Copyrights

Copyright © 2019 Symantec Corp. All rights reserved. Symantec, the Symantec Logo, the Checkmark Logo, Blue Coat, and the Blue Coat logo are trademarks or registered trademarks of Symantec Corp. or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE. SYMANTEC CORPORATION PRODUCTS, TECHNICAL SERVICES, AND ANY OTHER TECHNICAL DATA REFERENCED IN THIS DOCUMENT ARE SUBJECT TO U.S. EXPORT CONTROL AND SANCTIONS LAWS, REGULATIONS AND REQUIREMENTS, AND MAY BE SUBJECT TO EXPORT OR IMPORT REGULATIONS IN OTHER COUNTRIES. YOU AGREE TO COMPLY STRICTLY WITH THESE LAWS, REGULATIONS AND REQUIREMENTS, AND ACKNOWLEDGE THAT YOU HAVE THE RESPONSIBILITY TO OBTAIN ANY LICENSES, PERMITS OR OTHER APPROVALS THAT MAY BE REQUIRED IN ORDER TO EXPORT, RE-EXPORT, TRANSFER IN COUNTRY OR IMPORT AFTER DELIVERY TO YOU.

Symantec Corporation

350 Ellis Street
Mountain View, CA 94043

www.symantec.com
Symantec Web Security Service: 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 Access 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.

This document provides conceptual information and installation tasks. The document breaks out information in the following sections.

- "About Web Security Service User Authentication" on page 10
- "About the Auth Connector Integration" on page 16
- "About SAML Integration" on page 33
- "Captive Portal Tasks" on page 110
- "Admin Tasks and Reference" on page 140
- "Troubleshoot..." on page 154

This document contains topics collected from the Web Security Service online documentation. For the complete doc set, see:

Symantec Support Site > WSS Documentation
### Notes—Remote Users/Unified Agent (E, F) .................................................. 12
### Notes—Mobile Users (A, B, E, F) .............................................................. 12
### Link Launch ............................................................................................... 12

### Select an Authentication Method .............................................................. 14
### Why is an Auth Method Required? .......................................................... 14
### Auth Connector ......................................................................................... 14
### Third-Party SAML .................................................................................... 14
### SAML With Auth Connector as IdP .......................................................... 15

### About the Auth Connector Integration .................................................... 16
#### A—Active Directory Connection ........................................................... 17
#### B—Portal Connection ............................................................................ 18
#### C—IPsec Connections ........................................................................... 18
#### D—User Connections ............................................................................ 18
#### E—Mobile/Remote Connections ............................................................. 18
   Example Configuration: ....................................................................... 20

### Deploy the AuthConnector ..................................................................... 21
#### About Failover ....................................................................................... 21
#### About Proxy Aware Capability ............................................................. 21
#### Technical Requirements ..................................................................... 21

### Review Imported Users and Groups ...................................................... 31
#### Imported From SAML .......................................................................... 31
#### Imported From the Auth Connector ....................................................... 31

### About SAML Integration ........................................................................ 33
#### SAML Review—Federation ................................................................. 33
#### Entities .................................................................................................. 33
#### Assertions .............................................................................................. 33
#### Overview Diagram ................................................................................ 34
#### SAML Flow ............................................................................................ 34
#### Support for Multiple AD Forests ............................................................ 35
#### Alternate Deployment ............................................................................ 35
#### Additional Information and Limitations ............................................... 35

### About the Auth Connector as a SAML IdP .............................................. 37
   Use Cases for Auth Connector as SAML IDP ........................................ 37
   Current Limitation .................................................................................. 37
   Data Flow ................................................................................................ 38
   About User/Group Memberships ............................................................ 39

### About Challenge-based Auth (Captive Portal) ....................................... 40
   A—Firewall/VPN/Guest WiFi Over IPSec .............................................. 40
   B—Explicit Proxy .................................................................................... 41
   C—Remote Users (Unified Agent) ............................................................ 41
D—Quick Authentication Demonstration (Roaming Captive Portal) .................................................. 41
Additional Information ................................................................................................................... 41
About Challenges ............................................................................................................................ 42
About Roaming Captive Portal ....................................................................................................... 43
Data Flow ........................................................................................................................................ 43
Additional Notes .............................................................................................................................. 44
Prepare Microsoft AD FS for Federation .......................................................................................... 45
Federate the Web Security Service and AD FS ............................................................................... 47
  Technical Requirements ................................................................................................................. 47
  Optional—Exempt Sources/Destinations from Authorization ......................................................... 50
Import Users and Groups for SAML Auth ......................................................................................... 51
Install The Auth Connector as the IDP ............................................................................................. 55
Integrate Auth Connector as the SAML IdP ...................................................................................... 62
  Technical Requirements ............................................................................................................... 62
Integrate Symantec VIP Access Manager as the SAML IdP ............................................................. 66
  Technical Requirements ............................................................................................................... 66
Integrate Microsoft Azure as the SAML IdP .................................................................................... 72
  Technical Requirements ............................................................................................................... 72
  Synchronization ............................................................................................................................ 85
  Policy ............................................................................................................................................. 85
  (Optional) Rebrand Login Page ..................................................................................................... 86
  Exemptions .................................................................................................................................... 86
Integrate Google G Suite as a SAML IdP ......................................................................................... 87
  Technical Requirements ............................................................................................................... 87
Integrate Okta as the SAML IdP ....................................................................................................... 94
  Technical Requirements ............................................................................................................... 94
  Synchronization ............................................................................................................................ 102
  Known Issue ................................................................................................................................. 102
Integrate Ping Identity as the SAML IdP .......................................................................................... 104
  Technical Requirements ............................................................................................................... 104
Captive Portal Tasks .......................................................................................................................... 110
Captive Portal Surrogates and Times ............................................................................................... 111
  Supported Access Methods .......................................................................................................... 111
  About the Authentication Policy .................................................................................................... 111
  Firewall/VPN Surrogate Types ...................................................................................................... 111
  Refresh Times ................................................................................................................................ 111
  Define Authentication Policy ......................................................................................................... 112
Enable Roaming Captive Portal ........................................................................................................ 118
Configure Browsers to Receive Auth Challenge .............................................................................. 121
Enable Roaming Captive Portal on iOS ............................................................................................ 123
Enable Roaming Captive Portal on Android ..................................................................................... 127
Captive Portal Surrogates and Times ............................................................................................... 130
  Supported Access Methods .......................................................................................................... 130
# About the Authentication Policy

Firewall/VPN Surrogate Types ..................................................... 130
Refresh Times ............................................................................. 130
Define Authentication Policy ......................................................... 131
Exempt From Authentication ......................................................... 137
   About Clients That Are Not Forms-Based .................................. 137

# Admin Tasks and Reference

Reference: Required Locations, Ports, and Protocols .......................... 141
   Symantec Resource .................................................................. 141
   Access Methods ..................................................................... 141
   Authentication ...................................................................... 144
   Cloud-to-Premises DLP ............................................................ 144
Reference: Authentication IP Addresses ............................................ 145
Forward Specific User and Group Names to the Service ....................... 146
Add a Gateway Firewall/VPN Location ........................................... 148
Add an Explicit Proxy Location ..................................................... 150
Add a Proxy Forwarding Location .................................................. 152

# Troubleshoot

Auth Connector ........................................................................... 154
SAML .......................................................................................... 154
New Users/Groups Are Not Available for Policy ............................... 154
I Entered the Incorrect AuthConnector Password ................................ 155
I Cannot Remove the Auth Connector from Windows Server 8 (Pro) ........ 155
Troubleshoot SAML Authentication ............................................... 155
   Certificate Warnings ............................................................... 155
   Certificate Errors ................................................................ 156
   Internet Explorer Sessions ....................................................... 156
   Other Errors ......................................................................... 156
   SAML Bypass List .................................................................. 157
Captive Portal Diagnostic Messages .................................................. 158
About Web Security Service User Authentication

The configured Symantec Web Security Service access method determines how the service recognizes users and groups that are viewable in reports and available for selection in advanced policy.

Why is an Auth Method Required?

Most Access Methods require an authentication method, which provides the user and group information necessary for pre-traffic policy creation and reporting. While deploying an authentication method might be not required for specified access methods, some WSS functionality becomes limited without it.

