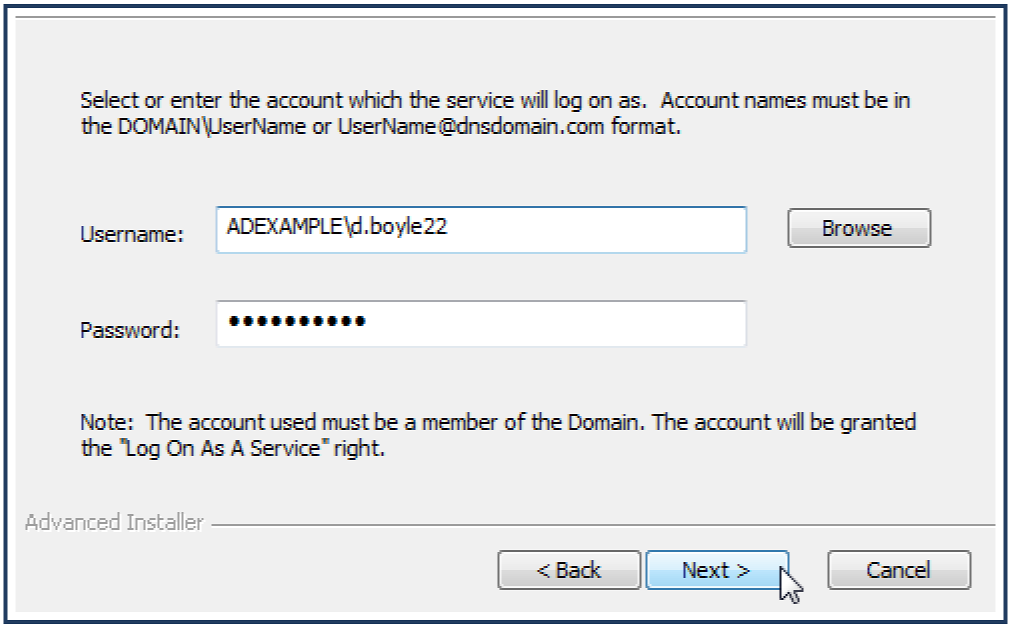
There two methods that create and maintain the IP-to-User map; the Auth Connector setup wizard described in this step provides a choice.

- Domain Controller Query—This is the default method for all connectivity methods. The Domain Controller Query (DCQ) instructs the Auth Connector to query all the domain controllers in your AD to identify users by their IP address when they log on. Each domain controller is contacted every 10 seconds to ensure detection of all logged on users. The Auth Connector contacts the WSS Control Pod through `auth.threatpulse.net` on port 443 and transfers the AD users and group names.

  The WSS returns IPsec endpoint information to the Auth Connector.

- ACLogon Application—For very large enterprises with many domain controllers spread out across locations, the DCQ method might create scalability issues; some user logons might be missed because the domain controllers cannot respond fast enough. The alternative is obtain the ACLogon App and make it available to each client system. **Step 8** describes how to distribute.

1. On the member server, navigate to where you downloaded the Auth Connector application and run the `AuthConnectorInstaller-#####.exe` file as Administrator.
2. Accept the standard program allowance and click **Next** on the first Wizard page.
3. The Select Installation folder page prompts the installation directory choice. Click next to accept the default (**C:\Program Files\Blue Coat Systems\BCCA\**) or select another directory.
4. Click **Next** to begin the Auth Connector configuration wizard.



Select or enter the account which the service will log on as. Account names must be in the DOMAIN\UserName or UserName@dnsdomain.com format.

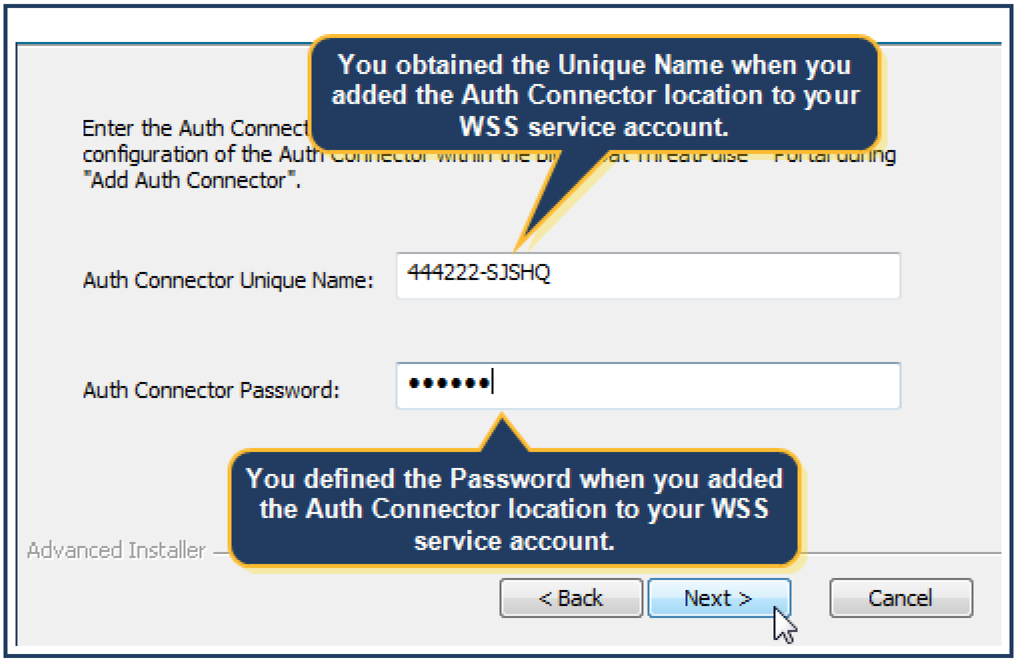
Username: ADEXAMPLE\d.boyle22

Password: •••••••••••

Note: The account used must be a member of the Domain. The account will be granted the "Log On As A Service" right.

Enter the Active Directory account access credentials and click **Next**.

5. Link this Auth Connector installation with the WSS by entering the **Auth Connector Unique Name** and **Password** that you obtained/defined during **Step 1**.



You obtained the Unique Name when you added the Auth Connector location to your WSS service account.

Enter the Auth Connect
configuration of the Auth Connector within the Bl at ThreatPulse Portal during
"Add Auth Connector".

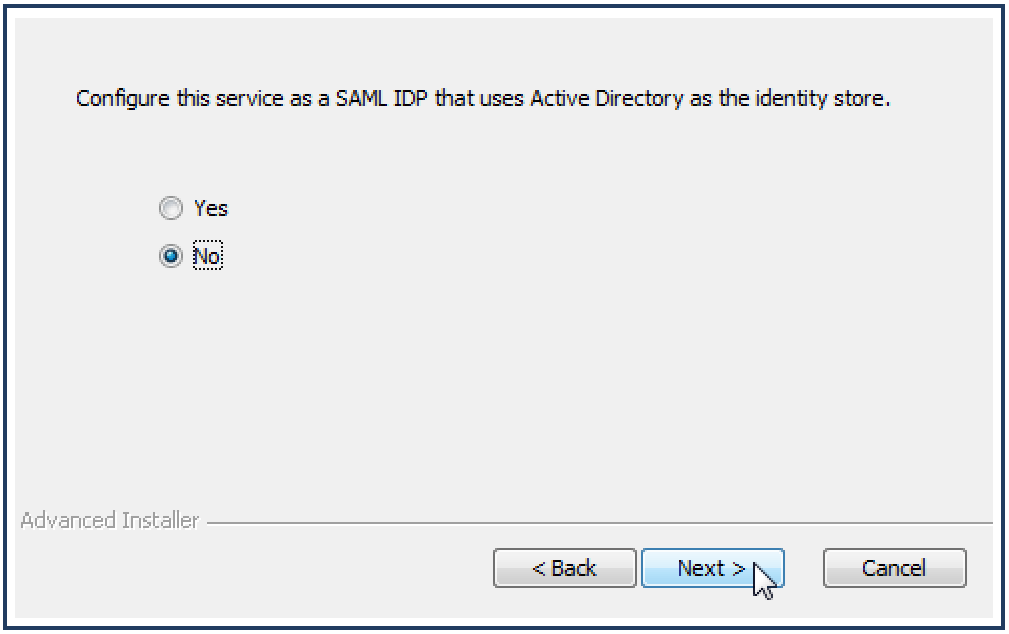
Auth Connector Unique Name: 444222-SJSHQ

Auth Connector Password: ••••••

You defined the Password when you added the Auth Connector location to your WSS service account.

Click **Next**.

6. Do you plan to implement Security Assertion Markup Language (SAML) authentication and employ the Auth Connector to serve as the Identity Provider (IdP)?

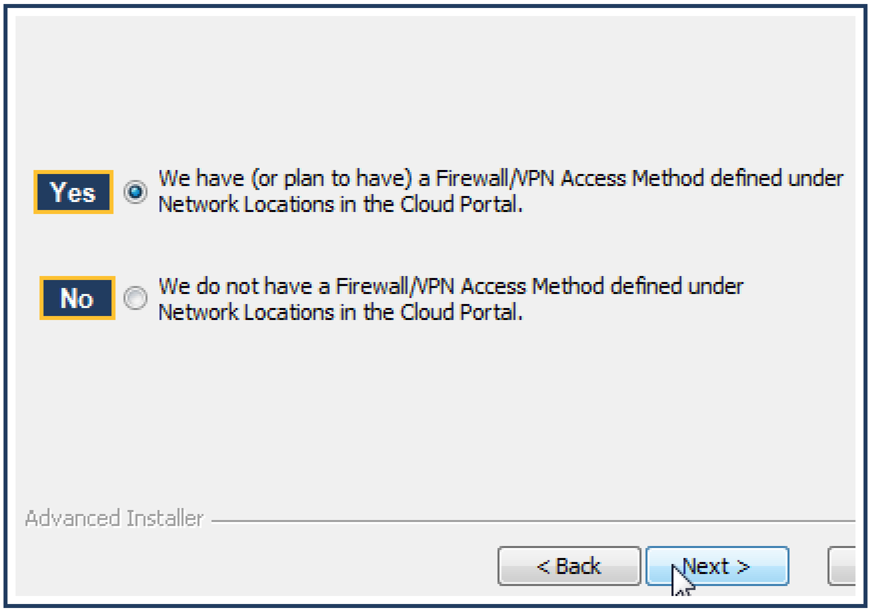


Configure this service as a SAML IDP that uses Active Directory as the identity store.

○ Yes
● No

Select **No** and click **Next**.

7. Does your WSS deployment involve Firewall/VPN locations?

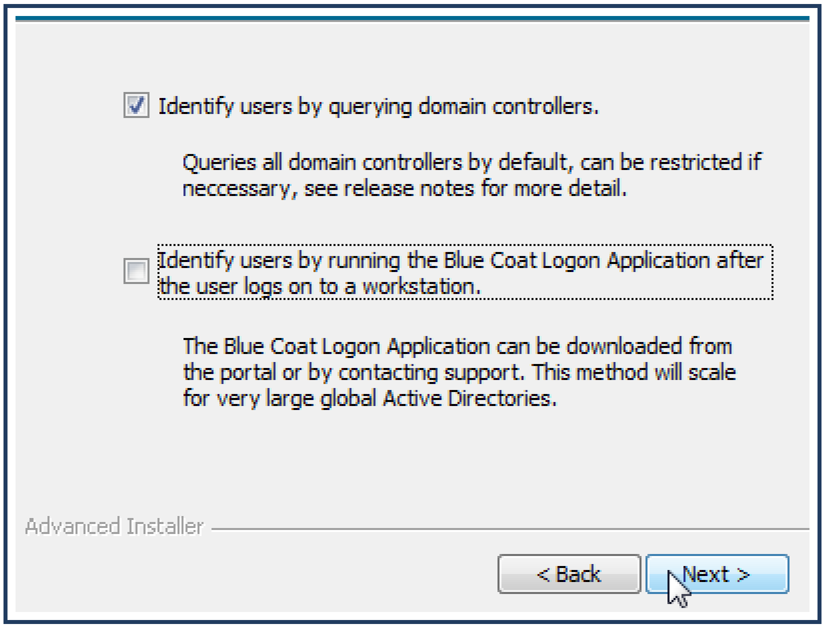


Yes ● We have (or plan to have) a Firewall/VPN Access Method defined under Network Locations in the Cloud Portal.

No ○ We do not have a Firewall/VPN Access Method defined under Network Locations in the Cloud Portal.

- If **Yes**, select **We have (or plan to have) a Firewall/VPN Access Method**, click **Next**, and proceed to **Step 7**.
- If **No**, select **We do not have a Firewall/VPN Access Method**, click **Next** and proceed to **Step 8**.

8. Firewall/VPN method only—As previously described, select how the Auth Connector resolves and maintains the IP-to-user map.



☑ Identify users by querying domain controllers.

Queries all domain controllers by default, can be restricted if neccessary, see release notes for more detail.

□ Identify users by running the Blue Coat Logon Application after the user logs on to a workstation.

The Blue Coat Logon Application can be downloaded from the portal or by contacting support. This method will scale for very large global Active Directories.

   a. Select an option.

      - **Domain Controller Query method**—Queries all domain controllers, although you can restrict the list.
      - **Symantec ACLogon Application**—Symantec recommends this option for very large enterprises with many domain controllers spread out across locations.

   b. Click **Next**.

      - If you selected the **Logon App** option, you are again prompted with the request to open port `80` on the device firewall. Click **Next**.

9. Click **Install**.

10. After the installation completes, click **Finish**.

Step 6–(Optional) Repeat Step 5 to install the backup Auth Connector on a second, live member server.

The **Auth Connector Unique Name** is slightly different–the same number appended with the name you assigned in **Step 1**.

Step 7–(Optional) Route Auth Connector traffic through a proxy.

An alternative to the direct connection to the WSS (on the default ports), you can route the Auth Connector connection through a proxy. Your enterprise deployment standards might dictate this requirement. To achieve this, you must manually edit the `bcca.ini` file, which exists in the Auth Connector package installed on the server.

1. Access the server that has the Auth Connector application.

2. Using a text editor, open the `bcca.ini` file. If you installed the Auth Connector in the default directory, find it in: **C:\Programs and Files (x86)\Blue Coat Systems\BCCA\**.

   The first few lines of the file contain the proxy settings.

   ```
   [Setup]
   ; proxy host to explicitly connect through, assumes port 443 on connect
   ; Proxy=
   ; Explicit proxy port to use to connect to proxy, default 8080
   ; Proxy_Port=
   ```

3. Add your settings as required.

   a. Specify the DNS name (or IP address) of the proxy.

   ```
   [Setup]
   ; proxy host to explicitly connect through, assumes port 443 on connect
   Proxy=example.proxy.com
   ```

   b. If the default connection port is not 8080, enter the correct port.

   ```
   [Setup]
   ; proxy host to explicitly connect through, assumes port 443 on connect
   Proxy=example.proxy.com
   ; Explicit proxy port to use to connect to proxy, default 8080
   Proxy_Port=8085
   ```

4. Save the file.

5. Allow the service to process some traffic, then check various reports to verify that you are receiving traffic from the specified groups/users.

Step 8–For Windows Server 2019 and DCQ Method Only

This step is only required if the member servers with Auth Connector are interacting with Windows Server 2019 through the domain controller query (DCP). Skip to **Step 9** if you are implementing the ACLogon method.

Beginning with Windows Server 2019, Microsoft added more restrictive access control to the `NetSessionEnum()` API. However, the Auth Connector uses this call to query domain controllers for user sessions (when DCQ is the method). In versions previous to Windows Server 2019, members in the **authenticated users** group were able to perform the call because any account that logged in automatically became a member of the **authenticated users** group while logged in. In Windows Server 2019, Microsoft removed the **authenticated users** group and replaced with the **administrators**, **computer operators**, and **power users** groups. Therefore, the Auth Connector cannot receive the authenticated users from the domain controllers. This results in a `cannot query domain controller <ip>; status=5:0x5:Access is denied` error message.

You must perform one of the following methods to complete the configuration for this method.

Option 1

This is the simplest option; however, be advised that this is a less secure security posture because the permission levels are elevated. In fact, your organization's security guidelines might rule that this option is unacceptable. Add the Auth Connector service account user to the **computer operators** group, as this group exists only on servers. The **administrators** group elevates the permissions too high; the **power users** group exists only on workstations.

Option 2

Change the registry value the Microsoft uses for `NetSessionEnum()` to allow the Auth Connector service user access. This option is the more secure choice.

> **Tip:** Symantec advises that only experienced network administrators perform this option.

You must run a powershell script on every domain controller (and any subsequent domain controllers you might add at a later time).

1. Obtain the script from the same step in the WSS Help System.

   http://portal.threatpulse.com/docs/sol/auth/ac/auth-conn-deploy.htm

2. Backup the registry key in case there is an issue that requires a revert.

   ```
   HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\DefaultSecurity\SrvsvcSessionInfo
   ```

3. You must run script as an administrator with elevated privileges. The elevated privileges are required to write the updated *security descriptor* to the registry.

4. If the script is run with no parameters, it prompts for the domain and user. The specified user (typically, the Auth Connector service user) is added to the DACL.

The specified user can also be a group that is allowed access to `NetSessionEnum()`. In this case, the Auth Connector service user must also be a member of the specified group.

Step 9—(If Necessary) Distribute the ACLogon to Client Systems

If you selected the ACLogon option as your Auth Connector solution, you must make the ACLogon application available on all client systems.

> **Tip:** Do *not* enable DCQ and ACLogon at the same time. This can result in mis-identified users.

Obtain the app from the same step in the WSS Help System.

http://portal.threatpulse.com/docs/sol/auth/ac/auth-conn-deploy.htm

The easiest way to deploy it is through Active Directory logon and logoff scripts implemented through group policy and the group policy editor in the AD. Any updates to the ACLogon version are then applied to the software on the AD, not the endpoints. The application is very small and does not consume disk space on the endpoint device.

- By default, both the DCQ and ACLogon create IP mappings in the Auth Connector without a TTL. The Auth Connector configuration file (`bcca.ini`) can define a time-to-live (TTL) in seconds for IP mappings. This is done in the `[CLSetup]` section.
- Combining this with the ACLogon `/interval seconds ####` to periodically update the IP mapping keeps the Auth Connector table up to date. Also, the ACLogon `/logout` parameter triggers an update on any user logout or restart event to clear that IP’s entry.

Example Configuration:

1. Setup a GPO with a login/logout script.

   ```
   Aclogon.exe /logoff /interval seconds 3600 Auth-Connector_hostname/IP
   ```

2. In the Auth Connector's `bcca.ini` file, add `ValidTTL 7200` in the [CLSetup] section.

The ACLogon authenticates to the Auth Connector every hour; if the Auth Connector does not receive an update from the ACLogon for that IP within two hours, the IP is removed from the mapping table. With `/logoff` specified for ACLogon, the IP is removed from the table if the user logs out, restarts, or shuts down the machine.

Step 10—Retrieve the User and Group Names from the AD.

The WSS responds reasonably quickly to new AD integrations. After that, the WSS automatically performs an AD refresh once a week to poll for newly added users.

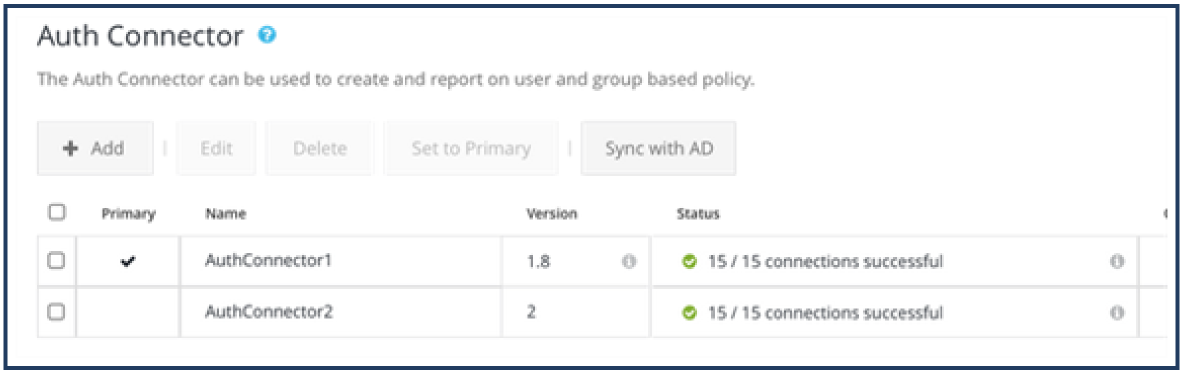
Group memberships are identified through a different process, however. The WSS re-queries group membership every 15 minutes (for active log-ins and users who are already authenticated).

- If you add a user to a new AD group and the user is *not* yet connected and authenticated, the WSS identifies their group membership when they connect.
- If you add a user to a new AD group and the user *is* already authenticated, it can take nearly 15 minutes for the WSS to re-query group membership.

To perform an on-demand retrieval of all user and group names, return to the **Identity > Auth Connector** page and click **Synchronize with AD**. Be advised that it might take up to 24 hours for you see the information in your portal. Avoid re-clicking the button more than once in a 24-hour period; doing so might overly clog the sync queue, causing slower results.

Step 11—Verify the Connection/Icon Descriptions.

As traffic begins to flow through the WSS, you can monitor the Auth Connector connections.

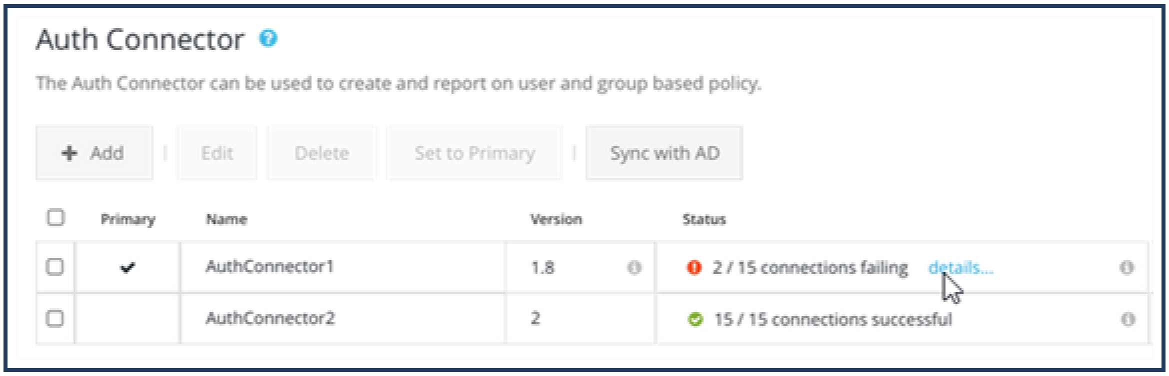


Auth Connector

The Auth Connector can be used to create and report on user and group based policy.

□	Primary	Name	Version	Status
□	✓	AuthConnector1	1.8	✓ 15 / 15 connections successful
□		AuthConnector2	2	✓ 15 / 15 connections successful

The above screenshot illustrates two Auth Connector performing with no issues.



Auth Connector

The Auth Connector can be used to create and report on user and group based policy.

□	Primary	Name	Version	Status
□	✓	AuthConnector1	1.8	! 2 / 15 connections failing details...
□		AuthConnector2	2	✓ 15 / 15 connections successful

The above screenshot illustrates that the Auth Connector has connection issues.

Click the **details** link. The portal displays a dialog that provides details, including the IPs to which the Auth Connector is trying connect, and troubleshooting suggestions.

Back on the **Identity > Auth Connector** page, review the Auth Connector status icons.

Icon	Connection Status Description
✓	The WSS and the installed Auth Connector are communicating successfully.

Icon	Connection Status Description
⚠	The WSS and the installed Auth Connector are communicating, but some connections (data path) are failing. Click the **details** link for more information. The WSS displays a dialog that contains IP address attempts and common troubleshooting tips.
⊖	The WSS has not yet detected this Auth Connector.
❗	Error –There is an credential error. Verify that the Auth Connector credentials in the WSS match the credentials used on the server. –This Auth Connector is disconnected. Disconnected since: *date time*. Verify WSS and Domain Controller configurations.

In the WSS portal (Solutions mode), click any report in which you expect to see user/group name information.

> **Tip:** If you recently added new users and/or groups to the Active Directory, they might not display in reports or display when selecting policy options because the WSS performs an automatic sync operation once every 24 hours. To perform an immediate, manual sync, click **Refresh**.

Click **Messages** (upper-right corner) and look for authentication errors.

Next Steps

- "Review Imported Users and Groups" on page 117
- "Exempt From Authentication" on page 126
- "Authentication Location Policy" on page 119

About SAML Authentication

The WSS supports Security Assertion Markup Language (SAML) authentication, which enables you to deploy the cloud solution and continue to use your current SAML deployment for Authentication.

REQUIREMENT: Only the Firewall/VPN and Explicit Proxy Access Methods with Captive Portal enabled support SAML integration.

SAML Review–Federation

Symantec assumes that you are familiar with SAML authentication. This document provides SAML information as it relates to WSS.

Federation allows access management to occur across organization boundaries. This standard allows two organizations to share information without compromising identities or revealing performed services.

Two *entities* comprise SAML authentication.

- Identity Provider (IdP)–Identify stores, which might contain a back-end directory of users. IdPs authenticate your users.
- Service Provider (SP)–Provides users with access to applications or services. In this deployment, WSS is the SP.

Your supported IdP and WSS must *federate*, or establish trust, before user authentication can occur. The WSS portal provides a configuration screen where you enter or import your IdP entity metadata.

WSS and the IdP exchange data in XML documents called *assertions*, which are sent to the Single Sign-On (SSO) Post or Redirect endpoints. After a user authenticates, the IdP sends an authentication assertion and the service establishes an authenticated session with the appropriate authorization for the user.

Identity Provider Technical Requirements

- WSS supports all SAML-compliant Identity Servers.
- To be compatible with the WSS, the IdP server must be capable of sending an assertion with a `NameID` that includes the user name and group information.
- Other WSS-required features include the following.
  - The WSS integration requires RSA or DSA public keys with a key strength of at least 2048.
  - REDIRECT binding for `AuthRequests` is the recommended use; however, you can use POST binding. The POST binding must be used for `AuthResponses`.
  - Assertions cannot be encrypted.
  - Must include a signing certificate with assertion (x509Certificate tab). For the signing certificate, SHA2 is recommended. SHA1 is supported but not recommended. MD5 is *not* supported.

  - WSS supports adding multiple signing certificates from the same IdP. This is required to handle the use case where an IdP's current signing certificate is about to expire and a new signing certificate will take over.

- Consider the following best practices.
  - To avoid looping, add an authentication bypass entry for domain of the IdP server. See "Exempt From Authentication" on page 126.
  - A redirect to the SAML IdP server from within a CORS-enabled application causes failure. You can verify this by using developer tools on the console. The best practice is whenever possible use the IP Surrogate method. If Cookie Surrogate is the only option, set longer timeout durations.

    > **Tip:** This issue is not encountered if the connectivity method is SEP with the Roaming SAML token.

  - WSS uses IP surrogates where possible for the SAML authentication mode. If it is imperative that you require the `origin-cookie-redirect` mode, which means it is compatible only with user-agents that can follow redirects and that support cookies, contact Symantec Technical Support.
  - With SAML integrated, WSS cannot authenticate explicit HTTPS requests without SSL Intercept enabled.
- The following Knowledge Base article lists what the WSS SAML policy currently bypasses.

  SAML Bypass List KB Article

Tested Identity Providers

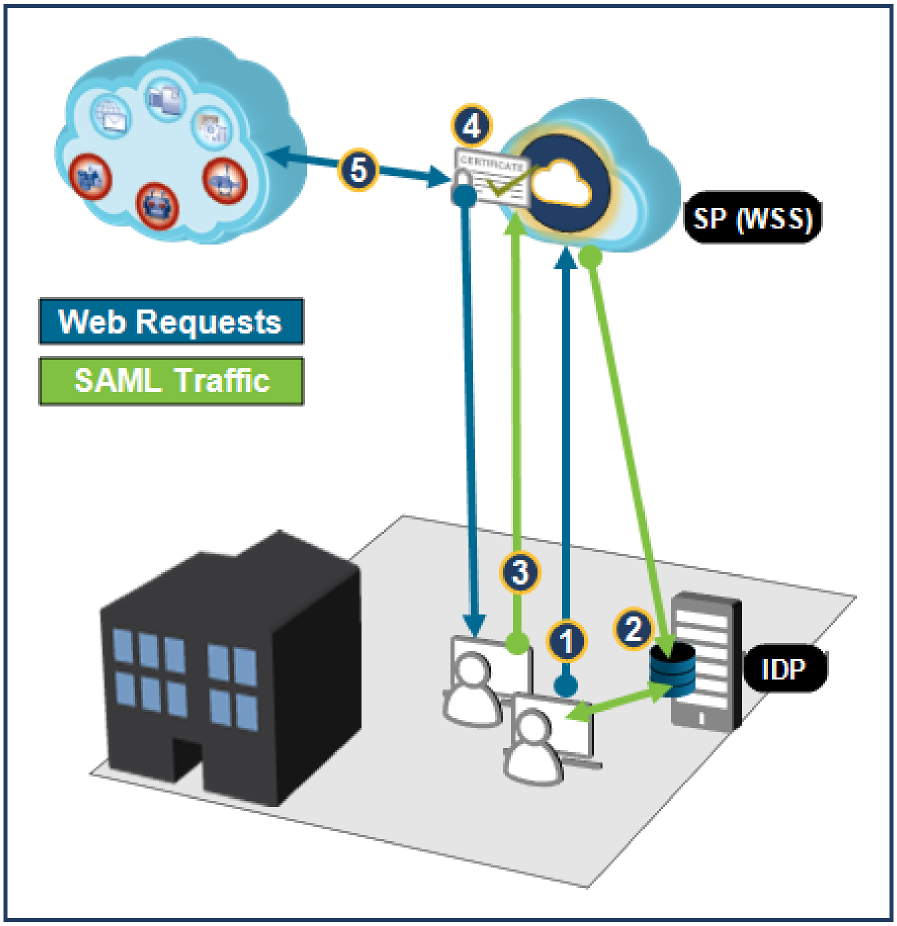
While any IdPs that satisfy the Technical Requirements listed in the previous section should work. Symantec tested and documented the following IdPs.

- Native to WSS methods.
  - Symantec tested and supports Microsoft® Active Directory Federation Services (AD FS) 2.0/3.0.
  - You can use the Auth Connector server as the IdP. The domain controller scales well, provides the group memberships, and automatically handles complexities, such as nested groups.

    For more detailed information, see "About the Auth Connector as a SAML IdP" on page 50.
- Symantec tested WSS with the following SAML IdPs.
  - Symantec VIP Access Manager (enables Single Sign-On)
  - Google G Suite
  - Microsoft Azure (with SCIM 2.0)
  - Okta
  - Ping ID

Flow Overview

The following diagram illustrates what occurs when a user requests a website that requires authentication.



SAML Flow

1—The SP (WSS) intercepts the user request and redirects the web browser to the IdP. The redirect URL includes the SAML authentication request that is submitted to the IdP's SSO service.

2—The IdP authenticates the user by asking for valid login credentials or checking for valid session cookies for stored credentials and sends the assertion to the browser.

3—The browser returns the assertion with the authentication response, which contains the user's username, to WSS (however, the service is not aware of the user's credentials).

4—The WSS validates the request using the corresponding public key, which is embedded in the IdP's signing certificate, and then retrieves the user name from the `Name ID` attribute in the assertion.

5—The WSS redirects the user to the website and creates an authenticated session for the user.

More Details

The following Knowledge Base discusses SAML connections in more technical detail.

About SAML Connections

Support for Multiple AD Forests

Symantec suggests two methods to authenticate users spread across multiple AD forests.

- Establish external forest trust relationships between one hub AD and the rest of the AD forests with one particular AD forest, then configure the hub AD as the IDP and federate it with WSS. In most cases, this requires bi-directional trusts.
- If bi-directional trusts are not administratively possible, install or enable ADFS in each AD forest and then create an ADFS-level trust between each ADFS server. This allows various types of trust relationships to exist for applications that federate with ADFS.

Configure This?

AD FS

- Proceed to "Import Users and Groups for SAML" on page 40.

Auth Connector

- "About the Auth Connector as a SAML IdP" on page 50
- "Deploy Auth Connector as SAML IdP" on page 53

Third-Party IdPs

- "Integrate Symantec VIP Access Manager as the SAML IdP" on page 93
- "Integrate Google G Suite as a SAML IdP" on page 81
- "Integrate Microsoft Azure as the SAML IdP" on page 57
- "Integrate Okta as the SAML IdP" on page 71
- "Integrate Ping Identity as the SAML IdP" on page 88

SEP

- Connectivity: WSS-SEP Roaming SAML

Import Users and Groups for SAML

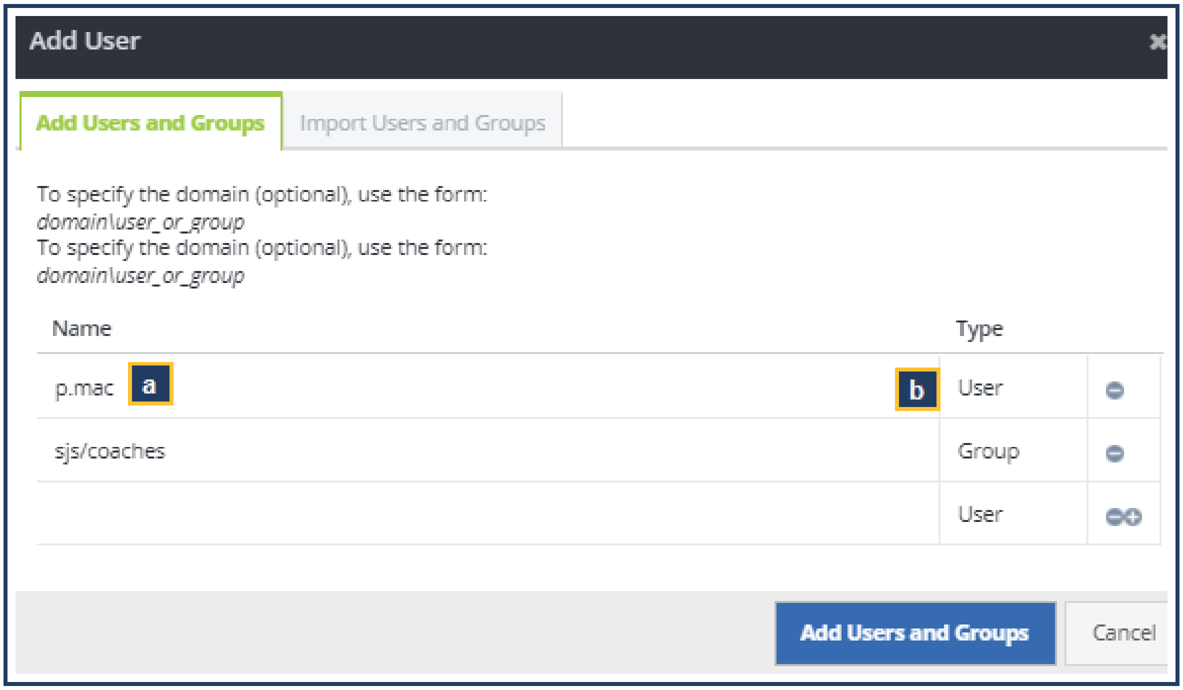
The Web Security Service portal provides a method to manually import usernames and/or group memberships. This is required if you are implementing Security Assertion Markup Language (SAML) as your only method to authenticate users and groups that are sending web traffic to WSS. Furthermore, you might need to add specific users or groups from domains that are not currently routing traffic to the cloud service.

