Managing Web Security Appliances

This chapter contains the following sections:

About Centralized Configuration Management

Centralized configuration management allows you to publish configurations from a Cisco Content Security Management appliance to up to 150 associated Web Security appliances, in order to:

- Simplify and speed management of web security policies by configuring or updating settings once on the Security Management appliance, instead of on each Web Security appliance.
- Ensure uniform policy enforcement across distributed networks.

There are two ways to publish settings to Web Security appliances:

- Using Configuration Masters
- Using configuration files from Web Security appliances (using Advanced File Publishing)

Determining the Correct Configuration Publishing Method

There are two different processes for publishing configurations from the Security Management appliance, and each publishes different settings. Some settings cannot be centrally managed.

To Configure	Do This
Features that appear under the Web Security Manager menu on the Web Security appliance, such as policies and custom URL categories. Exception: L4 Traffic Monitor (L4TM) settings are not included in Configuration Masters. The exact features supported depend on the configuration master version, which corresponds to an AsyncOS for Web Security version.	Publish a Configuration Master. Many features that are configurable in a Configuration Master also require configurations directly on the Web Security appliance in order to work. For example, SOCKS Policies are configurable via Configuration Master, but a SOCKS Proxy must first be configured directly on the Web Security appliance.
Note: Integration with a Cisco Identity Services Engine (ISE) must be configured independently on each Web Security appliance. Cisco Identity Services Engine settings cannot be published from a Cisco Content Security Management appliance.	Use Advanced File Publishing.
FIPS mode for Federal Information Processing Standard, Network/interface settings, DNS, Web Cache Communication Protocol (WCCP), upstream proxy groups, certificates, the proxy mode, time settings such as NTP, L4 Traffic Monitor (L4TM) settings, and authentication redirect hostname.	Configure settings directly on your managed Web Security appliances. See the AsyncOS for Cisco Web Security Appliances User Guide

Setting Up Configuration Masters to Centrally Manage Web Security Appliances

On This Appliance	Do This	More Information
—	Check for general configuration requirements and caveats.	See Important Notes About Using Configuration Masters, on page 3.
—	Determine the Configuration Master version to use for each Web Security appliance.	See Determine the Configuration Master Versions to Use, on page 4.
Web Security appliance**s**	On all target Web Security appliances, enable and configure the features and functionality that are required to support the policy and other settings that you will configure in Configuration Masters on the Security Management appliance.	—
Web Security appliance	**(Optional)** If you have a working Web Security appliance that can serve as a configuration model for all of your Web Security appliances, you can use a configuration file from that Web Security appliance to speed configuration of a Configuration Master in the Security Management appliance.	For instructions on downloading a configuration file from a Web Security appliance, see “Saving and Loading the Appliance Configuration” in the AsyncOS for Cisco Web Security Appliances User Guide.

On This Appliance	Do This	More Information
Security Management appliance	Enable and configure Centralized Configuration Management.	See Enabling Centralized Configuration Management on the Security Management Appliance, on page 4.
Security Management appliance	Initialize the Configuration Masters.	See Initializing and Configuring Configuration Masters, on page 4.
Security Management appliance	Associate Web Security appliances to the Configuration Masters.	See About Associating Web Security Appliances to Configuration Masters, on page 5.
Security Management appliance	Import and/or manually configure policies, custom URL categories, and/or a web proxy bypass list in the Configuration Masters.	See Configuring Settings to Publish , on page 6
Security Management appliance	Ensure that the features enabled on each Web Security appliance match the features enabled for the Configuration Master assigned to that appliance.	See Ensuring that Features are Enabled Consistently , on page 10.
Security Management appliance	After you have set up required Configuration Masters and enabled appropriate features, publish configurations to your Web Security appliances.	See Publishing a Configuration Master , on page 13.
Security Management appliance	Prepare in advance for possible URL Category set updates that can modify your existing Configuration Master settings.	Preparing For and Managing URL Category Set Updates , on page 23

Important Notes About Using Configuration Masters

Important Before you upgrade to AysncOS 12.0 and later, you may need to backup your Configuration Master setting. The Configuration Master versions 10.0 and earlier will be replaced with Configuration Master version 11.7 and later.

After you upgrade to this release, you must initialize new Configuration Masters or import the configurations from an existing Configuration Master. If you have an existing Configuration Master for a previous release (for example, 9.1), you can copy the settings to a new Configuration Master (for example, 11.5).

Due to the change in the Configuration Master version, the appliance list is lost from the Identities and Policies. You must re-associate the Web Security appliance in the Configuration Masters.

Note On each Web Security appliance that you will manage centrally, check to be sure that all Realm Names in Network > Authentication are unique across appliances, unless the settings for same-name realms are identical.

Determine the Configuration Master Versions to Use

Your Security Management appliance provides multiple Configuration Masters, so that you can centrally manage Web Security appliances that run different versions of AsyncOS for Web Security that support different features.

Each Configuration Master contains configurations to be used for a particular version or versions of AsyncOS for Web Security.

To determine which configuration master version to use for your versions of AsyncOS for Web Security, see the Compatibility Matrix at http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html.

Note The Configuration Master version should match the AsyncOS version on the Web Security appliance, as specified in the Compatibility Matrix. Publishing an older Configuration Master version to a newer Web Security appliance may fail if settings on the Web Security appliance do not match the settings in the Configuration Master. This can occur even if the Web Appliance Status detail page does not indicate any discrepancies. In this case, you must manually compare the configurations on each appliance.

Enabling Centralized Configuration Management on the Security Management Appliance

Step 1 On the Security Management appliance, choose **Management Appliance > Centralized Services > Web > Centralized Configuration Manager**.

Step 2 Click **Enable.**

Step 3 If you are enabling Centralized Configuration Management for the first time after running the System Setup Wizard, review the end user license agreement, and click **Accept**.

