Distributing Administrative Tasks

This chapter contains the following sections:

- Working with User Accounts, on page 1
- Managing Custom User Roles for Delegated Administration, on page 6
- Passphrases, on page 14
- Configuring Access to the Email Security Appliance , on page 21
- Displaying Messages to Administrative Users , on page 24
- Managing Secure Shell (SSH) Keys, on page 25
- Monitoring Administrative User Access , on page 28

Working with User Accounts

The Cisco appliance provides two methods for adding user accounts: creating user accounts on the Cisco appliances itself, and enabling user authentication using your own centralized authentication system, which can be either an LDAP or RADIUS directory. You can manage users and connections to external authentication sources on the **System Administration > Users** page in the GUI (or by using the **`userconfig`** command in the CLI). For information about using an external directory to authenticate users, see External Authentication, on page 15.

Optionally, you can enable two-factor authentication for specific user roles through:

- The System Administration > Users page in the web interface. See Two-Factor Authentication, on page 19.
- The `userconfig > twofactorauth` command in the CLI. See the *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances* .

The default user account for the system, admin, has all administrative privileges. The admin user account cannot be deleted, but you can change the passphrase and lock the account.

When you create a new user account, you assign the user to a predefined or a custom user role. Each role contains differing levels of permissions within the system.

Although there is no limit to the number of user accounts that you can create on the appliance , you cannot create user accounts with names that are reserved by the system. For example, you cannot create the user accounts named “operator” or “root.”

User Roles

Table 1: User Roles Listing

User Role	Description
admin	The admin user is the default user account for the system and has all administrative privileges. The admin user account is listed here for convenience, but it cannot be assigned via a user role, and it cannot be edited or deleted, aside from changing the passphrase. Only the admin user can issue the **`resetconfig`** and revert commands.
Administrator	User accounts with the Administrator role have full access to all configuration settings of the system. However, only the admin user has access to the **`resetconfig`** and **`revert`** commands. **Note** AsyncOS does not support multiple administrators configuring the appliance from the GUI simultaneously.
Technician	User accounts with the Technician role can perform system upgrades, reboot the appliance , and manage feature keys. Technicians can also perform the following actions in order to upgrade the appliance : • Suspend email delivery and receiving. • View status of workqueue and listeners. • Save and email configuration files. • Back up safelists and blocklists. Technicians cannot restore these lists. • Disconnect the appliance from a cluster. • Enable or disable remote service access for Cisco technical support. • Raise a support request.
Operator	User accounts with the Operator role are restricted from: • Creating or editing user accounts. • Issuing the **`resetconfig`** command. • Upgrading the appliance . • Issuing the **`systemsetup`** command or running the System Setup Wizard. • Issuing the **`adminaccessconfig`** command. • Performing some quarantine functions (including creating, editing, deleting, and centralizing quarantines). • Modifying LDAP server profile settings other than username and passphrase, if LDAP is enabled for external authentication. Otherwise, they have the same privileges as the Administrator role.
Guest	Users accounts with the Guest role can only view status information and reports. Users with the Guest role can also manage messages in quarantines, if access is enabled in a quarantine. Users with the Guest role cannot access Message Tracking.

User Role	Description
Read-Only Operator	User accounts with the Read-Only Operator role have access to view configuration information. Users with the Read-Only Operator role can make and submit changes to see how to configure a feature, but they cannot commit them. Users with this role can manage messages in quarantines, if access is enabled in a quarantine. Users with this role cannot access the following: • File system, FTP, or SCP. • Settings for creating, editing, deleting, or centralizing quarantines.
Help Desk User	User accounts with the Help Desk User role are restricted to: • Message tracking. • Managing messages in quarantines. Users with this role cannot access to the rest of the system, including the CLI. You need to enable access in each quarantine before a user with this role can manage them.
Custom user role	User accounts with a custom user role can only access email security features assigned to the role. These features can be any combination of DLP policies, email policies, reports, quarantines, local message tracking, encryption profiles, and the Trace debugging tool Trace debugging tool, . The users cannot access system configuration features, including enabling features globally. Only administrators can define custom user roles. See Managing Custom User Roles for Delegated Administration, on page 6 for more information. **Note** Users assigned to custom roles cannot access the CLI.

All roles defined in the above table can access both the GUI and the CLI, except the Help Desk User role and custom user roles, which can only access the GUI.

If you use an LDAP directory to authenticate users, you assign directory groups to user roles instead of individual users. When you assign a directory group to a user role, each user in that group receives the permissions defined for the user role. For more information, see External Authentication, on page 15.

Related Topics

- Managing Users, on page 3

Managing Users

The Users page lists the existing users for the system, including the username, full name, and user type or group.

From the Users page, you can:

- Add new users. For more information, see Adding Users , on page 4.
- Delete users. For more information, see Deleting Users, on page 5.
- Edit users, such as changing a user's passphrase and locking and unlocking a user's account. For more information, see Editing Users, on page 4.

- Force users to change their passphrases. See Force Users To Change Their Passphrases, on page 5.
- Configure user account and passphrase settings for local accounts. For more information, see Configuring Restrictive User Account and Passphrase Settings, on page 15.
- Enable the appliance to use an LDAP or RADIUS directory to authenticate users. For more information, see External Authentication, on page 15.
- Enable two-factor authentication for specific user roles. For more information, see Two-Factor Authentication, on page 19.
- Enable access for non-administrators to DLP Matched Content in Message Tracking. See Controlling Access to Sensitive Information in Message Tracking, on page 5 for more information.

Adding Users

Before You Begin

- Determine the user roles you will use.
  - For descriptions of predefined user roles, see User Roles , on page 2.
  - To create custom roles, see Managing Custom User Roles for Delegated Administration, on page 6.
- Specify your passphrase requirements. See Configuring Restrictive User Account and Passphrase Settings, on page 15.

