Release Notes for Forcepoint Web Security Direct Connect Endpoint for Mac (Build 19.08.0011)

Updated 4-Sept-2019

Applies to:	Forcepoint Web Security Cloud

This updated release of the Forcepoint Web Security Direct Connect Endpoint for Mac, known as build 19.08.0011, is an update of the previously released Forcepoint Web Security Direct Connect Endpoint for Mac, build 19.07.0239.

Use this release if:

- You are a brand-new Forcepoint Web Security cloud customer.

  or

- You have deployed an earlier Forcepoint Web Security Direct Connect Endpoint release in your organization, and one or more of the fixes in this release are important to you.

You do not need to use this release if:

- You have deployed an earlier Forcepoint Web Security Direct Connect Endpoint release and all is going well.

Use these Release Notes to learn what is in this release of the Forcepoint Web Security Direct Connect Endpoint.

- *New in this release*
- *Installation and upgrade*
- *Differences between the Mac and Windows versions of Forcepoint Web Security Direct Connect Endpoint*
- *Resolved and known issues*

For a full list of supported browsers and operating systems for each Forcepoint One Endpoint version, see the Certified Product Matrix.

For more information about past releases, see the Release Notes on the Forcepoint Web Security Endpoint Cloud documentation page.

New in this release

Updated 4-Sept-2019

Applies to:	Forcepoint Web Security Cloud

There are no new features in this release. This is an incremental release that contains content from the previous release (19.07.0239), along with quality improvements based on internal testing.

For more information about past releases, see the Release Notes on the Forcepoint Web Security Endpoint Cloud documentation page.

Support for latest browsers and operating systems

Browsers and operating systems are tested with existing versions of Forcepoint One Endpoint when they become available. For a full list of supported browsers and operating systems for each endpoint version, see the Certified Product Matrix.

When to use Forcepoint Web Security Direct Connect Endpoint

The Direct Connect Endpoint for Mac endpoint machines has been introduced alongside the existing Proxy Connect Endpoint. The Proxy Connect Endpoint will continue to be available and supported, and remains the default solution for securing roaming users in most situations.

The Direct Connect Endpoint extends roaming user protection to use cases where a proxy-based approach can be problematic. In general, you should consider using the Direct Connect Endpoint if the following applies to your organization:

- Geo-localized content: Localized content is critical; for example, your Marketing organization translates content into many languages.
- Unmanaged/third-party/complex networks: You have complex networks and changing network connections; for example, you have a remote workforce traveling and operating on client sites.
- Geographic firewalls: A geographical firewall prevents proxy use; for example, due to a national firewall or local network security system.
- Frequently changing network conditions: Frequent switching between different network connections; for example, using a mix of mobile, wifi and on-prem networks.
- Proxy unfriendly websites: You use a significant number of websites that do not work well with proxy technology and would otherwise require proxy bypass.
- Proxy unfriendly applications: You have non-browser and/or custom applications that require bypasses due to conflicts with proxy technology.

The Direct Connect Endpoint and Proxy Connect Endpoint software can both be used in the same customer deployment. However, only one type can be installed on an individual Mac endpoint machine.

Important

Although the Direct Connect Endpoint can provide improved security coverage as outlined in the use cases above, please check that the networking requirements and level of feature support are acceptable in your intended deployment.

Installation and upgrade

Updated 4-Sept-2019

Applies to:	Forcepoint Web Security Cloud

Hardware and operating systems

The following are minimum hardware recommendations for a machine with the Direct Connect Endpoint installed:

- 1 GHz or faster CPU
- 1 GB system memory
- 1 GB disk space

The following operating systems are supported:

- macOS 10.12.2 through 10.12.6
- macOS 10.13.0 through 10.13.6
- macOS 10.14.0 through 10.14.5

Enabling the macOS 10.14 kernel extension

When the endpoint machine loads the Direct Connect Endpoint for the first time, a window is shown to prompt you to enable the extension. You can enable the extension in **System Preferences > Security & Privacy**. For more information, see the User-Approved Kernel Extension Loading Technical Note from Apple.

> **Note**
> You must reboot the Mac endpoint machine after enabling the kernel extension. The Direct Connect Endpoint will not work correctly until the endpoint machine reboots.

Disabling the blocked kernel extension prompt

To disable macOS from prompting the user to allow kernel extensions, complete the following steps. Please note that following these steps automatically allows all kernel extensions.

1. Reboot the Mac endpoint machine in Recovery mode.
2. From the command line, run:

   ```
   spctl kext-consent disable
   ```
3. Reboot the Mac endpoint machine.

