v8.4.0 Release Notes for Web Protection Solutions

Release Notes | Forcepoint Web Security and Forcepoint URL Filtering |31-Jul-2017

Use the Release Notes to find information about what's new and improved for Forcepoint Web Security and Forcepoint URL Filtering in version 8.4.0.

For information about endpoint client software, please refer to the Release Notes for Forcepoint Web Security Endpoint.

✓ **Note**

The Content Gateway component is not included in Forcepoint URL Filter deployments. Content Gateway information applies only to Forcepoint Web Security.

Refer to the following when installing or upgrading to v8.4.

- Installing Forcepoint Web Security
- Installing Forcepoint URL Filtering
- When upgrading Web Security Gateway/Anywhere (v7.8.4) or TRITON AP-WEB (8.1.x, v8.2.x or 8.3.x), see Upgrade Instructions for Forcepoint Web Security
- When upgrading Web Filter *or* Web Security (v7.8.4) or Web Filter & Security (8.1.x, v8.2.x or 8.3.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 8.0

Upgrades to v8.4 are supported from v7.8.4, v8.1, v8.2, and v8.3. If you have an earlier version, or v8.0.x, there are interim steps to perform. These are shown below.

Your current version	**Step 1**	**Step 2**	**Step 3**	**Step 4**
v7.1.x	Upgrade to 7.6.x	Upgrade to 7.7.x	Upgrade to 7.8.4	Upgrade to 8.4.x
v7.5.x	Upgrade to 7.6.x	Upgrade to 7.7.x	Upgrade to 7.8.4	Upgrade to 8.4.x
v7.6.x	Upgrade to 7.7.x	Upgrade to 7.8.4	Upgrade to 8.4.x	none
v7.7.x	Upgrade to 7.8.4	Upgrade to 8.4.x	none	none
v7.8.1 v7.8.2 v7.8.3	Upgrade to 7.8.4	Upgrade to 8.4.x	none	none
v7.8.4	Upgrade to 8.4.x	none	none	none
v8.0.x	Upgrade to 8.3.x*	Upgrade to 8.4.x	none	none
v8.1.x	Upgrade to 8.4.x	none	none	none
v8.2.x	Upgrade to 8.4.x	none	none	none
v8.3.x	Upgrade to 8.4.x	none	none	none

* TRITON AP-WEB customers upgrading from v8.0.x to v8.3 should install Content Gateway v8.3 Hotfix 3 if v8.3 will be used in production prior to upgrading to v8.4.

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 Red Hat Enterprise Linux 6.4 or earlier 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 |31-Jul-2017

Product mapping

Version 8.0 was the first product release that used a new, simplified product naming and grouping of the familiar product line.

Version 8.4 has reset the product names to better align with the company vision.

v8.4 Product Name	v8.0 Product Name	Original Name
Forcepoint URL Filtering	Web Filter & Security	Web Filter Web Security

v8.4 Product Name	v8.0 Product Name	Original Name
Forcepoint Web Security	TRITON AP-WEB	TRITON Web Security Gateway
Forcepoint Web Security with: ● Forcepoint Web Security Hybrid Module ● Forcepoint Web Security DLP Module ● Forcepoint Advanced Malware Detection (if purchased)	TRITON AP-WEB with: ● Web Hybrid Module ● Web DLP Module ● Web Sandbox Module (if purchased)	TRITON Web Security Gateway Anywhere

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 8.4.

Expanded Internet access for off-site users (hybrid)

A new option that allows off-site users to access URLs that would otherwise be blocked has been added. Available only for customers who purchase the Forcepoint Web Security Hybrid module, this feature provides a new setting that can be enabled to exclude roaming users from certain policy restrictions, giving them wider Internet access when not in the office.

A new option to **Permit when user is off-site** has been added as an advanced option to the following pages of Forcepoint Security Manager:

- Web > Main > Policy Management > Policies > Edit Policies
- Web > Main > Policy Management > Filters > Edit Category Filter
- Web > Main > Policy Management > Filter Components > Edit Categories > Add Category

Select a category in the Category Filter or the Categories list. If the selected category is permitted, **Permit when user is off-site** is selected by default and disabled. If the selected category is blocked, the option is enabled. When the option is checked, a new globe icon appears next to the category to which it applies.

✓ **Note**

This option is disabled and unchecked for categories added using the Management API.

The option is also provided on the **Main** > **Policy Management** > **Filter Components** > **Edit Categories** > **Override Action** page. Specify whether or not to **Change off-site permit settings** and click **Permit when user is off-site** to enable that setting for the selected category in all filters.

- By default, **Do not change current settings** is selected.
- If **Permit** is selected in the **Action** group box, the option is disabled, with **Permit when user is off-site** selected.

When **Permit when user is off-site** is enabled for a specific category, users who would ordinarily be denied access to sites within that category are permitted access when their browsing is done off-site.