The portal allows you to manually enter users and/or groups one at a time or import a text file that contains multiple entries.

Procedure

Option 1–Enter Manually

1. Navigate to **Identity > Users and Groups > Imported Users/Groups**.
2. Click **Add**. The service displays the Add dialog.



To specify the domain (optional), use the form:
domain\user_or_group
To specify the domain (optional), use the form:
domain\user_or_group

Name	Type
p.mac	User
sjs/coaches	Group
	User

   a. On the **Add Users and Groups** tab, enter a user or group **Name**.

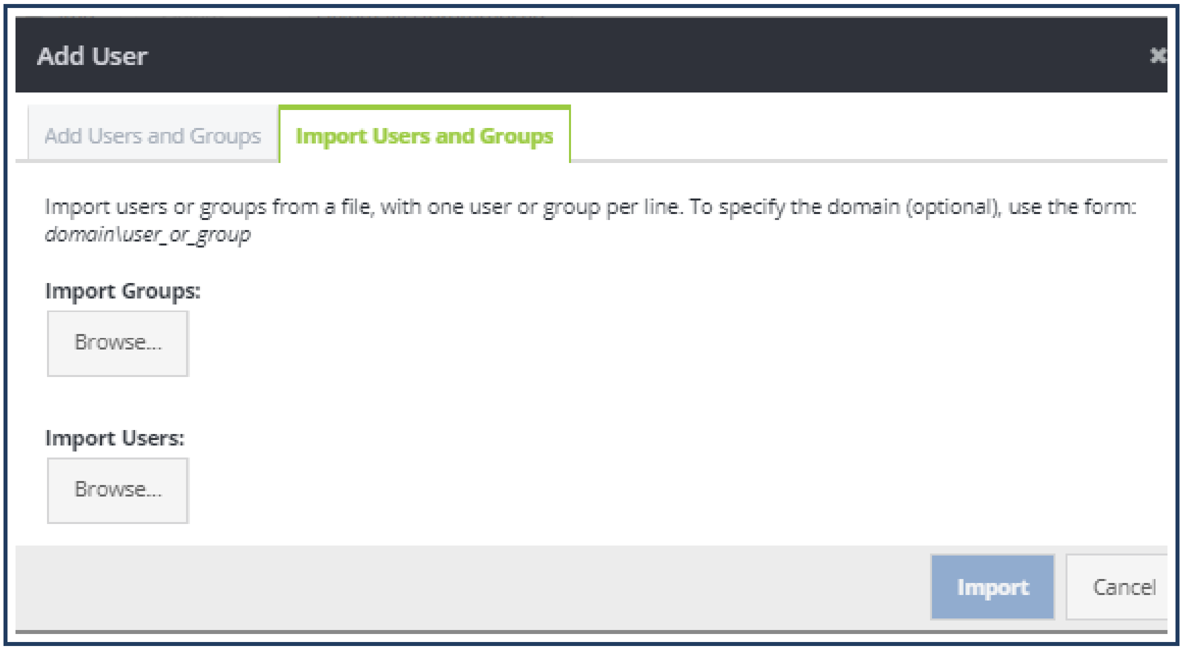
   b. Select the **Type**: **User** or **Group**.

   c. Add other names/groups as necessary.

   d. Click **Save**.

Option 2–Import List

1. **Pre-requisite**. Create text files that contain a lists of user and group names from your Active Directory or LDAP database. To import user and group names, create one file for each. Do not mix content in the files. The files must contain one entry per line. To match the format used by the Symantec Auth Connector, the entry formats are `domain\`*`user_name`* and `domain\`*`group_name`*. For example: **`sjs\d.boyle`**. You can either configure your SAML IdP to return user and group names in that format or retain the current format (which must match what you enter on the **Identity > SAML Authentication** page). Save the files in a location that you can access from the portal.
2. Navigate to **Identity > Users and Groups > Imported Users/Groups**.
3. Click **Add**. The service displays the Add dialog.



Import users or groups from a file, with one user or group per line. To specify the domain (optional), use the form: *domain\user_or_group*

   a. Select the **Import Users/Groups** tab.
   b. For either **Import Groups** or **Import Users**, click **Browse** and navigate to where you stored the text files containing the lists.
   c. Select the file and click **Open**.
   d. Click **Save**.
   e. Repeat if necessary; you can add more than one list of each type. If at list contains user and groups have already been imported, the service displays a notification dialog and does not re-add those names.

SCIM Option–Synchronize User/Group Population in an IdP

For supported IdPs, you can configure System for Cross-domain Identity Management (SCIM). Integrate the IdP with the WSS through an integration token. This allows you retain and manage users and groups in the vendor IdP interface.

The **Third-Party Sync** tab on the **Identity > Users and Groups** page provides the users and groups as provided by the IdP. After the IdP account is provisioned to use SCIM and a change is made to the user data through the IdP portal, the IdP automatically communicates that data change to the WSS. You can see the updated the users and groups in the portal. Subsequent synchronizations require less time; Symantec estimates between 15 and 45 minutes.

Following the initial data synchronization setup, it takes some time for all of the data to be pushed from Azure to WSS. After that initial data download completes, subsequent data updates from Azure require much less time because only the changes are pushed to the WSS.

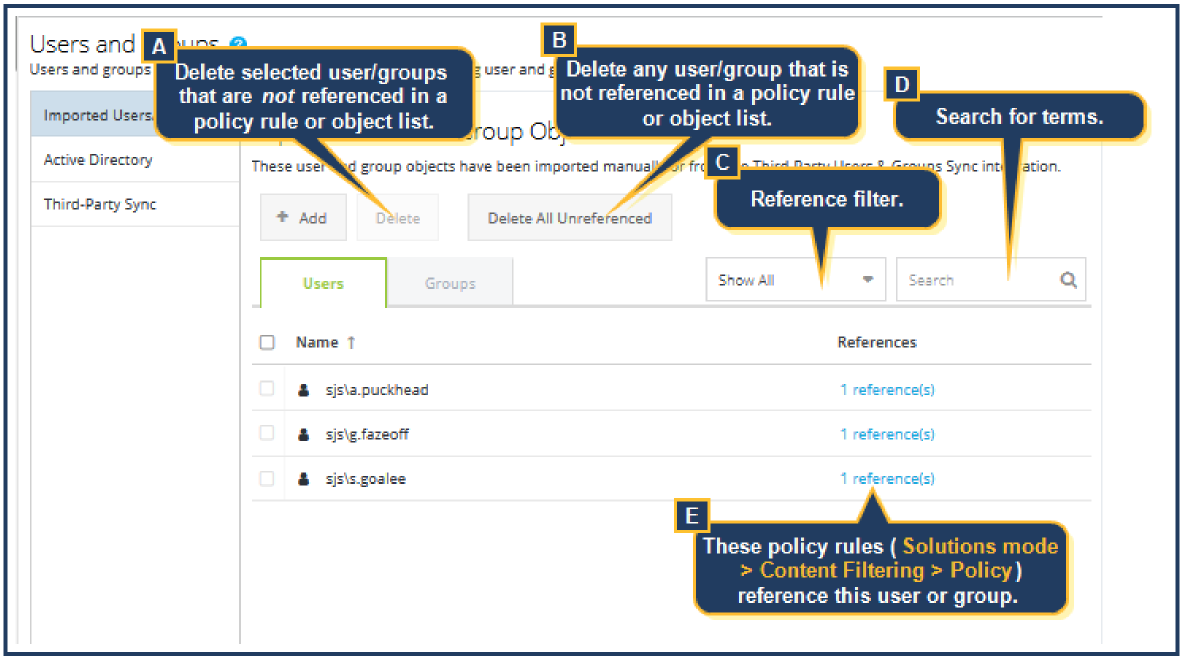
Only identity providers that support SCIM 2.0 are supported. The following IdP vendors provide SCIM support.

Each configuration topic describes how to integrate the vendor IdP with WSS.

- "Integrate Microsoft Azure as the SAML IdP" on page 57
- "Integrate Okta as the SAML IdP" on page 71

Manage Manually Imported Users and Groups

When you save manual entries or imported lists, the portal displays the users and groups.



These user and group objects have been imported manually or from Third Party Users & Groups Sync integration.

☐ Name ↑	References
☐ sjs\a.puckhead	1 reference(s)
☐ sjs\g.fazeoff	1 reference(s)
☐ sjs\s.goalee	1 reference(s)

A: Delete selected user/groups that are *not* referenced in a policy rule or object list.

B: Delete any user/group that is not referenced in a policy rule or object list.

C: Reference filter.

D: Search for terms.

E: These policy rules (Solutions mode > Content Filtering > Policy) reference this user or group.

Return to the **Users and Groups > Imported Users and Groups** screen to manage your manually imported users and groups.

A—You select any user and group and Delete them unless the user or group is currently referenced in Content Filtering policy or exists in a custom list object. (See **E** and **F** below.)

B—Remove All Unreferenced deletes all users or groups that not currently referenced in Content Filtering policy or in a custom list object.

C—By default, the service displays every imported name, sorted alphabetically by user and group name. From the **Show All** drop-down, filter to just **Referenced** in policy rules.

D—You can search for a specific name (if you know it) or for a string. For example, searching for Logan returns any name with Logan in it.

E—The **References** column indicates that a Content Filter policy rule exists that applies to the user or group (**Policy > Content Filtering**). Click the link to display the rule editor with the relevant wizard tab, which enables you to instantly edit and apply changes. For example, the **Who** tab that contains the selected user.

✓ Next Step

- Proceed to: "Prepare Microsoft AD FS for Federation" on page 44.

Prepare Microsoft AD FS for Federation

As part of the WSS and Security Assertion Markup Language (SAML) authentication integration, you must configure your Identify Provider (IdP) to trust the cloud service. This involves downloading the WSS metadata XML file and importing it to your IdP, and creating a Claim Rule for user identity.

This topic provides procedures for the Active Directory Federation Services (AD FS) 2.0 and assumes that you have installed and configured the administration software for this IdP. The following steps comprise the minimum required settings to create trust between the entities. For other settings that you might require for your deployment, refer to the AD FS documentation.

> **Tip:** Use **SHA2** for the Certificate Signature Algorithm. **SHA1** is supported, but not recommended. This recommendation is based on industry-recognized SAML best practices.

Procedure

Step 1—Obtain the WSS metadata file.

1. Navigate to **Identity > SAML Authentication**.
2. Click **Download Metadata**. Save the XML file to location from which you can access with the IdP.

Step 2—Import the WSS metadata to AD FS.

1. In the AD FS MCC, select **AD FS 2.0 > Trust Relationships > Relying Party Trusts**.
2. Select **Relying Party Trusts**; right-click and select **Add Relying Party Trust**. The MCC displays a wizard.
    a. Click **Start**.
    b. Select **Import data about the relying party from file**, navigate to the WSS metadata XML file, and import it.
    c. Click **Next** until you reach the final wizard screen. Verify that the **Open the Edit Claim Rules** option is selected.
    d. Click **Close**.

    The AD FS prompts you to edit claim rules. Proceed to the next step.
3. Add an IdP claim rule that instructs the IdP to include an attribute in the assertion that the SAML realm uses to identify a user.
    a. Click **Add Rule**.
    b. Ensure that the **Send LDAP Attributes as Claims** option is selected and click **Next**.
    c. For the **Claim Rule Name** option, enter **NameID**.

d. For the **Attribute Store** option, select **Active Directory**.

e. From the **LDAP Attribute** drop-down list, select **User-Principal-Name**.

f. From the **Outgoing Claim Type** drop-down list, select **NameID**.

g. Click **Finish**.

4. Click **OK**.

Next Step

- Proceed to "Federate the Web Security Service and AD FS" on page 46.

Federate the Web Security Service and AD FS

As described in "About SAML Authentication" on page 36, *federation* is the process by which two Security Assertion Markup Language (SAML) entities–the Identity Provider (IdP) and Service Provider (SP)–establish trust. For this deployment, the Web Security Service is the SP and federates with a supported IdP that currently provides SAML authentication in your network.

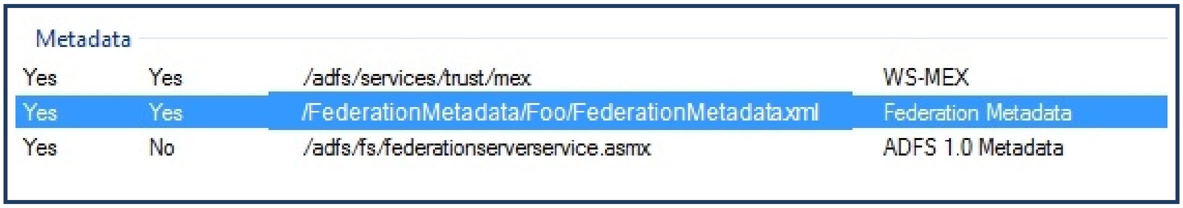
Technical Requirements

Port 8443 is required for browsers to post SAML assertions to a Web Security Service asset. Verify that this port is open on your gateway firewall devices.

Step 1–Export Metadata from the AD FS.

This step describes how to export the metadata from the IDP into an XML file that can be read by the WSS.

1. Log in to the AD FS 2.0 MMC.
2. Select **Services > Endpoints**. Locate the **Metadata** area for the URL beside the **Federation Metadata** type.



Metadata

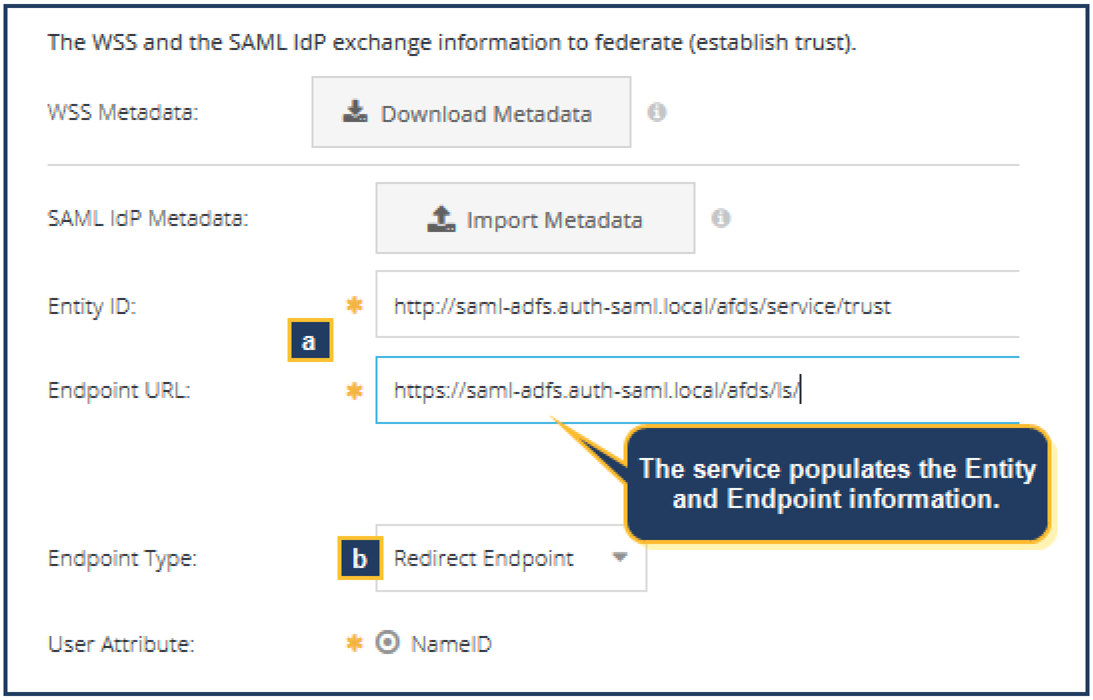
Yes	Yes	/adfs/services/trust/mex	WS-MEX
Yes	Yes	/FederationMetadata/Foo/FederationMetadata.xml	Federation Metadata
Yes	No	/adfs/fs/federationserverservice.asmx	ADFS 1.0 Metadata

3. Copy the URL and paste it into a browser address bar.
4. Save the XML document. If another person is to perform the WSS, ensure that file exists in a directory that is accessible by that person.

Step 2–Complete the Federation

To complete the federation, import the IdP metadata into WSS and assign a signing certificate chain.

1. Navigate to **Identity > SAML Authentication**.
2. Expand the **SAML Authentication** area.
3. Import the IdP metadata.



The WSS and the SAML IdP exchange information to federate (establish trust).

WSS Metadata:

SAML IdP Metadata:

Entity ID: * http://saml-adfs.auth-saml.local/afds/service/trust

Endpoint URL: * https://saml-adfs.auth-saml.local/afds/ls/

The service populates the Entity and Endpoint information.

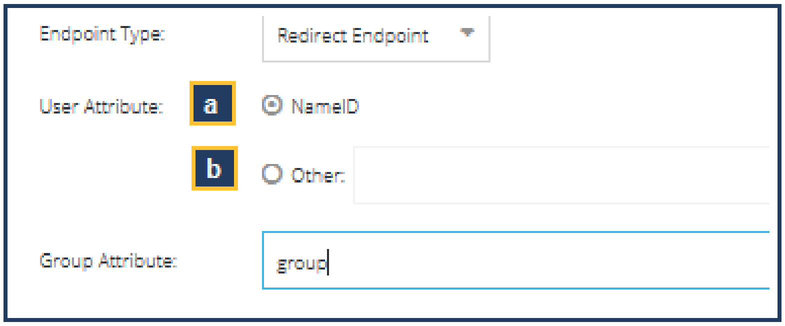
Endpoint Type: Redirect Endpoint

User Attribute: * ● NameID

a. Click **SAML IdP Metadata: Upload**, navigate to the file location and open the metadata XML file, which imports the data and populates the **Entity ID** and **Endpoint URL** fields with SAML entity trust information.

b. The imported metadata also includes the **Endpoint Type**. The **Redirect Endpoint** option is recommended over **Post Endpoint**. The browser redirects the request to the SAML endpoint, which is considered to be the simpler option. The **Post Endpoint** is available if the IdP only supports that endpoint type.

4. Review and confirm the **User Attribute** and **Group Attribute** formats.



Endpoint Type: Redirect Endpoint

User Attribute: ● NameID

○ Other:

Group Attribute: group

a. By default, WSS uses the SAML-standard **NameID** field as a **User Attribute**.

- The service accepts any format; however, to match the format used by the Auth Connector, the `NameID` attribute must be *`domain\username`*. Communicate with your IDP administrator.

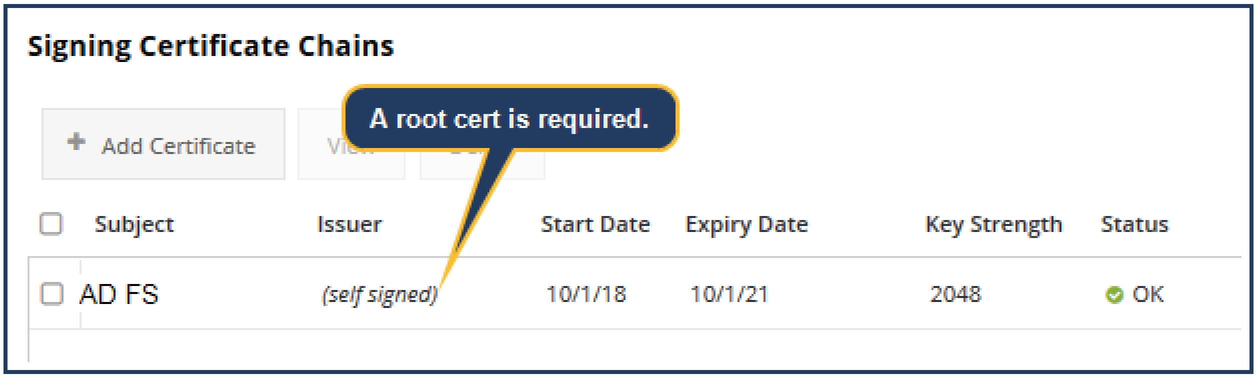
- The **Other** option is for when the IdP administrator has the user name in another attribute. Enter that attribute name in this field. Other use cases include manually entering the value if the metadata does not contain the attribute or if the metadata is not imported.

b. By default, WSS does not receive **Group Attribute** information because it pulls information from the **NameID** attribute. To obtain group names for use in policy and reports, you must instruct WSS as to which attribute to use.

IDP administrator: When the metadata does not contain a **Group Attribute**, consider the following.

- The `http://schemas.xmlsoap.org/claims/Group` schema is the most common ADFS group attribute.
- Alternatively, to configure the ADFS IdP to return user and group names in the *domain\username* format, use these attributes: `msDS-PrincipalName` for users and `Token-Groups—Qualified by Domain Name` for groups.
- Review the attributes the SAML IdP returned by SAML. Examine the browser network traffic and the packets coming from the SAML IdP. The packets contain Base64 encoded response with XML assertions.

5. Review the **Signing Certificate Chain**.



Signing Certificate Chains

☐ Subject	Issuer	Start Date	Expiry Date	Key Strength	Status
☐ AD FS	*(self signed)*	10/1/18	10/1/21	2048	✓ OK

If the metadata contains certificates, the service imports them and displays them in the Signing Certificates area.

- If the IdP's signing certificate is self-signed and imported to the service, that is sufficient.
- If the signing certificate is not self-signed, the chain must contain the IdP's signing certificate and all its parent certificates up to the root.
- The chain must contain the IdP's signing certificate and all its parent certificates up to the root.

Click **Add New Certificate** and paste in the certificate contents. Repeat to add other certificates in the chain as required.

> **Tip:** If the WSS portal displays any certificate-related errors, see "Troubleshoot SAML Authentication" on page 130.

6. Click **Save**.

Step 3–Verify Policy Sync

Turning authentication on and off triggers a policy update between the your account and WSS, but switching between SAML and Auth Connector authentication types requires the policy to be activated before an update occurs.

Navigate to **Policy > Content Filtering** and click **Activate**.

Step 4–Enable Captive Portal

If it is not already, you must enable Captive Portal for the Firewall/VPN or Explicit Proxy location and select **SAML** as the authentication method.

- Firewall/VPN (IPsec) method–Proceed to "Authentication Location Policy" on page 119.
- Remote Users–Navigate to **Identity > Authentication Policy**. This page contains the **Enable Captive Portal** option in **Rule G4**.

Optional–Exempt Sources/Destinations from Authorization

SAML and Captive Portal authentication methods use *re-directions*. Some network environments might not be compatible, which requires you to bypass sources or destinations to ensure client operations. You might have other reasons to bypass.

- See "Exempt From Authentication" on page 126.

✓ Next Step

- As authenticated user traffic begins to come in, verify the success of the integration. In **Solutions** mode, generate user-based reports and verify that they display expected authenticated employee names.
- If you encounter connection problems, see "Troubleshoot SAML Authentication" on page 130 for possible causes and resolutions.

About the Auth Connector as a SAML IdP

The WSS supports Security Assertion Markup Language (SAML) authentication, which enables you to deploy the cloud solution and continue to use your current SAML deployment for Authentication.

REQUIREMENT: Only the Firewall/VPN and Explicit Proxy Access Methods with Captive Portal enabled support SAML integration.

Instead of a third-party vendor SAML Identity Provider (IdP), the Auth Connector can function as the IdP. For a more general discussion of SAML authentication and WSS as a Service Provider (SP), see "About SAML Authentication" on page 36.

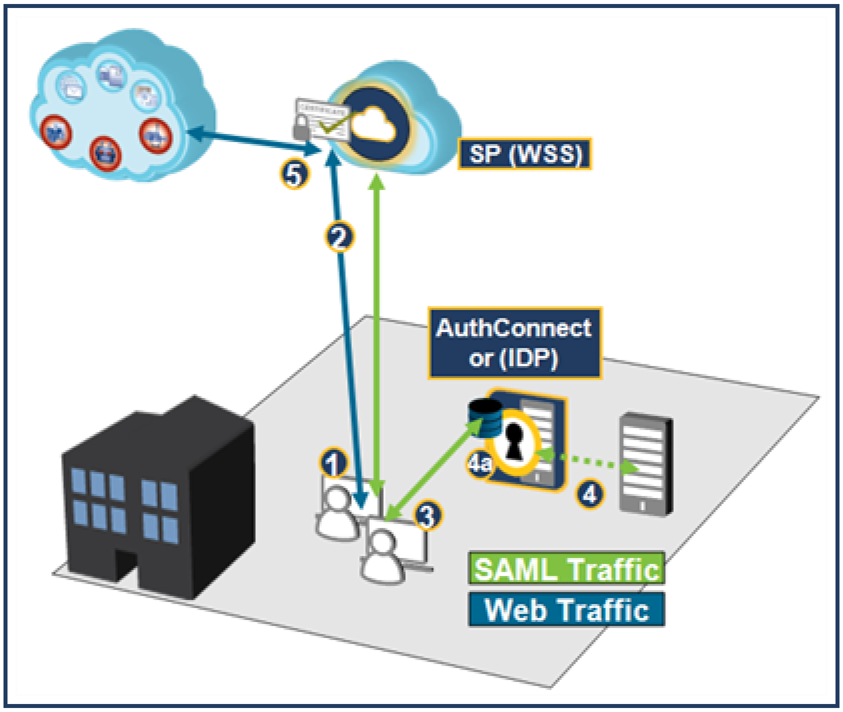
Use Cases for Auth Connector as SAML IdP

- Simpler configuration than integrating a third-party vendor.
- When specific configuration settings are met, provides Single Sign On (SSO) to users.
    - The client/workstation must belong to the Windows domain.
    - The logged in user must belong to the domain.
    - The browser must trust the IdP.

Current Limitation

- BASIC authentication is not supported.

Data Flow



1—The employee initiates a web request.

2—The SP (WSS) intercepts the user request and redirects the web browser to the IdP (the Auth Connector). The redirect URL includes the SAML authentication request. The IdP listens on port `80` for SAML requests.

3—The IdP returns a IWA 401-challenge to the client and sets the authentication headers both NTLM and Kerberos.

4—The IdP authenticates the user.

- If the client supports Kerberos, the IdP validates the credential on-box and returns the verdict.
- If Kerberos is not available, the IdP connects to the Active Directory (NTLM).

5—Upon a successful challenge, WSS receives the minted assertion with the now-known user name and group memberships from the browser (on port 8443), signs the certificate with the assigned key, and creates an authenticated session.

About User/Group Memberships

By default, the Auth Connector retrieves all users and groups. The configuration topic describes how to limit which groups are retreived.

WSS responds quickly to new AD integrations. After that, WSS automatically performs an AD refresh once a week to poll for newly added users.

However, group memberships are identified through a different process. WSS re-queries group membership every 15 minutes (for active log-ins and users who are already authenticated).

- If you add a user to a new AD group and the user is *not* yet connected and authenticated, WSS identifies their group membership when they connect.
- If you add a user to a new AD group and the user *is* already authenticated, it can take nearly 15 minutes for WSS to re-query group membership.

To perform an on-demand retrieval of all user and group names, return to the **Identity > Auth Connector** page and click **Sync with AD**. Be advised that it might take up to 24 hours for you see the information in your portal. Avoid re-clicking the button more than once in a 24-hour period; doing so might overly clog the sync queue, causing slower results.

Next Step

- See "Deploy Auth Connector as SAML IdP" on page 53.

Deploy Auth Connector as SAML IdP

If you do not want to implement a third-party Security Assertion Markup Language (SAML) authentication vendor Identity Provider (IdP), you can leverage the Auth Connector as the IdP. This is a simpler configuration that also keeps your Web Security Service deployment compartmentalized.

Because it uses IWA authentication (NTLM and Kerberos), group memberships are securely retrieved from the Windows access token. The domain controller scales well and provides the group memberships, and automatically handles complexities such as nested groups. This method also allows for SSO when specific configurations are met.

Technical Requirements

- To function as a SAML IdP, you must install the Auth Connector on a Windows domain member server, as it uses Windows system calls to authenticate the user and retrieve the user's group memberships.
- All redundant servers must share the same hostname, which is the hostname in the SAML redirect endpoint.
- The returned groups returned are subject to the AD group scoping rules.

  https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-security-groups

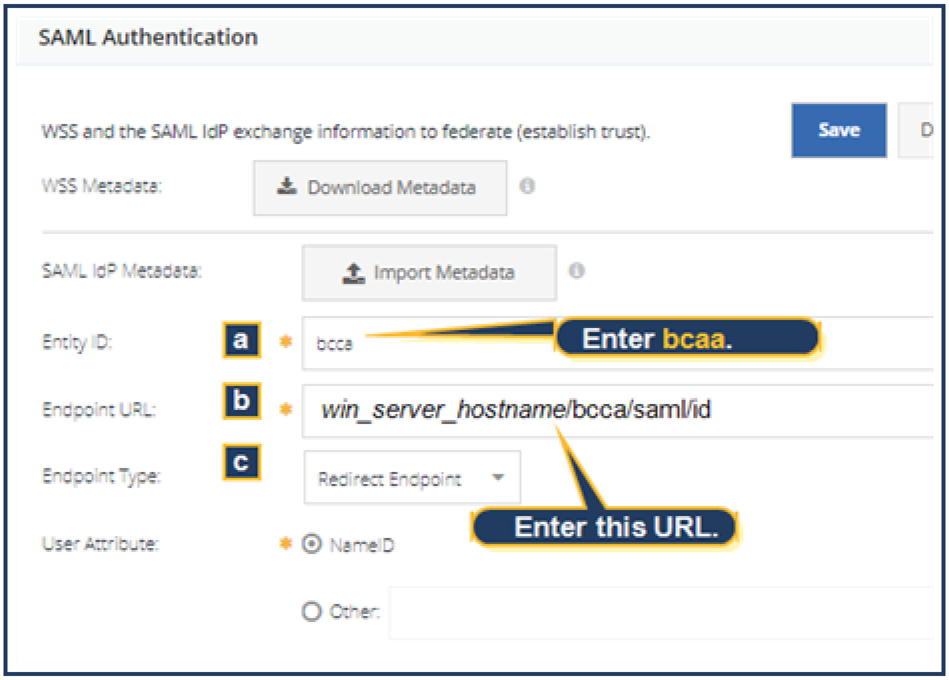
  The result is the domain controller provides the Auth Connector the domain and global groups in the its forest. If you can add a group to an ACL on the member server that has the Auth Connector, then the Domain Controller informs the Auth Connector.
- If you have previously used the Auth Connector authentication method and plan to switch to SAML or employ both methods and want to maintain policy based on usernames, you might have to re-examine policy to include both Auth Connector and SAML authenticated users.
- Verify that the following ports are open on the Windows firewall service on the Auth Connector server: `80`and `443`.
- If you require information about Captive Portal, see "About Captive Portal Authentication" on page 99.

Procedure

Step 1—Federate the Service and the Auth Connector.

This step establishes trust between WSS and the Auth Connector, which allows for SAML assertions.

1. Navigate to **Identity > Auth Connector**.
2. Expand the **SAML Authentication** area.
3. Import the Auth Connector IdP metadata.



WSS and the SAML IdP exchange information to federate (establish trust).

WSS Metadata:

SAML IdP Metadata:

Entity ID: * bcca

Endpoint URL: * *win_server_hostname*/bcca/saml/id

Endpoint Type: Redirect Endpoint

User Attribute: * ● NameID

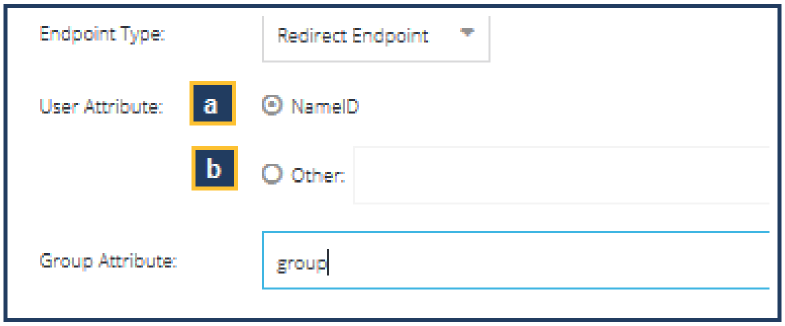
○ Other:

a. Enter **bcca** as the **Entity ID**.

b. Enter the following for the **Endpoint URL**: `http://win_server_hostname/bcca/saml/idp`, where *win_server_hostname* is the hostname of the server where the Auth Connector is installed.

c. Use the **Redirect Endpoint** versus the **Post Endpoint**. The browser redirects the request to the SAML endpoint, which is considered to be the simpler option.