Authentication Matrix by Access Method

<table>
<thead>
<tr>
<th>Access Method</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall/VPN</td>
<td>Auth Connector: Domain controller query.</td>
<td>Auth Connector: Client Logon Application (large enterprises with many domain controllers).</td>
<td>SAML with Auth Connector as IDP</td>
<td>SAML with AD FS (requires Captive Portal)</td>
<td>Captive Portal*</td>
<td>Captive Portal</td>
</tr>
<tr>
<td>Proxy Forwarding</td>
<td>Auth Connector required for pre-traffic custom policy based on user/group names.</td>
<td>Authentication occurs on local proxy device.</td>
<td>SAML with Auth Connector as IDP</td>
<td>SAML with AD FS (requires Captive Portal)</td>
<td>Captive Portal</td>
<td>Captive Portal</td>
</tr>
<tr>
<td>Explicit Proxy [known network location]</td>
<td>Auth Connector required if Captive Portal (E) is enabled (including SEP).</td>
<td>Auth Connector required for SEP Seamless Authentication.</td>
<td>SAML with Auth Connector as IDP</td>
<td>SAML with AD FS (requires Captive Portal)</td>
<td>Captive Portal</td>
<td>Captive Portal</td>
</tr>
<tr>
<td>Explicit Proxy [unknown network location]</td>
<td>Auth Connector required if Roaming Captive Portal (E) is enabled.</td>
<td>Roaming Captive Portal</td>
<td>SAML with Auth Connector as IDP</td>
<td>Captive Portal</td>
<td>Captive Portal</td>
<td>Captive Portal</td>
</tr>
</tbody>
</table>
### Authentication Options

<table>
<thead>
<tr>
<th>Access Method</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Agent</td>
<td>Auth Connector required for policy</td>
<td>based on group affiliation and/or if</td>
<td>Captive Portal</td>
<td>User information obtained from the</td>
<td>Captive Portal</td>
<td>User information obtained from the</td>
</tr>
<tr>
<td></td>
<td>Captive Portal</td>
<td>Captive Portal</td>
<td>Group affiliation.</td>
<td>local cached credentials, but the</td>
<td>Captive Portal</td>
<td>local cached credentials, but the</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Auth Connector is required to obtain</td>
<td></td>
<td>Auth Connector is required to obtain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Group affiliation.</td>
<td></td>
<td>Group affiliation.</td>
</tr>
</tbody>
</table>

* Form-based auth challenge.

### Source IP Available?

<table>
<thead>
<tr>
<th>Access Method</th>
<th>Original Client Source IP Available?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall/VPN (IPsec)</td>
<td>Yes</td>
</tr>
<tr>
<td>Explicit Proxy (from known</td>
<td>No</td>
</tr>
<tr>
<td>network location)</td>
<td></td>
</tr>
<tr>
<td>Explicit Proxy (from unknown</td>
<td>No</td>
</tr>
<tr>
<td>network location)</td>
<td></td>
</tr>
<tr>
<td>Trans-Proxy (explicit over</td>
<td>Yes</td>
</tr>
<tr>
<td>IPsec)</td>
<td></td>
</tr>
<tr>
<td>Proxy Forwarding</td>
<td>Yes (XFF)</td>
</tr>
<tr>
<td>Unified Agent</td>
<td>No</td>
</tr>
<tr>
<td>Mobile Device Service</td>
<td>No</td>
</tr>
</tbody>
</table>

### Notes—Firewall/VPN and Trans-Proxy Access Methods (A, B, C, D, E)

When deploying the VPN-to-VPN router/firewall device configuration and the Explicit Proxy over IPsec (Trans-Proxy) Access Methods, you must deploy an authentication method. You can deploy the Symantec Auth Connector, integrate with your existing SAML implementation, or use a hybrid (SAML with Auth Connector as the IDP). 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.

For more details about the about the ACLogon App, see the relevant section in "About the Auth Connector Integration" on page 16.
Notes—Proxy Forwarding (A, B, F)

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 if you plan to create custom policy based on your AD user/group names (applies to most solutions).

Notes—Explicit Proxy (PAC Files) (A, B, C, D, E)

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.

If you employ SEP with the Seamless Authentication option, Captive Portal is not required, but the Auth Connector is.

The Auth Connector is required if you plan to create custom policy based on your AD user/group names (applies to most solutions).

Alternate: integrate or deploy a SAML solution.

Notes—Remote Users/Unified Agent (E, F)

For users that access the corporate network from outside the corporate site (for example, remote or traveling/roaming users on laptops), you must install the Unified Agent application. The Unified 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.

Furthermore, the Auth Connector is required if you plan to create custom policy based on your AD group names.

Notes—Mobile Users (A, B, E, F)

When users enroll their registered devices, they must enter their network credentials. As long as the VPN profile remains on the device, the Web Security Service identifies web traffic per user. Requires the Auth Connector.

The Auth Connector is required if you also enable Roaming Captive Portal.

Link Launch

A, B (Auth Connector)

- Concept—"About the Auth Connector Integration" on page 16
  - Domain controller query and Client Logon Application for larger-scale deployments—"Deploy the AuthConnector" on page 21.

C,D (SAML)

Integrate with your existing Active Directory deployment.
SAML with Auth Connector as the Identity Provider (IDP).

- Concept—"About the Auth Connector as a SAML IdP" on page 37.
- Begin Integration—"Install The Auth Connector as the IDP" on page 55.

SAML with other IDP applications.

- Concept—"About SAML Integration" on page 33.
- "Integrate Symantec VIP Access Manager as the SAML IdP" on page 66
- "Integrate Google G Suite as a SAML IdP" on page 87
- "Integrate Microsoft Azure as the SAML IdP" on page 72
- "Integrate Okta as the SAML IdP" on page 94
- "Integrate Ping Identity as the SAML IdP" on page 104

**Note:** Captive Portal required with SAML.

E (Captive Portal)

- Concept—"About Challenge-based Auth (Captive Portal)" on page 40
  - "Captive Portal Surrogates and Times" on page 130 (Firewall/VPN and Explicit Proxy only)
- Concept—"About Roaming Captive Portal" on page 43
Select an Authentication Method

For employee credential information in access logs, which is required for reporting, and pre-traffic policy creation and enforcement, the Symantec Web Security Service must receive user and group information. While deploying an authentication method might be not required for specified access methods, some Web Security Service functionality becomes limited without it.

Why is an Auth Method Required?

Most Access Methods require an authentication method, which provides the user and group information necessary for pre-traffic policy creation and reporting. "About Web Security Service User Authentication" on page 10 provides an authentication matrix and additional notes per method.

Auth Connector

The Symantec Auth Connector is an authentication agent installed on your Active Directory.

- "About the Auth Connector Integration" on page 16—Describes the Auth Connector footprint and when it is required.
- "Deploy the AuthConnector" on page 21—Describes how to integrate the Auth Connector into your Active Directory environment.

Third-Party SAML

The Symantec Web Security Service 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.

- "About SAML Integration" on page 33—Describes the SAML integration.

Active Directory Federation Services (ADFS)

- "Import Users and Groups for SAML Auth" on page 51—Begin the SAML ADFS integration walkthrough.

Third-Party IdPs

- "Integrate Symantec VIP Access Manager as the SAML IdP" on page 66
- "Integrate Google G Suite as a SAML IdP" on page 87
- "Integrate Microsoft Azure as the SAML IdP" on page 72—With SCIM.
- "Integrate Okta as the SAML IdP" on page 94
- "Integrate Ping Identity as the SAML IdP" on page 104
SAML With Auth Connector as IdP

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

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

- "About the Auth Connector as a SAML IdP" on page 37—Describes how the Auth Connector provides this functionality.
- "Install The Auth Connector as the IDP" on page 55—Begin the walkthrough by installing the Auth Connector with the IDP configuration options.
About the Auth Connector Integration

The Auth Connector is 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 login and logout activity of domain users to build an IP-to-username-matrix.
- Informs the WSS of user login and logout 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.

If you are concerned about the scalability of your Domain Controller, install the Auth Connector onto member servers.

This section describes the Auth Connector agent network footprint.

When Is The Auth Connector Required?

The Auth Connector is not required for all Access Methods. However, as mentioned above, the Auth Connector is required if you plan to create custom policy based on user and group names and in some methods view reports based on user/groups—the sole exception is Explicit Proxy without Captive Portal enabled because no authentication occurs. The following matrix illustrates the Auth Connector use cases.

- **No**—The Auth Connector is not required to process your web traffic through the Web Security Service; however, some functionality might be limited.
- **Yes**—The Auth Connector is unconditionally required for that Access Method.
- **Pre-Traffic**—For some methods, you can create policy after employees generate traffic without the Auth Connector deployed. However, if you require to define policy before traffic begins, you must install the Auth Connector.