Procedure

Step 1 Choose **System Administration > Users**.
Step 2 Click **Add User.**
Step 3 Enter a login name for the user. Some words are reserved (such as “operator” or “root”).
Step 4 Enter the user’s full name.
Step 5 Select a predefined or custom user role.
Step 6 Enter a passphrase.
Step 7 Submit and commit your changes.

Editing Users

Use this procedure to change a passphrase, etc.

Procedure

Step 1 Choose **System Administration > Users**.
Step 2 Click the user’s name in the Users listing.
Step 3 Make changes to the user.

Step 4 Submit and commit your changes.

Force Users To Change Their Passphrases

Procedure

Step 1 Choose **System Administration > Users**.

Step 2 Select the users from the Users listing.

Step 3 Click **Enforce Passphrase Change**.

Step 4 Choose whether the users must change the passphrase during the next login or after a specified duration (in days).

Step 5 (Optional) If you are enforcing a passphrase change after a specified duration, set the grace period (in days) to reset the passphrase after the passphrase expires.

Step 6 Click **OK**.

Step 7 Submit and commit your changes.

Deleting Users

Procedure

Step 1 Click the trash can icon corresponding to the user's name in the Users listing.

Step 2 Confirm the deletion by clicking **Delete** in the warning dialog that appears.

Step 3 Commit your changes.

Controlling Access to Sensitive Information in Message Tracking

You may want to restrict administrative access to message details that are likely to include sensitive information:

- Messages that violate Data Loss Prevention (DLP) policies may include information such as corporate confidential information or personal information including credit card numbers and health records. By default, this content is visible to all users who have access to the appliance .
- URLs that are caught by outbreak filters or by content filters that are based on URL reputation or category may also be considered sensitive. By default, only users with Administrator privileges can view this content.

This sensitive content appears in dedicated tabs on the Message Details page for messages listed in Message Tracking results.

You can hide these tabs and their content from administrative users based on their user role. However, although there is an option to hide this sensitive content from users who have the Administrator role, any user with the Administrator role can change these permissions and thus view sensitive information at any time.

Before You Begin

Ensure that you have met the prerequisites for these features. See Displaying URL Details in Message Tracking.

Procedure

Step 1 Go to the **System Administration > Users** page.

Step 2 Under **Access to Sensitive Information in Message Tracking**, click **Edit Settings**.

Step 3 Select the roles for which you want to grant access to each type of sensitive information.

Custom roles without access to Message Tracking can never view this information and thus are not listed.

Step 4 Submit and commit your changes.

What to do next

Related Topics

- Message Tracking Details
- Displaying Sensitive DLP Data in Message Tracking
- Displaying URL Details in Message Tracking

Managing Custom User Roles for Delegated Administration

You can design custom user roles and delegate specific responsibilities to users that align with their roles within your organization, allowing these *delegated administrators* access only to the email security features they are responsible for and not the system configuration features that are not related to their roles. Delegated administration provides more flexible control over your users' access to the email security features on the appliance than the predefined administrator, operator, and help desk user roles.

For example, you may have users who are responsible for managing mail policies for specific domains on the appliance , but you do not want these users to access the system administration and security services configuration features, which the predefined administrator and operator roles grant. You can create a custom user role for mail policy administrators who can grant these users access to the mail policies they manage, along with other email security features that they can use to manage messages processed by these policies, such as Message Tracking and policy quarantines.

Use the **System Administration > User Roles** page in the GUI (or the `userconfig -> role` command in the CLI) to define custom user roles and manage the email security features for which they are responsible, such as mail policies, DLP policies, email reports, and quarantines. For a full list of email security features that delegated administrators can manage, see Assigning Access Privileges, on page 7. Custom roles can also be created when adding or editing a local user account using the **System Administration > Users** page. See Defining a Custom User Role When Adding a User Account, on page 12 for more information.

You should make sure when creating a custom user role so that its responsibilities don't overlap too much with the responsibilities of other delegated administrators. If multiple delegated administrators are responsible for the same content filter, for example, and use the content filter in different mail policies, the changes made to the filter by one delegated administrator may cause unintended side effects for the mail policies managed by other delegated administrators.

When you have created the custom user roles, you can assign local users and external authentication groups to them like any other user role. See Working with User Accounts, on page 1 for more information. Please note that users assigned to custom roles cannot access the CLI.

Related Topics

- Account Privileges Page, on page 7
- Assigning Access Privileges, on page 7
- Defining a Custom User Role, on page 12
- Defining a Custom User Role When Adding a User Account, on page 12
- Updating Responsibilities for a Custom User Role , on page 13
- Editing a Custom User Role, on page 13
- Duplicating a Custom User Role, on page 13
- Deleting a Custom User Role, on page 14

Account Privileges Page

When a delegated administrator logs into the appliance , the Account Privileges page displays links to the security features for which the delegated administrator is responsible and brief descriptions of their access privileges. A delegated administrator can return to this page by selecting Account Privileges in the Options menu. Delegated administrators can also access the features that they manage using the menu at the top of the web page.

The following figure shows an Account Privileges page for a delegated administrator with access to mail policies, email reporting, message tracking, and quarantines.

Figure 1: Account Privileges Page for a Delegated Administrator

Assigning Access Privileges

When creating a custom user role, you define the levels of access to the security features for which delegated administrators are responsible.

The security features available for delegated administrators to manage are:

- Incoming and outgoing mail policies and content filters.

- Data Loss Prevention (DLP) policies.
- Email reporting.
- Message Tracking.
- The Trace debugging tool.
- Spam, policy, virus, and outbreak quarantines.
- Cisco Email Encryption profiles.

After defining the access levels for a custom user role, you need to assign the specific mail policies, content filters, DLP policies, quarantines, or encryption profiles for which the delegated administrators will be responsible.

For example, you can create two different DLP policy administrator roles that are responsible for different DLP policies. One role is only responsible for DLP violations related to company confidentiality and acceptable use, while the other is responsible for DLP violations related to privacy protection. In addition to DLP policies access, these custom user roles can also be assigned privileges for tracking message data and viewing quarantines and reports. They can search for DLP violations related to the policies that they are responsible for in using Message Tracking.