Step 4 Submit and commit your changes.

Initializing and Configuring Configuration Masters

Initializing Configuration Masters

Note: After you initialize a configuration master, the Initialize option is not available. Instead, populate the Configuration Master using one of the methods described in Configuring Settings to Publish , on page 6 .

Step 1 On the Security Management appliance, choose **Web > Utilities > Configuration Masters**.

Step 2 Click **Initialize** in the Options column.

Step 3 On the Initialize Configuration Master page:

- If you have an existing Configuration Master for a previous release and you want to use or start with the same settings for the new Configuration Master, choose **Copy Configuration Master**. You can also import settings from an existing Configuration Master later.
- Otherwise, choose **Use default settings**.

Step 4 Click **Initialize**.

The Configuration Master is now available.

Step 5 Repeat for each Configuration Master version to initialize.

About Associating Web Security Appliances to Configuration Masters

For information about compatibility of configuration masters with Web Security versions, see Determine the Configuration Master Versions to Use, on page 4.

The simplest process for adding appliances to configuration masters depends on the situation:

If	Use This Procedure
You have not yet added Web Security appliances to the Security Management appliance	Adding Web Security Appliances and Associating Them with Configuration Master Versions , on page 5
You have already added Web Security appliances	Associating Configuration Master Versions to Web Security Appliances , on page 6

Adding Web Security Appliances and Associating Them with Configuration Master Versions

Use this procedure if you have not yet added your Web Security appliances to be centrally managed.

Before you begin

If you have not yet done so, choose the correct Configuration Master version for each Web Security appliance. See Determine the Configuration Master Versions to Use, on page 4.

Step 1 On the Security Management appliance, choose **Management Appliance > Centralized Services > Security Appliances**.

Step 2 Click Add Web Appliance.

Step 3 In the Appliance Name and IP Address text fields, type the appliance name and the IP address or resolvable hostname for the Management interface of the Web Security appliance.

Note If you enter a DNS name in the IP Address text field, it will be immediately resolved to an IP address when you click **Submit**.

Step 4 The Centralized Configuration Manager service is pre-selected.

Step 5 Click **Establish Connection.**

Step 6 Enter the user name and passphrase for an administrator account on the appliance to be managed, then click **Establish Connection**.

Note You enter the login credentials to pass a public SSH key for file transfers from the Security Management appliance to the remote appliance. The login credentials are not stored on the Security Management appliance.

Step 7 Wait for the Success message to appear above the table on the page.

Step 8 Choose the Configuration Master version to which you want to assign the appliance.

Step 9 Submit and commit your changes.

Step 10 Repeat this procedure for each Web Security Appliance for which you want to enable Centralized Configuration Management.

Associating Configuration Master Versions to Web Security Appliances

If you have already added Web Security appliances to the Security Management appliance, you can use the following procedure to quickly associate Web Security appliances with Configuration Master versions.

Before you begin

If you have not yet done so, choose the correct Configuration Master version for each Web Security appliance. See Determine the Configuration Master Versions to Use, on page 4.

Step 1 On the Security Management appliance, choose **Web > Utilities > Configuration Masters**.

Note If a Configuration Master shows as Disabled, you can enable it by clicking **Web > Utilities > Security Services Display**, then **Edit Display Settings**. Select the check box for that Configuration Master to enable it. For more information, see Enabling Features to Publish , on page 11.

Step 2 Click **Edit Appliance Assignment List**.

Step 3 In the rows of the appliances you want to associate, click to enter check marks in the **Masters** columns.

Step 4 Submit and commit your changes.

Configuring Settings to Publish

Set up your configuration masters with the settings you want to publish.

There are several ways to set up Configuration Masters:

If	Do This
You are upgrading from a previous release of AsyncOS for Security Management and You did not initialize a new Configuration Master version by copying an earlier, existing Configuration Master into the new version	Import the old version. See Importing from an Existing Configuration Master , on page 7.

If	Do This
You have already configured a Web Security appliance and want to use those same configurations for multiple Web Security appliances	Import a configuration file that you saved from that Web Security appliance into the Configuration Master. You may have saved this configuration file when you reviewed Setting Up Configuration Masters to Centrally Manage Web Security Appliances , on page 2. To import, see Importing Settings from a Web Security Appliance , on page 7.
You need to modify imported settings	See Configuring Web Security Features Directly in Configuration Masters, on page 8.
You have not yet configured policy settings, URL categories, or bypass settings on a Web Security appliance.	Configure these settings directly in an appropriate Configuration Master on the Security Management appliance. See Configuring Web Security Features Directly in Configuration Masters, on page 8.

Importing from an Existing Configuration Master

You can upgrade an existing configuration master to a new, higher configuration master version.

Step 1 On the Security Management appliance, choose **Web > Utilities > Configuration Masters**.

Step 2 In the Options column, click **Import Configuration**.

Step 3 For **Select Configuration Source**, select a Configuration Master from the list.

Step 4 Choose whether or not to include existing custom user roles in this configuration.

Step 5 Click **Import**.

What to do next

About Custom Web User Roles

Importing Settings from a Web Security Appliance

If you want to use an existing, working configuration from one of your Web Security appliances, you can import the configuration file to the Security Management appliance to create policy settings in a Configuration Master.

Before you begin

Verify compatibility of configuration files and Configuration Master versions. See Determine the Configuration Master Versions to Use, on page 4.

Caution You can import compatible web configuration files as often as you want, even if you have already published configurations to your managed Web Security appliances. Importing a configuration file to a Configuration Master completely overwrites the settings associated with the selected Configuration Master. In addition, the security services settings on the Security Services Display page are set to match the imported configuration.

Note If you attempt to import a configuration file that uses an older set of the URL Categories than the Security Management appliance has, the load will fail.

Step 1 Save a configuration file from the Web Security appliance.

