Web Security Cloud

Evaluation Guide

Revision A

Published 12 August 2024

Contents

Chapter 1

Starting your evaluation

Contents

Introduction

Thank you for choosing to evaluate Forcepoint Web Security Cloud.

This guide has been created to help you get the most out of your evaluation. It will help you get up and running with the service quickly, enabling you to trial Web Security Cloud's dynamic inbound and outbound web protection and analysis features.

For many organizations, use of the web is an intrinsic part of an employee's daily activity. At the same time, web threats are more sophisticated and complex than ever before. Many websites are highly dynamic, and traditional web security systems are unable to protect against a constantly evolving threat landscape. Forcepoint Web Security Cloud is built around the dynamic nature of the modern web, using real-time categorization and threat data, enabling businesses to leverage web-enabled productivity without sacrificing security and control.

Forcepoint Web Security Cloud enables you to:

- **Reduce business costs and complexity** with no on-site equipment to install or maintain, low administrative overhead, and built-in scalability for web gateway consolidation.
- **Increase protection** using Forcepoint's Advanced Classification Engine (ACE), ThreatSeeker Intelligence, and CASB to safely leverage the power of modern web tools.

  ACE offers contextual awareness, composite risk scoring, and multi-layered, real- time analysis of inbound and outbound web content with data-aware defenses for data theft protection.

  ThreatSeeker Intelligence continuously monitors web content for emerging threats, analyzing up to 5 billion requests per day. It feeds this intelligence to our advanced protection systems, allowing Forcepoint solutions to adapt quickly to a rapidly changing threat landscape.

  Forcepoint CASB is an integrated solution for cloud application access discovery, activity analysis, access control, security monitoring and enforcement, governance, policy compliance, and data loss prevention. CASB features are integrated into Web Security Cloud, allowing you to monitor and protect the use of cloud apps in your organization.
- **Retain control** with 24/7 access and flexible customization of policies, configuration settings, and reporting.

Requesting a free trial

Before you begin

You can request a demo of any Forcepoint product, or sign up for a free trial, via the Forcepoint website. To sign up for a trial:

Steps

1) Go to https://www.forcepoint.com/free-trials-demos
2) Under Web Security, select **Forcepoint Web Security Cloud Trial**.
3) If you already have a forcepoint.com account, log on using your account details. If you do not have an account, click **Register** and follow the steps to enter your details.
4) On the Registration page, fill out the request form and read the Evaluation Details information, then click **Continue**.
5) When prompted, read and accept the terms and conditions, then click **Confirm** to initiate the evaluation process.

Next steps

Shortly after you click **Confirm**, you will receive an email message containing links to the following:

- Forcepoint Cloud Security Gateway Portal (also referred to as the cloud portal)
- Forcepoint Web Security Cloud Getting Started Guide
- Support options.

If you are new to Forcepoint cloud-based products, the message also includes your portal username and a temporary password. You will be asked to change the password the first time you log on.

If you are already a Forcepoint cloud customer, Forcepoint Web Security Cloud is added to your account. Use your existing credentials to log on to the portal.

If you prefer to talk to a representative immediately, inside the U.S., call 1-800-723- 1166. Outside the U.S., please visit https://www.forcepoint.com/partners/find-a- partner to locate a reseller.

Getting set up

Once you have registered your trial account and received your logon credentials, access the cloud portal via:

https://admin.forcepoint.net/portal

Refer to the Web Security Cloud Getting Started Guide for help with setting up your account, using the intuitive cloud web setup wizard.

Once you have completed the setup wizard, you will have a default policy that applies a standard set of enforcement actions to all users in your organization. You can tailor your configuration as required, by:

- Creating different policies to control traffic from different egress IP addresses that you manage (for example, different branch locations).
- Setting your policies to identify/authenticate individual users
- Assigning users and groups to specific policies, allowing you to create separate policies for different departments.
- Creating category exceptions for specific users and groups, defining override settings for some users within the policy.
- Setting proxy bypass destinations to allow direct access for trusted sites and applications that do not need to use the cloud proxy.

For detailed information on any aspect of Forcepoint Web Security Cloud, refer to the Forcepoint Web Security Cloud Help, available on the Support site.