4. Review and confirm the **User Attribute** and **Group Attribute** formats.



Endpoint Type: Redirect Endpoint

User Attribute: ● NameID

○ Other:

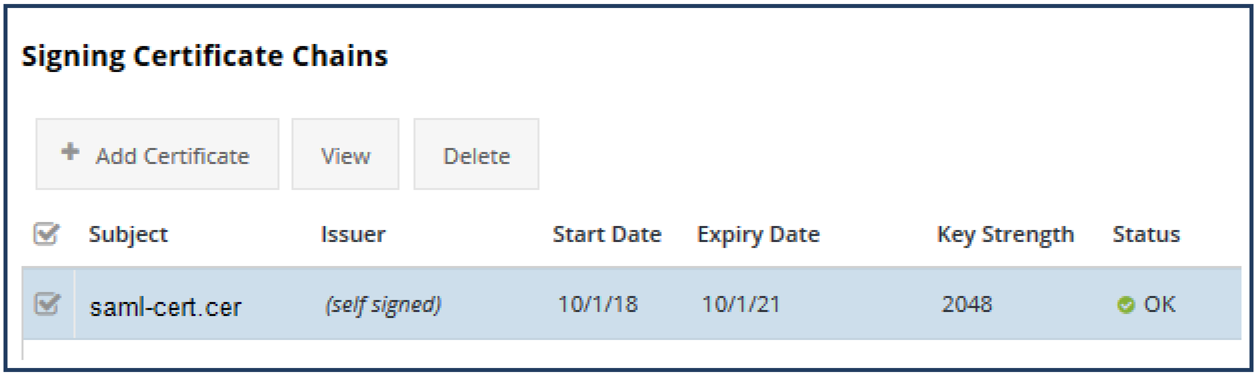
Group Attribute: group

a. By default, WSS uses the SAML-standard **NameID** field as a **User Attribute**.

- The `NameID` attribute format is *`domain\username`*.
- The **Other** option is for third-party SAML IdPs. No action required.

b. When the Auth Connector is used as the IdP, the **Group Attribute** field must have the **group** entry.

5. Add the Auth Connector IdP certificate.



Signing Certificate Chains

☑	Subject	Issuer	Start Date	Expiry Date	Key Strength	Status
☑	saml-cert.cer	*(self signed)*	10/1/18	10/1/21	2048	● OK

a. The Auth Connector installation wizard prompted you to select it as the SAML IdP ("Deploy the Auth Connector" on page 23, **Step 5.6**).

- If you selected this option, navigate to **C:\Programs and Files (x86)\Blue Coat Systems\BCCA\** and open the **saml-cert.cer** certificate file in a text editor.
- If you elected to use an existing one, open it in a text editor.

b. Click **Add New Certificate**.

c. Paste the contents of the certificate, beginning with `-----BEGIN CERTIFICATE-----` and ending with `-----END CERTIFICATE-----`.

d. Click **OK**.

> **Tip:** If the WSS displays any certificate-related errors, see "Troubleshoot SAML Authentication" on page 130.

6. Click **Save**.

Step 2–Configure browsers to trust the Auth Connector.

To allow the Kerberos/NTLM transactions, the client browsers must trust the Auth Connector agent. The browser cannot present a cached credential unless the site (the Auth Connector hostname) exists in the local/trusted site zone. You can accomplish this with various methods.

- Use group policy to configure browsers to add the Auth Connector hostname to their trusted sites.
- Manually configure browsers. For example, in Internet Explorer, navigate to **Tools > Internet Options > Security**. Add the hostname to the **Local Intranet** or **Trusted Sites** list.

Another option is to use a hostname with no dots (which might rely on an imputing DNS suffix).

Step 3–Specify Captive Portal Policy Per Location

Enable Captive Portal for the Firewall/VPN or Explicit Proxy location.

- See "Authentication Location Policy" on page 119.

Integrate Microsoft Azure as the SAML IdP

If you want to use Security Assertion Markup Language (SAML) authentication for the Web Security Service, but do not have your own Active Directory (AD) deployed, you can provision Microsoft® Azure™ as the SAML Identity Provider (IdP).

WSS supports the automatic synchronization of users and groups through the use of an integration token (described in the following procedure).

Technical Requirements

- Port `8443` is required for browsers to post SAML assertions to a WSS asset. Verify that this port is open on your gateway firewall devices.
- This integration requires the Azure AD Premium and Enterprise Mobility Suite products. During the procedure, you are prompted to begin trials if you do not already have them.
- To prevent browser looping, add the IdP lookup URL(s) to the Authentication Bypass list: `: aadcdn.msauth.net`.

  See "Exempt From Authentication" on page 126.

> **Tip:** This demonstration uses screenshots from the Azure Portal updated in Oct 2018.
> Microsoft might change the UI at their discretion.

Procedure

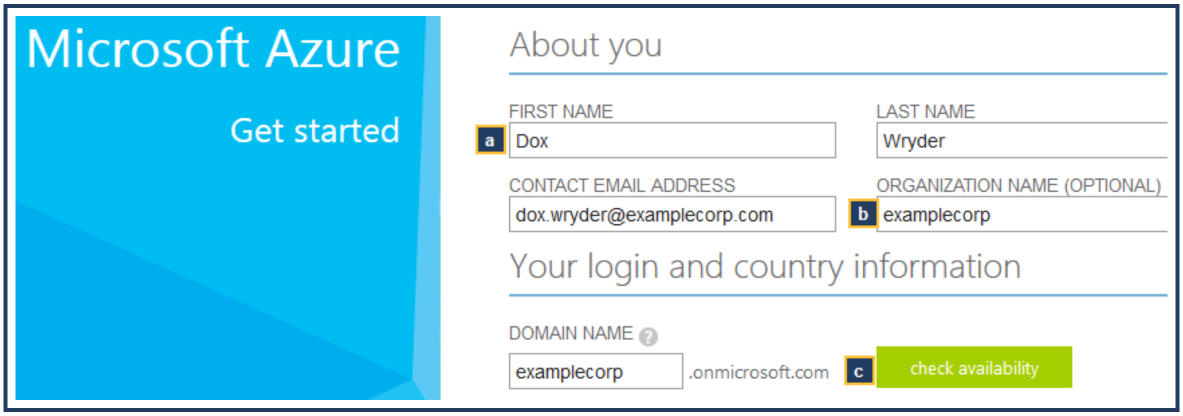
Step 1—Setup the Azure AD Accounts

If you do not have one, you must create a Microsoft Azure account, which establishes your contact and credit card information (for verification).

1. In a browser, access:

   https://account.azure.com/organization

2. Complete the required fields.



About you

FIRST NAME: Dox

LAST NAME: Wryder

CONTACT EMAIL ADDRESS: dox.wryder@examplecorp.com

ORGANIZATION NAME (OPTIONAL): examplecorp

Your login and country information

DOMAIN NAME ?: examplecorp .onmicrosoft.com

a. Enter your contact **Name** and **Email Address**.

b. The **Organization Name** is optional. If you enter one, the **Domain Name** mirrors the entry (hover over the tool tip (**?**)) to read more about this.

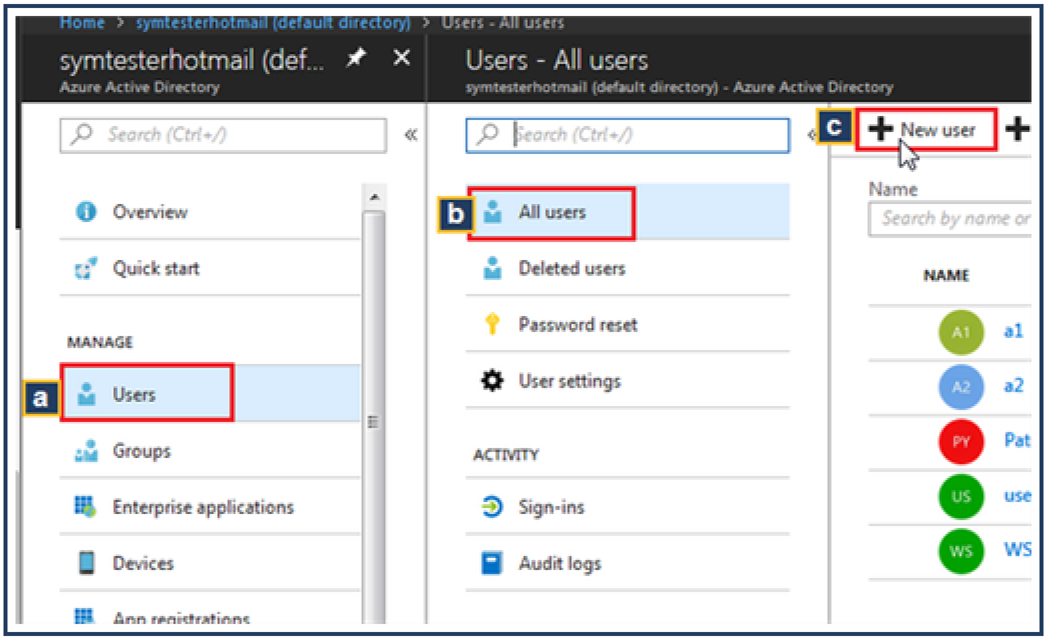
c. Click **Check Availability** to confirm that your domain name is not currently used by another party.

3. When complete, click **Sign In** (upper-right screen); the browser displays the Microsoft account log in page.

4. Log in using your organization's credentials.

Step 2—Add Users and Groups

1. In the Azure application, select **Azure Active Directory** (left-menu).



2. If your Azure account is not populated with **Users** or **Groups**, you can add them.

   a. Select **Users**.

   b. Select **All users**.

   c. Click **New User**. Azure displays a page to add them.

3. After adding users, you can add them to groups.

   a. Return to the **Azure Active Directory** page and select **Groups**.

   b. Select **All Groups**.

   c. Click **Add Group**. Enter the requested information.

   d. To add users to a group, on the group page select **Members**.

Step 3—Prepare Azure for the WSS

The next phase is to add the WSS as an application, which requires providing SAML Federation information obtained from your WSS portal.

1. Remaining in your Azure Portal, return to the main **Azure Active Directory** page.

2. Add the Symantec app.

   a. Select **Enterprise Applications**.

   b. Click **New Application**; click **Security**. The portal displays a list of known related applications.

   c. Scroll down to (or **Search** for) and select **Symantec Web Security Service**; click **Add**.

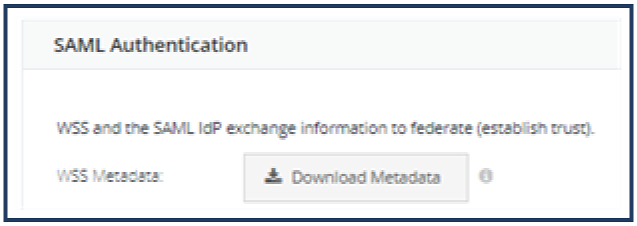
   d. Select **Single sign-on**, then select **SAML**.

3. To complete this step, you must log in to your WSS portal account (open a new browser tab) and obtain the meta data required to federate the two services.

   a. Navigate to **Identity > SAML Authentication**.

   b. Expand the **SAML Authentication** area.

   c. Click **Download Metadata**.



SAML Authentication

WSS and the SAML IdP exchange information to federate (establish trust).

   d. Open the download (browser) and view the contents.

   e. Record the following values (for example, copy to Notepad).

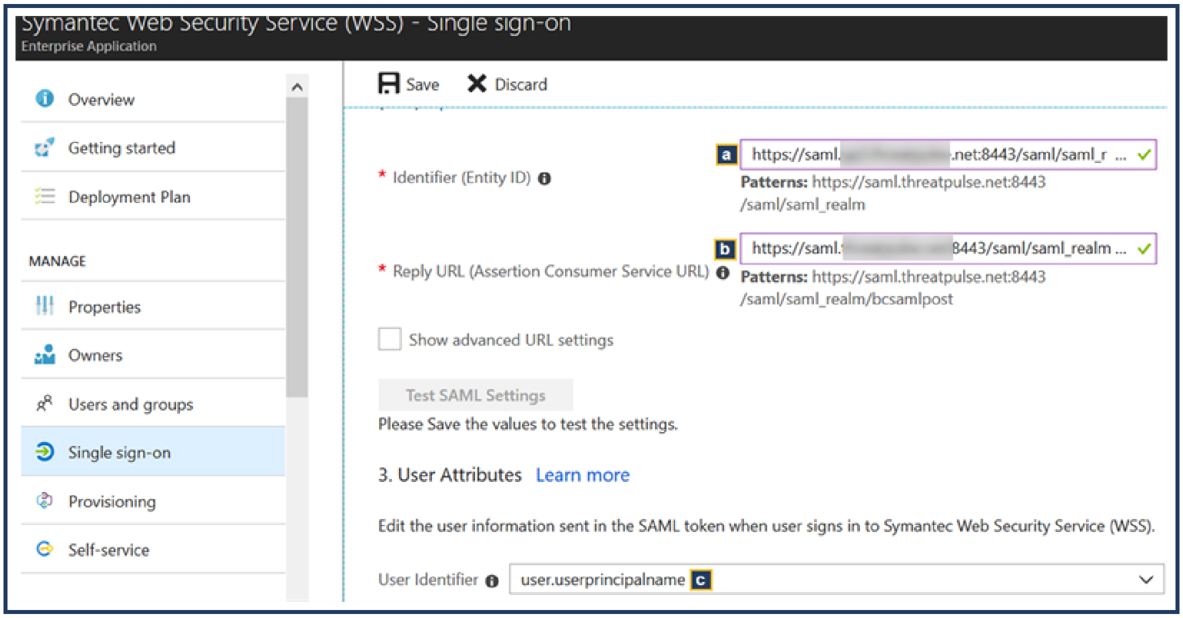
- The `EntityDescriptor`—

  `https://saml.threatpulse.net:8443/saml/saml_realm`

- The `AssertionConsumerService Location`—

  `https://saml.threatpulse.net:8443/saml/saml_realm/bcsamlpost`

4. Return to the Azure Portal tab.



Symantec Web Security Service (WSS) - Single sign-on
Enterprise Application

* Identifier (Entity ID): https://saml.[redacted].net:8443/saml/saml_r ... ✓
Patterns: https://saml.threatpulse.net:8443/saml/saml_realm

* Reply URL (Assertion Consumer Service URL): https://saml.[redacted]8443/saml/saml_realm ... ✓
Patterns: https://saml.threatpulse.net:8443/saml/saml_realm/bcsamlpost

□ Show advanced URL settings

Test SAML Settings
Please Save the values to test the settings.

3. User Attributes Learn more

Edit the user information sent in the SAML token when user signs in to Symantec Web Security Service (WSS).

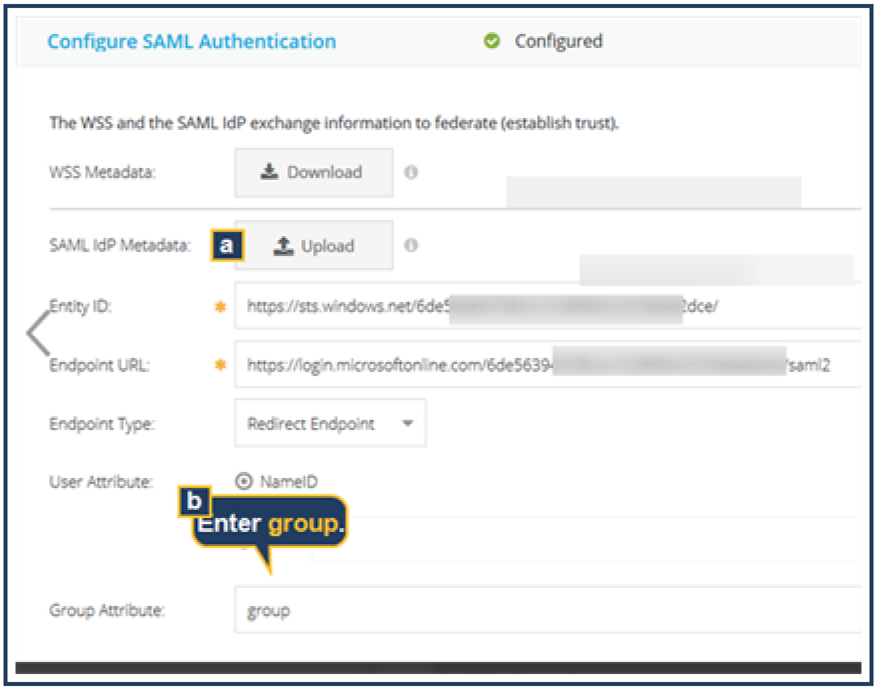
User Identifier: user.userprincipalname

   a. In the **Identifier** field, enter the `EntityDescriptor` value.
   b. In the **Reply URL** field, enter the `AssertionConsumerService Location` value.
   c. From the **User Identifier** drop-down list, select **user.userprinciplename**.
   d. Click **Save**. The interface displays a confirmation message.

5. Scroll down to **SAML Signing Certificate**. If you do not have an existing active or unused certificate, click **Create New Certificate** to create one; save it and make it **Active**.

   In the to-be-used certificate row, click the **Metadata XML** link in the **Download** column; save the file.

6. Return to the WSS portal tab.



Configure SAML Authentication ✓ Configured

The WSS and the SAML IdP exchange information to federate (establish trust).

WSS Metadata: Download

SAML IdP Metadata: Upload

Entity ID: * https://sts.windows.net/6de5[redacted]2dce/

Endpoint URL: * https://login.microsoftonline.com/6de5639[redacted]/saml2

Endpoint Type: Redirect Endpoint

User Attribute: ● NameID

Group Attribute: group

a. Click **SAML IdP Metadata: Upload**; browse to the saved Azure certificate file saved in the previous step and open it. The portal populates the **Entity ID**, **Endpoint URL**, and **Signing Certificate** fields.

b. In the **Group Attribute** field, enter **group**.

c. Click **Save**.

Step 4—Make Users Available for Authentication

In Azure, select which users and groups are available for SAML authentication.

1. In the Azure **Symantec Web Security Service** application, select **Users and Groups**.
2. Click **Add User**.
3. Select the users to include and click **Select**. Azure displays the Add Assignment dialog.
4. Click **Assign**.

Step 5—Test SAML

To perform an immediate configuration validation, you can explicitly proxy a browser of a client on the network to WSS.

1. In the WSS portal, add a location **(Connectivity > Locations)**. Name it SAML Azure Test, for example.
   a. Set to **Explicit Proxy**.
   b. **Save** the location.

2. Navigate to **Identity > Authentication Policy**.

    a. Click **Add Rule** and select **Explicit Proxy Locations**. The WSS displays the New Rule page.

    b. Click **Add Sources** and add the Explicit Proxy **Location**.

3. In the **Verdict** area,

    a. Enable **Captive Portal**.

    b. Select **SAML**.

4. Click **Add Rule**; click **Activate**.

5. Log in to the test client machine and configure the browser proxy settings to `proxy.threatpulse.net:8080`.

6. Restart the browser. If you see the Azure sign-in page, the SAML deployment is functioning.

    - If not, retrace the configuration steps.
    - If you encounter connection problems, see "Troubleshoot SAML Authentication" on page 130 for possible causes and resolutions.

Step 6–Include Group Identities in the Assertion

Azure does not return the list of groups that a given user currently belongs to in the SAML assertion for group policy enforcement. However, Azure allows for a created role for each group. By creating and mapping a role to a group, Azure returns the list of roles that a user belong to based on the groups that the user is in.

> **Note:** For WSS group-level policy to be valid, the name of the roles *must* match the name of the groups used in the WSS policies.

To be able to create group-based policies in the WSS, Azure provides the following steps that create roles for each user group.

Creating application roles affect the **Step 4—Make Users Available for Authentication** procedure. After creating roles, users and groups added to the Web Security Service SAML application no longer have Default Access as their default role. You must select the role for each user and group that you add to the application.

For users that are assigned to a specific application role but also belongs to a group with its own assigned role, both roles are included in the assertion. For example, **UserAB** is assigned to **roleA** and belongs to **groupB**, which has its own assignment of **roleB**.

1. Complete the procedure in the following article.

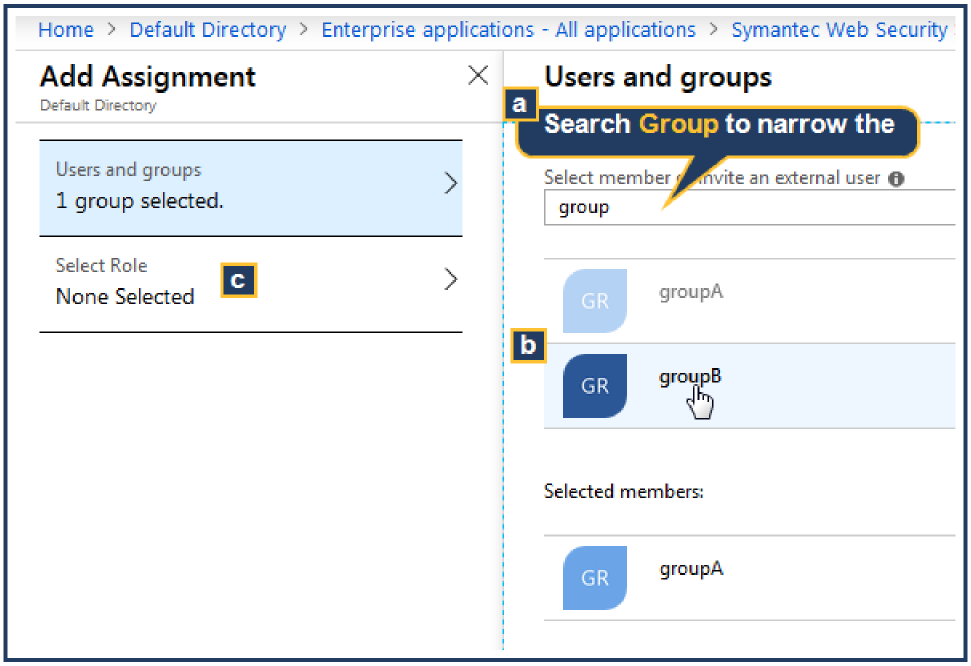
    https://docs.microsoft.com/en-us/azure/active-directory/active-directory-enterprise-app-role-management

    You can select any string for your role names–even ones that are identical to your group names–as long as the selected role names match the group names in your WSS policy. The following examples use the names **roleA** and **roleB** to match example WSS group names **roleA** and **roleB**. Azure AD returns these particular role information in plain text in the SAML assertion, thus *must* be mapped to the appropriate groups.

2. In the Azure **Symantec Web Security Service** application, select **Users and Groups**.

3. Click **Add User**.

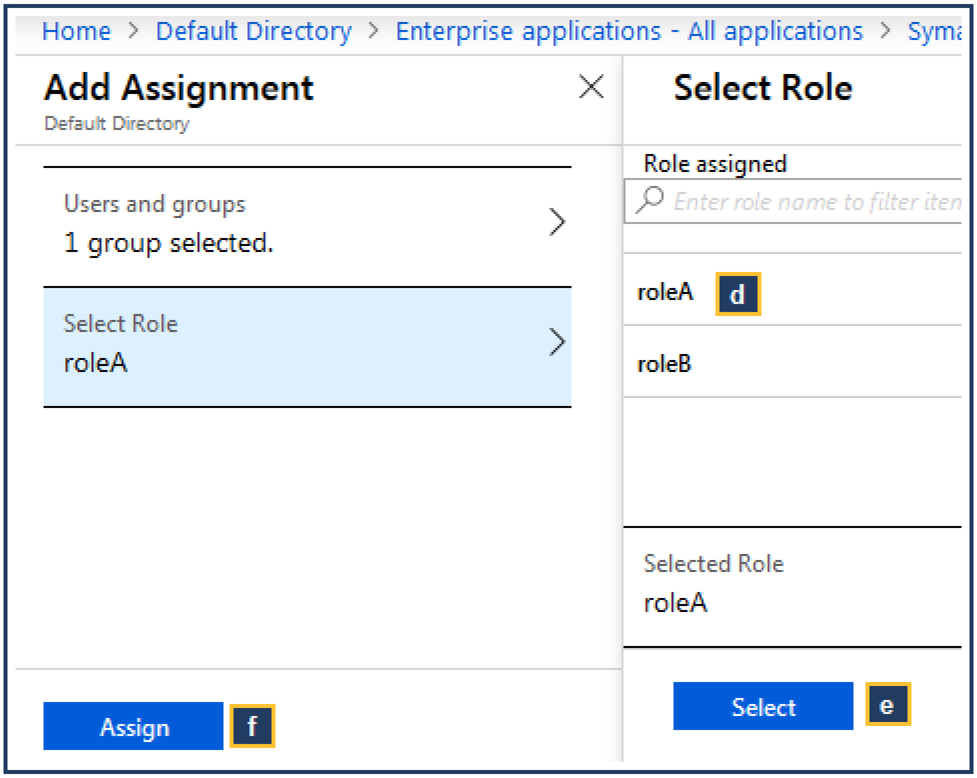
4. Select groups.


Home > Default Directory > Enterprise applications - All applications > Symantec Web Security
Add Assignment
Default Directory
Users and groups
1 group selected.
Select Role
None Selected
c
Users and groups
a
Search Group to narrow the
Select member or invite an external user
group
GR
groupA
b
GR
groupB
Selected members:
GR
groupA

   a. Use the **Search** field to narrow view from all users. This example limits the view to the **group** keyword.

   b. Select which groups are to be susceptible to WSS policies and click **Select**.

   c. Click **Select Role**.



Home > Default Directory > Enterprise applications - All applications > Syma
Add Assignment
Default Directory
Select Role
Role assigned
Enter role name to filter iten
d
e
f
Assign
Select

Users and groups
1 group selected.

Select Role
roleA

roleA
roleB

Selected Role
roleA

d. Select which roles are to be susceptible to WSS policies.

e. Click **Select**.

f. Click **Assign**.

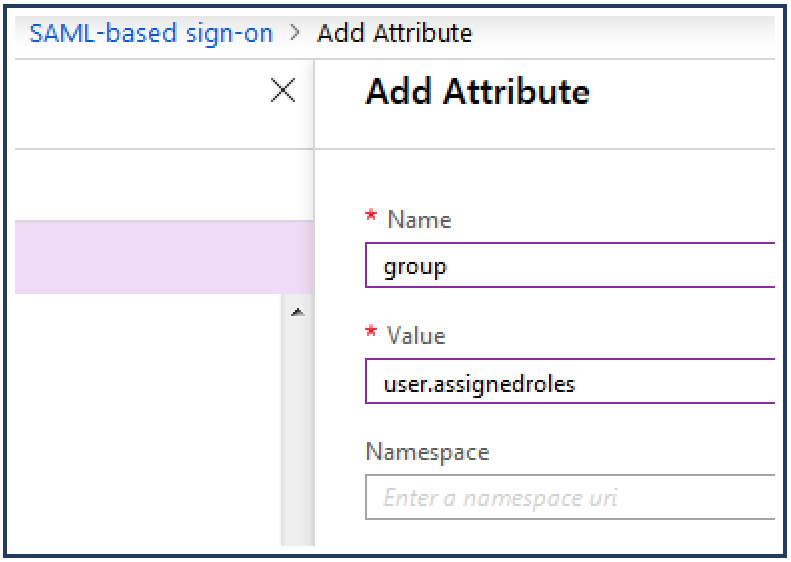
5. Repeat as necessary to assign all groups to roles.

6. Add the group attribute.

    a. Return to the WSS application (in Azure) and select **Single sign-on** from the left-menu.

    b. In the **User Attributes** area, select **View and edit all other user attributes**.

    c. Click the **Add Attribute** link.



SAML-based sign-on > Add Attribute

Add Attribute

* Name

group

* Value

user.assignedroles

Namespace

d. In the **Name** field, enter **`group`**.

e. In the **Value** field, enter **`user.assignedroles`**.

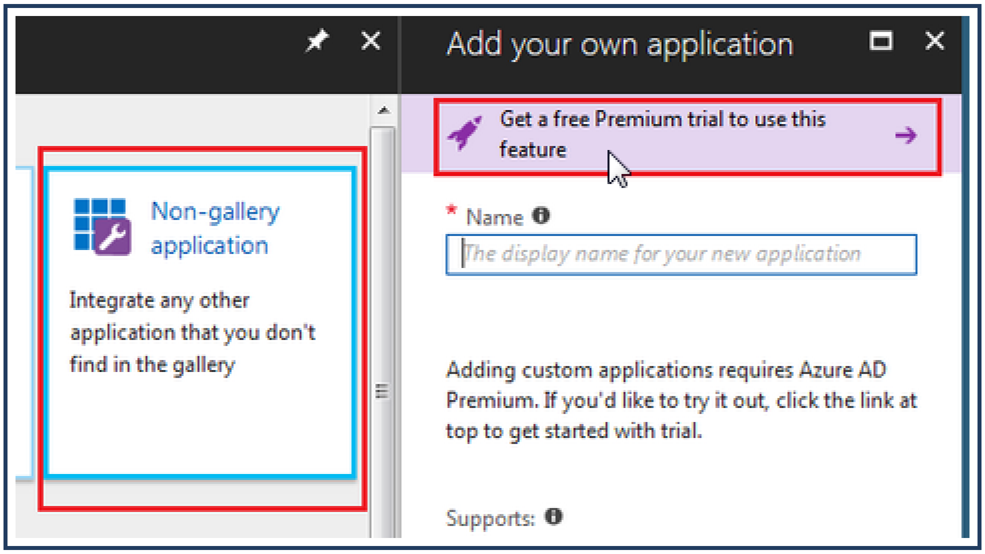
f. Click **OK**.

Step 7—Configure Automatic User/Group Population in the WSS.

Provision your Azure account to manage users and groups within the Azure portal yet have them automatically sync to the WSS portal. To achieve this, create a non-gallery application to integrate your portal account with the Azure account through the Secure Cross-domain Identity Management (SCIM) feature. See the SCIM section in "Import Users and Groups for SAML" on page 40 for details and prerequisites.

1. Select **Azure Active Directory > Enterprise Applications**.
2. Create the SCIM app.
   a. Click **New Application**.
   b. Select **All** and click **Non-gallery application**.
3. If you already have Premium AD and Enterprise Mobility Suite licenses, proceed to Step 6.

   Otherwise, click **Get a premium...**.



Add your own application

Non-gallery application

Integrate any other application that you don't find in the gallery

Get a free Premium trial to use this feature

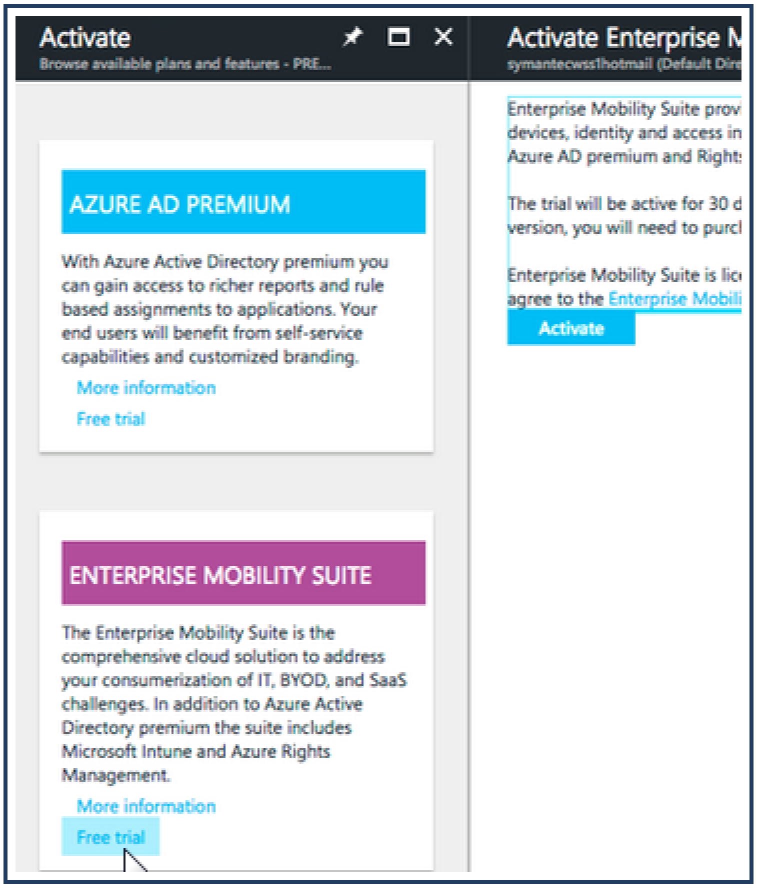
* Name

The display name for your new application

Adding custom applications requires Azure AD Premium. If you'd like to try it out, click the link at top to get started with trial.

Supports:

The Azure AD Premium and Enterprise Mobility Suite apps each have trial links. You must activate the ones you do not currently have.



Activate

Browse available plans and features - PRE...

AZURE AD PREMIUM

With Azure Active Directory premium you can gain access to richer reports and rule based assignments to applications. Your end users will benefit from self-service capabilities and customized branding.

More information

Free trial

ENTERPRISE MOBILITY SUITE

The Enterprise Mobility Suite is the comprehensive cloud solution to address your consumerization of IT, BYOD, and SaaS challenges. In addition to Azure Active Directory premium the suite includes Microsoft Intune and Azure Rights Management.

More information

Free trial

Activate Enterprise M

symantecwss1hotmail (Default Dire

Enterprise Mobility Suite prov
devices, identity and access in
Azure AD premium and Right:

The trial will be active for 30 d
version, you will need to purcl

Enterprise Mobility Suite is lic
agree to the Enterprise Mobili

Activate

4. Returning to the Add an Application screen, **Name** the application. For example, **symantecwss**.

   Click **Add** (bottom of screen).

5. Provision the WSS.

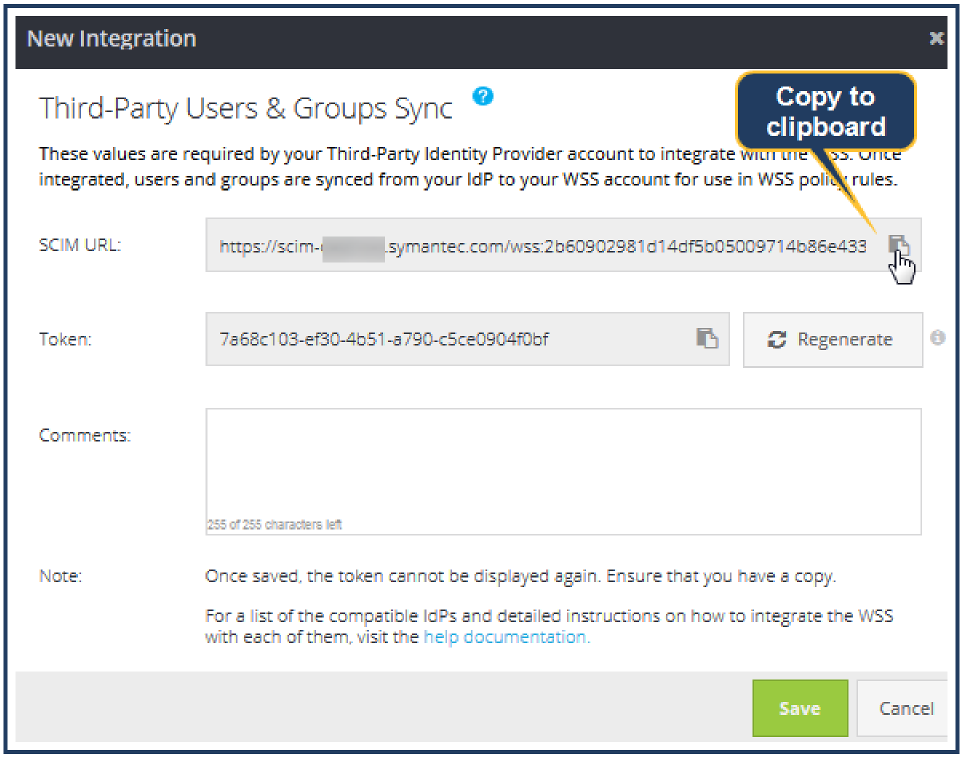
   a. Select **Provisioning**.

   b. From the **Provisioning Mode** drop-down list, select **Automatic**.

