Account Management
For SaaS Email and Web Security
## Contents

1. **What is Account Management**
   - Differences in administration for Service Providers ........................................ 5
   - Overview of the Control Console ................................................................. 5
     - The Control Console interface ........................................................................ 6
   - Initial creation of your customer account ......................................................... 7
   - Ensuring you can receive email from your service provider ............................ 7
   - Other documents you might need ...................................................................... 7
   - Using online Help ............................................................................................ 8
   - Search for domains and users .......................................................................... 9

2. **Customer setup**
   - Setting up your customer account .................................................................. 11
   - Aspects of user time zones you need to consider ............................................ 11
   - Customer Details page .................................................................................... 12
   - Changing the user interface to give it your company brand ............................. 12
     - Types of branding .......................................................................................... 13
     - Available branding attributes ...................................................................... 14
     - Branding at the customer and domain levels .............................................. 15
     - Rebrand the user interface at the customer level ........................................ 16
     - Branding page ................................................................................................ 17
   - Using distribution lists for status messages and Performance Reports ........... 19
     - Create a distribution list ................................................................................. 20

3. **Domain setup**
   - What is a domain ............................................................................................. 21
   - Review your list of domains ............................................................................. 21
   - View the details of a domain ............................................................................ 22
   - Assign a domain alias ..................................................................................... 23
   - Administer the default domain language ....................................................... 24
   - Rebrand the user interface of a domain .......................................................... 25

4. **Adding and managing users**
   - Types of user roles and privileges .................................................................. 27
     - Basic user access and privileges .................................................................. 27
     - Administrative user roles and privileges ..................................................... 29
     - Administrator page access ............................................................................ 30
     - Users who are protected from auto-deletion ............................................. 32
   - Enabling alias address capability for all users ................................................. 33
     - Benefits of alias addresses ........................................................................... 33
     - Enable alias address support ........................................................................ 34
   - Defining how users can sign in ......................................................................... 34
     - Set up password method of authentication ............................................... 35
     - Set up LDAP method of user authentication .............................................. 36
     - Set up IMAP method of user authentication .............................................. 38
     - Set up POP3 method of user authentication .............................................. 39
What is Account Management

Account Management is a set of administrative pages you use to configure and manage, in a single location, the entities shared by the Email Protection, Web Protection, and Email Archiving products.

Account Management entities include:

- Domains
- Users
- Groups of users that share a common email or web filtering policy.
- Other administrators, including other Customer Administrators, Domain Administrators, Quarantine Managers, Group Managers, and Reports Managers

Contents

- Differences in administration for Service Providers
- Overview of the Control Console
- Initial creation of your customer account
- Ensuring you can receive email from your service provider
- Other documents you might need
- Using online Help
- Search for domains and users

Differences in administration for Service Providers

This document is for use by Enterprise customers only. Service Provider customers do not administer groups for Email Protection and therefore, do not assign groups to email filtering policies. Instead, service provider customers assign policies directly to domains.

In addition, Domain Administrators for Service Provider customers have greater capabilities for managing users than do Domain Administrators for enterprise customers.

The capabilities for managing groups and the limitations for managing users, as described in this document, apply only to enterprise customers.

Overview of the Control Console

The Control Console is a Web-based administration tool that serves as your primary tool to manage administrators, domains, and users.

In addition, the Control Console is the primary tool to configure and monitor the features provided by the following products, if your company is enabled for them:
The Control Console interface

A number of elements of the Control Console interface are consistently available, regardless of the security products you are administering. However, the actual page elements might differ depending on which page is open and what role is signed in.

<table>
<thead>
<tr>
<th>Item Number</th>
<th>Page Item</th>
<th>What It Does</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User signed in and role</td>
<td>The user address and role of the user who is currently signed in.</td>
</tr>
<tr>
<td>2</td>
<td>Prior Sign in Date and Time</td>
<td>The date and time your user address and password were last used to sign in. If you had not signed in at the date and time listed, your sign credentials may have been compromised.</td>
</tr>
<tr>
<td>3</td>
<td>Sign out</td>
<td>A link that signs you out from the Control Console and returns you to the Sign In page.</td>
</tr>
<tr>
<td>4</td>
<td>What's New</td>
<td>A link that opens information about changes that have occurred since the last product release, as well as the changes that occurred in the previous two releases.</td>
</tr>
<tr>
<td>5</td>
<td>Search</td>
<td>The search field is a quick way to find a domain or user without clicking the Account Management tab and administration submenu tabs.</td>
</tr>
<tr>
<td>Item Number</td>
<td>Page Item</td>
<td>What It Does</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>6</td>
<td>Application tabs</td>
<td>The application tabs provide access to the primary administration and reporting pages for each application enabled for your company:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Email Protection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Web Protection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Email Archiving</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The <strong>Account Management</strong> tab is used to administer users, other administrators, domains, and other configuration elements that apply to multiple applications. The <strong>My Account</strong> tab is used to administer your own personal user account.</td>
</tr>
<tr>
<td>7</td>
<td>Administration submenu tabs</td>
<td>For each product, this set of tabs reflects the categories of elements you must administer for that product.</td>
</tr>
<tr>
<td>8</td>
<td>Links</td>
<td>Depending on the page, hyperlinks (&quot;links&quot;) may be available. Clicking a link performs a function, such as displaying more information or opening a new administration page to perform the indicated task.</td>
</tr>
<tr>
<td>9</td>
<td>Action button</td>
<td>Depending on the page, action buttons may appear which display a new page to add data or a confirmation to complete an action.</td>
</tr>
<tr>
<td>10</td>
<td>Navigation drop-down menus</td>
<td>From the top-level set of tabs, navigation drop-down menus allow you to quickly access the page you want, without clicking individual tabs.</td>
</tr>
</tbody>
</table>

### Initial creation of your customer account

Your service provider sets up your account within the Control Console. This setup includes defining the service package or bundle for your company. The three main applications, Email Protection, Web Protection, and Email Archiving can be standalone or part of a bundle of two or all of the applications.

### Ensuring you can receive email from your service provider

If you had or still have a different email security or filtering service, and your network is administered so that you can receive email only from IP addresses associated with that security service, you must administer your network to allow incoming email from the Control Console servers.

For example, a port in your company’s firewall might need to be enabled to receive email from the IP addresses of the Control Console servers.

This enablement is necessary in order for you and your users to set the initial password for access to the Control Console.

### Other documents you might need

Account Management is a self-contained subset of pages you access on the Control Console. You use it in conjunction with the administration pages for the previously-mentioned products. For information
on administering these products, see the online help in the Control Console or the documentation as listed below.

**Email Protection documents**
- Email Protection Quick Start Guide
- Email Protection Administrator Guide
- Intelligent Routing User Guide
- Email Continuity Administrator Quick Start Guide

**Web Protection documents**
- Web Protection Services Setup Guide
- WDS Connector Setup Guide

**Email Archiving documents**
- Email Archiving Administrator Guide
- Email Archiving Quick Setup Guide for Microsoft Exchange Server 2000
- Email Archiving Quick Setup Guide for Microsoft Exchange Server 2003
- Email Archiving Quick Setup Guide for Microsoft Exchange Server 2007
- Email Archiving Quick Setup Guide for Microsoft Exchange Server 2010

**User guides**
In addition, a variety of guides for your users are available:
- Email Protection User Guide
- Email Archiving User Guide
- Spam Control for Outlook
- Email Continuity User Quick Start Guide

---

**Using online Help**

Use online Help in the Control Console to find details on Account Management pages. You can also use the online Help for information on Email Archiving, Email Protection, and Web Protection pages, if enabled. Online Help describes the purpose of pages, the fields on the pages, and procedures that use the pages.

To open online Help, click Help on the page you are using. The Help page opens to the topics related to the task you are performing. You can use the table of contents to find other topics.

**Word search of online Help**

When the Help page is open and is the active page on the computer display, you can also press **Ctrl+F** to perform word searches within online Help.
Search for domains and users

Depending on your role and what entities have been administered, you can search all the entities to which you have access for a specific domain or user account. For example, Customer Administrator can search all the domains or user accounts for the customer. A Domain Administrator can search for all users for the domain that the administrator is responsible for.

Task
For option definitions, click Help in the interface.

1. From the Search drop-down list, select the type element you want to find:
   - Domains
   - Users

2. In the text field following the list, type all or part of a text character string for the name of the domain or user you want.
   The Control Console automatically displays a drop-down list of matches for the text string you type.

3. Click the match from the drop-down list of matches or complete typing the complete name of the domain or user.

4. Press Enter or click Go.
   The User Details or Domain Details page for the specific user or domain is displayed.
What is Account Management
Search for domains and users
Customer setup

Some capabilities of the Control Console that affect all users must be established for the customer.

Contents
- Setting up your customer account
- Aspects of user time zones you need to consider
- Customer Details page
- Changing the user interface to give it your company brand
- Using distribution lists for status messages and Performance Reports

Setting up your customer account

Some features of Control Console services uniquely serve the Customer Administrator or uniformly affect all levels of user roles in the way the Control Console displays information. You must administer these features as part of the customer account setup.

Aspects of user time zones you need to consider

The time zone is used to timestamp the events related to the user in the Control Console (for example, the email arrivals in quarantine).

You can set the time zone for individual users on the Create User or Edit User pages. You can also set a default time zone for all users on the Customer Details page. Finally, if a user has permissions to the Control Console, the user can change his or her time zone on the Preferences tab. The default time zone is applied to all user accounts for the customer unless you or the user manually sets an individual user's time zone later.

