End User Single Sign-On for Forcepoint Web Security Cloud

Forcepoint Web Security Cloud / End User Single Sign-on for Forcepoint Web Security Cloud

The end user single sign-on feature (SSO) allows seamless authentication for end users browsing via Forcepoint Web Security Cloud, using a supported identity provider (IdP). When enabled, the cloud service uses your identity provider to authenticate user identity, attributes, and roles using your enterprise directory.

Single sign-on is a convenient and secure way of sharing logon credentials across your estate, streamlining the authentication process across multiple systems, and providing seamless authentication in cases where the Forcepoint Web Security Endpoint cannot be used. Forcepoint uses the Security Assertion Markup Language (SAML 2.0) data format to send authentication requests to and receive responses from your identity provider. All communications between components are secured.

When single sign-on is enabled, end users are redirected to the identity provider specified in their policy when connecting to the proxy. Once users have been authenticated by the provider, they are directed back to the proxy, and the appropriate policy applied to their web request. Clients who have authenticated once do not need to re-authenticate for a set period of time.

This document covers the following topics:

- *Supported identity providers*
- *Configuration steps*
- *How single sign-on works*
  - *Authentication for roaming or remote users*
  - *SSO with tunneling*
  - *Auto-provisioning*
  - *Authentication decryption*
- *Limitations and recommendations*
- *Troubleshooting*

Supported identity providers

Single sign-on is a standards based service that supports any identity provider that supports the SAML 2.0 standard. Following is a partial list of the currently supported providers.

- Google IdP
- Microsoft Active Directory Federation Services
- Microsoft Azure Active Directory
- Okta
- OpenAM
- Oracle Identity Federation
- PingFederate

Note

Single sign-on can be used with pure cloud or hybrid solutions. Some of the providers listed above are not supported for use with Forcepoint Web Security Hybrid Module. Please contact Technical Support for details of currently supported identity providers for hybrid.

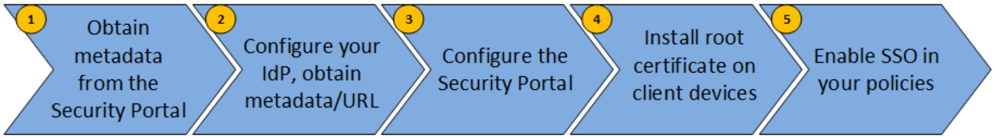
This document covers configuring single sign-on for the cloud service.

Configuration steps

Before you begin, ensure that you have the following pre-requisites:

- Administrator logon details for the Forcepoint Cloud Security Gateway Portal (also referred to as the cloud portal) with the single sign-on feature enabled in your account. Contact Technical Support if you do not have this feature.
- Access to a supported identity provider (either within your network, or a cloud service).

Follow the steps below to deploy single sign-on for your cloud account.


1
Obtain metadata from the Security Portal
2
Configure your IdP, obtain metadata/URL
3
Configure the Security Portal
4
Install root certificate on client devices
5
Enable SSO in your policies

1. Log on to the cloud portal and navigate to **Web** > **Settings** > **Single Sign-on**. Click the download links to save the following files:
   a. Forcepoint LLC Metadata: this XML file must be uploaded to your identity provider. (See the instructions in step 3.)
   b. Forcepoint LLC Root Certificate: this certificate must be installed on all clients that will use SSO authentication.
2. Log on to your identity provider and perform the following steps:
   a. Configure your identity provider with service details and metadata for the Forcepoint cloud service. Refer to the following articles in the Forcepoint Knowledge Base for detailed instructions on configuring the following packages to work with Forcepoint Web Security Cloud SSO:
      - Google IdP
      - Microsoft Acitive Directory Federation Services
      - Microsoft Azure Active Directory
      - Okta
      - PingFederate

   b. Obtain the identity provider's metadata. This will either be in the form of a URL, or a file you can download. (See the Knowledge Base articles listed above for further details.)
3. Returning to the cloud portal, navigate to **Web** > **Settings** > **Single Sign-on** and perform the following steps:
   a. For customers new to single sign-on, the Identity provider entry displays SAML 2.0 Compliant Identity Provider and cannot be changed.

