Forcepoint Web Security Cloud: 2021 Release Notes

Forcepoint Web Security Cloud | 2021 Release Notes | Last updated October 5, 2021

This document details product updates and new features added to Forcepoint Web Security Cloud during 2021.

What's new?

Accessing the Neo management portal

Added 07-Oct-2021

The Neo management portal is used to configure the Neo endpoint agent. Web Security Cloud customers must access the Neo management portal to, for example, change the auto-update setting or generate a release code, which is used by end users to uninstall the endpoint.

To assist Cloud Web Security customers, a link to the portal has been added to the **General** tab of the **Web > Settings > Endpoint** page of the Cloud Security Gateway Portal. Click the **Forcepoint Neo management portal** link to open the Neo management portal in a new tab. On the Neo management portal you can access the endpoint dashboard, endpoint management, and advanced settings.

Note that access to this option requires Modify Configuration permissions.

Previous updates

Neo for Mac

Added 19-July-2021

The new Neo endpoint agent released on 14-April-2021 (see *Neo integration*) is now available for macOS 11 (Big Sur). The Cloud Security Gateway Portal has been updated to provide Mac as an option for download when Neo is selected as the **Endpoint Type** in the Endpoint Client Download section of **Web Settings > Endpoint.**

When the Neo endpoint agent is installed on your Windows and macOS endpoints, there are important things to note.

- By default, the Neo endpoint has **Automatic updates** turned ON. If you wish to disable auto-update, contact Technical Support.
- This release for the macOS supports only the Intel chip. Support for the Apple M1 chip is planned for a future release.

For further information about the Neo endpoint release, see What's new in the Forcepoint Dynamic User Protection Help. Additional information can be found in this list of Known Issues.

Policy-level CASB

Added 06-July-2021

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 defined in Forcepoint Web Security Cloud.

After selecting the cloud applications on the **Web > Settings > Protected Cloud Apps** page of Cloud Security Gateway, use the **Forward traffic 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.

Note that the same list of cloud apps is applied in all cases.

Along with this new enhancement, a change has been made to the Cloud apps tab for a policy. Enable **Always allow access to cloud apps on the Allow Access list** to always permit user access to cloud apps that have been added to the Allow Access list. User requests to these applications are allowed regardless of how the corresponding category is configured on the Web Categories tab. See Filtering order action in the Cloud Security Gateway Portal help for details on how the cloud service applies filtering actions.

Integration with Data Protection Service and Forcepoint DLP

Added 06-July-2021

Forcepoint Web Security Cloud can now be configured to send user requests that present potential data loss to Forcepoint DLP for further inspection. Forcepoint DLP then returns it's finding to the cloud proxy for policy enforcement.

Support for data security handled by the cloud proxy (referred to as DLP Lite) is still available.

Use the **Web > Settings > Data Protection Settings** page to enable and configure the integration with Data Protection Service. See Data Protection Settings for more information.

When **Use Data Protection Service** has been selected on the new portal page, each new policy is created with a new Data Protection tab. User requests handled by policies configured to use Data Protection Service are then sent to Forcepoint DLP.

Note

Data Protection Service integration requires an additional license. If you would like further information on integrating with Data Protection Service, contact your account manager.

Neo integration

Added 14-Apr-2021

The new Neo endpoint agent can now be downloaded and configured in the Cloud Security Gateway Portal for use by web endpoint clients deployed in your network. The Neo endpoint agent is a single agent that installs on the endpoint machine and includes both proxy connect and direct connect modes. Once Neo is activated, the full functionality of proxy connect and direct connect is available. Neo uses the appropriate endpoint mode, based on network conditions. When proxy connect mode

is in use but can't connect to the proxy or if performance becomes an issue, Neo will switch to the direct connect mode.

Neo collects activity data from the endpoint and, for customers who have purchased Forcepoint Dynamic User Protection, sends the data there where it is analyzed for the purpose of risk score calculation.

Cloud app blocking now available to all customers

Added 14-Apr-2021

The cloud app blocking feature, initially announced on 7 May 2020 as available by request only, is now available to all Forcepoint Web Security Cloud customers.

As a reminder, this feature allows for policy enforcement for cloud applications. Requests to cloud applications can be blocked or allowed using options on a new tab available when configuring a policy (**Web > Policy Management > Policies**).

Use the **Cloud apps** tab to add cloud apps to a **Block Access** or **Allow Access** list. Policy enforcement is done based on the selections on each list. Policies are applied to user requests by first considering the category assigned to the site and then by applying the rules defined by the contents of the block and allow lists.

Note: customers with a Protected Cloud Apps license cannot select cloud apps already configured as protected on the **Web > Settings > Protected Cloud Apps** page. Those apps are automatically selected on the **Allow Access** list. They appear in search results on both lists, but cannot be selected or removed on either. Attempts by an end user to access these apps are forwarded to Forcepoint CASB for analysis and policy enforcement unless the app is in a blocked category (configured on the Web Categories tab).

The instructions found in Cloud Security Gateway Portal Help, also known as the Forcepoint Web Security Cloud Admin Guide, to contact Technical Support to enable this feature are no longer valid.

2020 updates

Last updated 07-Jan-2021

For details of new features added, and issues resolved during 2020, please see the Forcepoint Web Security Cloud 2020 Release Notes.

Resolved and known issues

To see the latest list of known and resolved issues for Forcepoint Web Security Cloud, see Resolved and known issues for Forcepoint Web Security Cloud - 2021 in the Forcepoint Knowledge Base.

You must log on to My Account to view the list.

Limited availability features

Last updated 08-Apr-2021

The table below lists Forcepoint Web Security Cloud features that are in a limited availability status. Limited availability features may have been released recently, or may need to be approved by your account manager before being added for your organization, due to additional configuration requirements, or other considerations.

If you are interested in enabling any of these features for your account, please contact Technical Support.

Feature	Description
Acceptable use policy	Allows administrators to require that end users periodically accept the terms of an acceptable use policy (AUP) before continuing to browse via the proxy. The feature can be set per policy, and users are required to accept the AUP every 1, 7, or 30 days. The AUP confirmation screen can be customized under **Web > Policy Management > Block & Notification Pages**. For further information, see the Forcepoint Security Portal Help.
Password policy for end users	Allows you to apply the same password policy requirements both for administrators accessing the cloud portal, and end users manually authenticating with the proxy. Password policy settings are configured on the **Account > Contacts** page. For further information, see the Forcepoint Security Portal Help.
Single sign-on	Single sign-on (SSO) allows seamless authentication for end users accessing the cloud proxy, using a supported identity provider. Suitable for pure cloud or hybrid solutions. Please contact Technical Support for details of currently supported identity providers. For further information, see Single Sign-On for Forcepoint Web Security Cloud.
Full traffic logging	Allows administrators to download full web traffic logs for retention and analysis, which can be useful for integration with third-party SIEM tools. Logs can be downloaded for 14 days and are provided in JSON format. For further information, see Configuring Full Traffic Logging on the Forcepoint Support website.
Remote Browser Isolation	Send blocked web requests to a third-party remote browser isolation provider, allowing the web page to be viewed outside of the organization's network. For further information, see Configure Remote Browser Isolation in the Security Portal Help.