AT&T Cloud Web Security Service: Authentication Deployment Guide

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

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

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

- One main option is the integration of the AT&T 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 User Authentication" on page 10
- "About the Auth Connector Integration" on page 20
- "About SAML Authentication" on page 37
- "About Captive Portal Authentication" on page 103
- "About Roaming Captive Portal" on page 107
- Admin Tasks and Reference
- Troubleshoot…

Full Cloud Web Security Service Help

http://portal.threatpulse.com/docs/sol/SOLDash.htm
# Table Of Contents

AT&T Cloud Web Security Service: Authentication Deployment Guide ............................................. 5

Table Of Contents ............................................................................................................................. 6

## About User Authentication ............................................................................................................ 10

Authenication Method Summaries ................................................................................................. 10

Authentication Methods by Connectivity ......................................................................................... 11

Supported Authentication Methods ................................................................................................. 12

Deployment Notes ............................................................................................................................ 12

Supported Authentication Methods ................................................................................................. 13

Deployment Notes ............................................................................................................................ 13

Supported Authentication Methods—Fixed Location ................................................................. 14

Deployment Notes ............................................................................................................................ 14

Supported Authentication Methods—Unknown Location .......................................................... 15

Deployment Notes ............................................................................................................................ 15

Supported Authentication Methods—Fixed Location ................................................................. 16

Deployment Notes ............................................................................................................................ 16

Supported Authentication Methods—Unknown Location .......................................................... 17

Deployment Notes ............................................................................................................................ 17

Mobile Devices ................................................................................................................................ 18

Cloud Connect Defense .................................................................................................................... 18

ChromeOS ....................................................................................................................................... 18

Deployment Notes ............................................................................................................................ 18

Learn More About Authentication Methods ................................................................................... 19

## About the Auth Connector Integration ......................................................................................... 20

Deploy the Auth Connector ............................................................................................................... 24

Technical Requirements ................................................................................................................... 24

Member Servers Installation Prerequisites ..................................................................................... 24

About Failover .................................................................................................................................. 25

About Proxy Aware Capability .......................................................................................................... 25

Procedure ......................................................................................................................................... 25

Example Configuration: .................................................................................................................... 34

## About SAML Authentication .......................................................................................................... 37

SAML Review—Federation ................................................................................................................. 37

Identity Provider Technical Requirements ....................................................................................... 37

Tested Identity Providers ................................................................................................................... 38

Flow Overview ................................................................................................................................... 39

SAML Flow ....................................................................................................................................... 39

Support for Multiple AD Forests ....................................................................................................... 40
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import Users and Groups for SAML</td>
<td>41</td>
</tr>
<tr>
<td>Procedure</td>
<td>41</td>
</tr>
<tr>
<td>Prepare Microsoft AD FS for Federation</td>
<td>45</td>
</tr>
<tr>
<td>Procedure</td>
<td>45</td>
</tr>
<tr>
<td>Federate the Web Security Service and AD FS</td>
<td>47</td>
</tr>
<tr>
<td>Technical Requirements</td>
<td>47</td>
</tr>
<tr>
<td>Optional—Exempt Sources/Destinations from Authorization</td>
<td>50</td>
</tr>
<tr>
<td>About the Auth Connector as a SAML IdP</td>
<td>51</td>
</tr>
<tr>
<td>Use Cases for Auth Connector as SAML IdP</td>
<td>51</td>
</tr>
<tr>
<td>Current Limitation</td>
<td>51</td>
</tr>
<tr>
<td>Data Flow</td>
<td>52</td>
</tr>
<tr>
<td>About User/Group Memberships</td>
<td>52</td>
</tr>
<tr>
<td>Deploy Auth Connector as SAML IdP</td>
<td>54</td>
</tr>
<tr>
<td>Technical Requirements</td>
<td>54</td>
</tr>
<tr>
<td>Procedure</td>
<td>54</td>
</tr>
<tr>
<td>Integrate Microsoft Azure as the SAML IdP</td>
<td>58</td>
</tr>
<tr>
<td>Technical Requirements</td>
<td>58</td>
</tr>
<tr>
<td>Synchronization</td>
<td>71</td>
</tr>
<tr>
<td>Policy</td>
<td>71</td>
</tr>
<tr>
<td>(Optional) Rebrand Login Page</td>
<td>72</td>
</tr>
<tr>
<td>Exemptions</td>
<td>72</td>
</tr>
<tr>
<td>Alternate Media</td>
<td>72</td>
</tr>
<tr>
<td>Integrate Okta as the SAML IdP</td>
<td>73</td>
</tr>
<tr>
<td>Technical Requirements</td>
<td>73</td>
</tr>
<tr>
<td>Procedure</td>
<td>73</td>
</tr>
<tr>
<td>Known Issue</td>
<td>81</td>
</tr>
<tr>
<td>Integrate Google G Suite as a SAML IdP</td>
<td>83</td>
</tr>
<tr>
<td>Technical Requirements</td>
<td>83</td>
</tr>
<tr>
<td>Procedure</td>
<td>83</td>
</tr>
<tr>
<td>Integrate Ping Identity as the SAML IdP</td>
<td>90</td>
</tr>
<tr>
<td>Technical Requirements</td>
<td>90</td>
</tr>
<tr>
<td>Procedure</td>
<td>90</td>
</tr>
<tr>
<td>Integrate Symantec VIP Access Manager as the SAML IdP</td>
<td>96</td>
</tr>
</tbody>
</table>
Exempt From Authentication ................................................................. 130
  About Clients That Are Not Forms-Based ........................................ 130
  Procedure ....................................................................................... 130

Reference: Authentication IP Addresses ............................................ 133

Troubleshoot SAML Authentication .................................................... 134
  Certificate Warnings ....................................................................... 134
  Certificate Errors .......................................................................... 134
  Clear Associated Auth Surrogates and Restart Authentication .......... 134
  Internet Explorer Sessions .............................................................. 135
  Other Errors .................................................................................. 135
  SAML Bypass List .......................................................................... 135
About User Authentication

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

Authentication Method Summaries

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

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

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

C—SAML with AD FS—The Cloud Web Security Service provides native support with Microsoft® Active Directory Federation Services (AD FS) 2.0.