<table>
<thead>
<tr>
<th>Access Method</th>
<th>Variations</th>
<th>Must Deploy</th>
<th>User Reporting</th>
<th>Pre-traffic Policy Creation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall/VPN</td>
<td>Standard IPsec</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Captive Portal enabled</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Explicit Over IPsec</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Proxy Forwarding</td>
<td>All</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Remote Users (Unified Agent or SEP)</td>
<td>Includes Captive Portal</td>
<td>Yes*</td>
<td></td>
<td>*Yes—Required if you plan to enforce group-based policies.</td>
</tr>
<tr>
<td></td>
<td>SEP with Seamless Authentication</td>
<td>No</td>
<td>No</td>
<td>No—Report-based user name policy only after users send traffic.</td>
</tr>
<tr>
<td>Mobile Device Service (MDS)</td>
<td>All</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Access Method Variations

<table>
<thead>
<tr>
<th>Access Method</th>
<th>Variations</th>
<th>Must Deploy</th>
<th>User Reporting</th>
<th>Pre-traffic Policy Creation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explicit Proxy</td>
<td>Standard</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Roaming Captive Portal enabled</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## With What Does the Auth Connector Communicate?

The Auth Connector comprises three communication footprints when completing a Web Security Service 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 Web Security Service 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)

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

- Domain Controller Query: This is the default method for all Access 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 Web Security Service Control Pod through auth.threatpulse.net on port 443 and transfers the AD users and group names.

  The Web Security Service returns IPsec endpoint information to the Auth Connector.

- AClonon 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 the AClonon App and make it available to each client system. See the About the AClonon App section below.

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

Tip: It is possible to limit this list to specific users and groups.

B—Portal Connection

The Auth Connector contacts the Web Security Service 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 and shows in a connected state.

D—User Connections

User web requests connect to the Data Pod. The Web Security Service 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 Unified 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 "Reference: Authentication IP Addresses" on page 145 prevents proper group membership identification, which causes group-based policies to fail.

About User/Group Memberships

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

Group memberships are identified through a different process, however. The Web Security Service 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 Web Security Service 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 Web Security Service to re-query group membership.

To perform an on-demand retrieval of all user and group names, return to the Authentication > Auth Connector tab 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.

About the ACLogon App

Symantec recommends this option 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. 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.

Obtain the application and release notes (see the Help to obtain the download).
Deploy the AuthConnector

To create custom policy based on user and group names before those groups generate traffic, you must download the Symantec Auth Connector to at least one or member server. The Auth Connector connects to the Symantec Web Security Service and provides the user/group information from the Active Directory (AD). See "About the Auth Connector Integration" on page 16, which provides more detail about the Auth Connector agent footprint.

For heightened security, Symantec strongly recommends installing the Auth Connector on a dedicated server that is not routing web transactions to and from the Web Security Service.

About Failover

To achieve failover, install Auth Connector on a second domain controller. 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 the Web Security Service. If the primary domain controller goes down, the backup immediately assumes the task.

The Auth Connector is proxy-aware.

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 below.

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 Web Security Service.

Member Servers Installation Prerequisites

- Windows Server 2008 R2 is the minimum version on which the Auth Connector can be installed.

- The installation requires:
  - The user performing the install be a member of the Domain to which the Auth Connector is installed.
  - The user have local administrative privileges on that machine.

- 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 is 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, the Web Security Service cannot identify users until the password matches.

- The Auth Connector requires that a newer Entrust CA certificate Entrust(2048) be installed on the Windows 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](http://support.microsoft.com/kb/931125).

**Procedure**

**Step 1—Add an Auth Connector location to the Web Security Service.**

1. Select **Authentication > Auth Connector**.
2. Click **Add Auth Connector**.
3. Connect to the service.

   ![Add Auth Connector](image)

   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 Web Security Service 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 back 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 selected as the **Primary**.

### Auth Connectors

<table>
<thead>
<tr>
<th>Primary</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SJSHQBackup [Edit]</td>
</tr>
<tr>
<td></td>
<td>SJSHQPrimary [Edit]</td>
</tr>
</tbody>
</table>

### 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 **Authentication > Auth Connector** tab, click **32-bit** in the **Download Windows Installer** area.
2. If this is the first time you are attempting to download the application, the portal displays the Profile dialog.
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 Unified Agent. The fields with blue asterisks (*) are required.

Click Save to update your profile and then close the dialog.

3. 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—Install the Primary Auth Connector on a Domain Controller or Member Server.

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

Tip: Only install the Auth Connector on a server that does not require protection provided by the Web Security Service. Connections to the service will work, but all users connected to that datapod location display in reports as unauthenticated user.
1. On the Domain Controller or 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.

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

5. Link this Auth Connector installation with the Web Security Service by entering the **Auth Connector Unique Name** and **Password** that you obtained/defined during **Step 1**.
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 Web Security Service deployment does not 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 Access Method only—You have a choice for how the Auth Connector resolves and maintains the IP-to-user map.
a. Select an option: Click **Next**.

**Tip:** For more details about the following two methods, see "About the Auth Connector Integration" on page 16.

- **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.

You must download the application and make it available to each client system. The easiest way to deploy it is through Active Directory logon and logoff scripts implemented through group policy and the group policy editor. Refer to the Client Application Release Notes for group policy information.

Obtain the application and release notes:

Obtain the app from the same step in the WebGuide version of this document.

http://portal.threatpulse.com/docs/am/AccessMethods/auth/authconn_config_ta.htm

b. Click **Next**.

- If you did not select the **Logon App** option, proceed to step 11.
- 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 5—(Optional) Repeat Step 4 to install the backup Auth Connector on a second, live Active Directory or member server.

The Auth Connector Unique Name is slightly different—the same number appended with the name you assigned in Step 2.

Step 6—Verify the Connection.

1. Back on the Authentication > Auth Connector page, review the Auth Connector status icons.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Connection Status Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>The Web Security Service and the installed Auth Connector are communicating.</td>
</tr>
<tr>
<td>🟡</td>
<td>The Web Security Service does not detect the specified Auth Connector.</td>
</tr>
<tr>
<td>🟢</td>
<td>An error related to the authentication process occurred. Verify that the Active Directory is functioning correctly.</td>
</tr>
<tr>
<td>🟢</td>
<td>A previously successful Auth Connector to Web Security Service configuration is currently not connected. Verify all Domain Controller and Web Security Service configurations.</td>
</tr>
</tbody>
</table>

2. In the Web Security Service 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 as the Web Security Service performs an automatic sync operation once every 24 hours. To perform an immediate, manual sync, click Refresh.

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

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

An alternative to the direct connection to the Web Security Service (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 Symantec 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.
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—(Optional) Specify which User and Group names are forwarded to the service.**

By default, the Auth Connector sends the following to the Web Security Service.

- 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).

If your LDAP deployment contains a large number of groups and users, consider sending user and group information for only those who require advanced policy checking. If you perform this option, do not open the firewall for outbound 443/tcp from the Auth Connector before you complete this task; if you do, the Auth Connector sends every name and policy gets applied. See .

**Step 9—Retrieve the User and Group Names from the AD.**

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

Group memberships are identified through a different process, however. The Web Security Service 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 Web Security Service 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 Web Security Service to re-query group membership.

To perform an on-demand retrieval of all user and group names, return to the **Authentication > Auth Connector** tab 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.

**Next Step**

- "Review Imported Users and Groups" on page 31
Review Imported Users and Groups

The Web Security Service can receive your employee user and group names from either the Auth Connector deployment method or from a SAML deployment—from manual importing or synchronized from a supported SAML Identity Provider (IDP).

Imported From SAML

If your authentication method is SAML, see "Import Users and Groups for SAML Auth" on page 51.

Imported From the Auth Connector

If you deploy the Symantec Auth Connector, the Web Security Service 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.

The Web Security Service automatically performs an AD refresh once a week; however, you can manually initiate a sync operation. In Service mode, select Authentication > 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—The Web Security Service performs an AD refresh once per week 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 (**Solutions** mode > **Content Filtering** > **Policy**). 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.

**Next Steps**

- "**Forward Specific User and Group Names to the Service**" on page 146
- "**Reference: Authentication IP Addresses**" on page 145
About SAML Integration

The Symantec Web Security Service 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 the Web Security Service.

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

Entities

Two *entities* comprise SAML authentication.

- Identity Provider (IdP)—Identify stores, which might contain a back-end directory of users. IdPs authenticate your users.
  - Natively, Symantec tested with and supports Microsoft® Active Directory Federation Services (AD FS) 2.0.
  - You can also use the Auth Connector as an IdP, which allows SSO when specific configurations are met. See "About the Auth Connector as a SAML IdP" on page 37.
  - The Web Security Service also supports the use of the following applications when configured to be a SAML IdP.
    - Symantec VIP Access Manager
    - Google G Suite
    - Microsoft Azure (with SCIM 2.0)
    - Okta
    - Ping ID
- Service Provider (SP)—Provides users with access to applications or services. In this deployment, the Web Security Service is the SP.