6. Back in the WSS portal, navigate to **Identity > SAML Authentication**.

   a. Expand the **SCIM Third-Party Users & Groups Sync** area.

   b. Click **Generate Integration Token**.



Third-Party Users & Groups Sync

These values are required by your Third-Party Identity Provider account to integrate with the WSS. Once integrated, users and groups are synced from your IdP to your WSS account for use in WSS policy rules.

SCIM URL: https://scim-[redacted].symantec.com/wss:2b60902981d14df5b05009714b86e433

Token: 7a68c103-ef30-4b51-a790-c5ce0904f0bf

Comments:

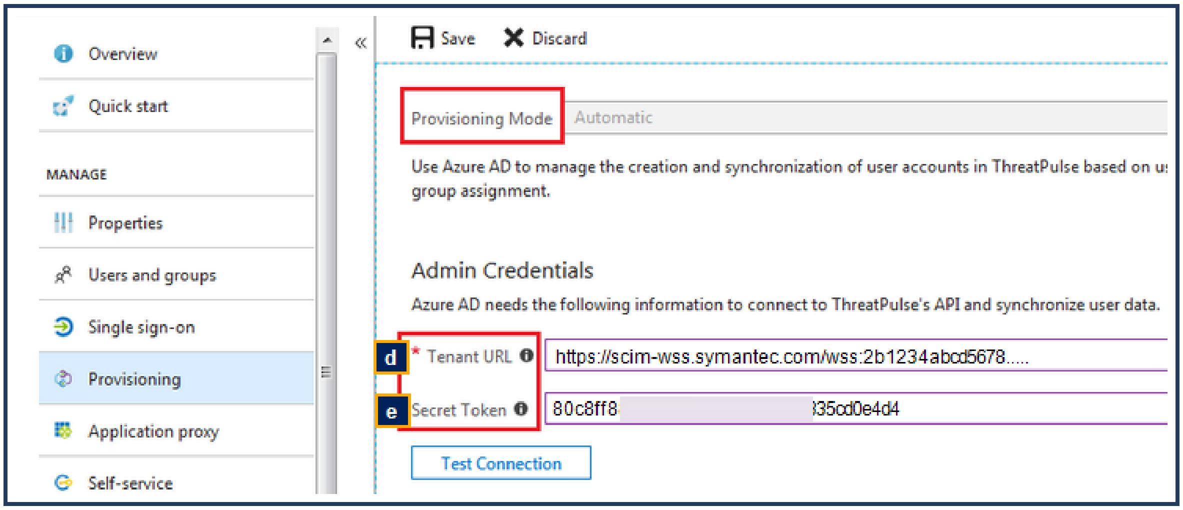
255 of 255 characters left

Note: Once saved, the token cannot be displayed again. Ensure that you have a copy.

For a list of the compatible IdPs and detailed instructions on how to integrate the WSS with each of them, visit the help documentation.

   c. The portal generates a unique **SCIM URL**. Click the Copy icon.

   d. Return to the Azure browser tab, **Admin Credentials** area.



Provisioning Mode: Automatic

Use Azure AD to manage the creation and synchronization of user accounts in ThreatPulse based on u: group assignment.

Admin Credentials

Azure AD needs the following information to connect to ThreatPulse's API and synchronize user data.

* Tenant URL: https://scim-wss.symantec.com/wss:2b1234abcd5678.....

Secret Token: 80c8ff8[redacted]35cd0e4d4

e. In the **Tenant URL field**, paste the SCIM URL.

f. Return to the WSS portal tab; copy the **Token**.

   In the Azure portal, paste into the **Secret Token** field.

7. Scroll to the **Settings** area.

   By default, **Provisioning Status** is set to **Off** and **Scope** is set to **Sync only assigned users and groups**.

   a. Set the **Provisioning Status** to **Off**.

   b. The **Scope** drop-down list presents two options:

      - **Sync all users and groups**

      - **Sync only assigned users and groups**—If you select this option, go to the following link to assist with ensuring you select which users and groups are synced to OSIAM.

        https://docs.microsoft.com/en-us/azure/active-directory/application-access-assignment-how-to-add-assignment

8. In the **Admin Credentials** area, click **Test Connection**. If successful, the Azure portal displays the following message: **The supplied credentials are authorized to enable provisioning**.

   If the test fails, try generating a new SCIM URL and token.

> **Tip:** In the WSS portal, navigate **Identity > Users & Groups**. On the Third-**Party Users and Groups** tab you can see how many Users and Groups were imported in the most recent sync operation.

Step 8—Limit the synced attributes to the minimum required set.

For network efficiency, you can limit the synced attributes; the WSS does not receive data it does not require for this feature.

1. Remaining on the **Provisioning** page, in the **Mappings** area click **Synchronize Azure Active Directory Groups to customappsso**.

2. In the Attribute Mapping dialog, delete all attributes *except* for **displayName**.

3. Click **Save**; click **Save** in the confirmation dialog.

   The Azure portal displays successful message in the upper-right of the screen.

4. Return to the **Provisioning > Mappings** area and select **Synchronize Azure Active Directory Users to customappsso**.

5. Delete all attributes *except* for **externalId**, **active**, and **userName**.

   > **Tip:** If deleting the **name.formatted** attribute causes a `SchemaInvalid` error when you try to save, include **name.formatted** to the list of attributes to keep and re-save.

6. Click **Save**; click **Save** in the confirmation dialog.

   The Azure portal displays successful message in the upper-right of the screen.

7. Click **Save**.

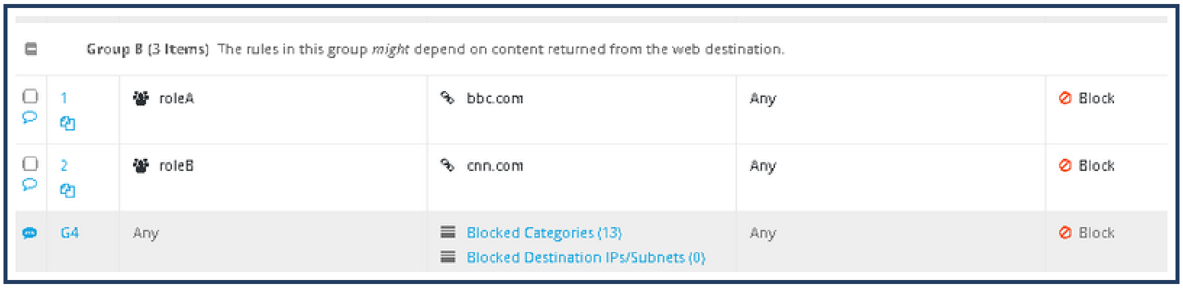
Synchronization

When you start the initial synchronization, it can take on the average of 15 to 45 minutes before Azure begins to send data to the WSS. Subsequent synchronizations require less time.

In the WSS portal, navigate to **Identity > SAML Authentication > Users and Groups > Third-Party Sync**. This page displays all of the users and groups provided by the IdP.

Policy

The various policy editors now include the group information as configured in Azure. You can select them and define group-based policies.



Group B (3 Items) The rules in this group *might* depend on content returned from the web destination.

□	1	roleA	bbc.com	Any	Block
□	2	roleB	cnn.com	Any	Block
	G4	Any	Blocked Categories (13) Blocked Destination IPs/Subnets (0)	Any	Block

In the above example, the policies to block **roleA** and **roleB** block all users who belong to groups that have been assigned as either **roleA** or **roleB** in their Azure Web Security Service SAML application.

(Optional) Rebrand Login Page

You can configure Azure to display the credential challenge to employees with the colors and logo of your company. If you do not opt to do so, employees receive the default Microsoft log in page. The follow Microsoft topic provides the procedure.

- Azure Rebrand Topic

Exemptions

Optional–Exempt Sources/Destinations from Authorization

SAML and Captive Portal authentication methods use *re-directions*. Some network environments might not be compatible, which requires you to bypass sources or destinations to ensure client operations. Or you might have other reasons to bypass.

- See "Exempt From Authentication" on page 126.

✓ Next Step

- As authenticated user traffic begins to come in, verify the success of the integration. In **Solutions** mode, generate user-based reports and verify that they display expected authenticated employee names.
- Decide whether or not further authentication policy is required. "Authentication Location Policy" on page 119.
- "Import Users and Groups for SAML" on page 40.

Alternate Media

Microsoft created a documentation topic that demonstrates the integration.

https://docs.microsoft.com/en-us/azure/active-directory/active-directory-saas-symantec-tutorial

Integrate Okta as the SAML IdP

If you want to use Security Assertion Markup Language (SAML) authentication for the Web Security Service, but do not have your own Active Directory (AD) deployed, you can provision Okta as the SAML Identity Provider (IdP).

WSS supports the automatic synchronization of users and groups through the use of an integration token (described in the following procedure).

Technical Requirements

- Port `8443` is required for browsers to post SAML assertions to a WSS asset. Verify that this port is open on your gateway firewall devices.
- To prevent browser looping, add the IdP lookup URL(s) to the Authentication Bypass list.
  - `op1static.oktacdn.com`
  - `okta.com`
  - `oktacdn.com`

  See "Exempt From Authentication" on page 126.
- This integration requires admin privileges on the Okta account. If you do not have an account, you can begin with the free Okta Developer Edition.

  https://developer.okta.com/signup/
- The procedure includes a step involving the Secure Cross-domain Identity Management (SCIM) feature.

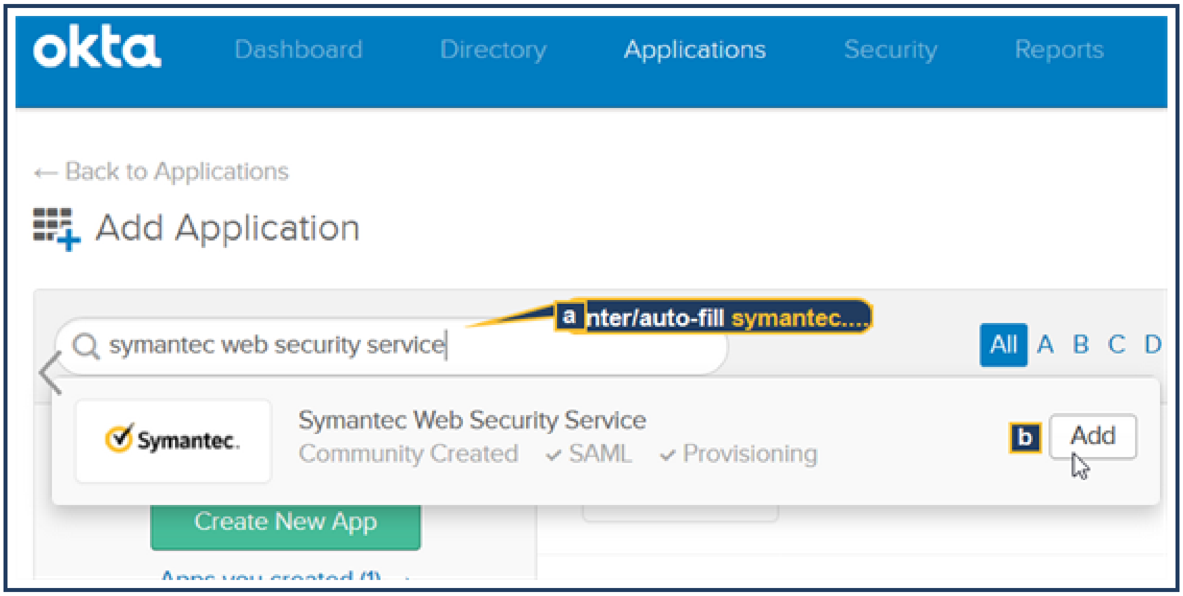
  See the SCIM section in "Import Users and Groups for SAML" on page 40 for details and prerequisites.

Procedure

Step 1—Add the Symantec WSS App

1. Log in, with Admin privileges, to your Okta organization account.
   a. Click **Classic UI**.
   b. In the top-menu, click **Applications**.
2. Add the Symantec app.

a. Click **Add Application**.


okta
Dashboard
Directory
Applications
Security
Reports
← Back to Applications
Add Application
symantec web security service
a nter/auto-fill symantec....
All A B C D
Symantec.
Symantec Web Security Service
Community Created ✓ SAML ✓ Provisioning
b Add
Create New App

b. Use the auto-fill search field to locate the **Symantec Web Security Service** app.

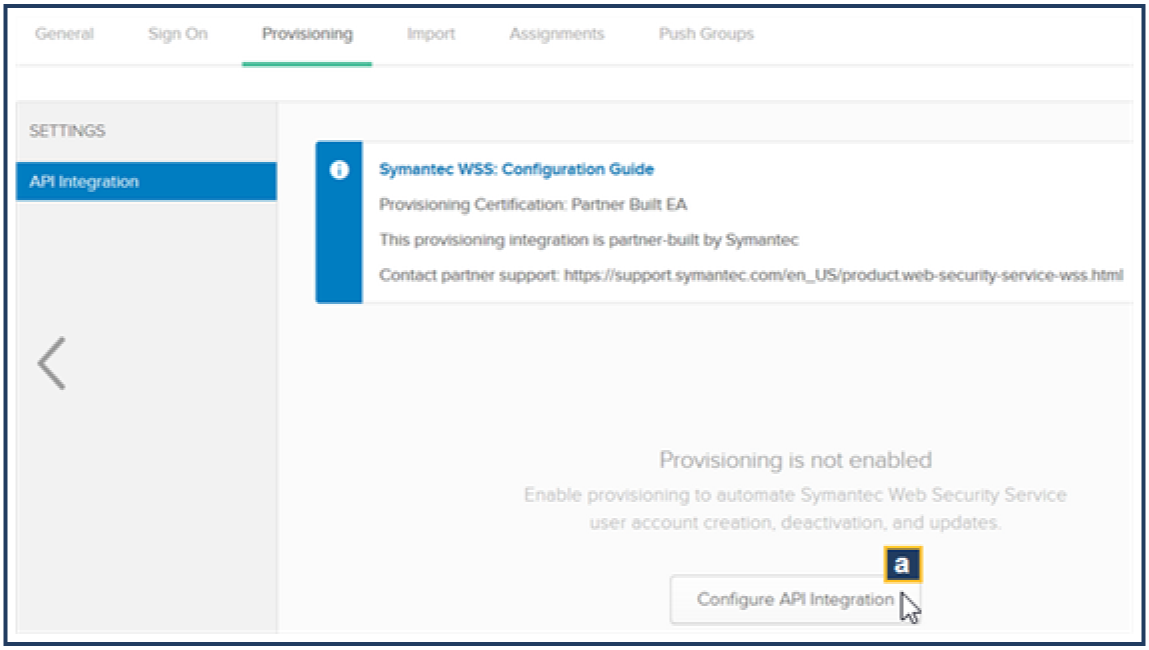
c. Click **Add**.

d. On the Add Symantec Web Security Service page, click **Done**.

Step 2–Configure Automatic User/Group Population in WSS.

Provision your Okta account to manage users and groups within the Okta portal yet have them automatically sync to the WSS portal (SCIM feature).

1. In Okta, click **Provisioning** on the application menu.



Symantec WSS: Configuration Guide

Provisioning Certification: Partner Built EA

This provisioning integration is partner-built by Symantec

Contact partner support: https://support.symantec.com/en_US/product.web-security-service-wss.html

Provisioning is not enabled

Enable provisioning to automate Symantec Web Security Service user account creation, deactivation, and updates.

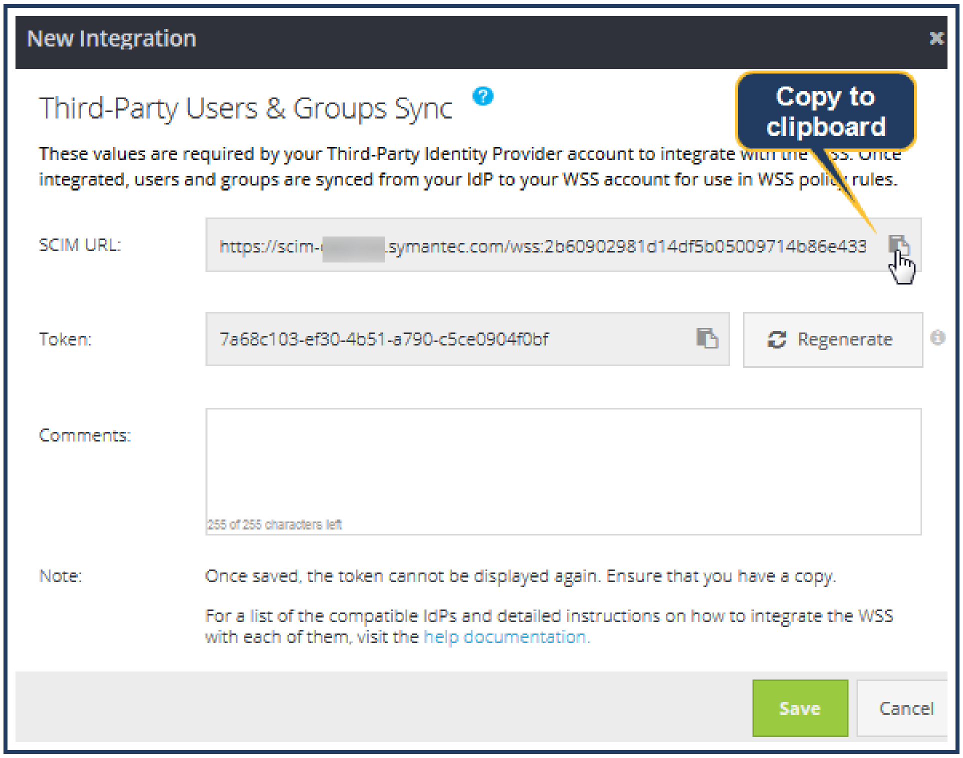
   a. Click **Configure API Integration**.

   b. Select **Enable API Integration**.

2. In the WSS portal, navigate to **Identity > SAML Authentication**.

   a. Expand the **Third-Party Users & Groups Sync** area.

   b. Click **View Integration Credentials**.



New Integration

Third-Party Users & Groups Sync

These values are required by your Third-Party Identity Provider account to integrate with the WSS. Once integrated, users and groups are synced from your IdP to your WSS account for use in WSS policy rules.

SCIM URL: https://scim-[redacted].symantec.com/wss:2b60902981d14df5b05009714b86e433

Token: 7a68c103-ef30-4b51-a790-c5ce0904f0bf

Comments:

255 of 255 characters left

Note: Once saved, the token cannot be displayed again. Ensure that you have a copy.

For a list of the compatible IdPs and detailed instructions on how to integrate the WSS with each of them, visit the help documentation.

c. The portal generates a unique **SCIM URL**. Click the Copy icon.

d. Return to the Okta browser tab API Integrations screen.

e. In the **Base URL** field, paste the SCIM URL.

f. Return to the WSS portal tab; copy the **Token**.

   In the Okta tab, paste into the **API Token** field.

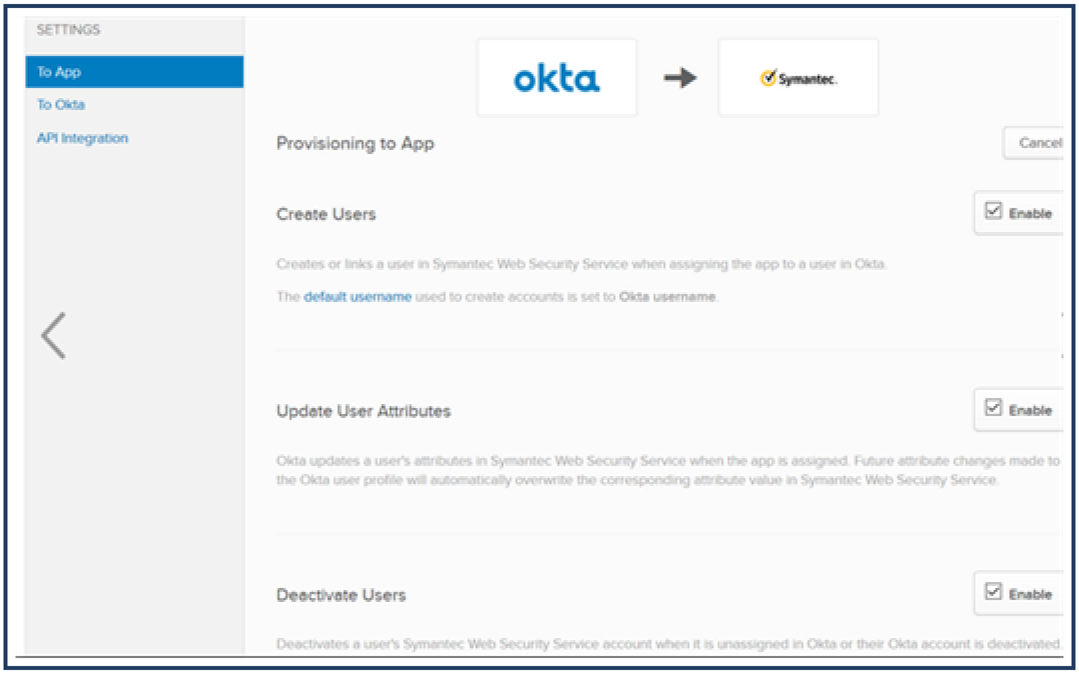
g. Click **Test API Credentials**.

   - If successful, the Okta portal displays the following message: **Symantec Web Security Service was verified successfully!**.
   - If the test fails, try generating a new token.

h. Click **Save**.

3. On the **Provisioning** tab, select **To App** from the **Settings** menu.

4. Click **Edit**.



Provisioning to App

Create Users ☑ Enable

Creates or links a user in Symantec Web Security Service when assigning the app to a user in Okta.

The default username used to create accounts is set to Okta username.

Update User Attributes ☑ Enable

Okta updates a user's attributes in Symantec Web Security Service when the app is assigned. Future attribute changes made to the Okta user profile will automatically overwrite the corresponding attribute value in Symantec Web Security Service.

Deactivate Users ☑ Enable

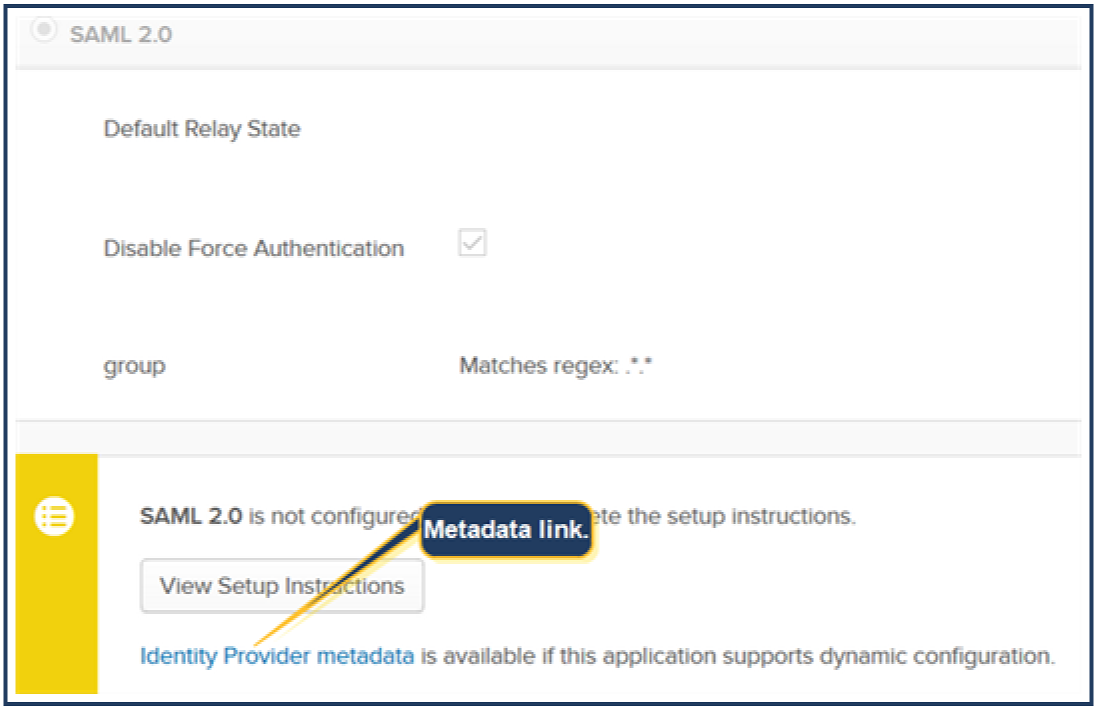
Deactivates a user's Symantec Web Security Service account when it is unassigned in Okta or their Okta account is deactivated.

a. Select **Create Users**, **Update User Attributed**, and **Deactivate Users**.

b. Click **Save**.

Step 3-Federate the Web Security Service.

1. Save the Okta metadata.



○ SAML 2.0

Default Relay State

Disable Force Authentication ☑

group Matches regex: .*.*

SAML 2.0 is not configured ... ete the setup instructions.

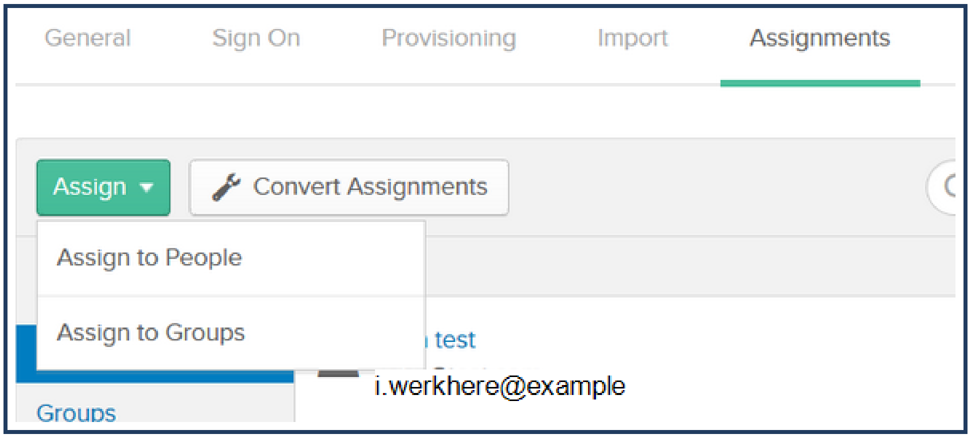
Identity Provider metadata is available if this application supports dynamic configuration.

a. In Okta, navigate to the Web Security Service app **Sign On** tab.

b. Click the **Identity Provider metadata** link and save the file to an accessible location. You or the admin will need to access to configure the WSS.

2. Assign the users and groups to the app.

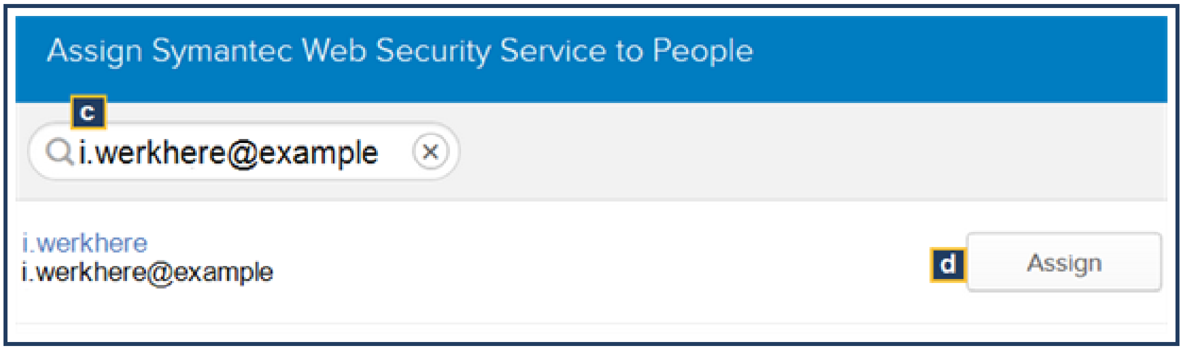
a. In the WSS app, click **Assignments**.

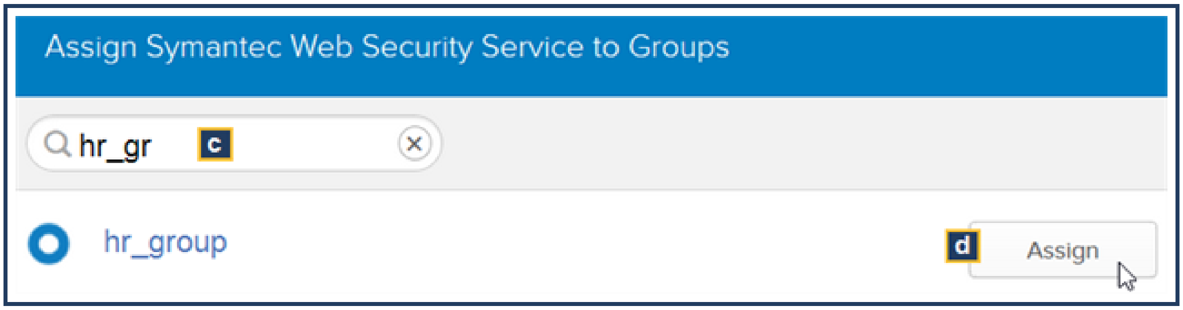


b. From the **Assign** drop-down list, select one of the following.

- **Assign to People** for individual use names;
- **Assign to Groups** to add group names.

c. Search for users and groups to add.





d. Click **Assign**.

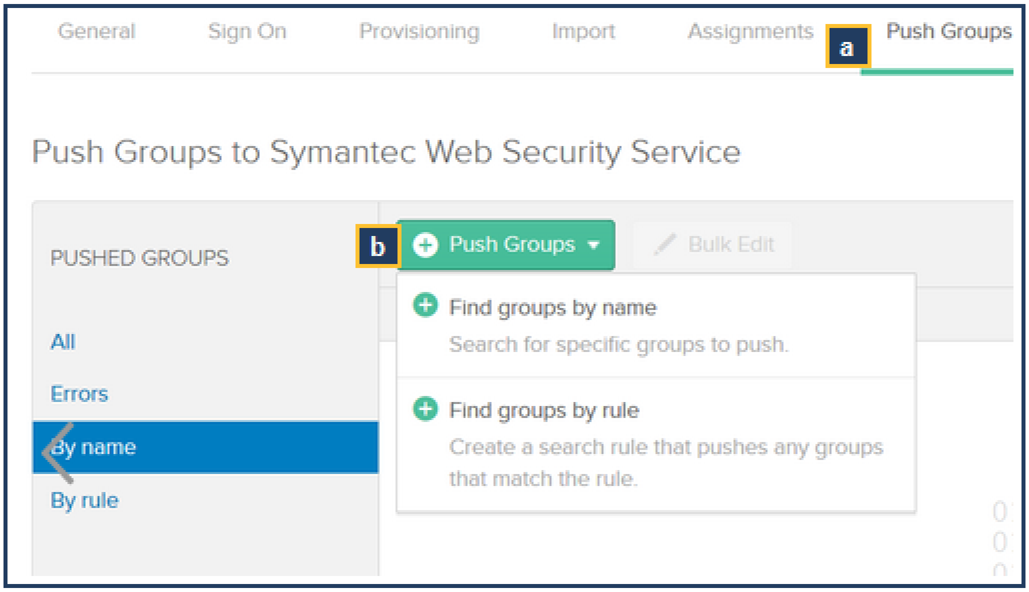
The portal displays a dialog for each user or group; each contains attributes. You can modify the group information.

e. Click **Save and Go Back**.

f. Repeat for remaining users and groups, as required.

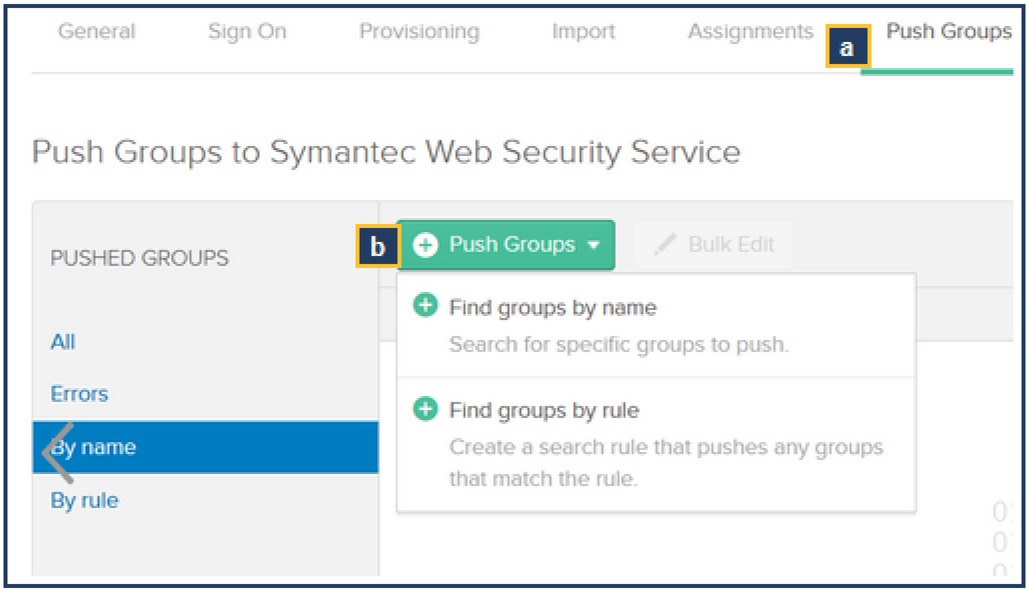
3. Push group data.

a. In the WSS app, click **Push Groups**.