The time zone represents the offset from Greenwich Mean Time (GMT) to the local time zone for the user of the user account. The time zone name is provided only for assistance. Use the hourly offset to determine which time zone to select. This setting does not affect the user's local machine (for example, it does not change the Windows time zone settings).

If you select a time zone different from the one used by the Email Protection data center, quarantined emails might appear on different dates in the quarantine area. For example, if the user's local time zone is set to New York, but the data center's time zone is Los Angeles, the user's local date will change at midnight in the local time zone, but the data center will still be using the previous day's date until it is 3:00 am in the local time zone. In this case, any emails that were quarantined after the local time zone passed midnight and until 3:00 am will still be listed for the previous day's date. Thus, you would have to select yesterday to view the email's quarantined from midnight to 3:00 am in the local time zone. When the time zone for the data center passes midnight, its local date will then match the local date for the user. You can display all the emails in a quarantine area to compensate for this behavior.
Customer Details page

Use the Customer Details page to view your contact information, number of users, and default time zone. In addition, you can change the default time zone.

<table>
<thead>
<tr>
<th>Table 2-1 Customer Details option definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option</strong></td>
</tr>
<tr>
<td>Customer Name</td>
</tr>
<tr>
<td>Address 1</td>
</tr>
<tr>
<td>Address 2</td>
</tr>
<tr>
<td>City</td>
</tr>
<tr>
<td>Zip/Postal</td>
</tr>
<tr>
<td>Telephone</td>
</tr>
<tr>
<td>Time Zone Default</td>
</tr>
<tr>
<td>Update</td>
</tr>
</tbody>
</table>

The time zone you select is applied to all user accounts for the customer unless:
- The time zone is set manually on the Create User page.
- The time zone is set manually on the Edit User page.
- A user with Control Console access changes it.

The time zone default setting allows you to apply the time zone to each new user when they are automatically created in the Control Console with Directory Integration or SMTP Discovery.

<table>
<thead>
<tr>
<th>Table 2-2 Additional Customer Details options (available, depending on the system configuration)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option</strong></td>
</tr>
<tr>
<td>Actual Users (all domains)</td>
</tr>
<tr>
<td>Billed Users (all domains)</td>
</tr>
<tr>
<td>Maximum Allowed Users (all domains)</td>
</tr>
</tbody>
</table>

Changing the user interface to give it your company brand

You can change settings to provide the Control Console with a “look and feel” that matches the look and feel of your company. This “rebranding” of the interface can be applied to all domains generically, to individual domains only, or at both levels.

This capability is available only if it is enabled by your provider. Also, customer-wide rebranding can be performed only by a user with the role of Customer Administrator or higher. Domain-specific branding can be performed by a Domain Administrator or higher.

You can configure branding settings in the Control Console to provide a “look and feel” customized to your organization. For example, you can designate that the default service provider logo image in the Control Console be replaced with your organization’s logo image. In addition, you provide a URL with preferred naming that your users can use to access the Control Console. For a list of all attributes available for branding, see Attributes of Branding.
By virtue of rebranding the interface for your company, you automatically rebrand the interface of your domains IF they are designated to use standard branding. See the descriptions that follow.

**Types of branding**
The branding type establishes the degree in which your company's name appears throughout the Control Console, spam reports, and notifications.

Your service provider enables you to perform one of four types of branding:

- **White label** branding — No logos or branding appear in the user interface. However, you can display and change the following items:
  - Your company host name, which appears when users log in or receive spam notifications.
  - The *From Email* address for Spam Reports
  - A custom support email address

You can also still specify a co-brand tagline for your company. This tagline is displayed below the customer logo for users of any of your domains if the domain is designated for co-branding.

With the white label branding option, copyright information is not displayed at the bottom of the page.

- **Private** branding — Your company logo and tagline appear in the user interface. In addition, you can change the following items:
  - Your company host name, which appears when users log in or receive spam notifications.
  - The *From Email* address for Spam Reports
  - A custom support email address

You can also still specify a co-brand tagline for your company. This tagline is displayed below the customer logo for users of any of your domains if the domain is designated for co-branding.

With the private branding option, copyright information is not displayed at the bottom of the page.
Co-branding — Your company logo appears, along with your provider’s co-brand tagline, in the user interface. In addition, you can change the following items:

- Your company host name, which appears when users log in or receive spam notifications.
- The From Email address for Spam Reports
- A custom support email address

Rebranding — Your company logo appears in the user interface without a tagline. In addition, you can change the following items:

- Your company host name, which appears when users log in or receive spam notifications.
- The From Email address for Spam Reports
- A custom support email address

You can also specify a co-brand tagline for your company. This tagline is displayed below the customer logo for users of any of your domains if the domain is designated for co-branding.

With the rebranding option, copyright information is not displayed at the bottom of the page.

Available branding attributes

In addition to the logo and tagline, rebranding affects other aspects of the user interface, depending on the branding type.

A branding type other than Standard must be enabled by your service provider for you to be able to access and manage the branding settings in the Branding Configuration page.

Table 2-3 How customizable attributes display depending on the branding type

<table>
<thead>
<tr>
<th>Customizable Attribute</th>
<th>Standard</th>
<th>White Label</th>
<th>Private</th>
<th>Co-brand</th>
<th>Rebrand</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company logo</td>
<td>No. Displays service provider logo</td>
<td>Removed from display</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Company tagline</td>
<td>No. Displays service provider tagline</td>
<td>Removed from display</td>
<td>Yes</td>
<td>No. Displays service provider tagline</td>
<td>Removed from display</td>
</tr>
</tbody>
</table>
Table 2-3 How customizable attributes display depending on the branding type *(continued)*

<table>
<thead>
<tr>
<th>Customizable Attribute</th>
<th>Standard</th>
<th>White Label</th>
<th>Private</th>
<th>Co-brand</th>
<th>Rebrand</th>
</tr>
</thead>
<tbody>
<tr>
<td>Co-brand tagline image</td>
<td>No. Displays service provider name</td>
<td>Yes. Applies only to dependent domain whose branding type is Co-brand.(^a)</td>
<td>Yes. Applies only to dependent domain whose branding type is Co-brand.(^a)</td>
<td>Yes. Applies only to dependent domain whose branding type is Co-brand.(^a)</td>
<td>Yes. Applies only to dependent domain whose branding type is Co-brand.(^a)</td>
</tr>
<tr>
<td>Control Console name</td>
<td>No. Displays “Control Console” or service provider name</td>
<td>Removed from display</td>
<td>Yes</td>
<td>No. Displays “Control Console” or service provider name</td>
<td>No. Displays “Control Console” or service provider name</td>
</tr>
<tr>
<td>Privacy Policy</td>
<td>No. Displays service provider policy</td>
<td>Removed from display</td>
<td>Removed from display</td>
<td>No. Displays service provider policy</td>
<td>Removed from display</td>
</tr>
<tr>
<td>Spam Control for Outlook URL</td>
<td>No. Displays service provider URL</td>
<td>Removed from display</td>
<td>Yes</td>
<td>No. Displays service provider URL</td>
<td>Yes</td>
</tr>
<tr>
<td>Support Email</td>
<td>No. Displays service provider email</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Custom Hostname</td>
<td>No. Displays service provider host name</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Copyright</td>
<td>Displayed automatically</td>
<td>Hidden automatically</td>
<td>Hidden automatically</td>
<td>Hidden automatically</td>
<td>Hidden automatically</td>
</tr>
</tbody>
</table>

\(^a\) If not set, Co-brand domains see logo of service provider.

**Branding at the customer and domain levels**

You can rebrand the Control Console interface at the customer level, domain level, or both.

Domain branding settings override customer branding settings. If the domain branding settings are not set, the customer branding settings are used as the defaults.

The following table lists the effect of branding configuration on your account and your domains.
### Branding Type

<table>
<thead>
<tr>
<th>Branding Type</th>
<th>Customer</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Private</strong></td>
<td>Replaces the standard or service-provider-defined logo, tagline, and other branding attributes with the customer’s preferred attributes. Becomes the branding for the customer’s domains that use standard branding. No copyright information is displayed.</td>
<td>Replaces the standard, service-provider-defined or customer-defined logo, tagline, and other branding attributes with the preferred attributes for the specific domain. No copyright is displayed.</td>
</tr>
<tr>
<td><strong>Co-brand</strong></td>
<td>Replaces the service-provider-defined logo and other branding attributes with the customer’s preferred attributes. Use the standard service provider logo/tagline. Becomes the branding for the customer’s domains that use standard branding.</td>
<td>Replaces the standard, supplier-defined, or customer-defined logo and other branding attributes with the preferred attributes for the specific domain. Uses the standard service-provider tagline or the customer’s tagline, if created. Copyright is displayed.</td>
</tr>
<tr>
<td><strong>Rebrand</strong></td>
<td>Replaces the standard logo, and other branding attributes with the customer’s preferred attributes. Does not use a tagline, but allows the assignment of a tagline for display for the customer’s domains. Becomes the branding for the customer’s domains that use standard branding. No copyright information is displayed.</td>
<td>Replaces the standard or customer-defined logo and other branding attributes with the preferred attributes for the specific domain. No tagline is used. No copyright is displayed.</td>
</tr>
</tbody>
</table>

### Rebrand the user interface at the customer level

Configure new branding settings in the Control Console to provide a customized “look and feel” for the user interface at the customer-level.

#### Before you begin

A branding type other than *Standard* must be enabled by your service provider for you to be able to access and manage the branding settings in the Branding Configuration page.