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

Assertions

The Web Security Service 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.
Overview Diagram

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

SAML Flow

1—The SP (Web Security Service) 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 the Web Security Service (however, the service is not aware of the user’s credentials).

4—The Web Security Service 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 Web Security Service redirects the user to the website and creates an authenticated session for the user.
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 the Web Security Service. 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.

Alternate Deployment

Because it uses the LDAP architecture, you can use the Auth Connector server as the IDP. All redundant servers must share the same hostname, which is the hostname in the SAML redirect endpoint.

Additional Information and Limitations

- The Web Security Service only supports SAML 2.0.

- The Web Security Service 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, the Web Security Service cannot authenticate explicit HTTPS requests without SSL Intercept enabled.

- The Web Security Service integration requires RSA or DSA public keys with a key strength of at least 2048.

- For the signing certificate, Symantec recommends SHA2; SHA1 is supported but not recommended. MD5 is not supported.

- 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.

- The following Knowledge Base article lists what the Web Security Service SAML policy currently bypasses.

  SAML Bypass List KB Article

Configure This?

AD FS

- Proceed to "Import Users and Groups for SAML Auth" on page 51.

The Web Security Service also supports the use of the following applications when configured to be a SAML IdP.

- "Integrate Symantec VIP Access Manager as the SAML IdP" on page 66

- "Integrate Google G Suite as a SAML IdP" on page 87
- "Integrate Microsoft Azure as the SAML IdP" on page 72
- "Integrate Okta as the SAML IdP" on page 94
- "Integrate Ping Identity as the SAML IdP" on page 104
About the Auth Connector as a SAML IdP

The Symantec Web Security Service 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 the Web Security Service as a Service Provider (SP), see "About SAML Integration" on page 33.

**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 (Symantec Web Security Service) 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, the Web Security Service 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

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

Group memberships are identified through a different process, however. The Web Security Service 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 Web Security Service 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 Web Security Service to re-query group membership.

To perform an on-demand retrieval of all user and group names, return to the Authentication > Auth Connector tab 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.

Next Step

- See "Integrate Auth Connector as the SAML IdP" on page 62.
About Challenge-based Auth (Captive Portal)

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 Unified 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 (Firewall/VPN and Explicit Proxy Access 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 Web Security Service 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 the Web Security Service 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 Symantec recommends using Cookie Surrogates. After a user authenticates from an IP address, all further requests from that IP address are treated as 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 the Web Security Service 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 access method neither provides authentication nor sends user and group information to the Web Security Service 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 the Web Security Service.

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

**C—Remote Users (Unified Agent)**

The Symantec Web Security Service provides the Captive Portal as an alternative method to check user credentials rather than the method provided natively by the Unified 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 and 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 the Web Security Service 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 the Web Security Service 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 Symantec Web Security Service 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, the Web Security Service 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). For other diagnostic entries, see "Captive Portal Diagnostic Messages" on page 158.

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 an 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 Access Method and credential refresh times for both the Firewall/VPN and Explicit Proxy Access 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 the Web Security Service is dropped; all other traffic continues normally.

  - If the fault is an Auth Connector problem, the user connects to the Web Security Service as an unauthenticated user.

- If you render an employee disabled, the Web Security Service 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 "Captive Portal Surrogates and Times" on page 130.

- Remote Users—Select Service mode > Mobility > Unified Agent. This page contains the Enable Captive Portal option.
About Roaming Captive Portal

The Symantec Web Security Service Roaming Captive Portal feature allows you to accomplish the following.

- Configure a browser for explicit proxy connections to the service, which then enforces user authentication for web sessions.
- Quickly connect a mobile device on the corporate network and demonstrate cloud service authentication and web protection.

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 Web Security Service 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 Web Security Service data pods locations on the planet.
3—On a laptop connected to the corporate Wi-Fi (B), configure a browser to explicitly proxy to the Web Security Service 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, the Web Security Service 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 the Web Security Service. 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 Web Security Service 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 the Web Security Service. Symantec provides a full Mobile Device Service (MDS) for iOS devices.

Implement This Feature?

This is not a stand-alone product. You must complete the initial configuration process and then configure Roaming Captive Portal from the Service mode > Authentication > Auth Connector page.

Proceed to "Enable Roaming Captive Portal" on page 118.
Prepare Microsoft AD FS for Federation

As part of the Symantec Web Security Service and Security Assertion Markup Language (SAML) authentication integration, you must configure your Identify Provider (IDP) to trust the cloud service. This involves downloading the Web Security Service 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 may require for your deployment, refer to the AD FS documentation.

Tip: Symantec recommends 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 Web Security Service metadata file.

1. In Service Mode, select the Authentication > SAML tab.
2. In the Downloads area on the right-side of the page, click the ThreatPulse Federation Metadata link; save the XML file to location from which you can access with the IDP.

Step 2—Import the Web Security Service 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 Web Security Service 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 47.
Federate the Web Security Service and AD FS

As described in "About SAML Integration" on page 33, 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 Symantec 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.

The first step is import from the Microsoft Active Directory Federation Services (AD FS) entity in your network to the Web Security Service. This topic describes how to export the metadata from the IDP into an XML file that can be read by the service.

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.

<table>
<thead>
<tr>
<th>Metadata</th>
<th></th>
<th>/adfs/services/trust/mex</th>
<th>WS-MEX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>/FederationMetadata/Foo/FederationMetadata.xml</td>
<td>Federation Metadata</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>/adfs/fs/federationserver/service.asmx</td>
<td>ADFS 1.0 Metadata</td>
</tr>
</tbody>
</table>

3. Copy the URL and paste it into a browser address bar.
4. Save the XML document. If another person is to perform the Web Security Service, 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 Web Security Service and assign a signing certificate chain.

1. In Service Mode, select the Authentication > SAML tab.
2. Expand the Configure SAML Authentication area.
3. Import the IDP metadata.
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**. Symantec recommends the **Redirect Endpoint** rather than the **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.

   a. By default, the Web Security Service 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: manually enter the value if the metadata does not contain the attribute or if the metadata is not imported.

   b. By default, the Web Security Service 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 the Web Security Service 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, Symantec recommends using 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.

<table>
<thead>
<tr>
<th>Signing Certificate Chains</th>
</tr>
</thead>
<tbody>
<tr>
<td>At least one valid certificate chain is required</td>
</tr>
</tbody>
</table>

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 Web Security Service portal displays any certificate-related errors, see "Troubleshoot SAML Authentication" on page 155.

6. Click Save.
Step 3—Verify Policy Sync

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

Navigate to Solutions mode > Content Filtering > Policy 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) Access Method—Proceed to "Captive Portal Surrogates and Times" on page 130.
- Remote Users—Select Service mode > Mobility > Unified Agent. This page contains the Enable Captive Portal option.

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 137.

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 155 for possible causes and resolutions.
Import Users and Groups for SAML Auth

The SymantecWeb 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 the Web Security Service. 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. In Service mode, select Authentication > Users and Groups > Imported Users/Groups.
2. Click Add. The service displays the Add dialog.

![Add User Dialog]

a. On the Add Users/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 SymantecAuth 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 Authentication > SAML page). Save the files in a location that you can access from the portal.

2. In Service mode, select Authentication > Users and Groups > Imported Users/Groups.

3. Click Add. The service displays the Add dialog.

- 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 a 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 Web Security Service through an integration token. This allows you to retain and manage users and groups in the vendor IdP interface.

The Third-Party Sync tab on the Authentication > 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 Web Security Service. 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 the Web Security Service. After that initial data download completes, subsequent data updates from Azure require much less time because only the changes are pushed to the Web Security Service.

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 the Web Security Service.

- "Integrate Microsoft Azure as the SAML IdP" on page 72
- "Integrate Okta as the SAML IdP" on page 94

Manage Manually Imported Users and Groups

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

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 are 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.
The References column indicates that a Content Filter policy rule exists that applies to the user or group (Solutions mode > Content Filtering > Policy). 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.

Next Step

- Proceed to: “Prepare Microsoft AD FS for Federation” on page 45.
Install The Auth Connector as the IDP

A deployment option for SymantecWeb Security Service Security Assertion Markup Language (SAML) authentication is to deploy the Auth Connector as an Identity Provider (IDP). This requires specific options in the Auth Connector installation.

Procedure

Pre-requisite: Minimum Auth Connector Version

If you are an existing Web Security Service customer, you might already have the Auth Connector implemented into your network. However, to function as a SAML IDP, the Auth Connector must be running the version provided by Symantec on the December 6th, 2013 update of the Web Security Service (or later). The minimum version ID is 2.5.1600.529106.

Obtain the latest version on the Service mode > Authentication > Auth Connector page.