For customers with multiple Policy Servers and mixed subscription keys, the **Permit when user is off-site option** is available only when connected to a Policy Server whose key enables the hybrid service. However, changes made when connected to a Policy Server whose key does not enable the hybrid service impacts the settings for the other Policy Server's categories. For example, if PolSvr1 has a subscription key that enables the hybrid service, but PolSvr2 has a key that does not:

- When connected to PolSvr2, if the action applied to a category is changed from permitted to blocked, the same category appears with the **Permit when user is off-site** option enabled but unchecked when connected to PolSvr1.
- When connected to PolSvr2, if the action applied to a category is changed from blocked to permitted, the same category appears with the option checked and disabled when connected to PolSvr1.

Policy enforcement for cloud applications

With version 8.4, policy enforcement for cloud applications is available. The data used for Cloud App reporting (added in v8.3) is used to enforce blocking of cloud application access when users are on-premises.

A new Cloud App Agent is included with each installation or upgrade of Filtering Service or Forcepoint Security Manager. The Cloud App Agent downloads the cloud app catalog in order to provide cloud application information to Filtering Service for policy enforcement and to Security Manager for inclusion in the new cloud app filters used to define policies. Since Cloud App Agent is always with Filtering Service or Forcepoint Security Manager, it does not display on the **Status** > **Deployment** > **Component List**.

A Cloud Apps database is included with your web protection software on each Cloud App Agent machine and each Cloud App Service machine. This database of cloud applications is used to enable basic functionality from the time you enter your subscription key.

- Database updates on the Cloud App Service machine are downloaded using the Master Database download schedule.

The database on the Cloud App Service machine is used for log data and reporting.

- Database updates on the Cloud App Agent machine occur each time the Master Database is downloaded. This includes both the scheduled Master Database downloads and, when Cloud App Agent is associated with Filtering Service, when a download is initiated using the **Update** option on the **Dashboard** > **Database Download** page.

  The Cloud Apps database is also downloaded each time the Forcepoint Security Manager service (Websense TRITON - Web Security) starts. The exception to this is when Filtering Service is on-box with Security Manager. If Filtering Service is on the same machine as Security Manager, database downloads are prompted by Filtering Service restarts only.

  When Cloud App Agent starts, the latest database is loaded into memory for use with Filtering Service (for policy enforcement) or Security Manager (to provide cloud app information on the various pages).

- Health Alerts and other text messages display when one of the new services is unable to download a database, is not running, or is otherwise unable to provide cloud app information to other components as needed.

Cloud app filters

To support cloud application use as part of policy enforcement, a new selection is available on the **Main** > **Policy Management** > **Filters** page. Cloud app filters can now be defined and used for policy enforcement.

Two predefined cloud app filters are listed.

- Monitor Only -- monitors cloud application access.

  The Monitor Only filter is the cloud app filter assigned to each of the predefined policies.

- Basic Security -- defined to block cloud applications that are considered high risk.

Any new cloud app filters that have been added are also be listed on this page. To duplicate an existing filter, mark the check box next to the filter name, and then click **Copy**. The copy is given the name of the original filter with the word copy appended for uniqueness, and then added to the list of filters. Edit the copy just as you would any other filter.

Click **Add** in the **Cloud App Filters** section and use the new **Main** > **Policy Management** > **Filters** > **Add Cloud App Filter** page to create a new cloud app filter.

1. Enter a unique **Filter name**. The name must be between 1 and 50 characters long, and cannot include any of the following characters:

   ```
   * < > ` ' { } ~ ! $ % & @ # " [ ] | \ ^ + = ? / ; : . ,
   ```

Filter name can include spaces, dashes, and apostrophes.

2. Enter a short **Description** of the filter. This appears next to the filter name in the Cloud App Filters section of the Filters page, and should explain the filter's purpose.

   The character restrictions that apply to filter names also apply to descriptions, with the following exceptions; periods (.), commas (.), and brackets ([,]) can be included in descriptions.

3. Select an entry from the **Base filter on** drop-down to use to begin creating a new Cloud App Filter.

   a. Select an existing filter to make a copy of it as the basis for the new filter.

   b. Select **Blank** under **Cloud App Filter Templates** to create a completely new filter, with no pre-defined settings.

4. Click **OK** to see and edit the new filter. The filter is added to the Cloud App Filters list on the Filters page.

   Click **Cancel** to return to the Filters page without adding a new filter.

Use the new **Main** > **Policy Management** > **Filters** > **Edit Cloud App Filter** page to continue customizing the new filter or make changes to a cloud application filter.

Important

Edits to a cloud application filter affect every policy that enforces the filter.

Policies that enforce a cloud application filter with the same name in another delegated administration role are not affected.

The filter name and description appear at the top of the page.

