CONTENTS

PREFACE

Preface xv
   Audience xv
   Document Organization xv
   Document Conventions xv
   Related Documentation xvi
   Additional Information xvi

PART I

Administration 17

CHAPTER 1

Introduction 1
   Overview 1

CHAPTER 2

Account Management 3
   Editing Your Account Details 3
   Changing Your Password 4
   Managing Login Access to Account 5
   Changing the Scanned IP Addresses 5
   Downloading a List of Dynamic DNS Addresses 6
   Managing Admin Users 7
      Creating a New Admin User 7
      Editing an Admin User 8
      Restricting Access to Reports 8
      Removing an Admin User 9
   Managing Service Notifications 9
   Role Permissions 9
Testing Authentication Settings 33
Testing Process 33
LDAP Testing 33
Setting the Cookie Duration 33
Downloading Audit Reports 34
Configuring the User Authentication Page 34

CHAPTER 6
Log Extraction 37
Overview 37
Reporting Attributes 38
Issuing a Key Pair 42

CHAPTER 7
Hosted Configuration 45
Uploading a New Configuration File 46
Managing Configuration Files 46
Removing Configuration Files 47

CHAPTER 8
Audits 49
Email Alerts 49
Access Audit 50
Activity Audit 51
Report Execution 52
Report Management 53
Log Extraction Audit 53

CHAPTER 9
Delegated Administration 55
Logging In to the Parent Organization 55
Enabling Subsidiary Organizations to Create Certificates 55
Enabling Subsidiary Organizations to Set Policies 56
Enabling HTTPS Inspection 57
Subsidiary Privacy Policy 57
Managing Exported and Imported Policy 58
Managing Filters, Schedules, and Dictionaries 59
Setting Global and Local User Messages 59
<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CHAPTER 14</strong></td>
</tr>
<tr>
<td>Managing Schedules</td>
</tr>
<tr>
<td>Creating a New Schedule 89</td>
</tr>
<tr>
<td>Editing a Schedule 90</td>
</tr>
<tr>
<td>Removing a Schedule 90</td>
</tr>
<tr>
<td><strong>CHAPTER 15</strong></td>
</tr>
<tr>
<td>Managing Policy</td>
</tr>
<tr>
<td>Creating a Rule 92</td>
</tr>
<tr>
<td>Editing a Rule 93</td>
</tr>
<tr>
<td>Removing a Rule 93</td>
</tr>
<tr>
<td>Backing Up a Policy 93</td>
</tr>
<tr>
<td>Restoring a Policy 94</td>
</tr>
<tr>
<td><strong>CHAPTER 16</strong></td>
</tr>
<tr>
<td>Managing Quotas</td>
</tr>
<tr>
<td>Creating a Quota 97</td>
</tr>
<tr>
<td>Editing a Quota 99</td>
</tr>
<tr>
<td>Removing a Quota 99</td>
</tr>
<tr>
<td><strong>CHAPTER 17</strong></td>
</tr>
<tr>
<td>Global Settings 101</td>
</tr>
<tr>
<td>Overview 101</td>
</tr>
<tr>
<td>SearchAhead 101</td>
</tr>
<tr>
<td>SafeSearch 102</td>
</tr>
<tr>
<td>Localization 103</td>
</tr>
<tr>
<td>HTTP/HTTPS Split 103</td>
</tr>
<tr>
<td>Acceptable Usage Policy 103</td>
</tr>
<tr>
<td>Dynamic Classification 103</td>
</tr>
<tr>
<td>Content Range Headers 103</td>
</tr>
<tr>
<td>Changing Global Settings 104</td>
</tr>
</tbody>
</table>
CHAPTER 23 Viewing Reports
  Viewing Reports Online
    Grid Chart
      Viewing Grid Data
      Adding and Removing Metrics
      Sorting Grid Data by Attribute
      Changing the Sort Metric
    Graphical Charts
      Bar Chart
      Column Chart
      Line Chart
      Pie Chart
  Downloading Reports
    Downloading PDF Reports
    Downloading CSV Reports

CHAPTER 24 Pre-Defined Searches
  Searches by Type

CHAPTER 25 Filtering Reports
  Adding Filters to a Search
    Adding a Filter
    Activating and Deactivating Filters
    Editing Filters
    Removing Filters
  Managing Filter Sets
    Adding a Filter Set
    Copying a Filter Set
    Renaming a Filter Set
    Editing a Filter Set
    Removing a Filter Set
CHAPTER 26

Reporting Attributes 143
Attributes List 143

CHAPTER 27

Creating a Search 153
Overview 153
Creating a Standard Search 154
Creating a Time Analysis Search 154
Creating a Detailed Search 155
Allowed Traffic 156
Downloading Detailed Reports as CSV 157
User Audit Reports 157
Creating a Search from a Predefined Search 157
Storing a Search 158
Editing a Search 159
Renaming a Search 159
Removing a Search 159
Removing an Empty Folder 160

CHAPTER 28

Composite Reports 161
Creating Composite Reports 161
Downloading Composite Reports 162
Editing Composite Reports 162
Removing Composite Reports 162

CHAPTER 29

Scheduled Reports 165
Email Groups 165
Creating an Email Group 165
Removing an Email Group 166
Email Recipients 166
Creating an Email Recipient 166
Removing an Email Recipient 166
Creating a Scheduled Report 167
Editing a Scheduled Report 168
Removing a Scheduled Report 168

CHAPTER 30 Portal 2.0 169
Overview 169
Dashboard 170
Quick Analysis Reports 170
Detailed Analysis Reports 172

PART IV Threat Analysis 175

CHAPTER 31 Advanced Threat Detection 177
Overview 177
Additional Benefits 178
Reports Tab 179
Dashboard Tab 179
Threats Tab 179

CHAPTER 32 Threats Tab 181
Dashboard 181
Confirmed Threats 181
Detected Incidents 183
Filtering Incidents 184
Settings 184
Incident Details 185
Incident Header 185
Parallel Coordinates 186
Web Flow Requests 186
Proxy Device Uploads 187

CHAPTER 33 Sandboxing 191
Overview 191
Startup 191
Dropped 191
Domains/IPs 192
CHAPTER 34  Investigating Incidents  193
  Overview  193
  Details  194

CHAPTER 35  CTA STIX/TAXII Service  197
  Overview  197
  Poll Service  198
    Poll Request  199
    Poll Response  200
    Poll Fulfillment  205
  Common Queries  206
    Users Affected by Confirmed Threats  206
    Users Affected by Confirmed Threats Within a Timeframe  206
    Users Affected by High Risk and High Confidence Incidents  207
    Users Affected by Campaign  207
    Command and Control Servers  207
  CTA Integration with Cisco ISE  207

APPENDIX A  Cisco Security Appliance Integration  209
  Overview  209
  Hybrid Web Security  209
  Transparent Redirection  212
    Configuring the Upstream Proxy  212
    Setting the Routing Policies  212
  CLI Settings  213

APPENDIX B  Cloud Web Security Mobile Browser  215
  Overview  215
  Provisioning  216
    Deliver the Application  216
<table>
<thead>
<tr>
<th>Application on iOS</th>
<th>216</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application on Android</td>
<td>217</td>
</tr>
<tr>
<td>Distributing the Configuration File</td>
<td>218</td>
</tr>
<tr>
<td>Configuration File Properties</td>
<td>218</td>
</tr>
<tr>
<td>Configuration File Template</td>
<td>219</td>
</tr>
<tr>
<td>Configuration on iOS</td>
<td>220</td>
</tr>
<tr>
<td>Configuration on Android</td>
<td>221</td>
</tr>
<tr>
<td>Policy</td>
<td>223</td>
</tr>
<tr>
<td>Authentication</td>
<td>223</td>
</tr>
<tr>
<td>Acceptable Usage Policy</td>
<td>223</td>
</tr>
<tr>
<td>Web Filtering</td>
<td>224</td>
</tr>
<tr>
<td>Cloud Bypass Whitelisting</td>
<td>224</td>
</tr>
<tr>
<td>HTTPS Inspection</td>
<td>224</td>
</tr>
<tr>
<td>Reporting</td>
<td>225</td>
</tr>
<tr>
<td>Branding</td>
<td>225</td>
</tr>
<tr>
<td>Captive Portal Detection</td>
<td>226</td>
</tr>
<tr>
<td>Trusted Network Detection</td>
<td>226</td>
</tr>
<tr>
<td>Beacon Server Configuration</td>
<td>227</td>
</tr>
<tr>
<td>Fail Open or Fail Closed</td>
<td>227</td>
</tr>
</tbody>
</table>
Preface

- Audience, on page xv
- Document Organization, on page xv
- Document Conventions, on page xv
- Related Documentation, on page xvi
- Additional Information, on page xvi

Audience

This document is intended primarily for network administrators and channel partners.

Document Organization

This guide is composed of four parts and appendices. The first part describes how to set up, configure, administer, and troubleshoot the service. The second part describes how to use Cisco Cloud Web Security to filter web content entering and leaving your network. The third part describes how to use the reporting functionality. The fourth part describes how to use the threat analysis service.

Document Conventions

This guide uses the following conventions:

<table>
<thead>
<tr>
<th>Item</th>
<th>Convention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commands and keywords.</td>
<td>boldface font.</td>
</tr>
<tr>
<td>Variables for which you supply values.</td>
<td>italic font.</td>
</tr>
<tr>
<td>Optional command keywords. You do not have to select any options.</td>
<td>[enclosed in brackets]</td>
</tr>
<tr>
<td>Required command keyword to be selected from a set of options. You must choose one option.</td>
<td>{options enclosed in braces</td>
</tr>
<tr>
<td>Displayed session and system information.</td>
<td>screen font.</td>
</tr>
<tr>
<td>Information you enter.</td>
<td>boldface screen font.</td>
</tr>
</tbody>
</table>
Related Documentation

- Cisco AnyConnect Secure Mobility Client Administrator Guide
- Cisco Cloud Web Security Connector Administrator Guide

Additional Information

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What’s New in Cisco Product Documentation at:

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What’s New in Cisco Product Documentation Really Simple Syndication (RSS) feed. The RSS feeds are a free service.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to:
http://www.cisco.com/go/trademarks

Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)
PART I

Administration

- Introduction, on page 1
- Account Management, on page 3
- User Management, on page 13
- Custom Headers, on page 17
- Authentication, on page 19
- Log Extraction, on page 37
- Hosted Configuration, on page 45
- Audits, on page 49
- Delegated Administration, on page 55
- Troubleshooting, on page 61
Overview

Cisco ScanCenter is the administration portal to Cisco Cloud Web Security (CWS). From here, you can manage users and groups, set filters and policy, monitor web traffic, analyze potential threats, and generate reports. This guide details the full set of functionality available to the Cisco ScanCenter administrator. Some functionality may not be present in your account, depending on your region, vendor, and licensing. Contact your Cisco sales representative for further information. Currently, the following web browsers are supported:

- Microsoft Internet Explorer 11.
- The current and previous version of Mozilla Firefox.
- The current and previous version of Google Chrome.

To return to a previous view, when there is a choice between using your web browser's back button and clicking the Cancel button, you should use the Cancel button.
CHAPTER 2

Account Management

- Editing Your Account Details, on page 3
- Changing Your Password, on page 4
- Managing Login Access to Account, on page 5
- Changing the Scanned IP Addresses, on page 5
- Downloading a List of Dynamic DNS Addresses, on page 6
- Managing Admin Users, on page 7
- Managing Service Notifications, on page 9
- Role Permissions, on page 9

Editing Your Account Details

Procedure

Step 1  Click the Admin tab to display the administration menus.
Step 2  In the Your Account menu, click Account Details to display the Account Details page.
Step 3  Expand the Personal Details section.
Step 4  In the Title drop-down list, choose your title.
Step 5  (Required) Enter your First Name.
Step 6  (Required) Enter your Last Name.
Step 7  Enter your cellular phone number in the Mobile Phone box.
Step 8  Expand the Organization Details section.
Step 9  Enter your Job Title.
Step 10  (Required) Enter your Organization Name.
Step 11  (Required) Enter your Telephone number.
Step 12  Enter your facsimile number in the Fax field.
Step 13  Enter your city in the City box.
Step 14  Enter your organization’s address, using up to three lines, in the Address boxes.
Step 15  Enter the URL of your organization’s Website.
Step 16  Expand the General Details section.
### Changing Your Password

When a new user is created and activated, or an administrator resets the password of a user who has forgotten their password, an email with password instructions is sent to the email address associated with that user.

Passwords expire after a set period of time; 90 days by default. This is configured for you by Cisco Customer Support. You can request that passwords do not expire. If your password has expired, you are prompted to change your password before you can access any other areas of Cisco ScanCenter. Also, you can change your password at any time.

Your new password cannot be the same as any of your five previous passwords. Also, it must contain:

- At least 8 characters
- One or more lower case letters
- One or more upper case letters
- One or more digits
- One or more of the following special characters: @#$%^&-=_!:?

---

**Note**

Clicking Reset does not reset your password. It only clears the boxes.

---

**Procedure**

**Step 1**
Click the Admin tab to display the administration menus.

**Step 2**
In the Your Account menu, click Change Password to display the Enter your new password pane.

**Step 3**
Enter the current password.

**Step 4**
Enter the new password in the Password and Confirm password boxes. As you type the password, the red crosses change to green check marks when each criterion is met.

**Step 5**
Once you have entered a valid password, click Save to change the password. Alternatively, click Cancel or navigate away from the page to abandon your changes.
Managing Login Access to Account

Procedure

Step 1  Click the Admin tab to display the administration menus.
Step 2  In the Your Account menu, click Authorized IPs to display the Limit Login Access page.
Step 3  Expand the Add IP Address/Network to Authorized Addresses section.
Step 4  Enter an IP address or a subnet mask in the Addresses field.
Step 5  Click Submit to add the IP address to the authorized list.
Step 6  Authorized IP addresses and networks are listed below the search field. You can search for, edit, or select items to be removed.
Step 7  In the Actions section, you can select what is done when there is a sign in from an unlisted, unauthorized IP address.
  • Send an email to your company administrator which notifies you of any attempt to sign in from an unauthorized IP address.
  • Forbid sign in from any unauthorized IP address or network subnet.
Step 8  Click Save to apply your changes. Alternatively, click Cancel or navigate to another page to abandon your changes.

Changing the Scanned IP Addresses

You must provide us with a list of egress IP addresses that send traffic from your network to our proxy servers.

Note

By default, only IPv4 addresses are enabled. Contact Cisco Customer Support if you require IPv6 address support.

Procedure

Step 1  Click the Admin tab to display the administration menus.
Step 2  In the Your Account menu, click Scanning IPs to display the Scanned IP Addresses pane.
Step 3  Add, remove, or change an IP address. Enter each IP address in CIDR notation. For example, 209.165.200.224/27 (IPv4) or 2001:DB8::/32 (IPv6). You should enter each IP address on a new line. Do not enter private or reserved IP addresses, for example 192.168.0.0/24. IPv4 addresses can also be entered with a netmask, for example 209.165.200.224/255.255.255.224.
Step 4  Click Save to proceed with your proposed changes. Alternatively, click Cancel or navigate away from the page to abandon your changes.
Step 5 On the Scanning IPs Confirmation Page, you are shown what is to be added or removed. Changing the scanned IP addresses will affect traffic from your network to our proxy servers. Click OK to submit your changes. Alternatively, click Cancel to go back and edit your proposed changes.

What to do next
Changes to the scanned IP addresses will normally be updated within one business day. A confirmation email will be sent when the changes are complete. If your change is urgent, contact Cisco Customer Support.

Downloading a List of Dynamic DNS Addresses

Typically, accessing the proxy servers from a dynamic IP address requires the use of Connector configured with group or company authentication keys.

The majority of Cisco and third-party routers can issue Dynamic DNS (DDNS) requests. DDNS enables the router to communicate with an external server to send its current external (WAN) IP address, so that other devices can connect to it using a static name resolved through normal DNS requests. The DDNS server is automatically updated if the external IP address changes. A DDNS update comprises a user name, password, and host name, which can be used by the service to authenticate these devices.

It is also possible to perform DDNS registration with client-side software.

Note
For transparent deployment, DDNS routers must support the ability to port forward traffic to the proxy servers. Alternatively, browser proxy settings (PAC, WPAD, and so on) may be used if required.

Cisco provides a proprietary DDNS service as a means to verify dynamic IP addresses against its authentication database. Any router that has a “custom” option for DDNS should be able to use this functionality.

For detailed instructions on configuring your router, see your router documentation.

Procedure

Step 1 If you have not already done so, create a group authentication key in Cisco ScanCenter.
Step 2 Create a “custom” DDNS on your router.
Step 3 Set the server to ddns.scansafe.net.
Step 4 Set a unique identifier for the username or equivalent parameter.
Step 5 Set the password to the group authentication key that you previously created.
Step 6 Set the hostname to one of the domains associated with your Cisco ScanCenter account, typically your email domain.
Step 7 Set the URL to /dir/register?hostname=. 
What to do next

To verify that your routers are working correctly, you may want to view a list of currently registered dynamic DNS addresses. The list is provided as a CSV file containing the current IP address for each device. It does not contain a history of device IP addresses.

To download the list, click the Admin tab to display the administration menus. In the Your Account menu, click Dynamic DNS.

Click Generate Audit to download a comma-separated value (CSV) list of the dynamic IP addresses currently registered with your account. The list contains user names, IP addresses, host names, and the date of the last update.

Managing Admin Users

The Manage Admin Users page enables you to create, edit, and remove admin users. The access rights of an admin user are determined by the role assigned to that user. The available roles are:

• Full Access
• Read Only
• Report Admin
• Admin with no Forensic Role
• HR
• Super User (only available to the default company super user)
• Threat Analysis
• Full Read Only

See Role Permissions, on page 9 for details of the access rights associated with each role.

Note

The default company super user can create, edit, and remove super users. Super users can create other admin users but cannot create super users of equal role. The default company super user cannot be removed.

Procedure

Step 1 Click the Admin tab to display the administration menus.
Step 2 In the Your Account menu, click Admin Users to display the Manage Admin Users page.

Creating a New Admin User

Procedure

Step 1 Click Create Admin User.
Step 2 Enter the email address of the new admin user in the Email Login box. This is the username.
Step 3
In the **Role** drop-down list, choose a role.

Step 4
Click **Submit** to create the new admin user. Alternatively, navigate away from the page to abandon your changes.

What to do next
Activate the admin user in order to grant access and allow the admin user to log in to Cisco ScanCenter. An email with password instructions is then sent to the admin user.

Editing an Admin User

To activate an inactive admin user, check the **Active** box.

To deactivate an active admin user, uncheck the **Active** box.

To reset or change the password of an admin user, click **Reset Password**. An email with password reset instructions is then sent to the admin user.

To unlock an admin user who has been locked out after multiple failed log-in attempts, click **Unlock**.

To change the role of an admin user, choose the required **Role** in the drop-down list.

---

**Note**

The organization super user account will never be locked. After 10 failed attempts in succession, the password is invalidated and an email with password setup instructions is then sent to the super user.

Restricting Access to Reports

You can restrict the data that an admin user is able to view when running reports. By default there are no restrictions in place.

**Note**

Filters will not be applied to scheduled reports. Filter sets cannot be applied to admin users.

For more information about filters, see Filtering Reports, on page 139.

Procedure

---

**Step 1**
Click **Filters** to display the list of attributes.

**Step 2**
Clear the check boxes of the attributes that you do not want to be viewed by the admin user.

**Step 3**
Add any filters you want to apply to online reports viewed by the admin user.

**Step 4**
Click **Save** to apply your changes. Alternatively, navigate away from the page to abandon your changes.
Removing an Admin User

Caution
When an admin user has been removed, it cannot be recovered. Instead, you must create a new admin user.

Procedure

Step 1
Select the check box for the required user. You can select multiple admin users to be removed.

Step 2
Click Remove. You will be prompted to confirm your action.

Managing Service Notifications

Service notifications are displayed in Cisco ScanCenter. Service notifications include new incidents, outages, planned maintenance, incident updates, new features, product updates, and functional changes. View service notifications by navigating to Admin > Your Account > Notifications. Service notifications are displayed with their Status; read or unread, Subject, Category icon; a blue circle for product and feature updates or a yellow triangle for service updates, and the Date Received. For each type of notification, you can create a list of email addresses for recipients to receive the notification. Regardless of these settings, service notifications are always displayed in Cisco ScanCenter. The recipient lists are used for service notifications only; no other emails are sent to these addresses.

Procedure

Step 1
Navigate to Admin > Your Account > Notifications.

Step 2
In the Manage Service Update Settings pane, select the desired check box or boxes.

Step 3
For each recipient, enter the email address in the field and click Add Recipient. You can remove unwanted email addresses by clicking the x icon within each address to remove.

Step 4
Click Apply to save your changes. Alternatively, navigate away from the page to abandon your changes.

Role Permissions

<table>
<thead>
<tr>
<th>Area</th>
<th>Company Super User</th>
<th>Super User</th>
<th>Full Access</th>
<th>Read Only</th>
<th>Full Read Only</th>
<th>HR</th>
<th>Admin (No Forensic)</th>
<th>Report Admin</th>
<th>Threat Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Messages</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>R</td>
<td>R</td>
<td></td>
<td>R/W</td>
<td>R/W</td>
<td>—</td>
</tr>
<tr>
<td>Email Alerts</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>R</td>
<td>R</td>
<td></td>
<td>R/W</td>
<td>R/W</td>
<td>—</td>
</tr>
<tr>
<td>Area</td>
<td>Company Super User</td>
<td>Super User</td>
<td>Full Access</td>
<td>Read Only</td>
<td>Full Read Only</td>
<td>HR</td>
<td>Admin (No Forensic)</td>
<td>Report Admin</td>
<td>Threat Analysis</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>--------------------</td>
<td>------------</td>
<td>-------------</td>
<td>-----------</td>
<td>----------------</td>
<td>----</td>
<td>-------------------</td>
<td>--------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Search/Time Analysis</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R/W</td>
<td>R/W</td>
<td>—</td>
</tr>
<tr>
<td>Detailed Search</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td></td>
<td>R</td>
<td>R</td>
<td>R/W</td>
<td>R/W</td>
<td>—</td>
</tr>
<tr>
<td>Filter Sets</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R/W</td>
<td>R/W</td>
<td>—</td>
</tr>
<tr>
<td>Store Search/Remove Stored Search</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td></td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Manage Composite Reports</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>R</td>
<td>—</td>
<td>R</td>
<td>R/W</td>
<td>R/W</td>
<td>—</td>
</tr>
<tr>
<td>Create/Edit Composite Reports</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td></td>
<td>—</td>
<td>—</td>
<td>R/W</td>
<td>R/W</td>
<td>—</td>
</tr>
<tr>
<td>Managed Scheduled Reports</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>R</td>
<td>—</td>
<td>—</td>
<td>R/W</td>
<td>R/W</td>
<td>—</td>
</tr>
<tr>
<td>Create/Edit Scheduled Reports</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td></td>
<td>—</td>
<td>—</td>
<td>R/W</td>
<td>R/W</td>
<td>—</td>
</tr>
<tr>
<td>Manage Email Recipients</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td></td>
<td>R</td>
<td>—</td>
<td>R/W</td>
<td>R/W</td>
<td>—</td>
</tr>
<tr>
<td>Allowed Traffic Reports</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
<td>R</td>
<td>R</td>
<td></td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>Spyware</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>R</td>
<td>—</td>
<td>R</td>
<td>R/W</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Web Filtering</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>R</td>
<td>—</td>
<td>R</td>
<td>R/W</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Web Filtering / ISR Exception</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td></td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Account Details</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R/W</td>
<td>R/W</td>
<td>R</td>
</tr>
<tr>
<td>Change Password</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>R</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
</tr>
<tr>
<td>Authorized IPs</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>R</td>
<td>—</td>
<td>R</td>
<td>R/W</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Scanning IPs</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td></td>
<td>R</td>
<td>—</td>
<td>R/W</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Area</td>
<td>Company Super User</td>
<td>Super User</td>
<td>Full Access</td>
<td>Read Only</td>
<td>Full Read Only</td>
<td>HR</td>
<td>Admin (No Forensic)</td>
<td>Report Admin</td>
<td>Threat Analysis</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------</td>
<td>------------</td>
<td>-------------</td>
<td>-----------</td>
<td>----------------</td>
<td>----</td>
<td>----------------------</td>
<td>--------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Admin Users</td>
<td>R/W</td>
<td>R/W</td>
<td>—</td>
<td>—</td>
<td>R</td>
<td></td>
<td>—</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dynamic DNS</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>—</td>
<td>R</td>
<td></td>
<td>R/W</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>—</td>
<td>R</td>
<td></td>
<td>R/W</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clientless Authentication</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>—</td>
<td>R</td>
<td></td>
<td>—</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User/Group Management</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>—</td>
<td>R</td>
<td></td>
<td>R/W</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit Settings</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>—</td>
<td>R</td>
<td></td>
<td>R/W</td>
<td>R/W</td>
<td></td>
</tr>
<tr>
<td>Activity/Access Audit</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>—</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Dictionaries/File Info DBs</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>R</td>
<td>R/W</td>
<td></td>
<td>R/W</td>
<td>R/W</td>
<td></td>
</tr>
<tr>
<td>Import User List</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>—</td>
<td>R</td>
<td></td>
<td>—</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTPS Inspection</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>R</td>
<td>R</td>
<td></td>
<td>R/W</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hosted Config</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>—</td>
<td>—</td>
<td></td>
<td>R/W</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log Extraction Credentials</td>
<td>R/W</td>
<td>R/W</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td></td>
<td>—</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threats Tab</td>
<td>R/W</td>
<td>R/W</td>
<td>R</td>
<td>—</td>
<td>R</td>
<td></td>
<td>R/W</td>
<td>R/W</td>
<td></td>
</tr>
<tr>
<td>Policy Backup/Restore</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>—</td>
<td>R</td>
<td></td>
<td>R/W</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Management</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>R</td>
<td>R</td>
<td></td>
<td>R/W</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Cisco ScanCenter Administrator Guide, Release 5.2
User Management

The user management area of Cisco ScanCenter enables you to create groups, edit groups and users, and import users, dictionaries, and file information. When using Cisco AnyConnect Secure Mobility Web Security or Connector (including Cisco Adaptive Security Appliance and Cisco Integrated Services Router connector functionality), groups enable you to implement role-based web access policy.

Groups are evaluated as follows:

1. If Connector is configured to send internal group details, a check is made to see if the supplied group name matches any groups configured in Cisco ScanCenter. If a match exists, the matched group is selected. If the user belongs to more than one group, then any group containing the string "webscan" will be given priority.
2. If the username is matched but no group is matched, a check is made to see if the user belongs to an existing group.
3. If the group cannot be matched but the internal IP address is present, a check is made to see if the IP address matches a group IP expression.
4. If the group cannot be matched, a check is made to see if the external IP address matches a group IP expression.

- Managing Groups, on page 13
- Managing Users, on page 15

Managing Groups

Two types of groups are supported in Cisco ScanCenter: directory groups and custom groups. Directory groups can be Windows Active Directory groups or LDAP groups. Custom groups enable you to create a group that contains any users, regardless of their Active Directory or LDAP group.

Procedure

Step 1 Click the Admin tab to display the administration menus.
Step 2 In the Management menu, click Groups to display the Manage Groups page.
Adding a Group

Before you begin

Before you can add a directory group, you must first create the Active Directory or LDAP group on your server.

Procedure

Step 1 Click Add Group.
Step 2 Choose a Group Type from the drop-down list. Select either Custom or Directory group.
Step 3 Enter a Group Name.
   a) Custom groups can be named any combination of up to 256 alphanumeric characters
   b) Directory groups must have the prefix WinNT:// or LDAP://
Step 4 Click Submit.

What to do next

To add multiple groups at the same time, create a CSV file listing the same user in different groups. Follow the form: group, username, email address. Import the user list using Importing a User List, on page 15. All the different groups are imported. You can then search for the common username that was used to bulk import the groups and delete the user from the Manage Users page at ScanCenter > Admin > Users.

Editing a Group

Procedure

Step 1 Navigate to Admin > Management > Groups to display the Manage Groups page.
Step 2 Click the hyperlink of the group name to display the Edit Custom Group page.
Step 3 To change the name, enter a new name for the group in the box and click Save. Alternatively, keep the existing name.
Step 4 Enter the required IP expressions, click Add, and click Save. For example:
   • Single IP address: 192.168.0.1
   • Multiple IP addresses: 192.168.0.1, 192.168.0.2, 192.168.0.3
   • IP address range: 192.168.0.0/255.255.0.0
Step 5 To remove an IP expression, select the check box next to the IP, click Remove, and click Save.
Step 6 Enter the required Active Directory or LDAP users in the Users box, click Add, and click Save.
Step 7 To remove users, select the check box next to the user, click Remove, and click Save.
Removing a Group

In the Manage Groups page, select the check box of the group to be removed, and then click Remove to permanently remove the group. You will be prompted to confirm your action. You can select multiple groups to be removed. You cannot remove a group that is associated with a policy.

**Caution**
When a custom group has been removed, it cannot be recovered. Instead, you must create the custom group again.

Managing Users

**Before you begin**
Users cannot be added individually. They must be imported from a text file containing a comma-separated list in the form `group, username, email address` for each user. When the list has been imported, individual users can be removed. Users cannot be edited. If you need to make changes, you should remove the existing user and import a new user with the appropriate details.

**Importing a User List**

**Procedure**

**Step 1**
Click the Admin tab to display the administration menus.

**Step 2**
In the Management menu, click Import User List to display the Import User List page.

**Step 3**
Click Browse then navigate to the file.

**Step 4**
Click Import. You will be notified if the file cannot be validated.
Removing Users

Procedure

Step 1  Click the Admin tab to display the administration menus.

Step 2  In the Management menu, click Users to display the Manage Users page.

Step 3  Select the check box of the user to be removed.

Step 4  Click Delete Selected. You will be prompted to confirm your action.

What to do next

You can select multiple users to be removed. You can search for a user by entering all or part of the username, in the Search box and clicking Search. To display the full list again, click Reload list.
Custom Headers

Some service providers require the use of custom HTTP headers to allow access to certain Web content. The Custom Headers page enables you to apply custom headers for specific websites and exclude specific groups from using custom headers.

- Configuring Custom Headers, on page 17

### Configuring Custom Headers

**Procedure**

- Navigate to Admin > Management > Custom Headers.
- Click Add New Header.
- Enter the Domain name that requires the header. For example, example.com. To apply headers to all domains enter an asterisk (*).
- Enter the HTTP Header Name. For example, DNT.

You cannot use the following headers as they are used by the Cisco Cloud Web Security service:

- Accept-Datetime
- Authorization
- Cache-Control
- Connection
- Cookie
- Content-Length
- Content-MD5
- Content-Type
- Date
- Expect
- From
- Host
- If-Match
- If-Modified-Since
- If-None-Match
- If-Range
- If-Unmodified-Since
• Max-Forwards
• Pragma
• Proxy-Authorization
• Proxy-Connection
• Range
• Referer
• Upgrade
• Via
• Warning
• X-Forwarded-For
• X-Forwarded-Proto

• Enter the **Header Value**. For example, 1.
• Ensure the **Enabled** check box is selected.
• (Optional). Exclude any groups for which you do not want the header to be added.
  a) Click **Add Group**.
  b) Enter the group name in the **Search** field and click **Go**.
  c) Click **Select**.
  d) Click **Confirm Selection**.

You can remove any unwanted groups by clicking the **Remove** icon.

• Click **Save** to apply your changes. Alternatively, click **Cancel** to abandon your changes.

**What to do next**

To remove any unwanted headers, select the required check boxes and click **Remove Selected**.

To edit a header, click any hyperlink for that header.

To switch headers on or off, edit the header, select or clear the **Enabled** check box as required and click **Save** to apply your changes.
CHAPTER 5

Authentication

Authentication is the act of confirming the identity of a user. Cisco ScanCenter enables you to control access to the web for each user or a group of users. Authentication enables you to enforce your organization’s policies and comply with regulations. Cisco ScanCenter can perform authentication without the need for client software, but you can also generate authentication keys for your organization, groups, and individual users for use with Cisco AnyConnect Secure Mobility Web Security, and Connector (including Cisco Adaptive Security Appliance and Cisco Integrated Services Router integrated connector). For further information see the relevant administrator guide. Before creating group or user keys, you should set up your groups and users. See User Management, on page 13.

- Company Keys, on page 19
- Group Keys, on page 20
- User Keys, on page 21
- Setting The User Email Message, on page 22
- Clientless Authentication, on page 23

Company Keys

The company key is used for organization-wide authentication.

Procedure

1. Click the Admin tab to display the administration menus.
2. In the Authentication menu, click Company Key to display the Company Key page.

What to do next

To deactivate an active key, click Deactivate. To activate a deactivated key, click Activate.
To permanently remove a key, click **Revoke**.

**Note**

Revoking or deactivating a key will prevent users from being able to authenticate with Cisco Cloud Web Security. When you have revoked a key, you must generate a new key.

To generate a company key, click **Create New**. The **Authentication Keys** page is displayed.

Copy the authentication key to a secure location.

**Caution**

For security reasons, the authentication key is displayed only once. If you lose the key, you must revoke the existing key and create a new key.

## Group Keys

### Before you begin

Group keys are used for authenticating groups of users. Before creating group keys, you should ensure that you have created the required groups. See User Management, on page 13.

### Procedure

**Step 1**

Click the **Admin** tab to display the administration menus.

**Step 2**

In the **Authentication** menu, click **Group Keys** to display the **Group Authentication Keys** page.
What to do next

To create and activate a key, click **Create Key**. The **Authentication Keys** page is displayed. Enter a group email address in the **Send via email to the user** box, click a domain in the list, and then click **Send** to send an email to members of the group.

To deactivate an active key, click **Deactivate**. To activate a deactivated key, click **Activate**.

You can search for a group by entering all or part of the group name in the Search box and clicking **Search**. To display the full list again, click **Reload list**.

---

**Note**

Removing a group will also remove the associated authentication key which cannot be recovered.

---

**Bulk Group Management**

You can activate, deactivate, and revoke group keys in bulk.

Click the check box to select a group with a key. You can click **Select All** to select the check box of all groups with keys or **Deselect All** to clear all check boxes.

Click **Activate Selected** to activate all the selected group keys.

Click **Deactivate Selected** to deactivate all the selected group keys.

Click **Revoke Selected** to permanently remove all the selected group keys.

---

**User Keys**

**Before you begin**

User keys are used for authenticating individual users. Before creating user keys, you should ensure that you have imported the required users. See **User Management**, on page 13.

**Procedure**

**Step 1**

Click the **Admin** tab to display the administration menus.

**Step 2**

In the **Authentication** menu, click **User Keys** to display the **User Authentication Keys** page.
What to do next

To create and activate a key, click Create Key. The Authentication Keys page is displayed. Enter a user email address in the Send via email to the user box, click a domain in the list, and click Send to send an email to the user.

To deactivate an active key, click Deactivate.

To activate a deactivated key, click Activate.

To enable mobile functionality for a user, select the Mobile checkbox. Alternatively, clear the check box to switch off mobile functionality. You will be prompted to confirm your action.

You can search for a user by entering all or part of the username in the Search box and clicking Search. To display the full list again, click Reload list.

Note
Removing a user will also remove the associated authentication key which cannot be recovered.

Bulk User Management

You can activate, deactivate, and revoke user keys in bulk.

Click the check box to select a user with a key. You can click Select All to select the check box of all users with keys or Deselect All to clear all check boxes.

Click Activate Selected to activate all the selected user keys.

Click Deactivate Selected to deactivate all the selected user keys.

Click Revoke Selected to delete all the selected user keys.

Setting The User Email Message

When an authentication key is configured for a user, it is sent to them in an email message.

Procedure

Step 1 Click the Admin tab to display the administration menus.

Step 2 In the Authentication menu, click Email Messages to display the Email Messages page.
Step 3  Edit the message in the first box. The text [username] and [company_name] will be replaced with the user’s name and your organization’s name.