Chapter 2

Working with Forcepoint Web Security Cloud

Contents

Introduction

To help you get the most of Forcepoint Web Security Cloud, this section offers an overview of key product features, with configuration instructions where appropriate.

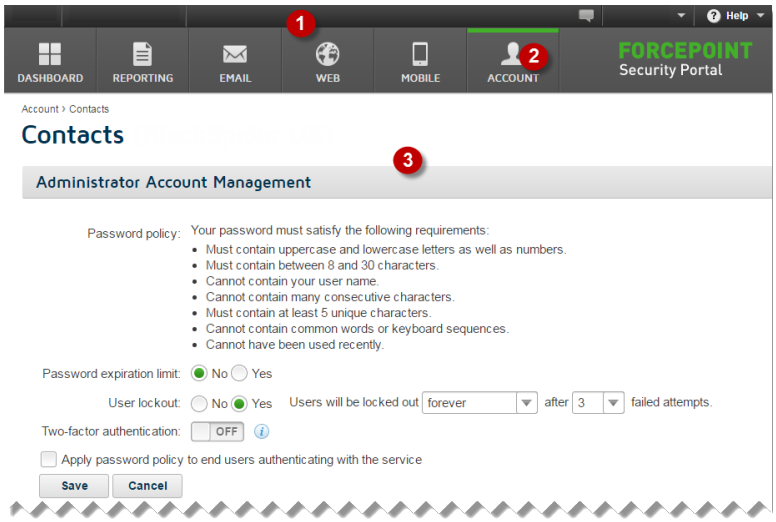
Use the following sections to learn more about what the product offers and try out its features.

Related concepts

Navigating the cloud portal on page 9
Using cloud portal dashboards on page 11
Configuring real-time malware analysis on page 12
Assigning actions to web categories on page 13
Configuring Data Security settings on page 15
Managing block and notification pages on page 17
Setting time periods on page 17
Deploying Forcepoint Web Security Endpoint on page 18
Using reporting tools on page 18
Next steps on page 19

Navigating the cloud portal

The cloud portal interface is divided into the following main areas:



1) Banner

2) Toolbar

3) Content pane

The **banner** shows:

- Any **alerts** or information messages that are available for your account. These include details of planned maintenance, and product release announcements.
- Your current **logon account**. When you're ready to end your administrative session, click the arrow next to the administrator name and select **Log Off**.
- The **Help** menu, from which you can access assistance for the page you are currently viewing, further product information, and Technical Support resources. The Help menu also includes:
  - A **Support PIN**, which must be used to authenticate your account when calling Technical Support.

    Each PIN is unique per portal user, and is generated when a user logs on. The PIN is valid for 24 hours after logon. After the 24-hour period has expired, a new PIN is generated at the next portal logon.

    Important

    In order to preserve and maintain the security of your data, Support representatives will not be able to provide customer support without a valid, up-to-date PIN.

  - Links to **Privacy & Security** information, including the Forcepoint, DLP, and security privacy policies and security and privacy-related product certifications.

The toolbar indicates which section of the cloud portal is currently active:

- **Dashboard** provides access to threat, productivity, bandwidth, and data security dashboards. See *Using cloud portal dashboards*.
- **Reporting** gives access to all reporting options, including account service reports, your saved reports, and the Report Catalog and Report Builder. See *Using reporting tools*.
- **Web** contains configuration and policy management settings for your web protection product. See:
  - *Configuring real-time malware analysis*
  - *Assigning actions to web categories*
  - *Managing block and notification pages*
  - *Setting time periods*

- *Using reporting tools*

- **Account** provides access to options that apply to all cloud services, including administrator management, directory synchronization, licenses, and groups.

When you select an item in the toolbar, a **navigation pane** drops down, containing the available navigation choices for that item. Click the toolbar item again to close the navigation pane.

The **content pane** varies according to the selection you make in the navigation pane.

Related concepts

Using cloud portal dashboards on page 11
Using reporting tools on page 18
Configuring real-time malware analysis on page 12
Assigning actions to web categories on page 13
Managing block and notification pages on page 17
Setting time periods on page 17

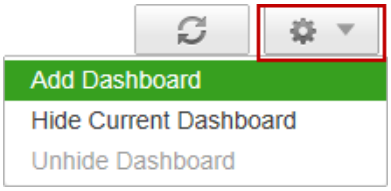
Using cloud portal dashboards

The dashboard provides a snapshot view of Forcepoint Web Security Cloud activity. To view your dashboard, click **Dashboard** on the cloud portal main menu bar.

