Release Notes for Web Protection Solutions

Release Notes | Forcepoint Web Security and Forcepoint URL Filtering | 29-APR-2022

Use the Release Notes to find information about what's new and improved for Forcepoint Web Security and Forcepoint URL Filtering in version 8.5.5.

> **Note**
> The Content Gateway component is not included in Forcepoint URL Filtering deployments. Content Gateway information applies only to Forcepoint Web Security.

Refer to the following when installing or upgrading to v8.5.5.

- Installing Forcepoint Web Security
- Installing Forcepoint URL Filtering
- When upgrading TRITON AP-WEB (v8.2.x or 8.3.x) or Forcepoint Web Security (8.4.x or 8.5.x), see Upgrade Instructions for Forcepoint Web Security
- When upgrading Web Filter & Security (v8.2.x or 8.3.x) or Forcepoint URL Filtering (8.4.x or 8.5.x), see Upgrade Instructions for Forcepoint URL Filtering
- Deployment and Installation Center

> **Important**
> **V-Series appliance users:**
>
> Some older V10000 and V5000 appliances are not supported with version 8.0.0 and higher.
>
> See V-Series appliances supported with version 8.x

For details on supported upgrade paths, see the Upgrade Guide: Forcepont Web Security for v8.5.x.

Important

If you are currently running a Web Security Gateway or Gateway Anywhere version earlier than v7.8.4, upgrade to v7.8.4 first. See this upgrade guide for instructions.

- Content Gateway Hotfix 94 must be applied to v7.7.x prior to upgrading Content Gateway (software or appliance) to v7.8.4. This retains the default Sync Mode setting for real-time analysis, and can prevent latency.
- Appliance Hotfix 90 must be applied to v7.7.x prior to upgrading the appliance to v7.8.4. See the v7.8.x Upgrade Instructions.

Customers currently using a Red Hat Enterprise Linux version earlier than 7.9 will need to upgrade their operating system prior to upgrading the product.

New in Web Protection Solutions

Release Notes | Forcepoint Web Security and Forcepoint URL Filtering | 29-APR-2022

Security enhancements

Forcepoint Security Labs Analysts continually assess potential security vulnerabilities which can be introduced by third-party libraries. Security improvements have been made in several areas in version 8.5.5.

A security update done for the v8.5.4 product release has resulted in a new requirement for a specific dynamic-link library (dll) when installing or upgrading v8.5.4 or v8.5.5 Forcepoint Web Security or Forcepoint URL Filtering software on a Windows platform.

If you have not recently downloaded the Visual C++ Redistributable Package from Microsoft, it is likely that the installation/upgrade will prompt with the error "Installation failed with error code 3004". The log file generated by the installation/upgrade process, available in the Temp folder of the user running the installer, will contain a line similar to:

```
java.lang.UnsatisfiedLinkError:
C:\Users\Administrator\AppData\Local\Temp\2\I1588276985\Wind
ows\resource\jre\bin\freetype.dll: Can't find dependent
libraries
```

The dependency referenced in this log entry is for **vcruntime140.dll**, a file that is part of the Redistributable Package.

Should the error occur during the install/upgrade process:

1. Close the error window but do NOT stop the install/upgrade process. Leave the installer window open.
2. Locate the latest 64-bit Redistributable Package for your Windows version from this site.
3. Download and install the package.
4. Return to the installation/upgrade window and continue the process.

Hybrid enhancements

Improvements have been made for the Hybrid Module of Forcepoint Web Security.

Generic SAML support for single sign-on

The single sign-on feature uses the Security Assertion Markup Language (SAML 2.0) data format to send authentication requests to and receive responses from your identity provider. Previously when configuring single sigh-on, a specific identity provider had to be selected from an available list of providers.

This enhancement provides support for any identity provider that supports the SAML 2.0 standard. A new selection, **SAML 2.0 Compliant Identity Provider**, is an option on the **Web > Settings > Hybrid Configuration > Hybrid User Identification** page of Forcement Security Manager. The metadata for your identity provider is configured as before.

PAC file size limit increase

The earlier 50KB limit for the PAC file sent by Sync Service to the hybrid service has been increased to 256KB. See What is the hybrid PAC file in Administrator Help for more information.

