

# Release Notes for TRITON AP-ENDPOINT Web Direct Connect for Windows (Build 3331)

Updated 10-Aug-2016

<b>Applies to:</b>	◆ TRITON AP-WEB with the Web Cloud Module
--------------------	---

TRITON AP-ENDPOINT Web now includes 2 endpoint client options:

- The **Direct Connect** endpoint is a new web endpoint client. It routes traffic directly to the Internet, and contacts a new endpoint cloud service to determine whether to block or permit a request, perform analysis of traffic content, and/or deliver endpoint configuration.

The Direct Connect endpoint may be beneficial for roaming users where proxy-type connections are problematic. This includes, for example, websites that do not work well with a proxy, areas where geographic firewalls prohibit the use of proxies, situations where localized content is required regardless of user location, and in complex/changing network environments.

- The existing web endpoint client is now called the **Proxy Connect** endpoint. It redirects traffic to the cloud proxy for analysis.

Use these Release Notes to learn what is in this version of the Direct Connect endpoint and why you might want to deploy it instead of or in addition to the Proxy Connect version.

- ◆ [New in this Release](#)
- ◆ [Deployment and Installation](#)
- ◆ [Known issues](#)



For a full list of supported browsers and operating systems for each endpoint version, see the [Certified Product Matrix](#).


# New in this Release



Now when you navigate to the **Web > Settings > Endpoint** page in the cloud portal, you have two types of endpoints to choose from: Direct Connect and Proxy Connect. You can deploy a combination of Direct Connect and Proxy Connect endpoint clients in your organization if desired.

**Note:** If the Direct Connect endpoint option is not shown on the Endpoint Client Download screen, please contact Forcepoint Technical Support to have it enabled for your account.

**Endpoint Client Download**

Endpoint type: ☒ Direct Connect  ☐ Proxy Connect 

Platform:  

Available version:  1.5.8.1.3255  [Release notes](#) *Supported on Windows 7, 8, 8.1, 10*

## When to use Direct Connect

---

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

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

- ◆ Geographic firewalls: A geographical firewall prevents proxy use; for example, due to a national firewall or local network security system.
- ◆ 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.
- ◆ 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 and Proxy Connect endpoints can both be used in the same customer deployment, however only one type can be installed on a PC.

Although Direct Connect 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 10-Aug-2016

<b>Applies to:</b>	◆ TRITON AP-WEB with the Web Cloud Module
--------------------	---

## 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

## Networking Requirements

---

### Firewall ports

- ◆ Direct Connect management channels over port 443
- ◆ Outbound connections on ports 80 and 443
- ◆ Alternatively use your proxy infrastructure. The 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.

## 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 Cloud TRITON Manager 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 Cloud TRITON Manager Help.

## Secure channel support

---

This version of the 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 1.0, 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 TRITON AP-ENDPOINT Web Direct Connect client software package, log onto the Cloud TRITON Manager, and then navigate 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 only on 32-bit or 64-bit Windows.
- Copy the GPO command that is provided if you intend to deploy the TRITON AP-ENDPOINT MSI package to client machines via GPO.

**Note:** If the Direct Connect endpoint option is not shown on the Endpoint Client Download screen, please contact Forcepoint Technical Support to have it enabled for your account.

## Deploying new Windows endpoints

---

There are a few ways to distribute the 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 Microsoft Group Policy Object (GPO) or other third-party deployment tool for Windows. If you need assistance, contact Forcepoint Technical Support.

For instructions, see “[Deploying Windows Endpoints](#)” in the Installation and Deployment Guide for Forcepoint Endpoint Solutions.

## Upgrading existing deployments

---

If you have existing Proxy Connect endpoints deployed, you must uninstall and re-install them to use Direct Connect.

## Configuring endpoint behavior

---

Following are some of the configuration options available in the Cloud TRITON Manager for both TRITON AP-ENDPOINT Web in Direct Connect mode. Note that all links go to the Forcepoint Technical Library.

- Web categorization
- Setting a default endpoint policy for roaming users. See [Deploying the endpoint for Windows](#).
- ◆ Auto-upgrade of previously installed Direct Connect endpoints build 325 upward. 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](#).

## Unsupported options

---

The following configuration options are not supported in the initial release of Direct Connect web endpoint but may be addressed in future releases.

### 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 for Schools

### Operational/Deployment:

- ◆ Mac OS PC platform support
- ◆ Data Center allocation based on end user egress IP. Does not impact geo-localization of content.
- ◆ Automatic initial endpoint deployment from cloud service
- ◆ Fallback mode block page cannot be customized via the cloud portal.

# Known issues

Updated 10-Aug-2016

<b>Applies to:</b>	◆ TRITON AP-WEB with the Web Cloud Module
--------------------	---

Following are the known issues for this release.

- ◆ Non-Proxied Destination lists have a temporary size limitation which may impact you. See this [knowledgebase article](#) for details.
- ◆ Fallback mode page can only be customized during endpoint install; it cannot be customized from the cloud portal.
- ◆ The Direct Connect endpoint and proxy-connected systems, such as the Proxy Connect endpoint, share the same Non-Proxied Destinations (site bypass) list.