Managing Forcepoint Web Security Cloud

Managing Forcepoint Web Security Cloud

This guide includes the following troubleshooting and management articles for Forcepoint Web Security Cloud:

- *Configuring browsers for a proxy service*
- *How the service works for roaming users*
- *Resetting the company master user portal account*

Configuring browsers for a proxy service

Configuring browsers for a proxy service | Forcepoint Web Security Cloud

Overview

This article describes how to configure various browsers for a proxy service.

- For browsers on Windows operating systems, see:
  - *Internet Explorer*, page 2
  - *Google Chrome*, page 2
  - *Firefox*, page 3
- For browsers on Mac OS X, see:
  - *Firefox*, page 3
  - *Safari*, page 3

Windows browser configuration

Internet Explorer

1. Go to **Tools** > **Internet Options**.
2. Select the Connections tab.
3. Click **LAN settings**.
4. Select **Use automatic configuration script**.
5. Make sure the field next to it contains the PAC file address relevant to your configuration. For example:

   http://webdefence.global.blackspider.com:8082/proxy.pac.
6. Click **OK** and then **OK** again.

Google Chrome

1. Click on the three lines in the top right and select Settings from the drop-down menu.
2. Click **Show advanced settings** (at the bottom of the page).
3. Under Network, click **Change proxy settings**.
4. Click **LAN settings**.
5. Select **Use automatic configuration script**.
6. Make sure the field next to it contains the PAC file address relevant to your configuration. For example:

http://webdefence.global.blackspider.com:8082/proxy.pac.

7. Click **OK** and then **OK** again.

Firefox

1. Go to **Tools** > **Options**. (In the latest version, click on the three lines in the top right and select **Options** from the drop-down menu).
2. Select the Advanced icon in the top menu.
3. Select the Network tab.
4. Click **Settings**.
5. Select **Automatic proxy configuration URL**.
6. Replace the contents of the field below with the PAC file address relevant to your configuration. For example:

   http://webdefence.global.blackspider.com:8082/proxy.pac.
7. Click **OK** and then **OK** again.

Mac OS X browser configuration

Firefox

1. Go to **Preferences**. (In the latest version, click on the three lines in the top right and select **Preferences** from the drop-down.)
2. Select the Advanced icon in the top menu.
3. Select the Network tab.
4. Click **Settings**.
5. Select **Automatic proxy configuration URL**.
6. Replace the contents of the field below with the PAC file address relevant to your configuration. For example:

   http://webdefence.global.blackspider.com:8082/proxy.pac.
7. Click **OK**.
8. Close the Preferences window.

Safari

1. Pull down the Safari menu and select **Preferences**.
2. Click **Advanced**.
3. Under Proxies, click **Change Settings**.
4. For Mac OS 10.5 and under:
   a. For the Configure Proxies option, select **Using a PAC file**.

    b. In the PAC file URL field, enter the PAC file address relevant to your configuration. For example:

    http://webdefence.global.blackspider.com:8082/proxy.pac.

    c. Click **Apply Now**.

5. For Mac OS 10.6 and higher:

    a. Under Select a protocol to configure, select **Automatic Proxy Configuration**.

    b. In the Proxy Configuration File URL field, enter the PAC file address relevant to your configuration. For example:

    http://webdefence.global.blackspider.com:8082/proxy.pac.

    c. Click **OK**.

6. Close and restart Safari.

How the service works for roaming users

How the service works for roaming users | Forcepoint Web Security Cloud

This article describes how the cloud service handles users who are roaming – that is, users accessing the Internet away from your network. Typically, this applies to users who are traveling or working at another location, and connecting their company laptop to a Wi-Fi network belonging to another organization, such as a hotel, a home network, or another business.

Directing traffic to the cloud service

In order for a roaming user to connect to the cloud service, they must either have Forcepoint Web Security Endpoint installed, or a proxy auto-configuration (PAC) file setting configured in their browser.

If the user has the endpoint client installed, this forces a connection to the cloud service to authenticate the user and apply policy settings appropriate for the user.

PAC files direct browser traffic to the cloud service, and are typically deployed to end user machines via a Windows Group Policy Object (GPO) or similar. Settings for end users are usually locked down so that they cannot be changed. For more information on PAC files, see Proxy auto-configuration (PAC) in the Forcepoint Web Security Cloud help.

A roaming user's ability to connect to the service may depend on any firewall restrictions that may be in place on their network, and the LAN settings configured in the roaming user's browser. By default, the cloud service uses port 8082 or 8087 to retrieve PAC files. In some networks, these ports may be locked down, which can cause problems for roaming users.

