Release Notes for Forcepoint Web Security Direct Connect Endpoint for Windows (Build 19.03.823)

Updated 23-April-2019

Applies to:	Forcepoint Web Security Cloud

This updated release of the Forcepoint Web Security Direct Connect Endpoint for Windows, known as build 19.03.823, is an update of the previously released Forcepoint Web Security Direct Connect Endpoint, build 3826.

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 Forcepoint Web Security Direct Connect Endpoint.

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

New in this release

Updated 23-April-2019

Applies to:	Forcepoint Web Security Cloud

Introducing Forcepoint Web Security Direct Connect Endpoint on the Forcepoint One Endpoint platform

Starting in this release, Forcepoint Web Security Direct Connect Endpoint (Direct Connect Endpoint) has been added to the Forcepoint One Endpoint platform. Forcepoint One Endpoint consolidates all installed Forcepoint One Endpoint agents, which now includes Forcepoint DLP Endpoint and Forcepoint Web Security Endpoints, under a single system tray icon.

This new version contains the Direct Connect Endpoint functionality familiar to current customers. No functionality was removed in the transition to Forcepoint One Endpoint.

IPv6 Compatibility Support

Direct Connect Endpoint supports dual stack endpoints, so both IPv4 and IPv6 requests from an endpoint machine are handled by the Direct Connect Endpoint proxy.

Direct Connect Endpoint can now:

- Access the Internet regardless of the IP protocol (IPv4, IPv6, or a mixed IPv4/IPv6 network).
- Show the correct IPv6 address in log files.

Direct Connect Endpoint policy lookup only supports IPv4 communications.

Support for Windows 10 October 2018 Update, version 1809

Direct Connect Endpoint is supported on Windows endpoint machines running the Windows 10, version 1809 operating system.

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 you deploy Direct Connect Endpoint to Windows endpoints with Firefox v53 or higher installed, follow the below deployment guidance:

Edit the **DCUserConfig.xml** configuration file to specify the following configuration parameters in “DCSetting”:

```
<FirefoxSetting FirefoxConfigCFGFileName="mozilla.cfg"
FirefoxConfigJSFileName="channel-perfs.js" />
```

When to use Forcepoint Web Security Direct Connect Endpoint

The Direct Connect Endpoint is available alongside the existing Forcepoint Web Security Proxy Connect Endpoint (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.

Direct Connect Endpoints and Proxy Connect Endpoints can both be used in the same customer deployment. However, only one type can be installed on a Windows 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.

Deployment and installation

Updated 23-April-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 Intel-compatible processor
- 1 GB system memory
- 1 GB disk space

The following operating systems are supported:

- Windows 7 SP1 or above
- Windows 8
- Windows 8.1
- Windows 10:
  - Windows 10, version 1511 (initial public release)
  - Windows 10 Anniversary Update, version 1607 (including Secure Boot mode)
  - Windows 10 Creators Update, version 1703 (including Secure Boot mode)
  - Windows 10 Fall Creators Update, version 1709 (including Secure Boot mode)
  - Windows 10 Spring Creators Update, version 1803 (including Secure Boot mode)
  - Windows 10 October 2018 Update, version 1809

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.

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.

Application support

By default, any running applications are subject to the same web enforcement policy on HTTP requests on port 80, and HTTPS requests on port 443.

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 end users' machines, the **Endpoint Bypass** tab on the **Web > Endpoint** page in the Forcepoint Security Portal enables you to 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.

Secure channel support

This version of the Direct Connect Endpoint supports secure channel handling through the host system infrastructure. Depending on the version of Windows on the installation machine, the endpoint communicates with the cloud service over:

- TLS 1.1 and 1.2

These channels follow the system proxy settings in a network environment where all traffic is proxied.

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.
- This version of the endpoint is currently supported on 32-bit or 64-bit Windows.
- Copy the **GPO code** that is provided if you intend to deploy the Direct Connect Endpoint MSI package to client machines via Microsoft Group Policy Object (GPO).

Deploying new Windows endpoints

There are a few ways to distribute the Direct Connect Endpoint software on Windows clients, including virtual desktop clients running Windows:

- Manually on each endpoint device, using the installation package supplied by Forcepoint.
- Using a GPO or other third-party deployment tool for Windows. If you need assistance, contact Forcepoint Technical Support.

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

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.

You must reboot the endpoint machine to complete the installation.

On an endpoint machine with Proxy Connect Endpoint installed:

You must uninstall the Proxy Connect Endpoint before installing the Direct Connect Endpoint. Both agents cannot be installed on the same endpoint machine.

You must reboot the endpoint machine after you uninstall the Proxy Connect Endpoint.

Auto-Update:

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

If you have disabled auto-update, endpoint machines show an error in the Diagnostics Tool stating that it cannot reach the auto-update service. This error may also display on endpoint machines that have enabled auto-update, but that have not been updated to the new Forcepoint One Endpoint version of the Direct Connect 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 Windows.
- Auto-update of previously installed Direct Connect Endpoint.
  Note: A Proxy Connect Endpoint cannot be auto-updated to a Direct Connect Endpoint.
- End user control. See Deploying the endpoint for Windows.
- Anti-tampering password. See Deploying the endpoint for Windows.
- 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

Resolved and known issues

Updated 23-April-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.