Step 4  Edit the signature in the second field.

Step 5  Click Submit to apply your changes. Alternatively, navigate away from the page to abandon your changes.

What to do next

You can click Restore Default Message to restore the default message.

Clientless Authentication

When you enable clientless authentication, Cisco Cloud Web Security authenticates users before allowing them to connect to a destination server. To achieve this, start by creating an Authenticate rule in Cisco ScanCenter for the user or group.

- Navigate to Web Filtering > Management > Policy.
- Click Create Rule.
- In the Rule Action pull-down list, select Authenticate.
- Create a rule for the user or group you wish to authenticate.
  - This rule triggers the process of first checking for a cookie. If no valid cookie is found, then the authentication process starts.
  - This rule can be applied only for specific groups or excluding specific groups.
  - Unlike the rule actions Block, Allow, and Warn, if the Authenticate rule action is matched, the policy continues to check subsequent rules in the policy.
  - Thus, the Authenticate rule is typically placed at the top of the policy in order to determine if the user has to be authenticated before applying the remaining rules in the policy.
For roaming users, this also requires configuring their browser to send traffic to the Cisco Cloud Web Security proxy server, typically using a PAC file.

Cisco ScanCenter supports the Lightweight Directory Access Protocol (LDAP) with standard and secure LDAP authentication.

To enable authentication, you must create at least one authentication realm. An authentication realm is a set of authentication servers (or a single server) supporting a single authentication protocol with a particular configuration. When you create more than one realm, your users will be able to select the realm with which they wish to authenticate with at the login screen.

**Note**

Clientless authentication requires enabling third-party cookies in the user's browser.

---

**LDAP Authentication**

The Lightweight Directory Access Protocol (LDAP) server database is a repository for employee directories. These directories include the names of employees and various types of personal data such as a phone number, email address, and other information that is exclusive to the individual employee. The LDAP database is composed of objects that contain attributes and values. Each object name is referred to as a Distinguished Name (DN). The location on the LDAP server where a search begins is called the Base Distinguished Name or base DN.

Cisco Cloud Web Security supports standard LDAP server authentication, Secure LDAP authentication, and StartTLS. Support for LDAP enables established installations to continue using their LDAP server database to authenticate users. For Secure LDAP, Cisco ScanCenter supports LDAP connections over TLS. The TLS protocol is an industry standard for ensuring confidentiality. TLS uses key encryption algorithms and Certificate Authority (CA) signed certificates allow the LDAP servers to verify the identity of the appliance. StartTLS uses certificates to identify the LDAP server before a connection is created.

**SAML Authentication**

Security Assertion Markup Language (SAML) is an XML-based standard for exchanging authentication and authorization data between different secure networks, sometimes referred to as security domains. The main problem that SAML solves is single sign-on between different security domains. Typically, this is users in one domain accessing a network (a different domain) using a web browser. This is sometimes referred to as web browser single sign-on.

To achieve web browser single sign-on, a SAML dialogue must take place between an entity in each domain, which SAML defines using the following terms:

- **Identity provider**. An identity provider (IdP) is an entity that produces SAML assertions. The identity provider is expected to authenticate its end users before producing a SAML assertion.

- **Service provider**. A service provider (SP) is an entity that consumes SAML assertions. Cisco Cloud Web Security is a service provider. The service provider relies on the identity provider to identify the end user and communicate that identification to the service provider in the SAML assertion. The service provider makes an access control decision based on the assertion.

SAML assertions are containers of information passed between identity providers and service providers inside SAML requests and responses. Assertions contain statements (such as authentication and authorization...
statements) that service providers use to make access control decisions. Assertions start with the `<saml:Assertion>` tag.

SAML dialogues are called flows, and flows can be initiated by either provider:

- **Service provider initiated flow.** The service provider (SP) is contacted by an end user requesting access so it starts a SAML dialogue by contacting the identity provider to provide identification for the user. For service provider initiated flows, the end user accesses the service provider using a URL that contains the service provider’s domain, such as `http://www.example.com/<URI>`.

- **Identity provider initiated flow.** The identity provider (IdP) starts a SAML dialogue by contacting the service provider requesting access on behalf of an end user. For identity provider initiated flows, the end user accesses the service provider using a URL that contains a local domain, such as `http://saas.example.com/<URI>`.

Cisco Cloud Web Security supports only service provider initiated flows and currently supports these SAML identity providers:

- PingFederate Server, version 5.0 or later
- Microsoft Active Directory Federated Services (ADFS), version 2.0 or later
- OpenAM, version 9.5.4 or later

For more information about SAML see [http://docs.oasis-open.org/security/saml/v2.0/](http://docs.oasis-open.org/security/saml/v2.0/).

### How Authentication Works

To authenticate users who access the Web, Cisco Cloud Web Security connects to an external authentication server or redirects users to an identity provider. An authentication server contains a list of users and their corresponding passwords organized into a hierarchy. For users on the network to successfully authenticate, they must provide valid authentication credentials (username and password as stored in the authentication server or by the identity provider). With an authentication server, when users access the Web through Cisco Cloud Web Security, the service communicates with both the client and the authentication server to authenticate the user and process the request. With an identity provider, Cisco Cloud Web Security redirects the user to the identity provider, which provides an authentication assertion.

Cisco Cloud Web Security supports the following authentication protocols:


- **StartTLS.** If your LDAP server supports the StartTLS extension, Cisco Cloud Web Security can establish Transport Layer Security with the server prior to authentication. StartTLS requires a server certificate on the LDAP server.

- **Security Assertion Markup Language (SAML).** Cisco Cloud Web Security uses a service provider initiated flow to authenticate the user with an external identity provider. This requires an identity provider (IdP) with SAML 2.0 support.

- **Basic Authentication.** Cisco Cloud Web Security allows a client application to provide authentication credentials in the form of a username and password when it makes a request.
Configuring Authentication Realms

Authentication realms reduce the changes required to your network and simplify provisioning users with Cisco Cloud Web Security.

Create, edit, and remove authentication realms. Manage certificates used by secure protocols.

Before configuring an LDAP authentication realm, you will need the following:

• **Server address.** Full address to your LDAP server; host, port, and protocol.
• **(Optional) Certificate.** Certificate to be used if you will be using a secure protocol, for example LDAPS.
• **LDAP access.** Cisco ScanCenter requires at least read-only access to your LDAP servers. The ports you need to open, and the IP addresses you must enable access for, can be found in your provisioning email.
• **Search base.** Location in the LDAP tree to start searching for users, and other related information.

Before configuring a SAML authentication realm, you will need the following:

• **Identity provider.** Correctly configured supported identity provider (IdP), accessible by your users from your internal network.
• **Service provider meta data.** This must be exported from Cisco ScanCenter and imported by your IdP.
• **Identity provider meta data.** This must be exported from your IdP and imported into Cisco ScanCenter.

---

**Note**

You must import certificates before creating an authentication realm that requires a secure protocol.

---

Obtaining Certificates

Cisco ScanCenter cannot generate Certificate Signing Requests (CSRs) for the purpose of obtaining a certificate. Therefore, to have a certificate created for the LDAP server, you must issue the signing request from another system. Save the key from this system because you will need to install it on the LDAP server later.

On a Windows server you can use Microsoft Certificate Services to generate a suitable certificate.

For information on using Microsoft Certificate Services, see your vendor documentation. Alternatively, you can use any UNIX machine with a recent version of OpenSSL installed. For information on generating a CSR using OpenSSL, see [http://www.modssl.org/docs/2.8/ssl_faq.html#ToC28.](http://www.modssl.org/docs/2.8/ssl_faq.html#ToC28)

Typically, LDAP servers use self-signed certificates. For information on creating and using your own Certificate Authority (CA), see [http://www.modssl.org/docs/2.8/ssl_faq.html#cert-ownca.](http://www.modssl.org/docs/2.8/ssl_faq.html#cert-ownca)

---

**Note**

Tools for generating and signing your own certificate are included with OpenSSL, free software from [http://www.openssl.org/](http://www.openssl.org/).

Alternatively, when the CSR has been generated, submit it to a Certificate Authority (CA). The CA will return the certificate in PEM format.
If you are acquiring a certificate for the first time, search the Internet for “certificate authority services SSL server certificates,” and choose the service that best meets the needs of your organization. Follow the service’s instructions for obtaining an SSL certificate.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Create a public-private key pair.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Generate a Certificate Signing Request (CSR).</td>
</tr>
<tr>
<td>Step 3</td>
<td>Self-sign the certificate. Alternatively, contact a Certificate Authority (CA) to sign the certificate. The certificate you upload must use the X.509 standard, and you must install the matching private key on your LDAP server.</td>
</tr>
</tbody>
</table>

### Managing Certificates

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Click the Admin tab to display the Authentication menu, then click Management to display the Upload LDAP Certificates panel.</th>
</tr>
</thead>
</table>
|        | **Upload LDAP Certificates**  
|        | Upload LDAP certificates to be used in secure communication with your organization's LDAP servers. |  
| Certificate Name | Certificate Subject | Remove |
| Test | CN=LDAP, DC=scanslab, DC=local | Y |
| ![Certificate Management Screen](image) |
| Step 2 | Enter a unique Certificate name. |
| Step 3 | Click Browse to navigate to and select the required certificate. |
| Step 4 | Click Add to upload the certificate. |

**What to do next**  
Click the Remove icon to remove a certificate.

### Authenticating Users

When users access the Web through Cisco Cloud Web Security, they may be prompted to enter a username and password. Cisco Cloud Web Security requires authentication credentials for some users depending on the configured Identity and Access Policy groups. Users should enter the username and password of the credentials that are recognized by your organization’s authentication server.
When enabling authentication with an LDAP authentication realm, ensure users do not enter the Windows domain name.

Working with Failed Authentication

Sometimes users are blocked from the Web due to authentication failure. The following list describes reasons for authentication failure and remedial actions that you can take:

• **Client application cannot perform authentication.** Some clients cannot perform authentication or cannot perform the type of authentication that is required. If a client application causes authentication to fail, you can create a web filtering rule to allow the client to connect.

• **Authentication server is unavailable.** An authentication server may be unavailable if the network connection is broken or if the server is experiencing a problem. You can set the desired behavior in the Failover options to block the user, use cached credentials, or apply the default policy.

• **Invalid credentials.** When a client passes invalid authentication credentials, Cisco Cloud Web Security continually requests valid credentials, essentially blocking access to the Web by default.

Working with Authentication Realms

An authentication realm is a set of authentication servers, a single server, or an identity provider that supports a single authentication protocol with a particular configuration. Each server in an LDAP realm shares the same logical database; any server will return the same results for a given user. Typically, a realm will have a one-to-one match with a Windows domain. The realm is the context in which usernames, group names, and so on should be unique.

You can perform any of the following tasks when configuring authentication:

• Include one or more authentication servers in a realm.

• Create one or more LDAP realms.

• Create one or more SAML realms.

• Edit existing authentication realms.

When using SAML, only one SAML realm can be active. All other SAML and LDAP realms must be inactive.

It is also possible to include an authentication server in multiple realms, although typically this is not required unless you use an Active Directory Global Catalog, which stores a limited read-only copy of data for multiple domains or realms.
Creating an LDAP Authentication Realm

Procedure

Step 1  Navigate to Admin > Authentication > Management to display the Authentication Realms pane.

Step 2  Click Add LDAP Realm to display the Network connection pane.

Step 3  Enter a unique Realm Name.

Step 4  For each server you want to add to the realm:
   a) Enter an IP address in IPv4 format or a hostname in the Host Name box.
   b) In the Protocol drop-down, choose the required protocol: LDAP, StartTLS, or SSL (LDAPS).
   c) Enter a Port. The default for LDAP and StartTLS is 389. The default for LDAPS is 636.
   d) Click Check Connection.

You can click Add Another Server to add as many servers as you want. You can click Remove server to remove any unwanted servers.

Step 5  When a connection has been successfully made, if your LDAP server accepts anonymous queries, select the Server Accepts Anonymous Queries check box. Alternatively, enter the LDAP server’s distinguished name in the Bind DN box, and enter the Password.

Step 6  Click Check Authentication.

Step 7  Accept or change the Search Base.

Step 8  In the Search Attribute drop-down list, choose the attribute that contains the username. This can be cn, uid, or sAMAccountName. Alternatively, select custom and enter an attribute in the box.

Step 9  In the User Filter Query drop-down list, choose a query to exclude non-user LDAP entries. This can be None or (objectClass=person). Alternatively, select custom and enter a query in the box.

Step 10 Accept or enter a Subject Attribute. This box must not be left empty.

Step 11  To locate users by attribute, click Group Member Of Attribute. Accept the memberOf attribute or click custom and enter an attribute in the box. Alternatively, to locate users by group, click Group Members Attribute. Accept the users attribute or click custom and enter an attribute in the box.

Step 12 Click Browse to populate the Exclude the following groups list.

Select the element’s check box to include an element. Elements may include:

- users
- groups
- organizational units (OUs)
- computers
- folders
- miscellaneous elements

Click the expand icon ( ▶ ) to expand or collapse an element.

Click the filter icon ( ▼ ) to add a filter to an element.

Click the filter enabled icon ( ◀ ) to edit or remove a filter.
Creating an LDAP Authentication Realm

Step 13 Click **Select** to add the selected elements. Alternatively, click **Cancel** to abandon your selection.

Step 14 Click **Browse** to populate the Use the following groups list.

Step 15 Click **Select** to add the selected elements. Alternatively, click **Cancel** to abandon your selection.

Step 16 (Optional) Click **Advanced settings** to display the additional settings:
   a) Enter number of nodes to traverse in the Nested Group Depth box.
   b) Enter the maximum number of groups to search in the Maximum Groups box.

Step 17 In the Groups Display drop-down list, choose WinNT groups or LDAP standard to determine how the groups will be displayed.

Step 18 Enter a user name in the Check Sample User box and click Check LDAP to verify your settings.

Step 19 Click the required failover option; Block user, Use cached credentials, or Grant default policy.

Step 20 (Optional) To exclude users from authentication:
   a) In the Custom Attributes pane, enter an LDAP Attribute to match.
   b) In the Rule Match drop-down list, choose an operator and enter a value in the box. The available operators are:
      • Equals
      • Less Than
      • Regex
      • Is True
      • Is False
   c) In the Action list click **Block User**.
   d) Click **Add**.
      You can click the **Remove** icon to remove the user filter.

Step 21 (Optional) To add users to a group for the duration of an authenticated session:
   a) In the Custom Attributes pane, enter an LDAP Attribute to match.
   b) In the Rule Match drop-down list, choose an operator and enter a value in the box. The available operators are:
      • Equals
      • Less Than
      • Regex
      • Is True
      • Is False
c) In the **Action** drop-down list, choose **Add to Group**.
d) Click **Add**.

You can click the **Remove** icon to remove the user filter.

**Note**  To add a user to a group, the group must exist in the LDAP directory with its name formatted as an LDAP distinguished name (DN).

**Step 22** When you have finished configuring the authentication realm, click **Apply settings**. Alternatively, navigate to another page to abandon your changes.

---

## Creating a SAML Authentication Realm

### Before you begin

Cisco Cloud Web Security SAML authentication requires a supported and correctly configured IdP accessible from your organization's network.

- To configure your IdP automatically, you will need the Cisco Cloud Web Security SAML metadata.
- To configure your IdP manually, you will need the individual service provider issuer ID, assertion consumer endpoint URL, and SAML request signing certificate.
- To configure Cisco ScanCenter automatically, you will need your IdP's metadata.
- To configure Cisco ScanCenter manually, you will need the IdP endpoint address, group attribute, and signing certificate in DER or PEM format.

In Cisco ScanCenter, create a custom group for each group you created at the IdP. The names must be an exact match. The IdP passes the group name to Cisco Cloud Web Security using the group attribute. Policy configured for the custom group is then applied to the SAML user based on their IdP group.

To download the metadata from Cisco ScanCenter, click the **Admin** tab to display the **Authentication** menu, then click **Management** to display the **Authentication Realms** pane. Click **Add SAML Realm** and then click **Export our SAML metadata** to download the metadata. For information on importing the metadata into your IdP, refer to your vendor's support documentation.

To obtain the individual service provider issuer ID and assertion consumer endpoint URL information and to download the SAML request signing certificate from Cisco ScanCenter, click the **Admin** tab to display the **Authentication** menu, then click **Management** to display the **Authentication Realms** pane. Click **Add SAML Realm** and then click **View our SAML configuration**. Make a note of the **Service Provider Issuer ID** and **Assertion Consumer Endpoint URL**. Then click **Export primary signing certificate**, and then click **Export secondary signing certificate** to download the primary and secondary SAML request certificates.

**Note**  Your IdP must send the Cisco Cloud Web Security username in the NameId attribute in the SAML assertion. For more information on configuring your IdP, exporting your IdP metadata, obtaining your IdP details, or downloading your IdP signing certificate, refer to your vendor's support documentation.
Procedure

Step 1  Click the Admin tab to display the Authentication menu, then click Management to display the Authentication Realms pane.

Step 2  Click Add SAML Realm.

Step 3  Click View our SAML configuration to display the SAML Realm Configuration pane.

Step 4  If you have your identity provider metadata, click Import your IdP metadata to import it. Alternatively, if you are configuring Cisco ScanCenter manually:
   a) Click Manually enter your IdP details.
   b) Enter a Realm Name.
   c) Enter the IdP Endpoint Address URL.
   d) Enter the Group Attribute name used by your IdP.
   e) Click Choose File to upload your IdP Signing Certificate.

You can click the Remove icon to remove an existing identity provider signing certificate.

Step 5  Click Apply settings. Alternatively, navigate away from the page to abandon your changes.

Note  You can edit the configuration and upload additional IdP certificates.

Managing Authentication Realms

To manage an existing authentication realm, click the Admin tab to display the Authentication menu, then click Management to display the Authentication Realms panel.

To activate an inactive realm, select the Active check box and click Apply settings.

To deactivate an active realm, clear the Active check box and click Apply settings.

To download an audit of a realm, click the CSV icon.

To remove a realm, click the Remove icon.

To change a realm, click the Edit icon.

Note  Multiple LDAP authentication realms can be active at the same time. However, when a SAML realm is active no other realms, LDAP or SAML, can be active.

Cisco Cloud Web Security Behavior with Multiple Realms

You can configure Cisco Cloud Web Security to provide users with a choice of authentication realms which may include multiple servers with different security protocols.

For example, you may want to configure multiple realms if your organization acquires another organization that has its own authentication server using the same or a different security protocol. That way, you can create one policy for all users.
Multiple Realms are not supported when using SAML.

Testing Authentication Settings

When you create or edit an authentication realm, you enter a lot of configuration settings to connect to an authentication server or identity provider. The information you enter is validated at each stage of the process to ensure the correct information has been entered.

Caution

If you make configuration changes to an LDAP server, you must edit your authentication realms in Cisco ScanCenter to match the changes or your users will not be able to authenticate.

Testing Process

When you test authentication settings, Cisco ScanCenter first verifies that the settings you entered for the realm are in valid formats. For example, if a field requires a text string and it currently contains a numeric value, Cisco ScanCenter informs you of that error.

If all fields contain valid values, Cisco ScanCenter performs different steps, depending on the security protocol. If the realm contains multiple authentication servers, Cisco ScanCenter goes through the testing process for each server in turn.

LDAP Testing

Cisco ScanCenter performs the following steps when testing LDAP authentication settings:

1. It ensures that the LDAP server is listening on the specified LDAP port.
2. If Secure LDAP is selected, Cisco ScanCenter ensures the LDAP server supports Secure LDAP.
3. If StartTLS is selected, Cisco ScanCenter ensures the LDAP server supports the StartTLS extension.
4. If the realm includes bind parameters, Cisco ScanCenter validates them by attempting to authenticate with the LDAP server.

Setting the Cookie Duration

Clientless authentication uses cookies stored in the browser. By default, cookies persist for the duration of the browser session. Enabling persistent cookies enables the user to close the browser without having to re-authenticate within the time period you choose.

Procedure

Step 1
Click the Admin tab to display the Authentication menu, then click Management to display the Cookie Expiry panel.
**Step 2**  (Optional) Select the **Use Persistent Cookies** check box to enable sessions to persist after the browser is closed.

**Step 3**  Enter the duration, in the format shown in the on-screen example, before group cookies expire in the **Group** box.

**Step 4**  Enter the duration, in the format shown in the on-screen example, before user cookies expire in the **User** box.

**Step 5**  Enter the duration, in the format shown in the on-screen example, before roaming cookies expire in the **Roaming** box.

**Step 6**  Click **Apply**. Alternatively, navigate away from the page to abandon your changes.

### Downloading Audit Reports

**Procedure**

**Step 1**  Click the **Admin** tab to display the **Authentication** menu, then click **Management** to display the **Download Audit Reports** panel.

**Step 2**  Click a **Period** the report will cover. The available options are:

- Last 5 Minutes
- Last Hour
- Last Day

**Step 3**  Click the **CSV** icon.

### Configuring the User Authentication Page

Cisco Cloud Web Security displays the User Authentication page when a user that is not already authenticated attempts to connect to the service.
Procedure

Step 1  Click the Admin tab to display the Authentication menu, then click User Messages to display the User Messages panel.

Step 2  Click Choose File and navigate to an image you want to be displayed on the page. The image can be in PNG, GIF, or JPEG format and must be no larger than 500K. It can be any pixel size you want, but you should use something appropriate for the screen size of the devices your users will connect to the service.

Step 3  Enter up to 1,000 characters of plain text in the Help text box.

Step 4  Enter the word or phrase you want to use in the User name text box.

Step 5  Enter the word or phrase you want to use in the Password text box.

Step 6  Enter up to 1,000 characters of plain text in the Disclaimer text box.

Step 7  Click Preview to display the User Authentication page.
Step 8  Click **Apply settings** to make your changes permanent. Alternatively, click **Cancel** to continue editing the **User Authentication** page or navigate away from the page to abandon your changes.
CHAPTER 6

Log Extraction

- Overview, on page 37
- Reporting Attributes, on page 38
- Issuing a Key Pair, on page 42

Overview

Cisco ScanCenter allows you to extract your data logs from the Cisco Cloud Web Security storage architecture. Configure secure and fully automated extraction of your web usage data for import and analysis using your SIEM platform S3-compatible Application Programming Interface (API). The log extraction service uses Amazon Simple Storage Service (S3) protocol only for the purpose of API compatibility; it does not use Amazon Web Services.

Data logs:

- compiled in World Wide Web Consortium (W3C) text format
- tab delimited with UTF-8 encoding
- placed in a dedicated storage bucket assigned to your company for your secure extraction
- allows you to choose what data you want to pull and when you want to extract the data
- typically available within 15 minutes after the event
- files deleted after five days

Note:

- If you have anonymization rules in place, all anonymized fields will also apply in the extracted log data.
- Visibility of the data in HTTPS traffic will be the same as in the WIRE reports.
- All accounts within the delegated administration hierarchy log data to the same location. Account details are visible in the master account.
- Child account data consolidated into a single bucket. Reporting attribute x-ss-company-id used to identify child accounts.
Reporting Attributes

25 commonly-used reporting attributes are included in the data logs. Four optional attributes can also be included.

The field prefixes are:

- c—client
- s—server
- cs—client to server
- sc—server to client
- x-ss—Cisco Cloud Web Security custom field

Note

The contents of the majority of attributes are normalized to lower case. However, for some attributes you may wish to view the original string as entered by the user. Attributes listed with “Original” in parentheses are available in normalized and original form.

datetime
Date and time

c-ip
Client IP address

cs(X-Forwarded-For)
Value of the X-Forwarded-For header

cs-username
(Original) Username logged in the form of WinNT://<username> or a custom text name

cs-method
(Original) Request method: CONNECT, GET, POST

cs-uri-scheme
Referrer protocol: FTP, HTTP, HTTPS

cs-host
(Original) Host part of the URL string; for example, in news.example.com/sport the host is news.example.com
**cs-uri-port**

Port number of web request

**cs-uri-path**

Path part of the URL string; for example, in `news.example.com/sport` the path is `/sport`

**cs-uri-query**

Query part of the URL string; for example, in `http://www.example.com/search?hl=en&q=free+screensavers&btnG=Example+Search&meta=&aq=f&oq=` the query is `hl=en&q=free+screensavers&btnG=Example+Search&meta=&aq=f&oq=`

**cs(User-Agent)**

(Original) Complete user agent string; for example, `Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)` (more information on user agent strings can be found at [http://www.useragentstring.com/pages/useragentstring.php](http://www.useragentstring.com/pages/useragentstring.php))

**cs(Content-Type)**

(Original) Request content type; for example, `image/gif, application/pdf, text/html, application/EDI-X12`

**cs-bytes**

Bytes sent

**sc-bytes**

Bytes received

**sc-status**

Response Status Code; for example, to find all web requests to pages that did not exist, you can filter by 404 (more information on status codes can be found at [http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html](http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html))

**sc(Content-Type)**

(Original) Response content type

**s-ip**

Destination IP address

**x-amp-score**

(Optional) AMP score of the request, if available

**x-amp-sha**

(Optional) Request/response SHA256 for the executable/PDF
### x-avc-app

(Optional) Human readable AVC application name

### x-avc-app-id

(Optional) AVC application ID, if detected

### x-ss-category

Web filtering category; the category codes that apply to the x-ss-category reporting attribute are:

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Code</th>
<th>Description</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>c:adlt</td>
<td>Adult</td>
<td>c:gamb</td>
<td>Gambling</td>
<td>c:pnet</td>
<td>Professional Networking</td>
</tr>
<tr>
<td>c:adv</td>
<td>Advertisements</td>
<td>c:game</td>
<td>Games</td>
<td>c:pol</td>
<td>Politics</td>
</tr>
<tr>
<td>c:alc</td>
<td>Alcohol</td>
<td>c:gov</td>
<td>Government and Law</td>
<td>c:porn</td>
<td>Pornography</td>
</tr>
<tr>
<td>c:art</td>
<td>Arts</td>
<td>c:hack</td>
<td>Hacking</td>
<td>c:ref</td>
<td>Reference</td>
</tr>
<tr>
<td>c:astr</td>
<td>Astrology</td>
<td>c:hate</td>
<td>Hate Speech</td>
<td>c:rel</td>
<td>Religion</td>
</tr>
<tr>
<td>c:aucr</td>
<td>Auctions</td>
<td>c:hlth</td>
<td>Health and Nutrition</td>
<td>c:rest</td>
<td>Real Estate</td>
</tr>
<tr>
<td>c:aud</td>
<td>Streaming Audio</td>
<td>c:ilac</td>
<td>Illegal Activities</td>
<td>c:saas</td>
<td>Saas and B2B</td>
</tr>
<tr>
<td>c:busi</td>
<td>Business and Industry</td>
<td>c:ildl</td>
<td>Illegal Downloads</td>
<td>c:sci</td>
<td>Science and Technology</td>
</tr>
<tr>
<td>c:card</td>
<td>Digital Postcards</td>
<td>c:img</td>
<td>Photo Search / Images</td>
<td>c:scty</td>
<td>Society and Culture</td>
</tr>
<tr>
<td>c:cell</td>
<td>Mobile Phones</td>
<td>c:infr</td>
<td>Infrastructure and Content Delivery</td>
<td>c:shop</td>
<td>Shopping</td>
</tr>
<tr>
<td>c:chat</td>
<td>Chat and Instant Messaging</td>
<td>c:job</td>
<td>Job Search</td>
<td>c:snet</td>
<td>Social Networking</td>
</tr>
<tr>
<td>c:comm</td>
<td>Online Communities</td>
<td>c:kids</td>
<td>Safe for Kids</td>
<td>c:socs</td>
<td>Social Science</td>
</tr>
<tr>
<td>c:comp</td>
<td>Computers and Internet</td>
<td>c:ling</td>
<td>Lingerie and Swimsuits</td>
<td>c:sprt</td>
<td>Sports and Recreation</td>
</tr>
<tr>
<td>c:cscc</td>
<td>Computer Security</td>
<td>c:lol</td>
<td>Humor</td>
<td>c:srch</td>
<td>Search Engines and Portals</td>
</tr>
<tr>
<td>c:date</td>
<td>Dating</td>
<td>c:lotr</td>
<td>Lotteries</td>
<td>c:swup</td>
<td>Software Updates</td>
</tr>
<tr>
<td>c:drug</td>
<td>Illegal Drugs</td>
<td>c:mail</td>
<td>Web-based E-mail</td>
<td>c:sxed</td>
<td>Sex Education</td>
</tr>
</tbody>
</table>
x-ss-last-rule-name
(Original) Policy rule name

x-ss-last-rule-action
Five rule actions to choose from: allow, authenticate, block, warn, inspect

x-ss-block-type
Type of block or pattern, specified in the filter, that generated the block

x-ss-block-value
String value that matched the block pattern

x-ss-referrer-host
(Original) Host part of the referrer URL string; for example, in news.example.com/sport the host is news.example.com

x-ss-external-ip
External IP address that Cisco Cloud Web Security gets from the customer (also known as the egress IP address); can also be the subnet of the external IP address (also known as the egress IP address subnet)
**Issuing a Key Pair**

Issue a key pair from the **Log Extraction** page in Cisco ScanCenter. Copy both keys into your SIEM platform S3-compatible API to enable extraction of data logs from your assigned bucket.

---

**Note**

We do not provide technical support for configuring SIEM devices or third-party products. In the event of an issue, consult the vendor-specific support team.

---

**Before you begin**

- The log extraction service must be enabled and provisioned for your company.
- Only your super user administrator can access the **Log Extraction** page.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Click the <strong>Admin</strong> tab to display the administration menus.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>In the <strong>Your Account</strong> menu, click <strong>Log Extraction</strong> to display the <strong>Log Extraction</strong> page.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>In the <strong>Bucket</strong> column of the <strong>Connection Details</strong> area, a dedicated bucket with a unique name based on your Company ID is created to hold your private data.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>In the <strong>Actions</strong> column of the <strong>Credentials</strong> area, click the <strong>Issue Key</strong> button.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>In the <strong>Warning</strong> dialog box, click the <strong>Issue &amp; Download</strong> button.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Save the resulting CSV file named <code>keypair.csv</code> to your downloads folder. The <strong>Access Key</strong> will be updated to show the generated key ID, but the secret key is not displayed anywhere in Cisco ScanCenter for the purpose of security. To maintain privacy, Cisco Customer Support will not ask for the secret key.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Open the saved CSV file named <code>keypair.csv</code> to view your <strong>accessKey</strong> and <strong>secretKey</strong>. The <strong>accessKey</strong> is a 20-character string, while the <strong>secretKey</strong> is a 40-character string.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>(Optional) The <strong>Log Extraction Attributes</strong> area lists some additional attributes you may select to add to exported logs. Additional services may need to be activated to see data in these fields. Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attribute Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>x-avc-app-id</td>
<td>AVC application ID, if detected</td>
</tr>
<tr>
<td>x-avc-app</td>
<td>Human readable AVC application name</td>
</tr>
<tr>
<td>x-amp-score</td>
<td>AMP score of the request, if available</td>
</tr>
<tr>
<td>x-amp-sha</td>
<td>Request/response SHA256 for the executable/PDF</td>
</tr>
</tbody>
</table>
What to do next

Copy the pair of keys into your API client and configure it for extraction.

For example, s3cmd is a free command-line tool that can be used as a client to test connectivity to the log extraction service.

After downloading and installing the s3cmd tool, edit the following variables in the s3cmd configuration file:

- Set `access_key` to your `accessKey`
- Set `secret_key` to your `secretKey`
- Set `host_base` to `vault.scansafe.com`
- Set `host_bucket` to `%(bucket)s.vault.scansafe.com`
- Set `use_https` to `True`
- Set `signature_v2` to `True`

As an example result, the variables would then appear as:

- `access_key=12345678901234567890`
- `secret_key=1234567890123456789012345678901234567890`
- `host_base=vault.scansafe.com`
- `host_bucket=%(bucket)s.vault.scansafe.com`
- `use_https=True`
- `signature_v2=True`

---

**Note**
The `%(bucket)s.vault.scansafe.com` value in the `host_bucket` variable does not use your dedicated bucket name.

For information on how to use the s3cmd tool, see:

- [http://s3tools.org/usage](http://s3tools.org/usage)
- [http://s3tools.org/s3cmd-howto](http://s3tools.org/s3cmd-howto)
- [http://s3tools.org/s3cmd-sync](http://s3tools.org/s3cmd-sync)

---

**Note**
Only read commands are allowed to access your bucket. For example, the `ls`, `get`, `debug`, `sync`, and `info` read commands are allowed, while the `put` write command is not allowed.
If the client application being used to access the Log Extraction API sends requests through the Cisco Cloud Web Security service, it may be challenged for authentication. If the client application is unable to respond to the authentication challenge correctly, the requests to the Log Extraction API will be blocked by the Cisco Cloud Web Security service. In this case, allow the client application direct access to the Log Extraction API by adding an exception for the URL vault.scansafe.com on TCP port 443.
Hosted Configuration

The hosted configuration area of Cisco ScanCenter enables you to upload and manage configuration files such as for PAC (proxy auto-config) and Cisco AnyConnect Secure Mobility Web Security.

Note the following prerequisites when working with hosted configuration:

- Test the PAC files to ensure that they function correctly before uploading them to Cisco ScanCenter.

- Upload the unscrambled version of the AnyConnect Web Security configuration file. The file is scrambled before it is served to your users, but you will still be able to download the plain text version.

- Allow access to the ingress IP addresses of the CWS towers/proxies for AnyConnect Web Security using TCP port 443 (and port 8080 in the case of deploying in plain mode). The list of proxies can be found at http://80.254.145.118/websecurity-config-v2ip.xml. This applies to the AnyConnect Web Security client in general, regardless of hosted configuration.

- The client itself must also be able to access 80.254.145.118 on TCP port 80 which it uses to fetch the list of proxy towers and keep itself up to date. This applies to the AnyConnect Web Security client in general, regardless of hosted configuration.

- Allow the AnyConnect Web Security module to make connections to Verisign over TCP port 80. On this range, clients check the certificate of revocation at Tj.symcb.com, T1.symcb.com, and T2.symcb.com.

- The AnyConnect client downloads its configuration files from the resource service through a hardcoded hostname in the AnyConnect binary. The request is made to hostedconfig.scansafe.net (IP address: 46.255.41.2). The exchange is encrypted over TCP port 443.

- Ensure clients are using the same license key (company/group/user) that is associated with the Hosted Config that is defined and hosted in Cisco ScanCenter.

- Client machines running the AnyConnect Web Security agent must have the Thawte Primary Root CA and Thawte SSL CA–G2 in the Trusted Root Certification Authority Store.

To view your hosted configuration files, click the Admin tab to display the administration menus. Then, in the Management menu, click Hosted Config.

- Uploading a New Configuration File, on page 46
- Managing Configuration Files, on page 46
- Removing Configuration Files, on page 47
Uploading a New Configuration File

Procedure

Step 1  Click the Upload Config tab to display the Upload Config page.
Step 2  Click the required file type in the Resource Format box.
Step 3  Enter a unique Description in the box.
Step 4  Click Browse to select a file to upload. There is a maximum file size limit of 500 kilobytes.
Step 5  Click Upload to upload the file.

Managing Configuration Files

When you have uploaded a file you can activate or deactivate it, upload newer versions, and delete versions.

Procedure

Step 1  Click the Admin tab to display the administration menus.
Step 2  In the Management menu, click Hosted Config to display the Hosted Config page.
Step 3  Click the Edit icon.
What to do next

To activate a configuration file, select the **Active** check box, then click **Save**. Alternatively, clear the check box to deactivate the configuration file, then click **Save**.

When there are two or more versions of a file, click **Default** to enable a specific version, then click **Save**.

To remove a specific version of a file, click **Delete**.

---

**Caution**

When you click **Delete** the file will be deleted immediately unless it is the default version. You will not be asked to confirm your action.