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

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


Depending on the how many Cloud Web Security Service connectivity methods your enterprise employs, you might require multiple methods.
Authentication Methods by Connectivity

The methods used to route employee web traffic to the Cloud Web Security Service dictates which authentication methods are available.
Firewall/VPN/IPsec

Supported Authentication Methods

- Auth Connector and DCQ
- Auth Connector and ACLogon
  
  The Cloud Web Security Service returns web-form challenge and credentials pass through the Auth Connector for validation.
- SAML (IP or Surrogate Cookie)
  
  The Cloud Web Security Service redirects to the SAML IdP for authentication; the returned assertion provides group-membership.
- Captive Portal (forms-based)

Deployment Notes

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

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

Is the original client source IP available?

- Yes.
Proxy Forwarding

Authentication is managed from the premises proxy, which communicates user and group affiliations in HTTP headers to the Cloud Web Security Service.

Supported Authentication Methods

- Auth Connector and DCQ
- Auth Connector and ACLogon

Deployment Notes

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

Is the original client source IP available?

- Yes (XFF).
Explicit Proxy

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

Supported Authentication Methods—Fixed Location

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

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

The Cloud Web Security Service returns web-form challenge and credentials pass through the Auth Connector for validation.

- SAML (Cookie Surrogate)

The Cloud Web Security Service redirects to the SAML IdP for authentication; the returned assertion provides group-membership.

Supported Authentication Methods—Unknown Location

You can distribute PAC files to clients; the PAC file forces the browser to send traffic to the Cloud Web Security Service.

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

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

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

- See SEP section for more information.

Is the original client source IP available?

- No.
As with Explicit Proxy, clients with Symantec Endpoint Protection (SEP) installed are routed to the Cloud Web Security Service through a PAC file configuration.

**Supported Authentication Methods—Fixed Location**

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

**Supported Authentication Methods—Unknown Location**

- Auth Connector and DCQ
- Auth Connector and ALogon
- SEP with Seamless Identification (recommended)
- SEP with Seamless Identification and Roaming SAML (recommended)
- Captive Portal

**Deployment Notes**

- The SEP solution has various authentication considerations.
- Identification: SEP returns the logged-in username. If the SEP agent is configured to use the Cloud Web Security Service integration token, the agent adds a new header (X-WSS-CLIENT-INFO) to the HTTP Connect requests. The new header has the token that points the Cloud Web Security Service to your tenant.

- AD and SAML: If identification fails, the Cloud Web Security Service authenticates the user per authentication policy and it returns a unique super cookie value per user. SEP uses the new cookie value in a all HTTP Connect requests (X-Bluecoat-Authorization).

**Is the original client source IP available?**

- No.
WSS Agent

Supported Authentication Methods

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

Deployment Notes

- The WSS Agent sends cached user credentials (login) and the Cloud Web Security Service user identification to the service. The access credential pop-up originates from the service. To have true challenge-based auth, enable the Captive Portal option.

- The Auth Connector is required if you plan to create custom policy based on your AD group names.

- When a client that has WSS Agent installed connects to corporate network, the agent goes into passive mode and the authentication occurs per the method configured on-premises.

Is the original client source IP available?

- No.
Mobile/Apps

The Cloud Web Security Service supports connections from various mobile and app-based solutions.

Mobile Devices

SEP-Mobile (iOS) and Android (app store)
- Auth Connector and DCQ
- Auth Connector and ACLogon
- Roaming Captive Portal

Cloud Connect Defense

An app for Windows 10 endpoints.
- Auth Connector and DCQ
- Auth Connector and ACLogon

ChromeOS

Protect Chromebooks and any client running ChromeOS
- Auth Connector and DCQ
- Auth Connector and ACLogon
- Roaming Captive Portal

Deployment Notes

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

Is the original client source IP available?

- No.

Learn More About Authentication Methods

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

- "About the Auth Connector Integration" on page 20
- "About SAML Authentication" on page 37
- "About Captive Portal Authentication" on page 103
- "About Roaming Captive Portal" on page 107
About the Auth Connector Integration

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

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

This section describes the Auth Connector agent network footprint.

When Is The Auth Connector Required?

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

The Auth Connector is not required for the following methods.

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

With What Does the Auth Connector Communicate?

The Auth Connector comprises three communication footprints when completing a Cloud 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 Cloud 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)

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

If you are employing the Firewall/VPN connectivity method, there are two methods that create and maintain the IP-to-User map; select the method from the Auth Connector setup wizard:
Domain Controller Query—This is the default method for all connectivity methods. The Domain Controller Query (DCQ) instructs the Auth Connector to query all the domain controllers in your AD to identify users by their IP address when they log on. Each domain controller is contacted every 10 seconds to ensure detection of all logged on users. The Auth Connector contacts the Cloud Web Security Service Control Pod through auth.threatpulse.net on port 443 and transfers the AD users and group names.