You can view which responsibilities are available to assign to a custom user role by clicking on the links for the assigned privileges in the Custom User Roles for Delegated Administration table on the User Roles page. See Updating Responsibilities for a Custom User Role , on page 13.

Related Topics

- Mail Policies and Content Filters, on page 8
- DLP Policies, on page 9
- Email Reporting, on page 10
- Message Tracking, on page 11
- Trace, on page 11
- Quarantines, on page 11
- Encryption Profiles, on page 11

Mail Policies and Content Filters

The Mail Policies and Content Filters access privileges define a delegated administrator's level of access to the incoming and outgoing mail policies and content filters on the appliance . You can assign specific mail policies and content filters to a custom user role, allowing only the delegated administrators belonging to this role, along with operators and administrators, to manage the mail policies and content filters.

All delegated administrators with this access privilege can view the default incoming and outgoing mail policies but they can only edit these policies if they have full access.

All delegated administrators with access privileges can create new content filters to use with their mail policies. A content filter created by a delegated administrator is available to the other delegated administrators assigned to the custom user role. Content filters that are not assigned to any custom user role are public and can be viewed by all delegated administrators with the mail policy access privilege. Content filters created by operators and administrators are *public* by default. Delegated administrators can enable or disable any existing content filters on mail policies assigned to their custom user role, but they cannot modify or delete public content filters.

If a delegated administrator deletes a content filter used by mail policies other than their own, or if the content filter is assigned to other custom user roles, AsyncOS does not delete the content filter from the system.

AsyncOS instead unlinks the content filter from the custom user role and removes it from the delegated administrator's mail policies. The content filter remains available to other custom user roles and mail policies.

Delegated administrators can use any text resource or dictionary in their content filters, but they cannot access the Text Resources or Dictionaries pages in the GUI to view or modify them. Delegated administrators also cannot create new text resources or dictionaries.

For outgoing mail policies, delegated administrators can enable or disable DLP policies but they cannot customize the DLP settings unless they also have DLP policy privileges.

You can assign one of the following access levels for mail policies and content filters to a custom user role:

- **No access**: Delegated administrators cannot view or edit mail policies and content filters on the appliance .
- **View assigned, edit assigned**: Delegated administrators can view and edit the mail policies and content filters assigned to the custom user role and create new content filters. Delegated administrators can edit a policy's Anti-Spam, Anti-Virus, and Outbreak Filters settings. They can enable their content filters for the policy, as well as disable any existing content filter assigned to the policy, regardless of whether they are responsible for it. Delegated administrators cannot modify a mail policy's name or its senders, recipients, or groups. Delegated administrators can modify the order of the content filters for mail policies assigned to their custom user role.
- **View all, edit assigned**: Delegated administrators can view all mail policies and content filters on the appliance , but they can only edit the ones assigned to the custom user role.

View all, edit all (full access): Delegated administrators have full access to all of the mail policies and content filters on the appliance , including the default mail policies, and have the ability to create new mail policies. Delegated administrators can modify the senders, recipients, and groups of all mail policies. They can also reorder mail policies.

You can assign individual mail policies and content filters to the custom user role using either the Email Security Manager or the Custom User Roles for Delegated Administration table on the User Roles page.

See Updating Responsibilities for a Custom User Role , on page 13 for information on using the Custom User Roles for Delegated Administration table to assign mail policies and content filters.

DLP Policies

The DLP Policies access privileges define a delegated administrator's level of access to the DLP policies via the DLP Policy Manager on the appliance . You can assign DLP policies to specific custom user roles, allowing delegated administrators, in addition to operators and administrators, to manage these policies. Delegated administrators with DLP access can also export DLP configuration files from the Data Loss Prevention Global Settings page.

If a delegated administrator also has mail policy privileges, they can customize the DLP policies. Delegated administrators can use any custom DLP dictionary for their DLP policies, but they cannot view or modify the custom DLP dictionaries.

You can assign one of the following access levels for DLP policies to a custom user role:

- **No access**: Delegated administrators cannot view or edit DLP policies on the appliance .
- **View assigned, edit assigned**: Delegated administrators can use the DLP Policy Manager to view and edit the DLP policies assigned to the custom user role. Delegated administrators cannot rename or reorder DLP policies in the DLP Policy Manager. Delegated administrators can export DLP configurations.
- **View all, edit assigned**: Delegated administrators can view and edit the DLP policies assigned to the custom user role. They can export DLP configurations. They can also view all DLP policies that are not

assigned to the custom user role but they cannot edit them. Delegated administrators cannot reorder DLP policies in the DLP Policy Manager or rename the policy.

- **View all, edit all (full access)**: Delegated administrators have full access to all of the DLP policies on the appliance , including the ability to create new ones. Delegated administrators can reorder DLP policies in the DLP Policy Manager. They cannot change the DLP mode that the appliance uses.

You can assign individual DLP policies to the custom user role using either the DLP Policy Manager or the Custom User Roles for Delegated Administration table on the User Roles page.

See Data Loss Prevention for more information on DLP policies and the DLP Policy Manager.

See Updating Responsibilities for a Custom User Role , on page 13 for information on using the Custom User Roles for Delegated Administration list to assign DLP policies.

Email Reporting

The Email Reporting access privileges define which reports and Email Security Monitor pages a delegated administrator can view, depending on the custom user role's access to mail policies, content filters, and DLP policies. These reports are not filtered for assigned policies; delegated administrators can view reports for mail and DLP policies that for which they are not responsible.