Step 1—Add an Auth Connector location to the Web Security Service.

1. Select Authentication > Auth Connector
2. Click Add Auth Connector.
3. Connect to the service.

![Add Auth Connector dialog]

   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 Web Security Service 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—Install the Primary Auth Connector on a Domain Controller or Member Server.**

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

1. On the Domain Controller or 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.

![Auth Connector Configuration Wizard](image)

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

5. Link this Auth Connector installation with the Web Security Service by entering the **Auth Connector Unique Name** and **Password** that you obtained/defined during **Step 1**.
6. This task is not part of the SAML IDP procedure.

Select **Yes** and click **Next**.

7. The Auth Connector requires port 80 open on the firewall device.
Select Open port 80... and click Next.

8. The Auth Connector IDP requires a self-signed cert for the federation with the Web Security Service.

- To generate the required self-signed cert, select Yes and click Next. When the installation completes, the Auth Connector generates the saml-cert.cer certificate and places it in C:\Programs and Files (x86)\Blue Coat Systems\BCCA. You will enter this certificate in SAML configuration step.

- If you already have a self-signed cert that you would rather use, select No and click Next.

9. Does your Web Security Service deployment does not involve Firewall/VPN locations?
If Yes, select **We have (or plan to have) a Firewall/VPN Access Method**, click **Next**, and proceed to Step 8.

If No, select **We do not have a Firewall/VPN Access Method**, click **Next** and proceed to Step 9.

10. Firewall/VPN Access Method only—You have a choice for how the Auth Connector resolves and maintains the IP-to-user map.

   ![Diagram](image)

   a. Select an option: Click **Next**.

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

      You must download the application and make it available to each client system. Refer to the Client Application Release Notes for group policy information. To obtain the application and release notes, go to [https://bto.bluecoat.com/documentation/All-Documents/Web Security Service](https://bto.bluecoat.com/documentation/All-Documents/Web Security Service).

      For more information about these two methods, see "About the Auth Connector Integration" on page 16.

   b. Click **Next**.

      - If you did not select the **Logon App** option, proceed to step 11.
      - If you selected the **Logon App** option, you are again prompted with the request to open port 80 on the device firewall. Click **Next**.

11. Click **Install**.

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

**Note:** To achieve redundancy, you must configure any additional Auth Connector servers to share the same hostname and implement a load balancer or DNS round-robin.
Step 3—(Optional) Specify which User and Group names are forwarded to the service.

By default, the Auth Connector sends the following to the Web Security Service.

- 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).

If your LDAP deployment contains a large number of groups and users, consider sending user and group information for only those who require advanced policy checking. If you perform this option, do not open the firewall for outbound 443/tcp from the Auth Connector before you complete this task; if you do, the Auth Connector sends every name and policy gets applied. See "Forward Specific User and Group Names to the Service" on page 146.

If you do not see new users or groups you added, it might not have been 24 hours since the last automatic refresh. See "New Users/Groups Are Not Available for Policy" on page 154.

Step 4—Verify the Connection.

1. Back on the **Network > Authentication** page, review the Auth Connector status icons.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Connection Status Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🟢</td>
<td>The Web Security Service and the installed Auth Connector are communicating.</td>
</tr>
<tr>
<td>🟥</td>
<td>The Web Security Service does not detect the specified Auth Connector.</td>
</tr>
<tr>
<td>🟢</td>
<td>An error related to the authentication process occurred. Verify that the Active Directory is functioning correctly.</td>
</tr>
<tr>
<td>🟢</td>
<td>A previously successful Auth Connector to Web Security Service configuration is currently not connected. Verify all Domain Controller and service configurations.</td>
</tr>
</tbody>
</table>

2. In the Web Security Service 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 as the Web Security Service performs an automatic sync operation once every 24 hours. To perform an immediate, manual sync, click **Synchronize with AD**.

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

- Proceed to "Integrate Auth Connector as the SAML IdP" on page 62.
Integrate Auth Connector as the 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 Symantec Auth Connector as the IdP. This is a simpler configuration that also keeps your Web Security Service deployment compartmentalized.

Technical Requirements

Verify that the following ports are open on the Windows firewall service on the Auth Connector server: 80 and 443.

Procedure

Step 1—Federate the Service and the Auth Connector.

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

1. In Service mode, select Authentication > SAML.
2. Expand the Configure SAML Authentication area.
3. Import the Auth Connector IdP metadata.

4. a. Enter **bcca** as the **Entity ID**.
5. 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. Symantec recommends 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.

![Attribute Formats](image)

a. By default, the Web Security Service 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. Import the self-signed Auth Connector IdP certificate.

![Certificate Chains](image)

a. The Auth Connector installation wizard prompted you to select either to generate a self-signed cert or use an existing one (*Install The Auth Connector as the IDP* on page 55, Step 2.8), the Auth Connector generated the required self-signed cert (**saml-cert.cer**).
   - If you elected to have the Auth Connector generate the certificate, 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 Web Security Service displays any certificate-related errors, see “Troubleshoot SAML Authentication” on page 155.

6. Click **Save**.

**Step 2—Specify locations as SAML-Authenticated**

If you did not enable **Captive Portal** and **SAML** authentication on the **Location** page of the Initial Configuration Wizard process, you must edit the location. 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.

- "Add a Gateway Firewall/VPN Location" on page 148
- "Add an Explicit Proxy Location" on page 150

If you require information about Captive Portal, see "About Challenge-based Auth (Captive Portal)" on page 40.

**Step 3—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).
Integrate Symantec VIP Access Manager as the SAML IdP

If you want to use Security Assertion Markup Language (SAML) authentication, 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 Web Security Service 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.
   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 Web Security Service**

The next phase is to export and add metadata to the Web Security Service 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 Web Security Service portal. Navigate to **Service mode > Authentication > SAML**.

4. Expand the **Configure SAML Authentication** area.
Step 3—Test

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

1. Add a **Network > Location**; name it SAML Test, for example.
   a. Set to **Explicit Proxy**.
   b. **Save** the location.

2. Navigate to **Authentication > Authentication Policy**.
   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 155 for possible causes and resolutions.

**Step 4—Import Users**

You must manually import the user list from the Symantec VIP Access Manager into the Web Security Service.

1. Download the user list in a spreadsheet format.

   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.
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 Web Security Service portal to import the usernames from the text file.

   a. Select **Service > Authentication > Users and Groups**.

   b. Select **Manual Import**.

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

   d. Select **Import Users/Groups**; 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. 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. "**Captive Portal Surrogates and Times**" on page 130.

- "**Import Users and Groups for SAML Auth**" on page 51.
Integrate Microsoft Azure as the SAML IdP

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

The Web Security Service 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 Web Security Service 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 137.

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.
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 Web Security Service

The next phase is to add the Web Security Service as an application, which requires providing SAML Federation information obtained from your Web Security Service 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 Web Security Service portal account (open a new browser tab) and obtain the meta data required to federate the two services.

   a. Select **Service mode** > **Authentication** > **SAML**.

   b. Expand the **Configure SAML Authentication** area.
c. Next to **WSS Metadata**, click **Download** link and download the data.

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.
Integrate Microsoft Azure as the SAML IdP/Page 76

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.

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 the Web Security Service.
1. Add a **Network > Location**; name it SAML Azure Test, for example.
   a. Set to **Explicit Proxy**.
   b. **Save** the location.

2. Navigate to **Authentication > Authentication Policy**.
   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 155 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 Web Security Service group-level policy to be valid, the name of the roles **must** match the name of the groups used in the Web Security Service policies.

To be able to create group-based policies in the Web Security Service, 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 Web Security Service policy. The following examples use the names roleA and roleB to match example Web Security Service 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.

   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 Web Security Service policies and click Select.
   c. Click Select Role.
d. Select which roles are to be susceptible to Web Security Service 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 Web Security Service 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.
d. In the **Name** field, enter *group*.

e. In the **Value** field, enter *userassignedroles*.

f. Click **OK**.


Provision your Azure account to manage users and groups within the Azure portal yet have them automatically sync to the Web Security Service 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 Auth" on page 51 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**...

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

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

   Click **Add** (bottom of screen).
5. Provision the Web Security Service.
   a. Select Provisioning.
   b. From the Provisioning Mode drop-down list, select Automatic.

6. In a new tab, access your Web Security Service portal and navigate to Service mode > Account Maintenance > Integrations.
   a. Click New Integration; in the New Integration dialog, select Third-Party Users & Groups Sync.