- The **Threat Dashboard** appears when you first access this page. It shows information about suspicious activity that may be related to malware threats in your network.

- The **Bandwidth Dashboard** shows information about traffic patterns in your network, including the categories, groups, and users consuming the most bandwidth.
- The **Productivity Dashboard** shows information about blocked requests, and activity in social media categories.
- The **Cloud Apps Dashboard** shows information about cloud app usage, by category and risk level.
- The **Data Security Dashboard** shows information about data loss and data threat incidents, including a timeline, incidents by content type, and top sources, destinations, and categories associated with incidents. See *Configuring Data Security settings*.

In addition to the predefined dashboards, you have the option to add up to 10 custom dashboards. To add a dashboard, click the Settings icon on any dashboard page, then click **Add Dashboard**.



Provide a name for the new dashboard, then use the Settings menu to populate your custom dashboard with up to 6 charts. You can either define new charts by selecting attributes, or use an existing report as the basis for creating new charts.

Each dashboard includes the following features:

- A number of charts that provide detailed web activity information. Most dashboard charts can be customized to change their display format (for example stacked column, area chart, line chart, bar chart, or pie chart).
- A summary statistic in the top left that covers web activity relevant to the current dashboard over a defined time period (the last day by default). You can select a different time period from the drop-down list: the alternative options are 1 hour, 4 hours, 8 hours, 12 hours, 3 days, 5 days, and 7 days.
- One or more filters that define the range of content shown in the charts.

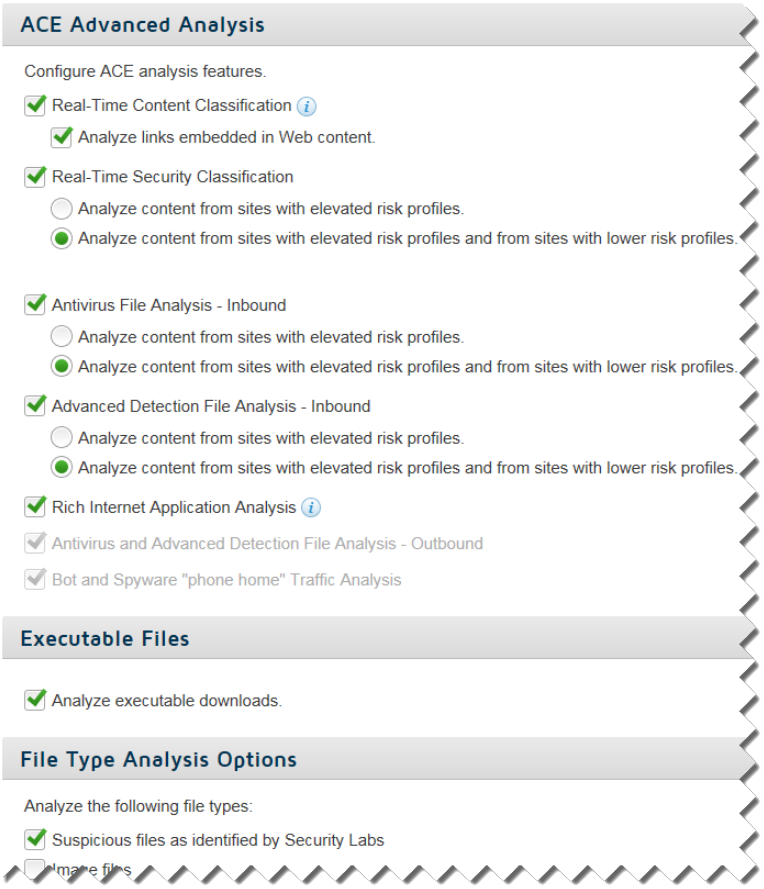
Related concepts
Configuring Data Security settings on page 15

Configuring real-time malware analysis

Forcepoint Web Security Cloud analyzes web content and detects threats using the Forcepoint Advanced Classification Engine (ACE). ACE provides inline, real-time composite defense assessments and adjusts your protection dynamically using on-the- fly content classification. You can configure how ACE analysis is performed in your web protection policies.

