Web Security Cloud

Getting Started Guide

Revision A

Contents

Introduction

Forcepoint Web Security Cloud is a flexible web protection solution that provides fine-tuned control over your users' web access, while providing comprehensive protection against web threats such as viruses, malware, data loss, and phishing attacks.

Forcepoint Web Security Cloud is intuitive to use and works out of the box with a default policy that applies common web filters. To make full use of its features, you can customize this default policy and configure your own policies to meet the needs of your organization.

This guide outlines the setup tasks required to get Forcepoint Web Security Cloud managing your web traffic. It also contains information on how to work with roaming users, and tips on tailoring policies for your organization. In the appendix you can find tips for preparing your end users for their new web protection system.

Detailed configuration information for Forcepoint Web Security Cloud is available in the Forcepoint Web Security Cloud Help. This can be accessed from within the cloud portal, or online here.

Note

This guide covers deploying the service as a purely cloud-based solution. If you are deploying with an I Series appliance, refer to the guide Deploying an I Series Appliance on the Forcepoint Support site.

Technical Support

If you have any questions during the set up phase, please contact your service provider or Forcepoint Technical Support. Technical information about Forcepoint products is available at the Forcepoint Support website.

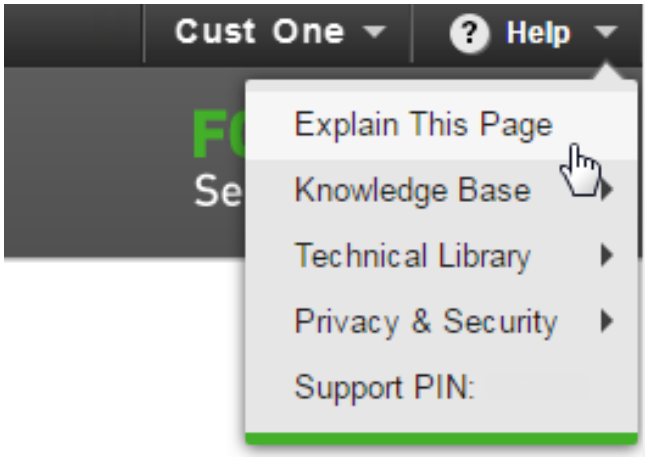
This site includes product documentation, release information, and a Knowledge Base detailing common configuration scenarios. Some material requires a Forcepoint Support login. For additional questions, the support portal offers an online support form. Just click **Contact Support**.

Tip

Create your support account when you first set up Forcepoint Web Security Cloud, so that access is readily available whenever you need support or updates.

Getting help

To get additional help while setting up the service, access the administrator help and other reference materials on the Forcepoint Support website, or from the Help menu in the cloud portal.



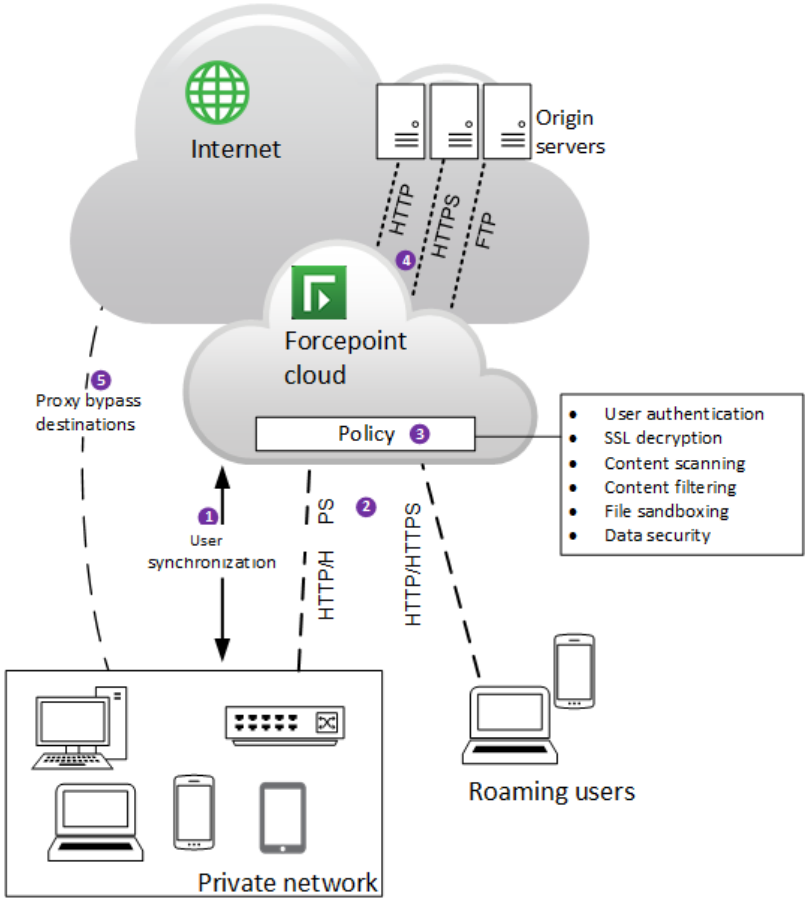
In addition, the portal provides a Resource Center that offers users various forms of assistance with product configuration and routine tasks. See Using the Resource Center in administrator help for more information.

How Forcepoint Web Security Cloud works

Forcepoint Web Security Cloud operates as a proxy server for HTTP and HTTPS traffic, as well as FTP over HTTP. When users request a web resource, their browsers do not connect directly to Internet web servers (shown in the following diagram as origin servers), but instead connect to the cloud proxy, which in turn relays requests to the origin server. This allows the cloud service to apply filtering rules and perform content scanning, providing protection against security threats, data loss, and inappropriate content.

The service can use various methods to identify and authenticate users: a Forcepoint Endpoint client, a third-party single sign-on identity provider, NTLM transparent identification, or manual authentication with a user name and password. Roaming users (those connecting from an unknown IP address) can be identified via the Forcepoint Endpoint client, via a single sign-on provider, or they are required to authenticate.

Optional SSL decryption allows the content of HTTPS sessions to be scanned, and allows the service to show the correct notification page to users (for example, a block page if the SSL site is in a category that is blocked). Content is re-encrypted after inspection. The following diagram shows a basic overview of web traffic protected by Forcepoint Web Security Cloud.



The diagram shows the following elements of the service.

1) Identity management allows user details to be synchronized with the cloud, enabling users to be identified and authenticated. This allows user- and group-level policy settings to be applied, as well as providing detailed user-level reporting.

2) Web traffic is directed to the cloud service from a private network, and from roaming users connecting from outside their LAN. There are various methods to redirect traffic (see in *Key concepts*).