   ![New Integration dialog](image)

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

   c. Return to the Azure browser tab, Admin Credentials area.
Integrate Microsoft Azure as the SAML IdP/Page 84

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

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

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

e. Return to the Web Security Service 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](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 Web Security Service portal, navigate to **Service** mode > **Account Maintenance** > **Integrations**. In the **Third-Party Users and Groups** area you can see how many Users and Groups were imported in the most recent sync operation.
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 a 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 a 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 Web Security Service. Subsequent synchronizations require less time.

In the Web Security Service portal, navigate to the **Service mode > Authentication > Users and Groups > Third-Party Sync** tab. 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.

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 137.

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. "Captive Portal Surrogates and Times" on page 130.
- "Import Users and Groups for SAML Auth" on page 51.

Alternate Media

Microsoft created a documentation topic that demonstrates the integration.

Integrate Google G Suite as a SAML IdP

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

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 Web Security Service 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 137.

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.


2. Provide a contact email address. As this is used for all account activity going forward, avoid using a personal account.
3. If 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**


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**.

   ![Enable SSO for SAML Application](image)

   Click the arrow on the right of the SymantecWSS line.

4. The interface displays the **Google IdP** dialog.
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.
Confirm that the page displays the same information as the above image, and click Next.

6. Define the Symantec Web Security Service details:
Symantec Web Security Service/Page 91

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.

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.
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 Web Security Service portal and navigate to **Service > Authentication > SAML**.
2. Expand the **Configure SAML Authentication** area.
Symantec Web Security Service/Page 93

a. Click **SAML IdP Metadata: 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 Web Security Service.

1. Add a **Network > Location**; name it SAML Google Test, for example.
   a. Set to **Explicit Proxy**.
   b. **Save** the location.

2. Navigate to **Authentication > Authentication Policy**.
   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 155 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. "Captive Portal Surrogates and Times" on page 130.

- "Import Users and Groups for SAML Auth" on page 51.
Integrate Okta as the SAML IdP

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

The Web Security Service 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 Web Security Service 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 137.

- 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 Auth" on page 51 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.
Symantec Web Security Service/Page 95

a. Click **Add Application**.

![Add Application](image)

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 the Web Security Service.**

Provision your Okta account to manage users and groups within the Okta portal yet have them automatically sync to the Web Security Service portal (SCIM feature).
1. In Okta, click **Provisioning** on the application menu.

   a. Click **Configure API Integration**.

   b. Select **Enable API Integration**.

2. In a new tab, access your Web Security Service portal and navigate to **Service** mode > **Account Maintenance** > **Integrations**.
a. Click **New Integration**; in the New Integration dialog, select **Third-Party Users & Groups Sync**.

![New Integration dialog](image)

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

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

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

e. Return to the Web Security Service portal tab; copy the **Token**.

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

f. 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.

g. Click **Save**.

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

4. Click **Edit**.
a. Select **Create Users**, **Update User Attributes**, and **Deactivate Users**.

b. Click **Save**.

### Step 3 - Federate the Web Security Service.

1. Save the Okta metadata.
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 Web Security Service.

2. Assign the users and groups to the app.

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

b. From the **Assign** drop-down list, select:
   - **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.

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.


   a. Navigate to **Service mode > Authentication > SAML**.

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

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

   d. Select **Post Endpoint**.
Test Step

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

1. Add a **Network > Location**; name it Okta Test, for example.
   a. Set to **Explicit Proxy**.
   b. **Save** the location.

2. Navigate to **Authentication > Authentication Policy**.
   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 155 for possible causes and resolutions.

Synchronization

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

In the Web Security Service portal, navigate to the **Service mode > Authentication > Users and Groups > Third-Party Sync** tab. This page displays all of the users and groups provided by the IdP.

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 Web Security Service 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. "Captive Portal Surrogates and Times" on page 130.
Integrate Ping Identity as the SAML IdP

If you want to use Security Assertion Markup Language (SAML) authentication, 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 Web Security Service 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 137.

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.
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 Web Security Service**

Enable the two services to communicate.

1. Log in to your Web Security Service portal.

2. Select **Service mode > Authentication > SAML**.
   
a. Select **Service mode > Authentication > SAML**.
   
b. Expand the **Configure SAML Authentication** area.
c. Next to **WSS Metadata**, click **Download** link and download the data.

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

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

I have the SAML 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


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

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


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

a. Click **SAML IdP Metadata: 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 Web Security Service.

1. Add a **Network > Location**; name it Ping Test, for example.

   a. Set to **Explicit Proxy**.
   
   b. Save the location.

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

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 155 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. "Captive Portal Surrogates and Times" on page 130.

- "Import Users and Groups for SAML Auth" on page 51.
Captive Portal Tasks

The following sections provide Captive Portal configuration information.

- "Captive Portal Surrogates and Times" on page 130
- "Enable Roaming Captive Portal" on page 118
- "Configure Browsers to Receive Auth Challenge" on page 121
- "Enable Roaming Captive Portal on Android" on page 127
- "Enable Roaming Captive Portal on iOS" on page 123
Captive Portal Surrogates and Times

For applicable Access Methods you can enable Captive Portal authentication (challenge-based). When this is enabled, users must enter credentials in browsers to access web-based content. See "About Challenge-based Auth (Captive Portal)" on page 40 for more information.

Supported Access Methods

The information in this topic applies only to the Firewall/VPN and Explicit Proxy Access Methods.

About the Authentication Policy

The Symantec Web Security Service provides an authentication policy editor in which you can enable Captive Portal, select the Surrogate type (when possible), and specify the duration of user logged-in sessions for fixed locations. The policy editor enables you to set different surrogate types and refresh times for each location (traffic source).

Firewall/VPN Surrogate Types

For locations that connect to the Web Security Service through the Firewall/VPN Access Method, you can decide which type of authentication surrogate to employ.

- **IP**–The Web Security Service 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.

- **Cookie**–The Web Security Service 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.

**Note:** For the Explicit Proxy Access Method, only the cookie surrogate is available.

Refresh Times

The refresh time determines how long the Web Security Service 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 Web Security Service datacenter, perhaps because of load-balancing, the user is re-prompted for credentials.
Define Authentication Policy

These procedures commence from the stage that you have locations defined in the portal. If you do not require information, see:

- Add a Gateway Firewall/VPN Location (IPsec)
- Add an Explicit Proxy Location

Procedures

Firewall/VPN Access Method

1. In the Web Security Service portal, select Service mode > Authentication > Authentication Policy.
2. Expand the Location Policy area.
3. Click Add Rule. The portal displays the policy editor.
4. Click VPN/Firewall Locations.
5. Click Add Sources.

Select a location option.

- **Locations**—These are the named locations you created on the Network > Add 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](image)

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

7. In the Verdict area, select the toggle to enable Captive Portal.
a. Select the **Authentication Method** that you have configured for the location(s).

If you have not 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 twenty four 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. In the Web Security Service portal, select **Service mode > Authentication > Authentication Policy**.
2. Expand the Location Policy area.

3. Click Add Rule. The portal displays the policy editor.

4. Click Explicit Proxy

5. Click Add Sources.

![Add Sources](image)

Select a location option.

- **Locations**—These are the named locations you created on the Network > Add 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.

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

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

The Symantec 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 Web Security Service portal, which includes specifying corporate e-mail domains.

1. Confirm the following prerequisites.

   - Be advised of the security risks exposed by this feature. See "About Roaming Captive Portal" on page 43.
   - Roaming Captive Portal requires a functioning Auth Connector deployment. See "Deploy the AuthConnector" on page 21.
   - 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.

2. In Service mode, select Authentication > Auth Connector.

3. Enable the features and add e-mail domains and sub-domains that your enterprise uses. For example, m.example.com. Each domain must be globally unique.

   a. Select **Enable Roaming Captive Portal**.

   b. Click **Add Domain**.

   c. In the **Add Domain** dialog, enter a **Domain** or sub-domain and click **Add**.
d. To add more domains, repeat Step c.

4. When you Enable Roaming Captive Portal, the Web Security Service displays the https://portal.threatpulse.com/roaming URL. This is the URL to configure the explicit proxy settings in browsers (mobile devices might require further configuration). Record this URL.

Next Selection

Configure a browser or mobile device to explicitly proxy to the Web Security Service roaming PAC file.
- See "Enable Roaming Captive Portal on iOS" on page 123.
- See "Enable Roaming Captive Portal on Android" on page 127.
Configure Browsers to Receive Auth Challenge

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

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 Web Security Service 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 Web Security Service 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 Web Security Service 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 on iOS

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

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

3. In the HTTP Proxy area, tap Auto. In the URL field, enter https://portal.threatpulse.com/roaming.
4. Test: Open the Safari browser app and browse to a website. The device displays an authentication challenge.
A successful challenge allows access (pending malware scan and policy check).