You can choose to protect your organization from inbound or outbound malware and executables. If you choose to block executables, any file whose contents appear to be executable is blocked. When a file upload or download is blocked, the user is presented with the notification page you select. This gives you peace of mind that the network remains uninfected while enabling employees to harness the business value of the dynamic web.

To view and edit the current protection rules for a policy, click the **Web Content & Security** tab.



Assigning actions to web categories

Forcepoint Web Security Cloud uses the Forcepoint URL Database to categorize websites. This database is the industry's most accurate, current, and comprehensive classification of URLs. A combination of proprietary classification software and human inspection is used to categorize and maintain URLs to ensure protection against today's blended threats. Content is sourced by our ThreatSeeker Intelligence network, global researchers around the globe, and customer submissions.

In web protection policies, each URL database category is associated with an **action**. The action tells the policy how to respond to user requests for websites in that category.

The available actions are:

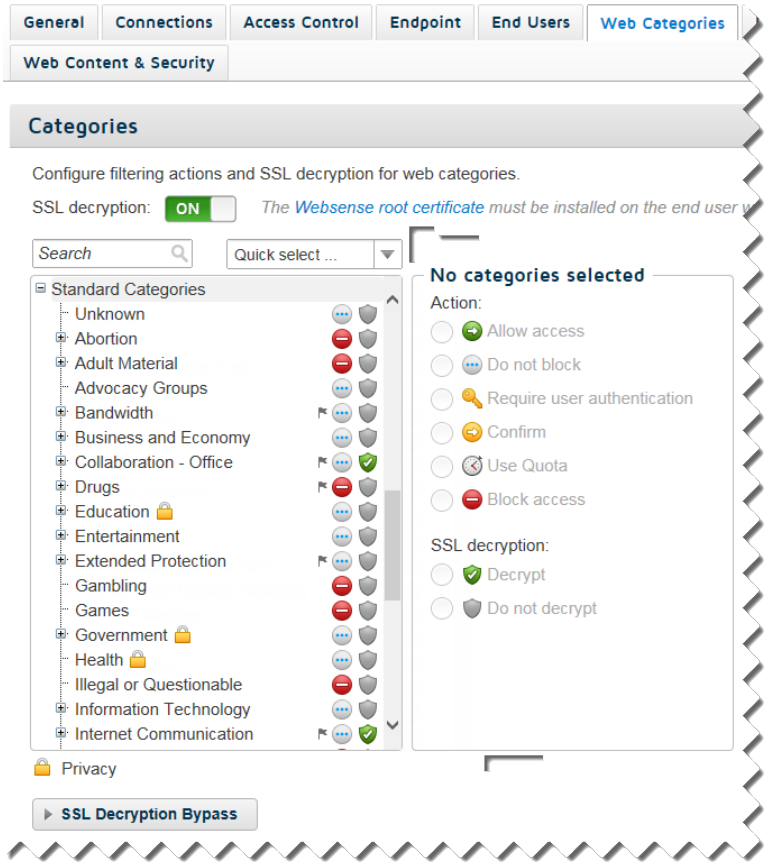
- **Allow access**: Ensures that websites within the category are always accessible.
- **Do not block**: The website is not blocked as part of this category, but can be blocked if it exists in another category that has the Block access action assigned.
- **Require user authentication**: Users must identify and authenticate themselves in order to access the site. This ensures that administrators can monitor who is accessing sites in the category.
- **Confirm**: Users receive a block page that prompts them to confirm that the site is being accessed for business purposes. Users who click **Continue** can access the site.
- **Use Quota**: Users receive a block page that asks them whether to use quota time to view the site. Users who click **Use Quota Time** can view the site for a predefined period.
- **Block access**: Users cannot access the site unless it also exists in another category that has been assigned the Allow access action.

In addition to assigning actions to categories, you can define whether or not encrypted websites within a category are decrypted for analysis. Depending on your account, this may allow:

- HTTPS traffic to be inspected to ensure the correct notification or authentication page is delivered to the end user
- HTTPS traffic in categories that you specify to be analyzed for malware and other threats.

To enable SSL decryption, switch the toggle at the top of the Web Categories tab to **ON**. Next, specify categories to be decrypted for analysis.