      For customers who had configured single sign-on prior to the introduction of the of SAML 2.0 Compliant Identity Provider option, the previously selected identity provider is displayed and a drop-down list offers the original provider and SAML 2.0 Compliant Identity Provider.

      It is recommended that all customers select SAML 2.0 Compliant Identity Provider.

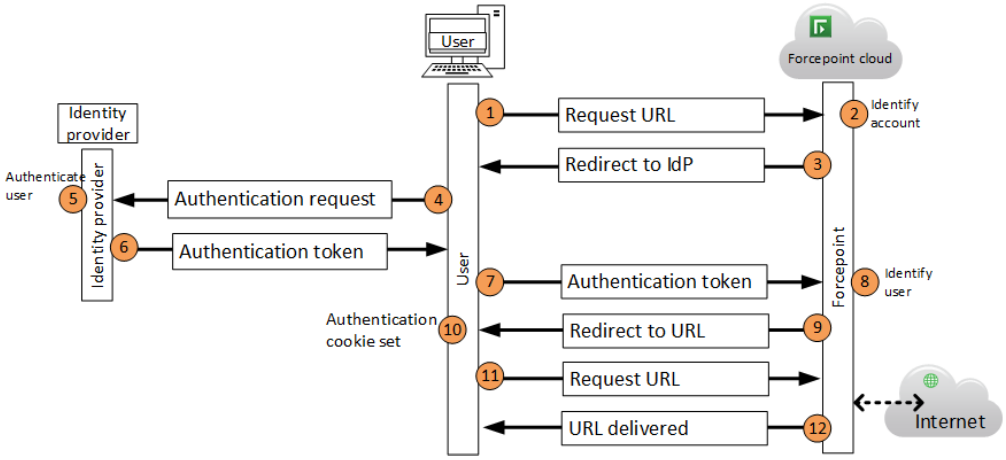
b. For Metadata source, select either URL or File upload. Provide the metadata obtained from your identity provider in step 2b. See Forcepoint Web Security Cloud Help - Configure Single Sign-On settings for further details.

c. If applicable, add the identity provider's hostnames as non-proxied domains using the on the **Web** > **Bypass Settings** > **Proxy Bypass** page. (Cloud-based IdPs perform additional redirects to URLs not present in the metadata. Check the Knowledge Base articles above for details of any required domains.)

4. Install the Forcepoint root certificate that you downloaded from the cloud portal on all client machines that will use SSO, using your preferred distribution method (such as Windows Group Policy Objects).
5. Enable SSO authentication in your policies, on the Access Control tab. See
6. Forcepoint Web Security Cloud Help - Access Control tab.

How single sign-on works

The following diagram illustrates how Forcepoint authenticates users via your identity provider.



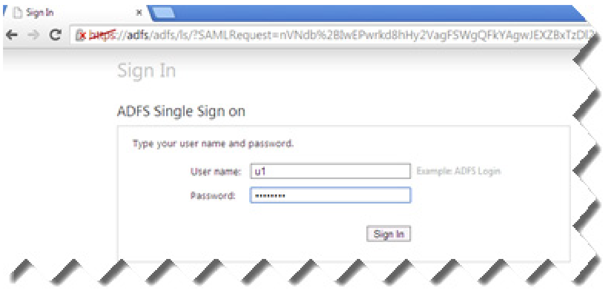
1. The user requests a web page via the cloud proxy.
2. The cloud service identifies the user’s account.
   a. For local users, this is based on the user’s IP address.
   b. For roaming users, this typically requires the user to enter an email address.
3. The service redirects the user’s browser to the identity provider configured for the account.
4. The user’s browser makes an authentication request to the identity provider.
5. The identity provider authenticates the user.
6. An authentication token is posted to the user’s browser.
7. The token is forwarded to the Forcepoint cloud service.
8. The token is validated against the identity provider’s metadata, and the user is identified. Policy settings for the user are checked, and the request is permitted or blocked.
9. The cloud service redirects the user’s browser back to the requested URL.
10. Account identification and authentication cookies are set in the user’s browser. The next time the user accesses the service, the user’s account is identified and the session authenticated via the cookie, without redirecting to the IdP.
11. The browser requests the URL for the second time.