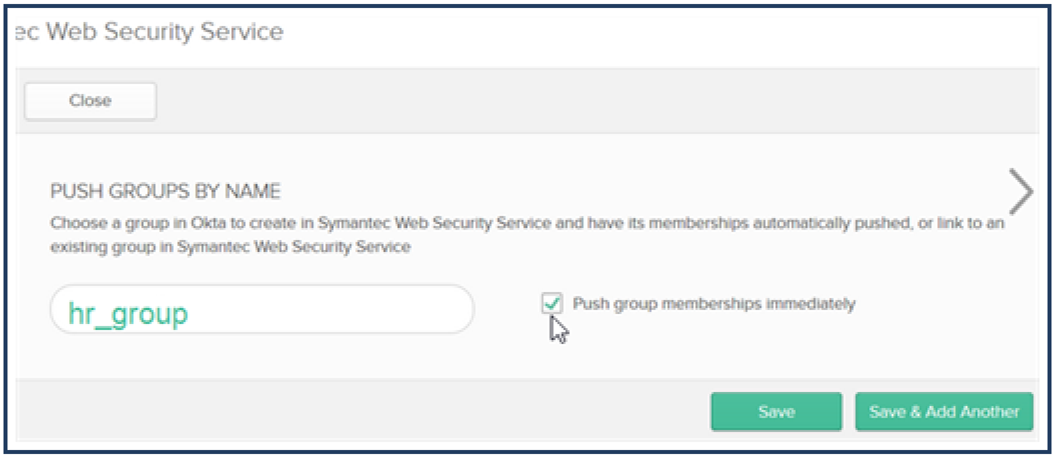


b. Select **Find groups by name** from the **Push Groups** menu.

c. Select your groups.



d. Select your groups.



PUSH GROUPS BY NAME

Choose a group in Okta to create in Symantec Web Security Service and have its memberships automatically pushed, or link to an existing group in Symantec Web Security Service

hr_group

☑ Push group memberships immediately

Verify that **Push group memberships immediately** is enabled.

e. Click **Save** when complete or **Save & Add Another** to repeat.

The **Push Status** column displays **Active** for each pushed group.

4. Return to the WSS portal.

   a. Navigate to **Identity > SAML Authentication**.

   b. Expand the **SAML Authentication** area.

   c. Click **Import Metadata**; navigate to the saved Okta metadata and import. The portal populates the **Entity ID**, **Endpoint URL**, and **Signing Certificate** fields.

   d. Select **Post Endpoint**.

e. In the **Group Attribute** field, enter **group**.

f. Click **Save**.

Test Step

To perform an immediate configuration validation, you can explicitly proxy a browser of a client on the network to the WSS.

1. In the WSS portal, add a location **(Connectivity > Locations)**; name it SAML Okta Test, for example.

   a. Set to **Explicit Proxy**.

   b. **Save** the location.

2. Navigate to **Identity > Authentication Policy**.

   a. Click **Add Rule** and select **Explicit Proxy Locations**. The WSS displays the New Rule page.

   b. Click **Add Sources** and add the Explicit Proxy **Location**.

3. In the **Verdict** area,

   a. Enable **Captive Portal**.

   b. Select **SAML**.

4. Click **Add Rule**; click **Activate**.

5. Log in to the test client machine and configure the browser proxy settings to `proxy.threatpulse.net:8080`.

6. Restart the browser. If you see the Okta sign-in page, the SAML deployment is functioning.

   If not, retrace the configuration steps.

   If you encounter connection problems, see "Troubleshoot SAML Authentication" on page 130 for possible causes and resolutions.

Known Issue

If you rename a group, Okta does not sync the modified group name and the **Push Status** for the group becomes **Inactive**. Attempt the following workaround.

1. Click **Inactive** and click **Unlink published group**.

2. In the Unlink Pushed Group dialog, ensure that **Delete the group in the target app (recommended)** is selected and click **Unlink**. This deletes the group in the WSS app's push list and the WSS portal.

3. Click **Push Groups**. You can **Find** groups by name.

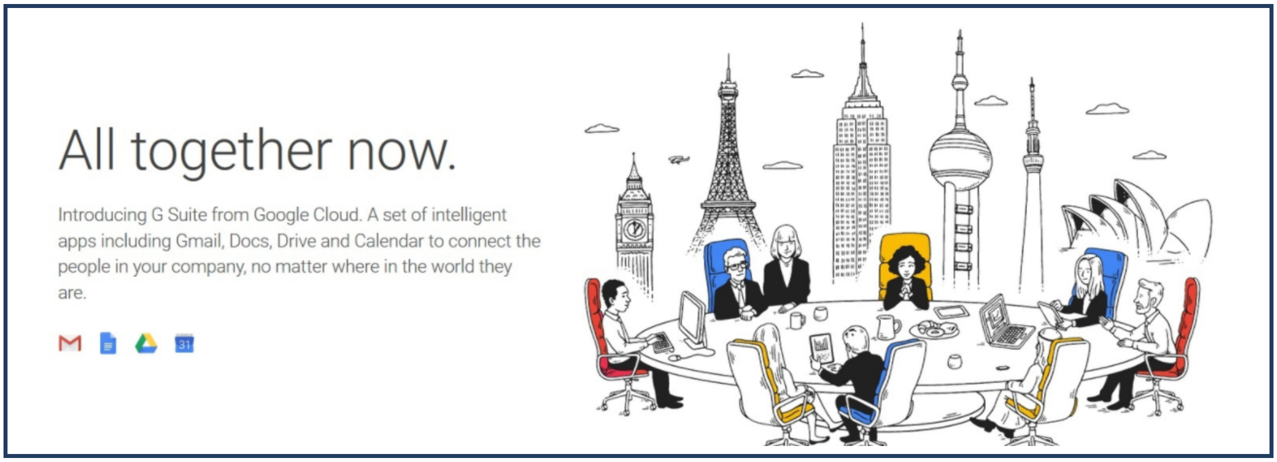
4. Search and select the modified group. Ensure that **Push group memberships immediately** is selected and click **Save**.

Next Steps

- As authenticated user traffic begins to come in, verify the success of the integration. In **Solutions** mode, generate user-based reports and verify that they display expected authenticated employee names.
- Decide whether or not further authentication policy is required. "Authentication Location Policy" on page 119.

Integrate Google G Suite as a SAML IdP

If you want to use Security Assertion Markup Language (SAML) authentication for the Web Security Service, but do not have your own Active Directory (AD) deployed, you can provision Google® G Suite™ as your company's SAML Identity Provider (IdP).



All together now.

Introducing G Suite from Google Cloud. A set of intelligent apps including Gmail, Docs, Drive and Calendar to connect the people in your company, no matter where in the world they are.

> **Tip:** For details on the benefits of using G Suite for your organization's authentication and cloud application needs, refer to the Google G Suite site.

Technical Requirements

- Before you can configure SAML authentication with Google G Suite to authenticate your WSS users, you must have the following.
  - A Google G Suite account
  - A domain name

  Google provides a free trial for all G Suite accounts, and offers domain name registration services. Google offers a support FAQ page for details on this choice here: **https://support.google.com/a/answer/53926?hl=en**.
- To prevent browser looping, add the IdP lookup URL(s) to the Authentication Bypass list: `accounts.google.com`.

  See "Exempt From Authentication" on page 126.

Procedure

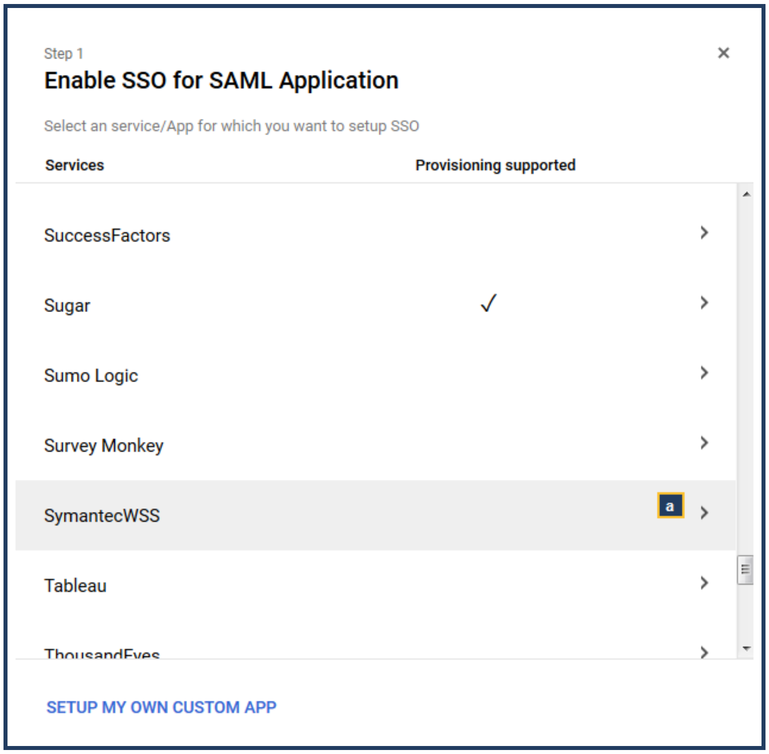
Google G Suite Registration

Register for the G Suite service. If you already have a Google G Suite account, proceed to Google G Suite SAML Configuration.

1. Browse to **https://gsuite.google.com**, and click **Get Started**.
2. Provide a contact email address. As this is used for all account activity going forward, avoid using a personal account.
3. If you your organization has a domain name, click **Yes, I Have One I Can Use** and enter it into the field provided. If your organization does not yet have a domain name, and would like to use Google's domain name registration services, click **No, I Need One**.
4. Using the domain name entered above, enter new user details for an email address you will use to administer your G Suite account. For example, `admin@myexample.com`. Define a password for the new account and click **Next** to proceed to **Add Domain Registration**.
5. Follow the remaining prompts to complete your account and domain registration.

Google G Suite SAML Configuration

1. Log in to the G Suite administration console at `https://admin.google.com`.
2. Click **SAML**, then click the plus (**+**) icon in the bottom-right of the page. The interface displays **Enable SSO for SAML Application** .
3. Scroll down the list of SAML Applications and locate **Symantec WSS**.



Step 1

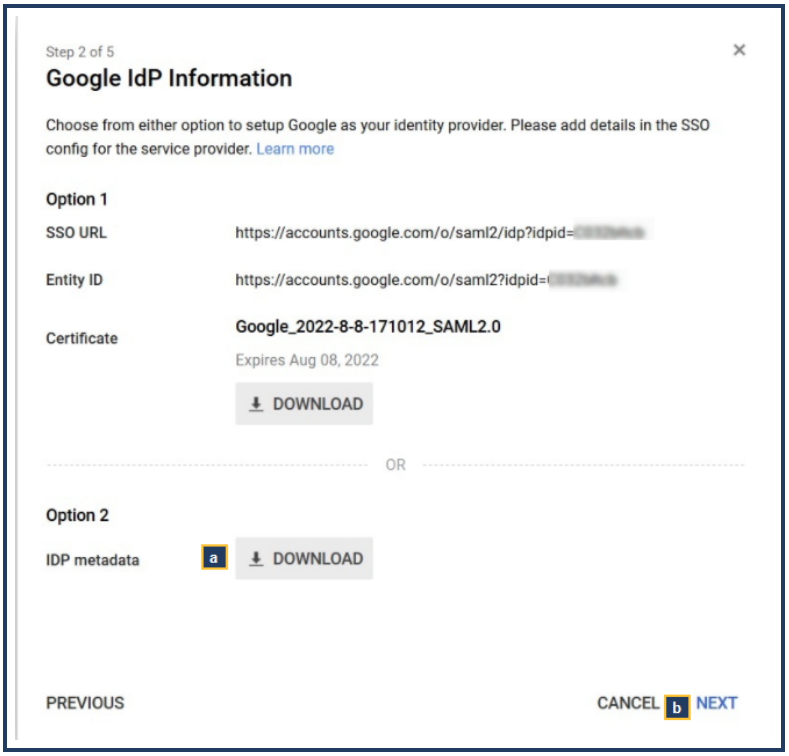
Enable SSO for SAML Application

Select an service/App for which you want to setup SSO

Services	Provisioning supported
SuccessFactors	
Sugar	✓
Sumo Logic	
Survey Monkey	
SymantecWSS	
Tableau	
ThousandEyes	

Click the arrow on the right of the SymantecWSS line.

4. The interface displays the **Google IdP** dialog.



Step 2 of 5

Google IdP Information

Choose from either option to setup Google as your identity provider. Please add details in the SSO config for the service provider. Learn more

Option 1

SSO URL https://accounts.google.com/o/saml2/idp?idpid=[redacted]

Entity ID https://accounts.google.com/o/saml2?idpid=[redacted]

Certificate Google_2022-8-8-171012_SAML2.0

Expires Aug 08, 2022

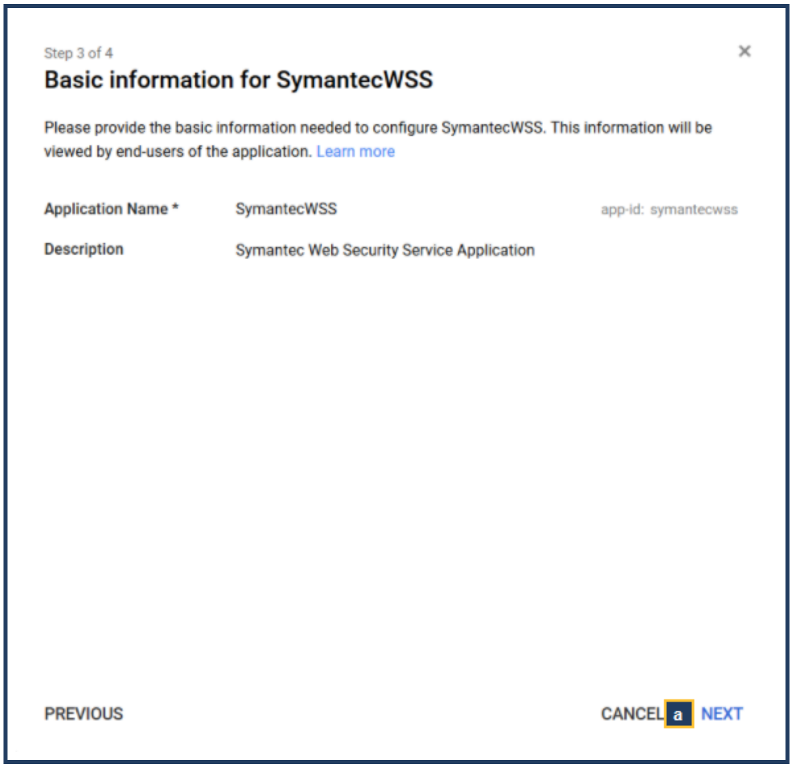
Option 2

IDP metadata

a. Click **Download** under **Option 2** to save the Google Identity Provider (IdP) file. This file is used later in the WSS portal to complete the association with Google.

b. Click **Next**.

5. Confirm basic information for your new SAML application.



Step 3 of 4

Basic information for SymantecWSS

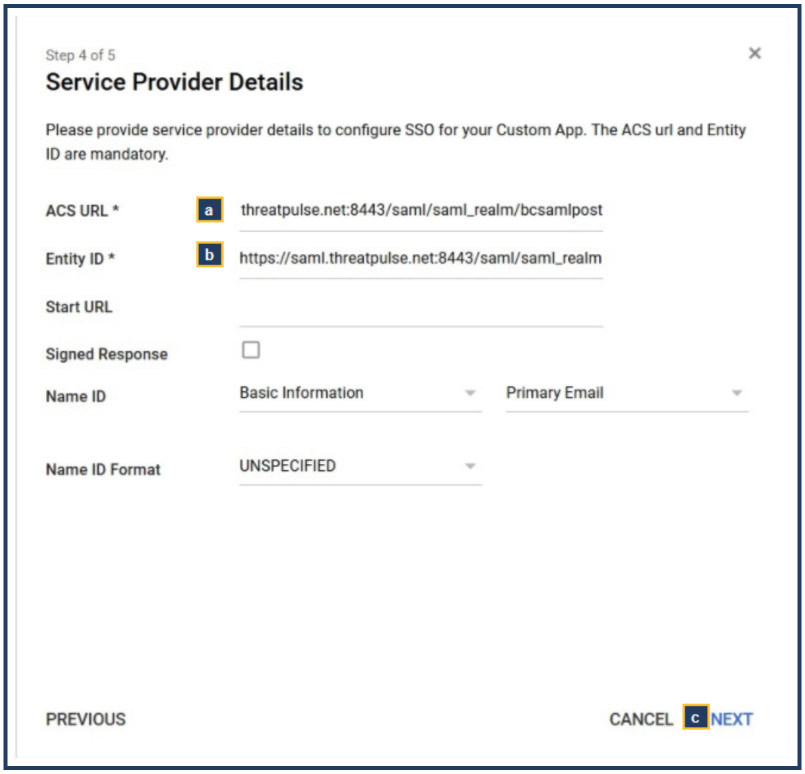
Please provide the basic information needed to configure SymantecWSS. This information will be viewed by end-users of the application. Learn more

Application Name * SymantecWSS app-id: symantecwss

Description Symantec Web Security Service Application

Confirm that the page displays the same information as the above image, and click **Next**.

6. Define the Symantec WSS details:



Step 4 of 5

Service Provider Details

Please provide service provider details to configure SSO for your Custom App. The ACS url and Entity ID are mandatory.

ACS URL * threatpulse.net:8443/saml/saml_realm/bcsamlpost

Entity ID * https://saml.threatpulse.net:8443/saml/saml_realm

Start URL

Signed Response □

Name ID Basic Information Primary Email

Name ID Format UNSPECIFIED

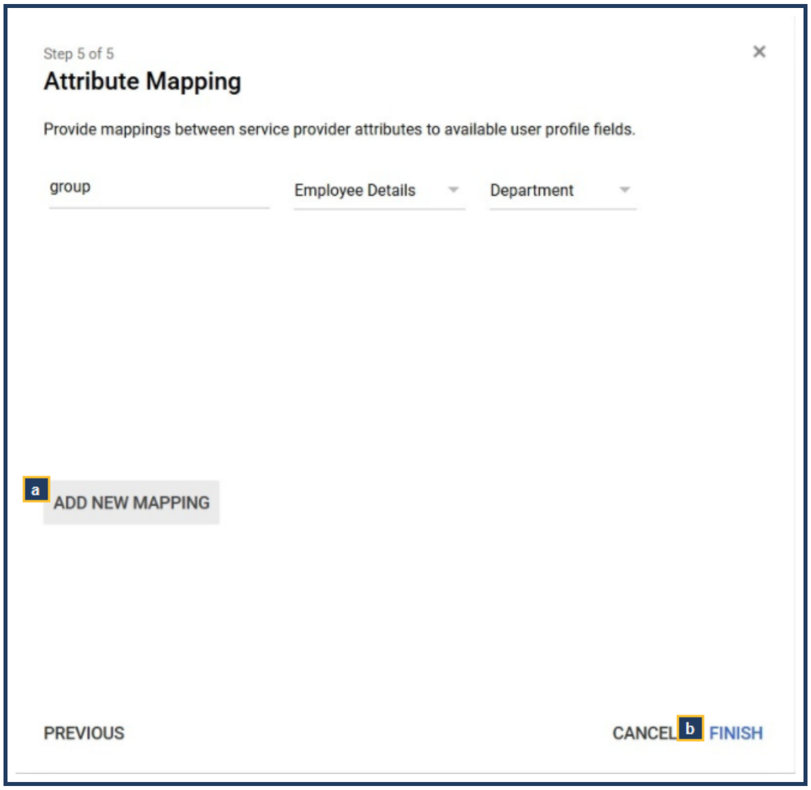
a. ACS URL: **threatpulse.net:8443/saml/saml_realm/bcsamlpost**

b. Entity ID: **https://saml.threatpulse.net:8443/saml/saml_realm**

c. You can leave other fields in their default state. Click **Next**.

7. Define the user and group identifiers for authentication.

   The group definitions that may currently exist in your WSS configuration cannot be imported to the G Suite authentication service. This page allows you to map group attributes to the Department group.



Step 5 of 5

Attribute Mapping

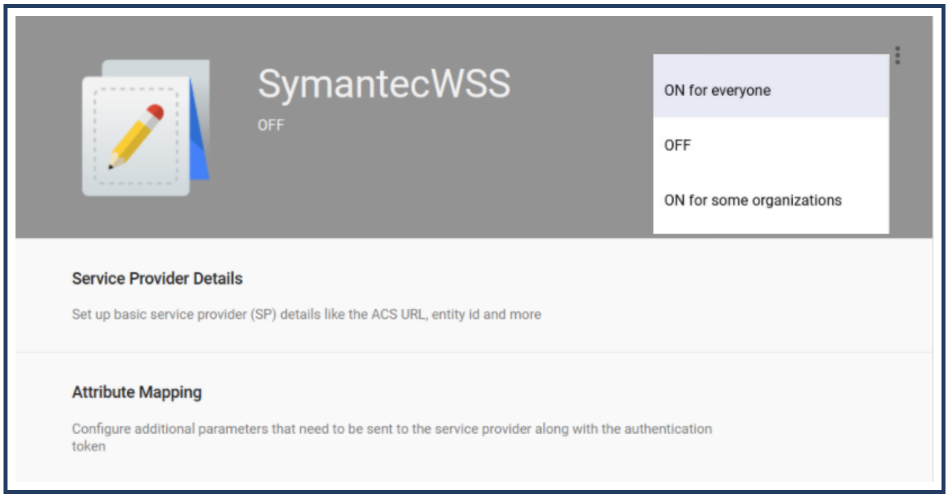
Provide mappings between service provider attributes to available user profile fields.

group | Employee Details | Department

a. Click **Add New Mapping** to use the **Department** field as the user group. The groups defined here as Departments can be used in WSS group policy.

b. Click **Finish**.

8. After you complete the G Suite application setup wizard, G Suite displays a settings page.


SymantecWSS

OFF

ON for everyone

OFF

ON for some organizations

Service Provider Details

Set up basic service provider (SP) details like the ACS URL, entity id and more

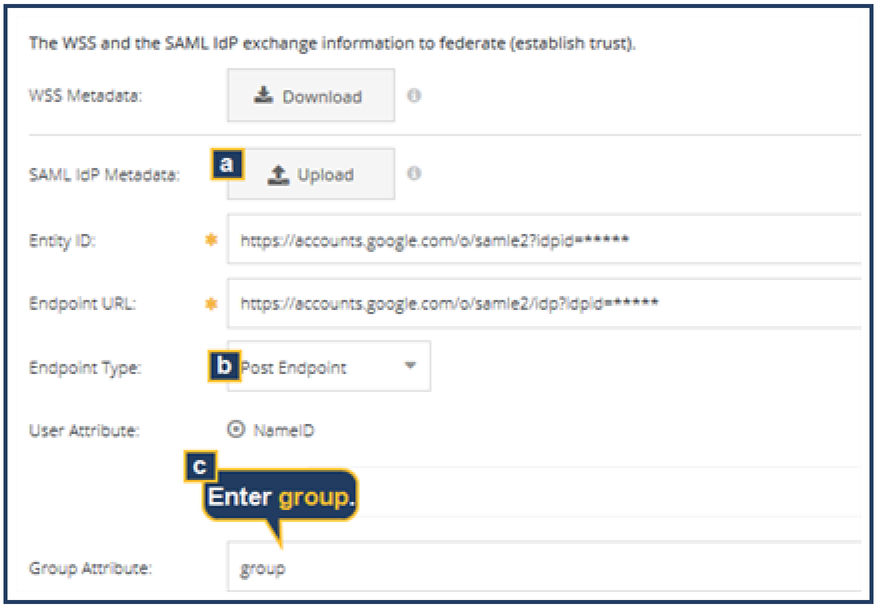
Attribute Mapping

Configure additional parameters that need to be sent to the service provider along with the authentication token

Click the three dot menu in the top right and select **ON for everyone** to enable SAML authentication for all users.

Federate G Suite With the Web Security Service Portal

1. Log in to the WSS portal and navigate to **Identity > SAML Authentication**.
2. Expand the **SAML Authentication** area.


The WSS and the SAML IdP exchange information to federate (establish trust).

WSS Metadata: Download

SAML IdP Metadata: Upload

Entity ID: * https://accounts.google.com/o/saml2?idpid=*****

Endpoint URL: * https://accounts.google.com/o/saml2/idp?idpid=*****

Endpoint Type: Post Endpoint

User Attribute: ● NameID

Group Attribute: group

a. Click **Upload**; browse to the saved Ping certificate file saved in the previous step and open it. The portal populates the **Entity ID**, **Endpoint URL**, and **Signing Certificate** fields.

b. From the **Endpoint Type** drop-down list, select **Post Endpoint**.

c. In the **Group Attribute** field, enter **group**.

d. Click **Save**.

Test Step

To perform an immediate configuration validation, you can explicitly proxy a browser of a client on the network to the WSS.

1. In the WSS portal, add a location **(Connectivity > Locations)**; name it SAML Google Test, for example.
   a. Set to **Explicit Proxy**.
   b. **Save** the location.
2. Navigate to **Identity > Authentication Policy**.
   a. Click **Add Rule** and select **Explicit Proxy Locations**. The WSS displays the New Rule page.
   b. Click **Add Sources** and add the Explicit Proxy **Location**.
3. In the **Verdict** area,
   a. Enable **Captive Portal**.
   b. Select **SAML**.
4. Click **Add Rule**; click **Activate**.
5. Log in to the test client machine and configure the browser proxy settings to `proxy.threatpulse.net:8080`.
6. Restart the browser. If you see the Google G Suite sign-in page, the SAML deployment is functioning.

   If not, retrace the configuration steps.

   If you encounter connection problems, see "Troubleshoot SAML Authentication" on page 130 for possible causes and resolutions.

✓ Next Step

- As authenticated user traffic begins to come in, verify the success of the integration. In **Solutions** mode, generate user-based reports and verify that they display expected authenticated employee names.
- Decide whether or not further authentication policy is required. "Authentication Location Policy" on page 119.
- "Import Users and Groups for SAML" on page 40.
- "Exempt From Authentication" on page 126.

Integrate Ping Identity as the SAML IdP

If you want to use Security Assertion Markup Language (SAML) authentication for the Web Security Service, but do not have your own Active Directory (AD) deployed, you can provision Ping Identity® as the SAML Identity Provider (IdP).

Technical Requirements

- Port `8443` is required for browsers to post SAML assertions to a WSS asset. Verify that this port is open on your gateway firewall devices.
- Ping Identity admin credentials.
- To prevent browser looping, add the IdP lookup URL(s) to the Authentication Bypass list.
  - `sso.connect.pingidentity.com`
  - `login.pingone.com`

  See "Exempt From Authentication" on page 126.

Procedure

Step1—Setup Ping Identity for SAML

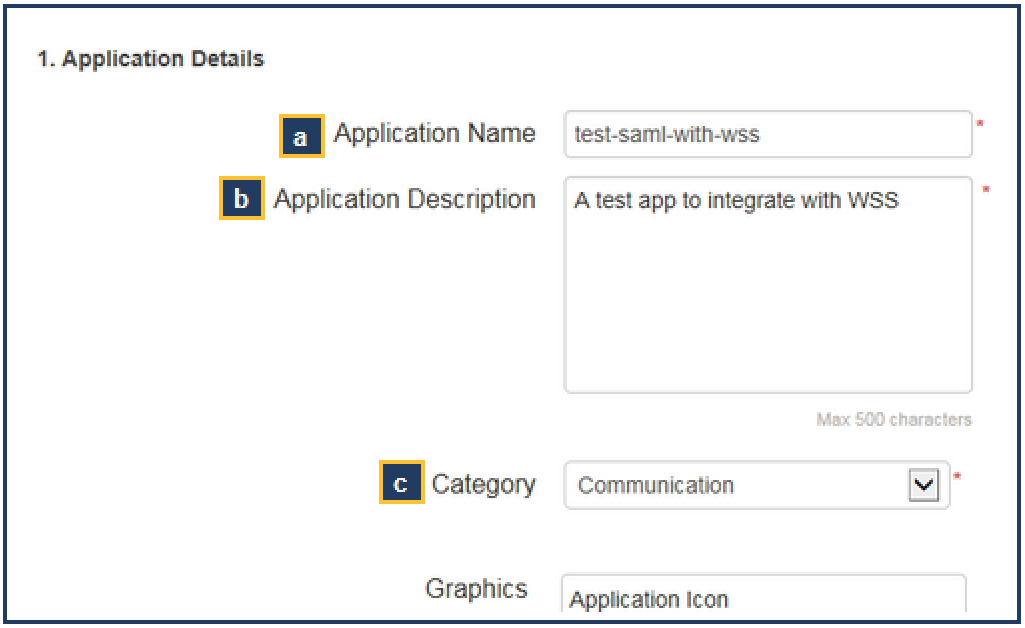
In the first phase, set up SAML authentication in the Ping Identity console.

1. Log in to Ping Identity.

   https://admin.pingone.com/web-portal/login

2. Add a SAML application.
   a. Select **Applications > My Applications**.
   b. From the **Add Application** drop-down list, select **New SAML Application**.

3. Complete area **1**, which identifies the **Application Details**.



1. Application Details

Application Name: test-saml-with-wss *

Application Description: A test app to integrate with WSS *

Max 500 characters

Category: Communication *

Graphics: Application Icon

a. Name the application.

b. (Recommended) Enter a **Description** for this application.

c. From the **Category** drop-down list, select **Communication**.

d. Click **Continue to Next Step**.

Step 2–Federate with the WSS

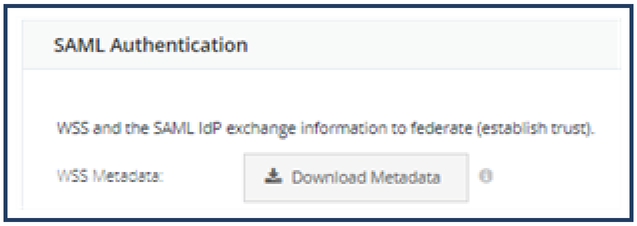
Enable the two services to communicate.

1. Log in to your WSS portal.

2. Navigate to **Identity > SAML Authentication**.

   a. Expand the **SAML Authentication** area.

   b. Click **Download Metadata** area.



SAML Authentication

WSS and the SAML IdP exchange information to federate (establish trust).

WSS Metadata:

   c. Open the download (browser) and view the contents.

   d. Record the following values (for example, copy to Notepad).

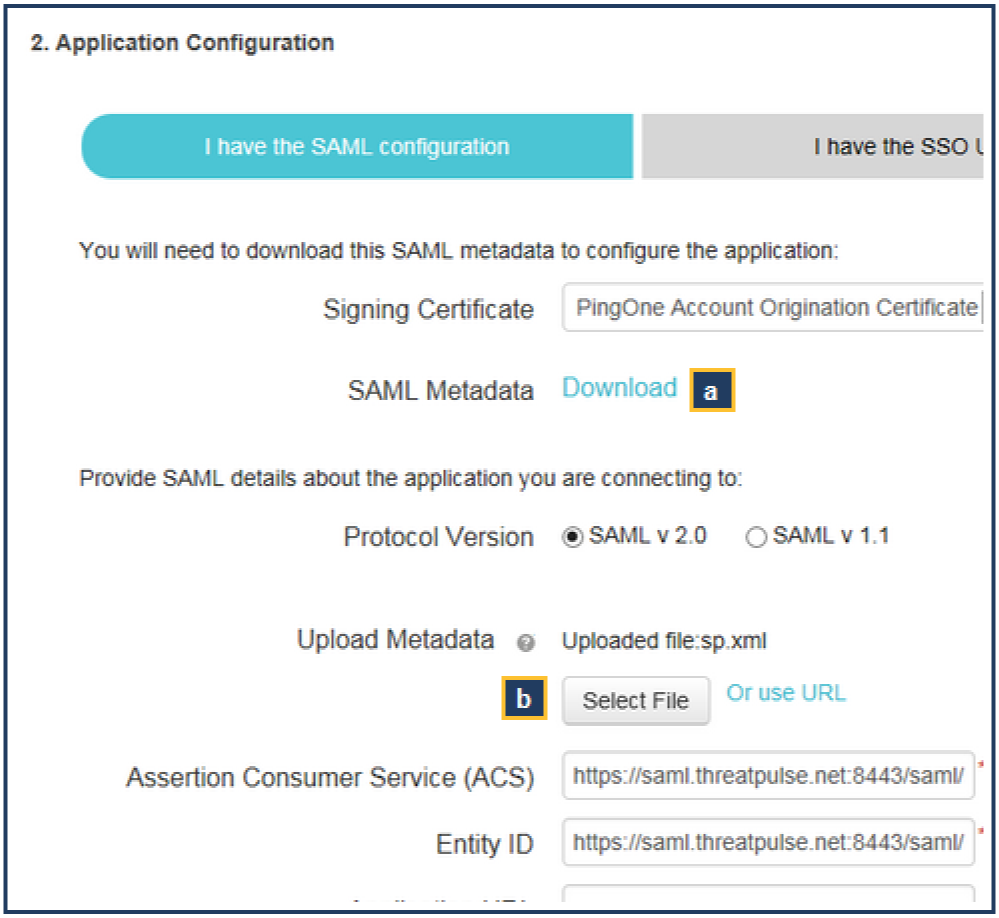
- The `EntityDescriptor`—

  `https://saml.threatpulse.net:8443/saml/saml_realm`

- The `AssertionConsumerService Location`—

  `https://saml.threatpulse.net:8443/saml/saml_realm/bcsamlpost`

3. Return to Ping Identity and continue with area **2** of the SAML application: **Application Configuration**.



2. Application Configuration

You will need to download this SAML metadata to configure the application:

Signing Certificate: PingOne Account Origination Certificate

SAML Metadata: Download

Provide SAML details about the application you are connecting to:

Protocol Version: ● SAML v 2.0 ○ SAML v 1.1

Upload Metadata: Uploaded file:sp.xml

Assertion Consumer Service (ACS): https://saml.threatpulse.net:8443/saml/

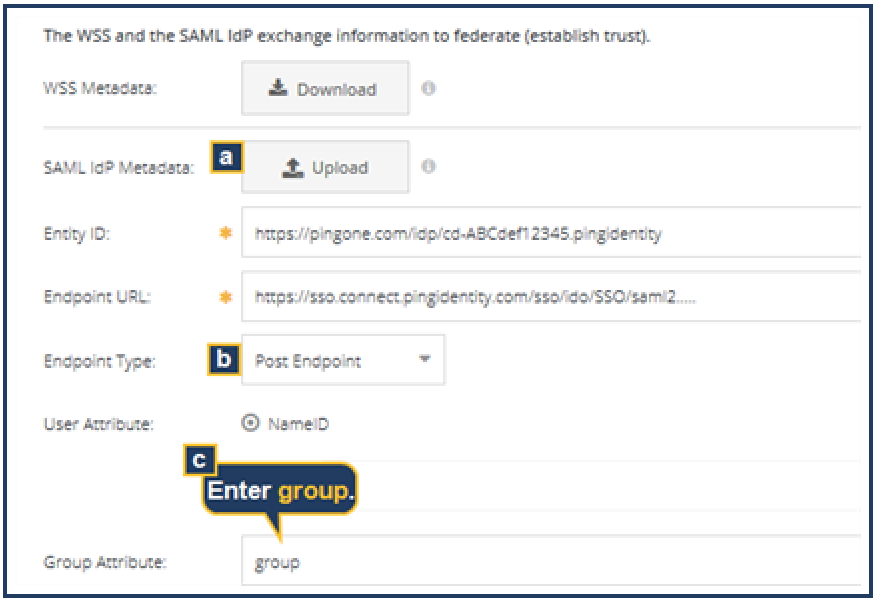
Entity ID: https://saml.threatpulse.net:8443/saml/

a. **Download** the Ping Identity **SAML Metadata** to a local directory.

b. **Upload** the WSS **Metadata**.