---

Removing Configuration Files

**Before you begin**

Only configuration files that are inactive can be completely removed.

---

**Caution**

Files are removed immediately. You will not be asked to confirm your actions.

---

**Procedure**

**Step 1**

Click the **Admin** tab to display the administration menus.

**Step 2**

In the **Management** menu, click **Hosted Config** to display the **Hosted Config** page.

**Step 3**

Click the **Delete** icon.
Audits

You can generate access and activity audits for your organization’s Cisco ScanCenter account. You can also configure email alerts to notify you of failed Cisco ScanCenter login attempts. You must have the correct role to be able to perform these tasks. For more information on roles, see Role Permissions, on page 9.

- Email Alerts, on page 49
- Access Audit, on page 50
- Activity Audit, on page 51
- Report Execution, on page 52
- Report Management, on page 53
- Log Extraction Audit, on page 53

Email Alerts

Procedure

Step 1  Click the Admin tab to display the administration menus.

Step 2  In the Audit menu, click Access Settings to display the Access Settings page.

<table>
<thead>
<tr>
<th>Login Failure Message Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the contact email is left blank, the superuser’s email address will be used.</td>
</tr>
<tr>
<td>Contact email in the login failure message: [field]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Email Alert Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable email alerts [checkbox]</td>
</tr>
<tr>
<td>Email addresses to be alerted in the event of login failures [fields]</td>
</tr>
<tr>
<td>Limit the rate of email alerts [dropdown: Max frequency 3, Period (hours) 1]</td>
</tr>
</tbody>
</table>

Save
Step 3 When a user account is locked, following a series of failed login attempts, the user is instructed to send an email to an administrator to unlock the account. Enter the administrate email address to display in the **Contact email in the login failure message** box. If no address is provided, the organization super user’s email address is displayed.

Step 4 Select the **Enable email alerts** check box to send an email whenever there is a failed login attempt.

Step 5 Enter up to five email addresses in the boxes.

Step 6 In the **Max frequency** drop-down, choose the number of email alerts to batch together (1 to 20).

Step 7 In the **Period** drop-down, choose the delay between emails in hours (1 to 24).

Step 8 Click **Save** to apply your changes. Alternatively, navigate away from the page to abandon your changes.

---

**Access Audit**

Generating an access audit enables you to see all the login attempts that have occurred in Cisco ScanCenter over a period of time, from a day up to a year.

**Procedure**

**Step 1** Click the **Admin** tab to display the administration menus.

**Step 2** In the **Audit** menu, click **ScanCenter Access**.

**Step 3** In the **Time Zone** drop-down list, choose a time zone. The default is UTC.

**Step 4** In the **Time Period** drop-down list, choose a pre-defined time period.

The pre-defined time periods are:

- Previous hour
- Previous day - yesterday
- Previous week - the last full week
- Last n hours (12, 24, 48, or 72)
- Last week - the previous seven days
- Last n weeks (2 or 3)
- Last month
- Last n months (2, 3, 4, 5, 6, 9, or 12)

Alternatively, click **Custom** and enter the required start and end dates and times:

a) Enter a start date in the box or click the **Calendar** icon to choose a date.

b) Choose a start time using the hour and minute lists. The time is shown using the 24-hour clock.

c) Enter an end date in the box or click the **Calendar** icon to choose a date.

d) Choose an end time using the hour and minute lists.

**Step 5** In the **Select Admin** section, clear the **All Admins** check box, and select an admin user in the **or select an Admin** drop-down list. Select the **Cisco Operations** Admin to include records of **ss_super actions**. Alternatively, select the **All Admins** check box to include all admin users.

**Step 6** Select the **Unsuccessful Login** check box to include unsuccessful login attempts in the audit. Alternatively, clear the check box to exclude unsuccessful login attempts.
Step 7 Select the Successful Login check box to include successful login attempts in the audit. Alternatively, clear the check box to exclude successful login attempts.

Step 8 Click Generate Audit to download the audit as a CSV file.

Activity Audit

Generating an activity audit enables you to see all the administration activity that has taken place in Cisco ScanCenter over a period of time, from a day up to a year. Audits provide a record of changes to administration, configuration, filtering, and policy. The audit is downloaded as a CSV file containing the username, category type, action, log time, and a description for each logged event.

Procedure

Step 1 Click the Admin tab to display the administration menus.

Step 2 In the Audit menu, click ScanCenter Activity.

Step 3 In the Time Zone drop-down list, choose a time zone. The default is UTC.

Step 4 In the Time Period drop-down list, choose a pre-defined time period. The pre-defined time periods are:

- Previous hour
- Previous day - yesterday
- Previous week - the last full week
- Last $n$ hours (12, 24, 48, or 72)
- Last week - the previous seven days
- Last $n$ weeks (2 or 3)
- Last month
- Last $n$ months (2, 3, 4, 5, 6, 9, or 12)

Alternatively, click Custom and enter the required start and end dates and times:

a) Enter a start date in the box or click the Calendar icon to choose a date.
b) Choose a start time using the hour and minute lists. The time is shown using the 24-hour clock.
c) Enter an end date in the box or click the Calendar icon to choose a date.
d) Choose an end time using the hour and minute lists.

Step 5 In the Select Admin section, clear the All Admins check box, and select an admin user in the or select an Admin drop-down list. Select the Cisco Operations Admin to include records of ss_super actions. Alternatively, select the All Admins check box to include all admin users.

Step 6 In the Select Category section, clear the All Categories check box, and select a category in the or select a Category drop-down list. The available categories are:

- Administration
- Filtering Policy
- HTTPS Inspection
- Spyware
- Web Virus Policy
Alternatively, select the All Categories check box to include all categories.

**Step 7**
In the Select Action section, clear the All Actions check box, and select an action in the or select an Action drop-down list. The available actions are:

- INSERT
- UPDATE
- DELETE

Alternatively, select the All Actions check box to include all actions.

**Step 8**
Click Generate Audit to download the audit as a CSV file.

---

**Report Execution**

Generating a report execution audit enables you to see all the reports that have been run in Cisco ScanCenter over a period of time, from a day up to a year. The audit is downloaded as a CSV file containing the username, report name, and log time.

**Procedure**

**Step 1**
Click the Admin tab to display the administration menus.

**Step 2**
In the Audit menu, click Report Execution to display the Report Execution page.

**Step 3**
In the Time Zone drop-down list, choose a time zone. The default is UTC.

**Step 4**
In the Time Period drop-down list, choose a pre-defined time period. The pre-defined time periods are:

- Previous hour
- Previous day - yesterday
- Previous week - the last full week
- Last n hours (12, 24, 48, or 72)
- Last week - the previous seven days
- Last n weeks (2 or 3)
- Last month
- Last n months (2, 3, 4, 5, 6, 9, or 12)

Alternatively, click Custom and enter the required start and end dates and times:

a) Enter a start date in the box or click the Calendar icon to choose a date.

b) Choose a start time using the hour and minute lists. The time is shown using the 24-hour clock.

c) Enter an end date in the box or click the Calendar icon to choose a date.

d) Choose an end time using the hour and minute lists.

**Step 5**
Click Generate Audit to download the audit as a CSV file.
Report Management

Generating a report management audit enables you to see who's created, modified, or deleted what reports and report related entities in Cisco ScanCenter over a period of time, from a day up to a year. The audit is downloaded as a CSV file containing the username, entity type, entity name, action, and log time.

**Procedure**

**Step 1** Click the Admin tab to display the administration menus.

**Step 2** In the Audit menu, click Report Management to display the Report Management page.

**Step 3** In the Time Zone drop-down list, choose a time zone. The default is UTC.

**Step 4** In the Time Period drop-down list, choose a pre-defined time period.

The pre-defined time periods are:

- Previous hour
- Previous day - yesterday
- Previous week - the last full week
- Last $n$ hours (12, 24, 48, or 72)
- Last week - the previous seven days
- Last $n$ weeks (2 or 3)
- Last month
- Last $n$ months (2, 3, 4, 5, 6, 9, or 12)

Alternatively, click Custom and enter the required start and end dates and times:

a) Enter a start date in the box or click the Calendar icon to choose a date.

b) Choose a start time using the hour and minute lists. The time is shown using the 24-hour clock.

c) Enter an end date in the box or click the Calendar icon to choose a date.

d) Choose an end time using the hour and minute lists.

**Step 5** Click Generate Audit to download the audit as a CSV file.

Log Extraction Audit

Generating a log extraction audit enables you to see all the log extractions that have been run in Cisco ScanCenter over a period of time, from a day up to a year. The audit is downloaded as a CSV file containing log date, access IP address, event type, quantity, and HTTP status code.

**Procedure**

**Step 1** Click the Admin tab to display the administration menus.

**Step 2** In the Audit menu, click Log Extraction.

**Step 3** In the Time Zone drop-down list, choose a time zone. The default is UTC.
Step 4  In the **Time Period** drop-down list, choose a pre-defined time period.

The pre-defined time periods are:

- Previous hour
- Previous day - yesterday
- Previous week - the last full week
- Last $n$ hours (12, 24, 48, or 72)
- Last week - the previous seven days
- Last $n$ weeks (2 or 3)
- Last month
- Last $n$ months (2, 3, 4, 5, 6, 9, or 12)

Alternatively, click **Custom** and enter the required start and end dates and times:

a) Enter a start date in the box or click the **Calendar** icon to choose a date.
b) Choose a start time using the hour and minute lists. The time is shown using the 24-hour clock.
c) Enter an end date in the box or click the **Calendar** icon to choose a date.
d) Choose an end time using the hour and minute lists.

Step 5  Click **Generate Audit** to download the audit as a CSV file.
Chapter 9

Delegated Administration

If you have opted to use delegated administration, you will be provided with access to a parent organization and two or more subsidiary organizations in Cisco ScanCenter. No traffic is passed via the parent organization, but any policies set there will be applied to all subsidiary organizations. Policies set at the subsidiary level will be applied only to that specified subsidiary organization.

- Logging In to the Parent Organization, on page 55
- Enabling Subsidiary Organizations to Create Certificates, on page 55
- Enabling Subsidiary Organizations to Set Policies, on page 56
- Managing Exported and Imported Policy, on page 58
- Managing Filters, Schedules, and Dictionaries, on page 59
- Setting Global and Local User Messages, on page 59
- Configuring Email Domains, on page 59
- Running Audits, on page 59
- Delegated Reporting, on page 59
- Threat Analysis Role, on page 60

Logging In to the Parent Organization

When you log in to the parent organization with the administrator password, the Delegated Administration page is displayed. The parent and child companies are displayed with their associated Seats and Last Use date.

Note

This view of child accounts while logged in to their parent account is only available to Company Super User and Full Access administrators.

Enabling Subsidiary Organizations to Create Certificates

To enable subsidiary organizations to set their own HTTPS Inspection policy, it is necessary to enable them to create their own certificates.
### Enabling Subsidiary Organizations to Set Policies

Policies set at the parent organization are applied automatically to subsidiary organizations but can only be viewed at the parent. Creating and activating an **Execute Subsidiary Policy** rule, enables subsidiary organizations to apply their own policies. The subsidiary rules will be applied after parent rules with a higher priority but before parent rules with a lower priority.

**Note**

Only the parent organization can edit the approved list of potentially unwanted programs.

### Procedure

| Step 1 | Log in to the parent organization as administrator. |
| Step 2 | On the **Delegated Administration** page, click the parent organization. |
| Step 3 | On the **Web Filtering > Management > Policy** page, click **Create Rule**. |
| Step 4 | In the **Rule Action** pull-down list, select **Execute Subsidiary Policy**. |
| Step 5 | Click **Create Rule**. You can create only one rule of this kind. |
Step 6  Select the **Active** check box to enable the **Execute Subsidiary Policy** rule action. This rule represents the policies set at each subsidiary organization.

Step 7  In the Move column, click the up and down arrows to set the order in which the parent and subsidiary policies will be applied.

Step 8  Click **Apply Changes**. The order will be updated.

Clearing the **Active** check box or removing the **Execute Subsidiary Policy** rule will prevent the subsidiary policies from being used.

---

**Enabling HTTPS Inspection**

**Before you begin**

Create and activate an **Execute Subsidiary Policy** rule to enable subsidiary organizations to apply their own policies. See **Enabling Subsidiary Organizations to Set Policies**, on page 56.

**Procedure**

**Step 1**  Log in to the parent organization as administrator.

**Step 2**  On the **Admin > HTTPS Inspection > Policy** page, click **Create HTTPS Rule**.

**Step 3**  In the **Certificate** pull-down list, select **Execute Subsidiary Policy**.

**Step 4**  Select the **Active** pull box to enable the rule action. Alternatively, clear the check box to activate the rule at another time.

**Step 5**  Click **Submit** to apply your changes. Alternatively, click **Cancel** or navigate away from the page to abandon your changes.

---

**Subsidiary Privacy Policy**

When delegated administration is enabled, it is possible for subsidiary organizations to set their own privacy policy.

As with all subsidiary policies, the privacy policy will be active only when the **Active** check box is selected.
Regardless of the priority assigned to the **Execute Subsidiary Policy** rule action, any subsidiary privacy policy will be applied immediately after the parent organization’s privacy rule actions.

---

**Note**

To enable a subsidiary organization to set its own HTTPS policy, the **Execute Subsidiary Policy** rule must be applied to the HTTPS inspection rule at the parent organization.

---

## Managing Exported and Imported Policy

An exported policy can be shared for import between parent and child companies, both within and outside of the same delegated administration family.

When importing an exported child policy into:

- The same child company:
  - Any links to parent filters or schedules will remain intact.
  - All exported data will be imported.

- A different child company within the same delegated administration family:
  - Any links to parent filters or schedules will remain intact.
  - All exported data, except for license keys and HTTPS certificates, will be imported.

- A different child company in a different delegated administration family is supported only if the child company does not have any links to its parent company.

When importing an exported parent policy within the same company:

- All exported data will be imported.

- Any child policy links to the parent filters, schedules, or certificates will remain intact.

- Any new filter, schedule, or certificate that has been added since the export and is currently in use by any child company, will not be removed. Effectively results in a merge with the contents of the export being imported.

- Any new filter, schedule or certificate that has been added since the export and is not currently in use by any child company, will be removed and replaced by the contents of the export being imported.

Importing to a different parent company in a different delegated administration family is supported, but:

- Any company, group, or user license keys will be removed.

- Any HTTPS certificates will be removed.

See **Backing Up a Policy, on page 93** and **Restoring a Policy, on page 94** for details on how to export and import a policy.
Managing Filters, Schedules, and Dictionaries

The filters, schedules, and dictionaries of the parent organization are available at the subsidiary organizations. There they can be viewed and used, but not edited. Filters, schedules, and dictionaries created at the subsidiary organization will not be available at the parent or other subsidiary organizations.

Setting Global and Local User Messages

By default any user messages set at the parent organization will be inherited by the subsidiary organizations.

Procedure

1. Log in to the subsidiary organization as an administrator.
2. Navigate to the required User Messages page.
3. Clear the Inherit Master alert page settings check box.
4. Enter the required message in the box.
5. Click Save to apply your changes.

Configuring Email Domains

Email domains configured at the parent organization are available at every subsidiary organization. This enables you to create an organization-wide email domain. Email domains configured at the subsidiary organization are only available at that organization.

Running Audits

Audits run at a subsidiary organization will only include information for that organization.

Delegated Reporting

Reports run at the parent organization will include results for all of the subsidiary organizations. In addition to the standard reporting attributes, the following attributes are available to refine your searches:

- **Company Name**—Name of the subsidiary organization
- **Company User**—Fully qualified user name including the subsidiary organization name
- **Company Group**—Fully qualified group name including the subsidiary organization name

Reports run at the subsidiary organization will include only results for that organization.
Saved searches will only be available to the organization where they were created. For example, a parent organization would not see the saved searches of a subsidiary organization.

**Threat Analysis Role**

Users with the Threat Analysis role in the parent organization also have access to the Threats tab of their subsidiary organizations. Users with the Threat Analysis role in the subsidiary organization have access to only their own.
CHAPTER 10

Troubleshooting

- Verifying Your Connection to Cisco Cloud Web Security, on page 61
- Service Status Portal, on page 62
- Verifying Policy, on page 62

Verifying Your Connection to Cisco Cloud Web Security

To verify that your connection to Cisco Cloud Web Security is correctly configured, Cisco provides a URL which returns diagnostic information about your connection.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>On a computer that is configured to connect to Cisco Cloud Web Security, open a web browser.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Enter the URL <a href="http://whoami.scansafe.net">http://whoami.scansafe.net</a>.</td>
</tr>
</tbody>
</table>

What to do next

If, for whatever reason, you are not currently connected to the service, the message “User is not currently using the service” is displayed. If you are connected, the following information is displayed:

- authUserName—Your authenticated username
- authenticated—Whether authentication was successful
- companyName—Name of your organization
- connectorVersion—Version of Connector providing the connection
- countryCode—Two-letter country code for your location
- externalIp—Egress IP address
- groupNames—List of user groups associated with your organization
- hash—Hash for your organization
- internalIp—Ingress IP address
- logicalTowerNumber—Data center to which you are currently connected
- staticGroupNames—List of static user groups associated with your organization
- userName—Your username
Service Status Portal

The Service Status Portal provides the current status of all Cisco Cloud Web Security datacenter locations. The portal supplements the Service Notifications and is not intended to replace them. Generally, updates will be first published to the Service Status Portal and then followed by a Service Notification. The Service Notification will provide additional detail and guidance depending on the type of notification. View the portal at http://servicestatus.sco.cisco.com/status

Verifying Policy

To ensure that your filtering settings are being applied as intended to users and groups, Cisco provides a tool called Policy Trace. For details of how to configure policy, see Filtering, on page 63.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>On a computer that is configured to connect to Cloud Web Security, open a Web browser.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Enter the URL <a href="http://policytrace.scansafe.net">http://policytrace.scansafe.net</a>. Providing you are connected to the Internet via Cloud Web Security a page will be displayed prompting you to enter a URL.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Enter URL box, enter the URL for which you want to run a policy trace then click Go. The policy actions that are applied to that website are displayed.</td>
</tr>
</tbody>
</table>

What to do next

The policy trace enables you to ensure the desired policy is applied. The policy trace information is presented in the following format:

Identified user '<user name>' from IP address <IP address> as part of company '<organization>'
User belongs to groups [<list of groups>]
Site categorized as '<category>'

Evaluating # HTTPS rules.
HTTPS rule '<rule name>' matches. Using certificate '<certificate name>' to decrypt.

Evaluating # rules after reading request headers.
Evaluating rule '<rule name>'
Deferring evaluation of rule '<rule name>'.
Headers missing. Skipping quota evaluation.
The website reputation score is <score>.

Evaluating # rules after reading response headers.
Evaluating rule '<rule name>'
Deferring evaluation of rule '<rule name>'

Evaluating # rules after reading the first part of the response body.
Evaluating rule '<rule name>'
Taking allow action because of category '<rule name>'
Found virus named '<virus name>'
Blocking connection because of a virus named '<virus name>'
PART II

Filtering

• Overview, on page 65
• Categories, on page 67
• Filters, on page 81
• Schedules, on page 89
• Policy, on page 91
• Quotas, on page 97
• Global Settings, on page 101
• Cloud Bypass, on page 107
• Spyware, on page 109
• Notifications, on page 111
• Secure Traffic Inspection, on page 113
Overview

Web filtering enables you to control the content that enters and leaves your organization’s internal network. From this area you can manage:

- **Filters.** Each filter contains a set of criteria to be matched before a rule is applied.
- **Schedules.** Control the time of day when rules are applied.
- **Policy.** Determines the order in which rules are applied.
- **Rules.** Composed of combinations of filters and schedules.
- **Quotas.** Control the amount of time your users may spend browsing.
- **Cloud Bypass.** Prevent specific entries from being blocked when using Cisco Integrated Services Routers (ISRs) to send traffic to Cisco Cloud Web Security.
- **Notifications.** Messages that are displayed to users when rules are applied, and email alerts that are sent to notify network administrators.
Categories

Cisco constantly evaluates the relevance of websites within a particular category to ensure the industry’s highest accuracy. The categories and website classifications used by Cisco Cloud Web Security are subject to change without notice. Cisco provides examples for test purposes only and does not endorse these websites.

- Category List, on page 67

Category List

Cisco classifies websites by category. Categories are the primary method for creating web filtering policies. The following list includes example websites that you can use to verify that your filtering policy works as intended.

**Adult**

Directed at adults, but not necessarily pornographic. May include adult clubs (strip clubs, swingers clubs, escort services, strippers); general information about sex, non-pornographic in nature; genital piercing; adult products or greeting cards; information about sex not in the context of health or disease.

- www.adultentertainmentexpo.com
- www.adultnetline.com

**Advertisements**

Banner and pop-up advertisements that often accompany a webpage; other advertising websites that provide advertisement content. Advertising services and sales are classified as “Business and Industry.”

- www.adforce.com
- www.doubleclick.com

**Alcohol**

Alcohol as a pleasurable activity; beer and wine making, cocktail recipes; liquor sellers, wineries, vineyards, breweries, alcohol distributors. Alcohol addiction is classified as “Health and Nutrition.” Bars and restaurants are classified as “Dining and Drinking.”

- www.samueladams.com
- www.whisky.com
Arts
Galleries and exhibitions; artists and art; photography; literature and books; performing arts and theater; musicals; ballet; museums; design; architecture. Cinema and television are classified as “Entertainment.”

- www.moma.org
- www.nga.gov

Astrology
Astrology, horoscope, fortune telling, numerology, psychic advice, tarot.

- www.astro.com
- www.astrology.com

Auctions
Online and offline auctions, auction houses, and classified advertisements.

- www.craigslist.com
- www.ebay.com

Business and Industry
Marketing, commerce, corporations, business practices, workforce, human resources, transportation, payroll, security and venture capital; office supplies; industrial equipment (process equipment), machines and mechanical systems; heating equipment, cooling equipment; materials handling equipment; packaging equipment; manufacturing; solids handling, metal fabrication, construction and building; passenger transportation; commerce; industrial design; construction, building materials; shipping and freight (freight services, trucking, freight forwarders, truckload carriers, freight and transportation brokers, expedited services, load and freight matching, track and trace, rail shipping, ocean shipping, road feeder services, moving and storage).

- www.freightcenter.com
- www.staples.com

Chat and Instant Messaging
Web-based instant messaging and chat rooms.

- www.icq.com
- www.meebo.com

Cheating and Plagiarism
Promoting cheating and selling written work, such as term papers, plagiarism.

- www.bestessays.com
- www.superiorpapers.com

Child Abuse Content
Worldwide illegal child sexual abuse content. In Cisco ScanCenter, Cisco blocks all child abuse content for all customers without exception, and for legal reasons keeps no logs. This category is never displayed in Cisco ScanCenter.
Note
In the Cisco Web Security Appliance, when URL categorization is enabled, this category is logged in the access logs regardless of whether the content is blocked.

Computer Security
Offering security products and services for corporate and home users.
- www.computersecurity.com
- www.symantec.com

Caution
Cisco ScanCenter is included in the Computer Security category. Therefore, any policies created for the Computer Security category will also apply to Cisco ScanCenter. For example, if you add a Web filter policy that blocks the Computer Security category, your access to Cisco ScanCenter will also be blocked. A workaround is to first whitelist the Cisco ScanCenter URL before blocking the Computer Security category.

Computers and Internet
Information about computers and software, such as hardware, software, software support; information for software engineers, programming and networking; website design; the web and Internet in general; computer science; computer graphics and clipart. “Freeware and Shareware” is a separate category.
- www.w3.org
- www.xml.com

Dating
Dating, online personals, matrimonial agencies.
- www.eharmony.com
- www.match.com

Digital Postcards
Enabling sending of digital postcards and e-cards.
- www.all-yours.net
- www.delivr.net

Dining and Drinking
Eating and drinking establishments; restaurants, bars, taverns, and pubs; restaurant guides and reviews.
- www.hideawaybrewpub.com
- www.restaurantrow.com

Do It Yourself (DIY) Projects
Guidance and information to create, improve, modify, decorate, and repair something without the aid of experts or professionals.
Dynamic and Residential

IP addresses of broadband links that usually indicate users attempting to access their home network, for example, for a remote session to a home computer.

Education

Education-related, such as schools, colleges, universities, teaching materials, and teachers’ resources; technical and vocational training; online training; education issues and policies; financial aid; school funding; standards and testing.

- www.education.com
- www.greatschools.org

Entertainment

Details or discussion of films; music and bands; television; celebrities and fan websites; entertainment news; celebrity gossip; entertainment venues. Compare with the “Arts” category.

- www.eonline.com
- www.ew.com

Extreme

Material of a sexually violent or criminal nature; violence and violent behavior; tasteless, often gory photographs, such as autopsy photos; photos of crime scenes, crime and accident victims; excessive obscene material; shock websites.

- www.car-accidents.com
- www.crime-scene-photos.com

Fashion

Clothing and fashion; hair salons; cosmetics; accessories; jewelry; perfume; pictures and text relating to body modification; tattoos and piercing; modeling agencies. Dermatological products are classified as “Health and Nutrition.”

- www.fashion.net
- www.findabeautysalon.com

File Transfer Services

File transfer services with the primary purpose of providing download services and hosted file sharing

- www.rapidshare.com
- www.yousendit.com

Filter Avoidance

Promoting and aiding undetectable and anonymous web usage, including cgi, php and glype anonymous proxy services.

- www.bypassschoolfilter.com
- www.filterbypass.com
Finance
Primarily financial in nature, such as accounting practices and accountants, taxation, taxes, banking, insurance, investing, the national economy, personal finance involving insurance of all types, credit cards, retirement and estate planning, loans, mortgages. Stock and shares are classified as “Online Trading.”

  • finance.yahoo.com
  • www.bankofamerica.com

Freeware and Shareware
Downloads of free software and shareware.

  • www.freewarehome.com
  • www.shareware.com

Gambling
Casinos and online gambling; bookmakers and odds; gambling advice; competitive racing in a gambling context; sports booking; sports gambling; services for spread betting on stocks and shares. Websites dealing with gambling addiction are classified as “Health and Nutrition.” Government-run lotteries are classified as “Lotteries.”

  • www.888.com
  • www.gambling.com

Games
Various card games, board games, word games, and video games; combat games; sports games; downloadable games; game reviews; cheat sheets; computer games and Internet games, such as role-playing games.

  • www.games.com
  • www.shockwave.com

Government and Law
Government websites; foreign relations; news and information relating to government and elections; information relating to the field of law, such as attorneys, law firms, law publications, legal reference material, courts, dockets, and legal associations; legislation and court decisions; civil rights issues; immigration; patents and copyrights; information relating to law enforcement and correctional systems; crime reporting, law enforcement, and crime statistics; military, such as the armed forces, military bases, military organizations; anti-terrorism.

  • www.law.com
  • www.usa.gov

Hacking
Discussing ways to bypass the security of websites, software, and computers.

  • www.gohacking.com
  • www.hackthissite.org
Hate Speech
Websites promoting hatred, intolerance, or discrimination on the basis of social group, color, religion, sexual orientation, disability, class, ethnicity, nationality, age, gender, gender identity; websites promoting racism, sexism, racist theology, hate music, neo-Nazi organizations, supremacism; Holocaust denial.
- www.kkk.com
- www.nazi.org

Health and Nutrition
Health care; diseases and disabilities; medical care; hospitals; doctors; medicinal drugs; mental health; psychiatry; pharmacology; exercise and fitness; physical disabilities; vitamins and supplements; sex in the context of health (disease and health care); tobacco use, alcohol use, drug use, and gambling in the context of health (disease and health care); food in general; food and beverage; cooking and recipes; food and nutrition, health, and dieting; cooking, including recipe and culinary websites; alternative medicine.
- www.health.com
- www.webmd.com

Humor
Jokes, sketches, comics, and other humorous content. Adult humor likely to offend is classified as “Adult.”
- www.humor.com
- www.jokes.com

Hunting
Professional or sport hunting, gun clubs and other hunting related sites.

Illegal Activities
Promoting crime, such as stealing, fraud, illegally accessing telephone networks; computer viruses; terrorism, bombs, and anarchy; websites depicting murder and suicide and explaining ways to commit them.
- www.ekran.no
- www.thedisease.net

Illegal Downloads
Providing the ability to download software or other materials, serial numbers, key generators, and tools for bypassing software protection in violation of copyright agreements. Torrents are classified as “Peer File Transfer.”
- www.keygenguru.com
- www.zcrack.com

Illegal Drugs
Information about recreational drugs, drug paraphernalia, drug purchase, and manufacture.
- www.cocaine.org
- www.hightimes.com
Infrastructure and Content Delivery
Content delivery infrastructure and dynamically generated content; websites that cannot be classified more specifically because they are secured or otherwise difficult to classify.

- www.akamai.net
- www.webstat.net

Internet Telephony
Telephonic services using the Internet.

- www.evaphone.com
- www.skype.com

Job Search
Career advice; resume writing and interviewing skills; job placement services; job databanks; permanent and temporary employment agencies; employer websites.

- www.careerbuilder.com
- www.monster.com

Lingerie and Swimsuits
Intimate apparel and swimwear, especially when modeled.

- www.swimsuits.com
- www.victoriassecret.com

Lotteries
Sweepstakes, contests, and state-sponsored lotteries.

- www.calottery.com
- www.flalottery.com

Military
Military, such as the armed forces, military bases, military organizations, and anti-terrorism.

Mobile Phones
Short Message Services (SMS); ringtones and mobile phone downloads. Cellular carrier websites are included in the “Business and Industry” category.

- www.cbfsms.com
- www.zedge.net

Nature
Natural resources; ecology and conservation; forests; wilderness; plants; flowers; forest conservation; forest, wilderness, and forestry practices; forest management (reforestation, forest protection, conservation, harvesting, forest health, thinning, and prescribed burning); agricultural practices (agriculture, gardening, horticulture, landscaping, planting, weed control, irrigation, pruning, and harvesting); pollution issues (air quality, hazardous
waste, pollution prevention, recycling, waste management, water quality, and the environmental cleanup industry); animals, pets, livestock, and zoology; biology; botany.

- www.enature.com
- www.nature.org

**News**

News, headlines, newspapers, television stations, magazines, weather, ski conditions.

- news.bbc.co.uk
- www.cnn.com

**Non-Governmental Organizations**

Non-governmental organizations such as clubs, lobbies, communities, non-profit organizations and labor unions.

- www.panda.org
- www.unions.org

**Non-Sexual Nudity**

Nudism and nudity; naturism; nudist camps; artistic nudes.

- www.artenuda.com
- www.naturistsociety.com

**Online Communities**

Affinity groups; special interest groups; web newsgroups; message boards. Excludes websites classified as “Professional Networking” or “Social Networking.”

- www.ieee.org
- www.igda.org

**Online Meetings**

Online meetings, desktop sharing, remote access, and other tools that facilitate multi-location collaboration.

**Online Storage and Backup**

Offsite and peer-to-peer storage for backup, sharing, and hosting.

- www.adrive.com
- www.dropbox.com

**Online Trading**

Online brokerages; websites that enable the user to trade stocks online; information relating to the stock market, stocks, bonds, mutual funds, brokers, stock analysis and commentary, stock screens, stock charts, IPOs, stock splits. Services for spread-betting on stocks and shares are classified as “Gambling.” Other financial services are classified as “Finance.”

- www.scottrade.com
- www.tdameritrade.com
Organizational Email
Websites used to access business email (often via Outlook Web Access).

Paranormal
UFOs, ghosts, cryptid, telekenesis, urban legends, and myths.

Parked Domains
Websites that monetize traffic from the domain using paid listings from an ad network, or are owned by “squatters” hoping to sell the domain name for a profit. These also include fake search websites which return paid ad links.

- www.domainzaar.com
- www.parked.com

Peer File Transfer
Peer-to-peer file request websites. Using this category in a web filter does not track the file transfers themselves.

- www.bittorrent.com
- www.limewire.com

Personal Sites
Websites about and from private individuals; personal homepage servers; websites with personal contents; personal blogs with no particular theme.

- www.karymullis.com
- www.stallman.org

Personal VPN
Virtual private network (VPN) sites or tools that are typically used for personal use and may or may not be approved for corporate use.

Photo Searches and Images
Facilitating the storing and searching for, images, photographs, and clip art.

- www.flickr.com
- www.photobucket.com

Politics
Websites of politicians; political parties; news and information on politics, elections, democracy, and voting.

- www.politics.com
- www.thisnation.com

Pornography
Sexually explicit text or depictions. Includes explicit anime and cartoons; general explicit depictions; other fetish material; explicit chat rooms; sex simulators; strip poker; adult movies; lewd art; web-based explicit email.
• www.redtube.com
• www.youporn.com

**Professional Networking**
Social networking for the purpose of career or professional development. See also “Social Networking.”
• www.linkedin.com
• www.europeanpwn.net

**Real Estate**
Information that would support the search for real estate; office and commercial space; real estate listings, such as rentals, apartments, and homes; house building.
• www.realtor.com
• www.zillow.com

**Reference**
City and state guides, maps, time, reference sources, dictionaries, libraries.
• www.wikipedia.org
• www.yellowpages.com

**Religion**
Religious content, information about religions, religious communities.
• www.religionfacts.com
• www.religioustolerance.org

**SaaS and B2B**
Web portals for online business services; online meetings.
• www.netsuite.com
• www.salesforce.com

**Safe for Kids**
Directed at, and specifically approved for, young children.
• kids.discovery.com
• www.nickjr.com

**Science and Technology**
Science and technology, such as aerospace, electronics, engineering, mathematics, and other similar disciplines; space exploration; meteorology; geography; environment; energy (fossil, nuclear, renewable); communications (telephones, telecommunications).
• www.physorg.com
• www.science.gov
Search Engines and Portals
Search engines and other initial points of access to information on the Internet.

• www.bing.com
• www.google.com

Sex Education
Factual websites dealing with sex, sexual health, contraception, pregnancy.

• www.avert.org
• www.scarleteen.com

Shopping
Bartering; online purchasing; coupons and free offers; general office supplies; online catalogs; online malls.

• www.amazon.com
• www.shopping.com

Social Networking
Social networking. See also “Professional Networking.”

• www.facebook.com
• www.twitter.com

Social Sciences
Sciences and history related to society; archaeology; anthropology; cultural studies; history; linguistics; geography; philosophy; psychology; women’s studies.

• www.anthropology.net
• www.archaeology.org

Society and Culture
Family and relationships; ethnicity; social organizations; genealogy; seniors; child-care.

• www.childcare.gov
• www.familysearch.org

Software Updates
Websites that host updates for software packages.

• www.softwarepatch.com
• www.versiontracker.com

Sports and Recreation
All sports, professional and amateur; recreational activities; fishing; fantasy sports; public parks; amusement parks; water parks; theme parks; zoos and aquariums; spas.

• www.espn.com
• www.recreation.gov
Streaming Audio
Real-time streaming audio content including Internet radio and audio feeds.

- www.live-radio.net
- www.shoutcast.com

Streaming Video
Real-time streaming video including Internet television, web casts, and video sharing.

- www.hulu.com
- www.youtube.com

Tobacco
Pro-tobacco websites; tobacco manufacturers; pipes and smoking products (not marketed for illegal drug use). Tobacco addiction is classified as “Health and Nutrition.”

- www.bat.com
- www.tobacco.org

Transportation
Personal transportation; information about cars and motorcycles; shopping for new and used cars and motorcycles; car clubs; boats, airplanes, recreational vehicles (RVs), and other similar items. Note, car and motorcycle racing is classified as “Sports and Recreation.”

- www.cars.com
- www.motorcycles.com

Travel
Business and personal travel; travel information; travel resources; travel agents; vacation packages; cruises; lodging and accommodation; travel transportation; flight booking; airfares; car rental; vacation homes.

- www.expedia.com
- www.lonelyplanet.com

Unclassified
Websites that are not in the Cisco database are recorded as unclassified for reporting purposes. This category may include mistyped URLs.