You can assign one of the following access levels for email reporting to a custom user role:

- **No access**: Delegated administrators cannot view reports on the appliance .
- **View relevant reports**: Delegated administrators can view reports on the Email Security Monitor pages related to their Mail Policies and Content Filters and DLP Policies access privileges. Delegated administrators with Mail Policies and Content Filters access privileges can view the following Email Security Monitor pages:
  - Overview
  - Incoming Mail
  - Outgoing Destinations
  - Outgoing Senders
  - Internal Users
  - Content Filters
  - Virus Outbreaks
  - Virus Types
  - Archived Reports

  Delegated administrators with DLP Policies access privileges can view the following Email Security Monitor pages:
  - Overview
  - DLP Incidents
  - Archived Reports
- **View all reports**: Delegated administrators can view all reports and Email Security Monitor pages on the appliance .

See the Using Email Security Monitor chapter for more information on email reporting and the Email Security Monitor.

Message Tracking

The Message Tracking access privileges define whether delegated administrators assigned to the custom user role have access to Message Tracking, including message content that may violate your organization's DLP policies if the DLP Tracking Policies option has been enabled on the **System Administration > Users** page and the custom user role also has DLP policies access privileges.

Delegated administrators can only search for the DLP violations for the DLP policies assigned to them.

See Tracking Messages for more information on Message Tracking.

See Controlling Access to Sensitive Information in Message Tracking, on page 5 for information for allowing delegated administrators access to viewing matched DLP content in Message Tracking.

Trace

The Trace access privileges define whether delegated administrators assigned to the custom user role can use Trace to debug the flow of messages through the system. Delegated administrators with access can run Trace and view all of the generated output. Trace results are not filtered based on the delegated administrator's mail or DLP policy privileges.

See Debugging Mail Flow Using Test Messages: Trace for more information on using Trace.

Quarantines

The Quarantines access privileges define whether delegated administrators can manage assigned quarantines. Delegated administrators can view and take actions on any message in an assigned quarantine, such as releasing or deleting messages, but cannot change the quarantine's configuration (e.g. the size, retention period, etc.), or create or delete quarantines.

You can assign any of the quarantines to the custom user role using either the Monitor > Quarantines page or the Custom User Roles for Delegated Administration table on the User Roles page.

See About Distributing Message Processing Tasks to Other Users and Configuring Administrative User Access to the Spam Quarantine for more information on assigning Quarantine management tasks to administrative users.

See Updating Responsibilities for a Custom User Role , on page 13 for information on using the Custom User Roles for Delegated Administration list to assign quarantines.

Encryption Profiles

The Encryption Profiles access privileges define whether delegated administrators can use encryption profiles assigned to their custom user role when editing content filters or DLP policies. Encryption profiles can only be assigned to custom user roles with mail or DLP policy access privileges. Encryption profiles that are not assigned to a custom role are available for use by all delegated administrators with mail or DLP policy privileges. Delegated administrators cannot view or modify any encryption profiles.

You can assign encryption profiles when creating or editing an encryption profile using the Security Services > IronPort Email Encryption page.

Defining a Custom User Role

User the User Roles page in the GUI (or the userconfig -> role command in the CLI) to define a new user role and assign its access privileges. The User Roles page displays all existing custom user roles on the appliance and the access privileges for each role.

Procedure

Step 1 Choose **System Administration > User Roles**.

Step 2 Click **Add User Role**.

Step 3 Enter a name for the user role.

Step 4 Enter a description of the user role and its privileges.

Step 5 Select the user role's access privileges. (See Assigning Access Privileges, on page 7 for more information on each type of access privilege.)

Step 6 Submit and commit your changes.

Defining a Custom User Role When Adding a User Account

You can create a new custom user role when adding or editing a local user account on the appliance .

See Managing Users, on page 3 for more information on adding a user account.

Procedure

Step 1 Go to the **System Administration > Users** page.

Step 2 Click **Add User**.

Step 3 When creating the user account, select Custom Roles.

Step 4 Select **Add Role**.

Step 5 Enter the name for the new role.

Step 6 Submit the new user account.

AsyncOS displays a notification that the new user account and custom user role have been added.

Step 7 Go to the **System Administration > User Roles** page.

Step 8 Click on the name of the custom user role in the Custom User Roles for Delegated Administration table.

Step 9 Enter a description of the user role and its privileges.

Step 10 Select the user role's access privileges. (See Assigning Access Privileges, on page 7 for more information on each type of access privilege.)

Step 11 Submit and commit your changes.

Updating Responsibilities for a Custom User Role

Procedure

Step 1 Go to the **System Administration > User Roles** page.

Step 2 Click the name of the access privilege for the custom user role you want to update.

AsyncOS displays a list of all the mail policies, content filters, DLP policies, or quarantines available on the appliance , along with the names of any other assigned custom user roles.

Step 3 Select the mail policies, content filters, DLP policies, or quarantines for which you want the delegated administrators assigned to be responsible.

Step 4 Submit and commit your changes.

Editing a Custom User Role

Procedure

Step 1 Go to the **System Administration > User Roles** page.

Step 2 Click the user role's name in the Custom User Roles for Delegated Administration listing.

Step 3 Make changes to the user role.

Step 4 Submit and commit your changes.

Duplicating a Custom User Role

You may want to create multiple custom user roles with similar access privileges but assign different responsibilities to different sets of users. For example, if the appliance handles messages for multiple domains, you may want to create custom user roles with similar access rights but for different mail policies based on the domain. This allows delegated administrators to manage mail policies for their domains without interfering with the responsibilities of other delegated administrators.

Procedure

Step 1 Go to the **System Administration > User Roles** page.

Step 2 Click the duplicate icon corresponding to the user role you want to duplicate in the Custom User Roles for Delegated Administration listing.

Step 3 Change the name of the custom user role.

Step 4 Make any access privilege changes required for the new custom user role.

Step 5 Submit and commit your changes.

Deleting a Custom User Role

When a custom role is deleted, users become unassigned and do not have access to the appliance . If you delete a custom user role that is assigned to one or more users, you do not receive a warning message. You should reassign any users that were assigned to the custom user role that you deleted.

Procedure

Step 1 Go to the **System Administration** > **User Roles** page.

Step 2 Click the trash can icon corresponding to the user role you want to delete in the Custom User Roles for Delegated Administration list.