   Click **Select File** and browse to the location of the saved XML file.

4. Return to the WSS portal **Identity > SAML Authentication** page.



The WSS and the SAML IdP exchange information to federate (establish trust).

WSS Metadata:

SAML IdP Metadata:

Entity ID: * https://pingone.com/idp/cd-ABCdef12345.pingidentity

Endpoint URL: * https://sso.connect.pingidentity.com/sso/ido/SSO/saml2.....

Endpoint Type: Post Endpoint

User Attribute: ● NameID

Group Attribute: group

a. Click **Upload**; browse to the saved Ping certificate file saved in the previous step and open it. The portal populates the **Entity ID**, **Endpoint URL**, and **Signing Certificate** fields.

b. For the **Endpoint Type**, select **Post Endpoint**.

c. In the **Group Attribute** field, enter group.

d. Click **Save**.

5. Return to Ping Identity.

   a. Click **Continue to Next Step**.

   b. Click **Save & Publish**.

   c. Click **Finish**.

Federation is now complete.

Step 3—Test

To perform an immediate configuration validation, you can explicitly proxy a browser of a client on the network to the WSS.

1. In the WSS portal, add a location **(Connectivity > Locations)**; name it SAML Ping Test, for example.

   a. Set to **Explicit Proxy**.

   b. **Save** the location.

2. Navigate to **Identity > Authentication Policy**.

   a. Click **Add Rule** and select **Explicit Proxy Locations**. The WSS displays the New Rule page.

   b. Click **Add Sources** and add the Explicit Proxy **Location**.

3. In the **Verdict** area,

   a. Enable **Captive Portal**.

   b. Select **SAML**.

4. Click **Add Rule**; click **Activate**.

5. Log in to the test client machine and configure the browser proxy settings to `proxy.threatpulse.net:8080`.

6. Restart the browser. If you see the Ping sign-in page, the SAML deployment is functioning.

   If not, retrace the configuration steps.

   If you encounter connection problems, see "Troubleshoot SAML Authentication" on page 130 for possible causes and resolutions.

✓ Next Step

- As authenticated user traffic begins to come in, verify the success of the integration. In **Solutions** mode, generate user-based reports and verify that they display expected authenticated employee names.

- Decide whether or not further authentication policy is required. "Authentication Location Policy" on page 119.

- "Import Users and Groups for SAML" on page 40.

- "Exempt From Authentication" on page 126.

Integrate Symantec VIP Access Manager as the SAML IdP

If you want to use Security Assertion Markup Language (SAML) authentication for the Web Security Service, but do not have your own Active Directory (AD) deployed, you can provision the Symantec VIP Access Manager as the SAML Identity Provider (IdP).

Technical Requirements

- Port 8443 is required for browsers to post SAML assertions to a WSS asset. Verify that this port is open on your gateway firewall devices.
- You must have access to the Symantec VIP Access Manager with administrator permissions.

Procedure

Step 1—Configure Symantec VIP for SAML

1. Log in to the Symantec VIP Access Manager.

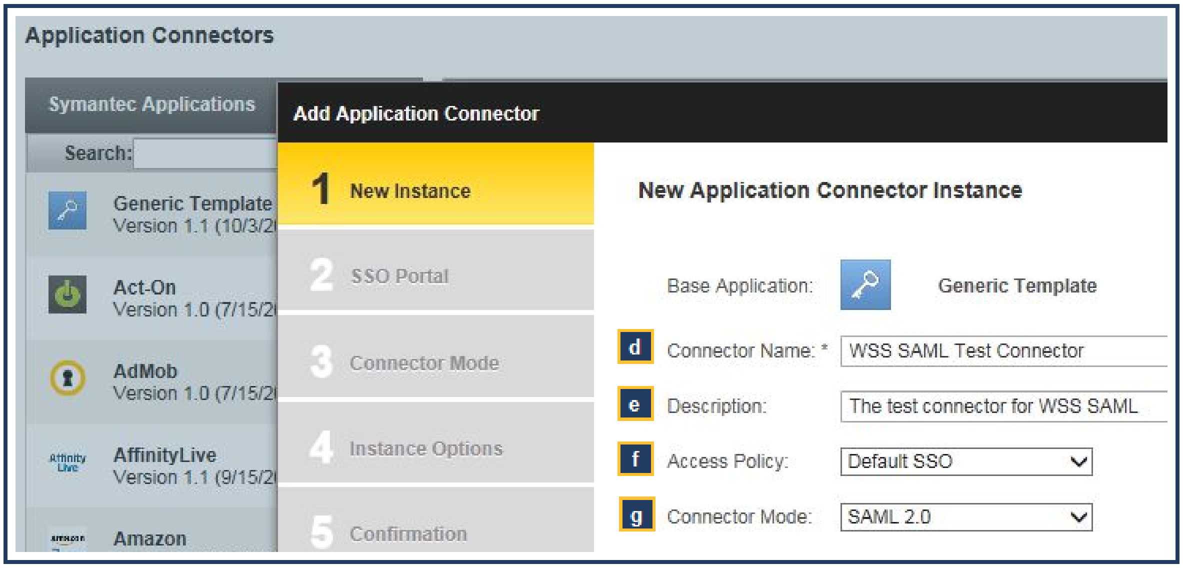
   https://samea3.websecurity.symclab.com/auth/

2. Create a new application connector.

   a. Select **Admin Console**.

   b. Click **Applications**; the portal displays the application connectors.

   c. Click **Generic Template**.



New Application Connector Instance

Base Application: Generic Template

d Connector Name: * WSS SAML Test Connector

e Description: The test connector for WSS SAML

f Access Policy: Default SSO

g Connector Mode: SAML 2.0

d. **Name** the Connector.

e. (Optional) Enter a **Description** so other admins know the purpose.

f. From the **Access Policy** drop-down list, select **Default SSO**.

g. From the **Connector Mode** drop-down list, select **SAML 2.0**.

h. Click **Next**.

3. Name the SSO application. On the **2. SSO Portal** page, enter the **Site Display Name**, which is how the connector is labeled on the application panel; click **Next**.

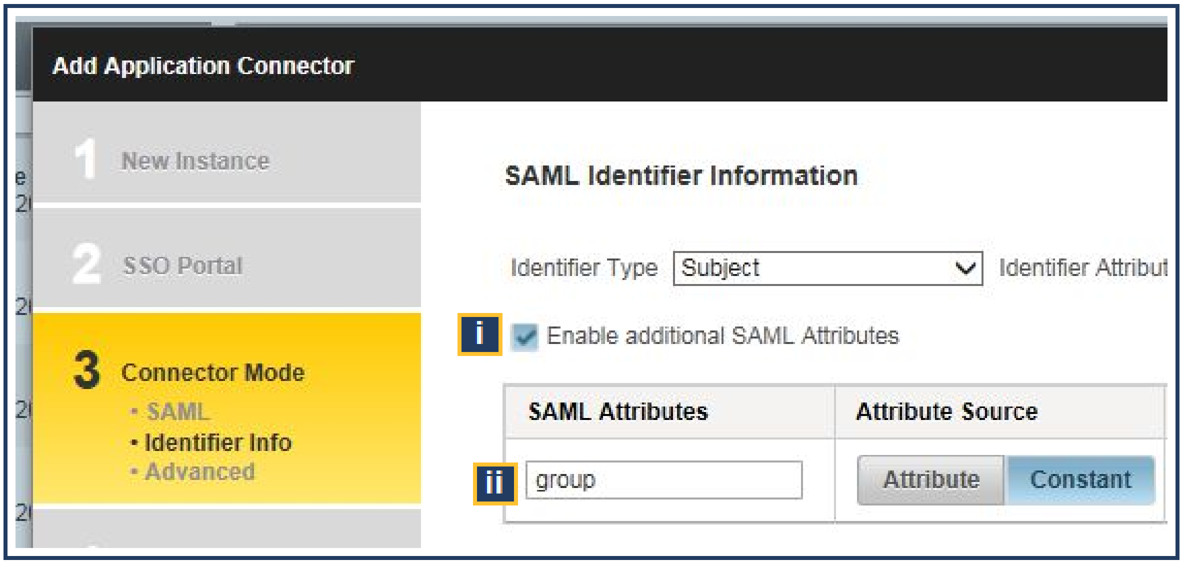
4. Define the Connector Mode.

a. On the **3. Connector Mode - SAML** page, enter the following information, which is part of the SAML Federation process.

- **Target URL**: **https://saml.threatpulse.net:8443/saml/saml_realm**
- **Mode**: **SP-Initiated**
- **ACS URL**: **https://saml.threatpulse.net:8443/saml/saml_realm/bcsamlpost**
- **SP Entity ID**: **https://saml.threatpulse.net:8443/saml/saml_realm**

Click **Next**.

b. Add the group attribute.



i. On the **3. Connector Mode - Identifier Info** page, select **Enable additional SAML Attributes**; the area expands.

ii. In the **SAML Attributes** field, enter **group**.

iii. Click **Next**.

c. On the **3. Connector Mode - Advanced** page, select the following:

- The **Include SSG-IdP Certificate in Response** option;
- From the **SSG-IdP Certificate** drop-down list, select **SSG-IDP Signer**.

Click **Next**.

5. On the **4. Instance Options** page, select **Enable Application Connector Instance at next publish**.

   Click **Next**.

6. Review the Connector information on the **5. Confirmation** page; click **Back** to perform any changes.

   When satisfied, click **Save**.

7. On the **6. Finished** page, click **Close**.

8. Commit the new configuration.

   a. In the upper-right corner, click **Publish**. The interface displays the Published Saved Changes dialog.

   b. Click **Commit**.

   c. Click **Confirm Changes**.

   d. Click **Close**.

Step 2–Federate the WSS

The next phase is to export and add metadata to the WSS as an application, which federates to the two services.

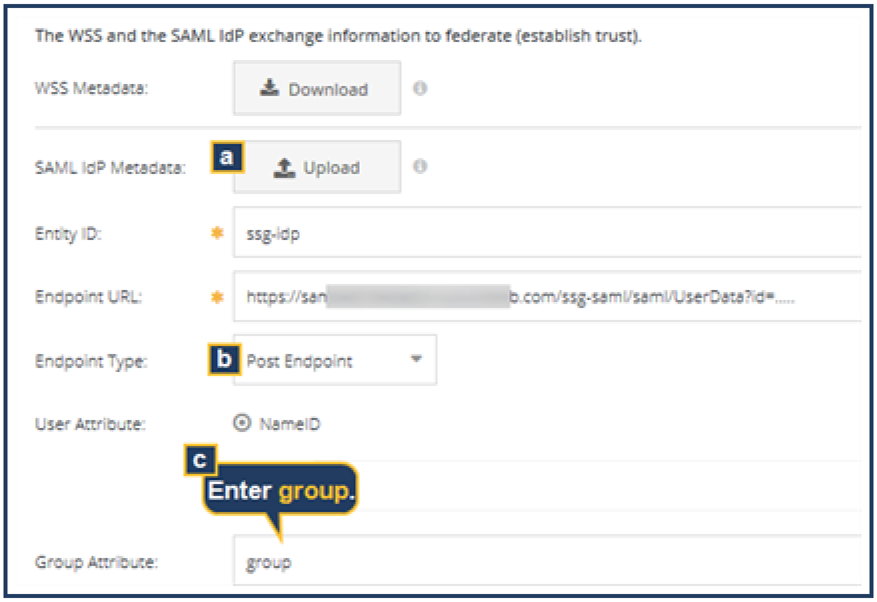
1. Remaining in the Symantec VIP Access Manager, select the Connector you created in the previous section from the **Applications** menu.

2. Click **Export IDP Metadata**.

   Save the IdP XML file. This contains the information required to Federate.

3. Access your WSS portal. Navigate to **Identity > SAML Authentication**.

4. Expand the **SAML Authentication** area.



The WSS and the SAML IdP exchange information to federate (establish trust).

WSS Metadata: Download

SAML IdP Metadata: Upload

Entity ID: * ssg-idp

Endpoint URL: * https://san[redacted]b.com/ssg-saml/saml/UserData?id=.....

Endpoint Type: Post Endpoint

User Attribute: ● NameID

Group Attribute: group

   a. Click **Upload**; browse to the saved Symantec VIP certificate file saved in the previous step and open it. The portal populates the **Entity ID**, **Endpoint URL**, and **Signing Certificate** fields.

   b. From the **Endpoint Type** drop-down list, select **Post Endpoint**.

   c. In the **Group Attribute** field, enter **group**.

   d. Click **Save**.

Step 3—Test

To perform an immediate configuration validation, you can explicitly proxy a browser of a client on the network to WSS.

1. In the WSS portal, add a location **(Connectivity > Locations)**. Name it SAML SymVIP Test, for example.

   a. Set to **Explicit Proxy**.

   b. **Save** the location.

2. Navigate to **Identity > Authentication Policy**.

   a. Click **Add Rule** and select **Explicit Proxy Locations**. The WSS displays the New Rule page.

   b. Click **Add Sources** and add the Explicit Proxy **Location**.

3. In the **Verdict** area,

   a. Enable **Captive Portal**.

   b. Select **SAML**.

4. Click **Add Rule**; click **Activate**.

5. Log in to the test client machine and configure the browser proxy settings to `proxy.threatpulse.net:8080`.

6. Restart the browser. If you see the VIP sign-in page, the SAML deployment is functioning.

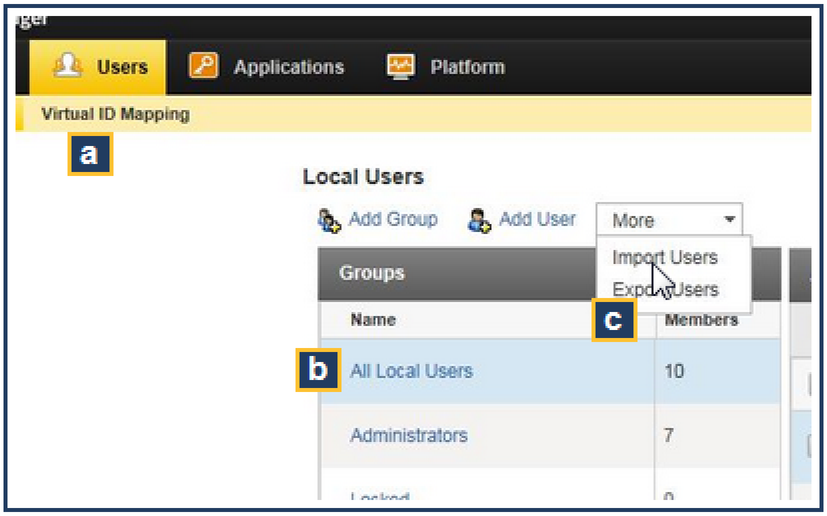
   If not, retrace the configuration steps.

   If you encounter connection problems, see "Troubleshoot SAML Authentication" on page 130 for possible causes and resolutions.

Step 4—Import Users

You must manually import the user list from the Symantec VIP Access Manager into WSS.

1. Download the user list in a spreadsheet format.



Name	Members
All Local Users	10
Administrators	7
Locked	0

   a. In the VIP Access Manager, select the **Users** tab.

   b. Select the **Local Users** row.

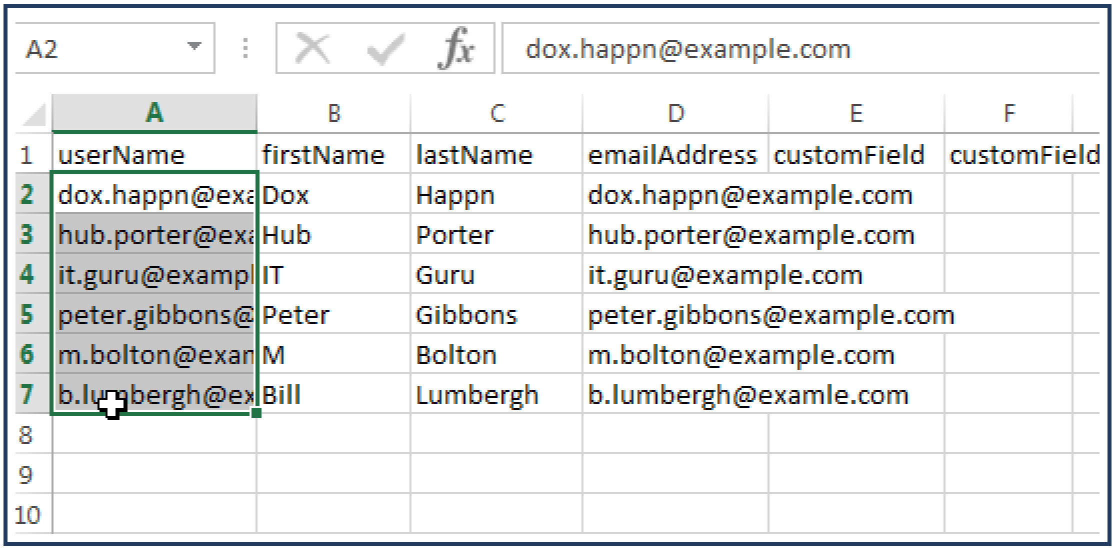
   c. From the **More** drop-down list, select **Export Users**.

   d. Save the .csv-formatted file.

2. Prepare the user list for import.

a. Open the saved .csv file in Excel.

b. Select the **userName** column.



A2

dox.happn@example.com

	A	B	C	D	E	F
1	userName	firstName	lastName	emailAddress	customField	customField
2	dox.happn@exa	Dox	Happn	dox.happn@example.com		
3	hub.porter@exa	Hub	Porter	hub.porter@example.com		
4	it.guru@exampl	IT	Guru	it.guru@example.com		
5	peter.gibbons@	Peter	Gibbons	peter.gibbons@example.com		
6	m.bolton@exan	M	Bolton	m.bolton@example.com		
7	b.lumbergh@ex	Bill	Lumbergh	b.lumbergh@examle.com		
8						
9						
10						

c. Copy all of the user names (*without* the **userName** column header) into your client's clipboard.

d. Open a text file and copy the user names into it; save the file.

3. Access the WSS portal to import the usernames from the text file.

   a. Select **Identity > Users and Groups > Imported Users/Groups**.

   b. Click **Add**. The portal displays the Add User dialog.

   c. Click **Import Users/Groups**.

   d. Under **Import Users**, click **Browse**.

   e. Navigate to the saved text file that contains the usernames and open it.

   The portal displays all of the usernames imported from the file.

Next Step

- As authenticated user traffic begins to come in, verify the success of the integration. Generate user-based reports and verify that they display expected authenticated employee names.
- Decide whether or not further authentication policy is required. "Authentication Location Policy" on page 119.
- "Import Users and Groups for SAML" on page 40.
- "Exempt From Authentication" on page 126.

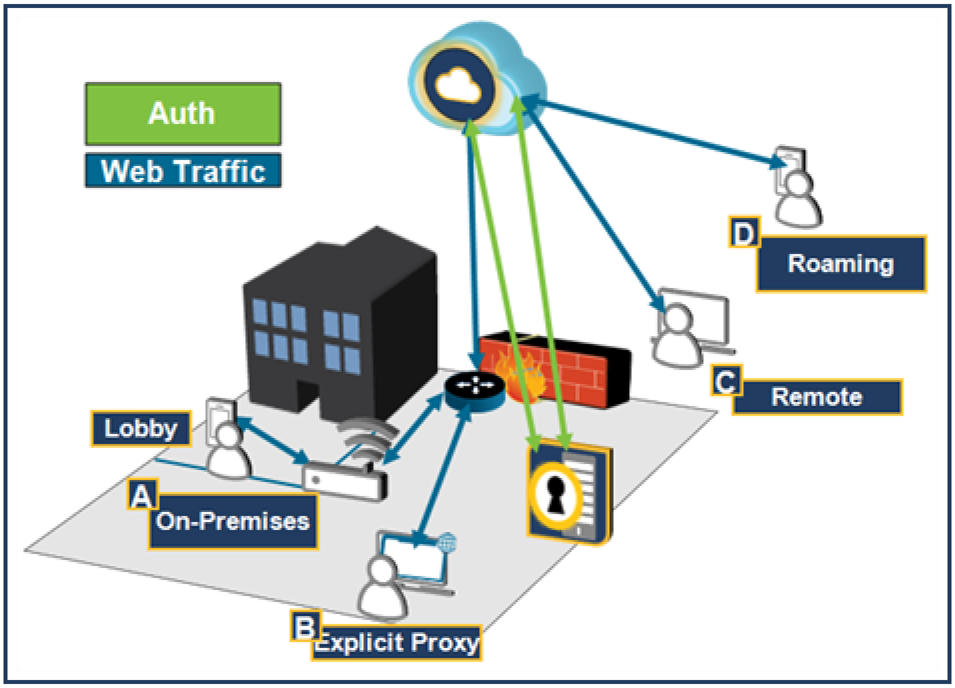
About Captive Portal Authentication

By definition, challenge-based authentication displays a credential dialog to users each time they open a web browser. Users must enter their corporate network username and password into the dialog and click **Accept** before performing web content requests. In this context, this feature is also commonly referred to as Captive Portal.

The Web Security Service provides the Captive Portal for the following deployment methods:

- As an alternative method to check user credentials rather than the method provided by the WSS Agent application that is installed on remote systems.
- Allows an authentication method for *BYOD*—employees access the network from their personal devices.
- This option also provides user credential checks for Explicit Proxy (PAC file) deployments.
- Required for SAML Authentication integration with the Firewall/VPN and Explicit Proxy methods.
- Quickly configure a browser or device for authentication demonstration.

The following diagram illustrates the various Captive Portal solutions based on employee-to-network connection method. All Captive Portal deployments require the Auth Connector application that integrates with your Active Directory to verify user credentials.



A—Firewall/VPN/Guest WiFi Over IPSec

The WSS recognizes a connection from firewall/router device as a fixed location (versus from a roaming user). Using the Authentication Policy Editor, you can specify the surrogate type (IP address or cookie) and authentication refresh intervals on a per-location basis.

With the proliferation of *bring your own devices* (BYOD), companies must find a way to accommodate employees who use their personal phones and tablets for both work and personal use. One method is to maintain a separate WiFi for BYOD use. The WiFi network might be seen by WSS as its own location or as one or subnets. With Captive Portal enabled, users must enter their network credentials. Closing and re-opening a browser window within that time does not trigger a new authentication challenge.

> **Note:** **DEPLOYMENT NOTE:** The following applies to IP surrogates only. For clients behind NAT'ed firewalls, the best practice is to use Cookie Surrogates.
> After a user authenticates from an IP address, all further requests from that IP address are treated as if from that user. If the client is behind a NAT or on a multi-user system, the first user's credentials are used. For example, Employee A requests web content and WSS successfully authenticates him. Employee B then connects, but she is not sent an authentication challenge. She is seen as Employee A and thus receives all policy designated for Employee A.

B—Explicit Proxy

By default, the Explicit Proxy method neither provides authentication nor sends user and group information to WSS for use in reports or custom policy. To make username/group information available, you must enable the Captive Portal option for each location configured in WSS.

Using the Authentication Policy Editor, you can specify the authentication refresh intervals on a per-location basis.

C—WSS Agent

WSS provides the Captive Portal as an alternative method to check user credentials rather than the method provided natively by the WSS Agent application that is installed on remote systems

Without Captive Portal enabled, remote users log into the corporate network using their cached credentials. With Captive Portal enabled, the challenge dialog initiates from the client system, which ensures that the correct person logging in is recorded. This allows the system to be accessed by multiple users. Furthermore, the benefit for network administrators is that you have more control of your network access. If a laptop becomes lost or you need to deny a remote employee access, change their status in the Active Directory; that user's access credentials are now denied.

D—Quick Authentication Demonstration (Roaming Captive Portal)

Roaming Captive Portal allows you to quickly connect a non-enrolled device (mobile device or laptop) to WSS and receive an authentication challenge. For browsers, this allows the enforcement of employee credentials to access web content. For mobile devices, this allows for quick demonstrations of authentication and policy. These browsers/devices are configured to explicitly proxy to WSS and a user's corporate e-mail addresses are used to validate access.

Additional Information

- Client systems must have third-party cookies enabled.
- Client systems must have the WSS SSL Root Certificate on their browsers. This is described in the configuration topics.

- If your enterprise comprises multiple domains, users must enter the full domain name rather than just their login name. For example, they must enter `alan.user@company.com`, not just `alan.user`.
- If the Auth Connector becomes unavailable, the user receives the following error message: `Authentication server error, connecting as unauthenticated user` (also, WSS adds the event to the diagnostic log). The behavior defaults to what happens when Captive Portal is not enabled. That is, the users' access credentials creates a tunnel. For diagnostic analysis, this Advanced dialog entry is `unauthenticated (`*`user_name`*`)`.
- Verify that each user to be authenticated has their e-mail address attribute populated in the AD (**User Properties** dialog **> General > E-mail**). For example, `EXAMPLECORP\alan.user` has an e-mail attribute of `alan.user@examplecorp.com`. If you are employing Exchange, default policies automatically create this attribute. If you are not employing Exchange and have a large number of users with undefined e-mail attributes in the AD, search online for resources about how to use a script to populate.

About Challenges

When Captive Portal is enabled–

- Challenges are based on each browser session. For example, users are challenged when they open Firefox and then can browse (including new tabs). If they then open a Internet Explorer browser, they must enter their credentials in that browser to continue.
- Entered passwords, represented as *auth tokens*, are retained in a *credential cache* on the device in the data center that is processing authentication for that client. They are not stored permanently in the cloud. The Authentication Policy Editor allows you to specify surrogate times for the Firewall/VPN methods and credential refresh times for both the Firewall/VPN and Explicit Proxy methods.

  The following conditions prompt employees to re-enter their credentials.

  - When the user attempts to reconnect to the web after those respective time thresholds.
  - Other network activity, such as that employee's data getting moved from one data pod to another.
- The Auth Connector abides by the lockout settings in the AD. For example, the AD is configured to allow three attempts to log in. If the third attempt fails, the user is locked out for 30 minutes before they can attempt again.
- If a lockout configuration exists and the user triggers it or if the user attempts to use an expired password:
  - All web-bound transaction intended for WSS is dropped; all other traffic continues normally.
  - If the fault is an Auth Connector problem, the user connects to WSS as an **unauthenticated user**.
- If you render an employee disabled, WSS requires 15 minutes to complete the transaction; the employee is still able to browse during that time period.

✓ Enable Captive Portal?

- Firewall/VPN (IPsec) Access Method–Proceed to "Authentication Location Policy" on page 119.
- Remote Users–Navigate to **Connectivity > WSS Agent**. This page contains the **Enable Captive Portal** option.

About Roaming Captive Portal

Roaming Captive Portal enables any proxy-enabled software (browsers and agents) to connect to the Web Security Service from any internet origin. When attempting to access internet content, users on roaming endpoints (connecting on non-corporate networks) receive prompts to enter credentials.

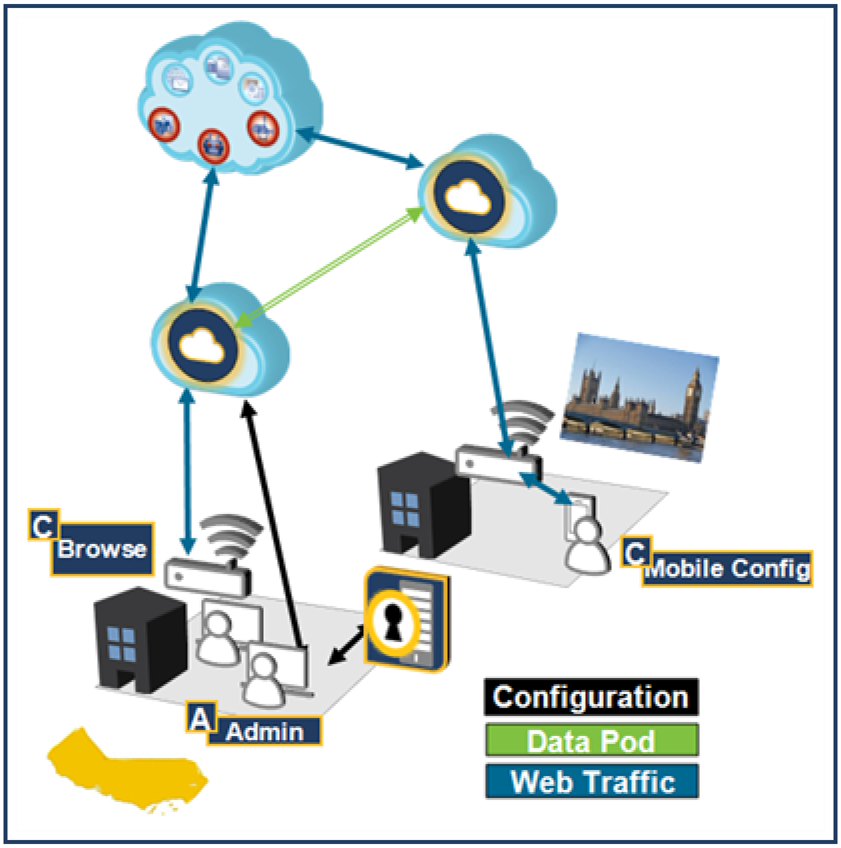
Employees must enter their credentials per the following.

- Once every 24 hours.
- After a system reboot.
- After a network change occurs (for example, moving from one WiFi network to another).

However, these connections do not inherently include the client logged-in user name for identification, authorization, or tenancy. Therefore, the solution requires the Auth Connector to provide WSS with the user and group information.

> **Tip:** If you deployment includes Symantec Endpoint Protection (SEP) clients, you can enable Roaming SAML Authentication. See the SEP topics in the WSS Help System.

Topography



- Configure a browser for explicit proxy connections to the service, which then enforces user authentication for web sessions.
- Connect a mobile devices to use the roaming PAC file.

Symantec provides a URL or hostname/port, then use corporate domain e-mail addresses and passwords to attempt access web-based content.

Data Flow

1–A WSS Admin (**A**) in the California corporate office performs the following tasks:

- Verifies that the Auth Connector is configured and functioning with the Active Directory (AD). This is required to validate user e-mail addresses.
- Adds one or more corporate e-mail domains, which are used by the Auth Connector to validate incoming employee connections.
- Enables Roaming Captive Portal, which yields the roaming PAC file URL.

2–These configurations are made available to all WSS data pod locations on the planet.

3–On a laptop connected to the corporate Wi-Fi (**B**), configure a browser to explicitly proxy to the WSS roaming PAC file. From the laptop, a tester initiates a web request, which routes to the data pod in California.

- The data pod receives the request. For now, the request registers as coming from a nondescript user. The service returns an `HTTP 407 Proxy Authentication Required` challenge.
- The tester enters his full corporate e-mail address and network password.
- The Auth Connector matches the domain/e-mail; if the match fails, the connection fails. Upon the first successful match, the data pod receives the policy configuration for this type of access method (assuming this is the first connection).

4–Upon successful challenge and data pod registration, WSS re-requests the web content. Policy checks and malware scanning occur and the employee receives or is denied the content based on those checks.

5–A tester (**C**) in the remote office in London configures the manual proxy setting on her mobile device, which is connected to the corporate Wi-Fi, to route web traffic to WSS. The London data pod, having received the e-mail domain, roaming captive portal, and policy configurations, initiates an authentication challenge on the device before allowing web-based content.

Additional Notes

Conflict With Coaching Policies

Known Issue: With Roaming Captive Portal enabled, Firefox and Internet Explorer browser return certificate errors (Secure Connection Failed) when a Coaching or possible Password Override policy is triggered. Chrome authenticates, but then also returns an error. Users can reload the page and receive the content.

Twenty-Four Hour Cached Credential Period

User credentials are stored in the WSS credential cache for 24 hours. If you disable Roaming Captive Portal, a user still has access during that time.

App Proxy-Aware Limitations

Many apps (especially on Android devices) are not proxy-aware; therefore, behavior on mobile devices might be erratic and is expected. The features is designed to quickly demonstrate geo-location-based employee awareness by WSS.

✓ Implement This Feature?

- Proceed to "Enable Roaming Captive Portal" on page 105.

Enable Roaming Captive Portal

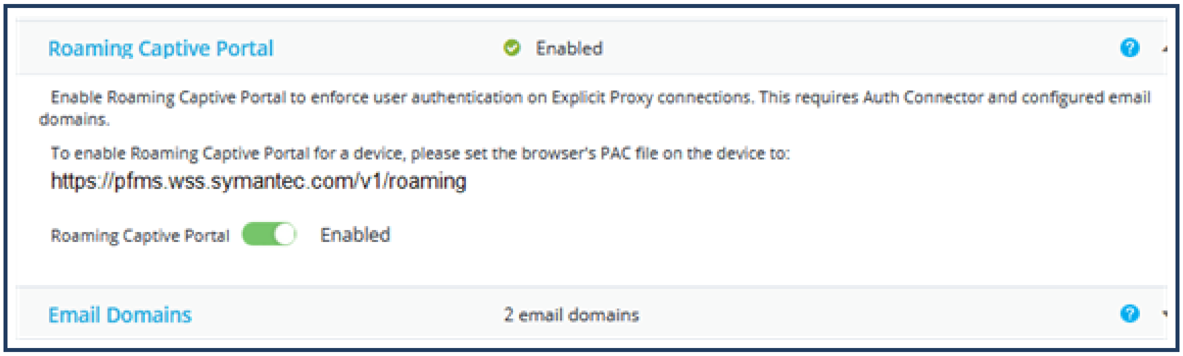
The Web Security Service provides the Roaming Captive Portal user authentication features, which allows for geo-location-awareness and quick demonstrations from browsers or non-enrolled devices. The first step is to enable Roaming Captive Portal in the WSS portal, which includes specifying corporate e-mail domains.