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

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

B—Portal Connection

The Auth Connector contacts the Cloud 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.

D—User Connections

User web requests connect to the Data Pod. The Cloud 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 WSS Agent, the following occurs.

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

Failure to allow the Auth Connector to connect to the Data Pod’s auth IP prevents proper group membership identification, which causes group-based policies to fail. See "Reference: Authentication IP Addresses” on page 133.

About User/Group Memberships

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

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

However, group memberships are identified through a different process. The Cloud 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 Cloud 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 Cloud 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.

**Auth Connector Ciphers**

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

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

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

AT&T recommends keeping the Windows Server up-to-date with the latest patches and updates on the systems running the Auth Connector.

**About the ACLogon App**

AT&T 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. This is described in the Deployment topic.
Deploy the Auth Connector

To create custom policy based on user and group names before those groups generate traffic, you must download the Auth Connector to at least one member server. The Auth Connector connects to the Web Security Service and provides the user/group information from the Active Directory (AD). See “About the Auth Connector Integration” on page 20, which provides more detail about the Auth Connector agent footprint.

Technical Requirements

- Direct Internet Requirement—The Auth Connector must have a direct connection to the internet. Do not allow the Auth Connector to connect through the same IPsec tunnel that goes to the Cloud Web Security Service.
- For a list of required ports, see https://knowledge.broadcom.com/external/article?legacyId=tech245943.
- The Auth Connector communicates with devices in the geographically located data centers. The Symantec Operations team maintains the following Knowledge Base article.
  
  ![Knowledge Base Article](https://knowledge.broadcom.com/external/article?legacyId=TECH240889)

Member Servers Installation Prerequisites

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

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

- On the member server, verify that the Authenticated Users read access is appropriate. This is specific to Windows 2019 but is also applicable to the earlier versions where admins applied deeper security; the Auth Connector
The installation prompts for a username and password. These are configured as the account under which Auth Connector runs. The user name must be in the form ADDOMAIN\user or user@dns_domainname.com, where ADDOMAIN is the NetBios name of the active directory to which the server the Auth Connector is installed on as a member. The installation grants this user account the Log on as a service privilege.

If the AD account password changes and the Auth Connector restarts, the Cloud 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 member server on which the Auth Connector runs. Verify this by browsing the Trusted Root Certification Authorities certificate list within the local machine store with mmc.exe and the certificates snap-in. If this Entrust certificated is not present in the list, you can update the CA certificates by downloading an update program from Microsoft at the following location: http://support.microsoft.com/kb/931125.

About Failover

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

About Proxy Aware Capability

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

Procedure

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

By default, the Auth Connector returns all group and usernames that are contained in your LDAP deployment to the Cloud 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.

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

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

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

- If the [Groups] and [Users] sections are empty, the Cloud 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 procedure.

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

1. In Service mode, select Authentication > Auth Connector.
2. Click Add Auth Connector.
3. Connect to the service.
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 Cloud 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 backup Auth Connector location that will receive data from a second, live domain controller. Repeat **Step 1**.

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

![Auth Connector](image)

**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, expand the **Download Installer** area.

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

2. Click **Download**.

3. If this is the first time you are attempting to download the application, the service displays the Profile dialog.
As a vendor that provides security services across the globe, AT&T supports and complies with United States and local export controls. As an authorized member of your enterprise/organization, you must complete this form before downloading the Auth Connector.

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

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

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

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

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

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

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

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

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

3. Locate the [Groups] and [Users] sections and add entries. You must use the same letter cases that match what is in the Active Directory. Add one entry per line. For example:

   ```
   [Groups]
   
   HQ-SALES\NAWest
   
   HQ-SALES\NANorthWest
   
   [Users]
   
   HQ-SALES\Administrator
   ```

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

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

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

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

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

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

1. On the member server, navigate to where you downloaded the Auth Connector application and run the `AuthConnectorInstaller-#####.exe` file as Administrator.

2. Accept the standard program allowance and click **Next** on the first Wizard page.

3. The Select Installation folder page prompts the installation directory choice. Click next to accept the default (`C:\Program Files\Blue Coat Systems\BCCA`) or select another directory.

4. Click **Next** to begin the Auth Connector configuration wizard.

Enter the Active Directory account access credentials and click **Next**.
5. Link this Auth Connector installation with the Cloud Web Security Service by entering the **Auth Connector Unique Name** and **Password** that you obtained/defined during Step 1.

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

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

Click **Next**.

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

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

7. Does your Cloud Web Security Service deployment involve Firewall/VPN locations?
If Yes, select **We have (or plan to have) a Firewall/VPN Access Method**, click **Next**, and proceed to **Step 7**.

If No, select **We do not have a Firewall/VPN Access Method**, click **Next** and proceed to **Step 8**.

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

   a. Select an option.

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

  b. Click **Next**.

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

9. Click **Install**.

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

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

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

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

An alternative to the direct connection to the Cloud 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 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.