12. The URL is retrieved and served to the user.

> **Note**
>
> The cloud service caches authentication sessions and sets a cookie in the user's browser upon successful authentication. Steps 3-10 above are performed only once per authenticated session.
>
> Users will only be re-authenticated if they clear their browser cookies, use a different browser, or do not re-authenticate for the session timeout duration, causing the cookie to expire. The session timeout duration is defined on the **Access Control** tab of your policy.

If the user's policy does not force authentication for requests with known IP addresses, the authentication process for local users happens without user interaction.

If the user's policy is set to **Always authenticate users on first access**, or if the user is requesting a category that requires authentication, the user receives the identity provider's sign in page. The sign in page below is an example from Microsoft AD FS. (This page can usually be customized via your identity provider's management console.)



~~https~~://adfs/adfs/ls/?SAMLRequest=nVNdb%2BlwEPwrkd8hHy2VagFSWgQFkYAgwJEXZBxTzDI2

Sign In

ADFS Single Sign on

Type your user name and password.

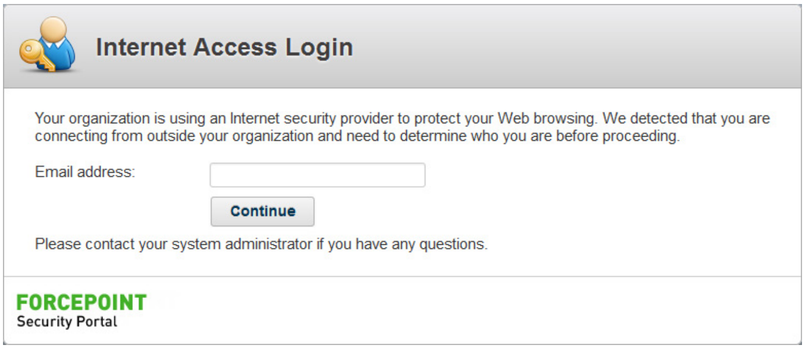
User name: u1

Password: ••••••••

After entering valid credentials, the user is redirected to the requested website.

Authentication for roaming or remote users

When roaming or remote users first connect from an unknown IP address, the cloud service must identify which account the user belongs to. In a default configuration, users connecting from an unknown IP address are required to identify themselves by entering their email address in a login form. This allows the proxy to match the roaming user to an account, in order to use the correct identity provider.



Internet Access Login

Your organization is using an Internet security provider to protect your Web browsing. We detected that you are connecting from outside your organization and need to determine who you are before proceeding.

Email address:

Please contact your system administrator if you have any questions.

When the user submits a valid email address, the corresponding account is identified, and identity provider details are used to generate an authentication request and redirect the user to the provider for authentication. (If a user enters an unrecognized email address, an error will be displayed on the form and they will have to retry.)

Users are typically only required to carry out this step once; following a successful authentication, a long-lived cookie containing the user's account ID is set, allowing the service to recognize the user's account without user interaction. This step will be required again if the user connects using a different browser, clears the browser's cookies, or does not re-authenticate for a long period, causing the cookie to expire. The default lifetime duration for the account identifier cookie is 6 months.

✓ **Note: dedicated ports (limited availability)**

For organizations that do not wish their roaming users to enter an email address upon first login, Forcepoint can configure a dedicated port for SSO authentication. This allows the service to identify the account for roaming users without requiring them to provide an email address.