Step 2 On the Security Management appliance, choose **Web > Utilities > Configuration Masters**.

Step 3 In the Options column, click **Import Configuration**.

Step 4 From the Select Configuration drop-down list, select **Web Configuration File**.

Step 5 In the New Master Defaults section, click **Browse** and select a valid configuration file from a Web Security appliance.

Step 6 Click **Import File.**

Step 7 Click **Import.**

Configuring Web Security Features Directly in Configuration Masters

You can configure the following functionality in a Configuration Master, depending on the version:

• Identities / Identification Profiles • SaaS Policies • Decryption Policies • Routing Policies • Access Policies • Web Traffic Tap Policies **Note** To define Web Traffic Tap Policies, you must enable the Web Traffic Tap feature in the Web Securiy appliacne. • Overall Bandwidth Limits	• Cisco Data Security • Outbound Malware Scanning • External Data Loss Prevention	• SOCKS Policies • Custom URL Categories • Defined Time Ranges/ and Quotas • Bypass Settings • L4 Traffic Monitor

To configure settings for each feature directly in a configuration master, choose **Web > Configuration Master** *<version>* **>** *<feature>* .

Except for the few items described in SMA-Specific Differences when Configuring Features in Configuration Masters , on page 9, instructions for configuring features in a Configuration Master are the same as instructions for configuring the same features on the Web Security appliance. For instructions, see the online help in your

Web Security appliance or the AsyncOS for Cisco Web Security Appliances User Guide for the AsyncOS version corresponding to the Configuration Master version. If necessary, consult the following topic to determine the correct Configuration Master for your Web Security appliance: Determine the Configuration Master Versions to Use, on page 4.

All versions of Web Security user guides are available from https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html.

SMA-Specific Differences when Configuring Features in Configuration Masters

When you configure a feature in a Configuration Master, note the following differences from configuring the same feature directly on the Web Security appliance.

Table 1: Feature Configuration: Differences between Configuration Master and Web Security Appliance

Feature or Page	Details
All features, especially new features in each release	For each feature that you configure in a Configuration Master, you must enable the feature in the Security Management appliance under Web > Utilities > Security Services Display. For more information, see Ensuring that Features are Enabled Consistently , on page 10.
Identities/Identification Profiles	• See Tip for Working with Identities/Identification Profiles in Configuration Masters , on page 10. • The **Identify Users Transparently** option when adding or editing an Identity/Identification Profile is available when a Web Security appliance with an authentication realm that supports transparent user identification has been added as a managed appliance.
Policies that use a Cisco Identity Services Engine (ISE) to identify users	Secure Group Tag (SGT) information is updated from the Web Security appliances approximately every five minutes. The management appliance does not communicate directly with the ISE server. To update the list of SGTs on demand, select **Web > Utilities > Web Appliance Status**, click a Web Security appliance that is connected to the ISE server, then click **Refresh Data**. Repeat as needed for other appliances. The common deployment scenario is that a company has only one ISE server (this is the whole point of ISE) that all WSAs connect to. Multiple ISE servers with different data are not supported.
Access Policies > Edit Group	When you configure the Identities /Identification Profiles and Users option in the Policy Member Definition section, the following applies if you use external directory servers: When you search for groups on the Edit Group page, only the first 500 matching results are displayed. If you do not see the desired group, you can add it to the “Authorized Groups” list by entering it in the Directory search field and clicking the **Add** button.
Access Policies > Web Reputation and Anti-Malware Settings	
SaaS Policies	The authentication option “Prompt SaaS users who have been discovered by transparent user identification” is available only when a Web Security appliance with an authentication realm that supports transparent user identification has been added as a managed appliance.

Tip for Working with Identities/Identification Profiles in Configuration Masters

When creating an Identity/Identification Profile on the Security Management appliance, you have the option of making it apply only to specific appliances. So for example, if you purchase a Security Management appliance and want to preserve the existing Web Security appliance configurations and the policies that were created for each Web Security appliance, you must load one file into the machine, and then add policies from other machines by hand.

One way to accomplish this is to make a set of Identities/Identification Profiles for each appliance, then have policies which refer to those Identities/Identification Profiles. When the Security Management appliance publishes the configuration, those Identities/Identification Profiles and the policies which refer to them will automatically be removed and disabled. Using this method, you do not have to configure anything manually. This is essentially a 'per-appliance' Identity/Identification Profile.

The only challenge with this method is if you have a default policy or Identity/Identification Profile that differs between sites. For example, if you have a policy set for "default allow with auth" at one site and a "default deny" at another. At this point you will need to create per-appliance Identities/Identification Profiles and policies just above the default; essentially creating your own "default" policy.

Ensuring that Features are Enabled Consistently

Before you publish a Configuration Master, you should ensure that it will publish and that the intended features will be enabled and configured as you expect them to be after publishing.

To do this, do both of the following:

- Comparing Enabled Features , on page 10
- Enabling Features to Publish , on page 11

Note If multiple Web Security appliances with different features enabled are assigned to the same Configuration Master, you should publish to each appliance separately, and perform these procedures before each publish.

Comparing Enabled Features

Verify that the features enabled on each Web Security appliance match the features enabled for the Configuration Master associated with that appliance.

Note If multiple Web Security appliances with different features enabled are assigned to the same Configuration Master, you should publish to each appliance separately, and perform this check before each publish.

Step 1 On the Security Management appliance, choose **Web > Utilities > Web Appliance Status**.

Step 2 Click the name of a Web Security appliance to which you will publish a Configuration Master.

Step 3 Scroll to the **Security Services** table.

Step 4 Verify that the Feature Keys for all enabled features are active and not expired.

Step 5 Compare the settings in the **Services** columns:

The **Web Appliance Service** column and the **Is Service Displayed on Management Appliance?** column should be consistent.