Weapons
Information relating to the purchase or use of conventional weapons such as gun sellers, gun auctions, gun classified ads, gun accessories, gun shows, and gun training; general information about guns; other weapons and graphic hunting sites may be included. Government military websites are classified as “Government and Law.”

- www.coldsteel.com
- www.gunbroker.com
**Web Hosting**
Website hosting; bandwidth services.
- www.bluehost.com
- www.godaddy.com

**Web Page Translation**
Translation of web pages between languages.
- babelfish.yahoo.com
- translate.google.com

**Web-Based Email**
Public web-based email services. Websites enabling individuals to access their company or organization’s email service are classified as “Organizational Email.”
- mail.yahoo.com
- www.hotmail.com
CHAPTER 13

Filters

- Managing Filters, on page 81
- Application Control, on page 81
- Viewing an Existing Filter, on page 83
- Creating a New Filter, on page 83
- Inbound Filters, on page 83
- Bi-directional Filters, on page 86
- Editing a Filter, on page 88
- Removing a Filter, on page 88

Managing Filters

Filters are used to control content that passes in to, and out of, your network. The following filter types are available:

- Categories (HTTP), on page 84
- Categories (HTTPS), on page 84
- Domains, on page 84
- Content Types, on page 84
- File Types, on page 85
- Applications, on page 86
- Exceptions, on page 87
- User Agents, on page 87

Application Control

Application control enables you to be more specific about the web applications and activities you want to filter than would be possible with URL or category filtering, for example:

- Evasive applications, such as anonymizers and encrypted tunnels.
- Collaboration applications, such as Cisco WebEx and instant messaging.
• Resource-intensive applications, such as streaming media.

There are different ways to block applications or accomplish the desired result. You can use the standard web filters instead of, or in addition to, application control. It is important that you place the rule containing application control filters in the desired order relative to any other rule, particularly when using Delegated Administration. When a rule allows access to a web resource, any subsequent rule that blocks access is ignored. You should take particular care with rules that include the following categories:

• Chat and Instant Messaging
• File Transfer Services
• Games
• Internet Telephony
• Peer File Transfer
• Professional Networking
• SaaS and B2B
• Search Engines and Portals
• Social Networking
• Streaming Audio
• Streaming Video

User Experience with Blocked Requests

When the application engine blocks a transaction, Cloud Web Security sends a block page to the end user. However, not all websites display the block page. For example, some Web 2.0 websites display dynamic content using JavaScript instead of a static web page and are not likely to display the block page. Users are still properly blocked from downloading malicious data, but they may not always be informed of this by the website.

Understanding Application Control Settings

Applications are controlled by selecting a class, such as social networking, a platform within that category, such as Facebook, a specific application, such as chat, a group of applications, such as games, or an action. The most common actions that you can control are:

• Download files
• Install software
• Like (social networking)
• Post
• Search
• Send email (web email)
• Tag (social networking)
• Upload files

The names of these actions may vary depending on the application provider.

Note

New classes, platforms, applications, and actions are periodically added to the application control engine by Cisco based on analysis of Cloud Web Security user traffic.
Classes, platforms, and applications can be thought of as nodes on a tree. When Cisco adds a new child node to the tree, it will automatically be included in any existing filters where the parent node is selected. For example, if a filter included the Social Networking > Facebook node, and a new application was added as a child of the Facebook node, it would automatically be selected in the filter.

### Viewing an Existing Filter

**Procedure**

1. **Step 1** Click the Web Filtering tab to display the Web Filtering menus.
2. **Step 2** In the Management menu, click Filters to display the filter management page.

<table>
<thead>
<tr>
<th>List of Filters</th>
<th>Filter Name</th>
<th>Created on</th>
<th>Edit</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>allboy</td>
<td></td>
<td>04 Sep 09 10:28 UTC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>default</td>
<td></td>
<td>02 Sep 09 09:05 UTC</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Creating a New Filter

**Procedure**

1. **Step 1** Click the Create Filter tab.
2. **Step 2** Enter a unique Filter Name.
3. **Step 3** For each filter type that you want to add to the filter, click the hyperlink in the left column and enter the details. You can use as many filter types as you want for each filter.

   **Note** If you add multiple filter types, they work with the OR condition: the filter is applied if the conditions are met for any of the filter types.

4. **Step 4** Click Save to apply your changes in each filter type.
5. **Step 5** Click Save all Settings to apply all your changes. Alternatively, navigate away from the page to abandon your changes.

### Inbound Filters

Inbound filters are applied to incoming content only.
Categories (HTTP)

Select the check boxes for the required categories. You can click Select All to select all the check boxes or Deselect all to clear all the check boxes. You can click Set to Default to copy the categories from the default filter. For a list of the available categories, see Category List, on page 67.

Categories (HTTPS)

Select the check boxes of the required categories. You can click Select All to select all the check boxes or Deselect all to clear all the check boxes. You can click Set to Default to copy the categories from the default filter or Copy HTTP selection to copy the categories from the HTTP settings for the filter. The available categories are the same as for HTTP.

Note

This option is available only if you select the Enable HTTP/HTTPS Split check box in the Separate HTTPS Restrictions section of the Web Filtering > Management > Global Settings page.

Domains

Enter the domains or URLs to be included in the filter. Each domain or URL should appear on its own line. You can use hostnames and subdomains, but you must omit the protocol (http://). You can click Sort Alphabetically to sort the list.

Enter the IP ranges to be included in the Networks/IPs box. These must be entered in the form of an IP address and a net mask, for example 192.0.2.0/24.

You can click Make Default to copy the settings from the default filter.

Note

There is a limit of 1,000 entries per Domain filter, and a total limit of 10,000 entries.

Content Types

Select the check boxes of the applications, audio, video, and image files that you want to block. You can select the Select All check box to select all the check boxes for a category or clear it to clear all the check boxes. You can click Select All to select all the check boxes or Deselect all to clear them. You can click Set to Default to copy the settings from the default filter.
In the box, enter any additional MIME types to block, for example text/html. Each MIME type must be entered on its own line. You can click **Sort Alphabetically** to sort the list.

### File Types

Select the check boxes of the inbound file types to block. You can click **Select All** to select all the check boxes or **Clear All** to clear them. You can click **Make Default** to copy the settings from the default filter.
Enter any additional file extensions (up to eight characters) in the box, for example 7z. Each file extension should be entered on its own line. You can click Sort Alphabetically to sort the list.

# Bi-directional Filters

Bi-directional filters are applied to incoming and outgoing content.

## Applications

Select the check boxes for the application types, applications, and activities to include in the filter. Controls can be applied to various activities, including:

- Like
- Post
- Upload
- Download
- Tag
- Install
- Search
- Send Email
Selecting a node selects all child nodes in the tree. However, the opposite is not true. Selecting all activities is not the same as selecting the application. Selecting all applications is not the same as selecting the application type.

You can Show Selected to expand all selected nodes or Collapse All to collapse all nodes.

You can begin typing in the Filter box to filter the visible categories.

⚠️ **Caution**

The Select All selects everything, even categories that have been hidden from display using the Filter box.

### Exceptions

Enter the domains or URLs to be excluded from the filter. Each domain or URL should appear on its own line. You can use hostnames and subdomains but you must omit the protocol (http://). You can click Sort Alphabetically to sort the list.

Enter the IP ranges to be included in the Networks/IPs box. These must be entered in the form of an IP address and a net mask, for example 192.0.2.0/24.

### User Agents

Select the required check boxes for the web browsers you want to include in the filter. You can select the All Versions check box to add every version, including future versions, of a given browser.

Enter any other user agents you want to include in the Custom User Agents box. Each user agent must be entered on a separate line. The following characters can be included:

- !<text>—does not equal <text>
- ^<text>—starts with <text>
- *—zero or more characters
- <text>$—string ends with <text>
Editing a Filter

Procedure

Step 1  On the Web Filtering > Management > Filters page, click the Edit icon next to the filter name.
Step 2  Click the hyperlink of the settings type you want to change.
Step 3  Make your changes.
Step 4  Click Save all Settings to apply your changes. Alternatively, navigate away from the page to abandon your changes.

Removing a Filter

On the Web Filtering > Management > Filters page, click the Delete icon next to the filter name.
CHAPTER 14

Schedules

- Managing Schedules, on page 89
- Creating a New Schedule, on page 89
- Editing a Schedule, on page 90
- Removing a Schedule, on page 90

Managing Schedules

Schedules are used to determine when policy rules are applied. You can add one or more schedules to a rule. It is also possible to add a schedule as an exception. For example, you could add a schedule of midnight to midnight to a rule to always block a specific website. You could then add a schedule that runs from 12:00 to 14:00 as an exception to permit users to access the website during their lunch break.

Schedules are applied in order of length (time duration), from shortest to longest. So in the previous example the schedule to enable user access from 12.00 to 14.00 would be applied first.

Procedure

Step 1
Click the Web Filtering tab to display the Web Filtering menus.

Step 2
In the Management menu, click Schedules to display the schedule management page.

<table>
<thead>
<tr>
<th>Schedule Name</th>
<th>Time</th>
<th>Time zone</th>
<th>Days</th>
</tr>
</thead>
<tbody>
<tr>
<td>lunch</td>
<td>From 22:00 to 14:00</td>
<td>UTC</td>
<td>Mon-Tue-Wed-Thur-Fri</td>
</tr>
<tr>
<td>working hours</td>
<td>From 08:00 to 18:00</td>
<td>UTC</td>
<td>Mon-Tue-Wed-Thur-Fri</td>
</tr>
<tr>
<td>anytime</td>
<td>From 00:00 to 23:00</td>
<td>UTC</td>
<td>Everyday</td>
</tr>
</tbody>
</table>

Creating a New Schedule

Procedure

Step 1
Click the Create Schedule tab.
Step 2  Enter a unique Schedule name.
Step 3  Click the required start time in the From drop-down lists.
Step 4  Click the required end time in the To drop-down lists.
Step 5  Click a Time Zone. The default is UTC.
Step 6  Select the check box for each day on which to apply the schedule.
Step 7  Click Create Schedule to apply your changes. Alternatively, navigate away from the page to abandon your changes.

Editing a Schedule

To edit a schedule, click the Edit icon. Make your changes then click Save to apply your changes. Alternatively, navigate away from the page to abandon your changes.

Removing a Schedule

To remove a schedule, click the Delete icon.
CHAPTER 15

Policy

- Managing Policy, on page 91
- Creating a Rule, on page 92
- Editing a Rule, on page 93
- Removing a Rule, on page 93
- Backing Up a Policy, on page 93
- Restoring a Policy, on page 94

Managing Policy

Policy enables you to set the rules for applying filters. Each rule has one of the following actions associated with it:

- **Allow**—Access is allowed, and data is stored for reporting purposes.
- **Anonymize**—User, group, internal, and external IP details are replaced with “undisclosed” in reporting data.
- **Authenticate**—The user must authenticate. Typically this is used with clientless authentication. For further information, see Authentication, on page 19.
- **Block**—Access is denied.
- **Warn**—Access is allowed only if the user clicks through the warning page.

⚠️ **Caution**

You must not use the default rule for authentication.

⚠️ **Caution**

Cisco ScanCenter is included in the Computer Security category. Therefore, any policies created for the Computer Security category will also apply to Cisco ScanCenter. For example, if you add a Web filter policy that blocks the Computer Security category, your access to Cisco ScanCenter will also be blocked. A workaround is to first whitelist the Cisco ScanCenter URL before blocking the Computer Security category.

⚠️ **Caution**

If you have Compatibility View turned on, Internet Explorer will send User Agents which may appear as other Web browsers. If you have a policy that blocks such types of Web browsers, then the Internet Explorer browser will also get blocked. A workaround is to first turn off Compatibility View in Internet Explorer.
There is a maximum of 100 enabled rules allowed for the policy.

**Procedure**

**Step 1** Navigate to **Web Filtering > Management > Policy** to display the Manage Policy tab.

**Step 2** Rules higher in the list will take priority over rules below it. Change the priority of a rule by clicking the up or down arrow icon in the **Move** column to move a rule up or down the list.

**Step 3** Select the **Active** check box to make the rule active. Alternatively, clear the check box to activate the rule at another time. Click **Apply Changes** to apply your changes. Alternatively, navigate away from the page to abandon your changes.

---

## Creating a Rule

**Procedure**

**Step 1** Click the **Create Rule** tab.

**Step 2** Enter a rule **Name**.

**Step 3** (Optional) Enter a **Description**. This is available only for HTTP rules and visible only while editing the rule.

**Step 4** Select the **Active** check box to make the rule active. Alternatively, clear the check box to activate the rule at another time.

**Step 5** In the **Rule Action** drop-down list, click an action. The available actions are:

- Block
- Allow
- Anonymize
- Warn
- Authenticate

**Step 6** For each group that you want to add to the rule:

a) Click **Add Group**.

b) Enter all or part of a group name in the **Filter** box.

c) Click **Select** to select the group.

d) Click **Confirm Selection**. You can click the **Delete** icon to remove any groups added by mistake.

e) Select the **Set as Exception** check box to exclude the group from the rule. Alternatively, clear the check box to apply the rule to the group.

**Step 7** For each filter that you want to add to the rule:

a) In the **Add Filter** drop-down list, choose a filter, and then click **Add**.

b) Select the **Set as Exception** check box to exclude the filter from the rule.

c) You can click the **Delete** icon to remove a filter added by mistake.
If you add multiple filters, they work with the AND condition: the rule is applied only if all of the filters are applied by meeting their conditions.

**Step 8**  
For each schedule that you want to add to the rule:

a) In the Add Schedule drop-down list, choose a schedule, and then click Add.

b) Select the Set as Exception check box to exclude the schedule from the rule.

c) You can click the Delete icon to remove a schedule added by mistake.

**Step 9**  
Click Create Rule to apply your changes. Alternatively, click Cancel or navigate away from the page to abandon your changes.

---

# Editing a Rule

To edit a rule, click the Edit icon. Make your changes, and then click Save to apply your changes. Alternatively, navigate away from the page to abandon your changes.

# Removing a Rule

To remove a rule, click the Delete icon. You cannot remove the default rule.

# Backing Up a Policy

**Procedure**

- **Step 1** Navigate to Web Filtering > Management > Policy Backup / Restore.
- **Step 2** Click the Policy Export panel.
- **Step 3** (Required) Enter a comment to be stored with the exported backup file. The comment can be used to both describe the purpose of the backup and identify the exported file. The comment will be shown when subsequently importing the file at a later time.
- **Step 4** Click Export. Policy export prepared and file download initiated.
- **Step 5** Depending on your OS and web browser, save the file to your local machine. Click Finish.

**What to do next**

The following components and their sub-components are exported:

- Policy filters
- Policy rules
- Auth groups
- Schedules
• Expression lists
• Custom headers
• HTTPS filters
• HTTPS rules
• HTTPS certificates
• Company, group, and user license keys
• Quotas

Restoring a Policy

Caution
Importing a policy will overwrite your existing policy. We recommend you back up your existing policy before importing.

Procedure

Step 1 Navigate to Web Filtering > Management > Policy Backup / Restore.
Step 2 Click the Policy Import panel.
Step 3 Click Select File and open the policy file you want to import.
Step 4 Click Check file to verify if the selected file is valid.
Step 5 Review the User (who exported the policy), Date (when the policy was exported), and Comment information. If you are sure that this is the correct file you want to import, click Continue. Otherwise, click Cancel.
Step 6 Importing a policy will overwrite your existing policy. In the Confirm dialog box, if you are sure you wish to continue, click Import. Otherwise, click Cancel.

What to do next

• Policy import successful. Your previous policy has been overwritten. Click Finish. Verify that the imported policy and its rules are as expected.

• Policy import failed. Could not process the policy. No changes were made to your policy. Check that the file is valid.

• Your request could not be completed because the policy service is unavailable. Contact Cisco Customer Support if this problem persists.
Policy export and import is supported between different companies. However, while company, group, and user license keys are included in exported policies, the license keys and HTTPS certificates will be removed if importing the policy into a different company. Generate new license keys and HTTPS certificates. Within the delegated administration hierarchy, see Managing Exported and Imported Policy, on page 58.
CHAPTER 16

Quotas

- Managing Quotas, on page 97
- Creating a Quota, on page 97
- Editing a Quota, on page 99
- Removing a Quota, on page 99

Managing Quotas

Quotas are used in conjunction with Connector, in workgroup mode, to control the time a user or group of users may spend browsing web content specified by your policy. If a quota is reached, the web requests for those users in the group are blocked until the next time the period starts. For more information, see the Connector Administrator Guide, Release 3.X.

Procedure

**Step 1**
Click the **Web Filtering** tab to display the **Web Filtering** menus.

**Step 2**
In the **Management** menu, click **Quotas** to display the quota management page. You can set the priority of a quota by clicking the **up** and **down** icons in the **Move** column and then clicking **Apply Changes**.

Creating a Quota

Procedure

**Step 1**
Click the **Create Quota** tab.
Step 2
Enter a quota Name.

Step 3
Select the Active check box to make the quota active. Alternatively, clear the check box to activate the quota at another time.

Step 4
For each group to be added to the quota:

a) Click Add Group.
b) Enter all or part of a group name in the Search box and click Go.
c) Click Select to select the group.
d) Click Confirm Selection. You can click the Delete icon to remove any groups added by mistake.
e) Select the Set as Exception check box to exclude the group from the quota. Alternatively, clear the check box to apply the quota to the group.

Step 5
In the Period drop-down list, choose the time period for the quota: daily or weekly.

Step 6
In the Bytes in drop-down list, choose the download limit. The available options are:

- Unlimited
- 5M (five megabytes)
- 10M
- 20M
- 50M
- 100M
- 200M
- 500M
- 1G (one gigabyte)

Step 7
In the Bytes out drop-down list, choose the upload limit. The available options are the same as for downloads.

Step 8
In the Time drop-down list, choose the time limit. The available options are:

- Unlimited
- 15 minutes
- 30 minutes
- 1 hour
- 2 hours
- 4 hours
- 8 hours

Step 9
In the Connections drop-down list, choose the number of allowed connections. The available options are:

- Unlimited
- 1,000
• 2,000
• 5,000
• 10,000
• 20,000
• 50,000
• 100,000

**Editing a Quota**

To edit a quota, click the **Edit** icon. Make your changes, and then click **Save** to apply your changes. Alternatively, navigate away from the page to abandon your changes.

**Removing a Quota**

To remove a quota, click the **Delete** icon. You cannot remove the default quota.
Removing a Quota
Global Settings

Overview

Global settings are applied to all users. From here you can:

- Enable SearchAhead.
- Enable SafeSearch.
- Enable localization.
- Enable separate filtering of HTTP and HTTPS traffic.
- Set your Acceptable Usage Policy (AUP) display preferences.
- Enable dynamic classification of unclassified websites.
- Enable content range headers.

SearchAhead

The web use of most users is based around a few websites they visit frequently and a search engine. It is often searches that lead to inappropriate or dangerous websites.

SearchAhead alerts users to potential risks by adding an icon to search results based on the web filtering policy that you have applied. It also provides advanced warning for websites that may host malware:

- Site meets organization’s Acceptable Use Policy and is safe to browse.
- Site is unclassified and may contain unsuitable content.
- Site does not meet organization’s Acceptable Use Policy and is blocked.
- Site is hazardous and may host spyware, viruses, or phishing.

The following search engines are supported:
The following categories always appear with a question mark, regardless of your policy:

- Adult
- Extreme
- Filter Avoidance
- Hacking
- Hate Speech
- Illegal Activities
- Illegal Downloads
- Illegal Drugs
- Peer File Transfer
- Pornography
- Unclassified

**SafeSearch**

SafeSearch helps block inappropriate, explicit, or potentially offensive content from your web search results. Enforce SafeSearch on supported search engines to ensure that the SafeSearch filter is enabled regardless of user setting. Currently, search engines supported in Cisco Cloud Web Security include:

- Google
- Yahoo!
- Bing
- Flickr
- YouTube
- Ask
- Yandex
- DuckDuckGo
- Dailymotion
- Dogpile

**Note**

Requires HTTPS Inspection functionality. This functionality allows Cisco Cloud Web Security to decrypt HTTPS traffic in order to apply policy, filtering, and scanning. By default, this functionality is switched off in Cisco ScanCenter. If you want to use this functionality, enable it in Cisco ScanCenter, create HTTPS Inspection policies, and generate a company-specific certificate. For more information, see Secure Traffic Inspection, on page 113.
Localization

When localization is enabled, Alert, SafeSearch, and Search Ahead present text in the user's preferred language as specified by their browser. If the user's preferred language is not supported, the text is presented in English.

HTTP/HTTPS Split

By default, the same category restrictions are applied to both HTTP and HTTPS traffic unless separate filtering is enabled.

Acceptable Usage Policy

When the Enable AUP for All Users check box is enabled, every user is presented with an Acceptable Usage Policy page when they access the Internet at a set interval, either daily or weekly. A default page is provided which you can modify, extend, or override completely with your own text and HTML. This feature requires CWS Connector. See Configuring Connector Acceptable Use Policy.

Note

This feature only works in conjunction with CWS Connector versions 2.50 and newer and the CWS Mobile Browser.

Dynamic Classification

When the Dynamic Classification Engine is enabled, the system attempts to identify the content of unclassified websites and apply your policy. Currently, categories supported include:

- Pornography
- Gambling
- Hate Speech
- Filter Avoidance
- Illegal Drugs
- Illegal Downloads

Note

Classification occurs as each page is downloaded. Pages will still appear unclassified in the Search Ahead results.

Content Range Headers

Apple iOS devices use content-range headers to connect to the Internet (for further information see http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html). Normally, Cisco Cloud Web Security does not support these headers. However, selecting the Enable Content Range Headers check box allows the
propagation of the HTTP range-related headers which enable users of these devices to access the Internet via Cisco Cloud Web Security.

Caution
There is a potential security risk if this feature is enabled. A specific attack directed from the client-side may try to download an infected file from a website in discrete parts. Cisco Cloud Web Security may not be able to recognize the separate parts as malware and may not block them. The client could then potentially reconstruct the original file to install malware on the device.

Cisco is not currently aware of any malware that behaves this way, and therefore does not believe that enabling this feature creates a material additional security risk. However, consider this risk before enabling the feature as Cisco does not accept responsibility for any consequences of enablement.

Changing Global Settings

Procedure

Step 1 Click the Web Filtering tab.
Step 2 In the Management menu, click Global Settings to display the Global Settings page.
Step 3 Select the Enable SearchAhead for All Users check box to enable SearchAhead. Alternatively, clear the check box to switch off SearchAhead.
Step 4 Click Save.
Step 5 Select the Enforce SafeSearch on Supported Search Engines check box to enable the feature. Alternatively, clear the check box to switch the feature off.
Step 6 Click Save.
Step 7 Select the Enable Localization check box to enable the localization feature. Alternatively, clear the check box to switch the feature off.
Step 8 Click Save.
Step 9 Clear the Enable HTTP/HTTPS Split check box to use the HTTP Web filtering settings for HTTPS traffic as well. Alternatively, select the check box to use separate filter settings for HTTP and HTTPS traffic.
Step 10 Click Save.
Step 11 Select the Enable AUP for All Users check box to display an acceptable usage policy page to users when they connect to the Internet. Alternatively, clear the check box to prevent the page from being displayed.
Step 12 Select the Include standard HTML page template for AUP page check box to include the standard AUP page template. Alternatively, clear the check box to display only the text or HTML that you supply.
Step 13 Click Daily or Weekly to set how often the AUP page is displayed.
Step 14 Enter the AUP text or HTML in the box. Alternatively, accept the default text.
Step 15 Click Save.
Step 16 Select the Enable Dynamic Classification check box to enable unclassified websites to be classified based on their content. Alternatively, clear the check box to switch off this functionality.
Step 17 Click Save.
Step 18 Select the Enable Content Range Headers check box to enable Apple iOS users to connect to the Internet via Cisco Cloud Web Security. Alternatively, clear the check box to disable content range headers.
Step 19  Click Save.
Cloud Bypass

Overview

By default, when a Cisco ISR is used to send traffic to the Cisco Cloud Web Security proxy servers, the policy you specify in Cisco ScanCenter will be applied to all websites. Using the cloud bypass feature, you can prevent specific websites from being scanned in the cloud by adding them to a bypass list.

Whitelist to Bypass Cloud Filtering

Assign bypass lists to Cisco ISRs based on the type of authentication key they’re using:

- Any Cisco ISR using the company key is assigned the default bypass list. See Company Keys, on page 19.
- Create other bypass lists for Cisco ISRs you’ve placed in custom groups that use group keys. See Managing Groups, on page 13 and Group Keys, on page 20.

Procedure

Step 1  Navigate to Web Filtering > Management > Cloud Bypass.
Step 2  For Cisco ISRs using the company key, click on the default bypass list, and skip to Step 6, on page 107.
Step 3  For Cisco ISRs you’ve placed in custom groups, click Create a New Bypass List.
Step 4  Enter a Name for the new bypass list.
Step 5  For each custom group of Cisco ISRs, enter its name in the Group name box and click Add. As you start to type in the name of the group, any group(s) matching what you’ve typed will appear. You may then select the group without having to type in the entire name.
Step 6  To add entries to the bypass list, first select each entry type from the drop-down list.

The available options are:
Whitelist to Bypass Cloud Filtering

<table>
<thead>
<tr>
<th>Entry Type</th>
<th>Cisco ISR G2</th>
<th>Cisco 4000 Series ISR</th>
<th>CWS Mobile Browser</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>available</td>
<td>limited to 64 entries, any more are discarded</td>
<td>available</td>
</tr>
<tr>
<td>Source IP address</td>
<td>available</td>
<td>available</td>
<td>available</td>
</tr>
<tr>
<td>Destination IP address</td>
<td>available</td>
<td>available</td>
<td>available</td>
</tr>
<tr>
<td>User-agent header</td>
<td>available</td>
<td>not supported</td>
<td>not supported</td>
</tr>
</tbody>
</table>

**Step 7**
Enter the corresponding entry details in the **Add Domain/IP/User-Agent** box and click **Add**.

**Step 8**
Click **Save** to apply your changes. Alternatively, click **Cancel** or navigate away from the page to abandon your changes.

---

**What to do next**

To edit a bypass list, click on its name.

- To remove a group, select the check box next to the group, click **Remove**, and click **Save**. Alternatively, click **Cancel** or navigate away from this page to abandon your changes.
- To remove an entry, select the check box next to the entry, click **Remove**, and click **Save**. Alternatively, click **Cancel** or navigate away from this page to abandon your changes.
- You can edit the default bypass list to manage entries in its allowed list. There are no groups in the default bypass list because the default bypass list is applied to Cisco ISRs using the company key.

To remove a bypass list, select the check box next to the list and click **Remove**. You cannot remove the **default** bypass list.

Cisco Cloud Web Security provides protection from spyware and web viruses. Cisco ScanCenter enables you to create approved lists of applications that will bypass spyware filtering and websites that will bypass web reputation filtering. By default, all incoming adware, spyware, and potentially unwanted applications (PUAs) are blocked. If, for some reason, an administrator requires a specific PUA to be permitted, it can be selected in an approved list. All PUAs are registered in the approved list when a download request is received.

All truly malicious code, such as viruses, worms, Trojans, back-doors, and key loggers are automatically blocked. Similarly, all known phishing exploits are automatically blocked by Cisco Cloud Web Security. The approved list applies to “grayware” which typically includes applications that hijack web browsing activities, redirect users to sponsored sites, monitor non-confidential browsing habits, create unwanted pop-up adverts, and so on.

### Allowing Applications Classified as Potentially Unwanted

With the spyware allowed list you can allow applications that Cisco has classified as potentially unwanted.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Click the Spyware tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Whitelists menu, click Spyware to display the Spyware page.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select the check boxes of the spyware to allow. You can enter part or all of the name of a spyware application in the Search box to find a spyware application.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Submit to apply your changes. Alternatively, navigate away from the page to abandon your changes.</td>
</tr>
</tbody>
</table>
Password Protected Archives

Cisco Cloud Web Security scans the files inside archives, such as zip files, for malware. However, it cannot scan password-protected (encrypted) archives. Because these archives could contain malware, they are classified as PUAs. However, you can enable users to access these files by selecting the Protected Archive check box in the Approved List.

⚠️ Caution

Enabling access to protected archives will globally allow all users to access these archives, which may contain PUAs.

Excluding Websites from Web Reputation Filtering

By default, Cisco Cloud Web Security blocks websites with a poor Web reputation score. You can prevent specific websites from being blocked by adding them to an allowed list. You can add a maximum of 1000 websites to the list.

Procedure

Step 1
Click the Spyware tab.

Step 2
In the Whitelist menu, click Web Reputation to display the Web Reputation page.

Step 3
Enter the required URL in the URL field. The URL can be a maximum of 256 characters in length.

Step 4
Click Add URL.

What to do next

You can click Check Reputation to open the SenderBase page for the website.

To remove a website from the allowed list, enter part or all of the URL in the Search box. Select the check box then click Remove.
Notifications

• Managing Notifications, on page 111
• User Messages, on page 111
• Email Alerts, on page 112

Managing Notifications

Notifications are the messages that appear on screen when a user attempts to access a page that is set to warn or block, including the email messages that are sent when this occurs. Notifications can be set for the following events:

• Web Virus
• Spyware
• Web Filtering

User Messages

Procedure

Step 1  Click the tab for the user messages to configure: Web Virus, Spyware, or Web Filtering.
Step 2  In the Notifications menu, click User Messages to display the User Messages page.
Step 3  Select the Include standard HTML page template for block page check box to include the default page contents. Alternatively, clear the check box to exclude the default page contents.
Step 4  Enter the message in plain text or HTML in the Customized Alert Page box. Alternatively, click Reset to restore the default message. You can use the following as replaceable parameters:

• #category
• #reason
• #url
• #username
In order to prevent the execution of potentially malicious scripts found in the **Customized Alert Page** box, only certain HTML tags are supported, as listed in the text on the **User Messages** page. Other HTML tags (such as script, for example) and their content are ignored and not included in the message generated to the user.

**Note**

- **Step 5** Click **Preview** to see your changes.
- **Step 6** Click **Save** to apply your changes. Alternatively, navigate away from the page to abandon your changes.
- **Step 7** If you are setting the user messages for Web Filtering:
  a) In the **Timeout Value** drop-down list, choose the delay in hours (0 to 24) between displaying a repeat warning for websites where the action is set to warn.
  b) Select the **Include standard HTML page template for warning page** check box to include the default page contents. Alternatively, clear the check box to exclude the default page contents.
  c) Enter the message in plain text or HTML in the **Customized Warn Alert Page** box. Alternatively, click **Reset** to restore the default message. You can use the same replaceable parameters as before.
- **Step 8** Click **Preview** to see your changes.
- **Step 9** Click **Save** to apply your changes. Alternatively, navigate away from the page to abandon your changes.

---

**Email Alerts**

**Procedure**

- **Step 1** Click the tab for the email alerts to configure: **Web Virus**, **Spyware**, or **Web Filtering**.
- **Step 2** In the **Notifications** menu, click **Email Alerts** to display the **Email Alerts** page.
- **Step 3** In the **Do you wish to be notified when a page is blocked?** drop-down list, click **Yes**.
- **Step 4** Enter up to five email addresses in the boxes.
- **Step 5** In the **Limit email alerts to** drop-down list, choose the number of email alerts to batch together (1 to 20).
- **Step 6** In the **per** drop-down list, choose the delay between emails in hours (1 to 24).
- **Step 7** Click **Save** to apply your changes. Alternatively, navigate away from the page to abandon your changes.

---

**Switching Off Email Alerts**

**Procedure**

- **Step 1** Click the tab for the email alerts you want to configure: **Web Virus**, **Spyware**, or **Web Filtering**.
- **Step 2** In the **Notifications** menu, click **Email Alerts** to display the **Email Alerts** page.
- **Step 3** In the **Do you wish to be notified when a page is blocked?** drop-down list, click **No**.
- **Step 4** Click **Save** to apply your changes. Alternatively, navigate away from the page to abandon your changes.
Secure Traffic Inspection

Overview

When a user connects to a website using HTTPS, the session is encrypted with a digital certificate. When secure traffic inspection is enabled, Cisco Cloud Web Security forwards all self-signed, expired, invalid, and revoked certificates.

Secure traffic inspection decrypts and scans the HTTPS traffic passing through Cisco Cloud Web Security for threats and carries out actions based on your policy settings. If the traffic is deemed safe, it is re-encrypted and passed back to your organization with a new SSL certificate.

All users must have an SSL certificate deployed to their web browser. You can generate a certificate in Cisco ScanCenter with Cisco as the Certificate Authority (CA), or alternatively, download a Certificate Signing Request (CSR) and use it with a tool (such as Microsoft Certificate Services or OpenSSL) to generate and upload your own certificate (where your organization is the CA). The certificate is then associated with your secure traffic inspection policy.

When using a CSR, the following fields must be present in the certificate:

X509v3 Basic Constraints:
    CA:TRUE

With OpenSSL, the command `openssl x509 -extfile v3_ca.txt -req -days 365 -in scancenter.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out scancenter.crt` performs this function, where `v3_ca.txt` contains the following:

subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid:always,issuer:always
basicConstraints = CA:TRUE

Two changes are required on the client:

1. Proxy settings for SSL traffic must be configured in the client web browser or on your organization’s firewall or gateway device.
2. The Cisco root certificate must be imported into the client web browser to enable it to trust SSL connections with Cisco Cloud Web Security.
Browsers may automatically import the certificate to the Intermediate Certificate Authorities store. However, the certificate must be placed in the Trusted Root Certificate store for Secure Traffic Inspection to function correctly.

**Legal Disclaimer**

It is your responsibility to determine if it is legal for you to inspect HTTPS traffic in your jurisdiction. Switching on this functionality will permit Cisco Cloud Web Security to inspect HTTPS traffic. While all such inspection is carried out automatically, rather than by individuals, such decryption may nonetheless be in breach of privacy laws in certain countries. By enabling this functionality, you agree that you have the legal right to decrypt this traffic in all relevant jurisdictions and that you have obtained all necessary consent from your users to do so.

In most jurisdictions you are required by law to inform your users that secure traffic is being inspected. It is possible to present an HTML page to the user that states that the session will be decrypted and that gives the user the option to continue or not. However, if you do this, you will not be able to use the standard warning page for other purposes.

**Procedure**

**Step 1**  
In Web Filtering > Notifications > User Messages, edit the Customized Warn Alert Page to display an HTTPS warning.

**Step 2**  
In the Timeout value drop-down list, click 0.

**Step 3**  
Clear the Include standard HTML page template for warning page check box.

**Note**  
If you also want to display warnings for non-HTTPS pages, you can select the check box and add the HTTPS warning to the standard Acceptable Use Policy warning.

**Step 4**  
Click Save to apply your changes.

**Step 5**  
In Web Filtering > Management > Global Settings, select the Enable HTTP/HTTPS split check box and click Save.

**Step 6**  
In Web Filtering > Management > Filters, create HTTPS filters for websites you want to block.

**Step 7**  
In Web Filtering > Management > Filters, create an HTTPS filter for all categories called “HTTPS warn.”

**Step 8**  
In Web Filtering > Management > Policy, create a block rule and add the HTTPS filters for websites you want to block.

**Step 9**  
In Web Filtering > Management > Policy, create a warn rule and add the “HTTPS warn” filter with the anytime schedule.

**Step 10**  
Ensure that the HTTPS warn rule has a lower priority than the HTTPS block rule, and then select the Activate check box for both rules.

To comply with privacy laws, notice is given to the user before the SSL connection is established.

You can exclude websites such as banking websites from secure traffic inspection. These websites will bypass secure traffic inspection, and the user will be connected to the site via a direct SSL connection.
Excluding the 'scansafe.com' domain from HTTPS inspection to avoid accidentally blocking your access to ScanCenter when web browsing via CWS. Otherwise, if you've locked yourself out, log onto ScanCenter from a device that is not being redirected to CWS and cancel the setting that locked you out.