The use of a dedicated port for SSO is a limited availability feature. Please contact Technical Support if you require further information about this option.

SSO with tunneling

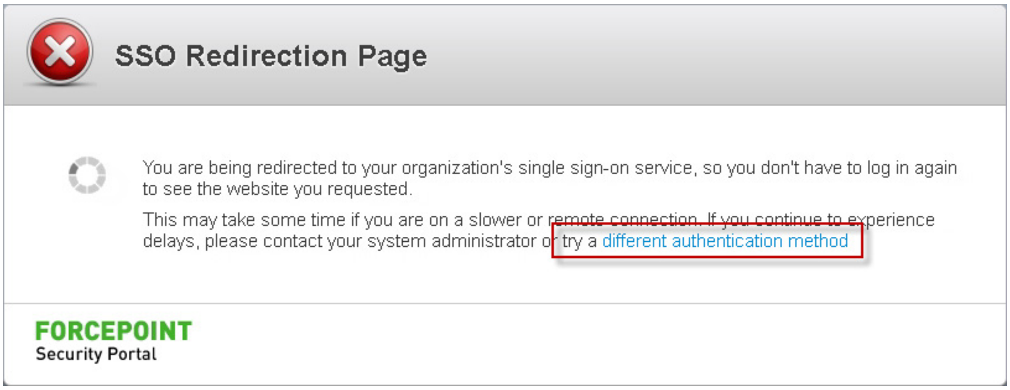
Single sign-on is supported for use with tunneling connectivity to the cloud service (IPsec Advanced, GRE, and EasyConnect).

Important

SSO with tunneling works only with GRE, IPsec Advanced, EasyConnect, etc. It does not work with Legacy IPsec.

Authentication fallback

If the service cannot communicate with the identity provider, users have the option to authenticate with the cloud service using a different mechanism. During the identity provider redirect process, a redirection page is shown. The page has a link that allows the user to cancel the single sign-on process and try a different authentication method.



SSO Redirection Page

You are being redirected to your organization's single sign-on service, so you don't have to log in again to see the website you requested.

This may take some time if you are on a slower or remote connection. If you continue to experience delays, please contact your system administrator or try a different authentication method

FORCEPOINT
Security Portal

When the user clicks this link, the service will first attempt to identify the user via transparent NTLM identification, before falling back to manual authentication (depending on the settings enabled in the user's policy). See [Forcepoint Web Security Cloud Help - Access Control tab]().

Note

For roaming users, manual form authentication is the only alternative method available.

Authentication fallback is not supported when using a dedicated port for SSO.

Auto-provisioning

Users that are unknown to the system can be auto-provisioned to a cloud policy following successful authentication with your identity provider. Auto-provisioned users are added to the policy using either the user's email address or NTLM ID contained in the authentication token provided by your identity provider.

Auto-provisioning is supported for local users, and roaming users browsing via a dedicated port. Auto-provisioning is not supported for roaming users identifying via the account identification page.

> **Note**
>
> The use of a dedicated port for SSO is a limited availability feature. Please contact Technical Support if you require further information.
>
> In order to auto-provision users to a specific policy when using dedicated ports, please contact Technical Support.

Authentication decryption

When single sign-on is enabled for an account, the cloud service performs authentication decryption by default for HTTPS traffic, regardless of whether SSL decryption is enabled in the policy. This is required in order to identify users.

Consequently, customers must download the Forcepoint root certificate and install it on all client machines that will use single sign-on. This ensures that end users browsing to HTTPS sites can be authenticated seamlessly via your identity provider. If the certificate is not installed, users will see a browser error stating that the site certificate is not valid.