This capability is available only if it is enabled by your provider. Also, this procedure can be performed only by a user with the role of Customer Administrator or higher.
Task

1 Select Account Manager | Customers | Branding.

The Branding Configuration page is displayed. The Branding Type field displays the type of branding you are enabled for.

2 Complete the fields as appropriate.

3 Click Save.

The logo image is not shown if you are using the White Label (no branding).

Branding page

Branding allows you to configure branding settings that customize the console to your company or domain. You can designate that the default logo image be replaced with your organization's logo image. When replacing your logo, be aware that lower-level branding settings override higher-level settings.

There are two places where the Branding page resides:

- If opened under the Customers | Customer Management set of pages, the settings defined here apply to the customer and will be the default settings applied to all of its domains.
- If opened under the Domains | Domain Management set of pages, the settings defined here apply only to the domains.

When branding settings are chosen at a lower level, they override the settings chosen at a higher level. For example, domain settings override customer settings, and customer settings override partner settings. If branding settings are not chosen at a level, the next higher level's settings are used.

A current domain link appears for Customer Administrators whose service includes multiple domains. Click the link and use the Select Domain page to select the domain you want.

The Branding Configuration page contains the following fields. Unless otherwise stated, the fields apply to all branding types.
Table 2-4  Branding field definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branding Type</td>
<td>Indicates the branding type enabled for the designated partner, customer, or domain. If you choose <strong>White Label</strong>, <strong>Rebrand</strong>, or <strong>Private</strong>, the standard copyright information is removed from all pages, and other options available for branding vary as described in this table.</td>
</tr>
<tr>
<td>Enable Branding</td>
<td>Click the checkbox to use the branding settings in this page for the partner, customer, or domain. If this box is not checked, the branding settings for the next higher level will be used.</td>
</tr>
<tr>
<td>Custom Hostname</td>
<td>Type a custom hostname. The custom hostname changes the name contained within the URL listed in the Spam Report and the URL for access to the Control Console. The custom hostname can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Your standard service URL that was identified in your service agreement prepended with your brand name (e.g. acme.console.service_provider.com).</td>
</tr>
<tr>
<td></td>
<td>• Your brand name that precedes portal or console and saascontrol.com (e.g. acme.console.saascontrol.com).</td>
</tr>
<tr>
<td></td>
<td>Use of portal or console depends on your original URL designated in your service agreement.</td>
</tr>
<tr>
<td>From Email</td>
<td>Enter the full email address to be used as the &quot;From:&quot; email address when Spam Reports and Performance Reports are generated and sent. This email address must be valid to support the user clicking the Reply button in his/her email application.</td>
</tr>
<tr>
<td>Support Email</td>
<td>Enter the full email address to be used as the &quot;From:&quot; email address for customer and/or technical support to handle lost password, alias email address, or other requests. This email address must be valid to support the user clicking the Reply button in his/her email application.</td>
</tr>
<tr>
<td>Site Name</td>
<td>(For <strong>Private</strong> branding only) Enter the full name that will be used to title the Control Console throughout the user interface pages. Once the change is saved, users will see the new site name the next time they log onto the Control Console.</td>
</tr>
<tr>
<td>Site Name Font</td>
<td>(For <strong>Private</strong> branding only) From the drop-down lists, select the following:</td>
</tr>
<tr>
<td></td>
<td>• Font typeface</td>
</tr>
<tr>
<td></td>
<td>• Font size</td>
</tr>
<tr>
<td></td>
<td>• Font style</td>
</tr>
<tr>
<td>Site Name Color</td>
<td>(For <strong>Private</strong> branding only) From the drop-down list, select one of the colors displayed. Or, type a palette color-code for a custom color and tint.</td>
</tr>
<tr>
<td>Site Name Vertical Rule</td>
<td>(For <strong>Private</strong> branding only) Select the checkbox to insert a vertical line between the logo and site name.</td>
</tr>
<tr>
<td>Spam Control for Outlook URL</td>
<td>(Applies only to the branding types <strong>Private</strong> and <strong>Rebrand</strong>) Type the full URL to the location where the Spam Control For Outlook® utility will be available for download. This field is used if the Allow users to download Spam Control For Outlook field is checked in the Email Protection Console.</td>
</tr>
<tr>
<td>Logo Image</td>
<td>(Applies only to the branding Types <strong>Private</strong>, <strong>Rebrand</strong> and <strong>Co-brand</strong>) Designates what logo image appears in the Control Console. The logo image must be a GIF image that is no larger than 190 pixels wide by 42 pixels high for Co-brand and 190 pixels wide by 63 pixels high for Rebrand. Click the Browse... button to select the logo image file. After you click Open in the File Selector dialog box, the path and file name appears in the Logo Image: text field.</td>
</tr>
<tr>
<td>Tagline Image</td>
<td>(Applies only to the branding type <strong>Private</strong>) Designates what secondary logo image to use in the Control Console pages. The tagline image appears below the logo Image. The tagline image must be a GIF image that is no larger than 190 pixels wide by 21 pixels high. For private branding, the tagline changes for the current account (partner, customer, or domain) in which the change was made. The tagline also becomes the standard tagline for the entities (customers, domains, or both) managed by the current account. Click the Browse... button to select the tagline image file. After you click Open in the File Selector dialog box, the path and file name appears in the Tagline Image: text field.</td>
</tr>
</tbody>
</table>
### Table 2-4 Branding field definitions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Co-brand Logo Image</td>
<td>(Applies only to the branding types Private, Rebrand, and White Label) The Co-brand logo or tagline is not applied to the current account in which the change was made. However, the logo/tagline becomes the Co-brand logo/tagline for any lower level entity (customers, domains, or both) that is Co-branded.</td>
</tr>
<tr>
<td>Image Preview Area</td>
<td>Displays the graphic files as they would appear in the Control Console pages.</td>
</tr>
</tbody>
</table>

### Table 2-5 Branding page toolbar definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save</td>
<td>Click to save your settings. It may take a few minutes before the new tagline image appears in the branded pages.</td>
</tr>
</tbody>
</table>

### Using distribution lists for status messages and Performance Reports

Distribution lists are lists of email addresses that should receive notifications of policy violations and, if enabled, performance reports.

When you have Email Protection, you can create distribution lists of designated users, normally administrators, who should receive automatic notifications of violations of the following aspects of an Email Protection policy:

- Anti-Spam Content Group
- Content Group
- Attachment Filename Policy

A distribution list can also be created to notify users when:

- Automatic spooling for Email Protection disaster recovery starts.
- Various failures and rejections occur with Directory Integration.

When you use MSP Connector, you can create distribution lists of designated users, normally administrators, who should receive automatic notifications of MSP exceptions.

Finally, a distribution list can be used to deliver performance reports.

In order for a distribution list to receive automatic notifications, you must assign the list to receive a “silent copy” notification within the configuration pages for the previously-mentioned aspects of a policy.

> List members must be fully qualified email addresses.
Create a distribution list

Create a distribution list so that the Control Console can send email to you and others for notifications of policy violations and, if enabled, performance reports.

Task

1. Select Account Management | Customers.

The Customer Distribution Lists page is displayed.

2. Click New.

A dialog box for the distribution list name is displayed.

3. Type the name of the distribution list and click OK.

4. Add users to the list.

   a. In the Member field, type the email address of an existing user.

   b. Click Add. The user is added to the list.

Members of a distribution list do not even need to have user accounts in the Control Console. In addition, the users you assign to a distribution list do not need to be in any specific group or domain. However, you might want to set up a distribution list for each group or domain and include in each list only administrators who are within that domain or group.
Domain setup

After the initial setup of your domains, you can perform additional tasks to better manage your domains.

Contents
- What is a domain
- Review your list of domains
- View the details of a domain
- Assign a domain alias
- Administer the default domain language
- Rebrand the user interface of a domain

What is a domain

A domain is an entity within a public or private network usually associated with the latter portion of user email addresses.

The domain entity defines the domain used for its email addresses (the part of the email address that follows the @ symbol). For example, in the email address of username@sampledomain.com, the domain is sampledomain.com. You must have defined a domain for your users to receive email. These domains are called primary domains to differentiate them from alias domain names. You must own the rights to the domain names and your email server must be configured to receive email for the domain names that are configured in Account Management.

In general, domains can be added, modified, or deleted only by your service provider.

Review your list of domains

The Domains list displays all primary domains, and if you choose, all associated alias domain names that you have defined.

Before you begin

If you are a Domain Administrator, you can see all domains for your company, but you can access and change only the domain for which you are responsible.

If you choose, you can also include, in the list of domains, alias domain names and, if Intelligent Routing is enabled, public domain names in the list of domains.

When your service begins, at least one domain must be administered so that the users within the domain can be added to the Control Console.
A primary domain is typically, though not always, associated with a single mail server. Let’s say your company, Lewis Magazine, uses six mail servers, each with its own primary domain name.

Your provisioner should have already assigned at least one domain within the Control Console. You must confirm that these domains, as provisioned, match the actual domain names within your network.

**Task**

1. Select **Account Management | Domains**.

   The **Domains List** page is displayed. The page lists the primary domains assigned in the Control Console.

2. Make sure that the list of domains matches those established in your network. Check with your network or mail server administrator to verify the domains.

3. To include any domain aliases that might have been added, click **Show Domain Aliases**.

4. To include any public domains, if Intelligent Routing is enabled and administered, click **Show Public Domains**. The **Type** column appears to display which domains in the list, if any, are public domains.