- Enabled = Yes
- Disabled and Not Configured = No or Disabled.
- N/A = Not Applicable. For example, the option may not be configurable using a Configuration Master, but is listed so that you can see the Feature Key status.

Configuration mismatches will appear in red text.

What to do next

If the enabled/disabled settings for a feature do not match, do one of the following:

- Change the relevant setting for the Configuration Master. See Enabling Features to Publish , on page 11.
- Enable or disable the feature on the Web Security Appliance. Some changes may impact multiple features. See the information about the relevant feature in the AsyncOS for Cisco Web Security Appliances User Guide.

Enabling Features to Publish

Enable the features for which you want to publish settings using a Configuration Master.

Before you begin

Determine which features must be enabled and disabled. See Comparing Enabled Features , on page 10.

Step 1 On the Security Management appliance, choose **Web > Utilities > Security Services Display**.

Step 2 Click **Edit Settings**.

The Edit Security Services Display page lists the features that appear in each Configuration Master.

"N/A" alongside a feature indicates that the feature is not available in that Configuration Master version.

Note Web Proxy is not listed as a feature, because it is assumed that the Web Proxy is enabled in order to execute any of the managed policy types on the Web Security appliances. If the Web Proxy is disabled, any policies published to the Web Security appliances will be ignored.

Step 3 (Optional) Hide Configuration Masters that you will not use. For instructions and cautions, see Disabling Unused Configuration Masters , on page 12 .

Step 4 For each Configuration Master that you will use, select or uncheck the Yes check box for each feature to enable.

Special notes for certain features (available options vary by Configuration Master version):

- Transparent Mode. If you use Forward mode, the proxy bypass feature will not be available.
- HTTPS Proxy. HTTPS proxy must be enabled in order to configure decryption policies.
- Upstream Proxy Groups. Upstream proxy groups must be available on your Web Security appliances if you want to use routing policies.

Step 5 Click **Submit.** The GUI displays specific warning messages if the changes you made to the security services settings will affect policies configured on your Web Security appliances. If you are sure that you want to submit your changes, click **Continue.**

Step 6 On the **Security Services Display** page, confirm that **Yes** appears alongside each option that you selected.

Step 7 Commit your changes.

What to do next

- Verify that all features are now correctly enabled or disabled for the appliance to which you will publish. See Comparing Enabled Features , on page 10.
- On each Web Security appliance to which you will publish, make sure the features are enabled consistently with the features you have enabled for the Configuration Master.

Disabling Unused Configuration Masters

You can choose not to display unused Configuration Masters.

However, at least one Configuration Master must be enabled.

Note When a Configuration Master is disabled, all references to it are removed from the GUI including the corresponding Configuration Master tab. Pending publish jobs that use the Configuration Master are deleted, and all Web Security appliances assigned to the hidden Configuration Master are re-categorized as not assigned.

Step 1 On the Security Management appliance, choose **Web > Utilities > Security Services Display**.

Step 2 Click **Edit Settings**.

Step 3 Uncheck the checkbox(es) for unused Configuration Masters

Step 4 Submit and commit your changes.

Setting Up to Use Advanced File Publishing

If your system is set up to use Configuration Masters, it is already set up for Advanced File Publishing.

Otherwise, complete procedures in the following topics, which apply to Advanced File Publishing as well as to publishing Configuration Masters.

- Enabling Centralized Configuration Management on the Security Management Appliance, on page 4
- Initializing Configuration Masters , on page 4
- About Associating Web Security Appliances to Configuration Masters, on page 5

Publishing Configurations to Web Security Appliances

- Publishing a Configuration Master , on page 13

• Publishing Configurations Using Advanced File Publishing, on page 16

Publishing a Configuration Master

After editing or importing settings in a Configuration Master, you can publish them to the Web Security appliances associated with the Configuration Master.

• Before You Publish a Configuration Master , on page 13
• Publishing a Configuration Master Now , on page 14
• Publishing a Configuration Master Later , on page 15
• Publishing a Configuration Master Using the Command Line Interface, on page 16

Before You Publish a Configuration Master

Publishing a Configuration Master overwrites existing policy information on the Web Security appliances associated to that Configuration Master.

For information about which settings you can configure using a Configuration Master, see Determining the Correct Configuration Publishing Method , on page 1.

All Publishing Jobs

- (First time only) You must follow the procedures in Setting Up Configuration Masters to Centrally Manage Web Security Appliances , on page 2.
- To ensure that the Configuration Master will publish and that the intended set of features will be enabled after publishing, verify the feature sets of each Web Security appliance and the associated Configuration Master and make any needed changes. See Comparing Enabled Features , on page 10 and if necessary, Enabling Features to Publish , on page 11. If you publish configurations for features that are not enabled on the target appliance, those configurations are not applied.

If different features are enabled on different Web Security appliances assigned to the same Configuration Master, you must publish to each appliance separately, and verify and enable features before each publish.

To identify configuration mismatches encountered during publishing, see Viewing Publish History, on page 18 .

- Save a configuration file from each target Web Security appliance before publishing, so that you can restore the existing configuration in case of problems with the published configuration. See the AsyncOS for Cisco Web Security Appliances User Guide for details.
- Any change that would cause a Web proxy restart when committed on the Web Security appliance will also cause a proxy restart when you publish it from the Security Management appliance. You will receive a warning in these situations.

Web Proxy restarts temporarily interrupt web security services.

- When you publish any change to an Identity/Identification Profile, all end-users must re-authenticate.

Special Situations

- If you have reverted AsyncOS on the target Web Security appliance, you may need to associate a different Configuration Master with that appliance.
- If you publish a Configuration Master to a Web Security appliance that does not have a realm configured with Transparent User Identification enabled, but you have selected Transparent User Identification in an Identity /Identification Profile or SaaS Policy:

- For Identities/Identification Profiles, Transparent User Identification is disabled and the Require Authentication option is selected instead.
- For SaaS Policies, the Transparent User Identification option is disabled and the default option (Always prompt SaaS users for proxy authentication) is selected instead.