3) Authentication, filtering and enforcement settings are applied by a policy, which determines which requests to allow or block, performs real-time content scanning, and applies data security filtering, helping to prevent inadvertent or malicious data loss.

4) When policy decisions have been applied, web requests are then forwarded to the origin server, and content is served to the user's browser. If content is blocked, or security threats are detected, configurable notification pages are shown, informing the user of the reason why access to the resource is not allowed.

5) Some web requests can go directly to the origin server, if the address is defined as a proxy bypass destination.
Secure (HTTPS) sessions are forwarded over a tunneled connection. If you enable SSL decryption, the content of these sessions can be scanned and policy settings applied, before the traffic is re-encrypted. This feature requires you to install a root certificate on end-users' machines, allowing clients to connect securely to the cloud proxy. (See Enabling SSL decryption in the Forcepoint Web Security Cloud help for more information.)

Related concepts
Key concepts on page 5

Key concepts

In order to get started with the service, you must arrange to forward your web traffic to the service, add users to the service (if required), and create policies to control web access (a default policy is pre-configured).

Traffic forwarding

In order for the service to perform filtering, you must redirect web traffic to the cloud service, and configure your firewall to allow access to the service on specific ports.

Traffic can be directed to the cloud service in a number of ways:

- A Forcepoint Endpoint: a lightweight software client that runs on end user devices, providing policy enforcement for web browsing.
- A browser PAC (proxy auto-config) file: a configuration script that can be configured in your users' browsers (via GPO or similar) to redirect browser requests to the service.
- Firewall redirection: a simple method implemented on your firewall to redirect all HTTP/HTTPS traffic to the service.
- Tunneling: IPsec or GRE connectivity to forward traffic to the service from a supported edge device.

Alternatively, a Forcepoint I Series appliance can be deployed in order to provide fast, flexible on-premises traffic analysis. If you have an existing on-premises proxy, this can be connected to the service via proxy chaining. For more information about forwarding traffic, see *Forwarding traffic*.

User synchronization

The service can identify and authenticate users in order to provide user and group-specific policy enforcement, and detailed user activity reporting. Users can be added manually, or identity management can be configured so that user details are automatically updated to the cloud service.

This step is optional; some organizations apply the same policies to all users based solely on IP address, without requiring users to authenticate.

Note

If your organization has roaming users (those who connect from locations outside of your network), those users must be registered and must identify themselves in order to use the service remotely. See *User registration methods*.

Policies

Policies allow or block access to web resources, and control your authentication, content filtering, security, and data loss prevention (DLP) settings. Exceptions can be configured to override or bypass policy settings per user or group.

Filtering is based on a set of web categories drawn from the Forcepoint URL Database, constantly updated by Forcepoint Security Labs, with security threats identified in real time by Forcepoint ThreatSeeker Intelligence.

A default policy is available, providing a set of standard web filtering settings. Once you are up and running with the service, you can edit this policy and create new ones, providing differing levels of access for different users and departments. (*See Tailoring your policies*.)

Related concepts
Forwarding traffic on page 11
User registration methods on page 15
Tailoring your policies on page 19

Getting started

This chapter covers logging on to the Forcepoint Cloud Security Gateway Portal, also referred to as the cloud portal, and getting started with Forcepoint Web Security Cloud.

Logging on to the cloud portal

1) Log on to the cloud portal: https://admin.forcepoint.net/portal

2) Enter your username and password and click **Log On**.

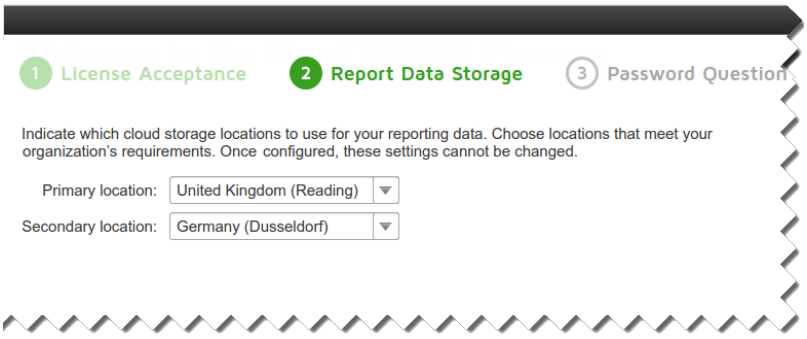
For the list of browsers supported for use with the cloud service, see the Cloud Security Browser Support Matrix in the Forcepoint Knowledge Base.

First-time logon

If you are logging on for the first time, a short first-time logon wizard will prompt you to:

1) Accept the license agreement for your product.

2) Select a primary and backup cloud data center for storing your reporting data.



Note

In most cases, the default data center locations should be used. These are chosen based on the location of your connection. They can be changed if your organization has localization or data sovereignty requirements.

3) Finally, provide an administrator email address and password recovery question that can be used to reset a lost password.

Once you have completed these steps, you are ready to configure your Forcepoint Web Security Cloud account.

Cloud Web setup

During the initial setup process, you need to configure your firewall to access Forcepoint Web Security Cloud, set up end-user registration and identity management, set up your first policy, and test your configuration. If you are not able to complete each step immediately, you can skip to the next step and complete any missed items later.

To begin, you will need to have:

- Your organization's external IP addresses.
- Knowledge of your organization's directory infrastructure or NTLM domains.

The stages of the setup are:

- *Step 1: Firewall Setup*
- *Step 2: End Users*
- *Step 3: Policy Setup*

Step 1: Firewall Setup

Your firewall must allow TCP connections outbound to Forcepoint data centers on specific ports. For details of the firewall ports required and how they are used, see Configuring your firewall to connect to the cloud service in the Web Security Cloud help.

Step 2: End Users

End user information can be sent to the cloud service in one of 2 ways:

- Use System for Cross-domain Identity Management (SCIM) (recommended) to provision user and group identity data from a cloud-based identity provider to the cloud service.
- **Synchronize users from my directory** (recommended when using a private Active Directory or LDAP) involves installing the Directory Synchronization Client in your network and configuring it to synchronize user and group information from your LDAP directory to the cloud service.
- Manually enter end user information (name, email address, and NTLM identity) to use in testing. User details are added to policies using the End Users tab options.

System for Cross-domain Identity Management (SCIM)

Your identity provider must be configured to work with the cloud service so that user and group data can be synchronized from the provider. See How the service works with SCIM in Cloud Security Help for more details.

Note

Okta and Microsoft Azure Active Directory are the only identity provided currently supported.