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

3. Add your settings as required.

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

   ```ini
   [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.

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

4. Save the file.

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

**Step 8—For Windows Server 2019 and DCQ Method Only**

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

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

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

**Option 1**

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

**Option 2**

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

**Tip:** AT&T advises that only experienced network administrators perform this option.

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

1. Obtain the script from the same step in the Cloud Web Security Service Help System.


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

   HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\DefaultSecurity\SrvsvcSessionInfo
3. You must run script as an administrator with elevated privileges. The elevated privileges are required to write the updated `security descriptor` to the registry.

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

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

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

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

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

Obtain the app from the same step in the Cloud Web Security Service Help 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 `/logoff` 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.

   ```
   C:\ACLogon\ACLogon.exe /logoff /interval seconds 3600 Auth-Connector_hostname/IP
   ```

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

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

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

The Cloud Web Security Service responds reasonably quickly to new AD integrations. After that, the Cloud 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 Cloud 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 Cloud 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 Cloud 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.

**Step 11—Verify the Connection/Icon Descriptions.**

As traffic begins to flow through the Cloud Web Security Service, you can monitor the Auth Connector connections.

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

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

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

Back on the 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>![checkmark]</td>
<td>The Cloud Web Security Service and the installed Auth Connector are communicating successfully.</td>
</tr>
<tr>
<td>![exclamation-mark]</td>
<td>The Cloud Web Security Service and the installed Auth Connector are communicating, but some connections (data path) are failing. Click the <strong>details</strong> link for more information. The Cloud Web Security Service displays a dialog that contains IP address attempts and common troubleshooting tips.</td>
</tr>
<tr>
<td>![exclamation-mark]</td>
<td>The Cloud Web Security Service has not yet detected this Auth Connector.</td>
</tr>
</tbody>
</table>
| ![error] | Error  
—There is an credential error. Verify that the Auth Connector credentials in the Cloud Web Security Service match the credentials used on the server.  
—This Auth Connector is disconnected. Disconnected since: *date time*. Verify Cloud Web Security Service and Domain Controller configurations. |

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

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

**Next Steps**

- "Review Imported Users and Groups" on page 121
- "Exempt From Authentication" on page 130
- "Authentication Location Policy" on page 123
About SAML Authentication

The AT&T Cloud 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

AT&T assumes that you are familiar with SAML authentication. This document provides SAML information as it relates to the Cloud 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.

Two entities comprise SAML authentication.

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

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

The Cloud 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.

Identity Provider Technical Requirements

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

- The Cloud Web Security Service supports adding multiple signing certificates from the same IdP. This is required to handle the use case where an IdP’s current signing certificate is about to expire and a new signing certificate will take over.

- Consider the following best practices.

  - To avoid looping, add an authentication bypass entry for domain of the IdP server. See "Exempt From Authentication" on page 130.

  - A redirect to the SAML IdP server from within a CORS-enabled application causes failure. You can verify this by using developer tools on the console. AT&T recommends whenever possible use the IP Surrogate method. If Cookie Surrogate is the only option, set longer timeout durations.

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

  - The Cloud 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 AT&T Technical Support.

  - With SAML integrated, the Cloud Web Security Service cannot authenticate explicit HTTPS requests without SSL Intercept enabled.

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

  ![SAML Bypass List KB Article](#)

**Tested Identity Providers**

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

- Native to Cloud Web Security Service methods.

  - AT&T tested and supports Microsoft® Active Directory Federation Services (AD FS) 2.0/3.0.

  - You can use the Auth Connector server as the IdP. The domain controller scales well, provides the group memberships, and automatically handles complexities, such as nested groups.

    For more detailed information, see "About the Auth Connector as a SAML IdP" on page 51.

- AT&T tested the Cloud Web Security Service with the following SAML IdPs.

  - Symantec VIP Access Manager (enables Single Sign-On)

  - Google G Suite

  - Microsoft Azure (with SCIM 2.0)
Flow Overview

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

SAML Flow

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

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

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

About SAML Connections

Support for Multiple AD Forests

AT&T 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 Cloud 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.

Configure This?

AD FS

- Proceed to "Import Users and Groups for SAML" on page 41.

Auth Connector

- "About the Auth Connector as a SAML IdP" on page 51
- "Deploy Auth Connector as SAML IdP" on page 54

Third-Party IdPs

- "Integrate Symantec VIP Access Manager as the SAML IdP" on page 96
- "Integrate Google G Suite as a SAML IdP" on page 83
- "Integrate Microsoft Azure as the SAML IdP" on page 58
- "Integrate Okta as the SAML IdP" on page 73
- "Integrate Ping Identity as the SAML IdP" on page 90

SEP

- Connectivity: WSS-SEP Roaming SAML
Import Users and Groups for SAML

The AT&T Web Security Service portal provides a method to manually import usernames and/or group memberships. This is required if you are implementing Security Assertion Markup Language (SAML) as your only method to authenticate users and groups that are sending web traffic to the Cloud 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.

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

2. 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 at list contains user and groups have already been imported, the service displays a notification dialog and does not re-add those names.

SCIM Option—Synchronize User/Group Population in an IdP

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

The Third-Party Sync tab on the 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 Cloud Web Security Service. You can see the updated the users and groups in the portal. Subsequent synchronizations require less time; AT&T 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 Cloud 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 Cloud Web Security Service.