Step 3 Confirm the deletion by clicking **Delete** in the warning dialog that appears.

Step 4 Commit your changes.

Passphrases

- Changing Your Passphrase, on page 14
- Locking and Unlocking a User Account, on page 14
- Configuring Restrictive User Account and Passphrase Settings, on page 15
- External Authentication, on page 15
- Two-Factor Authentication, on page 19

Changing Your Passphrase

Administrative users can change their own passphrases via the Options > Change Passphrase link at the top of the GUI.

As soon as you submit a new passphrase, you are logged out and taken to the log in screen.

In the CLI, use the passphrase or passwd command to change your passphrase. If you forget the passphrase for the admin user account, contact your customer support provider to reset the passphrase.

The passphrase command requires you to enter the old passphrase for security.

Note Changes to the passphrase take effect immediately and do not require you commit the change.

Locking and Unlocking a User Account

Locking a user account prevents a local user from logging into the appliance . A user account can be locked in one of the following ways:

- AsyncOS locks a user account if the user exceeded the maximum number of failed login attempts defined in the Local User Account & Passphrase Settings section.
- Administrators can manually lock user accounts for security purposes using the System Administration > Users page.

AsyncOS displays the reason why the user account was locked when you view the user account on the Edit User page.

To unlock a user account, open the user account by clicking on the user name in the Users listing and click **Unlock Account**.

To manually lock a local user account, open the user account by clicking on the user name in the Users listing and click **Lock Account**. AsyncOS displays a message saying that the user will be unable to log into the appliance and asks if you want to continue.

You can also configure all local user accounts to lock after users fail to login successfully after a configured number of attempts. For more information, see Configuring Restrictive User Account and Passphrase Settings, on page 15.

Note If you lock the admin account, you can only unlock it by logging in as the admin through a serial communications connection to the serial console port. The admin user can always access the appliance using the serial console port, even when the admin account is locked. See Connecting to the Appliance for more information on accessing the appliance using the serial console port.

Configuring Restrictive User Account and Passphrase Settings

You can define user account and passphrase restrictions to enforce organizational passphrase policies. The user account and passphrase restrictions apply to local users defined on the appliance . You can configure the following settings:

- **User account locking.** You can define how many failed login attempts cause the user to be locked out of the account.
- **Passphrase lifetime rules.** You can define how long a passphrase can exist before the user is required to change the passphrase after logging in.
- **Passphrase rules.** You can define what kinds of passphrases users can choose, such as which characters are optional or mandatory.

You define user account and passphrase restrictions on the System Administration > Users page in the Local User Account & Passphrase Settings section.

External Authentication

If you store user information in an LDAP or RADIUS directory on your network, you can configure your appliance to use the external directory to authenticate users who log in to the appliance . To set up the appliance to use an external directory for authentication, use the System Administration > Users page in the GUI or the userconfig command and the external subcommand in the CLI.

When external authentication is enabled and a user logs into the appliance , the appliance first determines if the user is the system defined “admin” account. If not, then the appliance checks the first configured external server to determine if the user is defined there. If the appliance cannot connect to the first external server, the appliance checks the next external server in the list.

For LDAP servers, if the user fails authentication on any external server, the appliance tries to authenticate the user as a local user defined on the appliance . If the user does not exist on any external server or on the appliance , or if the user enters the wrong passphrase, access to the appliance is denied.

If an external RADIUS server cannot be contacted, the next server in the list is tried. If all servers cannot be contacted, the appliance tries to authenticate the user as a local user defined on the appliance . However, if an external RADIUS server rejects a user for any reason, such as an incorrect passphrase or the user being absent, access to the appliance is denied.

Related Topics

- Enabling LDAP Authentication, on page 16
- Enabling RADIUS Authentication, on page 17
- Enable SAML Authentication, on page 18

Enabling LDAP Authentication

In addition to using an LDAP directory to authenticate users, you can assign LDAP groups to Cisco user roles. For example, you can assign users in the IT group to the Administrator user role, and you can assign users in the Support group to the Help Desk User role. If a user belongs to multiple LDAP groups with different user roles, AsyncOS grants the user the permissions for the most restrictive role. For example, if a user belongs to a group with Operator permissions and a group with Help Desk User permissions, AsyncOS grants the user the permissions for the Help Desk User role.

Note If an external user changes the user role for their LDAP group, the user should log out of the appliance and then log back in. The user will have the permissions of their new role.

Before You Begin

Define an LDAP server profile and an external authentication query for the LDAP server. For more information, see LDAP Queries

Procedure

Step 1 Choose **System Administration** > **Users**.

Step 2 Scroll down to the **External Authentication** section.

Step 3 Click **Enable**.

Step 4 Select the **Enable External Authentication** check box.

Step 5 Select **LDAP** for the authentication type.

Step 6 Enter the amount of time to store external authentication credentials in the web user interface.

Step 7 Select the LDAP external authentication query that authenticates users.

Step 8 Enter the number of seconds that the appliance waits for a response from the server before timing out.

Step 9 Enter the name of a group from the LDAP directory that you want the appliance to authenticate, and select the role for the users in the group.

Step 10 Optionally, click **Add Row** to add another directory group. Repeat steps 9 and 10 for each directory group that the appliance authenticates.

Step 11 Submit and commit your changes.

Enabling RADIUS Authentication

You can also use a RADIUS directory to authenticate users and assign groups of users to Cisco roles. The RADIUS server should support the CLASS attribute, which AsyncOS uses to assign users in the RADIUS directory to Cisco user roles. AsyncOS supports two authentication protocols for communicating with the RADIUS server: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).

To assign RADIUS users to Cisco user roles, first set the CLASS attribute on the RADIUS server with a string value of <radius-group> , which will be mapped to Cisco user roles. The CLASS attribute may contain letters, numbers, and a dash, but cannot start with a dash. AsyncOS does not support multiple values in the CLASS attribute. RADIUS users belonging to a group without a CLASS attribute or an unmapped CLASS attribute cannot log into the appliance .