To view the current categories for a policy, click the **Web Categories** tab.



Creating a custom category

You can set up your own custom categories, for example to allow access to specific websites without allowing access to the whole category that they belong to, or to block certain sites without blocking the whole category.

To create a custom category:

Steps

1) Go to the **Web** > **Policy Management** > **Custom Categories** page.

2) Click **Add**.

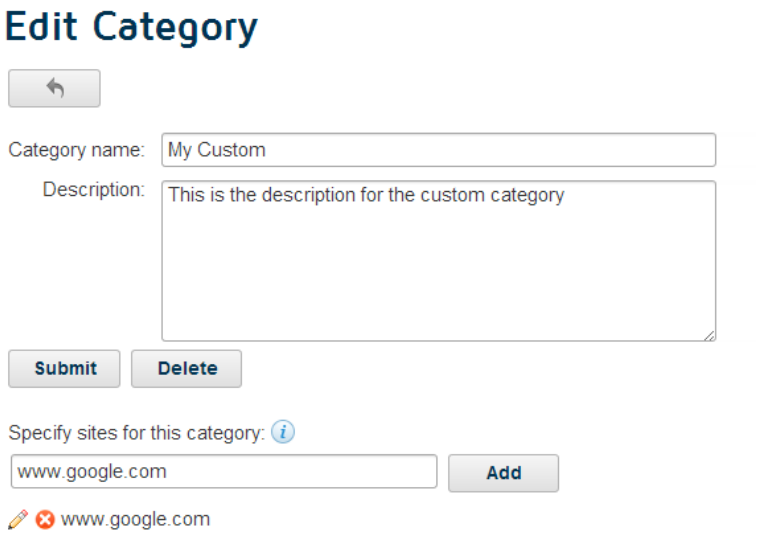
3) Enter a name and a description for your new category.

4) Click **Submit**.

5) In the **Specify sites for this category** field, type the address of a website (for example, www.google.com).

6) Click **Add**.

7) Repeat steps 5 and 6 for each site that you want to add to the category.



8) Click **Submit**.

9) Return to the Web Categories tab in your selected policy, and click the custom category you just created. On the page that appears, you can set the disposition for your new category, and add any user or group exceptions.

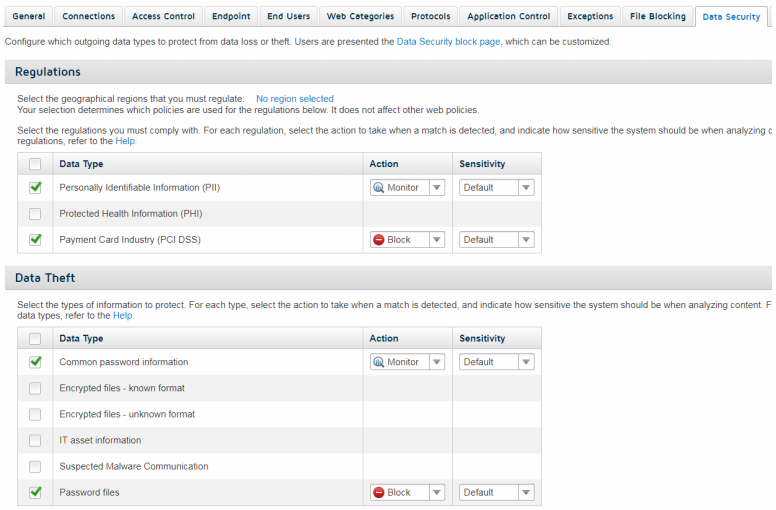
Configuring Data Security settings

For each policy that you create, you can enable data security monitoring and configure the types of data loss and data theft activity that you want to detect. You can use data security monitoring to detect:

- Violations of standard regulatory policies
- Data theft involving predefined types of information
- Web communication involving specific, custom phrases or patterns that may indicate transmission of sensitive or proprietary data.

Configuring data loss and data theft detection settings

Open a policy and select the **Data Security** tab to configure data loss and data theft detection settings.



To configure data loss and data theft detection settings:

Steps

1) To enable regulation-based data loss detection, click the link next to **Select the geographical regions that you want to regulate**, then select one or more regions in the pop-up window.