- "Integrate Microsoft Azure as the SAML IdP" on page 58
- "Integrate Okta as the SAML IdP" on page 73

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 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, which enables you to instantly edit and apply changes. For example, the **Who** tab that contains the selected user.

**Next Step**

- Proceed to: "Prepare Microsoft AD FS for Federation" on page 45.
Prepare Microsoft AD FS for Federation

As part of the AT&T 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 Cloud 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 might require for your deployment, refer to the AD FS documentation.

**Tip**: AT&T 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 Cloud 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 Authentication" on page 37, 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 AT&T Web Security Service is the SP and federates with a supported IdP that currently provides SAML authentication in your network.

Technical Requirements

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

Step 1—Export Metadata from the AD FS.

This step describes how to export the metadata from the IdP into an XML file that can be read by the Cloud Web Security 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.

3. Copy the URL and paste it into a browser address bar.

4. Save the XML document. If another person is to perform the Cloud 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 Cloud 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**. AT&T 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 Cloud 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 include manually entering the value if the metadata does not contain the attribute or if the metadata is not imported.

b. By default, the Cloud 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 Cloud 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, AT&T 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**.

![Signing Certificate Chains]

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 Cloud Web Security Service portal displays any certificate-related errors, see "Troubleshoot SAML Authentication" on page 134.

6. Click **Save**.

**Step 3—Verify Policy Sync**

Turning authentication on and off triggers a policy update between the your account and the Cloud 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) method—Proceed to "Authentication Location Policy" on page 123.
- Remote Users—Select **Service mode > Mobility > WSS 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. You might have other reasons to bypass.

- See "Exempt From Authentication" on page 130.

**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 134 for possible causes and resolutions.
About the Auth Connector as a SAML IdP

The AT&T Cloud 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 Cloud Web Security Service as a Service Provider (SP), see "About SAML Authentication" on page 37.

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 (Cloud 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 Cloud 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

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

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

However, group memberships are identified through a different process. The Cloud 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 Cloud 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 Cloud 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 "Deploy Auth Connector as SAML IdP" on page 54.
Deploy Auth Connector as SAML IdP

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

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

Technical Requirements

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


The result is the domain controller provides the Auth Connector the domain and global groups in the its forest. If you can add a group to an ACL on the member server that has the Auth Connector, then the Domain Controller informs the Auth Connector.

- If you have previously used the Auth Connector authentication method and plan to switch to SAML or employ both methods and want to maintain policy based on usernames, you might have to re-examine policy to include both Auth Connector and SAML authenticated users.
- Verify that the following ports are open on the Windows firewall service on the Auth Connector server: 80 and 443.
- If you require information about Captive Portal, see "About Captive Portal Authentication" on page 103.

Procedure

Step 1—Federate the Service and the Auth Connector.

This step establishes trust between the Cloud 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.
a. Enter **bcca** as the **Entity ID**.

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

c. AT&T 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.

   a. By default, the Cloud 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. Add the Auth Connector IdP certificate.
a. The Auth Connector installation wizard prompted you to select it as the SAML IdP ("Deploy the Auth Connector" on page 24, Step 5.6).
   - If you selected this option, navigate to C:\Programs and Files (x86)\Blue Coat Systems\BCCA\ and open the saml-cert.cer certificate file in a text editor.
   - If you elected to use an existing one, open it in a text editor.

b. Click Add New Certificate.

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

d. Click OK.

Tip: If the Cloud Web Security Service displays any certificate-related errors, see "Troubleshoot SAML Authentication" on page 134.

6. Click Save.

Step 2—Configure browsers to trust the Auth Connector.

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

- Use group policy to configure browsers to add the Auth Connector hostname to their trusted sites.

- Manually configure browsers. For example, in Internet Explorer, navigate to Tools > Internet Options > Security. Add the hostname to the Local Intranet or Trusted Sites list.

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

Step 3—Specify Captive Portal Policy Per Location

Enable Captive Portal for the Firewall/VPN or Explicit Proxy location.
See "Authentication Location Policy" on page 123.
Integrate Microsoft Azure as the SAML IdP

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

The Cloud 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 Cloud 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 130.

**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 Cloud 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 Cloud 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 Cloud 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.
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.userprincipalname`.

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.

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 Cloud 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 134 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 Cloud Web Security Service group-level policy to be valid, the name of the roles **must** match the name of the groups used in the Cloud Web Security Service policies.

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

c. Click Select Role.
d. Select which roles are to be susceptible to Cloud 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 Cloud 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 *user.assignedroles*.

f. Click **OK**.

**Step 7—Configure Automatic User/Group Population in the Cloud Web Security Service.**

Provision your Azure account to manage users and groups within the Azure portal yet have them automatically sync to the Cloud 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" on page 41 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 Cloud Web Security Service.
   a. Select **Provisioning**.
   b. From the **Provisioning Mode** drop-down list, select **Automatic**.

6. In a new tab, access your Cloud 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.
d. In the **Tenant URL field**, paste the SCIM URL.

e. Return to the Cloud 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.

      ![Provisioning Mode](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 Cloud 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. |

---

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

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

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