   If a primary domain that Email Archiving should serve is missing, you must ask your service provider to add it.

**View the details of a domain**

View the details of a domain to verify the features that are enabled and the number of users assigned. You can also verify or change the domain contact email and the number of email aliases each user is allowed to have.

For option definitions, click **Help** in the interface.

**Task**

1. Select **Account Management | Domains**

   The **Domain Management** list is displayed.
2. Click the domain whose details you want to see.

The Domain Details page is displayed.

Assign a domain alias

Assign alias domain names to domains if your mail servers, routers, or Active Directories are administered with domain aliases.

In brief, alias domain names are "virtual" domains that use the configurations for the primary domain. All user accounts in the primary domain will be automatically assigned alias email addresses using the alias domain name. Alias domain names are not separate entities within Account Management. Alias domain names might be created for reasons such as:

- Anticipation of email addressing that uses a similar but incorrect domain name. For example, if the primary domain name is acme.com, an alias might be acme.net or acmecompany.com, in anticipation that a send might use these domain names by mistake.

- Organizations within a domain use their own unique domain names such that email that might be sent over a company-wide umbrella domain name will still be delivered to the correct domain and the correct recipient. For example, if the primary domain for your Denver office is denver.acme.com, employees might also receive email at acme.com.

For option definitions, click Help in the interface.

A current domain link appears for Customer Administrators whose service includes multiple domains. Click the link and use the Select Domain page to select the domain you want.
Task
1 Select Account Manager | Domain.
2 Click the domain for which you want to add domain aliases.
3 Click Edit Aliases.

The Domain Aliases page is displayed.

4 In the text box to the left of Add, enter a domain alias name to be associated with the primary domain.
5 Click Add.

Administer the default domain language
You can administer the default language of the Control Console for users in a particular domain.
For option definitions, click Help in the interface.

Task
1 Select Account Manager | Domain.
2 Click the domain for which you want to add domain aliases.
3 Click Preferences.

The Domain Preferences page is displayed.
4 From the Select Default Language drop-down box, select the language you want this domain’s users to see when they log into the Control Console.

5 Click Save.

Rebrand the user interface of a domain

Configure new branding settings in the Control Console to provide a customized look and feel for a domain’s user interface.

Before you begin

A branding type other than Standard must be enabled by your service provider for you to be able to access and manage the branding settings in the Branding Configuration page.

This capability is available only if it is enabled by your provider. Also, this procedure can be performed only by a user with the role of Domain Administrator or higher.

Task

1 Click Account Manager | Domain | Branding.

The Branding Configuration page is displayed. The Branding Type field displays the type of branding you are enabled for.

2 Complete the fields as appropriate.

3 Click Save.

The logo image is not shown if you are using the White Label (no branding).
Domain setup
Rebrand the user interface of a domain
Adding and managing users

An initial and ongoing aspect of managing your Email Protection, Web Protection, or Email Archiving service is adding, changing, or deleting users who receive services from these three applications. In addition, you might need to perform a variety of support services for your users and yourself on an ongoing basis.

Contents
- Types of user roles and privileges
- Enabling alias address capability for all users
- Defining how users can sign in
- Setting the default time zone
- Adding users to the Control Console
- Managing existing users one-by-one

Types of user roles and privileges
Different types of users access the Control Console to use and modify services such Email Protection, Web Protection, and Email Archiving. These include basic end users, as well as various levels of administrators.

Contents
- Basic user access and privileges
- Administrative user roles and privileges
- Administrator page access
- Users who are protected from auto-deletion

Basic user access and privileges
To receive Email Protection, Web Protection, or Email Archiving services, each user must have an account, based on a primary email address, and assigned privileges within the Control Console.

A user’s account is identified by the user’s primary email address. In addition to a primary email address, each user account can optionally have one or more alias email addresses. A complete email address includes the prefix and the domain name (for example, username@sampledomain.com). The alias email addresses also receive the services of the three previously-listed products if they are defined within the Control Console.
You can enable users to access the Control Console themselves. However, to receive core services, a user does not need access to the Control Console. For example, the following occur regardless of whether a user has Control Console access:

- Email Protection quarantines a user’s email and sends the user a Spam Report.
- Email Archiving archives that user’s messages, though without access to the Control Console, the user cannot search for and retrieve those archived messages.
- Web Protection filters the Web sites the user tries to access.

However, as an administrator, you can allow users to sign into the Control Console. Such access allows users more capabilities and flexibility in managing their services. For Email Protection, for example, users with Control Console access can do the following:

- Manage their quarantine more robustly.
- Use more flexibility in defining sender addresses from which they want to receive email without filtering (Allow list) or sender addresses they want to block (Deny list).
- Define display preferences of their Spam Reports and Control Console pages.

The user’s primary email address may be defined in one of three ways:

- A Customer Administrator added it manually or with a batch file.
- If SMTP Discovery is enabled, Email Protection may have defined one for the user automatically when it received enough emails to a new email address in the domain. See Auto-Creation and Auto-Deletion of User Accounts (If Email Protection is Enabled).
- If Directory Integration is configured, Email Protection automatically synchronizes to your company’s Active Directory. See Creating new users with Directory Integration.
# Administrative user roles and privileges

As a customer of Email Protection, Web Protection, or Email Archiving applications, you can have administrators who access the Control Console with different levels of privileges within Account Management and within the three applications supported by Account Management.

<table>
<thead>
<tr>
<th>Administrative Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Administrator</td>
<td>The Group Administrator can:</td>
</tr>
<tr>
<td></td>
<td>• Add and remove members from one or more groups if assigned to those groups.</td>
</tr>
<tr>
<td></td>
<td>• Create, edit, and modify Email Protection policies for the assigned groups.</td>
</tr>
<tr>
<td></td>
<td>• View user lists and user details.</td>
</tr>
<tr>
<td></td>
<td>A Group Administrator does not need to be a member of a group in order to have these capabilities.</td>
</tr>
<tr>
<td></td>
<td>⊂ A Group Administrator cannot add or remove a group nor edit user information except for the Group Administrator's own user account.</td>
</tr>
<tr>
<td>Archive Compliance Officer</td>
<td>The Archive Compliance Officer can purge Email Archiving messages from the archive.</td>
</tr>
<tr>
<td>Reports Manager</td>
<td>For an assigned domain, the Reports Manager can:</td>
</tr>
<tr>
<td></td>
<td>• View reports available with Email Protection and/or Web Protection.</td>
</tr>
<tr>
<td></td>
<td>• Manage their own user preferences and all other tasks a user can perform.</td>
</tr>
<tr>
<td>Quarantine Manager</td>
<td>For an assigned domain, the Quarantine Manager can manage the same areas as a Reports Manager. If Email Protection is enabled, Quarantine Managers can also manage all users' quarantine for spam and other problematic messages in an assigned domain.</td>
</tr>
<tr>
<td>Domain Administrator</td>
<td>For an assigned domain, the Domain Administrator can:</td>
</tr>
<tr>
<td></td>
<td>• Manage the same areas as a Quarantine Manager.</td>
</tr>
<tr>
<td></td>
<td>• Manage server setup and authentication rules for the domain.</td>
</tr>
<tr>
<td>Customer Administrator</td>
<td>For all domains and groups, the Customer Administrator can:</td>
</tr>
<tr>
<td></td>
<td>• Manage the same areas as a Domain Administrator or Group Administrator.</td>
</tr>
<tr>
<td></td>
<td>• Manage passwords.</td>
</tr>
<tr>
<td></td>
<td>• Manage all user accounts for the customer.</td>
</tr>
<tr>
<td></td>
<td>• Manage Email Protection policies.</td>
</tr>
<tr>
<td></td>
<td>• Create and edit domain aliases.</td>
</tr>
<tr>
<td></td>
<td>• Create and delete groups.</td>
</tr>
<tr>
<td></td>
<td>• Manage other enabled options, such as Message Audit and Performance Reports.</td>
</tr>
<tr>
<td></td>
<td>⊂ A Customer Administrator cannot create, delete, or edit domains.</td>
</tr>
</tbody>
</table>
### Administrator page access

The following table lists the pages that each administrator role can access.