5. Browse to website that belongs to a category blocked by defined policy. If the page is blocked, the configuration was successful.
Enable Roaming Captive Portal on Android

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

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.
4. Set the Proxy hostname and port.
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.
Captive Portal Surrogates and Times

For applicable Access Methods you can enable Captive Portal authentication (challenge-based). When this is enabled, users must enter credentials in browsers to access web-based content. See “About Challenge-based Auth (Captive Portal)” on page 40 for more information.

Supported Access Methods

The information in this topic applies only to the Firewall/VPN and Explicit Proxy Access Methods.

About the Authentication Policy

The Symantec Web Security Service provides an authentication policy editor in which you can enable Captive Portal, select the Surrogate type (when possible), and specify the duration of user logged-in sessions for fixed locations. The policy editor enables you to set different surrogate types and refresh times for each location (traffic source).

Firewall/VPN Surrogate Types

For locations that connect to the Web Security Service through the Firewall/VPN Access Method, you can decide which type of authentication surrogate to employ.

- **IP**—The Web Security Service 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.

- **Cookie**—The Web Security Service 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.

  **Note:** For the Explicit Proxy Access Method, only the cookie surrogate is available.

Refresh Times

The refresh time determines how long the Web Security Service 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 Web Security Service datacenter, perhaps because of load-balancing, the user is re-prompted for credentials.
Define Authentication Policy

These procedures commence from the stage that you have locations defined in the portal. If you do no and not require information, see:

- Add a Gateway Firewall/VPN Location (IPsec)
- Add an Explicit Proxy Location

Procedures

Firewall/VPN Access Method

1. In the Web Security Service portal, select Service mode > Authentication > Authentication Policy.
2. Expand the Location Policy area.
3. Click Add Rule. The portal displays the policy editor.
4. Click VPN/Firewall Locations.
5. Click Add Sources.

Select a location option.

- Locations—These are the named locations you created on the Network > Add 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.

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

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

**Explicit Proxy Access Method**

1. In the Web Security Service portal, select **Service mode** > **Authentication** > **Authentication Policy**.
2. Expand the **Location 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 **Network > Add 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.

---

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

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

- 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.

<table>
<thead>
<tr>
<th>Exemptable Sources</th>
<th>Exemptable Destinations</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP addresses/Subnets</td>
<td>Domains/URLs</td>
</tr>
<tr>
<td>Locations</td>
<td>IP addresses/Subnets</td>
</tr>
<tr>
<td>Unified Agents</td>
<td>Web Applications</td>
</tr>
<tr>
<td>Mobile Devices</td>
<td>Categories</td>
</tr>
</tbody>
</table>

**Tip:** Symantec maintains a list of exempted sources and destinations, which are included in policies on assets in the datacenters.

**KB Article**

About Clients That Are Not Forms-Based

The Web Security Service has an option to exempt Unified Agent and mobile clients. Currently there is no use case to do this as these clients do not rely on redirection or forms-based authentication.

- Unified Agent—The credentials are supplied at system logon. If Captive Portal is enabled, Unified Agent still 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 Web Security Service versions.

**Procedure**

1. In the Web Security Service portal, select **Service mode > Authentication > Authenticati 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 Web Security Service account.

■ Unified 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.
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.
Admin Tasks and Reference

The following tasks are for Web Security Service administrators.

- "Reference: Required Locations, Ports, and Protocols" on page 141
- "Reference: Authentication IP Addresses" on page 145
- "Forward Specific User and Group Names to the Service" on page 146
- "Reference: Authentication IP Addresses" on page 145
- "Add a Gateway Firewall/VPN Location" on page 148
- "Add an Explicit Proxy Location" on page 150
Reference: Required Locations, Ports, and Protocols

Depending on your configured Symantec Web Security Service Access Methods, some ports, protocols, and locations must be opened on your firewalls to allow connectivity to the various cloud service components and data centers.

Symantec Resource

support.symantec.com Support site links to support tools and documentation.

Access Methods

<table>
<thead>
<tr>
<th>Access Method</th>
<th>Port(s)</th>
<th>Protocol</th>
<th>Resolves To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Security Service IP</td>
<td>80/443</td>
<td>IPsec/ESP</td>
<td>portal.threatpulse.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>199.19.250.192</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>199.116.168.192</td>
</tr>
<tr>
<td>Firewall/VPN (IPsec)</td>
<td>80/443</td>
<td>IPsec/ESP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>500</td>
<td>UDP (ISAKMP)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4500</td>
<td>UDP4500</td>
<td>IPsec/ESP if firewall is behind a NAT.</td>
</tr>
<tr>
<td>Proxy Forwarding</td>
<td>8080/8443</td>
<td>HTTP/HTTPS</td>
<td>Port 8080 to proxy.threatpulse.net</td>
</tr>
<tr>
<td></td>
<td>8084*</td>
<td></td>
<td>Port 8443 to proxy.threatpulse.net</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>*Port 8084 to proxy.threatpulse.net</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>*If this forwarding host is configured for local</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SSL interception.</td>
</tr>
<tr>
<td>Access Method</td>
<td>Port(s)</td>
<td>Protocol</td>
<td>Resolves To</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Explicit Proxy</td>
<td>PFMS: 443</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Firewall rules:**

- If your firewall allows white-listing by DNS, white-list `pfms.wss.symantec.com`; this is the preferred method.

- If your firewall does *not* allow white-listing by DNS:

  **Before April 5, 2019**—You must resolve the following two DNS addresses to obtain the IP addresses to allow.

    - **Primary:**
      
      `awseb-e-u-AWSEBLoa-PE6PFFKMNUY-297683686.us-west-2.elb.amazonaws.com`

    - **Backup:**
      
      `awseb-e-q-AWSEBLoa-WV7JEO9Y1011-1416580986.us-east-1.elb.amazonaws.com`

  Following April 5, you do not need to perform this task.

  **After April 5, 2019**—Allow the following static IP addresses.

    - `35.155.165.94`
    - `35.162.233.131`
    - `52.21.20.251`
    - `52.54.167.220`
    - `199.247.42.187`
    - `199.19.250.187`
## Access Method

<table>
<thead>
<tr>
<th>Access Method</th>
<th>Port(s)</th>
<th>Protocol</th>
<th>Resolves To</th>
</tr>
</thead>
</table>
| Explicit Over IPsec (Trans-Proxy)  | No Default Route: 80, 443 | UDP (v4.9.1+), TCP, SSL | ep.threatpulse.net resolves to 199.19.250.205  
ep-all.threatpulse.net returns the following.  
199.19.248.205  
199.19.250.205  
199.19.250.206  
199.19.250.207  
199.19.250.208  
199.19.250.209  
199.19.250.210  
199.19.250.211  
199.19.250.212  
199.19.250.213  
199.19.250.214  
ep-roundrobin.threatpulse.net returns all IPs in a round-robin fashion; each two-minute Time-To-Live (TTL) period returns a different address. |
| Unified Agent                      | 80, 443   | UDP (v4.9.1+), TCP, SSL | Port 80/443 to portal.threatpulse.com (199.19.250.192) (for captive network information and updates)  
Port 443 to ctc.threatpulse.com  
Port 443 to client.threatpulse.net (DNS fallback) |
| MDM (registered iOS and Android devices) | UDP 500 (ISAKMP) | IPSec/ESP | 199.19.250.195  
199.116.168.195  
If connectivity to the Web Security Service is behind stringent firewall rules, adjust the rules to allow traffic to pass to these IP addresses on port 443. |
| Hybrid Policy | UDP 4500 (NAT-T) | | |
## Authentication

<table>
<thead>
<tr>
<th>Auth Method</th>
<th>Port(s)</th>
<th>Protocol</th>
<th>Resolves To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth Connector</td>
<td>443</td>
<td>SSL</td>
<td>to auth.threatpulse.com:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>199.19.250.193</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>199.116.168.193</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>portal.threatpulse.com:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>199.19.250.192</td>
</tr>
<tr>
<td>Auth Connector to Active</td>
<td>139,445</td>
<td>TCP</td>
<td>Directory</td>
</tr>
<tr>
<td></td>
<td>389</td>
<td>LDAP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3268</td>
<td>ADSI LDAP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>135</td>
<td>Location Services</td>
<td></td>
</tr>
<tr>
<td></td>
<td>88</td>
<td>Kerberos</td>
<td></td>
</tr>
<tr>
<td></td>
<td>49152-65535</td>
<td>TCP</td>
<td>If installed on a new Windows Server 2012 Member rather than a Domain Controller.</td>
</tr>
<tr>
<td>AC-Logon App</td>
<td>80</td>
<td></td>
<td>Port 80 from all clients to the server.</td>
</tr>
<tr>
<td>SAML</td>
<td>8443 (over VPN)</td>
<td>Explicit and IPSec</td>
<td>to saml.threatpulse.net</td>
</tr>
<tr>
<td>Roaming Captive Portal</td>
<td>8080</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Cloud-to-Premises DLP

For connection coordination and management status.