You can avoid the potential limitation with using port 8082/8087 by deploying the alternate PAC file address for roaming users. The alternate address connects via port 80 or 443, the standard ports for web browsing. See the **Settings > General** page in the cloud portal for more details.

Identifying roaming users

When the cloud service receives a web request, it attempts to recognize the user's account and policy. If the endpoint client is installed, this automatically identifies the user to the service.

When a PAC file is being used, the service attempts to identify the user based on the source IP address of the request. The service first attempts to match the source IP address to a policy. (The source IP address is configured as a proxied connection in the Connections tab of the cloud portal. See the Defining Web Policies > Connections tab in the Forcepoint Web Security Cloud help.)

When users are roaming (working at home, at another business premises, or in a public location such as a hotel or an airport), the IP address is unlikely to be configured as a proxied connection in any account. In this case, the roaming user encounters one of the following scenarios:

- If you have deployed single sign-on for your account, upon first connecting, the roaming user must enter their email address. Once the user's account is identified, the service authenticates the user via the identity provider configured for the account. (A long-lived cookie is set, allowing the user to be authenticated seamlessly for subsequent sessions.)
- If neither the endpoint nor single sign-on is in use and the service cannot find the source IP address in any policy, then 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 cloud service then searches for the user in your policies. When it finds the user, the service knows who they are, which policy they are assigned, and consequently how to filter the request.

In order to log on, the user has to be registered. Roaming users must go through a one-time registration process before they can log on and browse.

For more information on setting up end user registration, see Defining Web Policies > End Users tab in the Forceoint Web Security Cloud help.

Common issues for roaming users

Registration problems

If you are having trouble registering with the cloud service, check the following:

- Are you typing in your name in the **Name** field and your email address in the **Email Address** field?
- Is your email address in a domain that is recognized by the company policy?

Logon problems

If you get an authentication error when you try to log on and browse, one of the following may be the issue:

- Have you registered with the cloud service? Unless you are part of an LDAP directory that is being synchronized with the cloud service, you must register with the service before gaining access to the web. Check with your system administrator if you are not sure how to register.
- Are you typing in your email address rather than your user name in the logon dialog box?
- Have you remembered your password correctly?

Remember that you register separately with the cloud service - your email address and password do not have to match any other logons that you may have.

- Are you visiting another company or roaming outside your company network?

  If so, the cloud service may be applying another company's policy. Because you are not a user registered in that policy, you can neither log on nor register. You must contact the company's web policy administrator and ask for access within their policy. They may do this by inviting you as an end user.

Connection failure while roaming

If an end user cannot connect to the web while out of the office in a remote location, the most likely explanation is that the PAC (Proxy Auto Configuration) file URL is not set in Internet Explorer. This URL is required for a roaming connection to the cloud service.

In Internet Explorer, go to **Tools** > **Internet Options** > **Connections**, and check the defined connections and their settings by selecting a connection and clicking the **Settings** button. Each one should have **Use automatic configuration script** checked and Address set to "http://webdefence.global.blackspider.com:8082/proxy.pac" or whatever is correct for your policy.

Make sure **Automatically detect settings** and **Use a proxy server for this connection** are unchecked.

Using the service from public Internet access points

For some public Internet access points, such as hotel or airport Wi-Fi networks, users must complete a network enrollment page (known as a captive portal) when they first access the network.

The following scenarios use the example of a roaming user connecting to a hotel Wi-Fi network in order to illustrate the default behavior of the cloud service when using the default PAC file setting (using port 8082). These examples are provided to demonstrate the limitations of this setting for roaming users. For recommendations and best practices, see *Recommendations for roaming users*, page 11.

> ✓ **Note**
>
> The following scenarios do not apply if the Forcepoint Web Security Endpoint client is installed, since the endpoint is able to manipulate proxy settings in real time – for example, to temporarily disable itself at public Internet access points to allow a roaming user to complete network enrollment via their browser.

Scenario 1 – no captive portal

In this scenario, the user is not required to complete a network enrollment or payment page when accessing the Internet. The roaming user's browser is configured with the standard PAC file on port 8082.

1. The user requests www.google.de.
2. The browser first requests the PAC file from webdefence.global.blackspider.com over port 8082. One of the following may apply:
   - If the firewall of the hotel does not block port 8082, then the browser will obtain the PAC file. The user will get the "You are connecting from an unrecognized location" logon page. Once they log on, the appropriate policy is applied.
   - If the firewall of the hotel blocks port 8082, then the browser will not be able to obtain the PAC file.