Tip

To comply with privacy laws, CWS does not record the Path or Query fields in the logs of HTTPS requests that are inspected. However, you are responsible for ensuring that the content decryption and encryption takes place in a closed loop and that no content is cached.

Caution

Secure Sockets Layer Certificates

When you generate an SSL certificate in Cisco ScanCenter, Cisco is the Certificate Authority (CA). If you want your organization to be the CA, generate a Certificate Signing Request (CSR) in Cisco ScanCenter, use that to generate the certificate, and then upload it to Cisco ScanCenter.

Procedure

Step 1 Click the Admin tab to display the administration menus.
Step 2 In the HTTPS Inspection menu, click Certificates to display the HTTPS Certificates page.

Creating a Certificate in Cisco ScanCenter

Procedure

Step 1 Click Admin, HTTPS Inspection, and Certificates.
Step 2 Click the Create a New Certificate tab.
Step 3 In the Duration drop-down, choose the number of years before the certificate expires. The available options are one year, three years, five years, or seven years.
Step 4 Enter an Identifier.
Step 5 Enter a unique Description.
Step 6 Click Submit to apply your changes. Alternatively, navigate away from the page to abandon your changes.

What to do next

In the List of Certificates table, go to the Action column to download the certificate with either CRT or PEM extension.

Note

The certificate with PEM extension is required for users of the CWS Mobile Browser with Chrome Extension.
Using an Externally Generated Certificate

Before you begin

If you want to generate your own SSL certificate with your organization as the CA, you need SSL software such as Microsoft Certificate Services (a component of Windows Server operating systems) or OpenSSL (a toolkit included with most UNIX and UNIX-like operating systems). If you are not familiar with using SSL software, you can use Cisco ScanCenter instead to create an SSL certificate.

Procedure

Step 1  Click Admin, HTTPS Inspection, and Certificates.
Step 2  Click the Create a CSR (Certificate Signing Request) tab.
Step 3  Enter a unique name for the CSR in the Identifier box.
Step 4  Enter a Description.
Step 5  Click Next to create the CSR.
Step 6  Click Download Your CSR to download the CSR to your computer.
Step 7  Use the downloaded CSR with your SSL software to generate your SSL certificate. For details, see your SSL software support documentation. You have 30 minutes to create and upload the certificate before your current session expires.
Step 8  After you have generated your SSL certificate, click Next.
Step 9  Click Select File and navigate to the SSL certificate to associate with the CSR.
Step 10 Click Upload.

Editing a Certificate Description

Procedure

Step 1  In the Description column, click the pencil icon next to the certificate.
Step 2  Enter a new Description.
Step 3  Click the check icon to apply your change. Alternatively, click the x icon or navigate away from the page to abandon your change.

Removing a Certificate

To remove an SSL certificate, click the box next to the certificate and click Remove. You will be prompted to confirm deleting the selected certificate.
Filters

Filters enable you to set the websites and categories that will be subject to HTTPS inspection. For more information on managing filters, see Managing Filters, on page 81. The following HTTPS filters are available:

- Categories
- Domains
- Exceptions
- Applications

Tip
Exclude the 'scansafe.com' domain from HTTPS inspection to avoid accidentally blocking your access to ScanCenter when web browsing via CWS. Otherwise, if you've locked yourself out, log onto ScanCenter from a device that is not being redirected to CWS and cancel the setting that locked you out.

Procedure

Step 1
Click the Admin tab to display the administration menus.

Step 2
In the HTTPS Inspection menu, click Filters to display the filters page.

Step 3
Applications that use the HTTPS protocol will not be matched against application filters unless HTTPS inspection is enabled for all traffic, or Application Decryption is enabled. If you have not enabled HTTPS inspection for all traffic and you want to enable application decryption, select the filter, and on the Applications page, select the Enable Application Decryption check box.

Policy

Policy enables you to set the rules for applying HTTPS filters.

Procedure

Step 1
On the Admin > HTTPS Inspection > Policy page, you can set the priority of a rule by clicking the up and down arrow icons and then clicking Save.

Step 2
Click Create HTTPS Rule.

Step 3
Enter a rule Name.

Step 4
In the Certificate pull-down list, select a previously generated certificate.

Step 5
In the Filter pull-down list, select a previously created filter.

Step 6
Select the Active check box to enable the rule action. Alternatively, clear the check box to activate the rule at another time.

Step 7
Search for each group that you want to use this rule by entering the group name and clicking Add Group. If no group is selected, this rule will apply to anyone. Select the Set as Exception check box to exclude this group from the rule.
Step 8  Click **Submit** to apply your changes. Alternatively, click **Cancel** or navigate away from the page to abandon your changes.
PART III

Reporting

• Overview, on page 121
• Viewing Reports, on page 127
• Pre-Defined Searches, on page 135
• Filtering Reports, on page 139
• Reporting Attributes, on page 143
• Creating a Search, on page 153
• Composite Reports, on page 161
• Scheduled Reports, on page 165
• Portal 2.0, on page 169
Overview

- Dashboard, on page 121
- Next Generation Dashboard and Reporting, on page 122
- Getting Started with Reports, on page 123
- Calculating Browse Time, on page 124
- Truncating Large Reports, on page 125

Dashboard

The dashboard gives you an overview of web activity at your organization over the last 24 hours.

Click the Dashboard tab to display the following data:

- All blocks
- Bandwidth usage
- Facebook usage
- Spyware blocks
- Web Filtering blocks
- Web Virus blocks
- AMP blocks

The following data is displayed:

- All blocks
- Top 10 users by blocks

Use the drop-down menu to select one of the following options to filter the results:

- Facebook usage
- Spyware blocks
- Web Filtering blocks
- Web Virus blocks
- AMP blocks

Select Bandwidth Usage to display data for:

- Total bandwidth used
- Bandwidth used by IP
Select **Facebook Usage** to display data for:

- Facebook hits over time
- Facebook bandwidth consumed over time
- Users making the most hits
- Top applications by hits
- Activity by hits
- Users consuming the most bandwidth

Select **AMP Blocks** to display data for:

- AMP blocks over the last two weeks
- Top SHA256s blocked by AMP over the last two weeks—Click on a bar in the bar graph to display the traffic for that SHA256
- Number of files sandboxed over the last two weeks
  - Sandboxing is recommended to monitor suspicious files found by AMP. With sandboxing enabled, potentially malicious files are analyzed in a virtual environment to determine if they contain malicious code. Sandboxing can be enabled by navigating to **Web Filtering > Management > Global Settings**
  - Click on a bar in the bar graph to display the **Sandbox Analysis** page
    - Select **Pending** status to display data for files either waiting to be or currently being inspected in a sandbox
    - Select **Completed** status to display data for files that have been inspected in a sandbox
    - Specify time zone, time period, or date range
    - **Submission time**—When the file was submitted to the sandboxing service
    - **Completion time**—When the sandboxing run was completed
    - **SHA256**—SHA256 hash of the file being examined
    - **Disposition**—Indicates whether the file was found to be clean or malicious
    - **Traffic Reports**—Hyperlink to a report of every transaction with a **Content SHA256** matching the SHA256 of this file
    - **Sandbox Reports**—Hyperlink to a report produced by the sandboxing service with details from the analysis of the file execution. See **Sandboxing, on page 191**

**Next Generation Dashboard and Reporting**

The next generation Cisco ScanCenter introduces a refreshed user interface featuring an enhanced dashboard and reporting portal.

Portal 2.0 is implemented in phases so that you can continue using Portal 1.0 and components of Portal 2.0 when they are made available.

Currently, these capabilities are not yet available in the dashboard and reporting components of Portal 2.0:

- Composite report
• Scheduled report
• User activity report
• AMP dashboard

For information on accessing and using the next generation portal, see Portal 2.0, on page 169.

Getting Started with Reports

The reporting functionality in Cisco ScanCenter is accessed from the Reports tab. Reports enable you to analyze:

• Applications
• Bandwidth
• Blocks
• Browse Time
• Browsers
• Categories
• Facebook
• Groups
• Hosts
• Legal Liability
• Malware
• Security
• Users

There are three generic types of report:

• Standard reports use conditions, and up to two attributes to provide more detailed information for a chosen time period.
• Time Analysis reports provide similar information to standard reports but for a single attribute over a chosen time period.
• Detailed reports use conditions and multiple attributes to provide a higher level of detail than standard reports for a chosen time period.

There are also two special report types:

• Allowed Traffic
• User Audit Reports

In addition to these reports there are other reports that can be accessed from the Admin tab. For further information, see Audits, on page 49.

Reports are generated by running searches. Cisco provides an extensive range of pre-defined searches. See Pre-Defined Searches, on page 135. You can use these as the starting point for creating your own searches, or you can create searches from scratch.

The main steps to create any type of report are the same:
Procedure

Step 1  Choose a time period for the search, from the last hour to the last year.
Step 2  Choose a pre-defined search or saved search, or create a new search.
Step 3  Add filters based on reporting attributes or metrics.
Step 4  Choose the number of results to view, from 10 to 1000.
Step 5  Choose a reporting attribute by which to group the results.
Step 6  Choose to sort the results by name, bandwidth, browse time, bytes sent, bytes received, or hits.
Step 7  Choose to view the top or bottom results.
Step 8  (Optional) Add a second reporting attribute by which to group the results.
Step 9  Choose to view the report as a grid, bar, column, pie or line chart.
Step 10 Click Launch search.
Step 11 Store the search for future use.

What to do next

There are more than 60 unique attributes to choose from, so it is best to start by using pre-defined searches.

In addition to creating and modifying searches, from the Reports pane you can:

- Create and manage sets of filters.
- Combine searches into composite reports.
- View reports online and print or export them.
- Download reports to view offline or import into a spreadsheet or word processor.
- Schedule reports for delivery by email to groups of recipients.

Note

The reporting functionality requires Adobe Flash 10 (or higher).

Calculating Browse Time

Because it is not possible to tell when a user is away from their computer, or viewing a page that has finished loading, browse time is calculated based on web requests made within a distinct minute.

Any distinct minute in which one or more web requests are made is counted as a single minute of browse time. For example, if a complex web page results in 100 web requests made within a distinct minute, it will count as one minute of browse time.

The actual time taken for a web page to load is not measured. If a web page takes one and a half minutes to load, then web requests will be made across two distinct minutes measured as two minutes of browse time. However, if a user spends an hour reading a simple web page that loaded within a distinct minute that does not refresh itself, this is measured as one minute of browse time.

When you create a reports including browse time, you should always use Host instead of URL to generate the most accurate report.
Browse Time should not be relied on as a metric in two-level reports because this can result in the double counting of requests. For example, if a site is classified in more than one category, or if different Web requests are made in the same minute. It is not possible to determine if a web page refreshed itself.

**Truncating Large Reports**

Occasionally you may enter search criteria that would produce a report that is so large that it cannot be processed. When this happens, Cisco Cloud Web Security modifies the results returned to enable the report to run. If the report is part of a scheduled report, this will be highlighted in the accompanying email. When viewing reports online, the relevant error message is displayed.

The original search is not modified. Reducing the time period may enable the search to run.

When a report of one or two levels, or a time analysis report, with the URL attribute is too large to run, the report will be modified:

- Where one of the attributes is URL, it is replaced with the Host attribute.
- Where the attributes are URL and Host, the result returned will be for a one-level report with Host as the attribute.
- Where the report is so large that even these measures will not allow the report to run, the report will not be run.
**Viewing Reports**

- Viewing Reports Online, on page 127
- Downloading Reports, on page 133

### Viewing Reports Online

Reports are generated from predefined or previously saved searches. They can be viewed online or downloaded as a PDF. When a report has been generated you can refine the search by adding filters or changing the conditions of the search. You can store your changes as a new search or replace a previously stored search.

**Procedure**

**Step 1**
Click the **Reports** tab to display the **Reports** page. Alternatively, in the **Reports** menu, click **Reports**. The available searches are displayed in two tables:

- Custom reports
- Predefined reports
Step 2 Searches do not include time period information so you must provide this each time you generate a report. In the Time Zone drop-down list, choose a time zone. The default is UTC.

Step 3 In the Time Period drop-down list, choose a predefined time period. The predefined time periods are:

- Previous hour
- Previous day (yesterday)
- Previous week (the last full week)
- Last $n$ hours ($12, 24, 48, \text{ or } 72$)
- Last week (the previous seven days)
- Last $n$ weeks (2 or 3)
- Last month
- Last $n$ months (2, 3, 4, 5, 6, 9, \text{ or } 12)

Alternatively, click Custom and enter the required start and end dates and times:

a) Enter a start date in the box or click the Calendar icon to choose a date.
b) Choose a start time using the hour and minute drop-down lists. The time is shown using the 24-hour clock.
c) Enter an end date in the box or click the Calendar icon to choose a date.
d) Choose an end time using the hour and minute drop-down lists.

Step 4 Select the Auto Run Report check box to run the search as soon as the report is opened. Alternatively, clear the check box to prevent the search running automatically.

Step 5 Click a folder to show or hide the searches for that folder.

Step 6 In the View as drop-down list, choose a chart type. The available charts depend on the type of report and may include:

- Bar
- Column
- Grid
- Line
- Pie
Step 7  
Click **Launch Search** to generate and view a report. Alternatively, click the **Download** icon to download the report in PDF format.

What to do next

When the report has been generated, you can click one of the icons for the available report types to change the way the report is displayed. The available icons depend on the type of report being viewed.

Grid Chart

The grid chart is the default way of viewing reports. From here you can change the data that is displayed in the other charts.

Viewing Grid Data

Choose the number of results to display per page from the **Show** list. The available options are:

- 10
- 25
- 50
- 100

Navigate through the pages using the **first**, **prev**, **next** and **last** buttons.

You can refine your search by clicking entries in the attribute columns. Click an entry, then click **is equal to** to include only that entry in the report. Alternatively, click **is not equal to** to exclude the entry. When you have made your changes, click **Launch search** to display the refined report.
Adding and Removing Metrics

Procedure

**Step 1**
Click the +|- button to display the **Choose which columns you would like to see** dialog.

**Step 2**
For each list entry click **hide** or **show**, as required. The following metrics are available:

- Host
- Bandwidth (the sum of bytes sent and received)
- Bandwidth (% Tot)
- Browse Time (distinct minutes spent browsing)
- Browse Time (% Tot)
- Bytes Received
- Bytes Received (% Tot)
- Bytes Sent
- Bytes Sent (% Tot)
- Hits
- Hits (% Tot)

**Step 3**
Click **Close** to close the dialog.

Sorting Grid Data by Attribute

The first column displays the primary and secondary attributes. Click the primary attribute name to sort by the primary attribute. Click the secondary attribute name to sort by the secondary attribute within the primary attribute sort order.

Changing the Sort Metric

Click any of the other columns to change the sort metric and re-run the report. For reports with two attributes, only the secondary sort metric is changed.

Graphical Charts

There are four types of graphical charts:

- Bar
- Column
- Line
- Pie

Click the hyperlink at the top of the chart to change the sort metric. The available metrics are:

- Bandwidth (Bytes)
- Browse Time (Min)
- Bytes Received
- Bytes Sent
- Hits
Right-click the chart to print or download it.

Choose **Print Chart** to print the chart.
Choose **Save as JPEG Image** to export the chart as a JPEG image.
Choose **Save as PNG Image** to export the chart as a PNG image.
Choose **Save as PDF** to export the chart as an Adobe PDF.

**Bar Chart**

The bar chart displays the data as horizontal bars.

**Column Chart**

The column chart displays the data as vertical bars.
**Line Chart**

The line chart displays time analysis data.

**Pie Chart**

The pie chart displays the data as a 2D or 3D pie chart.
Additional commands are available when you right-click the pie chart.

Click **Enable Rotation** to enable the chart to be rotated by clicking and dragging the chart. You cannot move slices while you are rotating the chart.

Click **Enable Slicing Movement** to enable the chart’s slices to be moved by clicking them. You cannot rotate the chart while you are moving slices.

Click **View 2D** to view a two-dimensional representation of the chart.

Click **View 3D** to view a three-dimensional representation of the chart.

### Downloading Reports

In addition to exporting reports in JPEG, PDF, and PNG format, you can also download reports directly.

### Downloading PDF Reports

To download a report in PDF format, view the report on-screen as normal and then click the **PDF** icon to download the report. Alternatively, you can download a report in PDF format without viewing the report on-screen.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Click the <strong>Reports</strong> tab to display the <strong>Reports</strong> pane. Alternatively, from the Reports menu, click <strong>Reports</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click a folder to show or hide the reports for that folder.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the <strong>View as</strong> drop-down list, choose a chart type. The available charts depend on the type of report and may include:</td>
</tr>
</tbody>
</table>
Downloading CSV Reports

Downloading a report in CSV (comma separated value) format enables you to open the report in a spreadsheet.

**Procedure**

**Step 1** View the report on screen, for example as a grid.
**Step 2** Click the CSV icon to download the report.
Pre-Defined Searches

- Searches by Type, on page 135

Searches by Type

Application Analysis
- What were the top ten applications by browse time?
- What were the top ten applications that consumed the most bandwidth?
- What were the top ten blocked applications and activities?
- Who were the top ten blocked users and from which applications?
- Who were the top ten blocked users and for which activities?
- Who were the top ten users by activity?
- Who were the top ten users that consumed the most bandwidth on media sites?
- Who were the top ten users that consumed the most bandwidth on social networking sites?

Bandwidth Analysis
- What was the bandwidth consumed by major content type?
- What was the bandwidth consumed by category?
- Which were the top ten categories that consumed the most bandwidth?
- What were the top ten social networking sites by bandwidth?
- What were the top ten multimedia sites by hits?
- Which groups consumed the most bandwidth in streaming media?
- Which groups consumed the most bandwidth?
- Which hosts consumed the most bandwidth for the top ten users?
- Which of the organization’s offices consumed the most bandwidth by internal subnets?
- Which of the organization’s offices consumed the most bandwidth?
- Which users consumed the most bandwidth?
- Who were the top ten users by number of hits?
- Who were the top users of streaming media?

Block Analysis
- What adware was blocked?
• What malware was blocked?
• What spyware was blocked?
• What viruses were blocked?
• What were the top ten blocked sites by hits?
• Which were the top ten blocked categories?
• Which hosts were blocked the most for the top ten users?
• Which users were blocked the most by which rules?
• Which users were blocked the most?
• Which Web filtering rules generated the most blocks and who were the top users for those blocks?
• Which Web filtering rules generated the most blocks?

**Browse Time Analysis**

• What was the browse time for the most popular hosts?
• Which users spent the most time on possible business use sites?
• Which users spent the most time on possible productivity reduction sites?
• Which users spent the most time online?

**Browser Analysis**

• What were the top ten user agents?
• What were the top ten browsers?
• What were the top ten user agent strings by hits by external IP?
• What were the top ten user agent strings by hits by groups?

**Category Analysis**

• What was the total number of hits for all categories?
• Which were the top ten categories visited by each internal subnet?

**Facebook Analysis**

• Which were the top ten categories visited by each internal subnet?
• What were the top ten Facebook applications that consumed the most bandwidth?
• What were the top ten blocked Facebook applications and activities?
• Who were the top ten blocked users from which Facebook applications?
• Who were the top ten blocked users for which Facebook activities?
• Who were the top ten users that consumed the most bandwidth on Facebook?

**Group Analysis**

• Which were the top ten groups by hits?
• Which were the top ten groups that consumed the most bandwidth?
• Who were the top ten users with the highest browse time for the top ten groups?

**Host Analysis**

• What was the number of hits for each of the most popular hosts?
• What were the top ten hosts by hits?
• What were the top ten hosts visited for each category?
Legal Liability Analysis

• What was the legal liability risk by category?
• Who were the top ten users browsing for illegal downloads?
• Who were the top ten users browsing in adult categories?

Malware Analysis

• How many phishing blocks were there over time?
• How many threat blocks were there over time?
• Which were the top ten groups with the highest number of spyware blocks?
• What were the top ten blocked adware hosts?
• What were the top ten blocked phishing hosts?
• What were the top ten blocked spyware hosts?
• What were the top ten threats blocked over HTTPS?
• What were the top ten threats blocked per protocol?
• Who were the top ten users browsing spyware hosts?
• Who were the top ten users making outbound spyware requests?
• Who were the top ten users with the highest number of virus blocks?
• Which were the top ten categories where users were blocked by Web Reputation?
• Which were the threat types blocked by Web Reputation?
• Who were the top ten users with the highest number of Web Reputation blocks?
• How many Web Reputation blocks were there over time?
• What malware was blocked by AMP?

Security Analysis

• Which were the top ten blocked categories for malware?
• Which were the top ten categories where users were blocked for spyware?
• Who were the top ten users blocked by Outbound Content Control?
• Who were the top ten users for each risk category?

User Analysis

• Who were the top ten users that browsed the leisure categories?
• Who were the top ten users by hits?
• Who were the top ten users that browsed the most?
CHAPTER 25

Filtering Reports

Filters enable you to refine searches by reporting attributes, metrics, or a combination of both. They can be used to narrow a predefined or saved search or applied when you are creating a search.

Activating and deactivating filters enables you to experiment to find the best set of filters to get the information you want, but only the active filters will be saved. You can also save the filters, separately from the search, as a filter set.

- Adding Filters to a Search, on page 139
- Managing Filter Sets, on page 141

Adding Filters to a Search

A search will include only the results returned where all filter conditions are met. However, only one exact match from the lists of values provided with the in list operators is required to return a result.

Adding a Filter

Procedure

Step 1 Click Add Filter.

Step 2 In the Select filter type drop-down list, choose the required type. The available options are:

- Attribute Filter
- Metric Filter
- Filter Set

Step 3 If you are adding an attribute filter:

a) In the Select attribute list, click the required attribute.

b) In the Select operator list, click the required operator. The available operators are:

- contains
- does not contain
- is equal to
- is not equal to
- in list (equals)
• is not in list (does not equal)
• in list (contains)
• is not in list (does not contain)
• is null
• is not null
• starts with
• does not start with

“Equal to” indicates a full match while “contains” indicates a partial match.

**Step 4** If you are adding a metric filter:

a) In the **Select metric** drop-down list, choose the required metric. The available options are:
   - Bandwidth (Bytes)
   - Browse Time (Min)
   - Bytes Received
   - Bytes Sent
   - Hits

b) In the **Select operator** drop-down list, choose the required operator. The available options are:
   - = (equal to)
   - > (greater than)
   - >= (greater than or equal to)
   - <> (not equal to)
   - <= (less than or equal to)
   - < (less than)

**Step 5** If you are adding an attribute or metric filter, enter a value in the box.

**Step 6** Click **Add** to add and activate the filter

---

**Activating and Deactivating Filters**

Active filters are shown with a green triangle. Inactive filters are shown with a red warning sign.

To activate a filter, click the filter then click **Activate**.

To deactivate a filter, click the filter then click **Deactivate**.

You can click **Select All** to select all the filters or **Select None** to clear the selected filters.

---

**Editing Filters**

To edit a filter, click the filter you want to edit. After you have made your changes, click **Save Changes**.

---

**Removing Filters**

To remove a filter, click **Remove**. You will not be prompted to confirm your action.
Tip
Unless you are certain you will not want to use the filter again, it is generally better to de
cativate a filter instead of removing it.

Managing Filter Sets
Filter sets enable you to combine frequently used filters into a reusable set. Filter sets can contain up to four nested filter sets and up to 20 individual filters. The predefined Active Traffic Only filter set can be used to exclude traffic that was not generated directly by your users. For example, active traffic would include requests generated by the user entering a URL in a browser or clicking a hyperlink, but would exclude external requests that a web page makes to load banners, Adobe Flash content, additional HTML, and so on.

Procedure

Step 1
Click the Reports tab to display the Reports menu.

Step 2
In the Reports menu, click Filter Sets.

Adding a Filter Set

Procedure

Step 1
Click Add.

Step 2
Enter a unique name for the filter set in the box.

Step 3
For each filter to add to the set:

a) Click Add Filter.

b) In the Select filter type drop-down list, choose a filter type. You can add attribute or metric filters, or existing filter sets. You can nest filter sets up to three levels deep.

c) Click Add.

Note
You can edit or remove individual filters contained in filter sets the in the same way you edit or remove filters contained in a report.

Copying a Filter Set

Procedure

Step 1
Click the filter set.
Renaming a Filter Set

Procedure

Step 1  Click the filter set.
Step 2  Enter a unique name in the box and press Enter.

Editing a Filter Set

Click the filter set, make your changes, and then click Save Changes.

Removing a Filter Set

Procedure

Step 1  Click the filter set.
Step 2  Click Delete to permanently remove the filter set.
CHAPTER 26

Reporting Attributes

Reporting attributes are the main filter applied to searches to generate reports.

- Attributes List, on page 143

Attributes List

The contents of the majority of attributes are normalized to lower case. However, for some attributes you may wish to view the original string as entered by the user. Attributes listed with “Original” in parentheses are available in normalized and original form.

Adware
The name of the adware block.

AMP Threat Name
The name of the malware detected and blocked by AMP.

Application Activity
The activity or web application.

Application Name
The name of the web application.

Application Name With Unclassified
The name of the web application or an unclassified result.

Block Type
The pattern, specified in the filter, that generated the block. It can be one of the following:

- adware
- amp_malware
- category (HTTP)
- category (HTTPS)
• content type
• domain/URL
• file type
• phishing
• possibly unwanted applications (PUAs)
• spyware
• virus
• webrep

**Note**

If more than one pattern is matched, the value of Block Pattern will be “multiple patterns.”

**Block Value**

The string that matched the block pattern. It can be one of the following:

• adware name
• AMP threat name
• category name
• full URL
• MIME type
• name of the content type
• name of the file type
• phishing name
• possibly unwanted application (PUA) name
• spyware name
• virus name
• webrep name

**Note**

Where the block was generated by an exception or by more than one pattern, the value of Block String will be “multiple strings.”

**Category**

The web filtering category.

When changes are made to the categories, existing customer data is not migrated. When creating reports, you must include the old and new category names with the “Category in list” filter to ensure that all the results are returned. Composite reports do not need to be updated because they will inherit the settings of the included reports.

Pre-defined reports are updated for you. For example, the “User Analysis” report “Where were the Top 10 Users browsing in the Categories Shopping, Music, Cinema/TV and Sport” originally included the filter “Category in list music, cinema/tv, online shopping, sports.” It now includes the filter “Category in list music, cinema/tv, online shopping, sports, entertainment, shopping, sports and recreation.”
Cipher Suite
Authentication and encryption types, e.g. TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, SSL_RSA_WITH_RC4_128_SHA, TLS_ECDHE_RSA_WITH_RC4_128_SHA, TLS_RSA_WITH_AES_128_CBC_SHA256.

Company Name
Name of the company associated with the data traffic.

Company/Group
Group for the company users, e.g. Active Directory.

Company/User
User associated with a given data traffic.

Connector ID
ID of the Connector software being used to monitor users, e.g. AnyConnect.

Connector Mode
The mode reported by Connector.

Connector OS Name (Original)
The name of the operating system reported by Connector.

Connector OS Version (Original)
The version of the operating system reported by Connector.

Connector ReUse ID
Flag specifying the reuse of the user authentication headers associated with a given connector in TCP connections.

Connector Version
Logs the version of Connector used to embed the directory information. Can be used to easily find out which versions of Connector are deployed in your environment.

Content SHA256
A SHA256 hash of the content sent to or uploaded by the user.

Country Dst Code
The two-letter ISO code of the country where the web server is located, derived from its IP address.

Country Src Code
The two-letter ISO code of the country where the client web browser is located, derived from its IP address.
Day of Month

Used for time series plotting (1 to 31).

Day of Week

Used for time series plotting (monday to sunday).

Destination IP

The IP address of the remote web server.

Domain Username (Original)

The username under which the user is logged in to the domain.

External IP

The IP address that Cisco Cloud Web Security gets from the customer (also known as the egress IP address), for example 192.0.2.0. Alternatively, the subnet of the IP address that Cisco Cloud Web Security gets from the customer (also known as the egress IP address subnet), for example 192.0.2.0/24.

forwarded for

IP address used to locate the origin of a request. For example, if given there is no DC in Africa, users connect to Brazil and are forwarded. This attribute identifies that the user requests actually originated in Africa.

Group (Original)

The name of the directory group logged, for example WinNT://US\SALES.

Note

Multiple directory groups can be logged for each user.

Group Domain

The name of the domain logged for the user.

Group Name Part (Original)

The name of directory group (not including either LDAP://<domain> or WinNT: //<domain>), for example for WinNT://US\SALES, the group name part is SALES.

Host (Original)

The host part of the URL string, for example, for news.example.com/sport, the host is news.example.com.

Note

Hosts are case insensitive.
**Hour**
Used for time series plotting.

**Inbound File Extension**
The file extension part of any inbound URL using the HTTP(S) protocol, for example, for `index.html` the file extension is `html`.

**Inbound File Name**
The filename part of any inbound URL using the HTTP(S) protocol, for example, `index.html`.

**Internal IP**
The IP address the Connector sees from the internal user, for example `192.168.2.10`. Alternatively, the IP address subnet that the Connector sees from the internal user, for example `192.0.2.0/24`.

---

**Note**
If an internal user is routed through a NAT device before reaching the internal proxy, the IP address, or subnet, that arrives at the Connector is logged.

**Malware**
The name of the malware block.

**Minute**
Used for time series plotting (00 to 59).

**Month**
Used for time series plotting (january to december).

**Outbound File Extension**
The file extension part of any outbound POST using the HTTP(S) protocol, for example for `resume.doc` the file extension is `doc`.

**Outbound File Name**
The filename part of any outbound POST using the HTTP(S) protocol, for example `resume.doc`.

**Path**
The path part of the URL string, for example, for `news.example.com/sport`, the path is `/sport`.

**Pattern Name**
See the Block Value attribute.
**Pattern Type**
See the Block Type attribute.

**Phishing**
The name of the phishing block.

**Policy Violation**
The block value where a web filtering rule resulted in a block.

**Port**
Port number of web request, for example, 80 or 443.

**Protocol**
- FTP
- HTTP
- HTTPS

**PUA**
Possibly Unwanted Application name.

**Query**
The query part of the URL string, for example, for http://www.example.com/search?hl=en&q=free+screensavers&btnG=Example+Search&meta=&aq=f&oq=, the query is hl=en&q=free+screensavers&btnG=Example+Search&meta=&aq=f&oq=.

---

**Note**
Using this attribute will increase the time that reports take to generate by a considerable amount.

**Referrer Host (Original)**
The host part of the referrer URL string, for example, for news.example.com/sport, the host is news.example.com.

**Referrer Path**
The path part of the referrer URL string, for example, for news.example.com/sport, the path is /sport.

**Referrer Port**
Port number of referrer, for example 80 or 443.

**Referrer Protocol**
- FTP
- HTTP
• HTTPS

Referrer Query
The query part of the referrer URL string, for example, for http://www.example.com/search?hl=en&q=free+screensavers&btnG=Example+Search&meta=&aq=f&oq=, the query is hl=en&q=free+screensavers&btnG=Example+Search&meta=&aq=f&oq=.

Referrer Second Level Domain
Normally the referrer organization, for example, in www.example.com, the second level domain is example.

Referrer Top Level Domain
Normally the last part of the referrer domain, for example, com, net, org, gov, and co.uk.

Referrer URL (Original)
The full referrer URL string.

Request Content MD5
The MD5 checksum of the user request.

Request Content Type (Original)
The request MIME type, for example, image/gif, application/pdf, text/html, application/EDI-X12.

Request Major Content Type
The type of request content, for example, if the response content type is application/pdf, then the corresponding major content type is application. Examples include:

• application
• audio
• image
• text
• video

Request Method (Original)
• CONNECT
• GET
• POST

Request Version (Original)
The request version, for example, HTTP/1.0 or HTTP/1.1.
Response Content Type (Original)

The response MIME type, for example, image/gif, application/pdf, text/html, application/EDI-X12.

Response Major Content Type

The type of response content, for example, if the response content type is application/pdf, the corresponding major content type is application. Examples include:

- application
- audio
- image
- text
- video

Response Status Code

Enables you to filter by the response status code, for example, to find all web requests to pages that did not exist, you can filter by 404. More information on status codes can be found at http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html.

Response Version (Original)

The response version, for example, HTTP/1.0 or HTTP/1.1.

Risk Class

The superclass under which the risk is grouped:

- possible business usage
- possible productivity reduction
- heavy bandwidth usage
- potential legal liability
- potential security risk

Rule Action

There are five rule actions you can choose from:

- allow
- authenticate
- block
- warn
- inspect

Note

If a website does not respond to a request, no Rule Action is assigned, but the request is still stored.

Rule Engine

The rule engine that generated the rule action:
• policy evaluator
• scanlet

Rule Name (Original)
The Cisco ScanCenter policy rule name.

Rule Stage
The part where the rule was applied, e.g. response_headers, response_body_start, reqmod.'

Second Level Domain
Typically the organization, for example, in www.example.com, the second level domain is example.

SHA256 Source
Indicates whether the Content SHA256 is a hash of the HTTP request post data or response data: request, response, or N/A.

Spyware
The name of the spyware block.

Threat Type
Each record can include multiple threat types from the following:
• adware
• category
• content type
• extension
• file match
• filter protocol
• phishing
• possibly unwanted applications (PUAs)
• quota
• regular expression
• spyware
• virus

Time Stamp
The time at which the rule action was applied in minutes and seconds. Available only in Detailed Search.

Top Level Domain
Typically the last part of the domain, for example, com, net, org, gov, and co.uk.

URL (Original)
The full URL string.
**User (Original)**
The logged username (if applicable). It can be in the form of WinNT://<username> or a custom text name.

**User Agent (Original)**
The complete user agent string, for example, Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1). More information on user agent strings can be found at http://www.useragentstring.com/pages/useragentstring.php.

**User Agent Application Name**
The user agent application name, for example, Mozilla. See User Agent.

**User Agent Application Version**
The user agent application version, for example, 4.0. See User Agent.

**User Agent Comp Platform**
The user agent platform token, for example, Windows NT 5.1. See User Agent.

**User Agent Comp Version**
The user agent version token, for example, MSIE 7.0. See User Agent.

**User Agent Compatibility**
The user agent compatibility flag, for example, compatible. See User Agent.

**User Domain Name**
The domain where the user that made the request belongs.

**User Domain Name Part**
A lowercase substring of the user domain name.

**Via**
A list of IP addresses identifying the intermediate proxies processing the user request.

**Virus**
The name of the Virus block, for example, Trojan.Downloader.abg.

**Web Reputation Threat**
See the Block Value attribute, given Block Type is webrep.

**Year**
Used for time series plotting.
Creating a Search

• Overview, on page 153
• Creating a Standard Search, on page 154
• Creating a Time Analysis Search, on page 154
• Creating a Detailed Search, on page 155
• User Audit Reports, on page 157
• Creating a Search from a Predefined Search, on page 157
• Storing a Search, on page 158
• Editing a Search, on page 159
• Renaming a Search, on page 159
• Removing a Search, on page 159
• Removing an Empty Folder, on page 160

Overview

Reports are generated by running one of the three available search types. Searches are refined by time period and filters.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Click the Reports tab to display the Reports menu.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>On the Reports menu, click Search.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the tab for the type of search to create. The tabs are:</td>
</tr>
<tr>
<td></td>
<td>• Search</td>
</tr>
<tr>
<td></td>
<td>• Time Analysis</td>
</tr>
<tr>
<td></td>
<td>• Detailed Search</td>
</tr>
</tbody>
</table>
Creating a Standard Search

Procedure

Step 1  Select a time period.
Step 2  Add any required filters.
Step 3  Enter the number of primary attributes to be displayed in the View first box (1 to 20000).
Step 4  In the primary attribute list, click the required primary attribute.
Step 5  In the primary sort metric list, click the required primary sort metric. The available metrics are:
   - Name
   - Bandwidth
   - Browse Time
   - Bytes Received
   - Bytes Sent
   - Hits
Step 6  Click the hyperlink to change the primary sort order. The hyperlink indicates the current order. For descending order, the top \( n \) results are shown. For ascending order, the bottom \( n \) results are shown.
Step 7  Clear the check box to exclude secondary attribute criteria. Alternatively select the check box to enable additional criteria, and then:
   a) Enter the number of secondary attributes to be displayed in the and their first box (1 to 20000).
   b) In the secondary attribute list, click the required attribute.
   c) In the secondary sort metric list, click the required sort metric.
   d) Click the hyperlink to change the secondary sort order.
   Note  The product of the values entered in the View first and the and their first boxes must be no larger than 20,000.
Step 8  Click Launch Search. When the report has been generated, it is displayed below the button.