Policy-level CASB

An enhancement to the Protected Cloud Apps feature has been made that allows policy enforcement for cloud applications by all or a subset of the filtering policies.

After selecting the cloud applications on the **Web > Settings > CASB Configuration > Protected Cloud Apps** page of Forcepoint Security Manager, use the **Forward to Forcepoint CASB** option to chose the policies that will forward requests to Forcepoint CASB for enforcement:

- For **All policies** (the default) to forward all user requests for the selected cloud apps.
- **Per policy** to choose specific policies to forward all user requests for the selected cloud apps.

When **Per policy** is selected, tables provide a method of indicating which policies should or should not forward requests to CASB. Filtering Service handles all user requests to a cloud app if the policy being applied is not configured to **Forward to Forcepoint CASB**.

Miscellaneous Enhancements

Other enhancements are included with the release of v8.5.5.

- Integration with Forcepoint RBI. A list of documentation available for that product can be found here.
- The **Web > Settings > CASB Configuration > Protected Cloud Apps** page now lists all custom cloud apps added in the CASB portal.
- Support for AlwaysOn Availability groups with Microsoft SQL Server has again been confirmed.
- The Redirect for HTTPS Authentication option, added to the Configuration > Security > Access Control > Global Authentication Options page of Content Gateway Manager has been removed. By default, for v8.5.5, the option is enabled.

  Configure the proxy.config.auth.ssl_autl_url variable in records.config to disable the feature. This setting disables (0) or enables (1) authentication of HTTPS requests over HTTPS, using port 8443. When disabled, authentication for HTTPS requests is done over HTTP, using port 8080.

Browser support

See the Certified Product Matrix for the latest list of supported browsers.

Logon application support

Logon Agent communicates with the logon application (LogonApp) on client machines to identify users as they log onto or off of Windows domains.

The logon application supports the following operating systems:

- Mac OS X 10.10 (64-bit)
- Microsoft Windows 8.1 Update 1 (32-bit and 64-bit; Windows 8.1 RT is not supported)
- Microsoft Windows 10

For more information about Logon Agent and the logon application, see the Using Logon Agent for Transparent User Identification white paper.

Third-party platform and product support

All components

This version adds support for:

- Microsoft SQL Server 2019
- Red Hat Enterprise Linux 7.9 and the corresponding version of CentOS
- VMware ESXi 7.0

This version ends support for:

- Red Hat Enterprise Linux 7.6 and the corresponding version of CentOS.
- Microsoft Windows Server 2012 (all versions)

See the full list of supported operating systems here.

See the Certified Product Matrix for the latest list of supported browsers.

Note

Newer versions of Google Chrome block Flash content. In order to successfully use your web solutions product, you will need to disable the blocking or use a different supported browser.

Note that installing web protection components on Windows Server 2012 or 2012 R2 requires Microsoft .NET Framework v.35 and v4.5. Install both and turn them both on before running the Forcepoint Security Installer.

Content Gateway

This version is supported on:

- Red Hat Enterprise Linux7.9 (and corresponding CentOS versions).

Important

Forcepoint Web Security customers using Red Hat Enterprise Linux or CentOS 7.x must disable **firewalld** prior to installing Content Gateway.

On the machine where Content Gateway will be installed, execute the following:

```
systemctl stop firewalld
systemctl disable firewalld
```

As a best practice, Red Hat Enterprise Linux systems that host Content Gateway should be registered with Red Hat Network and kept up-to-date with the latest security patches.

Important

You can update packages on your Red Hat Enterprise Linux installations and patch kernels if the underlying kernel upgrade does not change the kernel API.

Important

Content Gateway is designed to run on a dedicated machine and is not guaranteed to be compatible with other server applications installed on the same machine.

For a complete platform requirements information, see System requirements for this version in the Deployment and Installation Center.

Resolved and known issues

Release Notes | Forcepoint Web Security and Forcepoint URL Filtering | 29-APR-2022

A list of resolved and known issues in this release is available to Forcepoint Web Security or Forcepoint URL Filtering customers.