Technical Requirements

- Be advised of the security risks exposed by this feature. See "About Roaming Captive Portal" on page 102.
- Roaming Captive Portal requires a functioning Auth Connector deployment. See "Deploy the Auth Connector" on page 23.
- All endpoint clients must have the WSS root certificate.
- You must enable SSL interception policy for Mobile Device Sources..
- Verify that each user to be authenticated has their e-mail address attribute populated in the AD (**User Properties** dialog **> General > E-mail**). For example, `EXAMPLECORP\alan.user` has an e-mail attribute of `alan.user@examplecorp.com`. If you are employing Exchange, default policies automatically create this attribute. If you are not employing Exchange and have a large number of users with undefined e-mail attributes in the AD, search online for resources about how to use a script to populate.

Procedure

1. Navigate to **Identity > Auth Connector**.
2. Expand the **Roaming Captive Portal** area.
3. Toggle **Roaming Captive Portal** to **Enabled**.



Roaming Captive Portal ✓ Enabled

Enable Roaming Captive Portal to enforce user authentication on Explicit Proxy connections. This requires Auth Connector and configured email domains.

To enable Roaming Captive Portal for a device, please set the browser's PAC file on the device to:
https://pfms.wss.symantec.com/v1/roaming

Roaming Captive Portal Enabled

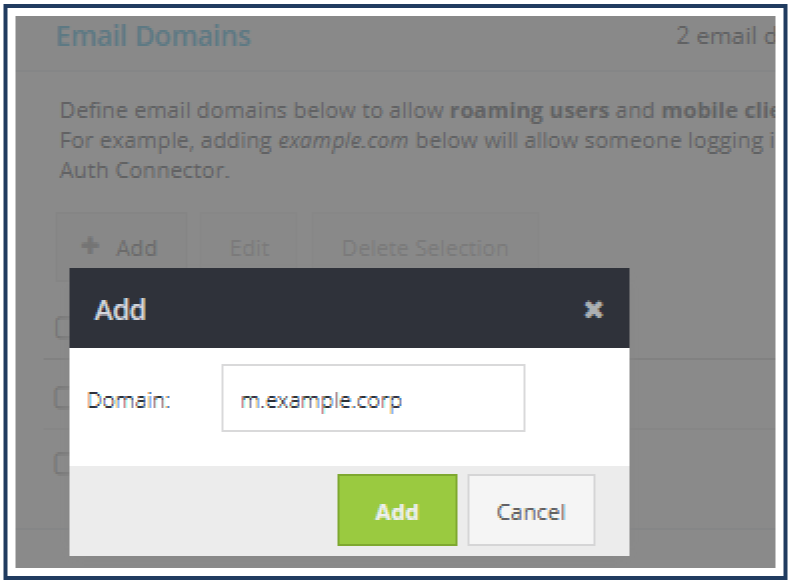
Email Domains 2 email domains

4. Add the email domain.

   a. Expand the **Email Domains** area.

   b. Click **Add**.

c. In the **Add** dialog, enter a **Domain** or sub-domain and click **Add**.

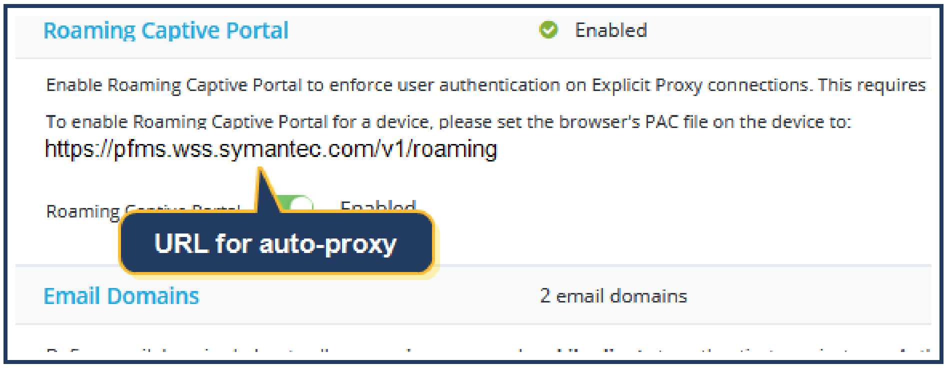


Email Domains 2 email d

Define email domains below to allow **roaming users** and **mobile cli**
For example, adding *example.com* below will allow someone logging i
Auth Connector.

Domain: m.example.corp

5. When you **Enable** Roaming Captive Portal, the WSS displays the **https://pfms.wss.symantec/v1/roaming** URL. This is the URL to configure the explicit proxy settings in browsers (mobile devices might require further configuration). Record this URL.



Roaming Captive Portal ✓ Enabled

Enable Roaming Captive Portal to enforce user authentication on Explicit Proxy connections. This requires

To enable Roaming Captive Portal for a device, please set the browser's PAC file on the device to:
https://pfms.wss.symantec.com/v1/roaming

Roaming Captive Portal: Enabled

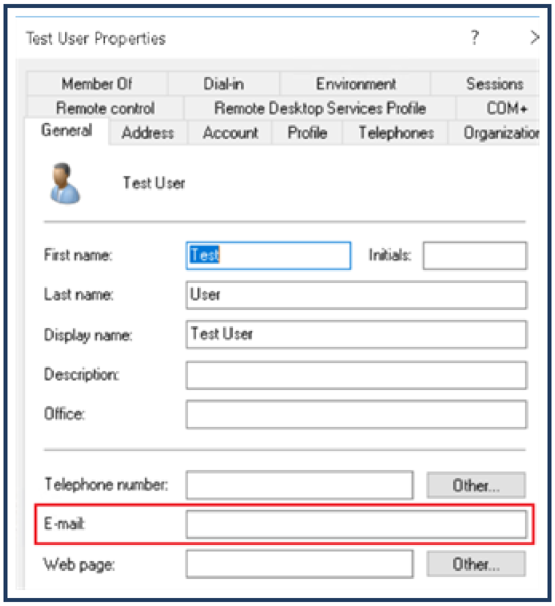
Email Domains 2 email domains

Troubleshooting Tip

If a client receives the following error:

```
Reason for challenge: General authentication failure due to bad user ID or authentication token.
```

The likely reason is the email domain requirement, as discussed in the Technical Requirements and **Step 4** above, was not completed or was mis-configured. To verify, check the client's User Properties.



Test User

First name: Test

Initials:

Last name: User

Display name: Test User

Description:

Office:

Telephone number:

E-mail:

Web page:

If the **E-mail** field is empty, the email domain was not correctly configured.

> **Tip:** When logging in with the email address, the username portion is not case sensitive. However, the **email domain** in use is case sensitive and must match exactly as it is defined in the portal.

Next Selection

Configure a browser or mobile device to explicitly proxy to the WSS roaming PAC file

- See "Configure Browsers for RCP" on page 108.
- See "Enable Roaming Captive Portal on iOS" on page 113
- See "Enable Roaming Captive Portal for Android" on page 110.

Configure Browsers for RCP

With Roaming Captive Portal enabled on the Symantec Web Security Service, you can demonstrate geo-location-based employee awareness by configuring a browser to explicitly proxy to the service roaming PAC file:

```
https://portal.threatpulse.com/roaming
```

For more details, see the following.

- See "About Roaming Captive Portal" on page 102.
- See "Enable Roaming Captive Portal" on page 105.

Procedure

Apple Safari

1. Select **Apple** menu **> System Preferences**.
2. Select the **Internet and Network** tab
3. Select an option:
   - If you are connected by cable to the network, select **Ethernet**.
   - If you are connected using WiFi, select the **AirPort** option.
4. Click **Advanced**. Enter the address of your PAC file in the **Address** field. For example, `https://portal.threatpulse.com/roaming`.
5. Click the **Proxies** tab.
   a. Select **Using a PAC file**.
   b. Enter the Web Security Service PAC file location in the **Address** field: `https://portal.threatpulse.com/roaming`.
6. Select **Quit** to exit System Preferences.

Google Chrome

1. In the top-right corner of the browser, select the **wrench** .
2. From the drop-down list, select **Options** . The browser displays the Google Chrome Options dialog.
3. In the **Network** section, click **Change proxy settings** to display the Internet Properties dialog.
4. Click the **Connections** tab.

5. In the **Local Area Network (LAN) Settings** section, click **LAN settings** to display the Local Area Network (LAN) Settings dialog.
    a. In the **Automatic configuration** area, select **Use automatic configuration script**.
    b. Enter the WSS PAC file location in the **Address** field:`https://portal.threatpulse.com/roaming`.
6. Click **OK** and exit out of all open dialogs.

Microsoft Internet Explorer

1. Select **Tools > Internet Options**.
2. Select the **Connections** tab.
3. If you are using a VPN connection, click **Add** to set up the connection wizard. If you are using a LAN connection, click **LAN settings**
4. LAN settings dialog:
    a. Select **Automatically detect settings** and **Use automatic configuration script**.
    b. Enter the WSS PAC file location in the **Address** field: `https://portal.threatpulse.com/roaming`.
5. Click **OK** and exit out of all open dialogs.

Mozilla Firefox

1. Select **Tools > Options**. The browser displays the Options dialog.
2. Select the **Advanced > Network** tab.
3. In the **Connections** area, click **Settings**.
4. Configure Connection Settings:
    a. Select **Automatic proxy configuration URL**.
    b. Enter the WSS PAC file location in the **Address** field: `https://portal.threatpulse.com/roaming`.
5. Click **OK** and exit out of all open dialogs.

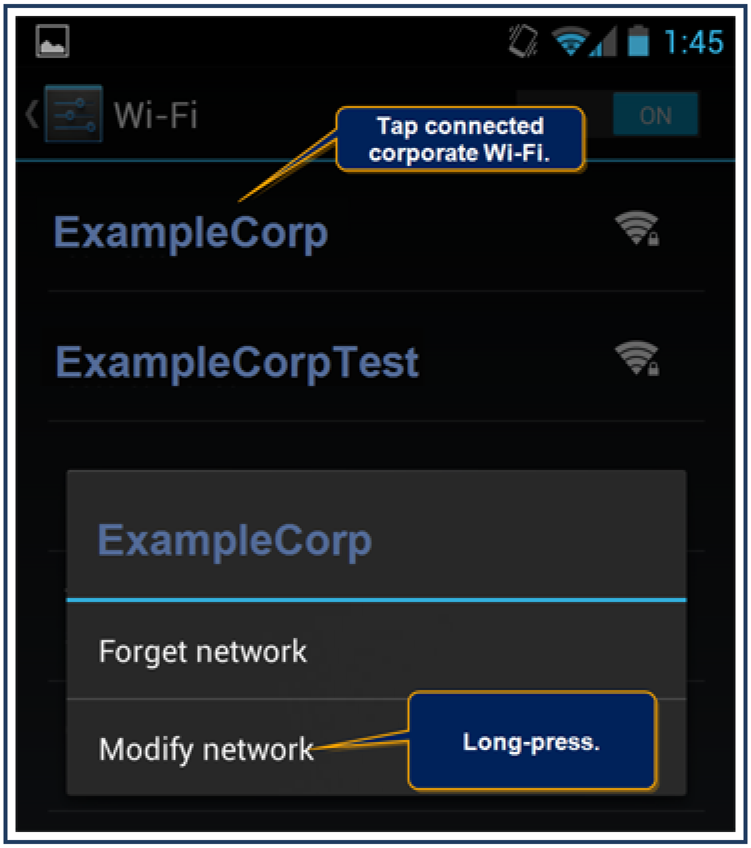
Enable Roaming Captive Portal for Android

With Roaming Captive Portal enabled on the SymantecWeb Security Service, employee Android devices can be configured to require an authentication challenge when requesting web content.

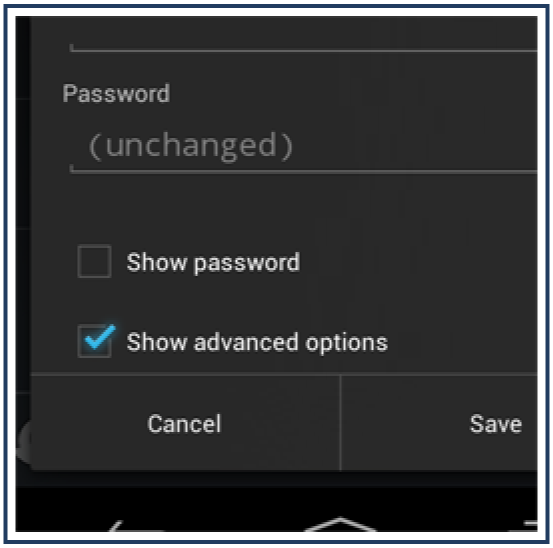
- See "About Roaming Captive Portal" on page 102.
- See "Enable Roaming Captive Portal" on page 105.

Procedure

1. On the device, tap **Settings**.
2. Tap **Wi-Fi** and tap your corporate network. Long-press **Modify Network** until the device displays the **Network Settings** page.



3. Scroll down and tap **Show Advanced Options**.



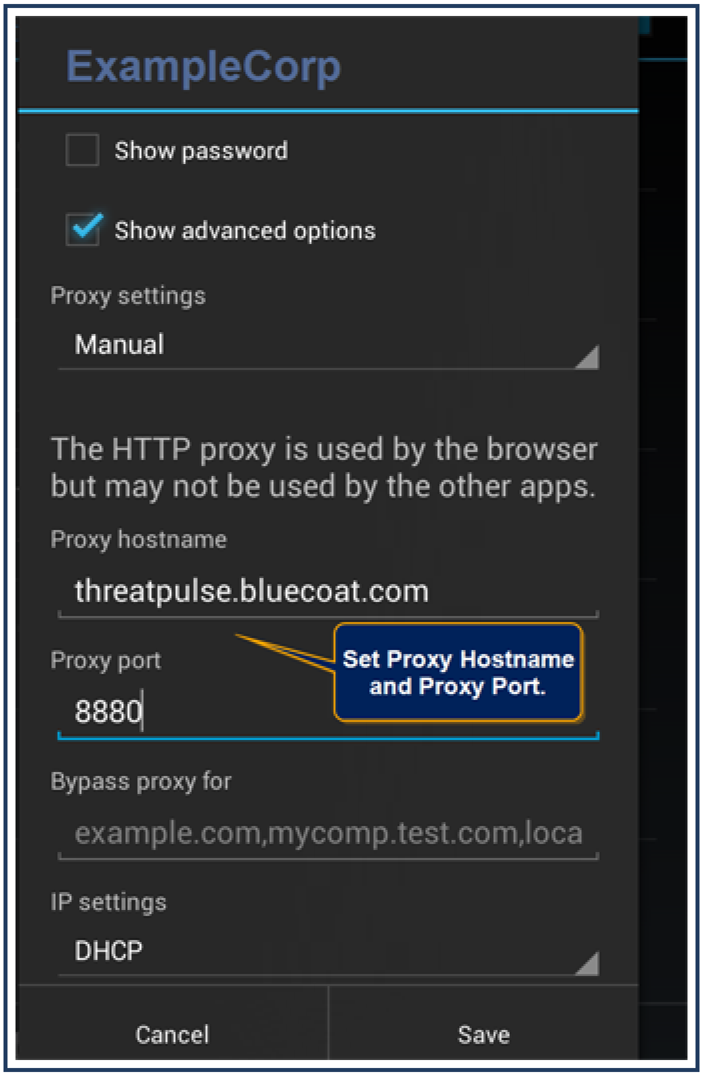
Password

(unchanged)

□ Show password

☑ Show advanced options

4. Set the Proxy hostname and port.



ExampleCorp

□ Show password

☑ Show advanced options

Proxy settings

Manual

The HTTP proxy is used by the browser but may not be used by the other apps.

Proxy hostname

threatpulse.bluecoat.com

Proxy port

8880

Set Proxy Hostname and Proxy Port.

Bypass proxy for

example.com,mycomp.test.com,loca

IP settings

DHCP

   a. In the **Proxy Settings** area, tap **Manual**.
   b. In the **Proxy Hostname** field, enter `threatpulse.bluecoat.com`.
   c. In the **Proxy Port** field, enter `8880`.
   d. Click **Save**.

5. Test: Open the mobile browser and browse to a website. The device displays an authentication challenge
6. Browse to a website that belongs to a category blocked by defined policy. If the page is blocked, the configuration was successful.

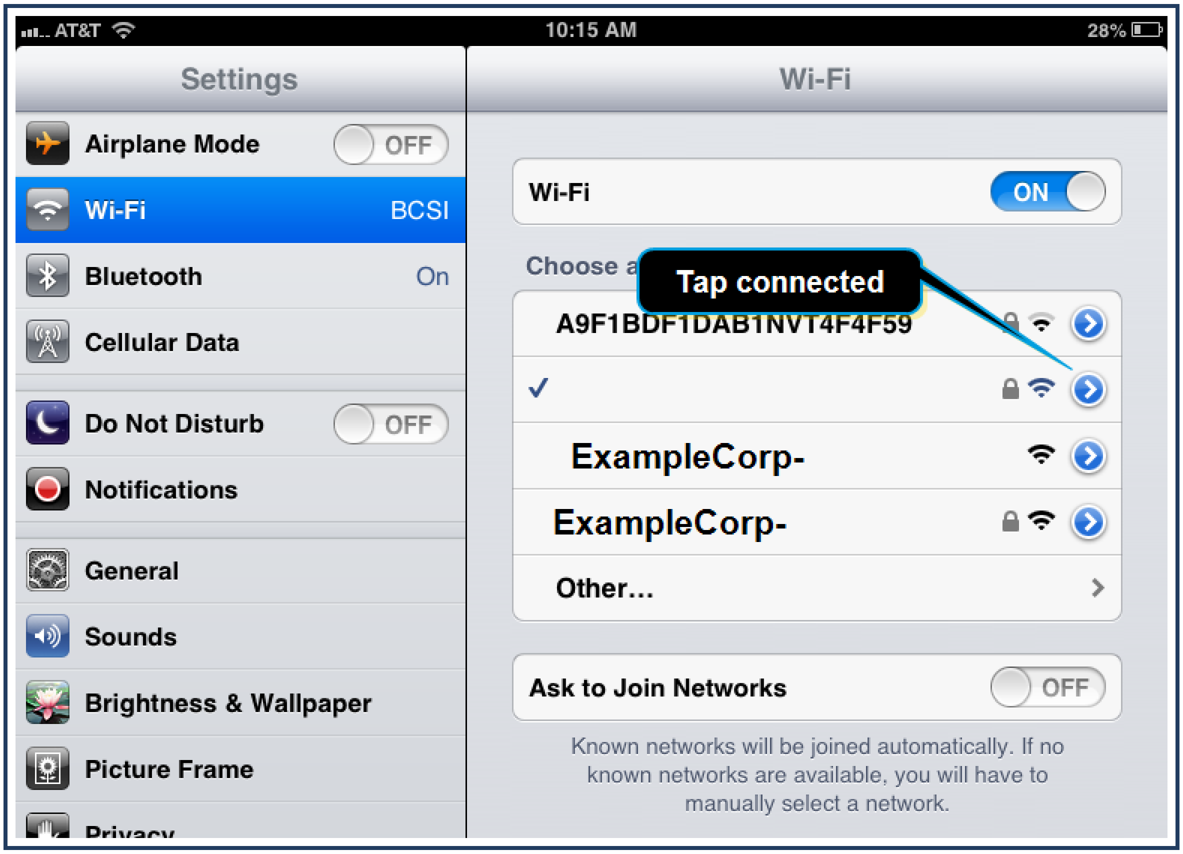
Enable Roaming Captive Portal on iOS

With Roaming Captive Portal enabled on the Symantec Web Security Service, employee iOS devices can be configured to require an authentication challenge when requesting web content.

- See "About Roaming Captive Portal" on page 102.
- See "Enable Roaming Captive Portal" on page 105.

Procedure

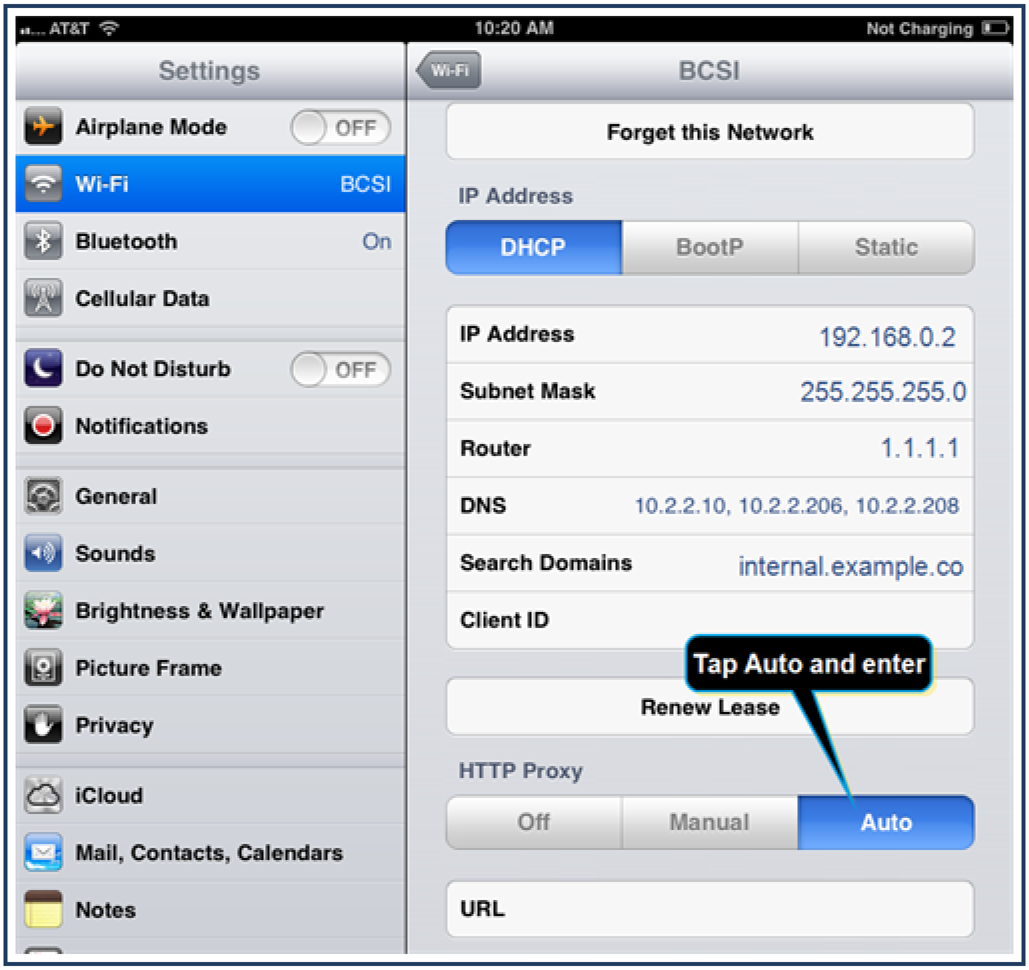
1. On the device, tap the **Settings** app.
2. Tap **Wi-Fi** and tap your corporate Wi-Fi network.



Tap connected

Known networks will be joined automatically. If no known networks are available, you will have to manually select a network.

3. In the **HTTP Proxy** area, tap **Auto**. In the **URL** field, enter `https://portal.threatpulse.com/roaming`.



IP Address 192.168.0.2

Subnet Mask 255.255.255.0

Router 1.1.1.1

DNS 10.2.2.10, 10.2.2.206, 10.2.2.208

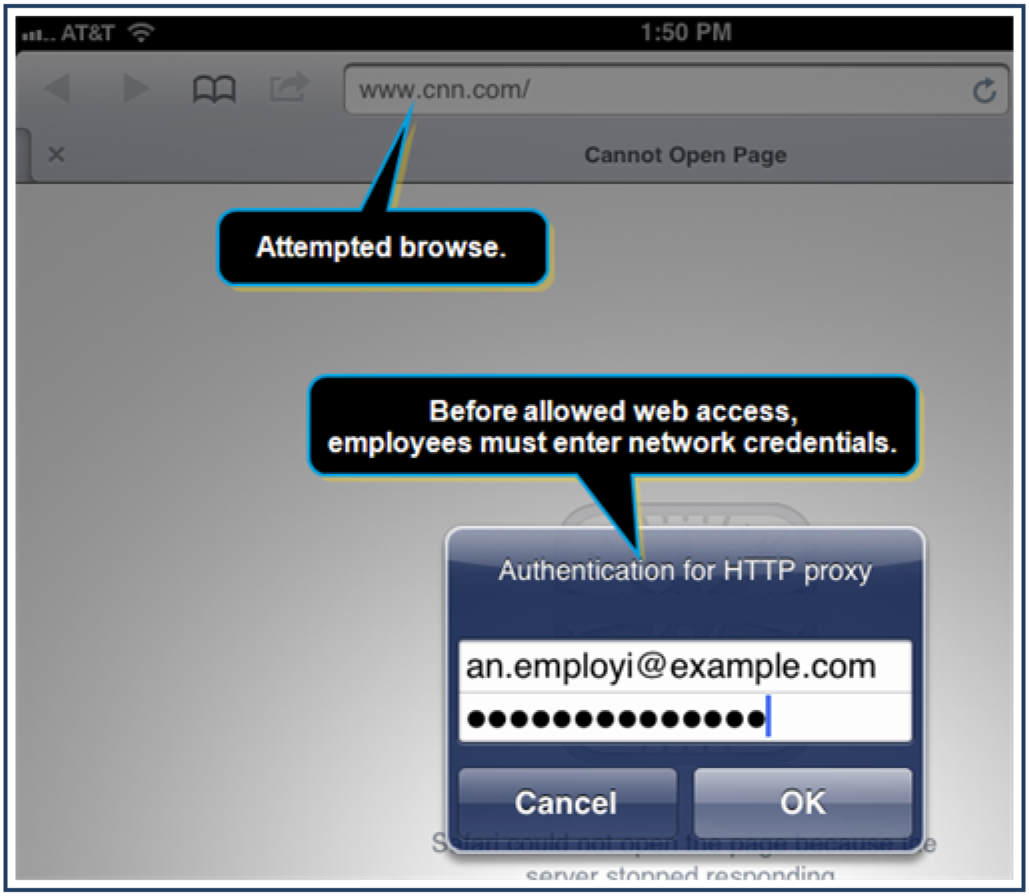
Search Domains internal.example.co

Client ID

URL

Tap Auto and enter

4. Test: Open the Safari browser app and browse to a website. The device displays an authentication challenge.



Attempted browse.

Before allowed web access, employees must enter network credentials.

www.cnn.com/

Cannot Open Page

Authentication for HTTP proxy

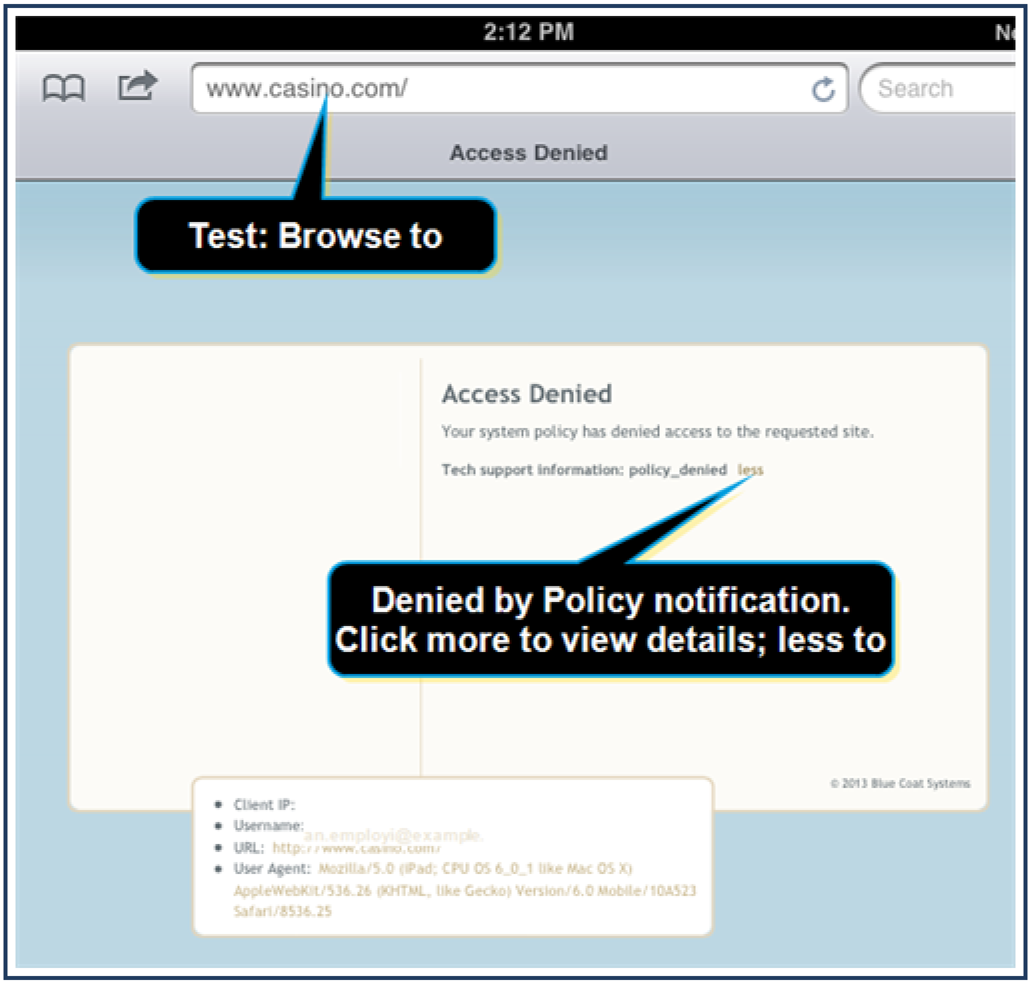
an.employi@example.com

●●●●●●●●●●●●●●

Safari could not open the page because the server stopped responding

A successful challenge allows access (pending malware scan and policy check).

5. Browse to a website that belongs to a category blocked by defined policy. If the page is blocked, the configuration was successful.



Test: Browse to

Access Denied

Your system policy has denied access to the requested site.

Tech support information: policy_denied less

Denied by Policy notification. Click more to view details; less to

© 2013 Blue Coat Systems

- Client IP:
- Username: an.employi@example.
- URL: http://www.casino.com/
- User Agent: Mozilla/5.0 (iPad; CPU OS 6_0_1 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A523 Safari/8536.25

Review Imported Users and Groups

The Web Security Service receives your employee user and group names from either the Auth Connector deployment method or from a SAML deployment.

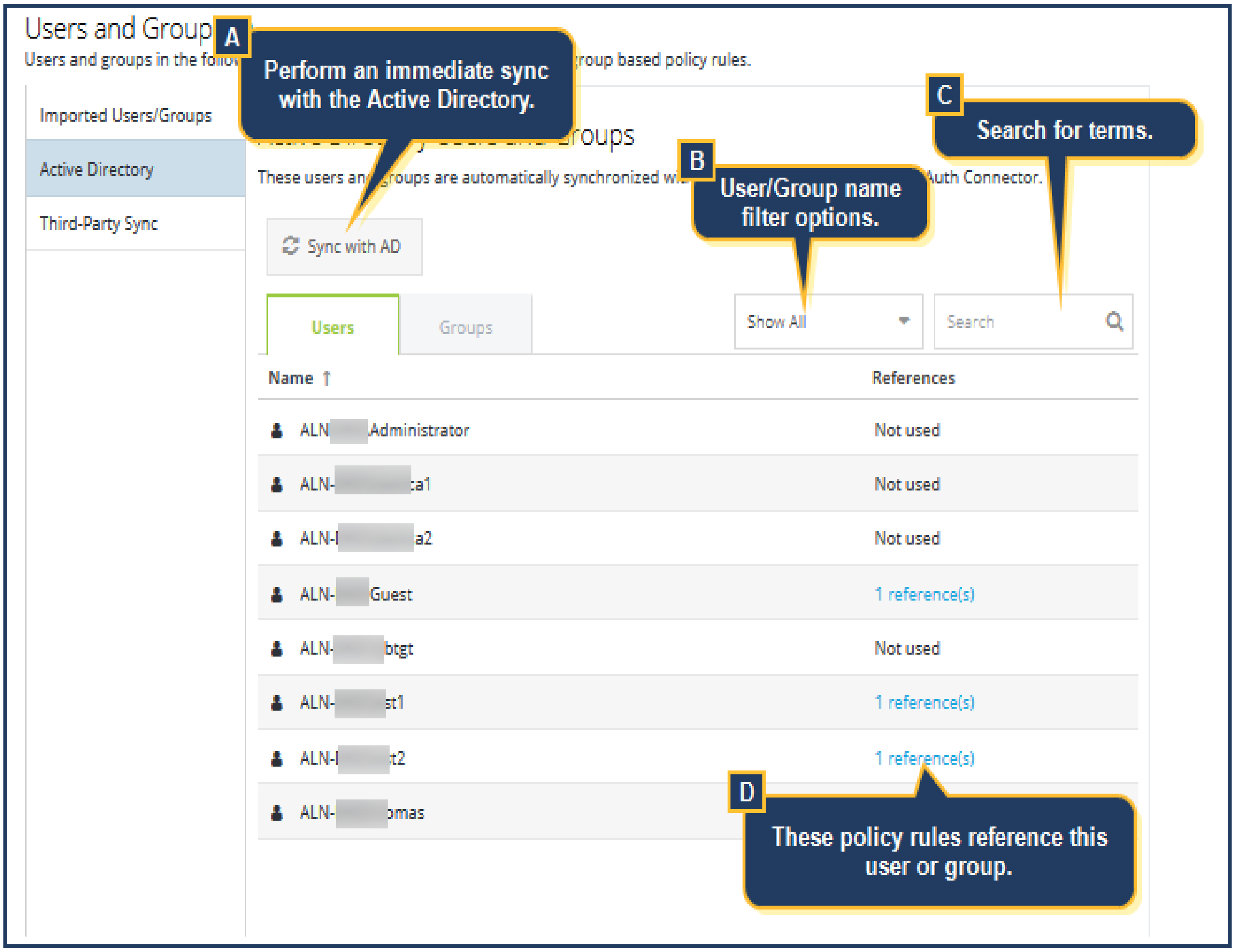
Imported From SAML

If your authentication method is SAML, see "Import Users and Groups for SAML" on page 40.