If the appliance cannot communicate with the RADIUS server, the user can log in with a local user account on the appliance .

Note If an external user changes the user role for their RADIUS group, the user should log out of the appliance and then log back in. The user will have the permissions of their new role.

Procedure

Step 1 On the **System Administration** > **Users** page, click **Enable**.

Step 2 Check the Enable External Authentication option if it is not enabled already.

Step 3 Enter the hostname for the RADIUS server.

Step 4 Enter the port number for the RADIUS server. The default port number is 1812.

Step 5 Enter the Shared Secret password for the RADIUS server.

Step 6 Enter the number of seconds for the appliance to wait for a response from the server before timing out.

Step 7 (Optional) Click **Add Row** to add another RADIUS server. Repeat steps 3 – 6 for each RADIUS server.

Note You can add up to ten RADIUS servers.

Step 8 Enter the number of seconds AsyncOS stores the external authentication credentials before contacting the RADIUS server again to re-authenticate in the “External Authentication Cache Timeout” field. Default is zero (0).

Note If the RADIUS server uses one-time passwords, for example passwords created from a token, enter zero (0). When the value is set to zero, AsyncOS does not contact the RADIUS server again to authenticate during the current session.

Step 9 Configure Group Mapping:

Setting	Description
Map externally authenticated users to multiple local roles.	AsyncOS assigns RADIUS users to appliance roles based on the RADIUS CLASS attribute. CLASS attribute requirements: • 3 character minimum • 253 character maximum • no colons, commas, or newline characters • one or more mapped CLASS attributes for each RADIUS user (With this setting, AsyncOS denies access to RADIUS users without a mapped CLASS attribute.) For RADIUS users with multiple CLASS attributes, AsyncOS assigns the most restrictive role. For example, if a RADIUS user has two CLASS attributes, which are mapped to the Operator and Read-Only Operator roles, AsyncOS assigns the RADIUS user to the Read-Only Operator role, which is more restrictive than the Operator role. These are the appliance roles ordered from least restrictive to most restrictive: • admin • Administrator • Technician • Operator cloudadmin • Read-only Operator • Help Desk User • Guest
Map all externally authenticated users to the Administrator role.	AsyncOS assigns RADIUS users to the Administrator role.

Step 10 Choose whether to map all externally authenticated users to the Administrator role or to different appliance user role types.

Step 11 If you map users to different role types, enter the group name as defined in the RADIUS CLASS attribute in the Group Name or Directory field, and choose an appliance role type from the Role field. You can add more role mappings by clicking **Add Row**.

For more information on user role types, see Working with User Accounts, on page 1.

Step 12 Submit and commit your changes.

Enable SAML Authentication

You can enable Single Sign On using SAML to authenticate users and assign groups of users to Cisco rules.

Before you begin

Make sure that you have configured the SAML profiles with Service Provider and Identity Provider settings. See How to Configure SSO on your Appliance.

Procedure

Step 1 Navigate to **System Administration > Users**.

Step 2 Scroll down to the **External Authentication** section.

Step 3 Click **Enable**.

Step 4 Select the **Enable External Authentication** check box.

Step 5 Select **SAML** as the authentication type from the drop-down list.

Step 6 **(Optional)** In the **External Authentication Attribute Name Map** field, enter the attribute name to search from the Group Mapping.

The Attribute Name depends on the attributes that you configure for the Identity Provider to relay the SAML response. The appliance will search for matching entries of the Attribute Name from SAML response against the attributes that you configure in the **Group Mapping** field. This is optional and if you do not configure, the appliance will search for matching entries of all attributes present in SAML response against configured Group Mapping field.

Step 7 In the **Group Mapping** field, enter the group name attribute as defined in the SAML directory based on the predefined or custom user role. You can click **Add Row** to add multiple role mappings.

The Group Mapping must contain a group attribute. You can add 'Unspecified Groups' attribute to authenticate SAML assertions or response.

For more information on types of user roles, see Working with User Accounts, on page 1.

Note The Group Mapping attributes are case-sensitive and must match exactly in order to return the proper results.

Step 8 Submit and commit your changes.

What to do next

After you enable SAML external authentication, you can use the **Use Single Sign On** link on the login page of the appliance and enter the username to log in to the appliance .

Two-Factor Authentication

You can use a RADIUS directory to configure two-factor authentication for specific user roles. The appliance supports the following authentication protocols for communicating with the RADIUS server:

- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)

You can enable two-factor authentication for the following user roles:

- predefined
- custom

The feature has been tested with:

- RSA Authentication Manager v8.2
- FreeRADIUS v1.1.7 and above
- ISE v1.4 and above

Related Topics

- Enabling Two-Factor Authentication, on page 20
- Disabling Two-Factor Authentication, on page 20

Enabling Two-Factor Authentication

Before You Begin

Make sure that you get the required RADIUS server details for two-factor authentication from your IT administrator.

Procedure

Step 1 On the **System Administration** > **Users** page, click **Enable** under Two-Factor Authentication.
Step 2 Enter the hostname or IP address of the RADIUS server.
Step 3 Enter the port number of the RADIUS server.
Step 4 Enter the Shared Secret password of the RADIUS server.
Step 5 Enter the number of seconds to wait for a response from the server before timing out.
Step 6 Select the appropriate authentication protocol.
Step 7 (Optional) Click **Add Row** to add another RADIUS server. Repeat steps 2 to 6 for each RADIUS server.

Note You can add up to ten RADIUS servers.

Step 8 Select the required user roles for which you want to enable two-factor authentication.
Step 9 Submit and commit your changes.

When two-factor authentication is enabled, the user is prompted to enter a passcode after entering the username and passphrase, to login to the appliance .

Disabling Two-Factor Authentication

Before You Begin

Make sure you have enabled two-factor authentication on your appliance .

Procedure

Step 1 On the **System Administration** > **Users** page, click **Edit Global Settings** under Two-Factor Authentication
Step 2 Deselect **Enable Two-Factor Authentication**.