- When you publish External DLP policies from a Security Management appliance to multiple Web Security appliances that are not configured for RSA servers, the Security Management appliance will send the following publish status warning:

"**The Security Services display settings configured for Configuration Master** <*version*> **do not currently reflect the state of one or more Security Services on Web Appliances associated with this publish request. The affected appliances are: "<***WSA Appliance Names***>". This may indicate a misconfiguration of the Security Services display settings for this particular Configuration Master. Go to the Web Appliance Status page for each appliance provides a detailed view to troubleshooting this issue. Do you want to continue publishing the configuration now?"**

If you decide to continue to publish, the Web Security appliance that is not configured for the RSA servers will receive the External DLP policies, but these policies will be disabled.The Web Security appliance External DLP page will not show the published policies if External DLP Server is not configured.

If the Scheme in the Identity /Identification Profile in the Configuration Master Was:	Then the Scheme in the Identity /Identification Profile on the Web Security Appliance Becomes
Use Kerberos	Use NTLMSSP or Basic
Use Kerberos or NTLMSSP	Use NTLMSSP
Use Kerberos or NTLMSSP or Basic	Use NTLMSSP or Basic

Publishing a Configuration Master Now

Before you begin

See important requirements and information in Before You Publish a Configuration Master , on page 13.

Step 1 On the Security Management appliance, choose **Web > Utilities > Publish to Web Appliances.**

Step 2 Click **Publish Configuration Now.**

Step 3 "System-generated job name" is selected by default, or enter a user-defined job name (80 characters or fewer).

Step 4 Select the Configuration Master to publish.

Step 5 Select the Web Security appliances to which you want to publish the Configuration Master. Choose "All assigned appliances" to publish the configuration to all appliances assigned to the Configuration Master.

or

Choose "Select appliances in list" to display the list of appliances assigned to the Configuration Master. Select the appliances to which you want to publish the configuration.

Step 6 Click **Publish.**

Red progress bars and text on the Publish in Progress page indicate that an error occurred during publishing. If another job is currently publishing, then your request will be executed when the previous job is complete.

Note Details of the job in progress also appear on the **Web > Utilities > Publish to Web Appliances** page. Click **Check Progress** to access the Publish in Progress page.

What to do next

Check to be sure your publish was completely successful. See Viewing Publish History, on page 18. Items that were not published completely will be noted.

Publishing a Configuration Master Later

Before you begin

See important requirements and information in Before You Publish a Configuration Master , on page 13.

Step 1 On the Security Management appliance, choose **Web > Utilities > Publish to Web Appliances**.

Step 2 Click **Schedule a Job.**

Step 3 "System-generated job name" is selected by default, or enter a user-defined job name (80 characters or fewer).

Step 4 Enter the date and time when you want to publish the Configuration Master.

Step 5 Select the Configuration Master to publish.

Step 6 Select the Web Security appliances to which you want to publish the Configuration Master. Choose "All assigned appliances" to publish the configuration to all appliances assigned to the Configuration Master.

or

Choose "Select appliances in list" to display the list of appliances assigned to the Configuration Master. Select the appliances to which you want to publish the configuration.

Step 7 Click **Submit.**

Step 8 View a list of scheduled jobs on the **Web > Utilities > Publish to Web Appliances** page. To edit a scheduled job, click the name of the job. To cancel a pending job, click the corresponding trash can icon and confirm that you want to delete the job.

Step 9 You may want to create a reminder for yourself (for example, in your calendar) to check after the scheduled publish time to be sure that your publish was completely successful.

Note If you reboot or upgrade the appliance before the scheduled publishing job occurs, you must reschedule the job.

What to do next

Check to be sure your publish was completely successful. See Viewing Publish History, on page 18. Items that were not published completely will be noted.

Publishing a Configuration Master Using the Command Line Interface

Note See important requirements and information in Before You Publish a Configuration Master , on page 13.

The Security Management appliance provides you with the ability to publish changes through a Configuration Master using the following CLI command:

publishconfig config_master [--*job_name*] [--*host_list* | *host_ip*]

where **config_master** is a supported configuration master version. This keyword is required. The option *job_name* is optional and will be generated if it is not specified.

The option *host_list* is a list of host names or IP addresses for Web Security appliances to be published, and will be published to all hosts assigned to the Configuration Master if not specified. The option *host_ip* can be multiple host IP addresses, each separated by a comma.

To verify that the **publishconfig** command was successful, check the **smad_logs** file. You can also verify that the publish history was successful from the Security Management appliance GUI by choosing **Web > Utilities > Web Appliance Status**. From this page choose the web appliance that you want the publish history details. Additionally, you can go the Publish History page: **Web > Utilities > Publish > Publish History**.

Publishing Configurations Using Advanced File Publishing

Use advanced file publish to push a compatible XML configuration file from your local file system to managed Web Security appliances.

For information about which settings you can configure using Advanced File Publishing, see Determining the Correct Configuration Publishing Method , on page 1.

To perform an advanced file publish:

- Advanced File Publish: Publish Configuration Now, on page 16
- Advanced File Publish: Publish Later, on page 17

Advanced File Publish: Publish Configuration Now

Before you begin

- Verify that the version of the configuration that you will publish is compatible with the AsyncOS version of the appliance to which you publish. See the Compatibility Matrix at http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html.
- On each destination Web Security appliance, back up the existing configuration on your Web Security appliance to a configuration file. See the AsyncOS for Cisco Web Security Appliances User Guide for details.

Step 1 From the source Web Security appliance, save a Configuration File.

For instructions on saving a configuration file from a Web Security appliance, see the AsyncOS for Cisco Web Security Appliances User Guide.