Directory Synchronization

To enable directory synchronization between your LDAP directory and the cloud service, start by creating the contact with Directory Synchronization permissions. The user name and password will be used by the Directory Synchronization Client to connect to the cloud service.

Refer to the Directory Synchronization Client Administrator's Guide for further information, including how to download and configure the client software.

Add Users manually

User accounts that you plan to use for testing can be added when a new policy is added. See the step for *Adding end users* when setting up a policy.

Related tasks
Step 3: Policy Setup on page 8

Step 3: Policy Setup

Use the **Web** > **Policy Management** > **Policies** page to create a basic policy to determine which websites can and cannot be accessed by users whose traffic is managed by the cloud service.

The steps below walk you through creating a very basic policy that you can customize later if necessary. See Defining Web Policies in Cloud Security Help for complete details.

1) Click **Add**.

2) Enter a policy name and administrator email address. This email address is used as the address from which system messages are sent.

3) Select a pre-defined policy template to use as the basis for your new policy:
   - **Default** blocks access to sites in commonly blocked categories, like Adult Material, Gambling, and sites that present a security risk, while permitting access to sites commonly used for business or educational purposes.
   - **Security only** blocks only sites that present a security risk (such as phishing related sites or sites that host malware) and permits access to all others.
   - **Monitor only** does not block any websites, but logs user activity for use in reporting.

4) Select a **Time zone** for this policy. This may be used both for time-based policy enforcement and reporting log records.

5) When you are finished, click **Save**.

Configuring policy connections

Select the **Connections** tab to identify the traffic originating from your organization that should be managed by the policy that you are creating.

Each connection is a public-facing IP address, range, or subnet for the gateway through which users' traffic reaches the Internet.

To get started, click **Add**, then:

1) Enter a unique **Name** and **Description** for the connection.

2) Select a connection **Type**: IP address, IP address range, or subnet.

3) Enter the connection definition for the type that you selected.

4) Optionally, select a **Time zone** for this connection. If no time zone is selected, the time zone defined for the policy as a whole is used.

5) Click **Continue**.

Repeat this process for each connection that you want to define for this policy.

Adding end users

The **End Users** tab is where all end-user registration configuration is performed. Registration is a method of getting user credentials into your cloud service account.

To get started with this new policy, select **Invite an end-user** in the User Management section.

1) In the **Name** field, enter the user's display name (for example, Jane Doe).

2) Enter the user's **Email address** (for example, jdoe@mydomain.com).

3) Enter the user's **NTLM identity** (for example, mydomain/jdoe).

4) Click **OK**.

Repeat this process as needed.

Directing user traffic to the cloud service

Use the **Default Pac file addresses** on the **Web** > **Settings** > **General** page to get the information you need to use a PAC file to direct user traffic from your browser to the cloud service.

Note

Forcepoint recommends performing initial testing using a PAC file manually configured in a browser. For details of other connectivity methods, see *Forwarding traffic*.

Perform the following steps on a machine that is inside the network that you defined as a connection in the previous step. (This may be the same machine that you are using to access the cloud portal.)

Configure Chrome to use a PAC file

1) Open Chrome on the selected machine.

2) Open the **Settings** menu.

3) Click the **Advanced Settings** link, then scroll down to the **Network** section.

4) Click **Change proxy settings**. This opens an Internet Explorer dialog box to the Connections tab.

5) Click **LAN Settings**.

6) Mark the **Use automatic configuration script** check box, then paste the URL from the portal page in the address field.

7) Click **OK** twice to close the dialog box.

Configure Internet Explorer to use a PAC file

1) Open Internet Explorer on the selected machine.

2) Open the **Internet options** menu.

3) Select the **Connections** tab, then click **LAN Settings**.

4) In the settings dialog box, mark the **Use automatic configuration script** check box and paste the URL from the portal page in the address field.

5) Click **OK** twice to close the dialog box.

Configure Firefox to use a PAC file

1) Open Firefox on the selected machine.

2) Open the **Options** menu.

3) Select the **Advanced** > **Network** tab.

4) Click **Settings**, in the **Connection** section at the top of the tab.

5) Select **Automatic proxy configuration URL** and paste in the URL from the portal page.

6) Click **OK**.

Note

We recommend that cookies are enabled in your browser to use the service. If cookies are not enabled, some features cannot work.

Related concepts

Forwarding traffic on page 11

Next steps

After completing the basic setup, you have all that is needed to test and begin deploying Forcepoint Web Security Cloud. Your account has a single policy that controls and secures your organization's web traffic, and traffic is directed to the service via your browser's PAC file configuration. By default, the service applies your policy settings to all traffic from the IP address defined in the policy.

To get the most out of the solution, you may wish to implement a different traffic forwarding method, enable end-user authentication, tailor your policies, and view and create reports. The rest of this document guides you through these more advanced topics as you continue to roll out your deployment. The remainder of the document is organized into the following topics:

- *Forwarding traffic*
- *Identifying users*
- *Next steps: configuring advanced features*

The appendix provides sample communications you can use to educate your users about your Forcepoint web protection solution (see *Preparing end users for deployment*).

Related concepts
Forwarding traffic on page 11
Identifying users on page 14
Next steps: configuring advanced features on page 19
Preparing end users for deployment on page 25

Forwarding traffic

In order for Forcepoint Web Security Cloud to filter your traffic, web requests must be redirected to the cloud service. There are a number of methods available to redirect traffic.

During the initial stages of an evaluation or while testing a deployment, we recommend that you manually configure a number of web browsers to use the Forcepoint Web Security Cloud PAC file to forward traffic to the service. This is described in *PAC file*.

The following table outlines all the traffic redirection methods available, which may be suitable for different organizations and different network environments.

Method	Summary	Recommended for
PAC file	The simplest method to direct browser traffic. Easily configured for a small number of browsers for testing purposes. Once you are happy that the service works as expected, you can deploy the PAC file to more users, via Windows GPO or similar. Further detail is given below (see *PAC file*).	Initial setup and testing. Organizations where software cannot be installed on end user devices or other types of connectivity cannot be used.
Endpoint client	A lightweight software application installed on end-user devices. The endpoint client seamlessly authenticates users, and provides policy enforcement for web browsing. Further detail is given below (see *Endpoint*).	Most scenarios where software can be installed on end user devices.
Firewall redirection	Transparently redirect all web traffic by configuring redirection rules on your firewall. For details on this connectivity method, see Firewall Redirect: Forwarding Traffic to the Cloud Service.	Networks with unmanaged devices, such as a guest Wi-Fi network or BYOD networks.