- Port 443 (traffic from client device)
- XMPP port 5222 to comm.threatpulse.com
Reference: Authentication IP Addresses

The Symantec Web Security Service Auth Connector communicates with devices in the geographically located data centers. The following are the list of authentication IP addresses by location.

The Symantec Operations team maintains the following Knowledge Base article.

Forward Specific User and Group Names to the Service

By default, the Auth Connector returns all group and usernames that are contained in your LDAP deployment to the Symantec Web Security Service 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. Sending that much information might cause Auth Connector resource constraints.

For large LDAP deployments, consider selecting which groups/users require Advanced Policy and forward only those names to the Web Security Service. For example, you have domains named HQ-QA, HQ-SALES, and HQ-OPERATIONS and only users in the HQ-SALES domain require Advanced Policy checks.

The bcca.ini file, which is part of the Auth Connector application, contains [Groups] and [Users] sections. You can add entries to one, either, or both:

- If the [Groups] and [Users] sections are empty, the Web Security Service 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 task.

**Procedure**

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

Each supported router/firewall device that is configured to send web traffic (VPN to VPN) to the Symantec Web Security Service requires an equivalent location configured in the service portal interface.

1. In Service Mode, select **Network > Locations**.

2. Click **Add Location**.

3. In the Add Location dialog, enter the **Location** and security information.

   a. The **Name** of the location. For example, the geo-physical location or office name.

   b. Select **Firewall/VPN** as the **Access Method**.

   c. Enter the **Gateway IP** address of the router interface used to communicate to the Web.

   d. Enter the **Authentication Key** (pre-shared key) used to authenticate communication from the router.

4. Enter resource and location information.
a. Select the **Estimated User** range that will be sending web requests through this gateway interface. Symantec uses this information to ensure proper resources.

b. Select a **Country** and **Time Zone**.

c. Fill out location information and enter comments (optional).

5. Click **Save**.

- The Firewall/VPN Access Method supports Captive Portal.
  - See "About Challenge-based Auth (Captive Portal)" on page 40.
  - See "Captive Portal Surrogates and Times" on page 130.
Add an Explicit Proxy Location

When configuring Explicit Proxy as the access method, each gateway IP address defined in a PAC file requires an equivalent Symantec Web Security Service location configuration.

1. In Service Mode, select Network > Locations.
2. Click Add Location.
3. Complete the Location dialog.

   ![Add Location Dialog]

   a. **Name** the location. For example, use the fixed geographical location or organization name.
   
   b. Select **Explicit Proxy** as the Access Method.
   
   c. Enter the **IP/Subnet** that forwards web traffic to the Web Security Service.

4. Enter resource and location information.
a. Select the **Estimated User** range that will be sending web requests through this gateway interface. Symantec uses this information to ensure proper resources.

b. Select a **Country** and **Time Zone**.

c. Fill out location information and enter comments (optional).

5. Click **Save**.

- The Firewall/VPN Access Method supports Captive Portal.
Add a Proxy Forwarding Location

Each forwarding host that is configured to send web traffic to the Symantec Web Security Service requires an equivalent location configuration. The service supports forwarded traffic from SymantecProxySG appliances and Microsoft Internet Security and Acceleration (ISA) 2006 or Microsoft Forefront Threat Management Gateway (TMG) proxy servers.

1. In Service Mode, select Network > Locations.
2. Click Add Location.
3. Complete the Location dialog.

Add Location

<table>
<thead>
<tr>
<th>Location Name:</th>
<th>EventStaff</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Method:</td>
<td>Proxy Forwarding</td>
</tr>
</tbody>
</table>

Proxy Forwarding

We've noticed that your IP address is the location you wish to add. Click here.

IP Address: 192.168.100.5

---

a. **Name** the location. For example, a location designation or employee group identification name.

b. Select **Proxy Forwarding** as the **Access Method**.

c. Enter the gateway IP/Subnet that you defined in the ProxySG forwarding host configuration dialog or ISA/TWG policy.

4. Enter resource and location information.
a. Select the Estimated User range that will be sending web requests through this gateway interface. Symantec uses this information to ensure proper resources.

b. Select a Country and Time Zone.

c. Fill out location information and enter comments (optional).

5. Click Save.

Next Step

- Verify Service Connectivity to Locations.
Troubleshoot...

Attempt to solve Auth Connector and SAML problems.

Auth Connector

- "I Entered the Incorrect AuthConnector Password" on the next page
- "I Cannot Remove the Auth Connector from Windows Server 8 (Pro)" on the next page
- "New Users/Groups Are Not Available for Policy" below

SAML

- "Troubleshoot SAML Authentication" on the next page

New Users/Groups Are Not Available for Policy

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

Group memberships are identified through a different process, however. The Web Security Service 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 Web Security Service 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 Web Security Service to re-query group membership.

To perform an on-demand retrieval of all user and group names, return to the Authentication > Auth Connector tab 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.

1. In Service Mode, select Authentication > AuthConnector.
2. Select a (connected) location.
3. Click Refresh.

![Auth Connectors Table]

- SJSHQPrimary [Edit]
- SJSHQBackup [Edit]
I Entered the Incorrect AuthConnector Password

If you entered the incorrect Symantec Web Security Service Auth Connector application password during the portal initial configuration task, perform the following steps to change it.

In Windows:

1. Select **Start > Control Panel > Add or Remove Programs**.
2. Select **Blue Coat ThreatPulse Auth Connector** and click **Change**. The system displays the Auth Connector configuration wizard.
3. Click **Next**.
4. Click **Modify**.
5. With the Auth Connector item selected, click **Next**.
6. Enter the correct password; click **Next**.
7. Click **Install**.

For additional debugging information, see [https://support.symantec.com/en_US/article.TECH242720.html](https://support.symantec.com/en_US/article.TECH242720.html).

I Cannot Remove the Auth Connector from Windows Server 8 (Pro)

If you are attempting to uninstall the Symantec Web Security Service Auth Connector and you receive an error, the error is likely the result of the DHCP Client Service locking the Auth Connector file (BCCA.EXE).

Go into services and stop the DHCP client service. This allows you to finish uninstalling the service.

For additional debugging information, see [https://support.symantec.com/en_US/article.TECH242720.html](https://support.symantec.com/en_US/article.TECH242720.html).

Troubleshoot SAML Authentication

Certificate Warnings

Sixty days before a certificate in the signing chain expires, the Symantec 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

- **Unsupported Algorithm**—Symantec supports and recommends SHA2 for the Web Security Service 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**—If Web Security Service 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.

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.


Other Errors

<table>
<thead>
<tr>
<th>SAML Error Description/Symptom</th>
<th>Possible Cause</th>
</tr>
</thead>
</table>
| 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. |
### SAML Error Description/Symptom

<table>
<thead>
<tr>
<th>Description</th>
<th>Possible Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Various run-time errors.</td>
<td>The IDP does not recognize the Web Security Service entity ID because the federation is broken (or was never created) at the IDP.</td>
</tr>
<tr>
<td>The IDP fails to authenticate a known valid user.</td>
<td>User does not exist or entered wrong password multiple times.</td>
</tr>
</tbody>
</table>

### SAML Bypass List

The following Knowledge Base article lists what the Web Security Service SAML policy currently bypasses.

[SAML Bypass List KB Article](#)
## Captive Portal Diagnostic Messages

When Captive Portal is enabled for remote clients on the Symantec Web Security Service, various messages are logged in association with user login activities and authentication. They display on the **Service mode > Troubleshooting > Mobile Clients** page.

<table>
<thead>
<tr>
<th>Log Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAResp&lt;0&gt; Captive Portal enabled: true</td>
<td>Indicates when Captive Portal was enabled (<strong>Service mode &gt; Network &gt; Mobility</strong>).</td>
</tr>
<tr>
<td>Captive portal authentication succeeded for <strong>username</strong></td>
<td>Indicates when a user successfully logged in.</td>
</tr>
<tr>
<td>Authentication server error, connecting as unauthenticated user</td>
<td>If the Auth Connector becomes unavailable, the user receives the following error message: <strong>Authentication server error, connecting as unauthenticated user</strong> (also, Web Security Service 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 (<strong>user_name</strong>).</td>
</tr>
<tr>
<td>Account restricted - CP auth failed for user: <strong>username</strong></td>
<td>A user attempted to login in with incorrect credentials more times than the set limit in the Active Directory.</td>
</tr>
</tbody>
</table>