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

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

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

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

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

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

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

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

7. Click **Save**.

**Synchronization**

When you start the initial synchronization, it can take on the average of 15 to 45 minutes before Azure begins to send data to the Cloud 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.

<table>
<thead>
<tr>
<th>Group</th>
<th>Policy</th>
<th>Source</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>roleA</td>
<td>bbc.com</td>
<td>Block</td>
</tr>
<tr>
<td>2</td>
<td>roleB</td>
<td>cnn.com</td>
<td>Block</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
<td></td>
<td>Block</td>
</tr>
</tbody>
</table>

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 130.

Next Step

- As authenticated user traffic begins to come in, verify the success of the integration. In Solutions mode, generate user-based reports and verify that they display expected authenticated employee names.
- Decide whether or not further authentication policy is required. "Authentication Location Policy" on page 123.
- "Import Users and Groups for SAML" on page 41.

Alternate Media

Microsoft created a documentation topic that demonstrates the integration.

Integrate Okta as the SAML IdP

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

The Cloud 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 Cloud 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 130.

- 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.


- The procedure includes a step involving the Secure Cross-domain Identity Management (SCIM) feature.

  See the SCIM section in "Import Users and Groups for SAML" on page 41 for details and prerequisites.

Procedure

Step 1—Add the Symantec WSS App

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

2. Add the Symantec app.
a. Click **Add Application**.

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 Cloud 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 Cloud 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 Cloud 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 Attributed, 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 Cloud Web Security Service.

2. Assign the users and groups to the app.

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

![Assignments](image)

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

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

c. Search for users and groups to add.

![Assign Symantec Web Security Service to People](image)
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**.
In the Group Attribute field, enter group.

Click Save.

Test Step

To perform an immediate configuration validation, you can explicitly proxy a browser of a client on the network to the Cloud 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 134 for possible causes and resolutions.

Known Issue

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

1. Click Inactive and click Unlink published group.
2. In the Unlink Pushed Group dialog, ensure that Delete the group in the target app (recommended) is selected and click Unlink. This deletes the group in the WSS app’s push list and the Cloud 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. "Authentication Location Policy" on page 123.
Integrate Google G Suite as a SAML IdP

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

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 Cloud 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 130.

Procedure

Google G Suite Registration

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


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

3. If you your organization has a domain name, click Yes, I Have One I Can Use and enter it into the field provided. If your organization does not yet have a domain name, and would like to use Google’s domain name registration services, click No, I Need One.

4. Using the domain name entered above, enter new user details for an email address you will use to administer your G Suite account. For example, admin@myexample.com. Define a password for the new account and click Next to proceed to Add Domain Registration.

5. Follow the remaining prompts to complete your account and domain registration.

Google G Suite SAML Configuration


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.

4. Click the arrow on the right of the SymantecWSS line.

5. 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 Cloud Web Security Service 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 AT&T Cloud Web Security Service details:
a. ACS URL: threatpulse.net:8443/saml/saml_realm/bcsamlpost
b. Entity ID: https://saml.threatpulse.net:8443/saml/saml_realm
c. You can leave other fields in their default state. Click Next.

7. Define the user and group identifiers for authentication.

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

![Attribute Mapping](image)

a. Click Add New Mapping to use the Department field as the user group. The groups defined here as Departments can be used in Cloud Web Security Service 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 Cloud Web Security Service portal and navigate to **Service > Authentication > SAML**.

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

   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 Cloud 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 134 for possible causes and resolutions.

Next Step

- As authenticated user traffic begins to come in, verify the success of the integration. In Solutions mode, generate user-based reports and verify that they display expected authenticated employee names.
- Decide whether or not further authentication policy is required. "Authentication Location Policy" on page 123.
- "Import Users and Groups for SAML" on page 41.
- "Exempt From Authentication" on page 130.
Integrate Ping Identity as the SAML IdP

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

Technical Requirements

- Port 8443 is required for browsers to post SAML assertions to a Cloud 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 130.

Procedure

Step 1—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 Cloud Web Security Service

Enable the two services to communicate.

1. Log in to your Cloud 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/bcsamllpost

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

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

- Signing Certificate: PingOne Account Origination Certificate
- SAML Metadata: Download

Provide SAML details about the application you are connecting to:

- Protocol Version: SAML v 2.0
- Upload Metadata: Select File or use URL
- Entity ID: https://saml.threatpulse.net:8443/saml/

4. Return to the Cloud Web Security Service portal Authentication > SAML page.

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

b. **Upload** the Cloud Web Security Service Metadata.

   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**.

Federação 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 Cloud 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 134 for possible causes and resolutions.

Next Step

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

- Decide whether or not further authentication policy is required. "Authentication Location Policy" on page 123.

- "Import Users and Groups for SAML" on page 41.

- "Exempt From Authentication" on page 130.
Integrate Symantec VIP Access Manager as the SAML IdP

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

Technical Requirements

- Port 8443 is required for browsers to post SAML assertions to a Cloud 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/bsamlpost
      - **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 Cloud Web Security Service

The next phase is to export and add metadata to the Cloud 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.


4. Expand the Configure SAML Authentication area.

   ![Configure SAML Authentication](image)

   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.

Step 3—Test