- Click **Rename** to change the filter name.

  Note that the rename option is not available for the Monitor Only filter.

- Type in the **Description** field to change the filter description.

The number next to **Policies using this filter** shows how many policies currently use the selected filter. If the cloud app filter is active, click **View Policies** for a list of policies that enforce the filter.

The bottom portion of the page shows the details of the filter you selected. To change the way clouds apps are filtered and logged:

1. Enable **Block all high risk apps** to block access to any cloud app that is considered high risk.

2. In the **Blocked apps** list, add specific cloud apps that should always be blocked, regardless of their risk level.

   a. Enter all or part of a cloud app name in the **Search** box.

b. A drop-down list appears, containing cloud app names that qualify for the search. As text is entered, the list of qualifying apps changes to match the search criteria. Each entry includes the risk level assigned to it.

   Search results are listed alphabetically within each risk level.

c. Select the app you wish to add to the blocked list from the list provided and click **Add**.

   The cloud app is added to the blocked list.

d. Remove an app by selecting it from the list and clicking **Delete**.

The number of apps included in the list is provided above the list box. Cloud apps in the list are sorted alphabetically within each risk level.

3. In the **Permitted apps** list, add cloud apps that should always be permitted.

   a. Enter all or part of a cloud app name in the **Search** box.

   b. A drop-down list appears, containing cloud app names that qualify for the search. As text is entered, the list of qualifying apps changes to match the search criteria. Each entry includes the risk level assigned to it.

      Search results are listed alphabetically within each risk level.

   c. Select the app you wish to add to the permitted list from the list provided and click **Add**.

      The cloud app is added to the permitted list.

   d. Remove an app by selecting it from the list and clicking **Delete**.

   The number of apps included in the list is provided above the list box. Cloud apps in the list are sorted alphabetically within each risk level.

> **Important**
>
> The **Permitted apps** list takes precedence over the **Block all high risk apps** option. Access to a high risk app that is on the permitted list is allowed even if **Block all high risk apps** is enabled.

4. If an app is selected that is already included in the list, a message appears to indicate that the app is already listed.

   Click **OK** to close the message window. No further action is taken.

5. If an app is selected for inclusion in the blocked or permitted list but is already in the other list, a message displays confirming that it should be removed from the original list and added to the new list.

   Click **OK** to remove it from the original list and add it as requested. Click **Cancel** to leave both lists unchanged.

6. After editing the filter, click **OK** to cache your changes and return to the Filters page. Changes are not implemented until you click **Save and Deploy**.

> **Note**
>
> When the Edit Cloud App Filter page displays, specific information from the Cloud Apps database is included. If communication with Cloud App Agent is lost, an error appears on the page. When this happens:
>
> - New apps cannot be added to the blocked or permitted lists.
> - Some of the details for existing filters is included, but details that are specifically pulled from the database (such as risk level) will be missing.
> - Although minimal changes can be made, it is advised that you wait until Cloud App Agent can communicate with Forcepoint Security Manager.

To activate a new cloud app filter, add it to a policy and apply the policy to clients.

Delete a filter by selecting it in the list on the Filters page and clicking **Delete**. Filters that are used in a policy cannot be deleted. The Monitor Only filter cannot be deleted since it is used as the default cloud apps filter when a new policy is added.

Policies

The **Main** > **Policy Management** > **Policies** > **Edit Policy** page has been modified with a new look and feel to accommodate cloud application filters, along with category and protocol filters.

- Access to the Category/Limited Access or Protocol Filter information is now provided in a new tab format.
- Cloud application filters are now included when creating a policy.

The new Edit Policies page allows for the usual Schedule entries, including Start, End, and Days entries, as well as drop-down selections for Category/Limited Access Filter, and Protocol Filter. A new Cloud App Filter drop-down selection is also provided. Use the drop-down option provided to select a different cloud app filter.

When adding or editing a policy, you must now select the **Cloud App Filter** to enforce for each time block. Select **Add Cloud App Filter** to add a new filter to enforce in this policy.

Below the schedule section are three tabs that can be used to view the filters associated with the specific time block that is selected in the schedule.

- Open the Category / Limited Access Filter tab to view details of the filter that is enforced during the selected time block.

  If a category filter is used in the policy, the tab contents match the **Main** > **Policy Management** > **Filters** > **Edit Category Filter** page, providing:

  - The filter description.
  - The filter contents (category names with actions to be applied).

    Use the search option provided to find a specific category in the list. Note, however, that the search option is not available if either the Permit All or Block All filter is selected.
  - The number of policies that enforce the same filter.
  - A section to the right to edit the category filter by changing the action assigned to a category, or adding advanced filtering options to selected categories.

  If a limited access filter is used in the policy, the tab contents match the **Main** > **Policy Management** > **Filters** > **Edit Limited Access Filter** page include:

  - The filter description.
  - A list box containing the sites previously added to the filter.