Supported decryption and proxy bypass settings

Because of the way single sign-on works, some bypass settings are either not supported, or may function differently for local and roaming users. Affected features are:

- **Authentication decryption bypass** (accessed via the **Web** > **Bypass Settings** > **SSL** tab). This setting is used to disable authentication decryption for certain categories across all policies.
- **Authentication bypass by user agent or destination** (accessed via the **Web** > **Bypass Settings** > **Authentication Bypass** tab). This setting completely bypasses authentication for specified user agents or hostnames across all policies.

- **SSL decryption bypass** (accessed via **Web** > **Policies** > **[policy name]** > **Web Categories** > **SSL Decryption Bypass**). This setting is used to disable SSL decryption for specified hostnames within each policy.

✓ **Note**

Non-proxied destinations are supported for both local and roaming users with SSO. Non-proxied domains are set globally on the **Web** > **Bypass Settings** > **Proxy Bypass** tab, or per policy under **Web** > **Policies** > **[policy name]** > **Connections** > **Proxy Bypass**.

Non-proxied domains bypass the proxy service entirely.

Behavior differences when these features are used alongside single sign-on are detailed in the following table.

Feature	Supported for local users?	Supported for roaming users?
Authentication decryption bypass	Supported. Authentication is not performed: users can browse anonymously for policy enforcement and reporting purposes.	Not supported. All HTTPS requests for roaming users are decrypted for authentication purposes in order to identify the user. Since the bypass setting can only be applied when the user's account has been identified, this setting is not applicable; roaming users will be authenticated.
Authentication bypass by user agent or hostname	Supported. Authentication is bypassed for specified user agents or hostnames. Users can browse anonymously for policy enforcement and reporting purposes.	Not supported. All HTTPS requests for roaming users are decrypted for authentication purposes in order to identify the user. Since the bypass setting can only be applied when the user's account has been identified, this setting is not applicable; roaming users will be authenticated.
SSL decryption bypass	Not supported. If SSL decryption is bypassed for a hostname, SSO cannot be used. Users see the manual authentication welcome page.	Not supported. If SSL decryption is bypassed for a hostname, SSO cannot be used. Users see the manual authentication welcome page.

Limitations and recommendations

The following table lists limitations and recommendations for using single sign-on.

Category	Limitation/recommendation
Supported clients	Single sign-on is supported only for web browsers. Other types of client cannot authenticate in this way. In order for other clients to work with the proxy service, you must enable authentication decryption bypass by user agent or destination. This is set on the **Web** > **Bypass Settings** > **Authentication Bypass** page. Note that authentication decryption bypass is not supported for roaming users.
Forcepoint root certificate	When single sign-on is enabled, the cloud service performs authentication decryption for HTTPS sites by default in order to identify users. Customers must download the Forcepoint root certificate and install it on all client machines that will use this method of authentication. This ensures that end users browsing to HTTPS sites can be authenticated seamlessly. If the certificate is not installed, users will see a browser error stating that the site certificate is not valid. Note that this applies to SSO over tunneling only if decryption is explicitly enabled in the policy.
SSLdecryption bypass: local users	If you have added categories to the SSL Decryption Bypass list via **Web** > **Policies** > **[policy name]** > **Web Categories** > **SSL Decryption Bypass**, users browsing HTTPS sites in these categories cannot be authenticated via your IdP. Users will see the manual authentication welcome page. Note that this does not apply to SSO over tunneling.
Authentication decryption: roaming users	For roaming users, the following authentication decryption settings are not supported: ● Authentication decryption bypass ● Authentication bypass by user agent or hostname ● SSL decryption bypass See *Supported decryption and proxy bypass settings*, page 9.
Auto-provisioning	Auto-provisioning is not supported for roaming users identifying via the account identification page.
Authentication fallback for dedicated ports	Authentication fallback is not supported when using dedicated ports. See *Authentication fallback*, page 8. Note that this does not apply to SSO over tunneling.