Imported From the Auth Connector

If you deploy the Auth Connector, WSS receives user and group names from the Active Directory (AD). You can review the user and group names as recognized by the service. In addition, you can see which names are currently referred to in policy rules.

WSS automatically performs an AD refresh once a week; however, you can manually initiate a sync operation. Navigate to **Identity > Users and Groups > Active Directory**. Be advised that it might take up to 24 hours for you see the information in your portal. Avoid re-clicking the button more than once in a 24-hour period; doing so might overly clog the sync queue, causing slower results.



A: Perform an immediate sync with the Active Directory.

B: User/Group name filter options.

C: Search for terms.

D: These policy rules reference this user or group.

Name ↑	References
ALN[redacted]Administrator	Not used
ALN-[redacted]a1	Not used
ALN-[redacted]a2	Not used
ALN-[redacted]Guest	1 reference(s)
ALN-[redacted]btgt	Not used
ALN-[redacted]st1	1 reference(s)
ALN-[redacted]t2	1 reference(s)
ALN-[redacted]mas	

A—WSS performs an AD refresh once per 24 hours. Click **Synchronize with AD** to perform an instant refresh and synchronize the most current user and group memberships.

B—By default, the service displays every imported AD name, sorted alphabetically by user and group name. From the **Show All** drop-down, filter just those **Referenced** in policy or any users that were **Deleted** from the AD.

C—You can search for a specific name (if you know it) or for a string. For example, searching for Logan returns any name with Logan in it.

D—The **Policy Rule Reference** column indicates that a Content Filter policy rule exists that applies to the user or group (**Policy > Content Filtering**). Click the link to display the rule editor with the relevant wizard tab. For example, the **Who** tab that contains the selected user, allowing you to instantly edit and apply changes.

Controls on the bottom of the page allow you to navigate back and forth to other pages and refresh the content.

Authentication Location Policy

WSS Authentication Policy enables you to define the authentication method employed depending on the fixed Firewall/VPN (IPsec) or Explicit Proxy location. This is helpful when you have a mix of authentication methods. For example, the Auth Connector provides authorization and authentication for all connections through on-premises firewall devices, but you employ a SAML IdP for remote locations connecting through Explicit Proxy. Or, if a location does not have access to an Auth Connector or SAML IdP, enable Captive Portal.

You can also enable Captive Portal (see "About Captive Portal Authentication" on page 99).

- **Firewall/VPN**—In the policy editor you specify the **Sources** and then define applicable parameters.
  - Select Locations. WSS detects **Firewall/VPN** Locations already defined on the **Connectivity > Locations** page. Or you can create a new one directly in the policy editor.
  - Select IP addresses as previously defined or you can define new addresses directly in the policy editor. For example, you are running tests from specific IP addresses/subnets.
  - The default authentication method is the Auth Connector. You can also enable Captive Portal and elect to use the Auth Connector or SAML as the authentication method.
- **Explicit Proxy**—In the policy editor you specify the **Sources** and the define applicable parameters.
  - Select Locations. The WSS detects **Explicit Proxy** Locations already defined on the **Connectivity > Locations** page. Or you can create a new one directly in the policy editor.
  - The default authentication method is the Auth Connector. You can also enable Captive Portal and select to use the Auth Connector or SAML as the authentication method.

About Captive Portal Policy

When this is enabled, users must enter credentials in browsers to access web-based content.

Firewall/VPN Surrogate Types

For locations that connect to WSS through the Firewall/VPN method, you can decide which type of authentication surrogate to employ.

- **IP**—WSS authenticates the client IP address. On the next authentication occurrence, the service remembers the requesting client by IP address. The service proceeds on the expectation that it is the same user. Symantec recommends this method to reduce the impact of CORS-related issues. The exception is if traffic comes through a circuit-level gateway where IP addresses are shared; you must use the Cookie method.
- **Cookie**—WSS authenticates and sets a browser cookie. On the next authentication occurrence, the service knows which client is connecting based on the cookie data. The cookie contains information for multiple users, which means that users can all connect from the same IP address. If you see CORS issues with this method, you can increase the

timeouts.

> **Note:** For the Explicit Proxy connectivity method, only the cookie surrogate is available.

Refresh Times

The refresh time determines how long WSS remembers its association with the client. When this time expires, the following occurs.

- If you are using the Auth Connector to provide the interaction between the service and your LDAP deployment, the client receives the credential dialog and they must re-authenticate.
- If you are employing a SAML authentication method for this method, the IdP attempts to renegotiate and the client might not receive a credential dialog.

There is no inactivity timeout, which means you must define a Captive Portal for each location.

If for some reason the client connects to another service asset in the WSS datacenter—perhaps because of load-balancing—the user is re-prompted for credentials.

More information.

- See "About Captive Portal Authentication" on page 99.
- Consult the WSS Agent documentation for Captive Portal information.

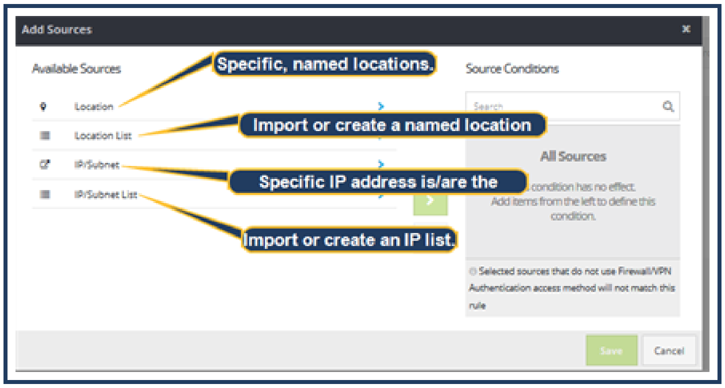
Define Authentication Policy

These procedures commence from the stage that you have locations defined in the portal.

Procedures

Firewall/VPN Access Method

1. Navigate to **Identity > Authentication Policy**.
2. Expand the **Authentication Policy** area.
3. Click **Add Rule**. The portal displays the policy editor.
4. Click **VPN/Firewall Locations**.
5. Click **Add Sources**.



Specific, named locations.

Import or create a named location

Specific IP address is/are the

Import or create an IP list.

condition has no effect.
Add items from the left to define this condition.

Selected sources that do not use Firewall/VPN Authentication access method will not match this rule

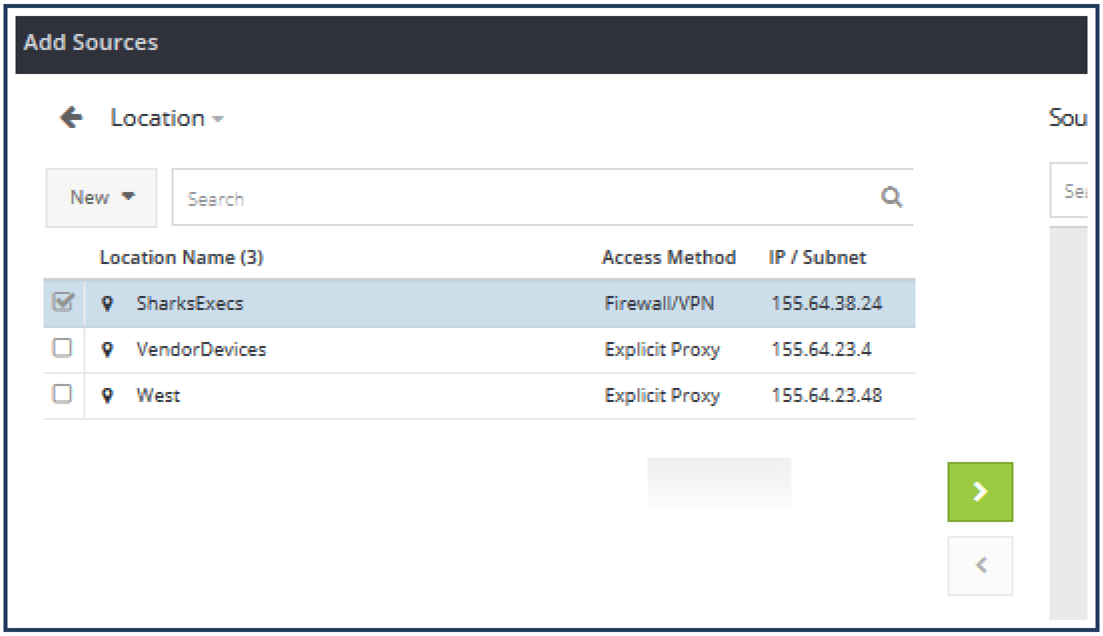
Select a location option.

- **Locations**–These are the named locations you created on the **Connectivity > Locations** page.
- **Location Lists**–If you used the **Object Library** to create a list of locations, you can select that with this option; or you create a new list of detected locations from this option.
- **IPs/Subnets**–You might have one or more internal segments that you are using to test a feature. You can enter the IP address(es) with this option.
- **IP/Subnet Lists**–If you used the **Object Library** to create a list of IP addresses, you can select that with this option; or you create a new list of detected IP addresses from this option.

> **Tip:** The policy you define depends on the authentication method–the Auth Connector or SAML. Do *not* mix locations that use different methods.

This procedure continues with the **Locations** option.

6. The policy editor displays all available locations. Take notice that this list includes Explicit Proxy locations if any are configured.



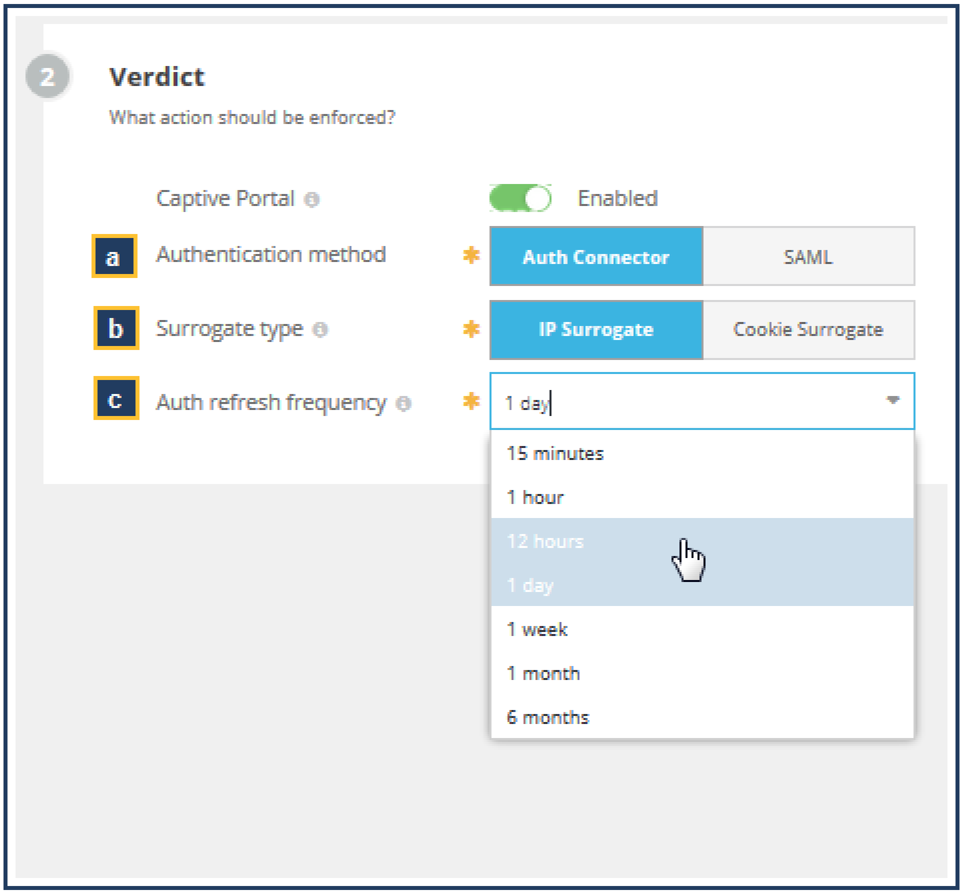
Add Sources

Location

		Location Name (3)	Access Method	IP / Subnet
☑		SharksExecs	Firewall/VPN	155.64.38.24
□		VendorDevices	Explicit Proxy	155.64.23.4
□		West	Explicit Proxy	155.64.23.48

Select one or more **Location Names** and click **Add**; click **Save**.

7. In the **Verdict** area, select the toggle to enable **Captive Portal**.



2 Verdict

What action should be enforced?

Captive Portal: Enabled

a Authentication method *: Auth Connector | SAML

b Surrogate type *: IP Surrogate | Cookie Surrogate

c Auth refresh frequency *: 1 day

a. Select the **Authentication Method** that you have configured for the location(s).

   If you not have yet configured the method, the portal displays a warning message that no Captive Portal enforcement occurs until it detects a method.

   > **Tip:** If you configured the Auth Connector as the SAML IdP, click **SAML**.

b. Select a **Surrogate Type**. Roll your mouse over the tool-tip icon if you require information about the difference between using an **IP** or **Cookie Surrogate**.

c. Select the **Auth Refresh Frequency**. By default, the setting is one day. That means 24 hours after authentication occurs, the client receives a credential dialog (for SAML, that might not occur).

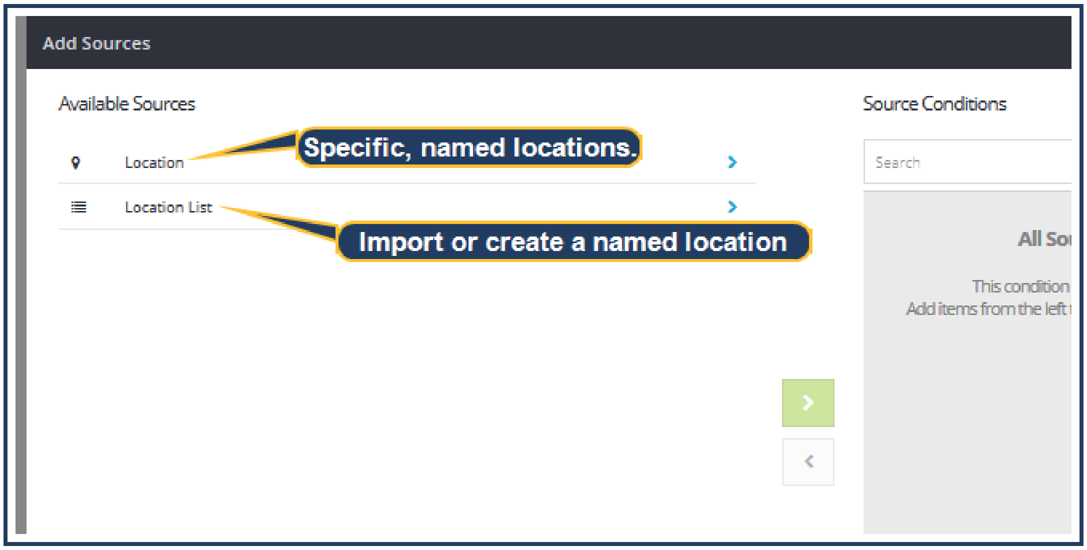
   Example Use Case–If the location is a guest WiFi network, you might elect to keep the frequency interval more brief versus a employee work segment.

d. Click **Finish**. The portal adds the new authentication rule row under Firewall/VPN Authentication.

8. Click **Activate**.

Explicit Proxy Access Method

1. Navigate to **Identity > Authentication Policy**.
2. Expand the **Authentication Policy** area.
3. Click **Add Rule**. The portal displays the policy editor.
4. Click **Explicit Proxy**.
5. Click **Add Sources**.



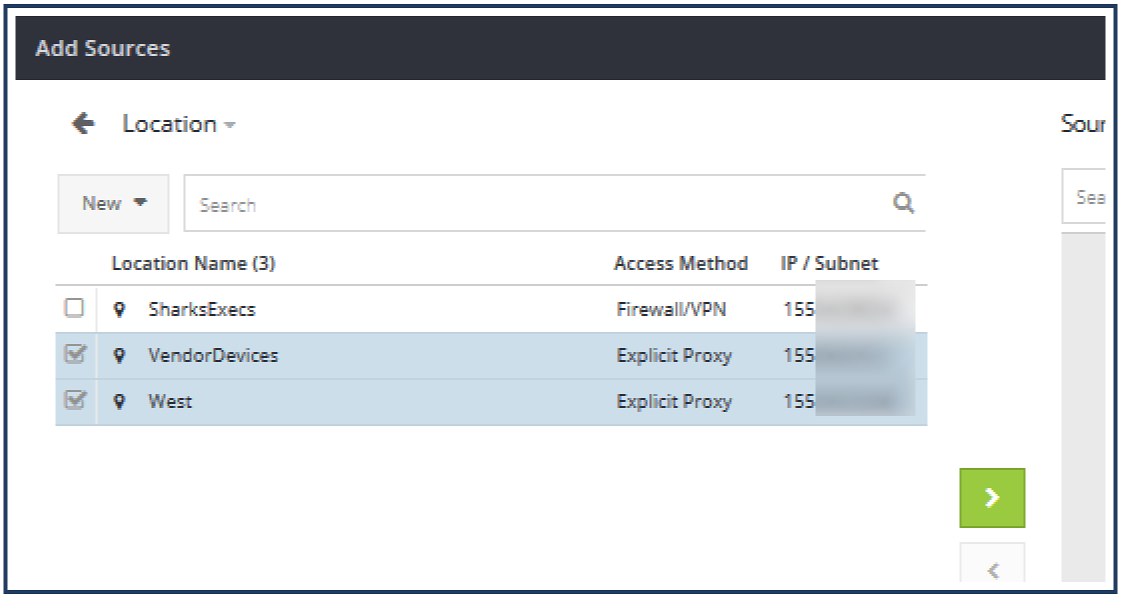
Select a location option.

- **Locations**–These are the named locations you created on the **Connectivity > Locations** page.
- **Location Lists**–If you used the **Object Library** to create a list of locations, you can select that with this option; or you can create a new list of detected locations from this option.

> **Tip:** The policy you define depends on the authentication method–the Auth Connector or SAML. Do *not* mix locations that use different methods.

This procedure continues with the **Locations** option.

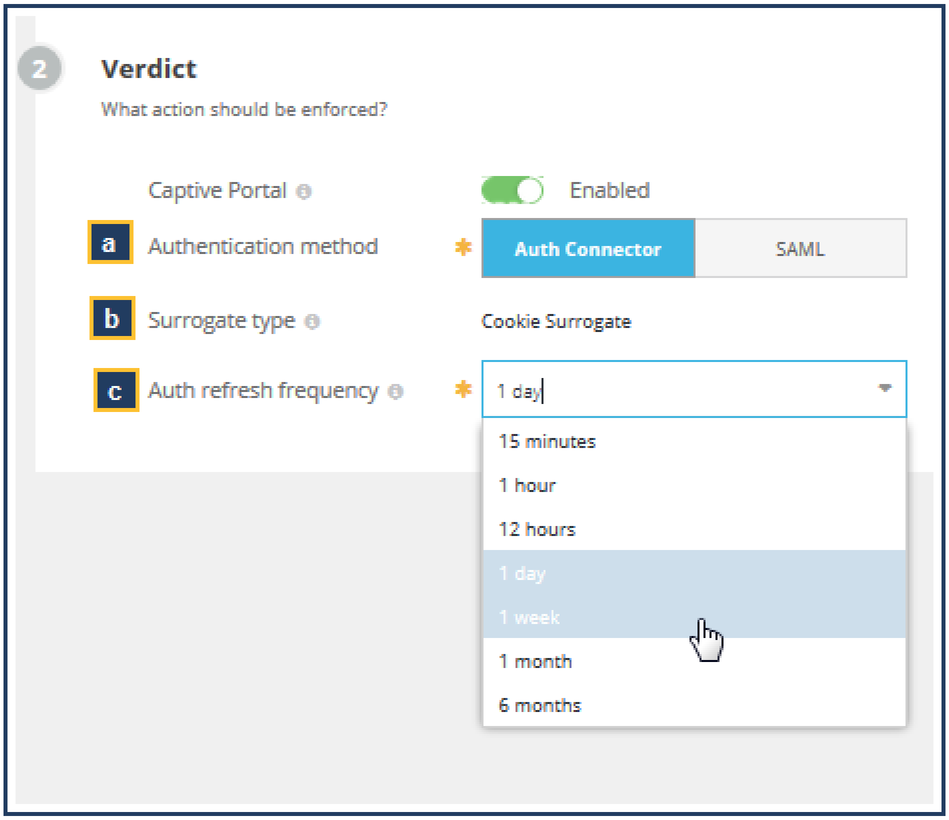
6. The policy editor displays all available locations. Take notice that this list includes Explicit Proxy locations if any are configured.



	Location Name (3)	Access Method	IP / Subnet
☐	SharksExecs	Firewall/VPN	155[redacted]
☑	VendorDevices	Explicit Proxy	155[redacted]
☑	West	Explicit Proxy	155[redacted]

Select one or more **Location Names** and click **Add**; click **Save**.

7. Select the toggle to enable **Captive Portal**.



2 Verdict

What action should be enforced?

Captive Portal: Enabled

Authentication method *: Auth Connector | SAML

Surrogate type: Cookie Surrogate

Auth refresh frequency *: 1 day

a. Select the **Authentication Method** that you have configured for the location(s).

   If you have not have yet configured the method, the portal displays a warning message that no Captive Portal enforcement occurs until it detects a method.

b. For Explicit Proxy, the only valid **Surrogate Type** is **Cookie**. See the Firewall/VPN Surrogate Types section above for details.

c. Select the **Auth Refresh Frequency**. By default, the setting is one day. That means twenty fours after authentication occurs, the client receives a credential dialog (for SAML, that might not occur).

   Example Use Case—If the location is a guest WiFi network, you might elect to keep the frequency interval more brief versus a employee work segment.

d. Click **Finish**. The portal adds the new authentication rule row under Firewall/VPN Authentication.

8. Click **Add Rule**; click **Activate**.

Exempt From Authentication

Captive Portal or SAML Web Security Service authentication methods, which are *redirection-based* methods, display a separate window for users to enter their credentials to continue. Some network issues might prevent the client systems from displaying these windows.

- CORS-related issues.
- Authentication looping with cloud-based IdP servers.
- The source device (for example, a legacy server) is not compatible with redirection-based authentication.
- A web application API call is not compatible with redirection-based authentication.

To mitigate this, add destinations and sources that you want exempted from authorization challenges.

Exemptable Sources	Exemptable Destinations
IP addresses/Subnets	Domains/URLs
Locations	IP addresses/Subnets
WSS Agent	Web Applications
Mobile Devices	Categories

About Clients That Are Not Forms-Based

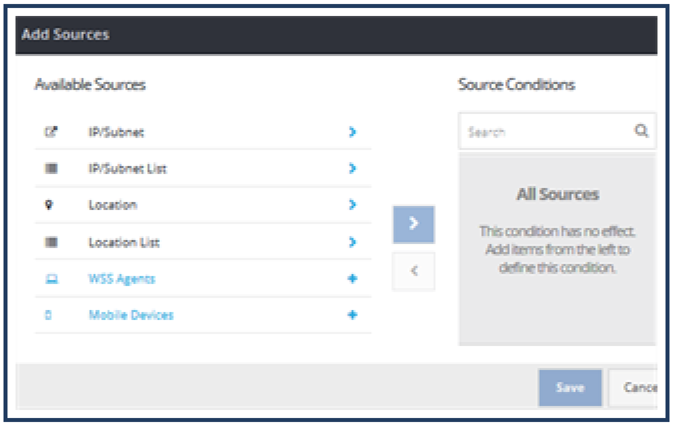
WSS has an option to exempt WSS Agent and mobile clients.

- WSS Agent:
  - If Captive portal is disabled, WSS Agent identifies itself as the logged-on user.
  - If Captive Portal is enabled, WSS Agent prompts for credentials before web requests are allowed.
- Mobile clients—The credentials are obtained from the installed certificate.

These options are here alternate authentication methods that might be supported in future WSS versions.

Procedure

1. Navigate to **Identity > Authentication Policy**.
2. Expand the **Global Exemptions** area.
3. Click **Add Auth Exemption**. The portal displays the Auth: New Exemption Rule.
4. Click **Add Sources**.



- All already configured entries or lists populate any selection. For example, if you click **Locations**, you can select from any location that currently sends traffic to the WSS account.
- **WSS Agents** and **Mobile Devices** are static objects; selecting them means the exemption applies to all connections from each of those access methods.

5. (Optional) If you need to quickly exempt a source, you can create a new entry from this wizard. For example, you need to immediately exempt a new IP address.

   a. Click **IPs/Subnets**.

   b. Select **New > IP/Subnet**.

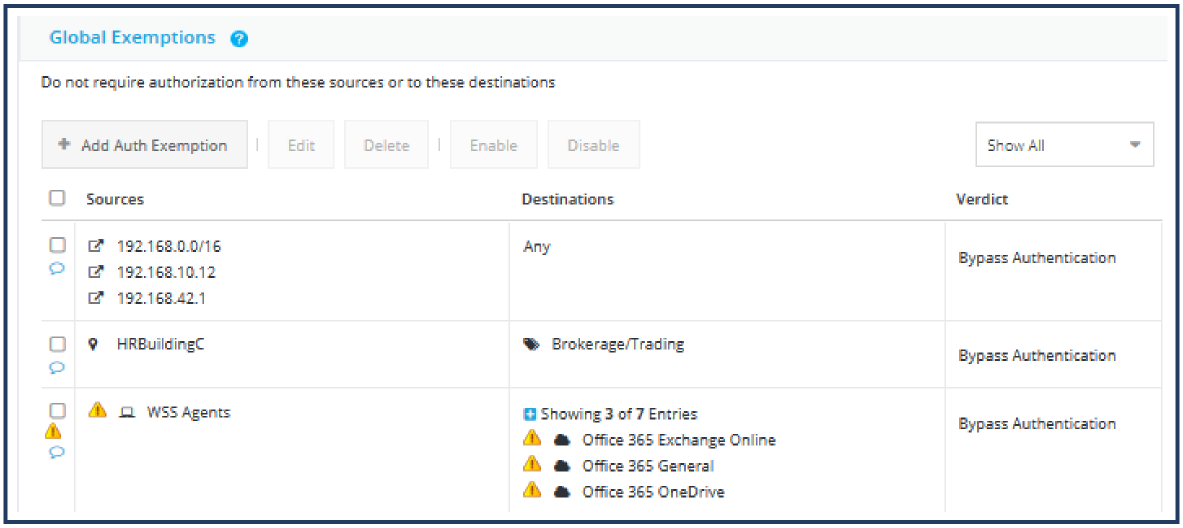
   c. Enter a new address (or import a list from a text file).

   d. Click **Save**.

6. Click **Add Destinations**.

   Select the destination elements that are exempt from authentication and click **Save**.

7. Click **Add Rule**. This creates a new Auth Exemption policy rule.



Do not require authorization from these sources or to these destinations

□	Sources	Destinations	Verdict
□	192.168.0.0/16 192.168.10.12 192.168.42.1	Any	Bypass Authentication
□	HRBuildingC	Brokerage/Trading	Bypass Authentication
□	⚠ WSS Agents	Showing 3 of 7 Entries ⚠ Office 365 Exchange Online ⚠ Office 365 General ⚠ Office 365 OneDrive	Bypass Authentication

8. You can add additional rule. When satisfied, click **Activate**.
9. Verify with your employees that their clients are no longer prompted for credentials because of the new policy.

Reference: Authentication IP Addresses

The Symantec Web Security Service Auth Connector communicates with devices in the geographically located data centers.

The Symantec Operations team maintains the following Knowledge Base article.

- https://knowledge.broadcom.com/external/article?articleId=165389

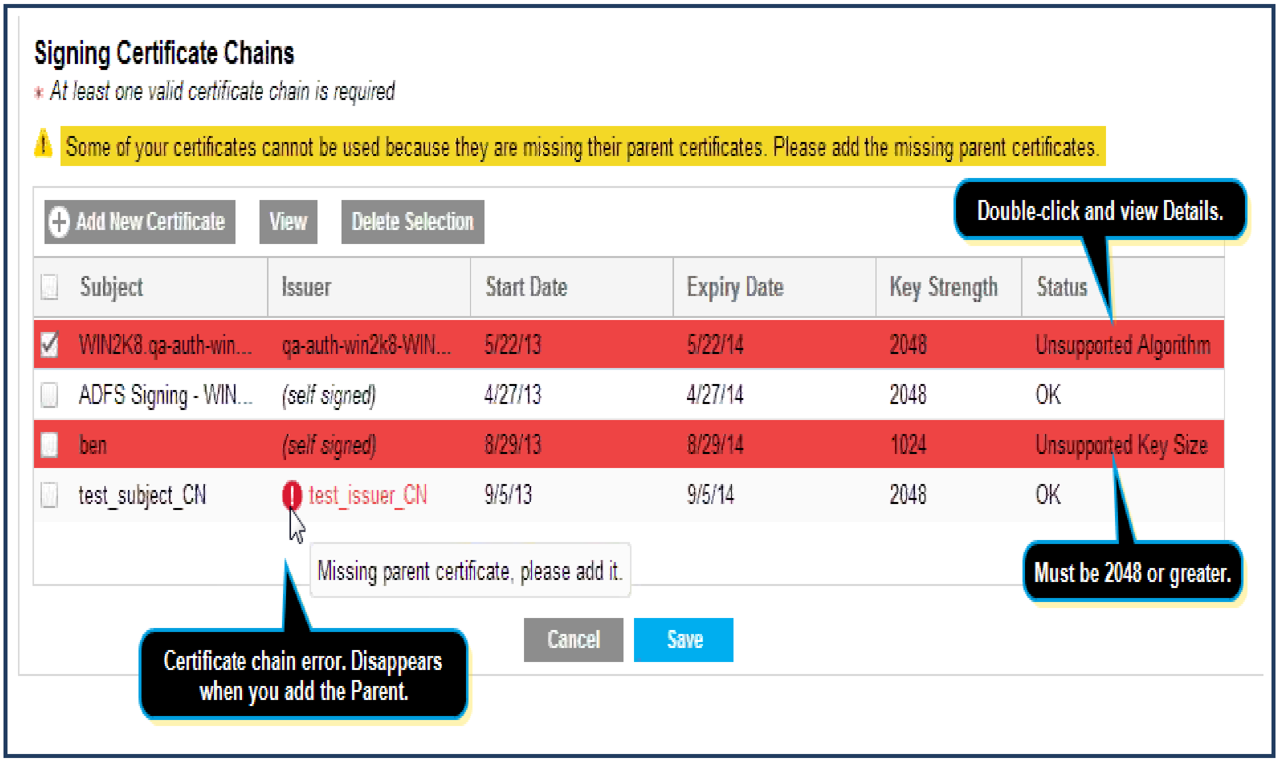
Troubleshoot SAML Authentication

Certificate Warnings

Sixty days before a certificate in the signing chain expires, the Web Security Service sends the administrators registered with the account a notification e-mail. Subsequent e-mails continue. This allows ample time to log in to the portal and add valid certificates.

Certificate Errors

Identity > SAML Authentication



Signing Certificate Chains

* *At least one valid certificate chain is required*

⚠ Some of your certificates cannot be used because they are missing their parent certificates. Please add the missing parent certificates.

□	Subject	Issuer	Start Date	Expiry Date	Key Strength	Status
☑	WIN2K8.qa-auth-win...	qa-auth-win2k8-WIN...	5/22/13	5/22/14	2048	Unsupported Algorithm
□	ADFS Signing - WIN...	*(self signed)*	4/27/13	4/27/14	2048	OK
□	ben	*(self signed)*	8/29/13	8/29/14	1024	Unsupported Key Size
□	test_subject_CN	! test_issuer_CN	9/5/13	9/5/14	2048	OK

Missing parent certificate, please add it.

Double-click and view Details.

Must be 2048 or greater.

Certificate chain error. Disappears when you add the Parent.

- **Unsupported Algorithm**–Symantec supports and recommends **SHA2** for WSS SAML integration. SHA1 is supported but not recommended. The limit for RSA and DSA algorithms is 2048.
- **Unsupported Key Size**–For appropriate security level, the **Key Size** must be 2048 or greater.
- **Issuer**–WSS detects a break in the certificate chain, it displays the orphaned certificate and prompts for you to add the correct parent certificate. Click **Add New Certificate** and add the contents.

Clear Associated Auth Surrogates and Restart Authentication

If a client is experiencing SAML-related connection issues with WSS, you can instruct the user to enter a URL that stops the connection to WSS. The URL is `https://notify.threatpulse.net/logout`. The following occurs.

- The user is logged out of the asset that currently maintains that connection in the WSS datacenter. If the user has existing valid sessions to other assets, those sessions will continue to be valid.
- The user is *not* logged out of the SAML IdP.
- If a user attempts to browse after logging out, they *might* be immediately be re-authenticated without the credential prompt. WSS redirects to the IdP, where the user is still logged in, for authentication. Typically, the IdP uses a session cookie to identify the user's authenticated session. The IdP then redirects back to WSS with a SAML assertion, and the user is signed back to the WSS asset. Because of this, the best practice is to invoke the URL in a logout script or after the browser is closed so that session cookies are forgotten.

Internet Explorer Sessions

Some 3rd party extensions in Internet Explorer might cause the process to hang and never fully close down. As a result, the sessions might not end when an employee closes the IE window. The sessions will eventually time out, however. To see more about this issue, refer to the following Microsoft article.

http://answers.microsoft.com/en-us/ie/forum/ie9-windows_vista/after-closing-ie-windows-iexploreexe-processes-are/a3b1536d-1732-4f63-92d3-8fa927946d80

Other Errors

SAML Error Description/Symptom	Possible Cause
Employees receiving **Failed to Connect** browser errors after attempting to authenticate.	■ The employee's browser might not trust the SSL server certificate from the IdP. ■ Certificate error or not correctly created.
Various run-time errors.	The IdP does not recognize the WSS entity ID because the federation is broken (or was never created) at the IdP.
The IdP fails to authenticate a known valid user.	User does not exist or entered wrong password multiple times.

SAML Bypass List

- The following Knowledge Base article lists what the WSS SAML policy currently bypasses.

  SAML Bypass List KB Article