Step 3 Submit and commit your changes.

Configuring Access to the Email Security Appliance

AsyncOS provides administrators controls to manage users' access to the appliance , including a timeout for Web UI session and an access list that specifies the IP addresses from which users and your organization's proxy servers can access the appliance .

Related Topics

- Configuring IP-Based Network Access, on page 21
- Configuring Session Timeouts, on page 23

Configuring IP-Based Network Access

You can control from which IP addresses users access the appliance by creating access lists for users who connect directly to the appliance and users who connect through a reverse proxy, if your organization uses reverse proxies for remote users.

Related Topics

- Direct Connections, on page 21
- Connecting Through a Proxy, on page 21
- Important Precautions When Restricting Network Access , on page 22
- Creating the Access List , on page 22

Direct Connections

You can specify the IP addresses, subnets, or CIDR addresses for machines that can connect to the appliance . Users can access the appliance from any machine with IP address from the access list. Users attempting to connect to the appliance from an address not included in the list are denied access.

Connecting Through a Proxy

If your organization's network uses reverse proxy servers between remote users' machines and the appliance , AsyncOS allows you create an access list with the IP addresses of the proxies that can connect to the appliance .

Even when using a reverse proxy, AsyncOS still validates the IP address of the remote user's machine against a list of IP addresses allowed for user connections. To send the remote user's IP address to the appliance , the proxy needs to include the x-forwarded-for HTTP header in its connection request to the appliance .

The x-forwarded-for header is a non-RFC standard HTTP header with the following format:

x-forwarded-for: client-ip, proxy1, proxy2,... CRLF .

The value for this header is a comma-separated list of IP addresses with the left-most address being the address of the remote user's machine, followed by the addresses of each successive proxy that forwarded the connection request. (The header name is configurable.) The appliance matches the remote user's IP address from the header and the connecting proxy's IP address against the allowed user and proxy IP addresses in the access list.

Note AsyncOS supports only IPv4 addresses in the x-forwarded-for header.

Important Precautions When Restricting Network Access

Caution! You may lose access to the appliance after submitting and committing network access changes if one of the following conditions is true:

- If you select **Only Allow Specific Connections** and do not include the IP address of your current machine (PC, appliance in a clustered environment, or Security Management appliance , etc.) in the list.
- If you select **Only Allow Specific Connections Through Proxy** and the IP address of the proxy currently connected to the appliance is not in the proxy list and the value of the Origin IP header is not in the list of allowed IP addresses.
- If you select **Only Allow Specific Connections Directly or Through Proxy** and
  - the value of the Origin IP header is not in the list of allowed IP addresses

    OR

  - the value of the Origin IP header is not in the list of allowed IP Addresses and the IP address of the proxy connected to the appliance is not in the list of allowed proxies.

Creating the Access List

You can create the network access list either via the GUI or the **`adminaccessconfig > ipaccess`** CLI command.

Before You Begin

Ensure that you will not lock yourself out of the appliance after changing network access settings. See Important Precautions When Restricting Network Access , on page 22.

Procedure

Step 1 Select **System Administration** > **Network Access**.

Step 2 Click **Edit Settings**.

Step 3 Select the mode of control for the access list:

Option	Description
Allow All	This mode allows all connections to the appliance . This is the default mode of operation.
Only Allow Specific Connections	This mode allows a user to connection to the appliance if the user's IP address matches the IP addresses, IP ranges, or CIDR ranges included in the access list.

Option	Description
Only Allow Specific Connections Through Proxy	This mode allows a user to connect to the appliance through a reverse proxy if the following conditions are met: • The connecting proxy's IP address is included in the access list's IP Address of Proxy Server field. • The proxy includes the **`x-forwarded-header`** HTTP header in its connection request. • The value of **`x-forwarded-header`** is not empty. • The remote user's IP address is included in x-forwarded-header and it matches the IP addresses, IP ranges, or CIDR ranges defined for users in the access list.
Only Allow Specific Connections Directly or Through Proxy	This mode allows users to connect through a reverse proxy or directly to the appliance if their IP address matches the IP addresses, IP ranges, or CIDR ranges included in the access list. The conditions for connecting through a proxy are the same as in the Only Allow Specific Connections Through Proxy mode.

Step 4 Enter the IP addresses from which users will be allowed to connect to the appliance .

You can enter an IP address, IP address range or CIDR range. Use commas to separate multiple entries.

Step 5 If connecting through a proxy is allowed, enter the following information:

a. The IP addresses of the proxies allowed to connect to the appliance . Use commas to separate multiple entries.

b. The name of the origin IP header that the proxy sends to the appliance , which contains the IP addresses of the remote user's machine and the proxy servers that forwarded the request. By default, the name of the header is x-forwarded-for .

Step 6 Ensure that you have not configured a change that will lock you out of the appliance after you submit and commit your changes.

Step 7 Submit and commit your changes.

Configuring Session Timeouts

• Configuring the Web UI Session Timeout, on page 23
• Configuring the CLI Session Timeout, on page 24

Configuring the Web UI Session Timeout

You can specify how long a user can be logged into the appliance's Web UI before AsyncOS logs the user out due to inactivity. This Web UI session timeout applies to:

• All users, including administrator
• HTTP and HTTPS sessions
• Cisco Spam Quarantine

Once AsyncOS logs a user out, the appliance redirects the user's web browser to login page.

Procedure

Step 1 Select **System Administration** > **Network Access**.

Step 2 Click **Edit Settings**.

Step 3 In the **Web UI Inactivity Timeout** field, enter the number of minutes users can be inactive before being logged out. You can define a timeout period between 5 and 1440 minutes.

Step 4 Submit and commit your changes.

What to do next

You can also use the adminaccessconfig command in CLI to configure Web UI session timeout. See *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances* .