Method	Summary	Recommended for
IPsec tunneling	Securely forward traffic over a virtual private network (VPN) using a supported firewall or router. For details on this connectivity method, see the Forcepoint IPsec Guide.	Networks with unmanaged devices, such as guest Wi-Fi networks or BYOD networks. Organizations that require increased security for web traffic.
GRE tunneling	Forward traffic over a GRE tunnel using a supported firewall or router. For details on this connectivity method, see the Forcepoint GRE Guide.	Networks with unmanaged devices, such as guest Wi-Fi networks or BYOD networks.
I Series appliance	Forcepoint appliance that performs fast on-premises URL analysis and application/protocol detection for web traffic, forwarding traffic to the cloud proxy where required. See Deploying an I Series Appliance on the Forcepoint Support site for more details.	Organizations that require on-premises traffic filtering and analysis.
Proxy chaining	Configure your existing on-premises proxy to forward traffic to the cloud service. See Configuring proxy chaining with the Forcepoint cloud service on the Forcepoint Support site for more details.	Organizations with an existing on-premises proxy where existing network infrastructure cannot be changed.

PAC file

A proxy auto-configuration (PAC) file defines how web browsers choose an appropriate proxy for fetching a given URL. The Forcepoint Web Security Cloud PAC file contains a number of global settings and includes any exclusions you add (for example, intranet sites) that should not use the cloud proxy.

All supported browsers have the ability to use PAC files. PAC files can be configured manually, or delivered via Windows GPO, or similar.

When configuring browsers to download the PAC file, you can specify either the standard PAC file URL or a policy-specific PAC file URL.

- Standard PAC file URL: if a user's browser requests the standard PAC file URL from a known IP address associated with a policy, the user will be served the policy-specific PAC file. If the standard PAC file is requested from an unknown IP (for example, roaming users), a global PAC file will be delivered.

  Example standard PAC file URL (HTTPS):

  ```
  https://pac.webdefence.global.blackspider.com:8087/proxy.pac
  ```

- Policy-specific PAC file URL: if a user's browser requests a policy-specific PAC file URL, then this policy-specific PAC file will always be served. This can be used to ensure that users always receive their policy-specific PAC file, even when connecting from unknown IP addresses, such as roaming users.

Example policy-specific PAC file URL (HTTPS):

```
https://pac.webdefence.global.blackspider.com:8087/proxy.pac?p=xxxxxx
```

(Where xxxxxx is a unique policy identifier.)

For more information on PAC files, see Proxy auto-configuration (PAC) in the Web Security Cloud help.

Endpoint

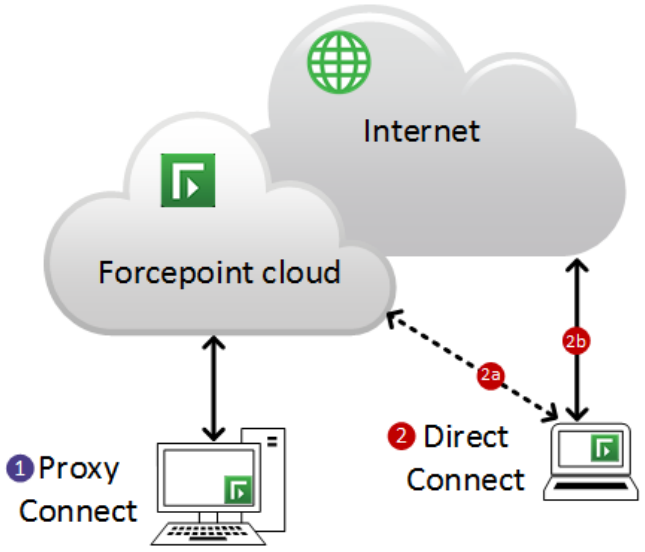
Forcepoint Endpoint clients run in the background on end user devices, providing a seamless browsing experience. Endpoint automatically authenticates users with the service, and provides policy enforcement and data security features. The endpoint client has been designed to consume minimal CPU, memory, and disk resources, and has tamper controls to prevent users disabling the software.

The endpoint client allows administrators to create policies that provide user-specific policy enforcement, with seamless authentication, full visibility of inbound and outbound traffic, and that don't restrict use of the device.

There are three versions of the endpoint client, each suited to different sets of end user needs:

- **Neo**: this endpoint client can be used in either proxy connect mode or direct connect mode, and can automatically switch from one to the other when necessary.
- **Proxy Connect**: also known as Classic Proxy Connect endpoint, this endpoint client redirects all traffic to the cloud proxy for analysis. Proxy Connect is recommended for most scenarios, and supports the widest set of security features.
- **Direct Connect**: also known as Classic Direct Connect endpoint, this endpoint client contacts the cloud service for each request to determine whether to block or permit a website, but routes the web traffic itself directly to the Internet. Direct Connect also routes traffic to the cloud service to perform content analysis, if configured in your policy. Direct Connect is recommended for scenarios in which proxy connections may be problematic, and in some circumstances can improve content localization.

The following diagram illustrates the connectivity for Proxy Connect (through Neo or the Classic Proxy Connect endpoint) and Direct Connect (through Neo or the Cassic Direct Connect endpoint).



The diagram shows the two different endpoint versions servicing a web request:

1) In the first scenario, Neo or the Classic Proxy Connect endpoint directs all web traffic via the cloud proxy. If the request is permitted, the proxy connects to the requested website and sends content back to the end-user client. (If the request is blocked, the user is shown a block page.)

2) In the second scenario, a web request via Neo or the Classic Direct Connect endpoint consists of two stages:

   a) The endpoint connects to the cloud service to look up the user's policy settings for the requested site.

   b) If the request is permitted, the client then redirects the request directly to the Internet. (If the request is blocked, the user is redirected to a block page.)

If required, you can deploy a combination of Proxy Connect and Direct Connect endpoints in your organization. However, only one classic endpoint instance (Classic Proxy Connect or Classic Directory Connect) can be installed on a client machine at any one time. The Neo endpoint agent includes both proxy connect and direct connect modes.

For more information about Forcepoint Endpoint software, including deployment options and configuration settings, see Web endpoint overview in the Web Security Cloud help.

Identifying users

Once you have completed the initial setup, a single policy applies enforcement to all traffic from your organization's egress IP. In order to implement per-user or per-group policy enforcement, Forcepoint Web Security Cloud must identify specific users. User identification also allows the service to log individuals' internet usage and provide user-based and group-based reporting.

This section discusses the options available for registering users with the service and identifying users when they access the proxy.