<table>
<thead>
<tr>
<th>Page Access</th>
<th>Feature Enablement Required</th>
<th>Customer Administrator</th>
<th>Domain Administrator</th>
<th>Quarantine Manager</th>
<th>Group Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branding</td>
<td>Yes. Branding type must be White Label, Co-branding, Private, or Rebrand.</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Distribution Lists</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>MSP Connector</td>
<td>Yes. MSP Connector must be enabled</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Performance Reports</td>
<td>Yes. Performance Reports must be enabled.</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Domains Tab</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain Accounts List</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Create Domain</td>
<td>Yes. Domain Administration must be enabled</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Delete Domain</td>
<td>Yes. Domain Administration must be enabled</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Edit Domain Aliases</td>
<td>Yes. Domain Administration must be enabled</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Page Access</td>
<td>Feature Enablement Required</td>
<td>Customer Administrator</td>
<td>Domain Administrator</td>
<td>Quarantine Manager</td>
<td>Group Administrator</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------</td>
<td>-------------------------</td>
<td>----------------------</td>
<td>--------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Edit Domain</td>
<td>Yes. Domain Administration must be enabled</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Branding</td>
<td>Yes. Branding and Domain Administration must be enabled</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>My Account Tab</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preferences</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Preferences</td>
<td>User Details</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Aliases</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Quarantine</td>
<td>Yes. Email Protection must be enabled.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Email Continuity</td>
<td>Yes. Email Continuity must be enabled.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Allowed Sender</td>
<td>Yes. Email Protection must be enabled.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Blocked Sender</td>
<td>Yes. Email Protection must be enabled.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Archived Messages</td>
<td>Yes. Email Archiving must be enabled.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Users Tab</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Accounts</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>New User</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Edit Users</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Delete Users</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>User Details</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>User Details</td>
<td>Group Administration :</td>
<td>User must be a Group Administrator</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>:User Details</td>
<td>Aliases</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>User Details: Group Membership</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>User Details: Email Protection</td>
<td>Yes. Email Protection must be enabled.</td>
<td>Yes</td>
<td>Yes, Display only.</td>
<td>Yes, Display only.</td>
<td>Yes, Display only.</td>
</tr>
<tr>
<td>User Details: Email Protection: Quarantine</td>
<td>Yes. Email Protection must be enabled.</td>
<td>Yes</td>
<td>Yes, Display only.</td>
<td>Yes, Display only.</td>
<td>No</td>
</tr>
<tr>
<td>Page Access</td>
<td>Feature Enablement Required</td>
<td>Customer Administrator</td>
<td>Domain Administrator</td>
<td>Quarantine Manager</td>
<td>Group Administrator</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------</td>
<td>-------------------------</td>
<td>----------------------</td>
<td>--------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>User Details: Email Protection: Email Continuity</td>
<td>Yes. Email Continuity must be enabled</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>User Details: Email Protection: Allowed Senders List</td>
<td>Yes. Email Protection must be enabled</td>
<td>Yes</td>
<td>Yes. Display only.</td>
<td>Yes. Display only.</td>
<td>No</td>
</tr>
<tr>
<td>User Details: Email Protection: Blocked Senders List</td>
<td>Yes. Email Protection must be enabled</td>
<td>Yes</td>
<td>Yes. Display only.</td>
<td>Yes. Display only.</td>
<td>No</td>
</tr>
<tr>
<td>User Details: Email Protection: Email Activity</td>
<td>Yes. Email Protection must be enabled</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>User Details: Web Protection</td>
<td>Yes. Web Protection must be enabled</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Batch Edit Users</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>User Details: User Synchronization</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Configuration Tab</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Directory Integration</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>User Authentication</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>User Aliases</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Groups tab</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Group List</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>New Group</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Edit Group: Group Details</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Edit Group: Members</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Edit Group: Domain Admins</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Edit Group: Email Protect Policies</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Users who are protected from auto-deletion**

A protected user account is one that cannot be deleted or made inactive via bulk or batch processes, including user synchronization, within the Control Console while the user account is in this status.

This account status is normally used for Customer Administrative-type accounts and prevents accidental deletion, via bulk or batch processes, of the account. For mail delivery, protected accounts are handled in the same way as any other active account.
A Protected - SSO user is a single sign-on (SSO) user who is added to the Control Console through the Application Programming Interface (API). This user cannot be deleted by any method within the Control Console. This type of user can be deleted only through the API.

**Enabling alias address capability for all users**

Enable alias addresses so the Control Console can provide services to user alias addresses as well as to primary email addresses.

**Contents**
- Benefits of alias addresses
- Enable alias address support

**Benefits of alias addresses**

An alias address is an alternate email address for a user that is associated with that user's primary email address. For example, a user might have the primary email address of `joesmith@acme.com` and an alias address of `jsmith@acme.com`, both of which are valid email addresses that receive email in a single primary mailbox.

Alias addresses normally exist in the customer’s Active Directory and allow senders to successfully send email without remembering the precise email address of the user or a new, recently-changed email address. You should enter a users' alias addresses into the Control Console.

The purpose of entering alias email addresses into the Control Console is the following:

- Consolidate emails received for multiple addresses into a single set of messages, or if Email Protection is enabled, a single set of quarantine areas (Virus, Spam, Content, and Attachments).
- Have a single Spam Report sent to the user for all quarantined spam emails. The Spam Report and any emails released from any quarantine are sent to the primary email address.
- Have the emails received for the alias email addresses be filtered using the same configurations defined for the primary email address.

**User alias addresses based on domain aliases**

If the user’s domain has alias domain names associated with it, additional alias email addresses using the prefix from the new alias email address will be created automatically for all the alias domain names. These additional alias email addresses cannot be edited individually and can be deleted only by deleting the relevant alias domain name from the domain.

**Who can configure alias email addresses**

If your role is an End User, Enterprise Domain Administrator, Quarantine Manager or Reports Manager, you cannot configure alias email addresses for other users. Also, you must configure your own personal alias email addresses in the User Aliases page.
Enable alias address support
Enable alias addresses for users so email sent to user alias addresses receives the same protection services that email to primary email addresses receives. You can also limit the number of alias addresses each user can have within the Control Console.

Before you begin
The default settings of the User Aliases page are controlled by the Partner Administrator or higher. If users have already defined alias email addresses in a domain and you change these settings, the settings apply to alias email addresses added thereafter. Any existing alias email addresses are not affected.

For example, if you disable alias email addresses, this action does not delete any currently defined alias email addresses, but prevents any new alias email addresses from being defined.

A current domain link appears for Customer Administrators whose service includes multiple domains. Click the link and use the Select Domain page to select the domain you want.

Task
1. Select Account Management | Configuration.
2. Click User Aliases.
   The User Aliases page is displayed.
3. Select the Allow users to manage user aliases checkbox to allow users to add, change, or remove their own aliases.
4. In the Set limit to [ ] aliases per user field, type a number of aliases each user can have.
5. Click Save.

Defining how users can sign in
If you want users to be able to log into the Control Console, for example to access their messages in Email Archiving or manage their aliases and passwords, you must define an authentication method for them.

The authentication method you define applies to Email Protection, Web Protection, and Email Archiving if these services are active for your company.

If Email Protection is running with Email Archiving, select Email Protection | Policies | Anti-Spam | Reporting and ensure that the Allow non-admin users to login directly to the Control Console option is enabled. Otherwise, no user can access the Control Console to search for and retrieve archived messages. With standalone Email Archiving, where Email Protection is not enabled, users automatically have permission to access the Control Console, provided they have a user address and password.
You must determine which one of the following authentication methods is used for signing in.

- Passwords
- Lightweight Directory Access Protocol (LDAP)
- Internet Message Access Protocol (IMAP)
- POP3

Depending on the authentication type, you might need the host name, access port number, server password, or other information to complete this task. The Control Console enforces password rules if you choose Passwords authentication. If you use LDAP, IMAP, or POP3 authentication, the Control Console uses whatever credentials it receives from your authentication server.

If you use the User Synchronization process to add users, it is recommended that you use LDAP authentication since this method allows you to take advantage of Active Directory and can save you a lot of time.

Set up password method of authentication

Set up password authentication so that users must log into the Control Console by entering a password on the Sign-in page.

**Before you begin**
If this authentication method is selected, each user must have a defined user account with a non-null password in the Control Console. No additional configuration is required to support this authentication method.

This feature does not affect users signing in by clicking a hyperlink in the Email Protection Spam Report.

For option definitions, click Help in the interface.

A current domain link appears for Customer Administrators whose service includes multiple domains. Click the link and use the Select Domain page to select the domain you want.

**Task**
1. Select Account Management | Configuration.
2. Click User Authentication.
3  From the Authentication Type drop-down box, select Passwords.

4  Click Save.

Set up LDAP method of user authentication
You can use the Lightweight Directory Access Protocol (LDAP) passwords defined in your corporate email servers to validate users signing into the Control Console via the Sign-in page.

Before you begin
Your Exchange Server’s Active Directory automatically uses LDAP, such that much of the information you use to configure the LDAP User Authentication is the same as that of the Directory Integration Setup.

To use this method of authentication, you must meet these requirements:

• Each user must have a defined user account in the Control Console.

• Before applying this authentication method, you must confirm connectivity to the authentication server by completing a transaction using a test email address and password.

• For multiple domains, you must test each domain: Select a domain from the drop-down list, configure the domain, click Test, then click Save.

This feature does not affect users signing in by clicking a hyperlink in the Email Protection Spam Report.

For option definitions, click Help in the interface.

A current domain link appears for Customer Administrators whose service includes multiple domains. Click the link and use the Select Domain page to select the domain you want.

Task
1  Collect necessary information about your company’s Active Directory.

2  Select Account Management | Configuration.

3  Click User Authentication.
4 From the Authentication Type drop-down box, select LDAP.

The LDAP Authentication fields are displayed.

![ LDAP Authentication screenshot ]

5 Complete the appropriate fields, and click Save.

**Example of AD LDAP authentication**

The following example illustrates how a customer might set up LDAP authentication.