2) Select the check box next to one or more types of regulation.

   Details about each regulation type are available in the cloud portal Help. Click **Help** > **Explain This Page** to open the Help system, then select **Data Security Content Classifiers** in the left navigation pane (near the bottom of the Contents tree).

3) Under Data Theft, mark the check box next to each type of data theft that you want to detect.

4) If you want to define custom classifiers for identifying transmission of your organization's sensitive or proprietary information:

   a) Use the **Web** > **Policy Management** > **Content Classifiers page** to define the phrases or patterns that you want to identify. (See Configure Content Classifiers in the Web Security Cloud help.)

   b) Return to the **Data Security** tab in your policy to configure how each classifier is used.

   Detailed information about defining classifiers is available in the Forcepoint Security Portal Help; click **Help** > **Explain This Page** on the Content Classifiers page.

Next steps

When data loss and data theft incidents are detected, information about them is available in the Data Security Dashboard, as well as the Report Builder and Report Catalog. See *Using reporting tools*, for information about using Report Builder and the Report Catalog.

For more information about how data security information is used and stored in the cloud portal, open the **Help** > **Privacy & Security** menu and select **Data Privacy FAQ**.

Related concepts

Using reporting tools on page 18

Managing block and notification pages

When a policy denies access to a resource or needs to inform the user of an event, Forcepoint Web Security Cloud can display an appropriate notification page. There is a standard set of notification pages included with Forcepoint Web Security Cloud, and you can either modify these to suit your needs, or add your own pages. You can then refer to the notification pages from any of your policies.

To view the list of notification pages, click **Web** in the portal's main menu bar, then under **Policy Management**, click **Block & Notification Pages**.

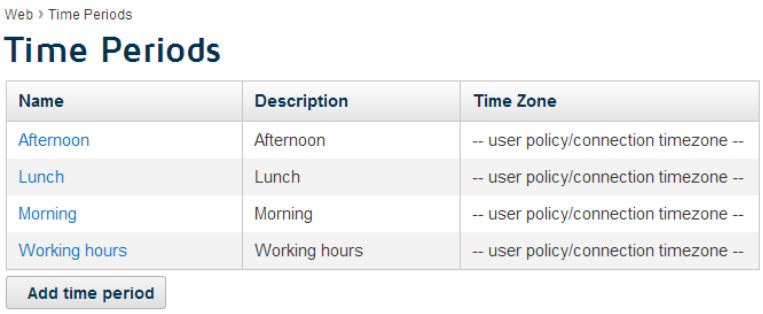
Each notification is a complete HTML page, and you can use any valid HTML within the pages. Some markup strings and tags are available – for example, an "access denied" image and a placeholder to contain the reason that a page was blocked. These tags are listed and described in the Forcepoint Web Security Cloud Help.

You can create multiple language versions of block and notification pages to display to end users, allowing a single corporate policy to be applied to a multi-national user base. If you create multiple language versions of standard or custom pages, the most appropriate version of the page is served to end users based on their browser settings. The language version displayed to end users will be the version that matches the primary language set in the user's browser, if a version exists for that language. If a version does not exist, the default language version will be used.

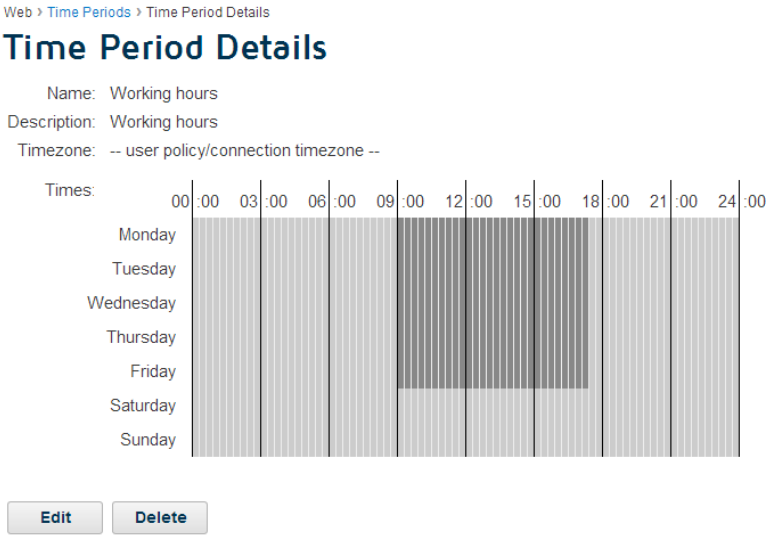
Setting time periods

Forcepoint Web Security Cloud allows you to restrict web surfing by time of day for either a whole policy or for defined website categories, users, and groups. This gives administrators the greatest possible flexibility to enable a customized acceptable use policy.