Policy selection by IP address

When the cloud service receives a web request, it first identifies the source of the request in order to find the user's account. If the request comes from an IP address that is defined as a connection in a policy, the service identifies the account, and, by default, applies the settings in that policy.

If you wish, you can define additional policies with different connection addresses, which can apply enforcement to different parts of your organization (as identified by egress IP). This is an easy way to apply different policy settings to different geographical offices, or network segments.

Tip

Using IP-based policy selection also allows users to browse anonymously, without having to authenticate. If user authentication is not required by the policy, enforcement actions are applied to all traffic coming from the egress IP, but users are not individually identified, and user-specific reporting data will not be available.

User authentication is always required for roaming users (those connecting from an unknown IP address), in order to identify the user's account and ensure that the user is entitled to access the service. Add IP addresses to your policies in the cloud portal via **Web** > **Policy Management** > **Policies**, using the **Connections** tab.

Policy selection by user

In order to implement user- or group-level control of your organization's web browsing, the service must be able to identify specific users when they request a web resource.

The process by which this occurs is as follows:

1) When a web request is received from an IP address that is defined as a proxied connection in a policy, the service first identifies the account and policy using the source IP address, and by default applies this connection-based policy. (For connections from unknown IP addresses, see *Working with remote users, page 23*.)

2) If the connection-based policy requires authentication (defined on the **Access Control** tab), the service will then identify the user.

3) Once identified, if the user is found to be assigned to a different policy, the user's policy overrides the connection-based policy, and settings from the user's own policy are enforced.

In order for this to occur, users must be registered with the service, and user authentication must be configured in your policy. See the sections that follow:

- *User registration methods*
- *User authentication methods*

Related concepts

Working with remote users on page 17
User registration methods on page 15
User authentication methods on page 17

User registration methods

You can register users with the service, and assign those users to policies, in a number of ways. User registration methods are as follows:

- Identity management
- By invitation
- Self-registration

Identity management

Registering your users via identity management is the most flexible and scalable option for user management.

We recommend that your synchronization includes:

- (Directory Synchronization) Users' NTLM IDs: these can be used to transparently identify users without the need for users to manually log on. (Note: if NTLM IDs are not included in the synchronization, users must perform a one-time self registration process when they first connect to the cloud service.)
- Groups that will be useful for policy enforcement purposes - for example, if members of different departments will have different policy settings. You can configure the cloud service to assign users to policies based on group membership, allowing you to manage policy assignment via your directory. You can also configure policy exceptions based on group membership.

Note

Forcepoint recommends that you include the minimum number of groups required for policy enforcement. Including more groups than necessary can impact performance.

For advice on configuring identity management, see Planning for your first synchronization in the Web Security Cloud help.

Once you have synchronized your users and groups, assign groups to the relevant policy via the **End Users** tab of the policy.

Registering by invitation

If you cannot use identity management, you can invite users to register via an option on the **End Users** tab of a policy. Users can be invited individually by email address, or in bulk via a CSV file. This option may be useful for users on your network who do not appear in your directory, such as third-party contractors.

When end users are invited, an email is sent inviting the user to create a password before using the service. Users are added to the policy after completing registration.

For further information, see Registering by invitation in the Web Security Cloud help.

Self registration

You can add email domains to your policies in order to allow users to self-register with the service using their email address. For example, if your users have email addresses in the form 'user@yourcompany.com', add 'yourcompany.com'. Add domains on the **End Users** tab of your policy, under Self Registration. Users registering using an email address at this domain will be assigned to the policy.

Domains can also be added at the account level, via **Web** > **Settings** > **Domains**. This allows you to associate the domain with all policies, allowing users to self-register to any policy in your account. The actual policy the user is assigned depends on the connection from which they connect - if this matches a proxied connection in a policy, the user is registered to that policy. Users connecting from unknown IP addresses are added to a default policy you can select. (See Configure Domain settings in the Web Security Cloud help.)

Users can self-register by clicking Register on the default logon page shown when they first attempt to browse, or by navigating directly to the self-registration URL:

```
http://www.mailcontrol.com/enduser/reg/index.mhtml
```

For further information, see End user self-registration in the Web Security Cloud help.

Managing user policy assignment

If you are using identity management, assign groups to the relevant policy via the **End Users** tab of the policy. Under **Identity Management**, click **Modify list of groups**, and select the groups that should be assigned to the policy.

User assignment to policies can be overridden per user by editing the user via the **Accounts** > **End Users** page.

You can also add users to policies using a CSV file. Navigate to **Web** > **Policies**. Upload a file under Policy Assignment.

Managing policy assignment via your directory

If you are using identity management you can manage user policy assignment entirely using your identity provider or LDAP directory. Once you have synchronized your users, assign groups to your policies as required.

On the **Account** > **Identity Management** screen, click **Edit**. For the User policy assignment setting, ensure **Follow group membership** is selected.

With this setting applied, moving users to a different group will automatically update their policy assignment in the portal.

User authentication methods

You can enable various methods to identify and authenticate users. User authentication is used if it is required by your policy, or if the user is accessing a website for which a policy exception is configured. Authentication is always required for roaming users connecting from an unknown IP address.

Tip

User authentication allows policy enforcement actions and policy exceptions to be applied to individual users or groups, as well as user-specific reporting data to be logged.

User authentication settings are configured on the **Access Control** tab of a policy. Authentication methods are listed below, in the order in which they are used by the service, if enabled in a policy.

- Forcepoint Web Security Endpoint: always used to identify the user, if installed on an end-user's machine.
- Single sign-on: if you have configured a supported third-party identity provider to authenticate your users, this provider is queried to identify and authenticate the user.
- NTLM identification: identifies users connecting from a known IP address via their NTLM credentials. (NTLM is not used for roaming users.)
- Secure form: if the user agent supports secure forms, users can enter their logon credentials if already registered, or choose to register with the service.
- Basic authentication: a user logon page is shown by default if the above options are not available. Users can enter their logon credentials if already registered, or choose to register with the service. Use the Welcome page setting to display a configurable welcome page before users are presented with the authentication dialog box.

Note

Basic authentication uses the HTTP authentication standard. While this is available as a default fall-back, Forcepoint recommends that you do not rely on this option, and enable at least one of the other authentication options.

Note

For secure form-based authentication and single sign-on, an authentication cookie is placed on the user's machine. Users do not need to re-authenticate for subsequent web browsing sessions, for a period of time defined by the Session Timeout option on the **Access Control** tab. For basic authentication, users are asked to authenticate whenever opening a new browser session.