To perform an immediate configuration validation, you can explicitly proxy a browser of a client on the network to the Cloud 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 134 for possible causes and resolutions.

**Step 4—Import Users**

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

1. Download the user list in a spreadsheet format.
In the VIP Access Manager, select the Users tab.

Select the Local Users row.

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

Save the .csv-formatted file.

Prepare the user list for import.

Open the saved .csv file in Excel.

Select the userName column.

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

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

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

Select Service > Authentication > Users and Groups.

Select Manual Import.

Click Add. The portal displays the Add User dialog.

Select Import Users/Groups; under Import Users, click Browse.

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. "Authentication Location Policy" on page 123.
- "Import Users and Groups for SAML" on page 41.
- "Exempt From Authentication" on page 130.
About Captive Portal Authentication

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

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

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

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

A—Firewall/VPN/Guest WiFi Over IPSec

The Cloud 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 Cloud 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, AT&T recommends using Cookie Surrogates. After a user authenticates from an IP address, all further requests from that IP address are treated as if from that user. If the client is behind a NAT or on a multi-user system, the first user’s credentials are used. For example, Employee A requests web content and the Cloud 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 method neither provides authentication nor sends user and group information to the Cloud 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 Cloud Web Security Service. Using the Authentication Policy Editor, you can specify the authentication refresh intervals on a per-location basis.

**C—WSS Agent**

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

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

**D—Quick Authentication Demonstration (Roaming Captive Portal)**

Roaming Captive Portal allows you to quickly connect a non-enrolled device (mobile device or laptop) to the Cloud 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 Cloud 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 Cloud 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 Cloud 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).

- 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 methods and credential refresh times for both the Firewall/VPN and Explicit Proxy methods.

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

- When the user attempts to reconnect to the web after those respective time thresholds.

- Other network activity, such as that employee’s data getting moved from one data pod to another.

- The Auth Connector abides by the lockout settings in the AD. For example, the AD is configured to allow three attempts to log in. If the third attempt fails, the user is locked out for 30 minutes before they can attempt again.

- If a lockout configuration exists and the user triggers it or if the user attempts to use an expired password:
  
  - All web-bound transaction intended for the Cloud Web Security Service is dropped; all other traffic continues normally.

  - If the fault is an Auth Connector problem, the user connects to the Cloud Web Security Service as an unauthenticated user.
If you render an employee disabled, the Cloud 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 "Authentication Location Policy" on page 123.
- Remote Users—Select Service mode > Mobility > WSS Agent. This page contains the Enable Captive Portal option.
About Roaming Captive Portal

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

Employees must enter their credentials per the following.

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

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

Tip: If you deployment includes Symantec Endpoint Protection (SEP) clients, you can enable Roaming SAML Authentication. See the SEP topics in the Cloud Web Security Service Help System.
Topography

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

AT&T 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 Cloud 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 Cloud Web Security Service data pod locations on the planet.

3—On a laptop connected to the corporate Wi-Fi (B), configure a browser to explicitly proxy to the Cloud 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 Cloud 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 Cloud 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 Cloud 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 Cloud Web Security Service.

---

**Implement This Feature?**

- Proceed to "Enable Roaming Captive Portal" on page 110.
Enable Roaming Captive Portal

The AT&T 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 Cloud Web Security Service portal, which includes specifying corporate e-mail domains.

Technical Requirements

- Be advised of the security risks exposed by this feature. See "About Roaming Captive Portal" on page 107.
- Roaming Captive Portal requires a functioning Auth Connector deployment. See "Deploy the Auth Connector" on page 24.
- All endpoint clients must have the Cloud Web Security Service root certificate.
- You must enable SSL interception policy for Mobile Device Sources..
- Verify that each user to be authenticated has their e-mail address attribute populated in the AD (User Properties dialog > General > E-mail). For example, EXAMPLECORP\alan.user has an e-mail attribute of alan.user@examplecorp.com. If you are employing Exchange, default policies automatically create this attribute. If you are not employing Exchange and have a large number of users with undefined e-mail attributes in the AD, search online for resources about how to use a script to populate.

Procedure

1. In Service mode, select Authentication > Auth Connector.
2. Expand the Roaming Captive Portal area.
3. Toggle Roaming Captive Portal to Enabled.
4. Add the email domain.
   a. Expand the Email Domains area.
   b. Click Add.
c. In the **Add** dialog, enter a **Domain** or sub-domain and click **Add**.

![Add Domain Dialog]

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

![Roaming Captive Portal]

**Next Selection**

Configure a browser or mobile device to explicitly proxy to the Cloud Web Security Service roaming PAC file.

- See "**Configure Browsers for RCP**" on page 112.
- See "**Enable Roaming Captive Portal on iOS**" on page 117.
- See "**Enable Roaming Captive Portal for Android**" on page 114.
Configure Browsers for RCP

With Roaming Captive Portal enabled on the AT&T 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://cloudwebsecurity.att.com/roaming

For more details, see the following.

- See "Enable Roaming Captive Portal" on page 110.

Procedure

Apple Safari

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

5. Click **OK** and exit out of all open dialogs.
Enable Roaming Captive Portal for Android

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

- See "Enable Roaming Captive Portal" on page 110.

Procedure

1. On the device, tap **Settings**.

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

3. Scroll down and tap **Show Advanced Options**.
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.
Enable Roaming Captive Portal on iOS

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

- See "Enable Roaming Captive Portal" on page 110.

Procedure

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://cloudwebsecurity.att.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 a website that belongs to a category blocked by defined policy. If the page is blocked, the configuration was successful.
Test: Browse to blocked category website.

Denied by Policy notification. Click more to view details; less to hide.
Review Imported Users and Groups

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

Imported From SAML

If your authentication method is SAML, see "Import Users and Groups for SAML" on page 41.