    Use the A**dd Sites** and **Add Expressions** button to add permitted URLs, IP addresses, or regular expressions to the filter.
  - To remove a site from the filter, mark the check box next to the URL, IP address, or expression, and then click **Delete**.
  - The number of policies that use the same filter.

  See Editing a category filter or Editing a limited access filter in *Administrator Help* for additional details.

- Select the Protocol Filter tab to view details of the protocol filter enforced for the time block.

  The detail section matches the **Main** > **Policy Management** > **Filters** > **Edit Protocol Filter** page, providing:

  - The filter description.
  - The filter contents (protocol names with actions to be applied).

    Use the search option provided to find a specific protocol in the list. Note, however, that the search option is not available if either the Permit All or Block All filter is selected.
  - The number of policies that enforce the same filter.
  - A section to the right to edit the filter by changing the action assigned to a protocol, or adding advanced filtering options to selected protocols.

  See Editing a protocol filter in *Administrator Help* for additional details.

- Open the Cloud App Filter tab to view details for the filter that is enforced during the selected time block.

  The detail section matches the **Main** > **Policy Management** > **Filters** > **Edit Cloud App Filter** page described earlier in this document.

  - The filter description.
  - The filter contents (**Block all high risk apps** checkbox and blocked and permitted apps lists).

    Enable or disable the checkbox and use the search options provided to find a specific cloud app for inclusion in either list.

    - The number of policies that enforce the same filter.
- When you finish editing a policy, click **OK** to cache your changes. Changes are not implemented until you click **Save and Deploy**.

> ✓ **Note**
>
> When you edit any filter from the Edit Policies page, the changes affect every policy that enforces the filter. Before editing a filter that is enforced by multiple policies, click the **This filter is active in** link to see which policies will be affected.

Note that the filter names and descriptions cannot be changed from the Edit Policies page. Those options are available only by accessing the filter directly from the **Main** > **Policy Management** > **Filters** page.

As usual, select a policy and click Delete to delete a policy.

> ✓ **Note**
>
> Audit log entries for changes that involve cloud app filters include details in the Type, Previous, and Current columns that may not be useful.

Delegated administration with cloud app filters

Cloud app filters are also available to delegated administrators.

- When a new delegated administration role is added, all Super Administrator cloud app filters are copied to the role when the **Copy all Super Administrator policies, filters, and filter components to the new role** is selected.
- On upgrade, the new action codes specific to cloud app enforcement are added to each delegated administration role.
- On the **Main** > **Policy Management** > **Filters** page, mark the check box next to a cloud app filter name and then click **Copy to Role** to copy the filter to a specific delegated administration role.

  Cloud app filters are also included when a policy is copied using the **Copy to Role** feature available on the **Main** > **Policy Management** > **Policies** page.
- The **Move to Role** option available on the **Main** > **Policy Management** > **Clients** page has also been modified to include cloud app filters with the new policy when a client is moved to a new role.

Enforcing policies with cloud app filters

To support the new cloud app enforcement, new action codes have been added. These actions are included in investigative reports, presentation reports, and the dashboard charts.

- Cloud app permitted

- Cloud app blocked
- When policies are enforced, the details provided in the cloud app filter are used to permit or block access to a request before category filters are applied. Policy exceptions assigned to the user are applied first. If no exception applies to the request, the appropriate policy is applied.
- The cloud app filter assigned to the policy is applied first.
  - If a specific cloud app is explicitly blocked or permitted, the request is blocked or permitted based on the cloud app filter.

    If a cloud app is explicitly permitted or blocked, additional lookup against the URL category is done to get category information for use in reporting and to confirm the URL is not assigned to a category in the Security Risk class.

    - If the cloud app is explicitly permitted or blocked but the URL is in a blocked Security Risk category, the request is blocked as a security risk.
    - If the URL is in a category that is not part of the Security Risk class, and the cloud app is explicitly permitted, the request is permitted even if the category is blocked.
    - If the URL is in a category that is not part of the Security Risk class, and the cloud app is explicitly blocked, the request is blocked even if the category is permitted.
  - If **Block all high risk apps** is enabled and the cloud app is considered high risk, the request is blocked unless the cloud app is explicitly permitted.

    If a cloud app is considered high risk, additional lookup against the URL category is done to retrieve category information for use in reporting and to determine if the category is assigned to the Security Risk class.

    - If the cloud app risk level is high, but the URL is in a blocked Security Risk category, the request is blocked as a security risk.
    - If the cloud app risk level is high, but the URL is not in a category that is part of the Security Risk class, the request is blocked based on the cloud app filter.
  - If the cloud app filter assigned to the policy being applied does not list the cloud app as specifically blocked or permitted, and **Block all high risk apps** is not enabled, enforcement is done using the category filters assigned to the policy.