Working with remote users

Forcepoint Web Security Cloud can protect and monitor users even when they are not in their typical office location, such as when working from home, connecting from a public access point, or using a third-party network. This section describes how Forcepoint Web Security Cloud handles roaming users connecting from a location other than their network domain.

When the cloud service receives a URL request, it first checks the source IP address of the request and searches all customer policies for a matching address. (The source IP address is configured as a connection in a policy's **Connections** tab in the cloud portal.) For roaming users, no match will be found. In this situation, the roaming user encounters one of the following scenarios:

- If the user's device has Neo, Classic Proxy Connect endpoint, or Classic Direct Connect endpoint installed, the endpoint client sends account and user information, allowing the service to identify the user seamlessly.
- If you have deployed single sign-on for your users, the roaming user is first asked to enter an email address, in order to identify the user's account, and is then authenticated by the identity provider. (Users are typically only required to enter an email address once; following a successful authentication, a long-lived cookie is set, allowing the service to recognize the user's account.)
- If neither Forcepoint Web Security Endpoint nor single sign-on is in use, and the service cannot find the source IP address in a policy, it responds with a logon page that states: "You are connecting from an unrecognized location." The user has to log on with their cloud service details. The service then searches for the user in its policies. When it finds the user, the appropriate policy settings are applied.
  In order to log on, the user has to be registered. If they have not already set a password to access the service, roaming users can go through a one-time self- registration process. See *User registration methods, page 20*.

Note

Some browsers can exhibit inconsistent behavior in certain circumstances, such as when used in public Internet access points in hotels and airports. For more information on configuring and troubleshooting access for roaming users, see Using cloud web protection from public Internet access points on the Forcepoint Support website.

Recommendations for remote users

The simplest solution for remote users is to install Neo, Classic Proxy Connect endpoint, or Classic Direct Connect endpoint on the client machine. Installing the endpoint client, either for roaming users or all users, ensures all web traffic receives policy enforcement from the cloud service, and users are authenticated seamlessly. When the endpoint client cannot connect to the cloud service, it allows Internet use to continue, applying filters that have been cached to provide as much protection as possible (known as Fallback mode).

For cases where the endpoint client cannot be installed:

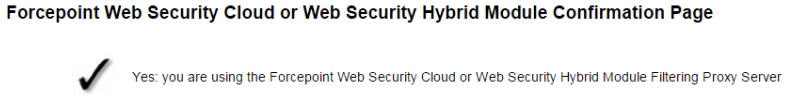
- Ensure that roaming users have a PAC file configured in their browser in order to direct web requests to the service. See Configuring browsers for a proxy service on the Forcepoint Support site for instructions.
- Use the **Alternate PAC file address** given on the **Web** > **Settings** > **General** page (or the policy-specific PAC file URL displayed on the **General** tab of your policy. This accesses the PAC file over port 80/443, which can address some issues with using the service from public networks.

For guidance on resolving specific issues that can arise for roaming users without an endpoint client installed, see How the service works for roaming users on the Forcepoint Support site.

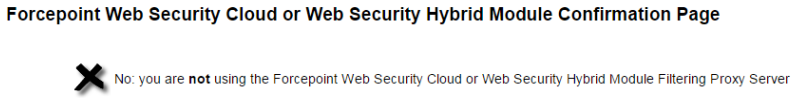
Testing whether a browser is using the proxy

A tool is available to help identify whether a browser has a proxied connection to Forcepoint Web Security Cloud. Find the **Proxy query page** link on the **Web** > **Settings** > **General** page in the cloud portal.

When you request the query page from a browser whose requests are routed through the Forcepoint Web Security Cloud proxy, it looks like this:



If you are not using the Forcepoint Web Security Cloud proxy (for example, you have lost your proxy connection or you are using Neo in direct connect mode or the Classic Direct Connect endpoint), it looks like this:



Next steps: configuring advanced features

Forcepoint Web Security Cloud includes many advanced features that allow you to configure your web protection product to meet the needs of your organization. This section covers some of the next steps you can take to help you get the most out of the service.

- *Tailoring your policies*
- *Customizing notification pages*
- *Adding non-proxied destinations*
- *Adding administrators*
- *Privacy protection*
- *Cloud service reporting*
- *Optional add-on modules*

Configuration advice for all of these features can be found in the Forcepoint Web Security Cloud Help. Some basic steps for configuring the service are outlined in the sections that follow.

Tailoring your policies

The default policy you configured using the initial setup applies a standard set of enforcement actions to all users in your organization. (For reference, the standard default web configuration is summarized in the topic Standard Web Configuration in the Web Security Cloud help.)

Forcepoint Web Security Cloud also allows you to create more granular policy configuration on an IP address, user or group basis. For example, specific users or departments may be permitted to access particular web resources, or you may define times of day when certain resources are restricted or permitted for some users. For data security, some users may be permitted to share sensitive information, while it is restricted for others.

There are a number of ways to make your web policies more granular:

- Create different policies to control traffic from different egress IP addresses that you manage (for example, different branch locations).
- Assign users and groups to specific policies, allowing you to create separate policies for different departments. By default, user and group policy assignment overrides connection-specific policy assignment.
- Create category exceptions for specific users and groups, defining override settings for some users within the policy.

The approach you take depends on the scale and complexity of your setup. You may deploy a combination of the above methods.

Tip

As a best practice, Forcepoint recommends that you keep the number of policies to the minimum necessary to provide granular protection across your organization. This helps to lower the administration overhead when making changes across multiple policies.

Web category filtering

Forcepoint Web Security Cloud includes over 95 website categories, designed to help you apply policy filtering to your organization's web traffic. Website classifications are drawn from the Forcepoint URL Database, the industry's most accurate, current, and comprehensive classification of URLs. Website classifications are updated according to automated threat monitoring from Forcepoint Threatseeker Intelligence, research by Forcepoint Security Labs, and intelligence from customer feedback.

In addition to standard categories, you can create your own custom categories in order to classify specific websites. Use the **Policy Management** > **Custom Categories** page to define your own categories.

Click the **Web Categories** tab in a policy to configure the action you want to take when users try to access websites in each of the categories.

In the standard categories section, child categories are indented under their parent categories. Parent categories allow specific categories to be grouped by a more generic description. You can set an action for a parent category without it affecting the child category, or apply the action to all sub-categories.

The following actions can be applied to your categories:

- **Allow access** means that any website within the category is always accessible, regardless of whether it exists in another category that has the **Block access** action.

  Note

  Websites blocked by a security category override this action, and are always blocked.