Networking Requirements

Firewall ports

- Direct Connect Endpoint management channels over port 443
- Outbound connections on ports 80 and 443
- Alternatively use your proxy infrastructure. Direct Connect Endpoint itself does not use PAC files, but it is able to operate with your PAC file settings if required.

Firewall settings

Local network infrastructure must allow access to Forcepoint Cloud IP range. (See Cloud service data center (cluster) IP addresses and port numbers for details.)

Fallback mode will engage if the Forcepoint Cloud IP range is blocked. In Fallback mode, the endpoint continues to prevent access to previously blocked sites, so users' computers are partially protected. For more information, see *Fallback mode* in the End User's Guide for Forcepoint One Endpoint.

Obtaining endpoint client software

To obtain the latest Direct Connect Endpoint client software package, log onto the Forcepoint Security Portal, and then go to **Web > Endpoint > General** to download the endpoint installation package.

You must set an anti-tampering password to enable the package download links.

Deploying new Mac endpoints

For instructions, see the Installation and Deployment Guide for Forcepoint One Endpoint.

Uninstalling Forcepoint Web Security Direct Connect Endpoint

To uninstall from the command line:

1. Open a terminal window and type the following command to uninstall the service:

   ```
   sudo wepsvc --uninstall
   ```

2. Type the root user **Password**.

3. If you provided an anti-tampering password in the Forcepoint Security Portal, type the anti-tampering password when prompted.

To uninstall from System Preferences:

1. Open System Preferences.
2. Click **Forcepoint** to open the Forcepoint Endpoint Preferences page.
3. Click the **Uninstall Endpoint** button.
4. If you provided an anti-tampering password in the Forcepoint Security Portal, you are prompted to provide the anti-tampering password.

   Type the anti-tampering password, then the root user password to continue.
5. Click **OK** to close the confirmation dialog window.

Starting and stopping Forcepoint Web Security Direct Connect Endpoint

1. Open a terminal window.
2. Type the following command to stop the service:

   ```
   sudo wepsvc --stop
   ```
3. Type the following command to check the status of the service:

   ```
   sudo wepsvc --status --wsdc
   ```
4. Type the following command to start the service:

   ```
   sudo wepsvc --start
   ```

Upgrading existing deployments

On an endpoint machine with a lower version of Direct Connect Endpoint installed:

You can install this version without uninstalling the lower version. Run the Direct Connect Endpoint installation package to automatically remove the installed version, then install this version.

On an endpoint machine with Proxy Connect Endpoint installed:

If you are upgrading an endpoint machine from the Proxy Connect Endpoint to the Direct Connect Endpoint, you must uninstall the Proxy Connect Endpoint before installing the Direct Connect Endpoint.

Auto-Update:

Automatic updates are enabled through the Forcepoint Security Portal. For more information, see the Upgrade Guide for Forcepoint One Endpoint.

> **Note**
> If you are upgrading to a combined deployment of Direct Connect Endpoint and Forcepoint DLP Endpoint, you must restart the endpoint machine to finalize the Forcepoint DLP Endpoint upgrade.

Deployment model support

This build supports the following deployment models:

- Behind third-party authenticating proxies (chained/explicit proxy)
- Behind third-party filtering proxies (chained/explicit proxy)
- Behind third-party Transparent proxies
- Behind on-premises IPsec (VPN) Edge device
  - The Direct Connect Endpoint will not be able to contact the disposition service, so it will fail open and traffic will be transparently re-directed. There is no end user impact.
- Behind on-premises Firewall re-direct
  - The Direct Connect Endpoint will not be able to contact the disposition service, so it will fail open and traffic will be transparently re-directed. There is no end user impact.

Application support

By default, any running applications are subject to the same web enforcement policy on port 80 (HTTP requests) and port 443 (HTTPS requests). Occasionally, some applications do not work properly in conjunction with endpoint enforcement. This might occur with, for example, custom-designed applications for your organization, or applications that need to contact an Internet location for updates.

If you are experiencing problems with applications on endpoint machines, go to the **Endpoint Bypass** tab on the **Web > Endpoint** page in the Forcepoint Security Portal and add the names of any application executables that you want to bypass endpoint policy enforcement. For more information, see Endpoint bypass in the Forcepoint Security Portal Help.