When a cloud app is explicitly blocked, the block happens prior to further lookup and the request is assigned the new “Cloud app blocked” action code. Requests for cloud apps that are explicitly permitted are assigned the new “Cloud app permitted” action code only when, after the URL lookup, no further reason is found to block the request

See the Enforcement order in *Administrator Help* for further details.

New block pages have been included to better handle cloud app blocking. As with category block pages, the cloud app block pages can be customized. See the Creating Custom Block Pages for details.

✓ **Note**

The Password Override and Account Override options assigned to clients and available for category block pages are not available for the new cloud apps block pages.

✓ **Note**

When an application that should be blocked is installed and accessed locally, access to the application is blocked but the client may experience unusual behavior. For example, if the application continues to attempt to launch, a new block page will be presented.

Enhancements to Cloud App reports

To incorporate the new cloud application enforcement feature and provide better usability, enhancements have been made to the report on cloud apps use found on the **Cloud Apps** tab of **Main** > **Reporting** > **Applications.**

- The filters used to determine the content of the Cloud App or Cloud App user reports have been relocated to the left of the report. This makes it easier to understand the impact of the filters.
- New filter options have been added to each report.
  - Requests

    Select **Blocked**, **Permitted**, or both to report on a specific set of requests.
  - User Access (available with the Hybrid Module for Forcepoint Security Manager)

    Select **On-site** to report on user requests that are managed in network or **Off-site** to report on requests made by roaming users. Select both to report on all requests, regardless of where they are managed.

✓ **Note**

Cloud app records that exist in the Log Database when an upgrade to v8.4 is done will be marked as On-site.

The linked pages (User Summary Report and Cloud App Summary) automatically use the Time period, Requests, and Users access filters selected on the main Cloud Apps page.

- For usability, if all boxes in the filter are checked, all data is included in the report. Similarly, if all boxes are unchecked (the default), all data is included. Mark a check box to filter the data in the report.
- The search entry box for each report page includes hint text explaining what the search will consider. For example, text entered for search on the Cloud app report is used to search the values in the Cloud App and Type columns.
- For consistency, the sort for all cloud app reports in table format is the last accessed date. The Cloud app table sorts first by Risk level.
- The report now includes details for on-site requests that were explicitly blocked by a Cloud app filter, and requests handled by the hybrid service (requires the Forcepoint Web Security - Hybrid Module).
- Additional columns have been added to the User Summary and Cloud App Summary reports to provide details for on-site and off-site cloud app requests, as well as blocked and permitted requests.
- Users who access the same cloud app through both the hybrid services and on-premises components (Filter Service and Content Gateway) now appear only once in the report. Separate requests are listed as on-site or off-site.
- Top 10 charts options have been changed to stacked column or stacked bar charts so that additional information can be included.

  Similarly, Usage Trend chart options are now multi-series line, stacked area, or stacked column.
- Hover over any data point or bar on a chart to view details of the value being charted.
- Pressing **Enter** is now an alternative to clicking **Search** when using that feature on the Cloud App or Cloud App User report.

  Note that you still need to click **Search** to use the feature on the User Summary Report and Cloud App Summary.
- The **Users Accessing** table that is part of the **User Summary Report** now offers the **User** entry as a link that opens an Investigative Report with more details for the browsing being done by that user on the date in the **Last Accessed** column.

  The link is available only to delegated administrators with permission to “access investigative reports”.
- Files created using the **Export to CSV** option available on the various report pages include data for the new columns added to the reports.

  In addition, the filenames contain the date and time the file was created.

  For example, an export from the Cloud App page now creates a file in the format cloudapps_yyyyMMdd_HHmmss.csv.
- To help avoid issues when exporting large amounts of data to CSV, the default timeout value has been updated to 30 seconds.

  ■

Authentication cookie sharing (Content Gateway)

Authentication credentials cached with cookie surrogates can now be shared across all nodes in a cluster.

Prior to v8.4, when cookie mode caching is enabled, after a user is authenticated, the cookie for that user is later used for subsequent authentication attempts through the same Content Gateway machine. Requests by that same user that go through a different proxy require the user to provide a name and password.

With 8.4, when cookie mode caching is enabled, after a user is authenticated the cookie for that user can be used for subsequent authentication attempts by any of the proxies that are clustered with the proxy that did the initial authentication. This feature is especially useful in load balanced environments.

Cookie sharing is enabled on the **Configure** > **Security** > **Access Control** > **Global Authentication Options** page of Content Gateway manager.

- Enable either **Cache using Cookies only** or **Cache using both IP addresses and Cookies** in the Caching Method section of the page.

  Note that all proxies in the cluster must use the same caching method when cookie sharing is enabled.