In the following example, the customer collected the following data from the Active Directory server:

- The Exchange Server’s host name is denver.acme.com.
- The Active Directory server uses SSL.
- The Active Directory server communicates with LDAP over port 636, because SSL is turned on.
- The administrative user name that has been administered for Email Archiving to use for synchronization is sync. sync is associated with the Users directory.
- The domain name is the same as the host name, denver.acme.com.
- The password that the sync user name uses is test123.
- **Users** is the directory within Active Directory that contains all the users for authentication synchronization.
- The test email address that has been administered on the Exchange Server and Active Directory is testsync.denver.acme.com. The password is set to abcd123.
### Table 4-1 Sample field entries

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Type:</td>
<td>Exchange 2003</td>
</tr>
<tr>
<td>Server Hostname:</td>
<td>domain.com OR IP address</td>
</tr>
<tr>
<td>Enable SSL:</td>
<td>Select the checkbox if your LDAP server uses SSL. Then enter 636 in Server Port: below.</td>
</tr>
<tr>
<td>Server Port:</td>
<td>389 (unless your server uses SSL, then use 636)</td>
</tr>
<tr>
<td>Search BIND DN:</td>
<td>cn=Directory Manager</td>
</tr>
<tr>
<td>Search BIND Password:</td>
<td>Enter the password for the Directory Manager.</td>
</tr>
<tr>
<td>Search Base DN:</td>
<td>ou=Person,dc=domain,dc=com</td>
</tr>
<tr>
<td>Test Email Address:</td>
<td>Enter a valid, working email address. For example, <a href="mailto:admin@domain.com">admin@domain.com</a></td>
</tr>
<tr>
<td>Test Password:</td>
<td>Enter a password for the working email address.</td>
</tr>
</tbody>
</table>

**Definitions**

cn = common name (for example, Directory Manager)

dc = domain component (for example, for the domain "domain.com" use two dc items: dc=domain,dc=com)

ou = object class (for example, Person)

### Set up IMAP method of user authentication

IMAP Authentication designates that the Internet Message Access Protocol (IMAP) defined in your corporate email servers is used to validate users logging into the Control Console via the Sign-in page.

**Before you begin**

To use this method of authentication, you must meet these requirements:

- Each user must have a defined user account in the Control Console.
- Before applying this authentication method, you must confirm connectivity to the authentication server by completing a transaction using a test email address and password.
- For multiple domains, you must test each domain: Select a domain from the drop-down list, configure the domain, click Test, then click Save.

This feature does not affect users signing in by clicking a hyperlink in the Email Protection Spam Report.

For option definitions, click Help in the interface.

A current domain link appears for Customer Administrators whose service includes multiple domains. Click the link and use the Select Domain page to select the domain you want.

**Task**

1. Select Account Management | Configuration.
2. Click User Authentication.
3. From the Authentication Type drop-down list, select IMAP.

The IMAP Authentication fields are displayed.

4. Complete the appropriate fields, and click Save.

**Set up POP3 method of user authentication**

POP3 Authentication designates that the Post Office Protocol 3 (POP3) defined in your corporate email servers is used to validate users logging into the Control Console via the Sign-in page.

**Before you begin**

To use this method of authentication, you must meet these requirements:

- Each user must have a defined user account in the Control Console.
- Before applying this authentication method, you must confirm connectivity to the authentication server by completing a transaction using a test email address and password.
- For multiple domains, you must test each domain: Select a domain from the drop-down list, configure the domain, click Test, then click Save.

This feature does not affect users signing in by clicking a hyperlink in the Email Protection Spam Report.

For option definitions, click Help in the interface.

A current domain link appears for Customer Administrators whose service includes multiple domains. Click the link and use the Select Domain page to select the domain you want.

**Task**

1. Select Account Management | Configuration.
2. Click User Authentication.
3  From the Authentication Type drop-down box, select POP3.

The POP3 Authentication fields are displayed.

4  Complete the appropriate fields, and click Save.

Setting the default time zone

Setting a default time zone enables the Control Console to automatically assign the time zone to users when those users are automatically created in the Control Console with Directory Integration or SMTP Discovery.

Contents

- Aspects of user time zones you need to consider
- Set default time zone for users

Aspects of user time zones you need to consider

The time zone is used to timestamp the events related to the user in the Control Console (for example, the email arrivals in quarantine).

You can set the time zone for individual users on the Create User or Edit User pages. You can also set a default time zone for all users on the Customer Details page. Finally, if a user has permissions to the Control Console, the user can change his or her time zone on the Preferences tab. The default time zone is applied to all user accounts for the customer unless you or the user manually sets an individual user's time zone later.
The time zone represents the offset from Greenwich Mean Time (GMT) to the local time zone for the user of the user account. The time zone name is provided only for assistance. Use the hourly offset to determine which time zone to select. This setting does not affect the user's local machine (for example, it does not change the Windows time zone settings).

If you select a time zone different from the one used by the Email Protection data center, quarantined emails might appear on different dates in the quarantine area. For example, if the user's local time zone is set to New York, but the data center's time zone is Los Angeles, the user's local date will change at midnight in the local time zone, but the data center will still be using the previous day's date until it is 3:00 am in the local time zone. In this case, any emails that were quarantined after the local time zone passed midnight and until 3:00 am will still be listed for the previous day's date. Thus, you would have to select yesterday to view the email's quarantined from midnight to 3:00 am in the local time zone.

When the time zone for the data center passes midnight, its local date will then match the local date for the user. You can display all the emails in a quarantine area to compensate for this behavior.

Set default time zone for users

To automatically assign a default time zone to users who are automatically added to the Control Console, you must set a default time zone on the Customer Details page.

**Task**

1. Select Account Management | Customers | Details.

   The Customer Details page is displayed.

2. Next to the Time Zone Default field, click Update.

   An Update Time Zone Default page is displayed.

3. From the Time Zone Default drop-down list, select a time zone for your users, then click Update.
Adding users to the Control Console

After you have added users to the Control Console, they can begin to receive services. They can also manage their alias addresses and group assignments, customize spam filtering, and review their email or web activity.

Contents

- Automatic creation of user accounts (for Email Protection only)
- Review current list of users
- Add individual users manually
- Add users with a batch file
- Create administrator accounts
- Creating new users with Directory Integration

Automatic creation of user accounts (for Email Protection only)

SMTP Discovery automatically creates a user account in the Control Console after eight emails, within a rolling 24-hour period, have been successfully delivered to that user's primary email address. SMTP Discovery, which is enabled by default when a customer is subscribed to Email Protection, is a convenient way to add users to your service without any effort by you or other administrators.

If the user account does not receive enough messages by the time Message 1 expires, the expiration point for Message 2 becomes the new 24 hour period by which eight messages need to be delivered. This process continues until the full eight messages are delivered to the user account. When the account is created, the user is automatically assigned the role of "user."

Passwords for user sign-in to the Control Console are not included in SMTP Discovery. If you establish Password authentication as the authentication method for signing into the Control Console, then passwords must be self-assigned by the users when they sign-in, or an administrator must assign them on behalf of the users.

Email is still being filtered and flow continues for all users using the default inbound policy before the primary user account in the Control Console is auto-created. Once the criteria are met and the user account is created, messages to that user account are delivered according to the customer's email filtering policy.

The service will not re-create an account that already exists in the Control Console.

The Email Protection service automatically creates new user accounts if all the following is true:

- SMTP Discovery is enabled. SMTP Discovery, which is enabled by default, is a convenient way to add users to your service. However, this capability might also add users who are not real users at your company and not add users who are real.

- Three to eight emails for that email address have been received, passed filtering, and accepted by your email server within a configured time period (typically, a single day).

- A user account does not exist for the email address in the designated domain.

- The emails were not addressed to an alias domain name.

You use the User Creation Settings page within Email Protection to turn on or turn off SMTP Discovery. The SMTP Discovery capability of Email Protection also automatically deletes new user accounts.
Review current list of users

Review the current list of users for whom you are responsible. From the list, you can create new users, delete users no longer needing service, and access accounts of users for whom you want to change service or account information.

Before you begin

Group Administrators, Quarantine Managers, and Domain Administrators, as well as Customer Administrator and higher roles, can view user lists.

For option definitions, click Help in the interface.

Task

- Select Account Management | Users.

The User List page is displayed.

For a Quarantine Manager or Domain Administrator, only users in the administrator’s domain are displayed. The list displays the following information, as administered in the Control Console or as created via SMTP Discovery.

Tasks

- Filter the User List on page 44
  You can filter the list of users on the User List page based on one or more criteria you specify. To filter the User List page so that only users that match criteria you select are listed:
  - Change the columns of data displayed in the User List on page 45
    You can select which columns of data are displayed in the User List so that you can see all available data for each user or a subset of that data.
  - Create a .csv file of user data on page 45
    You can create a .csv file of user data to save data included on the Users List page to use for other purposes. You can also edit the user data in a .csv file that you downloaded and upload that file to the Batch Edit Users page.
Filter the User List

You can filter the list of users on the User List page based on one or more criteria you specify. To filter the User List page so that only users that match criteria you select are listed:

For option definitions, click Help in the interface.

Task

1. Select Account Management | Users.

2. In the User List page, place your cursor on the column heading whose criteria you want to use for filtering. Filter criteria are available on the following columns:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Address</td>
<td>List only user addresses that start with, contain, or equal the characters you enter. Domain aliases and public domain addresses are not listed.</td>
</tr>
<tr>
<td>Username</td>
<td>List only user names that start with, contain, or equal the characters you enter.</td>
</tr>
<tr>
<td>Last Signed In</td>
<td>List only users who signed in before, after, or on a specific date and time. You can also create a range of time based on the use of the Before and After options together.</td>
</tr>
<tr>
<td>Date Created</td>
<td>List only users who were created before, after, or on a specific date. You can also create a range of time based on the use of the Before and After options together.</td>
</tr>
<tr>
<td>Status</td>
<td>List only users who have one or two of the following statuses: Active, Inactive, Protected.</td>
</tr>
<tr>
<td>Primary/Alias</td>
<td>List users who are primary addresses only or aliases only.</td>
</tr>
<tr>
<td>Type</td>
<td>List only users or distribution lists, instead of both.</td>
</tr>
</tbody>
</table>

3. Click the column’s down arrow to display the first menu.

4. Use your cursor to highlight Filters.

5. From the Filter submenu, click the checkbox for the specific filtering option you want. You might also have to enter a value with which to select data as, for example, when filtering by Email Address.
Change the columns of data displayed in the User List
You can select which columns of data are displayed in the User List so that you can see all available data for each user or a subset of that data.
For option definitions, click Help in the interface.