- **Do not block** ensures that the site is not blocked under this rule, but if it also exists in another category that has an action of **Block access**, it is blocked under that category.
- **Confirm** means that users receive a block page, asking them to confirm that the site is being accessed for business purposes. Clicking **Continue** enables the user to view the site, and starts a timer. During a configurable time period (10 minutes by default), the user can visit any site that requires confirmation without receiving another block page. Once the time period ends, browsing to these sites requires the user to click Confirm again.
- **Use Quota** means that users receive a block page, asking them whether to use quota time to view the site. If users click **Use Quota Time**, they can view the site for a configurable period.
  Clicking **Use Quota Time** starts two timers: a quota session timer and a total quota allocation timer. The session length and total quota time available for each category depend on the options selected on the **General** tab.
- **Block access** blocks access to websites in this category unless they exist in another category with the **Allow access** action. When a site is blocked, you can choose a notification page to be displayed.

For more information, see Web Categories tab in the Web Security Cloud help.

Category exceptions

Exceptions allow the default action for a web category to be overridden for specified users and groups of users, and for defined time periods. For example, you can allow users to access certain categories outside of working hours, or apply a time quota between certain hours.

Define exceptions for a policy under **Category Exceptions** on the **Web Categories** tab. You can click a category to view the exception rules that apply to it.

Click **Add** to add a new exception.

Tip

Category exceptions are an easy way to apply more granular policy configuration for specific users and groups, without creating different policies.

For more information, see Exceptions in the Web Security Cloud help.

Testing filtering actions

To test how the proxy filters a specific website, use the Filtering Test feature on the **Web** > **Policies** page.

This feature can be used to test a specific URL for a named user, for traffic from your current IP address, an unknown IP address, or a specific IP address.

Enable file blocking

In addition to category-based web filtering, Forcepoint Web Security Cloud allows you to block users from accessing specific file types. File types can be blocked based on extension, or based on true file type. True file type blocking scans the file itself to determine its format, regardless of its extension.

File blocking can be configured per web category, or per user and group. For example, you can enable the Sports category, but prevent users from downloading multimedia files from sites in that category.

Important

Archived/compressed files are not extracted to determine if the contents contain a file that should be blocked based on the type or extension. However, they are inspected for malware. Archived and compressed files can be blocked, if needed, in which case, all files contained in those archived files are blocked.

Configure file blocking via the **File Blocking** tab of your policy. For more information, see File Blocking tab in the Web Security Cloud help.

Enable data security features

Use the Data Security tab to monitor and prevent the loss of sensitive data and intellectual property via the web. You can protect intellectual property, data that is protected by national legislation or industry regulation, and data suspected to be stolen by malware or malicious activities.

The service has a default set of content classifiers that can identify data types that are important for regulatory compliance, and you can create custom content classifiers that are used to identify intellectual property and other protected data types important for your organization. Once defined, these classifiers can be used to identify and filter traffic that may constitute attempted data theft. This traffic can be blocked, or monitored for reporting purposes. Configure content classifiers via **Web** > **Content Classifiers**. Configure data security settings in your policies using the **Data Security** tab.

For more information on getting started with this feature, see Data Loss Prevention in Forcepoint Web Security Cloud on the Forcepoint Support site.

ACE security scanning

The Forcepoint Advanced Classification Engine (ACE) identifies and classifies security threats such as malware, viruses, and compromised websites, in real time before they can enter your network. ACE is built into Forcepoint Web Security Cloud, and enabled by default with a standard set of scanning options. You can adjust your level of protection by selecting the types of sites, files, and applications whose content is analyzed, and defining exceptions for trusted hostnames.

View and edit your ACE settings via the **Web Content & Security** tab of your policy. For more information, see Web Content & Security tab in the Web Security Cloud help.

Customizing notification pages

When a policy denies access to a resource or needs to inform the user of an event, it serves a block or notification page, with a message informing the user of the action it has taken. Forcepoint Web Security Cloud comes with a standard set of notification pages covering all scenarios.

Notification pages are provided as editable templates. You can modify these to suit your needs, or add your own pages. You can then configure your policies to use your custom notification pages for a given action.

You can also create multiple language versions of your notification pages that will be displayed to a multi-national user base. The most appropriate language page is displayed based on the user's browser language settings.

Configure block and notification pages via **Web** > **Block & Notification** Pages. For more information, see Configure block and notification pages in the Web Security Cloud help.

Adding non-proxied destinations

You can define destinations that will bypass the cloud service, and that users will be able to access directly. Bypass destinations can be added per policy, or at the account level, applying to all policies.

Sites that you should add as bypass destinations can include, for example:

- Trusted services, such as organizational webmail.
- Antivirus update servers.
- Internal destinations that are not accessible to the cloud service.

Note

The cloud service PAC file bypasses private address blocks by default.

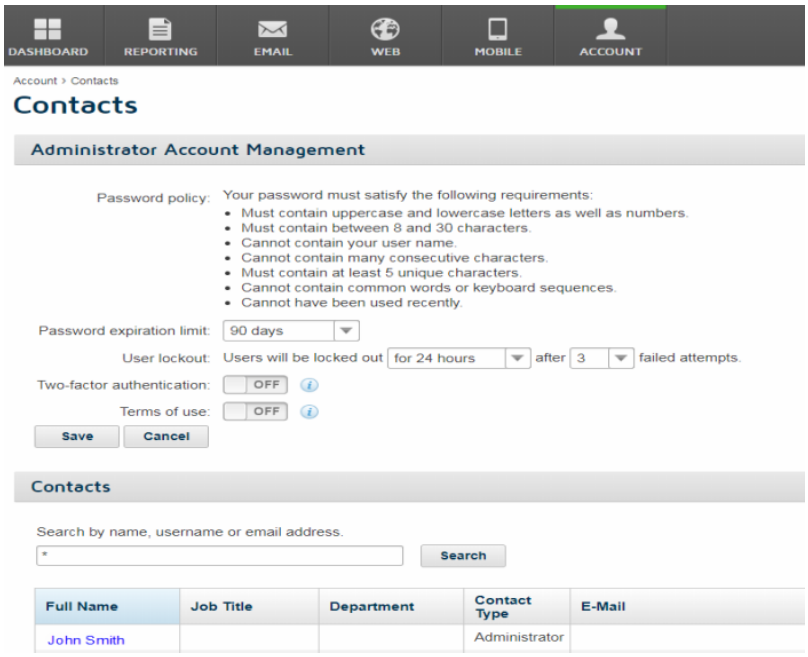
To add a bypass destination to a policy, navigate to **Web** > **Policies** > **[policy name]** > **Connections** tab. Add bypass destinations under **Proxy Bypass**. See Connections tab in the Web Security Cloud help.