- In the new Cookie Sharing section
  - Select **Enabled** to enable the feature.

    When cookie caching is enabled, this feature is automatically enabled.

    > **Note**
    >
    > Upgrades to v8.4 will automatically enable this feature if cookie caching has been enabled on the earlier version.

    Enabling the setting in the UI also updates a new parameter in records.config.

    ```
    proxy.config.auth.sharecookie
    ```

    Do not edit the config file to enable this feature. Use the UI setting.

  - Select **Choose File** for both Public and Private keys to import your own keys for use with this feature. Browse to the file you want to use and select it. Files must be in PEM format.

    The same keys must be imported for each proxy in the cluster.

  - After selecting each file, click **Import Keys** to import custom keys (recommended) and store them in the default location.

    Note that default keys are provided and are added when the product is installed or upgraded. The default file names and locations are:

    /opt/WCG/config/cookie_auth_public.pem

    /opt/WCG/config/cookie_auth_private.pem

Select the files you wish to import. The custom keys are automatically copied to this folder and renamed to the default names.

Important

When custom keys are imported, the default files provided by Forcepoint are overwritten. You should backup the default keys prior to importing. See **Save Public Key** and **Save Private Key** below.

Keys must be PKCS#1 RSA public keys and are RSA 1024/2048/4096 bit public and private key pairs without a passphrase. Use the following commands to generate keys:

```
openssl genrsa -out cookie_auth_private.pem 1024
```

```
openssl rsa -in cookie_auth_private.pem
-RSAPublicKey_out -out cookie_auth_public.pem
```

Change 1024 to 2048 or 4096 to generate 2048 or 4096 bit keys.

- Select **Save Public Key** and **Save Private Key** to make a backup of the files.

  Select the location and filenames to use for the backup copy, keeping in mind that the default names are always used for the active keys.

  Key files should be backed up prior to importing new keys.

When load balancing has been configured, all proxies must use the same setting for proxy.config.http.transparent_auth_hostname in records.config. The value must be the fully qualified domain name (FQDN) of the load balancer and can be configured on the **Configure** > **Security** > **Access Control** > **Global Configuration Options** page of Content Gateway manager. Enter the FQDN as the **Redirect Hostname**.

It can also be configured manually (not recommended) by updating records.config. For example, use the following command to set the value:

```
LOCAL proxy.config.http.transparent_auth_hostname STRING
loadBalancer.tcs.com
```

where loadBalancer.tsc.com is the FQDN of the load balancer.

Note the following feature limitations:

- Cookie caching limitations also apply to cookie sharing. Therefore, since cookie caching is not supported for CONNECT requests, cookie sharing is not supported.
- Custom keys must be imported manually using Content Gateway manager for each proxy in the cluster. Custom Keys are not synchronized across the cluster.
- Cookie sharing is not supported with client certificate authentication.

Automatic updates to Certificate Authority Tree (Content Gateway)

When installed, Content Gateway initially populates the Certificate Authority Tree (trusted certificate store) with the list qualified by Mozilla for Firefox, by Microsoft for Internet Explorer, and by Apple for Safari.

With version 8.4, the information in CA Tree is automatically updated on a regular basis as well as each time Content Gateway is restarted.Updating the CA tree avoids the potential for using a root CA that has expired, is no longer a root CA, or if the certificate revocation list URL of the root CA has changed.

The update process inserts new trusted CAs and updates existing CAs that have updated certificate revocation lists, and at the same time removes expired CAs, any CA that is no longer a root CA, and non-trusted CAs.

✓ **Note**

The update process maintains only Public certificates. Customers are responsible for maintaining Private certificates.

Enabled by default, the feature can be disabled by editing records.config using this command:

```
CONFIG proxy.config.ssl.catree_update INT 0
```

Restart Content Gateway after making this change.

Reset the value to 1 to re-enable the updates.

To avoid file corruption, checks are in place to confirm the availability and health of each new update. Update attempts that fail generate an informational alarm. The existing set of certificates continues to be used until the next successful download.

This feature:

- Requires SSL decryption to be enabled.
- Does not check existing certificate revocation lists during the update process.
- After upgrading to v8.4, when the initial CA Tree update occurs, CAs in the customer deployment but not in the 8.4 CA db, any CA that is no longer a root CA, and CAs that are no longer trusted are converted to a private CA. This process also removes expired CAs.

  After the initial update, review the CA Tree and remove any certificates that are no longer trusted or may be revoked.
- Does not re-add CAs explicitly removed by a customer.
- When an update is in progress, provides a warning on the **Configure** > **SSL** > **Certificates** pages that changes made when the update is running are lost. The

same message appears when a backup or restore is attempted.

Direct Connect Endpoint (hybrid)

A new Direct Connect Endpoint (DCEP) is available for Forcepoint Web Security customers who purchase the Forcepoint Web Security Hybrid Module. (Note that the existing web endpoint is now called Proxy Connect endpoint.)