Creating a Time Analysis Search

Procedure

Step 1  Select a time period.
Step 2  Add any required filters.
Step 3  In the View list, click the number of attributes to display (1 to 12).
Step 4  In the attribute list, click the required attribute.
Step 5  In the sort metric list, click the required sort metric. The available metrics are:
   - Name
• Bandwidth
• Browse Time
• Bytes Received
• Bytes Sent
• Hits

Step 6  Click the hyperlink to change the sort order.
Step 7  Click Launch Search. When the report has been generated, it is displayed below the button.

Creating a Detailed Search

Procedure

Step 1  Select a time period.
Step 2  Add any required filters.
Step 3  Choose between one and 15 reporting attributes to include in the report. The default attributes are Timestamp, Category, Group, Host, Internal IP, Path, Query, Rule Action, and User. To add one or more attributes:
   a) Click the Add/Remove columns hyperlink.
   b) In the attribute list, click the required attribute or attributes.
      To remove an attribute, hover over the attribute and click the Remove icon. Alternatively, Click the Add/Remove columns hyperlink, and then click the attribute or attributes you wish to remove. You cannot remove the Timestamp attribute.
Step 4  Click the attribute you want to sort by. Clicking the selected attribute changes the sort order, which is indicated by a triangle.
Step 5  Drag and drop the attributes to change the order of the columns in the report. Alternatively, accept the default order to use Timestamp as the sort order.
Step 6  Click Launch Search. When the report has been generated, it is displayed below the button.

What to do next

In some cases, the report shows no records. This could be caused by search criteria such as explicit filters or the specified time range. This could also be caused by the use of a derived attribute acting as an implicit filter.

Derived attributes are not directly mapped to columns in the database. Instead, they are derived from one or more database columns. For example, Content SHA256 is derived from a combination of Request SHA256 and Response SHA256. So, if both columns are NULL, then Content SHA256 is also NULL. By being implicitly filtered, the reporting service receives zero rows and shows no records.

Derived attributes include:
  • Adware
  • AMP Threat Name
  • Application Name
• Block Category
• Block Type
• Block Value
• Category
• Content SHA256
• Malware
• Pattern Name
• Pattern Type
• Phishing
• Policy Violation
• PUA
• Risk Class
• Spyware
• Threat Type
• Virus
• Web Reputation Threat

Allowed Traffic

You can also create a detailed report from an allowed traffic report. The allowed traffic report shows all of the allowed traffic by category for a single day. Security risks are shown as a colored icon in the hour column for the various filter categories with the following meanings:

• Red—High security risk.
• Yellow—Medium security risk.
• Green—Low security risk.

Procedure

Step 1  Click the Reports tab to display the Reports menu.
Step 2  In the Reports menu, click Allowed Traffic.
Step 3  In the Type drop-down list, choose a filter type:
  • User
  • Group
  • Internal IP
Step 4  Enter a Date in the box or click the Calendar icon to choose a date.
Step 5  Enter a username, group name, or internal IP address in the User/Group/IP box, for example, default.
Step 6  Click Search to view the report.
Step 7  Click the icon to display a detailed report of the risk.

## Downloading Detailed Reports as CSV

Downloading a detailed report in CSV (comma separated value) format enables you to open the report in a spreadsheet.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>View the report as a grid.</td>
</tr>
<tr>
<td>2</td>
<td>Click the CSV icon to download the report.</td>
</tr>
</tbody>
</table>

## User Audit Reports

User Audit reports provide more details about a specific user. These reports cannot be scheduled or added to a composite report. However, you can export the report in PDF or CSV format as with other reports.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Click the Reports tab to display the Reports page.</td>
</tr>
<tr>
<td>2</td>
<td>In the Reports menu, click User Audit.</td>
</tr>
<tr>
<td>3</td>
<td>Enter the IP address or full username string of the User.</td>
</tr>
<tr>
<td>4</td>
<td>Click Launch Search.</td>
</tr>
</tbody>
</table>

### Creating a Search from a Predefined Search

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Click the Reports tab to display the Reports page.</td>
</tr>
</tbody>
</table>
### Storing a Search

When you have run a search to generate a report, you can store the search criteria for future use.

#### Procedure

**Step 1**  
Click **Save**. Alternatively, click **Save as** to store a copy of the search. The **Use current settings to create a new Report** dialog is displayed.

- **Report title**  
  - Choose a report title (max. 256 characters): 
  - OR use the default name
  - **First 10 "Use"**

- **Report folder**  
  - Choose an existing folder from the list: 
  - OR
  - Create a new folder: **Folder name** (max. 256 characters)

**Step 2**  
Enter a name for the search (up to 256 characters) in the **Choose a report title** box. Alternatively, select the **use the default name** check box to use the name next to the check box.

**Step 3**  
In the **Choose an existing folder from the list** drop-down list, choose a folder. Alternatively, select the **Create a new folder** check box and enter a **Folder name** (up to 256 characters). If you select the default, (no folder), the search will be displayed at the top level.

**Step 4**  
Click **SUBMIT** to store the search. Alternatively, click **Close window** to abandon storing the search.
Editing a Search

Procedure

Step 1  Run the search.
Step 2  Edit the search criteria.
Step 3  Click Save to apply your changes. Alternatively, click Save as to store the modified search with a new name.

Note  You cannot replace a predefined search or a search that is part of a composite report. You must store the modified search with a new name.

Renaming a Search

Procedure

Step 1  Click the Reports tab to display the Reports page. Alternatively, on the Reports menu, click Reports.
Step 2  If the search that you wish to rename is contained within a folder, click the folder to display the search.
Step 3  Click the Rename icon.
Step 4  Enter a new name in the Enter new name box and press Enter. Alternatively, click the X icon to abandon renaming the search.

Removing a Search

Procedure

Step 1  Click the Reports tab to display the Reports page. Alternatively, on the Reports menu, click Reports.
Step 2  If the search that you wish to delete is contained within a folder, click the folder to display the search.
Step 3  Click the Delete icon. You will be prompted to confirm your action.
Step 4  In the dialog, click OK to remove the search. Alternatively, click Cancel to abandon removing the search.

Note  You cannot remove a search that is part of a composite report. You must first remove the search from the composite report. You cannot remove predefined searches.
Removing an Empty Folder

Procedure

- **Step 1** Click the Reports tab to display the Reports page. Alternatively, on the Reports menu, click Reports.
- **Step 2** Click the Delete icon. You will be prompted to confirm your action.
- **Step 3** In the dialog, click OK to remove the folder. Alternatively, click Cancel to abandon removing the folder.

**Note** You cannot remove a folder that is not empty. You must first remove any stored searches from the folder.
Composite Reports

- Creating Composite Reports, on page 161
- Downloading Composite Reports, on page 162
- Editing Composite Reports, on page 162
- Removing Composite Reports, on page 162

Creating Composite Reports

Composite reports enable you to combine the contents of two or more existing searches into a single report. You can also combine pre-defined searches with searches you have created yourself. You can combine a maximum of 20 searches in a composite report.

Procedure

Step 1 Click the Reports tab to display the Reports menu.
Step 2 On the Reports menu, click Composite Reports.
Step 3 Click the Create Composite Reports tab.
Step 4 Enter a name for the report in the Composite Report Name field.
Step 5 For each search to include:
   a) In the Reports to Include drop-down list, choose the required search.
   b) Click add.
      To change the order in which the searches will be displayed:
   a) In the Report table, click the required search.
b) Use the move up and move down icons to change the position of the search.

To remove a search from the composite report, click the Delete icon.

Step 6 Add any required filters or filter sets.
Step 7 Click Create Composite Report to store the composite report.

---

**Downloading Composite Reports**

**Procedure**

Step 1 Click the Reports tab to display the Reports menu.
Step 2 On the Reports menu, click Composite Reports.
Step 3 Click the Manage composite reports tab.
Step 4 Select a time period.
Step 5 Click the Download icon to download the composite report as a PDF.

---

**Editing Composite Reports**

**Procedure**

Step 1 Click the Reports tab to display the Reports menu.
Step 2 On the Reports menu, click Composite Reports.
Step 3 Click the Manage composite reports tab.
Step 4 Click the Edit icon next to the composite report to edit.
Step 5 When you have finished editing the report, click Save changes to apply your changes.

---

**Removing Composite Reports**

**Procedure**

Step 1 Click the Reports tab to display the Reports menu.
Step 2 On the Reports menu, click Composite Reports.
Step 3 Click the Manage composite reports tab.
**Step 4**  Click the **Delete** icon next to the composite report to remove. You will be prompted to confirm your action.
Scheduled Reports

Scheduling reports enables you send reports via email to specific recipients. Before scheduling a report, you must have created at least one email group with at least one recipient. There is a maximum limit to the number of reports that you can schedule, typically 75. Each report in a composite report counts as an individual report when determining if the maximum number of reports has been reached.

Caution

Users who have filters applied to their results, or attributes hidden, are not permitted to schedule reports. However, scheduled reports do not enforce user-level restrictions, and any user receiving a scheduled report will see the full report.

Email Groups

Email groups enable you to send scheduled reports to groups of recipients.

Creating an Email Group

Procedure

Step 1 Click the Reports tab to display the Reports menu.
Step 2 On the Reports menu, click Recipients.
Step 3 Enter a group name in the Groups box.
Step 4 Click Create new group.
Removing an Email Group

Procedure

Step 1  Click the Reports tab to display the Reports menu.
Step 2  On the Reports menu, click Recipients.
Step 3  Click the Delete group icon next to the group to remove.

Caution  You will not be asked to confirm your action. Removed groups cannot be recovered.

Email Recipients

Scheduled reports are sent to groups of email recipients. If you want to send a report to a single recipient, you must create a group with only one recipient.

Creating an Email Recipient

Procedure

Step 1  Click the Reports tab to display the Reports menu.
Step 2  On the Reports menu, click Recipients.
Step 3  Click the group to add recipients to.
Step 4  Enter the first part of the email address in the Recipients for box.
Step 5  In the @ list, click the last part of the email address. Only valid email domains for your organization are included in this list.
Step 6  Click Add recipient.

Removing an Email Recipient

Procedure

Step 1  Click the Reports tab to display the Reports menu.
Step 2  On the Reports menu, click Recipients.
Step 3  Click the group containing the recipients to remove.
Step 4  Click the Remove a recipient icon next to the email recipient to remove.
Creating a Scheduled Report

Procedure

**Step 1** Click the Reports tab to display the Reports menu.

**Step 2** On the Reports drop-down menu, click Scheduled Reports.

**Step 3** Click the Create Scheduled Report tab.

**Step 4** In the Create Scheduled Report area, enter a name for the scheduled report in the Scheduled Report Name field.

**Step 5** In the Delivery Schedule area, click one of the following to set when the report will run:

- Daily—Every day
- Weekly—Every week on the day specified
- Monthly—Every month on the first day of the month
- Four weekly—Every four weeks on the day specified

Reports contain data for the period up to midnight on the day before the report is run:

- Daily contains the previous 24 hours.
- Weekly contains the previous seven days.
- Monthly contains the previous month.
- Four weekly contains the previous 28 days.

**Step 6** If you chose weekly or four-weekly reports, you must choose a day on which they will run. In the Scheduled Day drop-down list, choose a day.

**Step 7** Select a Time Zone. This determines the hour at which the day begins for reporting purposes.

**Step 8** In the To (recipient group) drop-down list, choose a group.

**Step 9** In the Email Content area, enter the Subject for the generated e-mail, for example, Monthly bandwidth report.

**Step 10** Enter the Message for the email, for example, Report attached.

**Step 11** In the Report drop-down list, choose a pre-defined, stored, or composite report.

**Step 12** Click PDF to send the report as a PDF file. Alternatively, click CSV to send the report as a CSV file.

**Step 13** In the Security area, enter a password in the Enter Password and Confirm Password fields to set the password for the generated PDF or CSV file.

**Step 14** Click Save Changes to store the scheduled report.

---

**Caution** You will not be asked to confirm your action. Removed recipients cannot be recovered.
What to do next

Note
CSV files are sent as ZIP files with AES encryption. A program that supports this type of ZIP file is required to open these files.

Note
Detailed reports cannot be scheduled. This includes pre-defined reports that are detailed reports. If you must schedule detailed reports, consider using the Log Extraction feature, which allows detailed processing by third-party tools of all web transactions. See Log Extraction, on page 37.

Editing a Scheduled Report

Procedure

Step 1
Click the Reports tab to display the Reports menu.

Step 2
On the Reports menu, click Scheduled Reports.

Step 3
Click the Manage scheduled reports tab.

Step 4
Click the Edit icon next to the composite report to edit.

Step 5
When you have finished editing the report, click Save changes to apply your changes.

Removing a Scheduled Report

Procedure

Step 1
Click the Reports tab to display the Reports menu.

Step 2
On the Reports menu, click Scheduled Reports.

Step 3
Click the Manage scheduled reports tab.

Step 4
Click the Delete icon next to the scheduled report to remove. You will be asked to confirm that you want to remove the scheduled report.

Note
Removing a scheduled report does not remove the original report or email group.
Overview

Portal 2.0 offers you more flexibility in customizing the data you are shown and drilling down into metrics for faster response and greater efficiency when analyzing your traffic. To view the next generation portal, click the Launch Portal button on the Cisco ScanCenter Home page.

Note
Some functionality may not be present in your account, depending on your region, vendor, and licensing. Contact your Cisco sales representative for further information.

Near the upper left corner of the page, click the main menu icon to choose:

- **Dashboard**—Opens the Top Overview Dashboard page.
- **Analysis**—Opens the reporting pages: Quick Analysis, Detailed Analysis, and Saved Reports. Saved Reports include predefined reports (such as bandwidth analysis, application analysis, and block analysis) and favorite reports (custom report templates that have been created and saved).
- **Preferences**—Opens the User Preferences page where you can select your time zone, date format, and preferred language.
- **Portal 1.0**—Opens the Cisco ScanCenter Home page. Portal 2.0 is implemented in phases so that you can continue using Portal 1.0.

Note
Near the upper right corner of the page, click the speech bubble icon to submit feedback and feature requests.
Dashboard

The Top Overview Dashboard shows an overview of web activity in your network over the last 24 hours.

- The horizontal timeline shows the number of blocks and amount of bandwidth during each hour.
- Above the horizontal timeline are filters you can click to display the blocked (Blocks) or allowed (Bandwidth) traffic.
- Below the horizontal timeline are widgets that display data metrics you choose to view.
- Widgets are customizable.
- Drill down for more specifics by clicking on any information bar within the widgets.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Portal 2.0 main menu, select <strong>Dashboard</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select a time zone from the drop-down list. The dashboard time period covers the previous 24 hours.</td>
</tr>
<tr>
<td>Step 3</td>
<td>You may choose to view data for all traffic allowed or blocked by using the selectable filters above the horizontal timeline.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Within each widget, from the upper-right drop-down list, choose a metric to sort the data shown.</td>
</tr>
</tbody>
</table>
| Step 5 | (Optional) Click **Edit widgets** to make widget changes. Click **Save** to save your changes for the current admin user.  
  a) Add a widget by clicking **New widget**.  
  b) Remove a widget by clicking its circled x icon.  
  c) To reorder the widgets, click the directional icon to drag-and-drop each widget.  
  d) Edit a widget by clicking its pencil icon. You can then choose its chart type. |

What to do next

Drill down into the widgets for more focused information. For example, to view more detail on a particular user, click on that user listed within a widget. A new page is displayed showing information related only to that user. A user filter is added to the filters header. Then, to filter the data shown on that user, click on any information within the widgets. The widgets are updated and a second filter is added to the filters header. At any point, you can click the circled x icon in any filter to remove it from the header and update the data shown. Furthermore, if desired, click on more information to add a third filter to the filters header, which then automatically opens the Detailed Analysis page. See Detailed Analysis Reports, on page 172.

Quick Analysis Reports

Procedure

| Step 1 | In the Portal 2.0 main menu, select **Analysis** and click the **Quick** analysis tab. |
Step 2 Select a time zone from the drop-down list.

Step 3 Select a predefined time period, or click Custom and enter the required start and end dates and times:
• Click the From box to choose a start date.
• Click the clock icon to choose a start time using the hour and minute selector arrows. The time is shown using the 24-hour clock.
• Click the To box to choose an end date.
• Click the clock icon to choose an end time using the hour and minute selector arrows.

Step 4 Select a type of report:
• Single-level report with one reporting attribute
• Dual-level report with two attributes
• Time-based trending report
• User audit report

Step 5 For the type of report, select at least one reporting attribute.

Step 6 For the type of report, select at least one sorting metric.

Step 7 Select a number from 1 to 20,000 of records to be shown.

Step 8 Select a filter set from the drop-down list. If the list is empty, create and add filters.
   a) Select an attribute or a metric.
   b) Select an operator.
   c) Enter a value.
   d) Click Add to add the filter you have created to the current set.
   e) Optionally, repeat these steps to create and add more filters as needed to the current set.
   f) To enable or disable filters, click the corresponding toggle switch to the right of that filter.
   g) To delete individual filters out of a set, click the circular x button to the right of that filter.
   h) To save the set, click Save filters and enter a name for the filter set.

Step 9 Click Search to generate and display the results table.

Step 10 Optionally, click the sorting arrows in any column header to sort the table rows according to the data in that column.

Step 11 Optionally, rearrange the columns by clicking and dragging by their headers.

What to do next
Click the + sign in the filter header to expand or minimize the section for modifying the report or filter parameters.

To save yourself time spent having to replicate the search, click Save Report, enter a descriptive name, and click Save. This saves the report search template you have created to the Favorite Reports section of the Saved Reports page.

Click Export to download the report to your device as a CSV or PDF file.
Detailed Analysis Reports

Procedure

Step 1  In the Portal 2.0 main menu, select Analysis and click the Detailed analysis tab.

Step 2  Select a time zone from the drop-down list.

Step 3  Select a predefined time period, or click Custom and enter the required start and end dates and times:
   • Click the From box to choose a start date.
   • Click the clock icon to choose a start time using the hour and minute selector arrows. The time is shown using the 24-hour clock.
   • Click the To box to choose an end date.
   • Click the clock icon to choose an end time using the hour and minute selector arrows.

Step 4  Select a filter set from the drop-down list. If the list is empty, create and add filters.
   a) Select an attribute or a metric.
   b) Select an operator.
   c) Enter a value.
   d) Click Add to add the filter you have created to the current set.
   e) Optionally, repeat these steps to create and add more filters as needed to the current set.
   f) To enable or disable filters, click the corresponding toggle switch to the right of that filter.
   g) To delete individual filters out of a set, click the circular x button to the right of that filter.
   h) To save the set, click Save filters and enter a name for the filter set.

Step 5  Select which columns appear in the results table.
   a) To add a column, select the attribute or metric from the drop-down list and click Add.
   b) To remove a column, click the circular x button in its box.
   c) For information on reporting attributes, see Attributes List, on page 143.

Step 6  Click Search to generate the results table. As seen in the status bar above the table, running search results are gathered in chunks dynamically.
   • Click Pause to suspend the data gathering process. To modify search parameters, you can click the + sign on the filter header to expand the section for editing filters and table columns. Click Close to minimize the editing section.
   • Click Resume to continue from where you paused.
   • Click Search to restart the search.

Step 7  The left panel of the table lists filters you may use to refine the results shown. Click any See more to open a subpanel where you can also search for certain text within the results. Click See less to close the subpanel.

Step 8  Optionally, click the sorting arrows in any column header to sort the table rows according to the data in that column.
Step 9

Optionally, rearrange the columns by clicking and dragging by their headers.

What to do next

To modify the report, click the + sign on the filter header to expand or minimize the section for editing filter and table parameters.

Click Export to download the report to your device as a CSV file.
PART IV

Threat Analysis

• Advanced Threat Detection, on page 177
• Threats Tab, on page 181
• Sandboxing, on page 191
• Investigating Incidents, on page 193
• CTA STIX/TAXII Service, on page 197
Advanced Threat Detection

Overview

Cisco Cloud Web Security consists of multiple security technologies designed to protect your network throughout the full attack continuum. Cisco Cloud Web Security Premium adds Advanced Threat Detection (ATD) services to Cisco Cloud Web Security Essentials and provides additional features that enhance the protection of your network from advanced cyber threats.

- Advanced Malware Protection (AMP) operates in the during and after phases of the attack continuum.
  - In the during phase, scans file reputation to automatically detect and block known and emerging malware threats in real time.
  - In the after phase, performs behavioral analysis of suspicious files in a virtual sandbox environment to prevent malicious files from affecting your network. Cumulative analysis and intelligence information about the files collected from the community are shared through a sandbox report.
  - Tracks the spread of any file within your network and continuously monitors file reputation over time. If a file reputation changes to malicious or is found by file sandboxing to be malicious, AMP provides retrospective alerting in the after phase. AMP identifies every instance of the file within your network to address the problem of malicious files passing through perimeter defenses that are later deemed a threat.

- Cognitive Threat Analytics (CTA) extends Cisco Cloud Web Security into the after phase of the attack continuum.
  - Actively monitors your network to spot behavior outside the norm.
  - Automatically detects suspicious activity inside your network.
  - Using behavioral analysis of network traffic to detect anomalies, identifies symptoms of malware infection or data breach.
  - Reduces the time to discover threats operating inside your network.
• Performs independent (of any global feeds) analysis of your web traffic to detect attacks targeted against your network.

• Delivers local security intelligence specific to your network environment.

• Uses advanced statistical modeling and machine-learning to identify new threats.

---

**Note**

AMP and CTA are activated as part of the provisioning process for Cisco Cloud Web Security Premium. No additional configuration within Cisco ScanCenter is required.

---

**Caution**

In cases where the size of the executable file is larger than 128KB, streaming of the file to the browser begins before the file scan is completed. If the AMP scan finds the file to be malicious, a TCP Reset is sent to the browser to stop the file download. However, if the TCP Reset gets blocked, the connection is closed, but the partially downloaded file remains available.

---

**Additional Benefits**

• Continuous monitoring reduces time-to-detect and helps you prioritize the investigation of attacks on your network.

• Identifies hosts infected by malware or compromised with advanced threat infections that were able to sneak by other security measures.

• Provides context information including user identities, threat indicators, descriptions of malicious behavior, and precision ratings of verdicts.

• Uncovers persistent, complex infections that penetrated other defenses to establish command-and-control (C&C) communication channels.

• Proactively detects and blocks malware by analyzing Web traffic metadata, making it harder for the attack to evade the ATD system.

• Fuzzy fingerprinting automatically detects polymorphic variants of known malware.

• Provides a bigger picture of the threat by focusing on the attacker rather than just the exploit or particular malware.

• Rather than just react to attacks, helps you stay ahead of the attacker through the use of machine learning and advanced statistical and predictive modeling.

• Adaptive capabilities that respond to new threats as they emerge.

• No need to manually create and maintain rule sets.
Reports Tab

In the during phase, AMP examines the reputation of select file types traversing your network perimeter. If the file reputation is malicious, AMP blocks the file and reports to Cisco ScanCenter. Information on malware blocked inline by AMP is found in the Malware Analysis section of the Reports tab.

Dashboard Tab

Information on files sandboxed by AMP during the after phase is found in the Dashboard tab and AMP Blocks section. See Dashboard, on page 121.

Threats Tab

Incidents and their general details are listed in the Threats tab.

• CTA incident—CTA analyzes network traffic collected in Web proxy logs to detect anomalies. Behaviors that do not conform to an established standard are possible threats and are reported to Cisco ScanCenter as incidents.

• AMP retrospective incident—in cases where the file reputation is clean or unknown at the time of download, but later the file reputation changes to malicious or is found by file sandboxing to be malicious, AMP reports the file to Cisco ScanCenter as a retrospective incident.

For more information on the Threats tab, see Threats Tab, on page 181.
Threats Tab

- Dashboard, on page 181
- Confirmed Threats, on page 181
- Detected Incidents, on page 183
- Incident Details, on page 185
- Proxy Device Uploads, on page 187

Dashboard

The CTA Dashboard page provides an overview of your network health and what threats are affecting it:

- Health Status. Shows an overall summary of threats discovered in your network by their risk level. Unresolved users are grouped by risk category. Note that a high number of lower risk threats may lead to more serious threats over time.

- Relative Threat Exposure. Threat exposure based on your number of incidents and their risk level, compared to other companies within your same sector, similarly sized companies, and all companies globally.

- Specific Behaviors. High-level breakdown of the detected threats and unresolved behaviors in your network.

- Highest Risk. Unresolved incidents that currently pose the highest risk to your network and require your immediate attention.

- Top Risk Escalations. Unresolved incidents that have recently showed an increase in risk.

Confirmed Threats

The Confirmed page shows information about confirmed threat campaigns in your network.

- Threats spanning across multiple users
- 100% confirmed breaches, no false positives
- Ready for fast remediation, directly actionable
- Cisco Collective Security Intelligence, additional information provided for context
Threat campaigns are listed in the vertical panel at the right of the page.

- At the top of the threat list panel are check boxes for the incident states: Triage, Investigating, Remediating, and Resolved. Use these four check boxes to filter what threats are shown in the vertical panel. For example, uncheck the Resolved box to hide threats containing incidents marked in the Resolved state.

- Threats are sorted top-to-bottom by risk level with the highest-risk threat at the top.

Click a threat to view its information to the left of the vertical panel.

- #Cxxxxx—Incidents detected with correlated behavior are grouped into a threat cluster. Each threat is then labeled with a unique hash-tag group name.
  
  - Risk level—Number from a scale of 1 to 10 representing the risk of the threat impacting your network. A higher number indicates a higher risk. We recommend you prioritize your analysis by investigating higher risk threats and the incidents clustered within them before lower risk threats.
  
  - Confidence—Percentage indicating the precision of the detection category. A higher number indicates a higher confidence that the symptoms are correctly classified and the incident represents a valid threat on your network.
  
  - Incidents Bar—Horizontal, graphical bar showing the number of incidents clustered in the threat.
    - Number of incidents are broken down per incident state, corresponding to the varying shades of the four incident state boxes.
    - For example, in the bar shown here, there are 17 incidents in the Triage state, 12 incidents in the Investigating state, 21 incidents in the Remediating state, and 80 incidents in the Resolved state.

  - Click any cluster number to view a table displaying information on the incidents in that state.

- Affecting—Number of your users affected by this threat within the past 45 days. Also shows number of users affected at other companies to help you determine if the threat is targeted.

- Occurrence—When this behavior occurred, when it was first seen, and when it was last seen.

Below the threat summary are sections showing more details on the selected threat:

- Description of the threat and recommended actions to remediate.

- List of affected users and graph showing number of users exhibiting malicious behaviors over time.

- Example web requests representing threat behavior in your network. If the URL contains an encoded part, the system attempts to show the decoded content here.

- Cisco Cloud Web Security malware blocks observed for users in your network affected by this threat.

- AMP Threat Grid Global Intelligence—Common endpoint content security signatures and behaviors associated with global traffic samples of the threat.
  - Common files appearing in global threat samples that may be present on endpoints, percent chance these files are created or modified by malware on endpoints, and severity of the file type
  - Common endpoint behaviors associated with similar threats seen in samples from AMP Threat Grid
Detected Incidents

The CTA system monitors your web proxy logs but does not inspect the content of the communications. The CTA system focuses on identifying malicious web browsing behaviors and presents incidents derived from the behavioral symptoms of an infection. The Detected page shows an overview of detected incidents which may be suspected threats, including noncorrelated CTA incidents and AMP retrospective incidents. You can also view the correlated CTA incidents that were grouped into verified threats on the Confirmed page.

- **Incident**—Type of dominant behavior detected on an individual, including its Risk and Confidence levels, and whether it's part of a cluster or confirmed threat. Clusters are a collection of incidents that have similar malware symptoms.
  - Risk—Number from a scale of 1 to 10 representing the risk of the incident. A higher number indicates a higher risk. We recommend you prioritize your analysis of incidents by investigating higher risk incidents before lower risk incidents.
  - Confidence—Percentage number indicating the precision of the detection category. A higher number indicates a higher confidence that the symptoms are correctly classified and the incident represents a valid threat on your network. Applies to CTA incidents only.

- **UserIdentity**—UserID and IP address of the affected user.
  - IP addresses can be reassigned to multiple users over time, so the CTA system models by user. This important system enhancement provides more consistent results.
  - A user may be assigned more than one IP address over time. The CTA system tracks these assignments and displays all the IP addresses that have been assigned to the user during the selected time period.

- **IP Reputation**—The rating of the remote server contacted represents an aggregation of known sources the user has communicated with during each incident. The rating is not used in the Anomaly Detection Engine for detection. Instead, the rating is provided to the security analyst as an informational aid to better understand the (global intelligence) context in which the detection of an incident occurred.
  - Red—Number of remote servers contacted with a poor IP reputation rating (–10 to –6).
  - Orange—Number of remote servers contacted with no record in the Global Intelligence database or a neutral rating (–5 to +5).
  - Green—Number of remote servers contacted with a good IP reputation rating (+6 to +10).

- **Duration**—How long and when this behavior occurred. Also refer to First Seen and Last Seen columns.

- **State**—Incident marked as triage, reoccurring, investigating, remediating, resolved, a false positive, or to be ignored.

- **Activity Types**—Types of activity detected in this incident including severity level. Each incident is formed by a number of activities. Each activity represents malware behavioral symptoms. Hover over a cell to show all the activity types associated with that incident. Activity types are sorted top-to-bottom by severity level with the most severe activity at the top.
Filtering Incidents

You can filter which incidents are shown by:

- Date selector—Click each field to open a calendar and choose the start (From) and end (To) dates.
  - By default, the previous 45 days are shown.
  - The maximum date range is 45 days.
  - The available date range is the previous 45 days.
  - You can also quick click 1 day, 3 days, 7 days, 30 days, or 45 days.

- Search field—Enter any username, client IP address, or incident name (no regular expressions or wildcards), and click the Filter button.

- Show—There are check boxes to show AMP and/or CTA incidents, confirmed and/or low confidence incidents, and tabs to show incidents by what state they're in:
  - Triage—(Default) Incidents that are new or reoccurring and need to be investigated.
  - Investigating—Incidents under investigation and being worked on.
  - Remediating—Incidents in the process of being resolved, devices pending cleaning.
  - Resolved
    - Remediated—Incidents that have been remediated, devices have been cleaned.
    - False Positives—Incidents assessed to be false positives.
    - Ignored—Incidents marked to be ignored and not investigated. For example, incidents for devices in a guest Wi-Fi zone.

- All—All incidents regardless of state or marking.

Note: Incidents can be marked by using the drop-down list on the Incident Details page. See Incident Details, on page 185.

Settings

Click the global settings menu icon (sandwich) in the upper-right corner of the page:

- Email Notifications—Enter email addresses to be sent a summary of new and updated incidents every 24 hours.

- CTA STIX/TAXII Service—Use the STIX/TAXII service to pull information on incidents detected by CTA down to your SIEM client for further analysis, incident response, and data archival. See CTA STIX/TAXII Service, on page 197
• **Device Accounts**—Upload telemetry data in log files from one or more source proxy devices to the CTA system for analysis. To access this service, the External Telemetry feature must be enabled and provisioned for your company. If you do not have the External Telemetry feature, contact your Cisco Cloud Web Security account team. See *Proxy Device Uploads, on page 187.*

• **Permanent Filter**—Enter IPv4 addresses for client hosts, networks, or ranges (separated by commas) that you want hidden from the list of incidents.

• **Release Notes**—Summarizes updates, changes, and fixes per release.

In the table header and below the global settings menu button:

- Click the download button to export the incidents (from the current filter displayed) to a CSV file on your device.
- Click the page settings button to select what columns are displayed.
- Click the sorting arrow in any column header to sort the table rows according to the information in that column.
- Resize any column width by dragging the line between the column header cells.
- Reorder table columns by selecting a column (click on its header) and once the pointer changes to crossing arrows, drag and drop the column by its header to a new location in the table.

To further investigate an incident, hover in the row of that incident and the row becomes highlighted. Click in the row to open the incident details page. Alternately, you can open the incident details page in a new window by right-clicking the incident and choosing *Open incident in a new window.*

### Incident Details

An incident typically consists of multiple activities or types of suspicious behavior. There are three main sections on the incident details page.

#### Incident Header

The first main section is the incident header:

- **Incident Classification**—Type of dominant behavior detected, including its Risk and Confidence levels.
  - **Risk**—Number from a scale of 1 to 10 representing the risk of the incident infecting the network. A higher number indicates a higher risk. Therefore, we recommend you prioritize your analysis of incidents by investigating higher risk incidents before lower risk incidents.
  - **Confidence**—Percentage number indicating the precision of the detection category. A higher number indicates a higher confidence that the symptoms are correctly classified and the incident represents a valid threat on the network. Applies to CTA incidents only.

- Use the drop-down list to mark the incident as triage, investigating, remediating, resolved as threat, resolved as false positive, or resolved as ignored. This marking serves two main purposes. One, it categorizes incidents to aid the workflow of incident management and analysis. Two, it becomes part of community feedback that Cisco uses to improve the detection algorithms. Remember to mark the incident after investigation. In the table of listed incidents, the marking is shown in the **State** column.
**Parallel Coordinates**

The second main section is the parallel coordinates graph showing relationships between time, activity, domain, IP address, and autonomous system:

- At-a-glance shows information about the activities in the incident and their associations.
- Hover over each coordinate node in the line graph to show its interconnected information.
- Domains that are targets for persistent connections are highlighted in bold with a PERS indicator.
- Click the drop-down icon next to a domain name for more details.
- IP address includes country location and IP reputation.
- Click the drop-down icon next to an IP address for more details.
- Can be used to filter web flows by selecting and clicking one or more nodes. The associated web flows are then listed in the table below the graph.

**Web Flow Requests**

The third main section is a table listing details of the web flow requests:

- **Client IP**—IP address used on client.
- **Client Port**—TCP/UDP port used on client.
- **Server IP**—IP address used on server. Includes country flag of server location, if known, and the IP reputation score of the server. A red box next to the server indicates a negative IP reputation for that server. Domain names are included. The negative IP reputation could indicate suspicious communication from a domain operated by an attacker.
- **Server Port**—TCP/UDP port used on server.
- **Bytes Up**—Amount of data sent to server.
- **Bytes Down**—Amount of data received from server.
- **Header Content Type**—Content type in the HTTP header sent by the remote server.
- **Body Content Type**—Content type detected in the response body. Can differ from Header Content Type in cases where, for example, the malicious host tries to get through proxy or firewall filtering rules.
- **URL**—Unified Resource Locator of the server accessed by the client. Hover over the URL, and if the URL contains an encoded part, the system attempts to show the decoded content here. Often reveals commands and data passed through.
- **Referrer**—HTTP header field identifying the address of the URL that linked to the resource being requested.
- **HTTP Status**—HTTP status code returned from the server. A red box with an "x" next to the status code indicates that the flow was blocked by the Web proxy.
- **Timestamp**—Time connection started.
- **Duration**—How long the event lasted.
- **User Agent**—Type of browser used during activity.
- **Category**—Site category (for example, gambling and social sites).
- **Filename**—Name of file that was downloaded (AMP-specific field).
- **SHA-256**—Secure Hash Algorithm SHA-256 computed for the file (AMP-specific field). If a sandbox report of the file is available, an icon appears next to the SHA-256. Hover over the icon and click View full report to open the sandbox report in a new window. A red skull-and-crossbones icon indicates that the file was found to be malicious. See Sandboxing, on page 191.