To access the current policies in your account and to create new policies, click **Web** in the portal's main menu bar, then click **Time periods**.



Each account has 4 default time periods: Afternoon, Lunch, Morning, and Working hours. You can view or edit existing time periods, and also create new ones to suit your company's requirements. For example, click the **Working hours** period.



The dark area defines the actual time period. Each division is a 15 minute period; notice that when you roll your mouse over the area, the actual time is displayed below the time chart. If the time period has been allocated to one or more policies, the policy names are listed in the Used in field.

You can click **Edit** to set a different time period, with either a single click or by clicking and dragging to cover a wider area on the time chart. You can also tie the time period to a specific time zone.

Once you have set up your time periods, you can apply them to policies. To do this, navigate to the relevant policy and on the **General** tab, select options and configure exceptions with the Internet Availability controls. Here you can define granular access rules for groups and individual users.

Deploying Forcepoint Web Security Endpoint

Forcepoint Web Security Endpoint is designed to provide a seamless experience to end users for authenticating and directing traffic to the Forcepoint Web Security Cloud infrastructure. Administrators can create policies that provide full visibility into inbound and outbound traffic, but that don't restrict use of the device.

The endpoint has been designed to consume minimal CPU, memory, and disk resources. It can be deployed on Windows and Mac operating systems.

To enable the use of the endpoint for some or all of your end users, you must deploy it to those users. For more information, see Deploying Web Security Endpoint in the cloud web Getting Started Guide.

Using reporting tools

Forcepoint Web Security Cloud provides exceptional reporting functionality with a 360-degree view of web traffic and usage. Administrators can view pre-defined summary reports, drill down for detailed forensics, and create granular, customized reports using an intuitive drag and drop interface.

To define your own reports, navigate to **Reporting** > **Report Builder**, then select **Web Security** (for all web activity) or **Data Security** (for activity associated with data loss or data theft incidents).

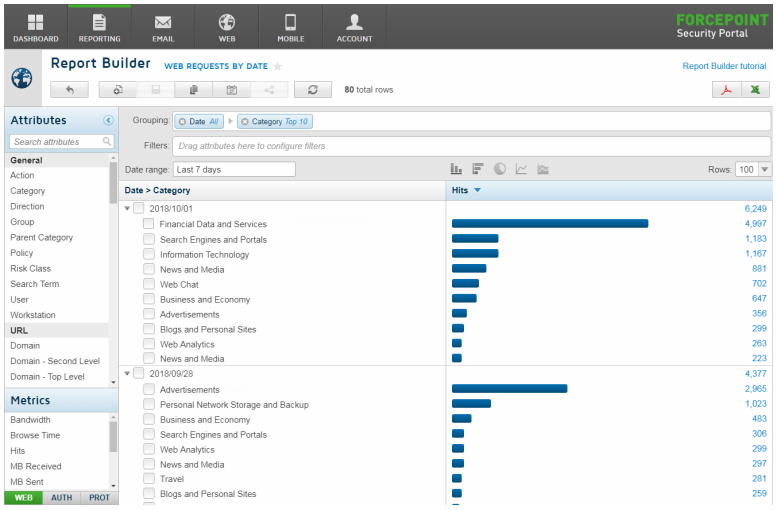
In Report Builder, use the attributes and metrics in the left pane to generate multi- level, flexible reports that allow you to analyze information from different perspectives and gain insight into your organization's Internet usage.

Once you have selected the attributes and metrics to display, you can add filters for the report such as policies, users, or domains, and also define a date range.

When you run your report, you can drill down into the report data by clicking any item top open the **Transaction Viewer** (for general web activity) or the **Incident Manager** (for data security incidents). Here, you can access all available details about individual transactions or incidents that warrant further investigation.