DCEP can be enabled by hybrid customers and DCEP client software is then included using **View Files** in the Forcepoint Web Security Endpoint section of the **Settings** > **Hybrid Configuration** > **Hybrid User Identification** page of Security Manager.

They hybrid service authentication reports now include DCEP and Policy Connect Endpoint as separate entries.

✓ **Note**

Some of the details provided on the authentication report are not available for DCEP connections.

This new endpoint is appropriate if:

- A geographical firewall prevents proxy use; for example, due to a national firewall or local network security system.
- Localized content is critical; for example, the customer's marketing organization translates content into many languages.
- The customer has complex networks and changing network connections; for example, the customer has a large remote workforce and traveling consultants.

Communication is established between the endpoint and the proxy, and when DCEP detects the proxy, it confirms that the endpoint and the proxy belong to the same customer and authenticate with each other. Then, endpoint puts itself into Standby mode and allows Forcepoint Web Security to provide policy enforcement for clients in the network.

The Content Gateway installation process has been updated to include **Endpoint Authentication Server port** in the list of configurable port assignments.

For additional information about Direct Connect and Proxy Connect endpoints, see the Endpoint Installation Guide.

SIEM enhancements

Hybrid data sent to SIEM solution

In earlier versions, hybrid log data forwarded to Log Server by Sync Service was not also forwarded to a configured SIEM solution. With v8.4, hybrid log data is forwarded to the **SIEM Integration** configured on the **Settings** > **General** page.

Enhancement to SIEM integration support

In previous versions of the product, a different SIEM solution could be configured for each Policy Server using the **Settings** > **General** > **SIEM Integration** option. Data handled by the Filtering Services associated with that Policy Server would be forwarded to that SIEM solution.

With v8.4, data for each Policy Server (including those without a SIEM solution) is sent to all SIEM solutions configured for other Policy Servers assigned to the same Policy Broker. This is true whether Policy Server was installed and assigned to a specific Policy Broker, or Policy Server was connected to a Policy Broker using the **Web** > **Settings** > **General** > **Policy Broker** page of Security Manager.

Miscellaneous SIEM enhancements

Additional enhancement have been made to Forcepoint Web Security SIEM integration.

- The login ID string has been added to the data that is forwarded to each SIEM solution. Add the login ID to customized SIEM format strings using the key loginID.
- Data that is specific to cloud app enforcement can be included in the data forwarded to each SIEM solution.

  Add the following keys to your format string to include cloud app details:

  - cloudAppName is the name of the cloud application requested.
  - cloudAppID represents an internal ID assigned to the application.
  - cloudAppRiskLevel is the risk level (high, medium, or low) assigned to the application.
  - cloudAppType is the type of cloud application requested (for example, Finance).

Content Gateway enhancements

Enhancements have been made to Content Gateway to improve usability.

- The Content Gateway manager has been updated to accommodate customers who require more than 8 ports for a WCCP service group.

The file editor accessed from the **Configure** > **Networking** > **WCCP** page now provides two options for **Ports**.

  - Select **Specify ports** to enter up to 8 ports in a comma separated list.
  - Select **All ports** to redirect traffic from all ports.

  A reminder that there must be a corresponding ARM rule for every port specified in an enabled WCCP service group is provided.

- Some Content Gateway authentication methods now support the use of @ in the user name.

  In earlier versions, if you selected an authentication method on the **Configure** > **My Proxy** > **Basic** page of Content Gateway Manager, and added users to your directory service in the format user1@mycompany.com, authentication would fail. Authentication would be successful only if the same users were entered in the format user1_mycompany.com.

  New options are now available that allow the user1@mycompany.com format.

  When using rule-based authentication and adding a **New Domain** on the **Configure** > **Security** > **Access Control** > **Domains** page with the LDAP **Authentication Method**, the available LDAP Server Types are now:

  - sAMAccountName (MS AD)
  - userPrincipleName (MS AD)
  - uid (Other LDAP)

  When the selected authentication method is LDAP, and adding an LDAP Server on the **Configure** > **Security** > **Access Control** > **LDAP** page, the available Server Types are now:

  - Microsoft Active Directory (sAMAccountName)
  - Microsoft Active Directory (userPrincipleName)
  - Other

  In both cases, userPrincipleName supports the user1@mycompany.com format.

- A new variable in records.config has been added so that all websites added to the SSL Incident List using the **By Certificate** option work as expected.

  When an SSL website is requested without an SNI (server name indication), the Common Name in the website's certificate may not match the URL hostname. When that happens, future requests to the same website will not match the SSL Incident database.