     The browser will continue to try to obtain the PAC file over port 8082 until it times out. (By default, Internet Explorer will time out after 20 seconds.)

     Once the browser times out trying to obtain the PAC file, it will then attempt to follow the proxy server setting, if configured.

     If this is blank, the browser will connect via port 80.

     The hotel firewall does not block port 80, so the roaming user will connect to www.google.de over port 80.

     As such the user will be connecting to the Internet directly, instead of via the cloud service – the browser is not using the PAC file to direct traffic to the cloud proxy. No policy enforcement will be applied. The user will not be able to use the cloud service, as port 8082 is blocked.

     For guidance on resolving this issue for roaming users, see the recommendations detailed in the section *Recommendations for roaming users*, page 11.

Scenario 2 – captive portal

In this scenario, the hotel Wi-Fi redirects users' browsers to an online enrollment page (a captive portal) before allowing the user to connect to the Internet. The roaming user's browser is configured with the standard PAC file on port 8082

1. The user requests www.google.de.
2. The browser first requests the PAC file from webdefence.global.blackspider.com over port 8082.
3. The hotel's firewall checks its access control list (ACL) for the user's MAC address. The MAC address is not on the firewall's ACL, because the user has not yet registered.
4. Using the PAC file setting, the browser requests the PAC file from webdefence.global.blackspider.com over port 8082. Since the firewall does not recognize the user's MAC address, it does not allow the request for the PAC file.

The firewall does not respond with the captive portal on port 8082, which is a non-standard port for web browsing. Because most HTTP requests use port 80, the firewall expects web requests on port 80.

Note

It is possible, though unlikely, that the firewall will respond to web requests on port 8082 with the captive portal. In this case, the user will receive the enrollment page, and the browser will retrieve its PAC file. When the user attempts to browse, the they will be directed to the "You are connecting from an unrecognized location" logon page. Once they log on, the appropriate policy is applied.

If the firewall has been configured to serve the captive portal for requests on port 80 (most likely), the following occurs.

The browser continues to try to retrieve the PAC file over port 8082 until it times out. (By default, Internet Explorer will time out after 20 seconds.)

Once the browser times out trying to obtain the PAC file, it will then attempt to follow the proxy server setting, if configured.

- If this is blank, the browser will connect via port 80. The hotel firewall will now respond with the enrollment page on port 80. The user will complete registration, and the firewall will register the user's MAC address. Now that the user's MAC address is registered, the firewall will allow requests on all ports for that machine. The roaming user now is connecting to www.google.de over port 80 (it is not using the PAC file to direct traffic to the cloud proxy). As such, the user will be connecting directly to the Internet for this browser session, with no policy enforcement applied.

  Only when the user opens a new browser session (that is, a new browser window), the browser will then request the PAC file over port 8082.

  Because the user has registered, the user will now be directed to the "You are connecting from an unrecognized location" logon page. Once the user logs on, the appropriate policy is applied.

- If the browser has a proxy server setting configured, the browser attempts to connect to this proxy. For example, if the proxy server is configured as webdefence.global.blackspider.com and the port as 8081, then the browser will attempt to connect to webdefence.global.blackspider.com over port 8081.

  However, because the firewall does not find the user's MAC address on its ACL, it does not allow the request. The firewall is not configured to respond with the enrollment page on port 8081.

  At this point, the browser times out. The user cannot then connect to the Internet at all.

- If the browser is configured with a third-party proxy server, abc.com over port 80, then the browser will attempt to connect to this third-party proxy over port 80. As the firewall receives the request on port 80, it responds with the enrollment page. The user can complete enrollment, and the firewall will register the user's MAC address. The firewall will now allow requests out on all ports for that MAC address. Consequently, the roaming user now is connecting to www.google.de over port 80 via the proxy, abc.com for this browser session.

Only if the user opens a new browser session, i.e. a new browser window, will the browser then request the PAC file over port 8082.

Because the user's MAC address has been registered, the user will now be directed to the "You are connecting from an unrecognized location" logon page. Once the user logs on, the appropriate policy is applied.

For guidance on resolving these issues for roaming users, see the recommendations detailed in the section *Recommendations for roaming users*, page 11.

Using the service from home networks

Users connecting from home networks are treated as roaming, and are identified by the endpoint client, or by IP address, as described in *Identifying roaming users*, page 5.