Step 2 On the Security Management appliance window, choose **Web > Utilities > Publish to Web Appliances**.

Step 3 Click **Publish Configuration Now.**

Step 4 "System-generated job name" is selected by default, or enter a job name (up to 80 characters).

Step 5 For **Configuration Master to Publish**, select **Advanced file options**.

Step 6 Click **Browse** to select the file that you saved in Step 1.

Step 7 From the Web Appliances drop-down list, choose **Select appliances in list** or **All assigned to Master** and then select the appliances to which you want to publish the configuration file.

Step 8 Click **Publish.**

Advanced File Publish: Publish Later

Before you begin

- Verify that the version of the configuration that you will publish is compatible with the AsyncOS version of the appliance to which you publish. See the Compatibility Matrix at http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html.
- On each destination Web Security appliance, back up the existing configuration on your Web Security appliance to a configuration file. See the AsyncOS for Cisco Web Security Appliances User Guide for details.

Step 1 From the source Web Security appliance, save a Configuration File.

For instructions on saving a configuration file from a Web Security appliance, see the AsyncOS for Cisco Web Security Appliances User Guide.

Step 2 On the Security Management appliance, choose **Web > Utilities > Publish to Web Appliances**.

Step 3 Click **Schedule a Job.**

Step 4 **System-generated job name** is selected by default, or enter a job name (up to 80 characters).

Step 5 Enter the date and time when you want to publish the configuration.

Step 6 For **Configuration Master to Publish**, select **Advanced file options**, then click **Browse** to select the configuration file that you saved in Step 1.

Step 7 From the Web Appliances drop-down list, choose **Select appliances in list** or **All assigned to Master** and then select the appliances to which you want to publish the configuration file.

Step 8 Click **Publish.**

Viewing Status and History of Publishing Jobs

To View	Do This
A list of publishing jobs that are scheduled but have not yet occurred	Choose **Web > Utilities > Publish to Web Appliances** and look in the **Pending Jobs** section.
A list of the last published configuration per appliance	Choose **Web > Utilities > Web Appliance Status** and look at the **Last Published Configuration** information.

To View	Do This
The status of a publishing job that is currently in progress	Choose **Web > Utilities > Publish to Web Appliances** and look in the **Publishing Progress** section.
History of all or any publishing jobs to all or any appliances	See Viewing Publish History

Viewing Publish History

Viewing the publish history is useful for checking for errors that may have occurred during publishing, or to identify mismatches between configured functionality and features enabled on target appliances.

Step 1 On the Security Management appliance, choose **Web > Utilities > Publish History**.

Step 2 To view additional details about a particular job, click the specific job name in the Job Name column.

Step 3 View more information:

- To view status details about a particular appliance in the job, click a **Details** link.

The Web Appliance Publish Details page appears.

- To view additional details about a particular appliance in the job, click the appliance name.

The **Web > Utilities > Web Appliance Status** page appears.

Centralized Upgrade Management

You can simultaneously upgrade multiple Web Security appliances (WSAs) using a single Security Management Appliance (SMA). You also can apply a different software upgrade to each WSA.

- Setting Up Centralized Upgrade Management for Web Security Appliances, on page 18
- Selecting and Downloading WSA Upgrades, on page 20
- Using the Install Wizard, on page 21

Setting Up Centralized Upgrade Management for Web Security Appliances

Follow these steps to configure the Centralized Upgrade service on this Security Management Appliance:

- Enable the Centralized Upgrade Manager, on page 19
- Adding the Centralized Upgrade Service to Each Managed Web Security Appliance, on page 19

Enable the Centralized Upgrade Manager

Before you begin

- All Web Security appliances should be configured and working as expected before you enable centralized upgrade management.
- You must enable centralized upgrades individually on each managed Web Security appliance that will receive centralized upgrades.

Note To enable Centralized Upgrades in the CLI, use

```
applianceconfig > services > [...] > Enable Centralized Upgrade >
Y
```

- Be sure the appropriate feature key is installed on the Security Management Appliance.

Step 1 On the Security Management appliance, select the **Management Appliance** page, and then choose **Centralized Services > Centralized Upgrade Manager**.

Step 2 Click **Edit Settings**.

Step 3 Check **Enable**.

Step 4 Submit and commit your changes.

Adding the Centralized Upgrade Service to Each Managed Web Security Appliance

After enabling the Centralized Upgrade Manager on the Security Management appliance, you must add the desired Web Security appliance(s) to the Upgrade Manager roster by enabling Centralized Upgrades on the individual managed WSA(s).

Step 1 On the Security Management appliance, select the **Management Appliance** page, and then choose **Centralized Services > Security Appliances**.

Step 2 If you have not yet added Web Security appliances, or you need to add additional appliances for centralized upgrade management:

a) Click **Add Web Appliance**.

b) In the Appliance Name and IP Address text fields, type the appliance name and the IP address for the Management interface of the Web Security appliance.

Note A DNS name may be entered in the IP Address text field, however, it will be resolved to an IP address when you click **Submit**.

c) Be sure to check **Centralized Upgrades**.

d) Click **Establish Connection**.

e) Enter the user name and passphrase for an administrator account on the appliance to be managed, then click **Establish Connection**.

Note You enter the login credentials to pass a public SSH key for file transfers from the Security Management appliance to the remote appliance. The login credentials are not stored on the Security Management appliance.

Wait for the Success message to appear above the table on the page.

f) Click Test Connection.

Read test results above the table.

g) Click **Submit**.

Repeat this procedure for each WSA you want to add to the managed Web Security appliance list while simultaneously enabling Centralized Upgrade management.

Step 3 To enable Centralized Upgrade management on a WSA already on this list of managed appliances:

a) Click the name of the Web Security appliance to open its Edit Web Security Appliance Settings page.
b) Select **Centralized Upgrades** in the WSA Centralized Services section.
c) Click **Submit**.