In the Search field, enter any client IP address, server IP address, URL, or SHA value (no regular expressions or wildcards), and click the Filter button.

Click the page settings button to select what columns are displayed. Click the sorting arrow in any column header to sort the table rows according to the information in that column. Reorder the columns by clicking and dragging by their headers.

At the bottom of the page below the table is a single row footer showing summary statistics for the selected web flows: traffic amount, percentage blocked, number of requests, total duration, user agents, no referrer percentage, and HTTP status code.

### Proxy Device Uploads

Upload telemetry data in log files from proxy devices such as the Cisco Web Security Appliance (WSA) and Blue Coat ProxySG to the CTA system for analysis.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Click the <strong>Threats</strong> tab.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click the global settings menu icon in the upper-right corner of the page, and select <strong>Device Accounts</strong> to open the setup wizard.</td>
</tr>
</tbody>
</table>

**Note**  
If there's already at least one existing device account, the setup is skipped and the Device Accounts page is displayed.
Step 3: When you're ready to start the setup wizard to add a device account, click Let's Get Started.

Step 4: Choose how the telemetry data is uploaded from the device by selecting either automatic or manual upload from the dropdown. The CTA system supports only one upload method at a time; they cannot be combined.

Note: To switch from automatic to manual uploading, all proxy devices must first be removed from the automatic uploading configuration.

Step 5: If you selected the automatic upload method, choose what protocol is used to transfer the log files by selecting either SCP or HTTPS.

a) Enter a name for this device, and click Add Account.
b) If you selected SCP:
   • Copy the information (host, port, directory, username) to paste into your Cisco WSA configuration. For security reasons, the information is displayed only once.
   • For details on how to configure your Cisco WSA, see its Configuration Guide.
   • Once the Cisco WSA Management Console returns a public SSH key, copy and paste the public SSH key into the device account.
   • Click Finish.
   • Optionally, you can enter the public SSH key later by navigating to the Device Accounts page and clicking the device.

c) If you selected HTTPS:
   • Copy the information (host, port, path, username, password) to paste into your Blue Coat ProxySG configuration.
   • For details on how to configure your Blue Coat ProxySG, see its Configuration Guide.
   • Click Finish.

Step 6: If you selected the manual upload method:

a) Validate the format of your log file(s). Follow these preparation guidelines:
   • W3C log files created by Cisco WSA and Blue Coat proxies are supported.
   • All log files must be compressed in GZip (*.gz) format.
   • Each log file must be smaller than 1 GB. A log file bigger than 1 GB should be divided into multiple, smaller files. Ensure separate time intervals do not overlap and every file contains the same correct header.
   • Total time interval covered by the log files should be greater than two days.
   • Each log file must be for a specific, non-overlapping time interval.
   • Each log file must contain log entries in ascending time order; older entries before newer entries.
   • Log files should be sorted alphabetically/numerically and uploaded in order according to time; older files should be uploaded before newer files. Within a single upload, the uploading component automatically sorts the files. If you upload multiple times, ensure you always upload newer data than before. If the naming convention used by default in the proxy log files is retained, the file names are already correctly sorted.
• Data older than previously uploaded data will not be processed.
• The content of the log files must match certain criteria to be valid for uploading.
  • We offer you a Log Validation Tool to check your log files before uploading.
  • Copy-and-paste the beginning 20 lines of your log file into the Log Validation Tool to check for errors.
  • Any errors are displayed, and while you correct them, the tool will automatically continue to check for errors.

b) Click either Add files to select log files to be uploaded or drag-and-drop log files into the upload box.

Note Click Clear files to clear all files added to the upload box.

c) Clicking Start upload uploads the selected log files to the CTA system for analysis. Allow the CTA system some time before seeing results.

Note To minimize the risk of dropping data, the CTA system starts processing the uploaded data after 5 hours. This gives you time to complete all your uploads and ensure everything is in place and in proper order before processing starts.

Caution Trying to switch from manual to automatic immediately aborts all uploading and stops processing of uploaded data. All uploaded data is discarded.

Note Closing or navigating away from the page will stop any current file upload.

Note You cannot use automatic uploading unless you first stop all manual uploading. If the switch is made before all the data is processed, some analysis data may be lost from the transition. To ensure the system does not drop any data, perform the switch after 24 hours after the last manual upload.

What to do next

The Device Accounts page lists the proxy devices along with their information. The Status column shows the status of each device:

• New—Incomplete configuration for SCP, may be missing public SSH key
• Provisioning—Account in the process of being provisioned, not yet ready
• Ready—Account successfully created
• Error—Hover cursor over status to display a popup message explaining the error

From this overview page, you can add more device accounts, or click any device to remove it, enter a public SSH key, or troubleshoot.

Although it is possible to share an account between multiple devices or upload processes, we recommend you use a separate account for each device to minimize the possibility of filename conflicts and simplify troubleshooting upload problems.
When your device account is ready, click to view the **Confirmed** or **Detected** pages for insight into any suspicious activities in your network. For more information, see Threats Tab, on page 181.

---

**Note**  
Data is typically available within two to three days after provisioning is complete.
Sandboxing

The Sandbox Report shows the results of the file analysis in the Talos virtual sandboxing environment. Cumulative analysis and information about the files collected from the greater community are also shared through the report.

- Overview, on page 191
- Startup, on page 191
- Dropped, on page 191
- Domains/IPs, on page 192
- Static, on page 192
- Network, on page 192
- Behavior, on page 192

Overview

The General Information section contains information about the sandbox instance that executed the analyzed file.

The Signature Overview section contains behaviors that were observed in the analyzed binary. The behaviors are stack-ranked and color-coded. Each section also displays a color-coded rating scale to represent the maliciousness. At the left end of the rating scale, green indicates benign. On the right end, red indicates malicious. These ratings can be used at-a-glance to determine if the analyzed file is relatively benign, suspicious, or malicious. Use this high-level information to assign degrees of urgency which help you decide the order in which incidents are investigated.

Startup

The Startup section contains a list of files that execute during startup, while the cleanup section contains a list of files that execute during shutdown.

Dropped

The Created/Dropped Files section contains a list of files that were created by the sample under analysis and dropped in the sandbox while the file was being analyzed.
Domains/IPs

The Contacted Domains and Contacted IPs list domains and IP addresses that were involved during analysis.

Static

The Static File Information section contains information about the file that was uploaded, prior to execution in the virtual sandboxing environment. This information is collected by parsing the file on disk and can be used to search other threat intelligence sources for additional details.

The Static PE information section describes the portable executable file and can be used to get a quick understanding of the properties of the application. For example:

• The **Entrypoint** field in the General section can be used to determine if the file is packed.

• The **Resources**, Imports, and Exports can sometimes give you a general understanding of what the executable does. However, note that this information can be obfuscated if the file is packed, leaving only the Resources, Imports, and Exports of the packer exposed until the file is unpacked or executed.

• The **Version Info** and Possible Origin can sometimes be used to tell when the file was compiled and on what language version of operating system the file was compiled. This can give you hints about the origin of the attack. However, note that this information can be obfuscated or spoofed.

Network

The Network Behavior section contains a summary of all of the interesting network traffic that was generated while analyzing the file.

TCP Packets and UDP Packets list all of the TCP/UDP traffic observed while analyzing the file. The IP address and port information can be used to create rudimentary rules on a firewall to restrict ingress/egress activity to certain IP addresses and ports that are known to be associated with malicious code.

DNS Queries lists all of the DNS transactions that were observed while analyzing the file. The query information can be used to detect hosts that are infected on your network, or as a guideline on what domain names need to be blocked in order to control an infection on your network.

HTTP subsections contain HTTP traffic that was observed while analyzing the file. The HTTP information can be used to write network IDS signatures or to block communication with these hosts at the network perimeter.

Behavior

The System Behavior section lists the activities observed while analyzing the file. You can also show or hide the windows behavior details.
Investigating Incidents

Overview

Respond to an incident based on its confidence and risk levels:

- **High risk and high confidence.** The endpoint is likely compromised with an advanced threat that has already circumvented signature or rule-based endpoint security. It is unlikely you will be able to remove the threat with endpoint cleaning tools. Reimage or rebuild the endpoint without backing up the user profile completely; backup documents only. When CTA detects an active malware infection, this usually requires manual action from your SOC and Desktop teams.

- **Medium confidence or medium risk.** The endpoint likely contains malware that can be cleaned with endpoint cleaning tools. Run endpoint scanning and antivirus cleaning tools of your choice. Clean any infections found and monitor the endpoint. If the problem persists, perform a reimage and rebuild of the endpoint without backing up the user profile completely; backup documents only.

- **Everything else (low confidence and low risk).** The endpoint may or may not be infected. The alert might be linked with the user following spam or phishing URLs. Perform a normal scan and remove any infections found. If nothing is found, monitor the endpoint for any escalations to prevent malware progress.

Confidence levels:

- High (100% to 95%)
- Medium (94% to 85%)
- Low (84% to 0%)

Risk levels:

- Critical (10)
- High (9, 8)
- Medium (7, 6)
- Low (5, 4, 3, 2, 1)
Details

Procedure

Step 1
Information on malware blocked inline by AMP is found in the Malware Analysis section of the Reports tab.

Step 2
Information on files sandboxed by AMP during the after phase is found in the CWS Dashboard tab and AMP Blocks section. See Dashboard, on page 121.

Step 3
Click the Threats tab and CTA Dashboard.

a) Health status. Shows an overall summary of threats discovered in your network by their risk level. Unresolved users are grouped by risk category. Note that a high number of lower risk threats may lead to more serious threats over time.

b) Relative threat exposure. Threat exposure based on your number of incidents and their risk level, compared to other companies within your same sector, similarly sized companies, and all companies globally.

c) Specific behaviors. High-level breakdown of the detected threats and unresolved behaviors in your network.

d) Highest risk. Unresolved incidents that currently pose the highest risk to your network and require your immediate attention.

e) Top risk escalations. Unresolved incidents that have recently showed an increase in risk.

Step 4
Click the Threats tab and Confirmed.

a) This section shows confirmed threats and breaches on your network (incidents with a 100% confidence level) and their associated information.

b) Incidents detected with correlated behavior are grouped into a threat campaign, and each threat campaign is then labeled with a unique hash-tag group name.

c) Threat campaigns are listed in the vertical panel at the right of the page. You can check the state boxes to filter what threat campaigns are shown in the panel.

d) A higher risk number indicates a higher risk of the threat impacting your network. Prioritize your analysis by investigating higher risk threats including the incidents clustered within them.

e) These incidents to not require much time for investigation; they require immediate action. Set up recovery processes to adjust your workflow for CTA findings.

f) Review the threat-specific description and the recommended action for a more targeted remediation.

Step 5
Click the Threats tab and Detected.

a) This section shows an overview of detected incidents, including noncorrelated CTA incidents and AMP retrospective incidents. You can also view the correlated CTA incidents that were grouped into threats in the Confirmed section.

b) You can filter which incidents are shown by choosing AMP and/or CTA and adjusting the date selector, search field, preferences, and state.

c) Use the Email Notifications page to enter email addresses to be sent a summary of new and updated incidents every 24 hours.

Step 6
To start investigating an incident, click that incident to review its details. Investigate incidents with higher risk and confidence first. An incident typically consists of multiple activities or types of suspicious behavior.

Step 7
Identify the affected device or server.

Step 8
The SHA-256 hash of any malicious files found is also listed here. Hover over the red skull-and-crossbones icon and click View full report to open the sandbox report in a new window. See Sandboxing, on page 191.
**Step 9**

Inspect the parallel coordinates graph which at-a-glance shows information about the activities in the incident. Hover over each coordinate node in the line graph to show its interconnected information.

a) Start with the highest severity and work your way down.

b) Note the information in the Time column. Verify how long the malware activity has been reported. One of the characteristics of advanced malware activity is that the communication is persistent for a long time. If the incident has been reported for several days or weeks, it increases the chance that it was produced by advanced malware.

c) Identify any recent ongoing activity. Focus on any activities that have occurred within the past 48 hours.

d) Look for activities that occur in parallel and may suggest a C&C communication channel in use.

e) Review the connected lines. Do the domains make sense together? Are they related? A domain with changing IP addresses is suspicious. Correlate it with the web flows table to determine if the domain was transferring data.

f) Are activities tied to the same AS or different systems from different owners and different locations? May be an indicator of systems that have been hacked and used as attack sources.

**Step 10**

The graph can be used to filter web flows. Select and click one or more nodes to show the associated web flows.

a) Note the box next to the server. A red box indicates a negative IP reputation for that server. Domain names are included. The negative IP reputation could indicate suspicious communication from a domain operated by an attacker.

b) Note the HTTP status code returned from the server. A red box with an "x" next to the status code indicates that the flow was blocked by the web proxy. Focus on any incidents that have at least one command-and-control (C&C) channel which is not being blocked and thereby allowing the malware to operate.

c) If a sandbox report of the file is available, an icon appears next to the SHA-256. Hover over the icon and click View full report to open the sandbox report in a new window. A red skull-and-crossbones icon indicates that the file was found to be malicious. See Sandboxing, on page 191.

**Step 11**

Detected incidents have less than a 100% confidence level. Based on the details of the actual incident, the following factors may lower or raise the reported risk:

<table>
<thead>
<tr>
<th>Lowers Risk</th>
<th>Raises Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reported activities are already blocked by the proxy.</td>
<td>Reported activities are not already blocked by the proxy.</td>
</tr>
<tr>
<td>The incident characteristics (for ex. visited URLs) are distinct for one</td>
<td>The incident characteristics (for ex. visited URLs) repeat for many users.</td>
</tr>
<tr>
<td>incident only.</td>
<td></td>
</tr>
<tr>
<td>The total mass of the incident is one activity with a few requests.</td>
<td>The incident detail shows long-term, heavy, and persistent behavior.</td>
</tr>
<tr>
<td>Incident detail displays a low amount of data transfer.</td>
<td>Incident detail displays a high amount of data transfer, especially uploads.</td>
</tr>
</tbody>
</table>

**What to do next**

Analyze the information you gathered to conclude if this incident is a threat to your network. In the incident details page, mark the incident as resolved as threat, resolved as false positive, or resolved as ignored.
Follow your organization's standard incident response procedure to mitigate the threat. Collecting more threat intelligence from internal systems is a good practice before you perform any action. Keep in mind that you are operating in the after-breach phase of the attack continuum. This means that traditional security measures in the during phase may not have been successful in completely removing the threat and you may need to reimage the affected endpoint.

---

**Note**

To reduce the number of false positives, not all incidents are immediately blocked up front. Anomalies are detected and reported as incidents for investigation. After some analysis, monitoring, and tracking time, threats are confirmed to be blocked. However, threats like morphing malware may modify its behavior to avoid detection. Therefore, CTA persistently analyzes files over time and sends information to SenderBase to update the Web-Based Reputation Score (WBRS). Cisco Cloud Web Security may then block the threat, but this should not be considered the final, all-encompassing solution. Sometimes what Cisco Cloud Web Security blocks may be only part of the communication. For example, some malware may stash data and exfiltrate it later when you connect from a location not protected by Cisco Cloud Web Security. To be thorough, reimage the infected device.

---
CHAPTER 35

CTA STIX/TAXII Service

Overview, on page 197
• Poll Service, on page 198
• Common Queries, on page 206
• CTA Integration with Cisco ISE, on page 207

Overview

Cisco ScanCenter allows you to pull information on incidents detected by CTA down to your client for further correlation analysis and archival. The service supports MITRE's Trusted Automated eXchange of Indicator Information (TAXII) standard for integration with your Security Information and Event Management (SIEM) system. The TAXII standard specifies transport mechanisms used to share cyber threat information between systems.

For more information on TAXII, see:
https://taxii.mitre.org/
http://taxiiproject.github.io/

The information in each incident is represented using the Structured Threat Information eXpression (STIX) language format. STIX is a structured language used to describe cyber threat information so it can be shared, stored, and analyzed in a consistent manner. The STIX format allows CTA to represent its breach detection findings in a hierarchical format. The TAXII service uses a subset of the STIX language to describe the incidents CTA has detected. Currently, the supported objects include:

• Campaign—Confirmed threat category, if available
• Incident—Anomalous activity
• TTP—Tactics, Techniques, and Procedures
• Observable—Web requests
• Indicator—Pattern identifying observable conditions

For more information on STIX, see:
https://stix.mitre.org/
Poll Service

The poll service uses standardized TAXII transport mechanisms to send incident information from CTA to clients that support the TAXII standard. To pull incident information, the TAXII client sends a poll request to the TAXII poll service. HTTP basic authentication is used to restrict access for authorized users only. The TAXII poll service then responds by sending incident information from CTA to the TAXII client. HTTPS protocol is used to secure all data transfers.

Your SIEM or other security work-flow system must natively support STIX/TAXII. Configure your third-party TAXII client to periodically poll the TAXII poll service.

- To obtain your account information, log into Cisco ScanCenter and request CTA STIX/TAXII service.
  - Click the Threats tab.
  - Click the global settings icon in the upper-right corner.
  - Click CTA STIX/TAXII API.
  - Click the Add account button.
  - Enter a name to identify your account, and then click the Add account button.

- After the provisioning process is completed, your account information is displayed. Copy this account information to a secure location before closing the window.

  **Note**
  For security reasons, the secret password is displayed only once. If you lose the secret password, you must revoke the existing secret password and generate a new secret password.

  - Copy your unique attributes into your third-party TAXII client:
    - pollEndpoint or feed service URL = https://taxii.cloudsec.sco.cisco.com/skym-taxii-ws/PollService
    - username
    - password
    - collection name or feed name

  **Note**
  In August 2018, Cognitive Intelligence (formerly Cognitive Threat Analytics or CTA) started its migration to a new location in Amazon Web Services, which resulted in new IP addresses and an additional URL to access and use the service. To maintain access to the service, it may be necessary to update your outbound firewall rules. After the switchover in November 2018, you will no longer be able to successfully send data to the old data ingest service IP address. Specific details on the required changes and other important information can be found in the Field Notice.
We do not provide technical support for configuring third-party products or SIEM devices. In the event of an issue, consult the vendor-specific support team.

Alternatively, you may download and use an example TAXII client from Cisco. If your SIEM or other security system does not natively support STIX/TAXII, Cisco provides a lightweight Java TAXII Log Adapter that you can deploy to a Linux or Windows VM environment next to your SIEM. Click the link provided to view setup instructions. The adapter uses the TAXII API to perform regular polling of any new intelligence and delivers data in STIX messages. The STIX messages are then transformed by the adapter into other formats accepted by common SIEM systems.

To support the stability, performance, and availability of the poll service:

- Only one poll request from any single TAXII client is allowed within every 10 minutes. Otherwise, a status message indicating this error is returned.
- Each poll request may retrieve incident information spanning up to three days.
- Incident information is stored for retrieval for up to 30 days.

**Poll Request**

The following is an example of a poll request from your TAXII client to the TAXII poll service.

Method is POST.

HTTP Request headers:

```
x-taxii-content-type: urn:taxii.mitre.org:message:xml:1.1
x-taxii-protocol: urn:taxii.mitre.org:protocol:http:1.1
x-taxii-services: urn:taxii.mitre.org:services:1.1
x-taxii-accept: urn:taxii.mitre.org:message:xml:1.1
content-type: application/xml
accept: application/xml
authorization: Basic ...
```

Request body:

```
<taxii_11:Poll_Request xmlns:taxii_11="http://taxii.mitre.org/messages/taxii_xml_binding-1.1"
   message_id=" " collection_name=" ">
  <taxii_11:Exclusive_Begin_Timestamp>2015-01-16T00:00:00+00:00</taxii_11:Exclusive_Begin_Timestamp>
  <taxii_11:Inclusive_End_Timestamp>2015-01-17T00:00:00+00:00</taxii_11:Inclusive_End_Timestamp>
  <taxii_11:Poll_Parameters allow_asynch="false"/>
  <taxii_11:Response_Type>FULL</taxii_11:Response_Type>
</taxii_11:Poll_Request>
```

**Supported Request Parameters**

<table>
<thead>
<tr>
<th>Poll_Request</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported Request Parameters</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>message_id</td>
<td>A randomly generated string for each request, according to the TAXII specification. Regenerate a unique string for every request.</td>
</tr>
<tr>
<td>collection_name</td>
<td>Name of collection to extract or pull from the CTA service. This attribute will be provided to you by Cisco after the provisioning process is completed.</td>
</tr>
<tr>
<td>Exclusive_Begin_Timestamp</td>
<td>Adjust this value according to your timeframe.</td>
</tr>
<tr>
<td>Inclusive_End_Timestamp</td>
<td>Adjust this value according to your timeframe.</td>
</tr>
<tr>
<td>Poll_Parameters</td>
<td></td>
</tr>
<tr>
<td>allow_asynch</td>
<td>Always set this attribute to false.</td>
</tr>
</tbody>
</table>

The maximum supported difference between **Exclusive_Begin_Timestamp** and **Inclusive_End_Timestamp** is three days. In case the difference is more, the returned result is limited to the last three days before **Inclusive_End_Timestamp**.

### Poll Response

The following is an example of a poll response from the TAXII poll service to the TAXII client.

HTTP Response headers:

```plaintext
x-taxii-content-type: urn:taxii.mitre.org:message:xml:1.1
x-taxii-protocol: urn:taxii.mitre.org:protocol:http:1.1
x-taxii-services: urn:taxii.mitre.org:services:1.1
```

Response body:

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<t:Poll_Response xmlns:t="http://taxii.mitre.org/messages/taxii_xml_binding-1.1"
xmlns:c="http://cybox.mitre.org/cybox-2"
xmlns:cc="http://cybox.mitre.org/common-2"
xmlns:co="http://cybox.mitre.org/objects#CustomObject-1"
xmlns:coa="http://stix.mitre.org/CourseOfAction-1"
xmlns:sc="http://stix.mitre.org/common-1"
xmlns:ind="http://stix.mitre.org/Indicator-2"
xmlns:ttp="http://stix.mitre.org/TTP-1"
xmlns:inc="http://stix.mitre.org/Incident-1"
xmlns:s="http://stix.mitre.org/stix-1"
collection_name=" " more="true"
result_id="" result_part_number="1"
in_response_to="generatedMessageID" message_id="responseMessageID">
<t:Exclusive_Begin_Timestamp>2015-01-17T15:11:00.648Z</t:Exclusive_Begin_Timestamp>
<t:Inclusive_End_Timestamp>2015-01-20T15:11:00.649Z</t:Inclusive_End_Timestamp>
<t:Content_Block>
<t:Content_Binding binding_id="STIX.XML_1.1"/>
<t:Content>
Id="cta:package-1412045744-66911c07-c9b8-4389-8888-00e438f58c2e"
```
timestamp="2015-01-20T15:11:02.766Z" version="1.1.1">
<s:STIX_Header>
<s:Package_Intent>Incident</s:Package_Intent>
<s:Information_Source>
<sc:Identity id="cta:customer-1234567890"/>
<sc:Tools>
<cc:Tool id="cta:tool-cta">
<cc:Name>Cognitive Threat Analytics</cc:Name>
<cc:Vendor>Cisco</cc:Vendor>
</cc:Tool>
<cc:Tool id="cta:tool-amp">
<cc:Name>Advanced Malware Protection</cc:Name>
<cc:Vendor>Cisco</cc:Vendor>
</cc:Tool>
</sc:Tools>
</s:Information_Source>
</s:STIX_Header>
</s:Incidents>
</s:STIX_Header>

<s:Incident xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:type="inc:IncidentType"
  id="cta:incident-1412045744_f8bae03fb2ff7d6185907ae3240d_ITMAL1">
  <inc:Title>malware|using automatically generated domain (DGA)</inc:Title>
  <inc:Victim>
    <sc:Name>JohnDoe</sc:Name>
  </inc:Victim>
  <inc:Related_Indicators>
    <inc:Related_Indicator>
      <sc:Indicator id="cta:indicator-1412045744_1421623800000_f8bae03fb2ff7d6185907ae3240d_0">
        <ind:Observable>
          <c:Observable_Composition operator="AND">
            <c:Observable>
              <c:Object>
                <c:Properties xsi:type="co:CustomObjectType">
                  <cc:Custom_Properties>
                    <cc:Property name="timestamp">1421623882432</cc:Property>
                    <cc:Property name="xElapsedTime">1810</cc:Property>
                    <cc:Property name="scHttpStatus">0</cc:Property>
                    <cc:Property name="csContentBytes">622</cc:Property>
                    <cc:Property name="scContentBytes">907</cc:Property>
                    <cc:Property name="csUrl"></cc:Property>
                    <cc:Property name="sIP">195.22.26.231</cc:Property>
                    <cc:Property name="cIP">33.196.39.11</cc:Property>
                    <cc:Property name="cUsername">JohnDoe</cc:Property>
                    <cc:Property name="sReputation">-580</cc:Property>
                    <cc:Property name="sCategory">unclassified</cc:Property>
                  </cc:Custom_Properties>
                </c:Properties>
              </c:Object>
            </c:Observable>
            <c:Observable>
              <c:Object>
                <c:Properties xsi:type="co:CustomObjectType">
                  <cc:Custom_Properties>
                    <cc:Property name="timestamp">1421623896635</cc:Property>
                    <cc:Property name="xElapsedTime">1942</cc:Property>
                    <cc:Property name="scHttpStatus">0</cc:Property>
                    <cc:Property name="csContentBytes">361</cc:Property>
                    <cc:Property name="scContentBytes">582</cc:Property>
                    <cc:Property name="csUrl"></cc:Property>
                    <cc:Property name="sIP">195.22.26.231</cc:Property>
                    <cc:Property name="cIP">33.196.39.11</cc:Property>
                    <cc:Property name="cUsername">JohnDoe</cc:Property>
                    <cc:Property name="sReputation">-580</cc:Property>
                    <cc:Property name="sCategory">unclassified</cc:Property>
                  </cc:Custom_Properties>
                </c:Properties>
              </c:Object>
            </c:Observable>
          </c:Observable_Composition>
        </ind:Observable>
      </sc:Indicator>
    </inc:Related_Indicator>
  </inc:Related_Indicators>
</s:Incident>
<cc:Property name="sReputation">-580</cc:Property>
<cc:Property name="sCategory">unclassified</cc:Property>
</c:Custom_Properties>
</c:Properties>
</c:Object>
</c:Observable_Composition>
</ind:Observable>
</ind:Observable_Composition>
</sc:TTP>
</ind:Indicated_TTP>
</sc:Indicator>
</inc:Related_Indicator>
</inc:Related_Indicators>
<inc:Discovery_Method>Log Review</inc:Discovery_Method>
<inc:COA_Requested>
<inc:Course_Of_Action xsi:type="coa:CourseOfActionType">
<coa:Stage>Remedy</coa:Stage>
<coa:Type>Eradication</coa:Type>
<coa:Parameter_Observables cybox_major_version="2" cybox_minor_version="1">
<coa:Parameter_Observable Package_Shape="proxy">
<cc:Time>
<cc:Produced_Time>2016-08-15T17:02:02.616Z</cc:Produced_Time>
</cc:Time>
</coa:Parameter_Observable>
</coa:Parameter_Observables>
</inc:Course_Of_Action>
</inc:COA_Requested>
<inc:Confidence>
<sc:Value>Low</sc:Value>
</inc:Confidence>
<inc:Information_Source>
<sc:Tools>
<cc:Tool idref="cta:tool-cta"/>
</sc:Tools>
</inc:Information_Source>
</s:Incident>
</s:Incidents>
</s:STIX_Package>
</t:Content>
</t:Content_Block>
</t:Poll_Response>
In **Poll_Response**, if there are no more threat items, the two attributes of `more` and `result_id` are not present. When `more=true` is present, you can request the next pages of the response by using a **Poll_Fulfillment**.

### Supported Response Objects

<table>
<thead>
<tr>
<th>Supported Response Objects</th>
<th>Description of Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poll_Response</td>
<td></td>
</tr>
<tr>
<td>collection_name</td>
<td>Name of collection to extract or pull from the CTA service. This attribute will be provided to you by Cisco after the provisioning process is completed.</td>
</tr>
<tr>
<td>result_id</td>
<td>Copy this value to the poll fulfillment request.</td>
</tr>
<tr>
<td>Exclusive_Begin_Timestamp</td>
<td>Exclusive beginning of the time range covered by this poll response. Absence of this field indicates that the poll response covers the earliest time for this TAXII data feed.</td>
</tr>
<tr>
<td>Inclusive_End_Timestamp</td>
<td>Inclusive end of the time range covered by this poll response.</td>
</tr>
<tr>
<td>Content_Block</td>
<td>Returned content.</td>
</tr>
<tr>
<td>Content_Binding</td>
<td></td>
</tr>
<tr>
<td>Content</td>
<td></td>
</tr>
<tr>
<td>STIX_Package</td>
<td>Information about the STIX language.</td>
</tr>
<tr>
<td>STIX_Header</td>
<td>Information about this package of STIX content.</td>
</tr>
<tr>
<td>Incidents</td>
<td>One or more incidents.</td>
</tr>
<tr>
<td>Incident</td>
<td>Information about a single incident.</td>
</tr>
<tr>
<td>Title</td>
<td>Title describing this incident.</td>
</tr>
<tr>
<td>Victim</td>
<td>Information about the victim of this incident.</td>
</tr>
<tr>
<td>Related_Indicators</td>
<td>Identifies indicators related to this incident.</td>
</tr>
<tr>
<td>Related_Indicator</td>
<td>Identifies a single indicator related to this incident.</td>
</tr>
<tr>
<td>Indicator</td>
<td>Indicator made up of a pattern that identifies certain observable conditions as well as contextual information about the pattern's meaning, how and when it should be acted upon, etc.</td>
</tr>
<tr>
<td>Observable</td>
<td>Relevant observable for this indicator.</td>
</tr>
<tr>
<td>Observable_Composition</td>
<td>Enables specifying higher-order composite observables by composing logical combinations of other observables.</td>
</tr>
<tr>
<td>Supported Response Objects</td>
<td>Description of Field</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Observable</td>
<td>Represents a single observable.</td>
</tr>
<tr>
<td>Object</td>
<td>Identifying characteristics of a specific object (e.g. file, registry key, process)</td>
</tr>
<tr>
<td>Properties</td>
<td>Properties that were enumerated as a result of the action on the object.</td>
</tr>
<tr>
<td>Custom_Properties</td>
<td>Enables specifying a set of custom object properties that may not be defined in existing Properties schemas.</td>
</tr>
<tr>
<td>Property</td>
<td>A single property that was enumerated as a result of the action on the object.</td>
</tr>
<tr>
<td>Indicated_TTP</td>
<td>Specifies the relevant Tactics, Techniques, and Procedures (TTP) indicated by this indicator.</td>
</tr>
<tr>
<td>Discovery_Method</td>
<td>Information about the method and/or tool used to discover the code.</td>
</tr>
<tr>
<td>COA_Request</td>
<td>Recommended course of actions for this incident.</td>
</tr>
<tr>
<td>Confidence</td>
<td>Information about the level of confidence held in the characterization of this incident.</td>
</tr>
<tr>
<td>Information_Source</td>
<td>Information about the source of this incident.</td>
</tr>
<tr>
<td>Tools</td>
<td>Information about the source of this incident.</td>
</tr>
<tr>
<td>Tool</td>
<td>Which tool, CTA or AMP, detected this incident.</td>
</tr>
</tbody>
</table>

In case of an error, an error message is returned. For example:

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<t:Status_Message
    xmlns:t="http://taxii.mitre.org/messages/taxii_xml_binding-1"
    xmlns:c="http://cybox.mitre.org/cybox-2"
    xmlns:cc="http://cybox.mitre.org/common-2"
    xmlns:co="http://cybox.mitre.org/objects#CustomObject-1"
    xmlns:sc="http://stix.mitre.org/common-1"
    xmlns:ind="http://stix.mitre.org/Indicator-2"
    xmlns:ttp="http://stix.mitre.org/TTP-1"
    xmlns:inc="http://stix.mitre.org/Incident-1"
    xmlns:s="http://stix.mitre.org/stix-1"
    status_type="FAILURE" in_response_to="23537"
    message_id="16ed0b75-2af6-4537-b71c-da00e0a0c419">  
  <t:Message>An error occurred during request processing.</t:Message>
</t:Status_Message>  
```

<table>
<thead>
<tr>
<th>TAXII status_type</th>
<th>Description of Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>User is not authenticated, HTTP response status code of 404</td>
<td></td>
</tr>
<tr>
<td>User is not authorized, HTTP response status code of 401</td>
<td></td>
</tr>
</tbody>
</table>
### Poll Fulfillment

The following is an example of a poll fulfillment request from your TAXII client to the TAXII poll service.

**Method is POST.**

**HTTP Request headers:**

```plaintext
x-taxii-content-type: urn:taxii.mitre.org:message:xml:1.1
x-taxii-protocol: urn:taxii.mitre.org:protocol:http:1.1
x-taxii-services: urn:taxii.mitre.org:services:1.1
x-taxii-accept: urn:taxii.mitre.org:message:xml:1.1
content-type: application/xml
accept: application/xml
authorization: Basic ...
```

**Request body:**

```xml
<taxii_11:Poll_Request
xmlns:taxii_11="http://taxii.mitre.org/messages/taxii_xml_binding-1.1"
message_id="" collection_name=""
result_id="" result_part_number="2" />

<taxii_11:Exclusive_Begin_Timestamp>2015-01-16T00:00:00+00:00</taxii_11:Exclusive_Begin_Timestamp>

<taxii_11:Inclusive_End_Timestamp>2015-01-17T00:00:00+00:00</taxii_11:Inclusive_End_Timestamp>

<taxii_11:Poll_Parameters allow_asynch="false"/>
<taxii_11:Response_Type>FULL</taxii_11:Response_Type>
</taxii_11:Poll_Parameters>
</taxii_11:Poll_Request>
```

---

**Supported Request Parameters**

<table>
<thead>
<tr>
<th>Poll_Request</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>message_id</td>
<td>A randomly generated string for each request, according to the TAXII specification. Regenerate a unique string for every request.</td>
</tr>
<tr>
<td>collection_name</td>
<td>Name of collection to extract or pull from the CTA service. This attribute will be provided to you by Cisco after the provisioning process is completed.</td>
</tr>
<tr>
<td>result_id</td>
<td>Paste this value from the poll response.</td>
</tr>
<tr>
<td>result_part_number</td>
<td>Increment this value by 1 from the value in the poll response.</td>
</tr>
<tr>
<td>Exclusive_Begin_Timestamp</td>
<td>Adjust this value according to your timeframe.</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>TAXII status_type</th>
<th>Description of Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>BAD_MESSAGE</td>
<td>Invalid request message, refer to Message parameter</td>
</tr>
<tr>
<td>FAILURE</td>
<td>Unspecified error, refer to Message parameter</td>
</tr>
</tbody>
</table>
### Supported Request Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inclusive_End_Timestamp</td>
<td>Adjust this value according to your timeframe.</td>
</tr>
<tr>
<td>Poll_Parameters</td>
<td>Always set this attribute to false.</td>
</tr>
<tr>
<td>allow_asynch</td>
<td></td>
</tr>
</tbody>
</table>

Note: The maximum supported difference between `Exclusive_Begin_Timestamp` and `Inclusive_End_Timestamp` is three days. In case the difference is more, the returned result is limited to the last three days before `Inclusive_End_Timestamp`.

### Common Queries

This section describes some common queries used in the Cisco STIX/TAXII API to help prioritize findings for further investigation. The syntax used in the example queries is based on SPLUNK integration and is symbolic. The particular fields and values may differ depending on your local integration, but the meaning of the queries is broadly applicable across SIEM systems and integrations.

Tip: If you are collecting other data in SPLUNK, prepend your query with host, index, or source name to search through only CTA data.