  To force the proxy to add an outbound SNI (server name indication), enable the following variable:

  ```
  proxy.config.ssl.client.set_sni INT 1
  ```

- Browser limitations require configuring a specific port in order for certain Content Gateway graphs to display properly. To avoid any issues, the **Monitor** > **My Proxy** > **Node** and **Monitor** > **My Proxy** > **Graphs** pages on Content Gateway manager will be disabled until a port is specified in records.config (in /opt/WCG/config, by default).

  Update this variable to enable the Node and Graphs pages:

  ```
  proxy.config.admin.overseer_port INT ##
  ```

where ## is a valid port number.

A restart of Content Gateway is required for this variable to take effect.

Customers using an appliance should contact Technical Support for assistance with the port change.

- To better support deployments that include Forcepoint DLP, new variables have been added to records.config.

  ```
  proxy.config.dss.large_file_threshold
  proxy.config.dss.analysis_timeout_for_large_file
  ```

  With these settings, a default value of 5MB (large_file_threshold) is used to determine how large a file should be before a longer period of time than the current default of 10 seconds is given for analysis time. With this setting, any file larger than 5MB is given, by default, 20 seconds (analysis_timeout_for_large_file) for analysis.
- POST requests received from Google Chrome are now being authenticated as expected.
- Content Gateway now parses the Content-Disposition header to extract the filename from it.

  ■

Reporting optimizations

Changes have been made to some of the reporting components, including the Log Database and Log Server, to provide improved functionality for logging and reporting.

- Since newer versions of Google Chrome block Flash content, reporting components have been updated to remove the use of Flash widgets.
- Real-time Monitor has been updated to use a more recent version of Java. No changes to functionality were made.
- The Log Database has been enhanced to support the new policy enforcement for cloud applications feature and the corresponding reporting feature.

  Note that customers who currently use custom reporting tools may be impacted by the Log Database schema changes.

General enhancements

Changes have been made in order to make the product more user friendly and to better protect our customers.

- (Hybrid) To help avoid hybrid log data loss:
  - The Sync Service Communication Results table on the **Main** > **Status** > **Hybrid Services** page has been redesigned to provide additional information.

- ■ Health Alerts have been updated to provide new warnings when there are issue with Sync Service.
- ■ The **Collect and Retrieve Reporting Data** section of the **Settings** > **Hybrid Configuration** > **Scheduling** page has been updated with additional text and warnings to explain the dangers of changing the default values.

  In addition, values of 5 and 10 minutes have been added to the **Retrieve data every** drop-down selections. Default internal settings used for data retrieval have also been modified to allow for a more complete download of hybrid log records.

- The **Apply to Subcategories** and **Apply to Group** options used when editing category filters, protocol filters, and filter lock options have been relocated on their respective management console pages to better indicate their full functionality.
- The **Aggressive analysis** option for **Antivirus Scanning** in the Security Threats: File Analysis section of **Settings** > **Scanning** > **Scanning Options** is now enabled by default. Antivirus analysis is applied to inbound files, increasing the protection that Forcepoint Web Security provides.

  This setting is not be changed by the upgrade process.
- The **Print Policies To File** option available on the **Main** > **Policy Management** > **Policies** page has been updated to include both policy exception and cloud app filter details.

Install and upgrade improvements

Improvements have been made to the installation and upgrade screens and process.

The Web Hybrid Module Components screens has been re-organized to make it more intuitive.

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.

Removed in this version

Technical support for Windows Active Directory in mixed mode ends with v8.4. Forcepoint Web Security and Forcepoint URL Filtering continue to offer mixed mode as a directory service option.

Functionality will be removed in the next release. It is recommended that customers currently using Window Active Directory in mixed mode move to a different directory service.

See Product Support Life Cycle for additional information about planned support of existing products.

Third-party platform and product support

All components

This version adds support for:

- Microsoft Windows Server 2016
- Microsoft SQL Server 2014, SP2
- Microsoft SQL Server 2016

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 Linux 7.0, 7.1, 7.2, and 7.3 (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
> ```

- Red Hat Enterprise Linux 6 series, 64-bit, Basic Server (and the corresponding CentOS versions).
  - Version 6.8
  - Version 6.7
  - Version 6.6
  - Version 6.5

> **Note**
>
> Product testing encountered a kernel bug in version 2.6.32-431 that can impact performance. However, Content Gateway features were tested on this version of the OS and passed the certification tests.

- V-Series appliances

> **Important**
>
> Customers currently using Red Hat Enterprise Linux 6.3 or 6.4 will need to upgrade their operating system prior to upgrading the product.

“Best effort” support for the version of Red Hat Enterprise Linux and CentOS listed above is provided. Under “best effort” support, Technical Support makes a best effort to troubleshoot cases in standard fashion until the issue is deemed a Red Hat Enterprise Linux- or CentOS-specific issue, at which point you must contact Red Hat directly for assistance.

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 |31-Jul-2017

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