Category	Limitation/recommendation
SSO over tunneling	For on premises users, if the first site request by a user is to an HTTPS site and the applicable policy has SSL decryption disabled, the proxy will allow the user anonymously until the user browses to an HTTP or a decrypted HTTPS site and the user is authenticated.
Authentication for roaming and remote users	Roaming user requests to sites that use cross-origin resource sharing (CORS) may be blocked. These sites normally do not send cookies so the correct policy cannot be determined when cookie-based authentication is used. For sites that use CORS, any cross-origin resource domains that are requested can be added as Proxy Bypass destinations to avoid the issue.

Troubleshooting

This section outlines some common issues with single sign-on, with suggested solutions.

Problem	Suggested solutions
The identity provider login page is not displayed.	Check that the IDP's hostname or IP address can be reached. Check that the user's PAC file contains port 8006 (or the dedicated port for your account). If you are using a custom PAC file, this must be manually edited to include the relevant SSO port. Check that the **Always authenticate users on first access** setting is enabled in your policy. If the authentication cookie is already set, the page is not displayed. Clear your browser's cookies.
A certificate error is shown when browsing to HTTPS sites.	Ensure you have installed the Forcepoint root certificate on your client machine.
"Failed Authentication" message is displayed.	The single sign-on error page is shown if a user cannot be authenticated by your IDP. The page displays a brief status message (for example, "Reason: Invalid response from authentication gateway"). To help diagnose the problem, display the HTML source of the page to access more detailed technical information taken from the IDP's SAML response. This information will be useful if you need to contact Technical Support. See *Failed Authentication page*, page 14.
Fallback authentication link is not visible on the SSO redirect page	If you are using dedicated ports, this is expected behavior. Authentication fallback is not supported for dedicated ports.

If you are still experiencing issues, contact Forcepoint Technical Support. Ensure you have gathered the following information:

- **Error page HTML**

  If you receive a "Failed Authentication" page, save the HTML source. This contains technical information from your IDP on the nature of the authentication issue. See *Failed Authentication page*, page 14.

- **IdP configuration details/screenshots**

  If possible, provide screenshots of your IDP configuration.

- **IdP event logs**

  If applicable, obtain the event logs from your identity provider.

- **HAR file**

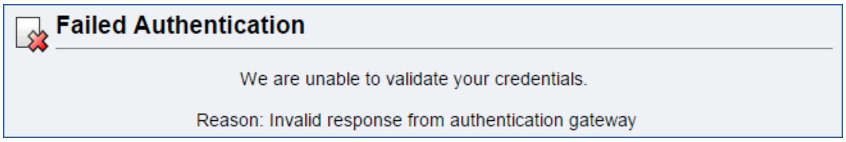
  To help diagnose network issues, you can generate a .HAR (HTTP Archive) file to log your browser's interaction with a particular website. HAR files can be generated using Google Chrome’s Developer Tools, as well as other software packages.

- **Packet captures**

  Capture your network traffic using a package such as Wireshark or FiddlerCap.

Failed Authentication page

The single-sign on error page includes information in the HTML source that may be useful in troubleshooting authentication issues.



Failed Authentication

We are unable to validate your credentials.

Reason: Invalid response from authentication gateway

For example, the HTML source for the error page shown above contains the following information in the <body> of the message:

```
<body>
 <div align="center">
  <div id="pagecontainer">
  <img src="https://www.websense.com/images/block.png" class="icon" />
  <h1>Failed Authentication</h1>
   <div align="center">
We are unable to validate your credentials.
  <br /><br />
Reason: Invalid response from authentication gateway
  <!-- Technical Information:
StatusCode=urn:oasis:names:tc:SAML:2.0:status:Responder
StatusMessage= -->
   </div>
  </div>
 </div>
</body>
```

The “Technical Information” section provides detailed information about the failure. This information is provided by the identity provider, and is therefore dependent on which identity provider you have configured.

The example shown above is taken from Microsoft AD FS, and the error message details are available at the following URL: https://msdn.microsoft.com/en-us/library/hh269642.aspx

Document last updated: August 10, 2022