To add a bypass destination that applies to all policies, navigate to **Web** > **Bypass Settings** > **Proxy Bypass** tab. See Adding and importing sites that bypass the proxy in the Web Security Cloud help.

Adding administrators

To add additional administrators, go to the **Account** > **Contacts** page. Your administrator contacts can be given a portal login, and permissions to manage certain features, as well as policy-level permissions, allowing them to view or modify settings for particular policies.

This allows you to delegate responsibility for administration to particular departments.



Best practices for administrator access

As a best practice, set the administrator's initial password to a randomly generated string that meets the minimum password requirements, and require that the password is changed when the administrator first logs on, using the **Change password next log on option**.

Configure password policy settings for your account that require passwords to expire automatically after a set number of days, and that lock users out after a number of incorrect login attempts.

Tip

For further security, enable two-factor authentication, requiring the administrator to use a supported authenticator app (such as Google Authenticator) to access the portal. See Two-factor authentication in the Web Security Cloud help.

For more information on securing administrator access, see Adding a contact in the Web Security Cloud help.

Privacy protection

The cloud portal provides options to prevent end-user identifying information and data security incident trigger values from appearing in logs and reports. If required, you can collect this information for security threats, even when it is not collected for other web traffic.

Review and configure privacy options on the **Account** > **Privacy Protection** page in the cloud portal. Here, you can anonymize selected end user attributes for all policies, or specific policies, and define whether data security incident triggers are stored and displayed in reports.

Cloud service reporting

The available reports for web traffic and analysis are located in the navigation pane under **Reporting**.

The **Report Catalog** contains a number of predefined reports that cover common scenarios, available in bar chart, trend chart, and table formats. You can copy any predefined report to apply your own filters to create a custom report, and share your reports with other administrators. Custom reports appear in the Report Catalog in a folder called “My Reports”.

The **Report Builder** offers an enhanced model for creating multi-level, flexible reports that allow you to analyze information from different perspectives and gain insight into your organization’s Internet usage. If a high-level summary shows areas of potential concern, you can drill down to find more details and use **Transaction Viewer** for granular reports on individual transactions.

You can also do the following:

- Download report results as a comma-separated values (CSV) file or as a PDF file.
- Save the reports you generate most frequently and want to be able to locate quickly.
- Schedule one or more saved reports for regular delivery.

For more information about reporting and the full list of available reports, see Report Center in Web Security Cloud help.

Optional add-on modules

The following optional licenses are available as add-on modules for Web Security Cloud.

Module	Description
Advanced Malware Detection for Web	Advanced cloud-hosted file sandboxing capabilities, providing detailed analysis of suspicious files. See the Advanced Malware Detection product page on the Forcepoint website.
Cloud App Control	Integration with Forcepoint CASB, providing granular control and protection of the cloud apps used in your organization. See the Forcepoint Cloud Security Gateway Integration Guide on the Support site.
Web Data Retention	The base reporting data retention period is 90 days. Extended data retention is available, to extend this to a total duration of: - 6 months - 12 months - 18 months

Please contact your account manager for further information about purchasing these modules.

Preparing end users for deployment

Before deploying Forcepoint Web Security Cloud, you should inform your users what the service does and how it impacts them. This may be a legal requirement in some countries. Below is some sample text that you can use as a model for an initial communication. You can also customize the registration email templates and pre-logon welcome page, if you are going to use them.

Introduction to the Forcepoint Web Security Cloud service

Forcepoint Web Security Cloud is an advanced web protection service that we have deployed to protect Internet users from computer viruses and other webbased threats such as spyware. All of our Internet traffic is directed to data centers where these threats are filtered out and our Internet acceptable use policy is enforced.

Many websites contain viruses or inappropriate and potentially offensive content. Links to these sites may show up in search results, and the type of content may not be obvious until it is too late. Forcepoint Web Security Cloud allows us to block these sites.

Internet acceptable use policy

We have published an Internet acceptable use policy that outlines your responsibilities as an individual when using company resources to access the Internet. Forcepoint Web Security Cloud allows us to enforce this policy, report on web usage, and block inappropriate downloads. In the event that a website is blocked, you are presented with a page explaining why.

We recognize that different people need to access different types of websites to perform their jobs, so if sites that you are trying to access are being blocked, please email XXXX, include the website address and the reason why you need to access it. The full website address can be copied from your browser address bar.

Note

For information about acceptable use policy notices, see Notification pages in the cloud portal Help. This feature is not available for I Series appliance deployments.

End-users who must self-register to connect to the Internet through the cloud service should have the following instructions:

Registering to use Forcepoint Web Security Cloud

To use the Forcepoint Web Security Cloud service, you first need to complete a simple, one-time registration process:

If not using bulk registration

1) Click the link below. It takes you to the end-user registration portal.

```
https://www.mailcontrol.com/enduser/reg/index.mhtml
```

2) Enter your name and email address and click **Submit**.

3) When you receive an email from Forcepoint, click the link it contains.

If using bulk registration

You will receive an email containing a link that you should click.

If using basic authentication:

This takes you to the end-user registration portal. Enter the password that you want to use when you access the web (twice), and click **Submit**.

Registration is now complete, and you are not required to register again. To check that you are correctly registered, shut down all browsers and open a new one. When you try and access a website, you are first asked to log in. Type the email address and password that you used to register with Forcepoint Web Security Cloud and click **OK**. You may want to check the box that invites you to save these login details to simplify future logins.

If using NTLM transparent identification without directory synchronization:

This takes you to the end-user registration portal. Enter the password that you want to use when you access the web (twice), and click **Submit**.

Now enter a URL, such as www.forcepoint.com, into your browser address bar and you are presented with the final registration page.

Type the email address and password that you used to register with Forcepoint Web Security Cloud into the appropriate boxes.

If using basic authentication:

Logging in when you access the web

You need to log in every time you open a new browser to access the Internet. If you leave your browser open, you are not required to log in again. If you need a second browser window, do not launch a new browser. In your existing one, click **File** > **New Window**. This opens a new browser session without you having to login again.

For remote users who use Forcepoint Web Security Cloud with basic authentication when working remotely:

Accessing the Internet when you are not in the office

When you are working in the office, Forcepoint Web Security Cloud is able to recognize that you work for COMPANY NAME and can protect you from Internet threats according to our policy. To ensure that you are still protected when you are not working from the office, when you access the Internet, you are asked to log in. You must use the email address and password that you entered during Forcepoint Web Security Cloud registration before you can continue.

Published 12 August 2024