Imported From the Auth Connector

If you deploy the Auth Connector, the Cloud 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 Cloud 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 Cloud Web Security Service performs an AD refresh once per 24 hours. Click **Synchronize with AD** to perform an instant refresh and synchronize the most current user and group memberships.

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

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

D—The **Policy Rule Reference** column indicates that a Content Filter policy rule exists that applies to the user or group (**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.
Authentication Location Policy

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

You can also enable Captive Portal (see "About Captive Portal Authentication" on page 103).

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

- **Explicit Proxy**—In the policy editor you specify the **Sources** and the define applicable parameters.
  - Select Locations. The Cloud Web Security Service detects Explicit Proxy Locations already defined on the **Service** mode > **Network > Locations** tab. Or you can create a new one directly in the policy editor.
  - The default authentication method is the Auth Connector. You can also enable Captive Portal and select to use the Auth Connector or SAML as the authentication method.

About Captive Portal Policy

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

Firewall/VPN Surrogate Types

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

- **IP**—The Cloud 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. AT&T recommends this method to reduce the impact of CORS-related issues. The exception is if traffic comes through a circuit-level gateway where IP addresses are shared; you must use the Cookie method.

- **Cookie**—The Cloud 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. If you see CORS issues with this method, you can increase the timeouts.
Note: For the Explicit Proxy connectivity method, only the cookie surrogate is available.

Refresh Times

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

More information.

- See "About Captive Portal Authentication" on page 103.
- Consult the WSS Agent documentation for Captive Portal information.

Define Authentication Policy

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

Procedures

Firewall/VPN Access Method

1. In the Cloud 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 24 hours after authentication occurs, the client receives a credential dialog (for SAML, that might not occur).

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

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

8. Click Activate.

Explicit Proxy Access Method

1. In the Cloud 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]

-specific, named locations.

-import or create a named location list.
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 can create a new list of detected locations from this option.

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

This procedure continues with the Locations option.

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

   ![Add Sources](image)

   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.

- CORS-related issues.
- Authentication looping with cloud-based IdP servers.
- The source device (for example, a legacy server) is not compatible with redirection-based authentication.
- A web application API call is not compatible with redirection-based authentication.

To mitigate this, add destinations and sources that you want exempted from authorization challenges.

<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>WSS Agent</td>
<td>Web Applications</td>
</tr>
<tr>
<td>Mobile Devices</td>
<td>Categories</td>
</tr>
</tbody>
</table>

About Clients That Are Not Forms-Based

The Cloud Web Security Service has an option to exempt WSS Agent and mobile clients.

- WSS Agent—
  - If Captive portal is disabled, WSS Agent identifies itself as the logged-on user.
  - If Captive Portal is enabled, WSS Agent prompts for credentials before web requests are allowed.
- Mobile clients—The credentials are obtained from the installed certificate.

These options are here alternate authentication methods that might be supported in future Cloud Web Security Service versions.

Procedure

1. Select **Service mode > Authentication > Authentication Policy**.
2. Expand the **Global Exemptions** area.
3. Click **Add Auth Exemption**. The portal displays the Auth: New Exemption Rule.
4. Click **Add Sources**.
All already configured entries or lists populate any selection. For example, if you click **Locations**, you can select from any location that currently sends traffic to the Cloud Web Security Service account.

- **WSS Agents** and **Mobile Devices** are static objects; selecting them means the exemption applies to all connections from each of those access methods.

5. **(Optional)** If you need to quickly exempt a source, you can create a new entry from this wizard. For example, you need to immediately exempt a new IP address.
   - a. Click **IPs/Subnets**.
   - b. Select **New > IP/Subnet**.
   - c. Enter a new address (or import a list from a text file).
   - d. Click **Save**.

6. Click **Add Destinations**.

   Select the destination elements that are exempt from authentication and click **Save**.

7. Click **Add Rule**. This creates a new Auth Exemption policy rule.
8. You can add additional rule. When satisfied, click **Activate**.

9. Verify with your employees that their clients are no longer prompted for credentials because of the new policy.
Reference: Authentication IP Addresses

The Web Security Service Auth Connector communicates with devices in the geographically located data centers.

The Symantec Operations team maintains the following Knowledge Base article.

https://knowledge.broadcom.com/external/article?articleId=165389
Troubleshoot SAML Authentication

Certificate Warnings

Sixty days before a certificate in the signing chain expires, the AT&T 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**—AT&T supports and recommends SHA2 for the Cloud 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 Cloud 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.

Clear Associated Auth Surrogates and Restart Authentication

If a client is experiencing SAML-related connection issues with the Cloud Web Security Service, you can instruct the user to enter a URL that stops the connection to the Cloud Web Security Service. The URL is https://notify.threatpulse.net/logout. The following occurs.
The user is logged out of the asset that currently maintains that connection in the Cloud Web Security Service datacenter. If the user has existing valid sessions to other assets, those sessions will continue to be valid.

The user is not logged out of the SAML IdP.

If a user attempts to browse after logging out, they might be immediately be re-authenticated without the credential prompt. The Cloud Web Security Service redirects to the IdP, where the user is still logged in, for authentication. Typically, the IdP uses a session cookie to identify the user’s authenticated session. The IdP then redirects back to the Cloud Web Security Service with a SAML assertion, and the user is signed back to the Cloud Web Security Service asset. Because of this, AT&T recommends invoking the URL in a logout script or after the browser is closed so that session cookies are forgotten.

Internet Explorer Sessions

Some 3rd party extensions in Internet Explorer might cause the process to hang and never fully close down. As a result, the sessions might not end when an employee closes the IE window. The sessions will eventually time out, however. To see more about this issue, refer to the following Microsoft article.


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.                      |
| Various run-time errors.                                           | The IdP does not recognize the Cloud Web Security Service entity ID because the federation is broken (or was never created) at the IdP. |
| The IdP fails to authenticate a known valid user.                  | User does not exist or entered wrong password multiple times. |

SAML Bypass List

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

  SAML Bypass List KB Article