In some circumstances, home users might connect to their network, launch a browser, and find that they are not using the Web Security Cloud service. This can happen for two reasons:

- The user launches the browser before the computer receives its IP configuration information.
- The computer connects to a network that uses a router that does not have an IP address assigned. This can occur with some Internet connections that use dynamically assigned IP addresses such as some home broadband connections. If the connection hasn't been used for some time, the router's lease for its IP address may have expired.

In the case of the Proxy Connect endpoint, if this occurs, the browser tries to retrieve its PAC file, and fails. If the computer is assigned an IP address immediately after the failure, the browser can fall back to accessing the Internet directly without retrying the PAC file. When endpoints can't connect to the cloud service, they allow Internet use to continue, and apply filters that have been cached, in order to provide as much protection as possible. This is known as Fallback mode.

If you encounter this issue, the possible solutions are as follows:

- Deploy Forcepoint Web Security Endpoint

  Installing the endpoint, either for all or just for roaming users, ensures that all web traffic receives enforcement from the cloud service.

- Configure an explicit proxy

  Some browsers allow you to configure an explicit proxy in addition to using a PAC file. You must ensure that you also add the global non-proxied destinations contained in the Web Security Cloud PAC file as proxy exceptions. Failure to do so could result in the service being inaccessible. For information on accessing the cloud service PAC file, see Proxy auto-configuration (PAC) in the Forcepoint Web Security Cloud help.

Adding an explicit proxy for roaming users ensures that users are always protected, with no user intervention. However, you must manually update any non-proxied destinations you add to the cloud service. In some circumstances, it can also prevent connectivity from some public Internet access points. See *Using the service from public Internet access points* for more details.

Recommendations for roaming users

The following are recommendations and best practices to help ensure that roaming users are protected when connecting via public or home networks.

- The best solution for roaming users who must connect from public or home networks is to deploy the Forcepoint Web Security Endpoint. The endpoint is network-aware, and is able to temporarily disable itself to allow network enrollment from public access points.
- If you cannot use the endpoint, best practice is to deploy the alternate PAC file address for roaming users. This PAC file is retrieved over port 80, meaning that users are redirected to a network's captive portal for enrollment. This is also recommended for users who may connect from networks where non-standard ports for browsing may be locked down. See the **Settings** > **General** page in the cloud portal.
- You can configure users' browsers with their policy-specific PAC file address (visible under the General tab in your policy). Then configure the browser home page as a non-proxied destination (configurable under Proxy Bypass in the Connections tab of your policy). This will cause the browser to make the request for the home page over port 80, causing firewalls to respond with the enrollment page.
- For home users who experience connection issues, consider using or an explicit proxy configuration in addition to the PAC file URL.
- Remote users may be able to establish a VPN connection to your office, and connect from the IP address of your office network. As such, the IP address will be recognized and users will not have to log on via the "You are connecting from an unrecognized location" page. As they are connected to the office, users will also be able to use transparent identification with their network NTLM ID.

  Note that some public networks may block ports 1723 or 47, typically used for VPN, and that captive portal enrollment may be required before the VPN can be established.VPN solutions that use port 80 are available.

Resetting the company master user portal account

Resetting the company master user portal account | Forcepoint Web Security Cloud

Overview

Each Forcepoint Cloud Security Gateway Portal (also referred to a the cloud portal) account has a super administrator user, known as the company master user. This user is the initial contact for your account and has the highest rights and privileges. This article describes what to do if you lose access to the company master user account, and cannot use the automated password recovery procedure.

Resetting the password or creating a new logon account

You might find that you need Support assistance with a password reset or a completely new logon account in the following situations:

- The only IT administrator has left the company.
- The only IT administrator has forgotten the account password and cannot reset it.
- Nobody at your organization knows who is responsible for the service, or who has a portal account.

In order to create a new account or reset the password on an existing account, you must supply Forcepoint with written instructions nominating a person as the portal administrator. The written instructions should come from an authorized person (for example, the company IT manager or the nominee's direct manager), and adhere to the following rules:

- The letter must be written on paper with the company letterhead.
- The authorizer's name and job title must be included, and clearly legible.
- The authorizer and the nominee for portal administrator must be two different people.
- The letter must specify the name and contact details of the nominee.

The written authorization can be sent to Forcepoint by post or by fax.

These steps are necessary because Forcepoint takes your account security very seriously. We then take steps to verify your details before resetting the password or creating a new logon account. This can take 2 business days, assuming the supplied written authorization is acceptable.

Document last updated: May 17, 2022