Task
1  Select Account Management | Users.
2  From the User List page, click the down arrow of any column heading and select Columns from the menu.

A list of data types appears.
3  Select the checkboxes for the types of data you want to display.

Create a .csv file of user data
You can create a .csv file of user data to save data included on the Users List page to use for other purposes. You can also edit the user data in a .csv file that you downloaded and upload that file to the Batch Edit Users page.

You can download more data types from the User List page than you can upload in a batch file to the Batch Edit Users page. For example, you can download the user type and date created information from the Users List page, but you cannot edit the user type or date created by uploading a batch file. If you upload a batch file that contains more data columns than are allowed in the Batch Edit Users page, those extra columns are ignored in the upload.

For option definitions, click Help in the interface.

Task
1  Select Account Management | Users.
2  Click the down arrow of any column heading and select Columns from the menu.
3  Select the checkboxes for the types of data you want to include in the file.
4  Click Download.
   The Download page appears.
Select one of two options:

- Grid Content — Includes the data currently displayed in the Users List page.
- Customized Content — Enables the Download Field list; select the data types to include.

Primary email addresses are downloaded automatically, regardless of the other data types you select. Conversely, alias addresses are never downloaded, regardless of the data types you select.

If you include time zone data in the .csv file, only the time zone name for each user is included. Time zone offsets to Greenwich Mean Time (GMT) are not included. However, you can modify the file to add or modify users and upload it again on the Batch Edit Users page. The Control Console then automatically recalculates and displays the GMT offset for each user, based on the time zone names in the file.

Click Download and save the .csv file in Microsoft Excel.

Add individual users manually

Add, one-by-one, user email addresses to the Control Console so Email Protection, Email Archiving, or Web Protection services can be applied to them. A highly-recommended alternative to this task is to use Directory Integration so that you can add all users in your company's Active Directory with a single click of a button.

For Email Archiving, the following cautions apply:

- You must add your users to the Control Console before setting up your first Archiving Mail Source. Any emails archived for a user before the user account and all aliases are created will be searchable and viewable only by the Customer Administrator.
- All user level legal holds will not be available until user accounts are created. For more information see the Email Archiving Administrator Guide and Online Help.

Users' email addresses might already exist if your service already includes Email Protection, Email Archiving, or Web Protection.

You cannot add a user with the status Protected - SSO using the Control Console. This type of user must be added using the Application Programming Interface (API).

For option definitions, click Help in the interface.

Task

1. Select Account Management | Users.
2. Click New.
3 In the **Creation Modes** drop-down list, select Individual.

The Create New User fields are displayed.

![New User interface](image)

4 Complete the appropriate fields, and click **Save**.

**Add users with a batch file**

The **New User** page allows you to create multiple user accounts by either entering multiple email addresses or uploading a predefined text or .csv (Excel) file containing a list of the new email addresses and optional user names and alias email addresses.

For option definitions, click **Help** in the interface.
**Task**

1. Open a text editor, for example Notepad, to create your file of addresses.

2. On the first line of the file, type the primary domain address for a user, followed by a user name separated by commas, and any other alias addresses desired separated by commas. The user name does not include a domain name suffix. See the following example:

   Example: "smith,j"@acme.com, joesmith, joestsmith@acme.com, jsmith@denver.acme.com, joemith@denver.acme.com

   If the local name, or handle, portion of an email address contains commas, you must enclose that portion of the address in double-double quotes (" ").

   Example: "smith,j"@acme.com, joesmith, joestsmith@acme.com, jsmith@denver.acme.com, joemith@denver.acme.com

   If you do not include a user name for a user, you must still include the commas to specify that there is no user name.

   Example: jsmith@acme.com, , joesmith@acme.com

   Up to five aliases can be created per user, depending on your company’s configuration. The alias addresses must be full-qualified domain addresses, but can have domains that are different from the primary email address. Only one user name is allowed per user.

3. Press Enter or an equivalent key to create a hard return and start a new line in the file.

4. Create one line of addresses per user. Email addresses must be unique.

5. Save the file to your computer’s hard drive with a file name of your choice.

   The file size can be up to 100 KB. A .csv file for batch edit users can be encoded in any of the following formats:
   - UTF-8 without Byte Order Mark (BOM)
   - UTF-8 with BOM
   - UCS2 - Big Endian
   - ANSI (See note below)
   - UCS2 - Little Endian

   These formats apply to both single-byte (such as French or Russian) and double-byte (such as Traditional Chinese, Japanese) characters. By default, Notepad and Microsoft Excel support single-byte ANSI formats only. As a result, double-byte characters might not be saved correctly in ANSI using these editors. Therefore, if you are creating a .csv file in Notepad or Excel and are including multibyte characters, it is recommended that you save the file in UTF-8 without BOM encoding.
6 Select Account Management | Users.

7 Click New.

8 From the Creation Mode drop-down list, select Batch.

The New User page changes to show batch creation fields.

9 Click Browse. Search for and select the file you just created.

10 Click Upload File.

11 Complete the appropriate fields, and click Save.

Create administrator accounts

You or another administrator for your company should have been given a Customer Administrator user address by your service provider. Depending on your business needs, you can add other administrators with equal or more limited administrative privileges.

Before you begin

This procedure can be performed only by a user with the role of Customer Administrator or higher.

For option definitions, click Help in the interface.
**Task**

1. Decide what administrative role each administrator should have.
2. Click *Account Management* | *Users*.
3. Click *New*.
4. In the *Creation Modes* drop-down list, select *Individual*.
5. In the *Email Address* field, type the handle or prefix portion of the administrator’s email address.
6. In the drop-down list that follows *Email Address* field, select the domain of the administrator. If the administrator has an address in more than one domain, select the domain for the address that should be the administrator’s primary address.
7. From the *Role* drop-down menu, select one of the following administrative roles for the administrator:
   - Reports Manager
   - Archive Compliance Officer
   - Group Manager
   - Quarantine Manager
   - Domain Administrator
   - Customer Administrator
8. From the *Type* drop-down list, select *User*.
9. Complete other fields as appropriate, and click *Save*.

### Creating new users with Directory Integration

Use Directory Integration to automatically synchronize the Control Console with the user accounts in your company’s Active Directory. This synchronization automatically adds to the Control Console all, or large numbers of, users.

### Contents
- What is Directory Integration
- Set up Directory Integration
- Schedule Directory Integration to run
- Enable Directory Services Connector
- Run review and approve user synchronization manually
- Review historical user synchronizations
- Download the User Synchronization History page
- How Directory Services Connector affects what you do on the Control Console

### What is Directory Integration

Use Directory Integration to automatically synchronize the Control Console with the user accounts in your company’s Active Directory. This synchronization automatically adds to the Control Console all, or large numbers of, users.

Because you can save time and ensure a high level of accuracy, it is recommended that you use Directory Integration to add user email addresses to the Control Console. Directory Integration is especially important if you are using Intelligent Routing. See the *Intelligent Routing User Guide*.
Active Directory domain or email domain

You must choose whether you want to synchronize an Active Directory domain or an email domain. When you synchronize an Active Directory domain, the synchronization can include multiple email domains that are part of the tree or forest structure containing the domain you specify. In this case, each user account is synchronized and all email addresses, for all domains known to the Active Directory domain, for those user accounts are synchronized.

For example, if a user has a primary email address in Active Directory of jsmith@acme.com, but the user also has the email addresses jsmith@denver.acme.com and jsmith@sales.acme.com, the primary email address is synchronized, and the other two email addresses are synchronized as alias addresses.

To synchronize Active Directory domains, you must use Directory Services Connector (see "Directory Services Connector"). You cannot synchronize an Active Directory domain using the Control Console.

When you choose to synchronize by email domain, you specify just that domain, and only user email addresses in that domain are synchronized. Thus, if the user has the email address jsmith@acme.com and jsmith@denver.acme.com, and you synchronize domain acme.com, the synchronization will include jsmith@acme.com, but not jsmith@denver.acme.com.

You can perform email domain level synchronizations using the Control Console. Legacy customers can also use the old version of Directory Services Connector, version 1.1, though this version is no longer available to download.

Directory Services Connector

As an alternative to using Directory Integration from the Control Console, you can synchronize your Active Directory (AD) using the Directory Services Connector, which is an add-on package to McAfee ePolicy Orchestrator (McAfee ePO). The Directory Services Connector, because it is on your company premises, initiates a connection from your ePO and AD and "pushes" data to the Control Console. In contrast, when you set up and run Directory Integration from the Control Console, the Control Console initiates a connection to your Active Directory and "pulls" data from it. Unlike synchronizations run from the Control Console, Directory Services Connector also allows you to synchronize all email addresses identified in the Active Directory domain, including those that are in different email domains. From the Control Console, you must synchronize the addresses in one email domain at a time.

The Directory Services Connector also allows you to synchronize groups in AD domains so that groups in the Control Console match groups in the AD domain. This capability also allows the Directory Services Connector to automatically assign users to groups in the Control Console when you run an AD domain synchronization.