### Users Affected by Confirmed Threats

This query returns all users with confirmed threats and may be reported to your Incident Response Team for desktop remediation. If these incidents are also high risk, consider reimaging the affected device. This query generates a table with usernames and campaign names by which they are affected. Search for nonempty campaign name and then deduplicate username+campaign pairs:

```sql
campaign!="" | table cUsername campaign | dedup cUsername campaign | sort + cUsername
```

Alternatively, with multi-value field for campaign name:

```sql
campaign!="" | transaction cUsername | table cUsername campaign | sort + cUsername
```

### Users Affected by Confirmed Threats Within a Timeframe

This query also includes first-seen and last-seen columns. Search for nonempty campaign, aggregate by username+campaign pair, and compute min and max of the web-flow time stamp. Results are in epoch-milliseconds and can be converted to calendar time, if necessary.

```sql
campaign!="" | stats min(timestamp) max(timestamp) by cUsername campaign
```

Alternatively, include the epoch conversion using the strftime function. This example divides the time stamp by 1000 to remove milliseconds:

```sql
campaign!="" | stats min(timestamp) as oldest max(timestamp) as newest by cUsername campaign
```

Users Affected by High Risk and High Confidence Incidents

This query generates a priority list table of high risk and high confidence users regardless of whether they have a confirmed campaign. Search for high risk, high confidence, and deduplicate usernames. Since all these incidents are both high risk and high confidence, consider reimaging the affected device.

```
confidence="High" risk="High" | dedup cUsername | table cUsername campaign
```

Users Affected by Campaign

This query generates a chart of the number of infected users over time and broken down by campaign. Search for nonempty campaign, bin by a time span of one day, and compute a distinct count of usernames within that bin.

```
campaign!="" | timechart dc(cUsername) span=1d by campaign
```

Note

In SPLUNK, the time chart shortcut can be used.

Command and Control Servers

This query generates a list of all detected command-and-control (C&C) servers in the Confirmed category. Search for nonempty campaign, while showing server IP address and campaign, and then deduplicate server IP addresses. The result lists C&C IP destination addresses being used by the infected devices to maintain C&C communication. For each C&C IP address, you also see which Threat campaign it is involved with. Can be used to query other systems for more intelligence, provide indicators of compromise (IOCs), and identify malicious processes and applications on the infected endpoint.

```
campaign!="" | table sIP campaign | dedup sIP
```

CTA Integration with Cisco ISE

Cisco Identity Services Engine (ISE) is a security policy management platform that provides secure access to network resources. Cisco ISE functions as a policy decision point and enables enterprises to ensure compliance, enhance infrastructure security, and streamline service operations. Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. You can then use that information to make proactive governance decisions by tying identity to various elements in the network.

CTA integrates with Cisco ISE to deliver a network-level quarantine, which features the ability to cut an infected device from the network so that no sensitive data can be exfiltrated further. The integration between CTA and Cisco ISE uses STIX/TAXII. For critical-level risk findings in which the system is able to attribute the infection to an individual user, Cisco ISE receives a Requested Course of Action that suggests a Threat Centric Network Access Control (TC-NAC) Quarantine, which is part of the Cisco Rapid Threat Containment framework. Depending on the risk associated with an infection, the Requested Course of Action could be Monitoring, Eradication, Internal Blocking, or a combination. Internal Blocking is the course of action intended to be used in the blocking policies in TC-NAC. For more information, see Cisco Rapid Threat Containment.
You can develop your own solution by using Cisco ISE and the data feed provided by the CTA STIX/TAXII service. The data feed includes information on identifying the infected device and the action to be performed. You can define quarantine policies in Cisco ISE based on the recommendations in the CTA STIX/TAXII feed. For information on how to configure the CTA adapter in Cisco ISE, see the Cisco ISE Administrator Guide, Release 2.2.

**Note**

CTA works with user identities listed in the web proxy logs as client IP's or user names. Specifically, in the case of an IP addresses, the IP address that is available through the proxy logs may be an IP address that collides with another IP address (for another device) on the internal corporate network. For example, roaming users connected via AnyConnect with a split-tunnel directly to the Internet may acquire a local IP address they have at home (for instance, a 10.0.0.x address), which may collide with an IP address in an overlapping private range used in the internal corporate network. When you define the Rapid Threat Containment policies, consider your logical network architecture to avoid quarantine actions being applied to mismatched devices.
Cisco Security Appliance Integration

- Overview, on page 209
- Hybrid Web Security, on page 209
- Transparent Redirection, on page 212

Overview

Cisco Cloud Web Security supports integration with on-premises security appliances:

- Cisco Adaptive Security Appliance (ASA)
- Cisco Integrated Services Router (ISR)
- Cisco Web Security Appliance (WSA)

To connect your security appliance with Cisco Cloud Web Security, see the deployment guides:

For details on further configuration, see the support documentation for the security appliance.

Tip

Test that the service is working by going to http://www.eicar.org and attempt to download their Anti-Malware Testfile. This should generate a block message.

Hybrid Web Security

Hybrid Web Security provides unified cloud and on-premises policy enforcement and threat defense using security policies you define in Cisco ScanCenter. Register your on-premises WSA with Cisco ScanCenter to automatically download and periodically update your security policies from the CWS cloud.

Before you begin

Connect, install, and configure your security appliance to operate in Hybrid Web Security mode. For information on how to set up a Cisco WSA, see:
• Release Notes for AsyncOS 9.2 for Cisco Web Security Appliances
• AsyncOS 9.2 for Cisco Web Security Appliances User Guide (primarily Chapters 2 and 3)

Note
Both CWS and WSA require a Certificate Authority signed certificate to authenticate and secure communications between them. Generate this certificate externally and upload the certificate and its key to both Cisco ScanCenter and the Cisco WSA.

Procedure

Step 1
In Cisco ScanCenter, navigate to Admin > Management > Hybrid Web Security.

Step 2
Click Generate Token.

Step 3
After the new authorization token is generated, click Copy Token to Clipboard.

Step 4
Paste the authorization token in the setup of the security appliance. Specifically in the Cisco WSA, paste the token in the Enter Authorization Key dialog box on the Web Policy Connectivity page of the System Setup Wizard. Refer to Chapter 3 in the AsyncOS 9.2 for Cisco Web Security Appliances User Guide.

Note
An unregistered token expires after 1 hour. If the token expires before use, generate a new token.

Note
One unique token is generated for use on any one security appliance. For multiple security appliances, repeat these steps to generate multiple tokens.

Step 5
In the Registered WSAs section, a table lists the security appliances currently and successfully registered with CWS. To remove an appliance, select its check box and click Deregister.

What to do next
Upon successful registration, the security appliance downloads your Cisco Cloud Web Security policy from Cisco ScanCenter.

• Every time you modify your CWS policy in Cisco ScanCenter, the whole policy is downloaded to the security appliance to synchronize policies.

• By default, every two minutes, the Cisco WSA checks to see if there is an updated policy to download.

• For information on configuring security policy and web filtering, see Overview, on page 65.

• In the Cisco WSA, view its Reporting > System Status page to check the status of its hybrid registration with CWS.

Note
Some items that are configurable in Cisco ScanCenter are not yet supported for downloading by the Cisco WSA.

The following items must be configured directly on the Cisco WSA:

• Email Alert Settings. Frequency of email alerts you want to receive.
• Customized Alerts. Custom text and other settings for Block and AUP/EUA pages.

• Global Settings. Enabling of settings such as SearchAhead, SafeSearch, AUP (EUA on the WSA), Dynamic Classification Engine, Content Range Headers, and Sandboxing.

• Authentication Realms. Authentication realms must be configured directly on the Cisco WSA shortly after the System Setup Wizard finishes configuring Hybrid Web Security mode. In CWS, an authentication realm refers to SAML and EasyID. On the Cisco WSA, the types supported are different and usually refer to NTLM (SAML is not yet supported on the Cisco WSA). If CWS rules have either 'auth-user-name' or authentication groups configured, on the Cisco WSA you must configure authentication realms and custom identification profiles with authentication enabled. For more information, see the AsyncOS 9.2 for Cisco Web Security Appliances User Guide (primarily Chapters 6 and 7).

Note
Conversion and download of any HTTPS rules or authentication group rules is skipped during Cisco WSA hybrid set-up. These rules are automatically completed only after you set up the Cisco WSA in Hybrid Web Security mode and configure HTTPS proxy, authentication realms, and identification profiles, as CWS-to-WSA policy updates occur every two minutes.

The following items are not currently supported for use on on-premises security appliances and do not get downloaded by the Cisco WSA:

• Anonymize CWS Action Type. Any rule assigned the Anonymize action.

• Authenticate CWS Action Type. Any rule assigned the Authenticate action.

• Warn CWS Action Type. Any rule assigned the Warn action.

• Outbound Filters. Any rule using a filter that contains any Keyword, Outbound File Type, Preconfigured ID, or Regular Expression. Inbound extensions are also not supported.

• Whitelisting sets of domains and URLs to bypass Spyware or Web Reputation (WebRep) scanning at the global level.

• Delegated Administration. The Cisco WSA does not incorporate the concept of delegated administration. CWS will send a merged policy configuration.

• SafeSearch. Works with Google, Yahoo and Bing. Because they are moving to HTTPS, we require HTTPS inspection to be enabled in the cloud.

For additional information, including warnings, caveats, and what functionality is and is not supported, see:

• Release Notes for AsyncOS 9.2 for Cisco Web Security Appliances

• AsyncOS 9.2 for Cisco Web Security Appliances User Guide (primarily Chapter 2)

Note
Translation of both default and user-defined CWS policies to WSA policies is not a one-to-one conversion. However, the action that results from application of a particular policy in both environments is the same. In other words, the Block or Allow decision is always consistent, regardless of the sequence of rules “fired” in both cases. This allows rule evaluation in the proxy to be optimized for better performance without compromising consistent behavior.
Transparent Redirection

The Cisco WSA can be configured to enable usernames, internal IP addresses, and domain groups to be sent using PIM to Cisco Cloud Web Security without needing to make end-user changes. There are several ways to achieve this but Cisco recommends using an explicit proxy, PAC file, or WPAD. The Cisco WSA is a network-level proxy and makes transparent redirection possible for network-based clients without requiring additional agents, such as Cisco Cloud Web Security Connector.

Note

You must switch off scanning and the additional features of the Cisco WSA. However, you can enable caching. When using the Cisco WSA in transparent mode, user granularity is available for HTTP traffic only. To pass HTTPS traffic to Cisco Cloud Web Security, enable HTTPS inspection, providing that it is legal to do so in your jurisdiction.

Configuring the Upstream Proxy

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>On the WSA, click <strong>Network</strong> &gt; <strong>Upstream Proxies</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Click <strong>Add Group</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>In the <strong>Name</strong> field, enter <strong>WebSecurity</strong>.</td>
</tr>
<tr>
<td>4</td>
<td>In the <strong>Proxy Servers</strong> area, enter the <strong>Proxy Address</strong>, <strong>Port</strong> and the number of <strong>Reconnection Attempts</strong> for each of the Cisco Cloud Web Security proxy servers (found in your provisioning email). Typically the port will be <strong>8080</strong>, and the number of reconnection attempts should be <strong>2</strong>.</td>
</tr>
<tr>
<td>5</td>
<td>In the <strong>Load Balancing</strong> drop-down list, choose a method. Typically this will be <strong>None (Failover)</strong>.</td>
</tr>
<tr>
<td>6</td>
<td>Click a <strong>Failure Handling</strong> method to specify how to handle requests if the primary and secondary Cisco Cloud Web Security proxies are both unavailable. This should be <strong>Drop requests</strong>.</td>
</tr>
<tr>
<td>7</td>
<td>Click <strong>Submit</strong> to apply your changes. Alternatively, click <strong>Cancel</strong> to abandon your changes.</td>
</tr>
<tr>
<td>8</td>
<td>Click <strong>Commit Changes</strong>.</td>
</tr>
</tbody>
</table>

Setting the Routing Policies

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>On the WSA, click <strong>Web Security Manager</strong> &gt; <strong>Routing Policies</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Edit the default routing policy, and in the <strong>Upstream Proxy Group</strong> drop-down list, choose <strong>WebSecurity</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>Click <strong>Submit</strong> to apply your changes. Alternatively, click <strong>Cancel</strong> to abandon your changes.</td>
</tr>
</tbody>
</table>
CLI Settings

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log in to the CLI and enter <code>advancedproxyconfig</code>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>At the parameter group select prompt, enter <code>caching</code>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>At the caching options prompt, enter 4 to select Customized Mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Accept the default values until you are prompted to enter the Time in seconds after which an explicit IMS Refresh request must be issued.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Enter 0.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Enter <code>commit</code> to make the change, and then enter a description of the change.</td>
</tr>
</tbody>
</table>
Cloud Web Security Mobile Browser

- Overview, on page 215
- Provisioning, on page 216
- Policy, on page 223
- Branding, on page 225
- Captive Portal Detection, on page 226
- Trusted Network Detection, on page 226
- Fail Open or Fail Closed, on page 227

Overview

The Cisco Cloud Web Security (CWS) Mobile Browser solution allows you to set up and deploy a secure web browser onto your mobile devices and protect its web usage with Cisco CWS. HTTP/HTTPS traffic is redirected to Cisco CWS for inspection and controlled by the policy you configure in Cisco ScanCenter.

Table 1: Operating Systems and Mobile Devices Currently Supported

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Mobile Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple iOS 8.4 and higher</td>
<td>iPhone 5, 5s, 6, 6 Plus, 6s, 6s Plus</td>
</tr>
<tr>
<td></td>
<td>iPad 3, 4, Air, Air 2, all Mini models</td>
</tr>
<tr>
<td></td>
<td>iPad Pro is not supported</td>
</tr>
<tr>
<td>Android 4.4 and higher</td>
<td>Any mobile smartphone or tablet should be supported.</td>
</tr>
<tr>
<td>Android 6.0 is not supported</td>
<td>Testing has been performed on devices including Samsung Galaxy S6, LG Nexus 5, LG Nexus 4, and ASUS Nexus 7. Devices running Android variants, such as Kindle, are not supported.</td>
</tr>
</tbody>
</table>

Note

We do not provide technical support for third-party products such as the mobile device. For any issues with the mobile device, consult the vendor-specific support team.
Currently, the Shift_JIS character encoding set is not supported.

The Cisco CWS Mobile Browser (referred to here as mobile browser) has two separate user interfaces: one for mobile smartphones and one for tablets. These user interfaces have been designed to make efficient use of screen space on both form factors. Also, the iOS and Android user interfaces differ, reflecting the differing design languages to match expectations of how to interact with the app.

The following main functionalities are supported in the mobile browser:

- Multiwindow (smartphone) or multitab (tablet) browsing
- Web search using the address bar, configurable search engine (defaults to Google)
- Browsing history and bookmarks
- Sharing content through email, SMS, and various other applications
- Ability to clear cookies, cache, and browsing history

Depending on your policy configured in Cisco ScanCenter, the browsing history may still be recorded on the Cisco CWS server.

- Ability to email diagnostic logs to an email address

Diagnostic logs should be included in any bug reports.

- Ability to brand the new window or tab screen with your company name and logo
- Your company name and logo would be clickable with your corporate URL

Provisioning

The mobile browser provisioning process consists of delivering the application to install on the mobile device and distributing the configuration file to configure the application.

Deliver the Application

This section describes how to deliver the mobile browser app across your inventory of mobile devices running either iOS or Android.

Application on iOS

The two options to deliver the mobile browser app on iOS are:

- Automated process using mobile device management software.

Deliver Application Using Management Software

One way to deliver the mobile browser on iOS is using Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) software. This method allows you to silently and efficiently deliver the application to your mobile devices running iOS. To use this method, your MDM or EMM software provider must support application delivery using Apple's App Store and Managed App Configuration.

Note

Cisco does not provide support for third-party MDM or EMM software. Contact the vendor of your third-party management software for information on how to use their product for app deployment.

Using your third-party MDM or EMM software:

Procedure

Step 1
Create a policy to deploy an App Store application.

Step 2
Search for "CWS Browser" in the App Store, and select the application.

Step 3
Configure the policy to deploy the mobile browser app.

Step 4
Deploy the policy. The app gets pushed to your target devices and becomes visible on the device's Home Screen.

What to do next

Cisco may issue updated builds of the mobile browser that address issues or add functionality. Whether you automatically receive updates depends on your MDM or EMM policy.

Deliver Application Using App Store

Another way to deliver the mobile browser on iOS is directly installing the application using Apple's App Store. Instruct your users to open the App Store to find, download, and install the "CWS Browser" app. To avoid accidentally installing an incorrect application, email your users with an up-to-date and direct link to the App Store listing for the mobile browser.

Note

Cisco may issue updated builds of the mobile browser that address issues or add functionality. Whether you automatically receive updates depends on whether you have configured your inventory of iOS devices to receive automatic updates from the App Store.

Application on Android

The mobile browser app for Android is a binary in .apk format. Android application package (APK) is the package file format used by the Android operating system for distribution and installation of application software. The mobile browser app is hosted on the Google Play store. Instruct your users to open the Google Play store to find, download, and install the "CWS Browser" app. To avoid accidentally installing an incorrect
application, email your users an up-to-date and direct link to the Google Play store listing for the mobile browser.

Another way to deliver the mobile browser from the Google Play store is using MDM or EMM software. Currently, Cisco does not support this method or provide support for third-party MDM or EMM software. Contact the vendor of your third-party management software to determine if this method is possible.

Note
Cisco may publish updated builds of the mobile browser to the Google Play store that address issues or add functionality. If you have configured your inventory of Android devices to automatically update from the Google Play store, these updated builds may be installed automatically.

Distributing the Configuration File

The configuration file contains information that determines the behavior and functionality of the mobile browser app. Use a file manager, not the download manager, to open the configuration file as type other. On both iOS and Android, the configuration file must have the .cwsconfig extension. Both iOS and Android configuration files use the same property=value format. You can populate the properties in the file with values to suit your deployment needs. Distribute the configuration file onto your mobile devices using email, web distribution, or management software on iOS.

Configuration File Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Expected Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cws_aup_enabled</td>
<td>true or false</td>
<td>Whether AUP functionality is enabled; see Acceptable Usage Policy, on page 223.</td>
</tr>
<tr>
<td>cws_auth_licence_key</td>
<td>String containing your license key.</td>
<td>(Required) Your Cisco CWS license key (company, group, or user) is required to authenticate the device.</td>
</tr>
<tr>
<td>cws_company_image</td>
<td>Base 64 representation of an image.</td>
<td>Your company image or logo; see Branding, on page 225.</td>
</tr>
<tr>
<td>cws_company_text</td>
<td>String containing your company name.</td>
<td>Your company name; see Branding, on page 225.</td>
</tr>
<tr>
<td>cws_company_url</td>
<td>String containing your company web URL</td>
<td>Your company URL; see Branding, on page 225.</td>
</tr>
<tr>
<td>cws_easyid_saml_enabled</td>
<td>true or false</td>
<td>Whether EasyID or SAML is being used. Hints to the mobile browser to allow third-party cookies.</td>
</tr>
<tr>
<td>Property</td>
<td>Expected Value</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>cws_exception_poll_interval</td>
<td>Number in seconds.</td>
<td>Time in seconds specifying how often the whitelist configuration is retrieved.</td>
</tr>
<tr>
<td></td>
<td>Default is 3600.</td>
<td></td>
</tr>
<tr>
<td>cws_fail_open_enabled</td>
<td>true or false</td>
<td>Whether the browser should fail open on a proxy error; see Fail Open or Fail Closed, on page 227.</td>
</tr>
<tr>
<td></td>
<td>Default is false for fail closed.</td>
<td></td>
</tr>
<tr>
<td>cws_trusted_network_beacons</td>
<td>Comma-separated array containing: hostname:port</td>
<td>SHA256 certificate hash</td>
</tr>
<tr>
<td></td>
<td>Default is empty.</td>
<td></td>
</tr>
<tr>
<td>cws_trusted_network_poll_interval</td>
<td>Number in seconds.</td>
<td>Time in seconds specifying how often the beacon server is polled to detect the presence of a trusted network.</td>
</tr>
<tr>
<td></td>
<td>Default is 300.</td>
<td></td>
</tr>
<tr>
<td>mdm_vendor</td>
<td>String containing the MDM name.</td>
<td>(iOS only) Name of the MDM software used for provisioning.</td>
</tr>
<tr>
<td></td>
<td>Default is empty.</td>
<td></td>
</tr>
<tr>
<td>mdm_version</td>
<td>String containing the MDM version.</td>
<td>(iOS only) Version of the MDM software used for provisioning.</td>
</tr>
</tbody>
</table>

### Configuration File Template

The following configuration file template may be used to create your company-specific configuration file. For information on each property and its expected value, see Configuration File Properties, on page 218.

**Note**

The `cws_auth_licence_key` property value is required. All other properties are optional. If you wish to omit a property and inherit its default value, completely remove the property from the configuration file, do not leave it blank. For example, if you do not want to configure a company-specific logo, remove the entire `cws_company_image=` line.

**Configuration File Template for iOS:**

```plaintext
cws_aup_enabled=false
cws_auth_licence_key=
cws_company_image=
cws_company_text=
cws_company_url=
cws_easyid_saml_enabled=false
cws_exception_poll_interval=3600
cws_fail_open_enabled=false
cws_trusted_network_beacons=
cws_trusted_network_poll_interval=300
mdm_vendor=
mdm_version=
```
Configuration on iOS

There are three options to distribute the configuration file onto mobile devices running iOS.

Deliver Configuration Using Email

Distribute the configuration file using email.

Before you begin

Once you have created your configuration file as a property list, ensure that it has the .cwsconfig file extension. For example, testfile.cwsconfig

Ensure that the user has installed the mobile browser from the App Store before attempting to install the configuration.

Procedure

- **Step 1**: Attach the .cwsconfig file to an email.
- **Step 2**: Send the email to an email address the user has configured in the email client on their mobile device, which may or may not be their corporate address.
- **Step 3**: After installing the CWS Browser from the App Store, open the email.
- **Step 4**: Tap and hold on the attachment. After a few seconds, the share sheet appears.
- **Step 5**: Select **Copy to CWS Browser**. The mobile browser opens and configures itself based on the configuration file.

Deliver Configuration Using Intranet Web Server

Distribute the configuration file by hosting the configuration file on a web server within your corporate Intranet.
Before you begin

Once you have created your configuration file as a property list, ensure that it has the .cwsconfig file extension. For example, testfile.cwsconfig

Ensure that the user has installed the mobile browser before attempting to install the configuration.

Procedure

| Step 1 | Add to your web server configuration a MIME type of application/cwsconfig for the .cwsconfig file name extension. |
| Step 2 | Upload the .cwsconfig file to a web server on your corporate Intranet. |
| Step 3 | Distribute the web URL for the .cwsconfig file to your users by a means such as email. |
| Step 4 | After installing the mobile browser app, use Safari on the mobile device to browse to the web URL from Step 3. |
| Step 5 | Tap the screen, select Open In, and choose Copy to CWS Browser. The mobile browser opens and configures itself based on the configuration file. |

Deliver Configuration Using Management Software

Distribute the configuration file using MDM or EMM software. This method allows you to silently and efficiently deliver the configuration file to your mobile devices running iOS. To use this method, your MDM or EMM software provider must support delivery using Apple's Managed App Configuration. This method is also secure: once the app is configured, it rejects any attempt to reconfigure it, which prevents accidental or malicious reconfiguration.

Not all MDM and EMM solutions support Apple's Managed App Configuration. Contact the vendor of your third-party management software to find out if this feature is supported and how to configure it. Cisco does not provide support for third-party MDM or EMM software.

Procedure

| Step 1 | When configuring the Managed App Configuration, you are prompted to specify the Bundle Identifier. Enter com.cisco.cwsbrowser |
| Step 2 | Specify the configuration properties as property=value pairs. |
| Step 3 | Once the Managed App Configuration settings are pushed to the mobile devices, the mobile browser automatically picks up the configuration with no additional steps required. |

Configuration on Android

There are two options to distribute the configuration file onto mobile devices running Android.
Note
There is a known issue on Android regarding installation of the configuration file. The app will not accept a new or updated configuration file if the app is running in the background. Therefore, after downloading the app, swipe to close the app before installing the configuration file.

Deliver Configuration Using Email

Distribute the configuration file using email.

Before you begin
Once you have created your configuration file as a property list, ensure that it has the .cwsconfig file extension. For example, testfile.cwsconfig
Ensure that the user has installed the mobile browser from the Google Play store before attempting to install the configuration.

Procedure

Step 1
Attach the .cwsconfig file to an email.

Step 2
Send the email to an email address the user has configured in the email client on their mobile device, which may or may not be their corporate address.

Step 3
After installing the CWS Browser from the Google Play store, open the email.

Step 4
Tap the attachment. You are prompted with a list of apps with which to open the configuration file.

Step 5
Select CWS Browser. The mobile browser opens and configures itself based on the configuration file.

Deliver Configuration Using Intranet Web Server

Distribute the configuration file by hosting the configuration file on a web server within your corporate Intranet.

Before you begin
Once you have created your configuration file as a property list, ensure that it has the .cwsconfig file extension. For example, testfile.cwsconfig
Ensure that the user has installed the mobile browser before attempting to install the configuration.
The web server must not require authentication; it must not use techniques such as HTTP basic, digest auth, or NTLM.

Procedure

Step 1
Add to your web server configuration a MIME type of application/cwsconfig for the .cwsconfig file name extension.

Step 2
Upload the .cwsconfig file to a web server on your corporate Intranet.

Step 3
Distribute the web URL for the .cwsconfig file to your users by a means such as email.
Step 4 After installing the mobile browser app, use Chrome on the mobile device to browse to the web URL from Step 3.

Step 5 Chrome automatically offers to open the URL in the mobile browser, at which point the mobile browser loads the file and applies the configuration.

Policy

Authentication

When using the mobile browser, user authentication is supported in three ways:

- License Key. The simplest form of authentication is license key authentication in which you create a license key representing your whole company (company key), a group of users (group key) or a specific user (user key). Each of these levels of key granularities is supported by the mobile browser.

- In conjunction with the license key, you may establish user granularity by using SAML or EasyID. SAML works by authenticating the user on the mobile browser with your company's identity provider (IdP).

- EasyID works by authenticating them directly against your LDAP server. The user is prompted to authenticate upon hitting an authenticate policy, which is defined in Cisco ScanCenter. For more information about SAML, EasyID, and authenticate rules, see Authentication, on page 19.

Third-party cookies must be enabled in the mobile browser for EasyID or SAML to function correctly. For the mobile browser to be compatible with EasyID or SAML authentication, the cws_easyid_saml_enabled property must be set to true in the configuration file. This setting enforces that third-party cookies must be enabled in the mobile browser.

Note

Due to limitations in the Android app, if you wish to use SAML authentication with the Android app, your IdP must be exposed to the public Internet. Also, the IdP must not be whitelisted in the Cloud Bypass list. In other words, requests to the IdP must go through the CWS proxy. Ensure that any domains associated with your IdP are exempted from any authentication policy. Also, you may wish to exempt your IdP from any HTTPS Inspection policy.

Acceptable Usage Policy

AUP is a feature that allows you to ensure that your employees read your company AUP either every day or every week. This feature is also part of the CWS Connector, so you may already have it configured. For more information on how to configure the AUP, see Acceptable Usage Policy, on page 103.

Note

Set the cws_aup_enabled property in the mobile browser configuration file to true.
Web Filtering

Web filtering policy is configured using Cisco ScanCenter, the portal to Cisco CWS.

- Block access to certain websites.
- Warn a user about browsing to certain websites.
- Anonymize user information from reporting on certain websites.

If you are using a group key to authenticate the mobile browser as recommended, you may want to create special policies to apply to this group. For information on how to create policies in Cisco ScanCenter, see Policy, on page 91.

Cloud Bypass Whitelisting

The mobile browser supports the Cloud Bypass functionality used by Cisco ISR G2 and Cisco 4000 Series ISR routers with Cisco CWS. Cloud Bypass allows you to create a whitelist specifying a set of domains you do not want scanned by Cisco CWS. If a request to one of these web pages is made through the mobile browser, it is sent directly to the Internet rather than through the Cisco CWS proxy.

One use case for this functionality is internal domains such as Intranet sites that are not accessible through Cisco CWS infrastructure. Another use case is requests to sensitive domains where you may not wish to proxy requests for legal or policy reasons.

The whitelist itself is hosted in the cloud and configured through Cisco ScanCenter. For more information on how to create a whitelist, see Cloud Bypass, on page 107.

The whitelist is retrieved from the cloud by the mobile browser every configurable number of seconds. The `cws_exception_poll_interval` property in the mobile browser configuration file has a default of every 3600 seconds. When the app restarts, it also retrieves the whitelist. If there is an error when retrieving the whitelist, the previous version of the whitelist is used.

---

**Note**

A limitation exists on the Android version of the mobile browser where resource requests inherit the whitelist state of the parent page. For example, you load a page such as `Cisco.com/page1.html` and this page contains resources such as `opendns.com/image.jpg`. If Cisco.com is whitelisted, the request to `opendns.com/image.jpg` is also whitelisted, and vice versa.

HTTPS Inspection

The mobile browser supports the Cisco CWS HTTPS Inspection functionality. This functionality allows Cisco CWS to decrypt HTTPS traffic in order to apply policy, filtering, and scanning. By default, this functionality is switched off in Cisco ScanCenter. If you want to use this functionality, enable it in Cisco ScanCenter, create HTTPS Inspection policies, and generate a company-specific certificate. For more information, see Secure Traffic Inspection, on page 113.

Once this functionality is enabled in Cisco ScanCenter, install the company-specific certificate onto the mobile device. The mobile browser reads this certificate from the device trust store. If you do not install the certificate, you may be presented with certificate warnings when browsing to inspected HTTPS websites.
Use your company's MDM or EMM to install the certificate. Alternatively, send the certificate as an email attachment, or host the certificate on a web server for the user to navigate to and download. The mobile browser app itself does not handle certificate installation.

**Reporting**

As with any other Connector, web traffic from the mobile browser is logged in the Cisco CWS reporting service. For more information on reporting in Cisco ScanCenter, see [Getting Started with Reports](#), on page 123.

Specific telemetry reported by the mobile browser include:

- Connector OS name. For example, iPhone OS.
- Connector OS version. For example, 9.0.2.
- Connector version.
  - For the mobile browser, SMBx.x.x where x.x.x is the version number.
  - For example, SMB1.0.1.
- Connector GUID.
  - Android only.
  - For example, 18502ABC.
  - Corresponds to the device serial number.
  - Field is anonymized if you browse to a site under an anonymization rule.

**Branding**

In the mobile browser, you can apply your corporate branding to the new window page. Customize this page by setting the following properties in the mobile browser configuration file:

- Corporate logo.
  - Set `cws_company_image` to a base 64 encoded string representing your image.
  - Get the base 64 encoding of your logo by running the following command in the terminal or command prompt (Windows users must install OpenSSL):
    ```
    $ openssl base64 -in corporateLogo.jpg
    ```
- Corporate text. Set `cws_company_text` to your company name.
- Corporate URL. Set `cws_company_url` to your corporate home page.
Captive Portal Detection

The Captive Portal Detection functionality in the mobile browser allows you to browse the Internet even when you are connected to a captive portal network. A captive portal network is a Wi-Fi network that requires you to log in to a web page before you are permitted access to the Internet. These networks are commonly found in airports, hotels, and coffee shops.

On iOS, the operating system detects and handles captive portal networks. When you connect to a captive portal network, the operating system presents you with the sign-in page, and enforces you to either log in or cancel your connection request. Therefore, the mobile browser on iOS does not need any special functionality to be compatible with captive portal networks. However, in cases where the captive portal network attempts to tamper with or bypass the iOS captive portal network detection, such networks may be incompatible with the mobile browser.

On Android, the operating system partially handles captive portal networks: it can detect when it is connected to a captive portal network but will not enforce the user to sign in or abandon their connection attempt. Therefore, the mobile browser on Android has detection and handling functionality built in. When the mobile browser on Android detects a captive portal network, it stops forwarding traffic to Cisco CWS. You then sign into the captive portal network, as you would normally on another web browser such as Chrome. Once you have signed in, the mobile browser detects that wider internet access has been restored, and begins redirecting traffic to Cisco CWS.

Note

Some captive portal networks block proxies. TCP port 8080 is used by the mobile browser. Such captive portal networks are incompatible with the mobile browser unless the fail open functionality is enabled. For more information, see Fail Open or Fail Closed, on page 227.

Trusted Network Detection

The Trusted Network Detection (TND) functionality allows you to configure the mobile browser to know when it is on what you define as a trusted network. When the mobile browser is being used on a trusted network, it will not redirect traffic to Cisco CWS and instead, sends traffic directly to the Internet.

One use case for this functionality is defining your internal network as a trusted network. This allows the mobile browser to access internal resources on your Intranet when on your corporate Wi-Fi or VPN. Another use case is if you have another on-premises Cisco CWS Connector or Cisco security product that you would prefer the mobile browser traffic to be routed through.

TND is configured by specifying a set of beacon servers and ports that the mobile browser can attempt a TLS handshake with. The beacon servers do not require any specialized software. The mobile browser must be given a SHA256 checksum or fingerprint of the certificate for the beacon server. The mobile browser attempts a TLS handshake with this server and compares the checksum with its expected checksum. If there is a match, the mobile browser then knows that it is on a trusted network and stops sending its traffic to Cisco CWS. If there are multiple trusted network beacon servers defined, they are polled in sequential order until one matches. If none of them match, the mobile browser then knows that it is on an untrusted network and will proxy its traffic to Cisco CWS.

TND polling is triggered upon a network change: for example change of Wi-Fi network, Wi-Fi to cellular, cellular to Wi-Fi, or VPN connection gets established or disconnected. Also, TND polling occurs in every
configurable number of seconds. Configure the number of seconds by setting the `cws_trusted_network_poll_interval` property in the mobile browser configuration file. The default value is 300 seconds.

**Beacon Server Configuration**

TND beacon servers are specified in the configuration file using the `cws_trusted_network Beacons` property. The property is a string with the following format:

```
BeaconServer_1:BeaconPort_1|SHA256HASH_1, BeaconServer_2:BeaconPort_2|SHA256HASH_2, ...
```

For example:

```
web.intranet.com:443|900fc753b7fe06eb30d092620244e0c83d78d6c0324612de068274a86077476,
ash.intranet.com:22|343d7b76e59cbf9cb9d5b2d4917d7ab89b809ccd95e824fdee5837d5971c6
```

One way to obtain the SHA256 hash of your server certificate is to use the following command in a Unix terminal:

```
$ openssl s_client -connect web.intranet.com:443 > /dev/null
</dev/null | openssl x509 -noout -fingerprint -sha256
```

Be sure to remove the colons to get:

```
SHA256 Fingerprint=
```

**Fail Open or Fail Closed**

The mobile browser allows you to specify its behavior in case it's unable to connect to Cisco CWS. Choose `fail open` to allow all mobile browser web traffic to go directly to the Internet, or choose `fail closed` to block all mobile browser web traffic until connectivity is restored.

Examples of events that could trigger a `fail open` or `fail closed` scenario include:

- Cisco CWS infrastructure error or outage.
- DNS failure on the network.
- TCP port 8080 or communication with Cisco CWS blocked by a firewall.
- Packet loss between the network and Cisco CWS.
- Other network connectivity issues.

By default, the mobile browser fails closed. `Fail open` can be enabled by changing the `cws_fail_open_enabled` property in the mobile browser configuration file to true.
A captive portal network is a special case handled differently. For information, see Captive Portal Detection, on page 226.

If fail open is enabled, the mobile browser temporarily disables redirection of traffic to Cisco CWS and checks whether Cisco CWS is reachable again after 60 seconds. If Cisco CWS is reachable, the mobile browser redirects its traffic to Cisco CWS. If not, another attempt is made after two minutes, three minutes, four minutes, and every eight minutes, if needed. If you quit the app entirely, dismissing it from the multitasking menu on the OS, and reopen it, this also triggers a fail open check.