Configuring the CLI Session Timeout

You can specify how long a user can be logged into the appliance's CLI before AsyncOS logs the user out due to inactivity. The CLI session timeout applies:

- To all users, including administrator
- Only to the connections using Secure Shell (SSH), SCP, and direct serial connection

Note Any uncommitted configuration changes at the time of CLI session timeout will be lost. Make sure that you commit the configuration changes as soon as they are made.

Procedure

Step 1 Select **System Administration** > **Network Access**.

Step 2 Click **Edit Settings**.

Step 3 In the **CLI Inactivity Timeout** field, enter the number of minutes users can be inactive before being logged out. You can define a timeout period between 5 and 1440 minutes.

Step 4 Submit and commit your changes.

What to do next

You can also use the adminaccessconfig command in CLI to configure CLI session timeout. See *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances* .

Displaying Messages to Administrative Users

- Displaying a Message Before Login , on page 25

• Displaying a Message After Login , on page 25

Displaying a Message Before Login

You can configure the appliance to display a message before a user attempts to log into the appliance through SSH, FTP, or Web UI. The login banner is customizable text that appears above the login prompt. You can use the login banner to display internal security information or best practice instructions for the appliance . For example, you can create a simple note that saying that unauthorized use of the appliance is prohibited or a detailed warning concerning the organization's right to review changes made by the user to the appliance .

Use the adminaccessconfig > banner command in the CLI to create the login banner. The maximum length of the login banner is 2000 characters to fit 80x25 consoles. A login banner can be imported from a file in the /data/pub/configuration directory on the appliance . After creating the banner, commit your changes.

Displaying a Message After Login

You can configure AsyncOS to display a welcome banner after a user successfully logs into the appliance through SSH, FTP, or Web UI. You can use the welcome banner to display internal security information or best practice instructions for the appliance .

Use the adminaccessconfig > welcome command in CLI to create the welcome banner. The maximum length of the welcome banner is 1600 characters.

You can import a welcome banner from a file in the /data/pub/configuration directory on your appliance . After creating the banner, commit your changes.

For more information, see *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances* .

Managing Secure Shell (SSH) Keys

Use the sshconfig command to:

- Add or delete secure shell (SSH) public User keys to the authorized_keys file of user accounts that have been configured on the system, including the admin account. This allows authentication to user accounts using SSH keys rather than passphrase challenge.
- Edit the following SSH server configuration settings:
  - Public Key Authentication Algorithms
  - Cipher Algorithms
  - KEX Algorithms
  - MAC Methods
  - Minimum Server Key Size.

Note To configure Host keys, which are used when performing SCP pushes of log files from the appliance to other host machines, use **`logconfig -> hostkeyconfig`** . For more information, see Logging.

Using **`hostkeyconfig`** , you can scan for keys of remote hosts and add them to the appliance .

Related Topics

- Example: Install a New Public Key, on page 26
- Example: Edit SSH Server Configuration, on page 26

Example: Install a New Public Key

In the following example, a new public key is installed for the administrator account:

```
mail.example.com> sshconfig
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
[]> userkey
Currently installed keys for admin:
Choose the operation you want to perform:
- NEW - Add a new key.
- USER - Switch to a different user to edit.
[]> new
Please enter the public SSH key for authorization.
Press enter on a blank line to finish.
[-paste public key for user authentication here-]
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
[]>
```

Example: Edit SSH Server Configuration

The following example shows how to edit the SSH server configuration.

```
mail.example.com> sshconfig
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
[]> sshd
ssh server config settings:
Public Key Authentication Algorithms:
        rsa1
        ssh-dss
        ssh-rsa
Cipher Algorithms:
        aes128-ctr
        aes192-ctr
        aes256-ctr
        arcfour256
        arcfour128
        aes128-cbc
        3des-cbc
        blowfish-cbc
        cast128-cbc
        aes192-cbc
        aes256-cbc
        arcfour
        rijndael-cbc@lysator.liu.se
MAC Methods:
        hmac-md5
        hmac-sha1
        umac-64@openssh.com
```

```
        hmac-ripemd160
        hmac-ripemd160@openssh.com
        hmac-sha1-96
        hmac-md5-96
Minimum Server Key Size:
        1024
KEX Algorithms:
        diffie-hellman-group-exchange-sha256
        diffie-hellman-group-exchange-sha1
        diffie-hellman-group14-sha1
        diffie-hellman-group1-sha1
Choose the operation you want to perform:
- SETUP - Setup SSH server configuration settings
[]> setup
Enter the Public Key Authentication Algorithms do you want to use
[rsa1,ssh-dss,ssh-rsa]> rsa1
Enter the Cipher Algorithms do you want to use
[aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,
cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se]> aes192-ctr
Enter the MAC Methods do you want to use
[hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,
hmac-md5-96]> hmac-sha1
Enter the Minimum Server Key Size do you want to use
[1024]> 2048
Enter the KEX Algorithms do you want to use
[diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,
diffie-hellman-group1-sha1]> diffie-hellman-group-exchange-sha1
ssh server config settings:
Public Key Authentication Algorithms:
        rsa1
Cipher Algorithms:
        aes192-ctr
MAC Methods:
        hmac-sha1
Minimum Server Key Size:
        2048
KEX Algorithms:
        diffie-hellman-group-exchange-sha1
Choose the operation you want to perform:
- SETUP - Setup SSH server configuration settings
[]>
```

Remote SSH Command Execution

The CLI allows commands to be run via remote SSH command execution. For example, the following command can be run from a remote host unchallenged if an SSH public key has been configured for the admin account on the appliance :

```
# ssh admin@mail3.example.com status

Enter "status detail" for more information.

Status as of: Mon Jan 20 17:24:15 2003

Last counter reset: Mon Jan 20 17:08:21 2003

System status: online

[rest of command deleted]
```

Monitoring Administrative User Access

To	Do This
View session details of all active users of the appliance	Click **Options** > **Active Sessions** at the top right of the page In the command-line interface, use the w , whoami and who commands.
View users who have recently logged into the appliance . The IP address of the remote host, and the login, logout, and total time are also displayed.	In the command-line interface, use the l ast command.