Repeat this procedure for each WSA on which you want to enable Centralized Upgrade management.

Step 4 Commit your changes.

What to do next

See About Adding Managed Appliances for more information about adding to and editing the list of managed appliances.

Selecting and Downloading WSA Upgrades

Step 1 On the Security Management appliance, select the **Web** page, and then choose **Utilities > Centralized Upgrade**.

Any appliances recently selected for upgrade, and the upgrade status, are listed.

Step 2 Click the **Upgrade Appliances** button on the Centralized Upgrade page.

All managed WSAs which can be upgraded are listed.

Step 3 Select each Web Security appliance to be upgraded by checking the box preceding its name in the list.

Step 4 Click either **Download Wizard** or **Download and Install Wizard**.

The Download Wizard lets you select upgrade packages for download to the selected WSA(s); this operation is download-only—you can install a downloaded package and restart each system later.

The Download and Install Wizard lets you select upgrade packages for download and immediate installation on the selected WSA(s). After installation, each system is restarted automatically.

Step 5 The Fetch Upgrades page of the launched wizard appears; when all available upgrades have been fetched for the selected WSAs (Completed Fetching Available Upgrades appears in the **Status** column of the WSA matrix), click **Next** to continue.

Step 6 The Available Upgrades page lists all available upgrade builds for each selected WSA; select up to five for comparison, and then click **Next**.

Step 7 The wizard's Upgrade Selection page presents a compatibility matrix of selected upgrades for each WSA; check the desired upgrade build for each WSA and then click **Next**.

Step 8 The Summary page lists summary information for each selected WSA and upgrade build; click **Next** to continue the wizard.

Step 9 Following a series of download checks such as WSA connection status, the Review page provides listings of download status for each WSA. Click **Begin Download** to being downloading an upgrade package to each selected WSA.

The Centralized Upgrade page displays download status information throughout the process.

What to do next

- **Download Wizard** – If you clicked this button at the beginning of this procedure, when download is complete, refresh the Centralized Upgrade page by choosing **Web > Utilities > Centralized Upgrade**, or by clicking the refresh-page button in your browser window.

  In addition to the listing of all managed WSAs which can be upgraded, another section of the Centralized Upgrade page now lists all WSAs to which upgrade packages have been downloaded.(You can click the trash can button displayed with each entry to delete the downloaded upgrade package from that WSA.)

  At any time you can select one or more WSAs in this list and then click Install Wizard to begin installation of the downloaded upgrade package on each selected WSA; when installation is complete on a WSA, it is restarted. See Using the Install Wizard, on page 21 for information about using this wizard.

- **Download and Install Wizard** – If you clicked this button at the beginning of this procedure, when download is complete, upgrade installation begins automatically; see Using the Install Wizard, on page 21, beginning with Step 2, for information about this process. When installation is complete, the WSA is restarted.

Using the Install Wizard

When the Install Wizard begins, whether automatically as part of the Download and Install process, or when you click the Install Wizard button on the Centralized Upgrade page after selecting one or more WSAs with downloaded but not-yet-installed upgrade packages, follow these step to configure installation.

Step 1 If installing previously downloaded upgrade packages:

a) Select the desired WSAs in the Web Appliances with Downloaded AsyncOS Versions section of the Centralized Upgrade page (**Web > Utilities > Centralized Upgrade**).

b) Click **Install Wizard**.

Step 2 On the Upgrade Preparation page of the wizard, for each selected WSA:

- Check **Save the current configuration to the configuration directory before upgrading** if you want a back-up copy of the WSA's current configuration saved to that system's `configuration` directory.
- If the **Save current configuration** option is checked, you can check **Mask passphrases in the configuration file** to have all current-configuration passphrases masked in the back-up copy. Note that the **Load Configuration** command cannot be used to reload back-up files with masked passphrases.
- If the **Save current configuration** option is checked, you can enter one or more email addresses into the **Email file** to field; a copy of the back-up configuration file is mailed to each address. Separate multiple addresses with commas.

Step 3 Click **Next**.

Step 4 The Upgrade Summary page lists upgrade-preparation information for each selected WSA; click **Next** to continue the wizard.

Step 5 Following a series of device checks such as connection status, the Review page provides a listing of installation status for each WSA. You can deselect devices that are showing an error. Click **Begin Install** to begin installing an upgrade package to each selected WSA.

You are returned to the Centralized Upgrade page where installation status information is displayed.

Note Each WSA will be restarted upon completion of the installation.

What to do next

Note Alternatively, you also can run the installer for any previously downloaded package from the WSA itself. That is, the downloaded upgrade package is listed on the WSA's **System Administration > System Upgrade** page, along with an Install button. See "Upgrading and Updating AsyncOS and Security Service Components" in the Cisco Web Security Appliances User Guide for more information.

Viewing Web Security Appliance Status

- Comparing Enabled Features , on page 10
- Viewing a Summary of Status of Web Appliances , on page 22
- Viewing Status of Individual Web Security Appliances, on page 22
- Web Appliance Status Details , on page 23

Viewing a Summary of Status of Web Appliances

The **Web > Utilities > Web Appliance Status** page provides a high-level summary of the Web Security appliances connected to your Security Management appliance.

The Web Appliance Status page displays a list of your connected Web Security appliances, including appliance name, IP address, AsyncOS version, last published configuration information (user, job name, and configuration version), number of security services enabled or disabled, and total number of connected appliances (up to 150). The warning icon indicates when attention is required for one of your connected appliances.

Viewing Status of Individual Web Security Appliances

The Appliance Status page provides a detailed view into the status of each connected appliance.

To view details for a managed Web Security appliance on the Web Appliance Status page, click the name of the appliance.