Fallback mode

If the Direct Connect Endpoint is unable to contact the Forcepoint cloud service, it moves into Fallback mode. The device is now partially protected by applying filters cached from previously blocked site visits. For example, if the user previously saw a block page when visiting Facebook, then the user would also see a block page when visiting Facebook while in Fallback mode. This block page indicates that it was a result of cached results. Once the network issue is resolved, normal filtering resumes.

For more information, see *Fallback mode* in the End User's Guide for Forcepoint One Endpoint.

Configuring endpoint behavior

Following are some of the configuration options available in the Forcepoint Security Portal for the Direct Connect Endpoint. Note that all links go to the Forcepoint Technical Library.

- Web categorization. See Web Categories.
- Setting a default endpoint policy for roaming users. See Deploying the endpoint for Mac.
- End user control. See Deploying the endpoint for Mac.
- Anti-tampering password. See Deploying the endpoint for Mac.
- Endpoint bypass settings.
- Policy exceptions by time, user, and group. See User and group exceptions for time-based access control.
- SSL inspection. See Enabling SSL decryption.
- Allowing end users to proceed when notified of certificate errors, and managing specific domains for certificate bypass. See Bypassing certificate verification.
- Non-proxied destination domains and IP addresses at account and policy level. These operate as non-enforcement destination domains for this version of the endpoint. The configured domains are added to the endpoint management service rather than the PAC file. See Adding and importing non-proxied destinations, and Connections tab.
- Endpoint reporting. See the Advanced section under Predefined reports.
- Data Center allocation based on end user egress IP. This does not impact geo-localization of content, but does require a software restart for the setting to take effect.

Unsupported options

The following configuration options are not currently supported by the Direct Connect Endpoint.

Functional:

- True File Type download blocking
- Executable file upload blocking
- Cloud Data Security (DLP)
- Social Media updates
- Low risk profile ACE scanning settings
- Scanning for malware on low risk profile sites
- File download blocking by size
- Endpoint browsing behind an iSeries appliance
- Acceptable Use landing page
- Bandwidth reporting
- YouTube restricted mode

Operational/Deployment:

- Automatic initial endpoint deployment from cloud service
- Fallback mode block page cannot be customized via the cloud portal

Differences between the Mac and Windows versions of Forcepoint Web Security Direct Connect Endpoint

Updated 4-Sept-2019

Applies to:	Forcepoint Web Security Cloud

Due to differences in how the Windows and macOS operating systems function, the brand new Mac Direct Connect Endpoint differs from the existing Windows Direct Connect Endpoint in the following ways:

Mac	Windows
The Mac Direct Connect service name is **wsdc**.	The Windows Direct Connect service name is **wsts**.
Fallback mode defaults to 125 seconds.	Fallback mode has three settings: ● Faster (65 seconds) ● Normal (125 seconds) ● Slower (245 seconds)
Fallback mode supports: ● Fail-Open (`EnableFailureOpen=1`) ● Fail-Close (`EnableFailureOpen=0`) ● Fail-Safe (`EnableFailureOpen=2`)	Fallback mode supports: ● Fail-Open (`EnableFailureOpen=1`) ● Fail-Safe (`EnableFailureOpen=2`)
The Fallback Fail-Safe (`EnableFailureOpen=2`) option uses the cloud block page.	The Fallback Fail-Safe (`EnableFailureOpen=2`) option uses the local cached cloud block page.
In Fallback mode, the local drive does not keep the cache after the wsdc service is restarted.	In Fallback mode, the local drive keeps the cache after the wsts service is restarted.

Mac	Windows
When anti-tampering is ON and the Direct Connect service is stopped, files in the install folder can be added, deleted, or modified.	When anti-tampering is ON and the Direct Connect service is stopped, files in the install folder cannot be added, deleted, or modified.
Enable the detailed (verbose mode) Direct Connect debug logs by typing the following command into the command line: `wepsvc --set-debug-level 31` The log file is located in the following folder: **/var/log/WebsenseEndpoint/dcdebug.log** End users can save debug logs to the Desktop by clicking **Collect Endpoint Info** in the diagnostics tool, but they are not as detailed. Disable verbose mode debug logs by typing the following command into the command line: `wepsvc --set-debug-level 7`	Enable the Direct Connect debug logs by clicking **Collect Endpoint Info** in the Forcepoint Web Security Endpoint Diagnostics Tool. The log file is generated on the endpoint machine's desktop.

Resolved and known issues

Updated 4-Sept-2019

Applies to:	Forcepoint Web Security Cloud

A list of resolved and known issues is available in the Forcepoint Knowledge Base. You must log on to My Account to view the list.