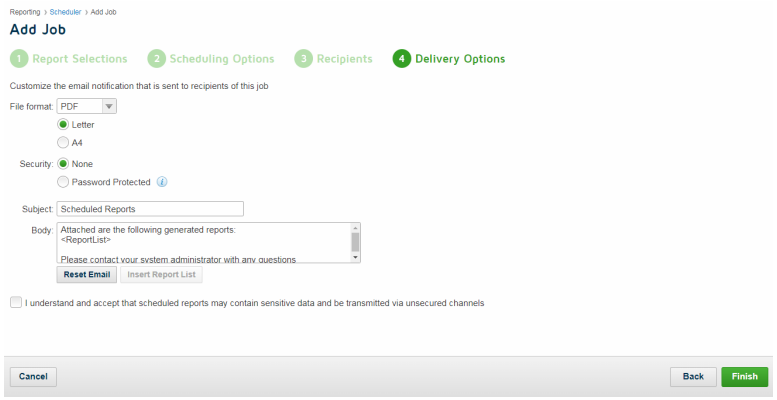
To select from a list of predefined reports, navigate to **Reporting** > **Report Catalog**.

Below is an example of a volumes report showing the requests for the most frequently visited categories per day, over a 7-day period.



Click a bar in the chart to drill down further and see details of all requests in each category. You can add further attributes to examine the data by users, group, site, policy, or any other relevant attribute. You can save a report, or export it to PDF or CSV.

Using the report scheduler, you can also schedule saved reports to run automatically and be distributed to your contacts via email.



For more information on the reporting tools available in the cloud portal, see Report Center in the Forcepoint Web Security Cloud help.

Next steps

Once you have set up users and customized your policies to meet the needs of your organization, there is little ongoing maintenance or configuration required with Forcepoint Web Security Cloud. However, it is a good practice to periodically use the dashboard and run reports to review and report on the ongoing web security protection provided by the service.

Administrators can schedule non-graphical versions of account summary reports to be sent to an email address on a daily, weekly, bi-weekly, or monthly basis.

Optional add-on modules

Additional Forcepoint Web Security Cloud modules are available to enhance and extend your web protection solution.

- With the Forcepoint Advanced Malware Detection for Web module, suspicious files can be forwarded to a cloud-hosted sandbox for analysis. The sandbox activates the file, observes its behavior, and compiles a report. If the file is malicious, an alert is sent to specified administrators.
- The Cloud App Control module integrates with Forcepoint CASB to provide granular control over the use of cloud-based applications (cloud apps) in your organization. You can nominate a set of cloud apps, sanctioned for use within your organization, to be protected.

Integration with Forcepoint Email Security

The close integration of Forcepoint Web Security Cloud and Forcepoint Email Security enables organizations to optimize their email use and to consolidate their cloud security protection capabilities for web and email with an integrated solution. Customers gain complete web and email security administered via the cloud portal, with the benefits of integrated reporting and management. Email Security Cloud delivers the following benefits:

- Blocks email threats such as spoofing, spyware, viruses and malware, phishing scams, and spam at their source, improving security, productivity, and saving business costs.
- Protects end users from the risks of accessing inappropriate and malicious web content accessed via email links, using ThreatSeeker Intelligence and leveraging the web proxy capabilities of Web Security Cloud to protect users against web threats in real time.
- Configured through a single management interface for email and web protection, requiring the administrator to manage only one set of users and groups and monitor usage through a single dashboard.

Thank you!

This guide has highlighted the most important aspects of administering Forcepoint Web Security Cloud, and demonstrated the following benefits:

- Threats are blocked before they reach your network, as shown by the statistics on the dashboard. This means reduced bandwidth and maintenance costs for your organization, while still allowing your users to safely leverage the power of dynamic web technology.
- Default policies enable immediate and effective web security with little administrative time required. Policies can be customized to meet the precise needs of your organization and your users while ensuring complete and effective web security.
- The dashboard and reporting functions enable you to track every aspect of web usage and security.
- Integration with Forcepoint Email Security provides a complete security solution with centralized policies and reporting.

Thank you for evaluating Forcepoint Web Security Cloud. For help or information about this or other Forcepoint solutions, please contact us:

https://www.forcepoint.com/contact- us