Status information includes general information about the connected Web Security appliances, their published configuration, publish history, feature key status, and so forth.

Note Only machines with support for centralized management will have data available for display.

Note Warning messages will appear if different versions of the Acceptable Use Control Engine on the Web Security appliance do not match with those on the Security Management appliance. An 'N/A' is displayed if the service is disabled or not present on the Web Security appliance.

Web Appliance Status Details

Most of the information on this page is pulled from the Web Security appliance:

- System status information (uptime, appliance model and serial number, AsyncOS version, build date, AsyncOS installation date and time, and host name)
- Configuration publish history (publish date/time, job name, configuration version, result of the publish, and user)
- Centralized reporting status, including time of last attempted data transfer
- Status of features on Web Security appliances (whether each feature is enabled, status of feature keys)
- Acceptable Use Controls Engine versions on the managed and managing appliances
- AnyConnect Secure Mobility settings on the Web Security appliance
- Cisco Identity Services Engine (ISE) servers to which this Web Security appliance is connected.
- Proxy settings (upstream proxies and HTTP ports to proxy) for the Web Security appliance
- Authentication service information (servers, schemes, realms, and sequences; whether Transparent User Identification is supported; and whether to block or permit traffic if authentication fails)

Tip It can take several minutes for the Web Appliance Status page to reflect recent configuration changes that occurred on the Web Security appliances. To refresh the data immediately, click the **Refresh Data** link. The time stamp on the page tells you when the data was last refreshed.

Preparing For and Managing URL Category Set Updates

In order to ensure that your system has the latest set of predefined URL categories available for managing web usage, the URL category set for Web Usage Controls (WUC) may be updated occasionally: By default, Web Security appliances download URL category set updates automatically from Cisco, and the Security Management appliance receives these updates automatically within a few minutes from managed Web Security appliances.

Because these updates can impact existing configurations and appliance behavior, you should prepare in advance for these updates and take action after they occur.

Actions that you should take include the following:

- Understand the Impacts of URL Category Set Updates , on page 24

Understand the Impacts of URL Category Set Updates

When URL category set updates occur, they may change the behavior of existing policies in Configuration Masters.

For essential information about actions you should take before and after URL category set updates, see the "Managing Updates to the Set of URL Categories" section of the "URL Filters" chapter in the AsyncOS for Cisco Web Security Appliances User Guide at the link provided in Documentation. Category descriptions are in the "URL Category Descriptions" section of the same chapter.

Ensure That You Will Receive Notifications and Alerts about URL Category Set Updates

To Receive	Do This
Advance notification of URL category set updates	Sign up now to receive notifications about your Cisco Content Security appliances, which will include notifications about URL category set updates. See Cisco Notification Service.
Alerts when URL category set updates have affected existing policy settings	Go to **Management Appliance > System Administration > Alerts** and make sure that you are configured to receive Warning-level alerts in the System category. More information about alerts is in Managing Alerts.

Specify Default Settings for New and Changed Categories

Before URL category set updates occur, you should specify default actions for new and merged categories in each policy that offers URL filtering, or import a configuration from a Web Security appliance that has these settings already configured.

For more information, see the "Choosing Default Settings for New and Changed Categories" section in the "URL Filters" chapter of the AsyncOS for Cisco Web Security Appliances User Guide or the online help on the Web Security appliance.

When the URL Category Set is Updated, Check Your Policy and Identity/Identification Profile Settings

URL category set updates trigger two types of alerts:

- Alerts about category changes
- Alerts about policies that have changed or been disabled as a result of category changes

When you receive alerts about URL category set changes, you should check your existing URL category-based policies and Identities/Identification Profiles to be sure they still meet your policy goals.

For more information about the kinds of changes that might require your attention, see the “Responding to Alerts about URL Category Set Updates” section in the AsyncOS for Cisco Web Security Appliances User Guide.

Application Visibility and Control (AVC) Updates

The SMA automatically uses the version of the AVC engine that exists on the majority of the Web Security appliances that it manages.

Troubleshooting Configuration Management Issues

In Configuration Master Identities/Identification Profiles, Groups Are Not Available

Problem

In **Web > Configuration Master > Identities/Identification Profiles**, the Policy membership definition page doesn't show the Groups option under Selected groups and Users.

Solution

If you have multiple Web Security appliances: On each WSA, in Network > Authentication, make sure Realm Names are unique across all WSAs, unless all settings are identical for same-name realms.

Tip To see realm names for each WSA, go to **Web > Utilities > Web Appliance Status**, click each appliance name, and scroll to the bottom of the details page.

Configuration Master Access Policies Web Reputation and Anti-Malware Settings Page Settings are Not as Expected

Problem

The **Access Policies > Web Reputation and Anti-Malware Settings** page in the configuration master is missing expected settings, including the Web Reputation Score threshold settings and the ability to choose anti-malware scanning engines. Or it includes these settings when you are using Adaptive Security on the Web Security appliance.

Solution

Available options depend on whether Adaptive Security is selected for that configuration master in Web > Utilities > Security Services Display settings.

Troubleshooting Configuration Publishing Failures

Problem

Publishing a configuration fails.

Solution

Look at the **Web > Utilities > Web Appliance Status** page. Publishing fails if:

- There is a discrepancy between the status in the “Web Appliance Service” column and the status in the “Is Service Displayed on Management Appliance?” column.
- Both columns show that the feature is enabled but the corresponding Feature Key is not active (for example, is expired).
- The Configuration Master version should match the AsyncOS version on the Web Security appliance. Publishing an older Configuration Master version to a newer Web Security appliance may fail if settings on the Web Security appliance do not match the settings in the Configuration Master. This can occur even if the Web Appliance Status page does not indicate any discrepancies.

What to do Next:

- Viewing Publish History, on page 18
- Comparing Enabled Features , on page 10
- Enabling Features to Publish , on page 11