To configure the Control Console so that it will accept and add users sent from the Directory Services Connector, select AD Domain in the Logical Structure field on the Directory Integration page. With AD Domain selected, links appear on the Directory Integration page so you can download the Directory Services Connector Setup Guide and download the Directory Services Connector software extension that you install within your McAfee ePO.

With pre-release-3.2 versions of Directory Services Connector, though you may have run a synchronization with the Directory Services Connector, you can still review and approve the results of that synchronization in the Control Console. For Directory Services Connector, 3.2 or later, you must approve the AD domain synchronizations through the Directory Services Connector only.
How does Directory Integration synchronize the user data

When run the first time, Directory Integration pulls all user email addresses from your Active Directory and creates accounts for those users. When run subsequently, Directory Integration does the following:

- Synchronizes its list with the Active Directory.
- Adds any new users to the Control Console.
- Tags users that are no longer in the Active Directory so you can delete them from the Control Console.
- Synchronizes users to groups only if you added the groups with Directory Services Connector. For groups that you manually add using the Control Console, you must continue to assign users to those groups only through the Control Console.

You can run Directory Integration manually or schedule it to run automatically at intervals you define.

Limitations on Directory Integration

Directory Integration has limitations, which apply whether the data is pushed from Directory Services Connector or pulled from the Control Console.

- You must run separate synchronizations for each Active Directory domain.
- You cannot limit the number of synchronization changes, except for changes from active to inactive status.
- Group synchronizations fail if an Active Directory group contains more than 25,000 users. The Control Console limits group membership to 25,000.
- You must use Active Directory.
- Directory Services Connector does not run on McAfee ePO version 4.6.0 and requires version 4.6.1 through 5.0.

Set up Directory Integration

Use the Directory Integration page to setup and test Active Directory (AD) authentication prior to synchronizing users. As an alternative, use the Directory Integration page to establish that you are using Directory Services Connector to synchronize your users (the push option in the Data Collection field). For directory integration to work, your AD server must be reachable via either a static IP address or a resolvable hostname.

Before you begin

The following restrictions apply:

- If Email Protection is running with Email Archiving, you must access Email Protection | Policies | Spam | Reporting and ensure that the field Allow non-admin users to login directly to the Control Console is enabled. Otherwise, no user can access the Control Console to search for and retrieve archived messages.

- With standalone Email Archiving, where Email Protection is not enabled, users automatically have permission to access the Control Console, provided they have a user address and password.
• Only a user with the role of Customer Administrator or higher can add, edit, or delete users.
• You cannot add a user with the status Protected - SSO using the Control Console. This type of user must be added using the Application Programming Interface (API).

If you use Directory Integration, explicit user creation is highly-recommended. See Set up User Creation Mode — SMTP Discovery or Explicit in the Email Protection Administrator Guide.

For option definitions, click Help in the interface.

**Task**
1. Collect necessary information about your company’s Active Directory.
2. Select Account Management | Configuration.
3. If necessary, click Directory Integration.
4 If necessary, from the Logical Structure drop-down list, select Email Domain.

The Directory Integration page is displayed.

5 Complete the appropriate fields, then click Save.

If you select AD Domain in the Logical Structure field, no other fields are displayed since the setup for the user synchronization must actually occur in the Directory Services Connector run from the customer’s premises. Any schedule of synchronizations previously defined in this page is discontinued. In addition, links appear on the Directory Integration page so you can download the Directory Services Connector Setup Guide and download the Directory Services Connector software extension that you install within your McAfee ePO.

Schedule Directory Integration to run
You can set up Directory Integration to run automatically according to a schedule you define so that the users within the Control Console always match those listed in your Active Directory.

Before you begin
If you selected AD Domain in the Logical Structure field on the Directory Integration page, the Sync button on the User List page is grayed out. Any schedule of synchronizations previously defined in this page is disabled. You must instead run Directory Integration using Directory Services Connector run from the customer’s premises. To download the Directory Services Connector software and Setup Guide, see the Directory Integration page.
Task
1 Select Account Management | Configuration.
2 If necessary, click Directory Integration.
3 If necessary, complete the appropriate fields in the Directory Settings portion of the page.
4 Click the Enable Automatic Synchronization and Approval checkbox.
5 From the Schedule drop-down list, select one of the following:
   • Once Per Day
   • Twice Per Day
   • Four Times Per Day
   If Enable Automatic Synchronization and Approval is on, then the first synchronization starts on the hour after you click Save. For example, if you click Save at 10:40 a.m., the first automatic synchronization will begin at 11:00 a.m. If you select Twice Per Day as the schedule, the next automatic synchronization will occur at 11:00 p.m.
   You cannot review and approve a scheduled synchronization. It is approved automatically.
6 In the User Deactivation Limit field, type a number to limit the number of addresses that can be changed from Active to Inactive when an automatic synchronization runs. The limit you enter can prevent an inadvertent change to inactive status on large numbers of addresses, an occurrence that would require a lot of manual work in the Control Console to correct.
7 Click Save.

Enable Directory Services Connector
To use the Directory Services Directory for user synchronization, you must set the Control Console to accept user synchronization data created from the Directory Services Connector.

Task
1 Select Account Management | Configuration.
2 Click Directory Integration.
3 From the Logical Structure drop-down list, select AD Domain.
   No other configuration fields are displayed, since you must use the Directory Services Connector to set up a user synchronization.
4 Click the Directory Services Connector Setup Guide link to download the documentation for installation and configuration of Directory Services Connector.
5 Click the Directory Services Connector Extension link to download the Directory Services Connector software.
You must then install this software in your McAfee ePolicy Orchestrator.

6 Click Save.
The Control Console now is ready to accept synchronization data created from the Directory Services Connector.

Even though you run a synchronization with the Directory Services Connector, you can still use the Review and Approve buttons on the User Synchronization page in the Control Console to review/approve the results of that synchronization.

Run review and approve user synchronization manually
After you have set up Directory Integration, you can manually run a user synchronization to add users identified in your company’s Active Directory (AD) into the Control Console. In this way, you can add all users who are in a single email domain at once, rather than adding the users individually or using SMTP Discovery.

**Before you begin**
Before you start the synchronization process, check the Edit User page for your own account to make sure your administrator email address is in the "Protected" state. This state ensures you can sign in later.

If you selected AD Domain in the Logical Structure field on the Directory Integration page, the Request Sync button on the User Synchronization page is hidden. You must run Directory Integration from the customer’s premises using Directory Services Connector. To download the Directory Services Connector software and Setup Guide, see the Directory Integration page.

Even if you run a synchronization with the Directory Services Connector, you can use the Review button on the User Synchronization page to review results. However, if you run the synchronization from Directory Services Connector, 3.2 or later, you must use Directory Services Connector to approve or reject the synchronization. The Approve and Reject buttons are grayed out on the User Synchronization Details page for synchronizations run with Directory Services Connector, 3.2.

For option definitions, click Help in the interface.
**Task**

1. Select **Account Management | Users**.

2. From the **User List** page, click **Sync**. The **User Synchronization** page is displayed.

   - Synchronizations that ran automatically according to the schedule on the **Directory Integration** page are automatically approved and appear on the **User Synchronization** page in the **Sync History** list.

3. Click **Request Sync**.

   If the synchronization is successful, you see the message **User Sync Successfully Initiated: {time_stamp}** above the **Status** area. The message changes to **Updated synchronization data is available** when the synchronization is complete.

   - The amount of time between the request to synchronize users and the "Updated synchronization data is available" message is determined based on the connection speed for the Active Directory and the number of users who are contained within the Active Directory.
4 Click Review.

The User Synchronization Details page is displayed.

The Group Changes and Group Membership tabs are also available.
5 Review all users listed on all tabs in the User Synchronization Details page.

6 If the data is correct, click Approve. If the data is not correct, click Reject.

If the synchronization was run from Directory Services Connector, 3.2 or later, the Approve and Reject buttons are grayed out. You must approve or reject the synchronization from Directory Services Connector, not from the Control Console.

Tasks

- **Filter the User Synchronization Details page on page 59**
  You can filter the list of users on the User Synchronization Details page based on one or more criteria you specify.

- **Change the columns displayed on the User Synchronization Details page on page 60**
  You can select which columns of data are displayed in the User Synchronization Details page so that you can see all available data for each address.

- **Download the User Synchronization Details page on page 61**
  Download the data from the User Synchronization Details page to save a copy as a .csv file.

**Filter the User Synchronization Details page**

You can filter the list of users on the User Synchronization Details page based on one or more criteria you specify.

For option definitions, click Help in the interface.

**Task**

1 In the User Synchronization Details page, place your cursor in the column heading whose criteria you want to use for filtering.

2 Click the column's down arrow to display the first menu.
3 Use your cursor to highlight Filters.

4 From the Filter submenu, click the checkbox for the specific filtering option or options you want. You might instead have to enter a value with which to select data as, for example, when filtering by Primary Address.

Change the columns displayed on the User Synchronization Details page

You can select which columns of data are displayed in the User Synchronization Details page so that you can see all available data for each address.

**Task**

1 On the User Synchronization Details page, click the down arrow of any column heading and select Columns from the menu.

A list of data types appears.

2 Select the checkboxes for the types of data you want to display.
Download the User Synchronization Details page
Download the data from the User Synchronization Details page to save a copy as a .csv file.

Task
• From the User Synchronization Details page, click Download.

The Control Console automatically generates a .csv file which you can save or open, normally using Microsoft Excel.

Review historical user synchronizations
You can review a user synchronization that you or another administrator previously approved or rejected. You cannot approve or reject a synchronization data set in the Sync History list since it has already been approved or rejected.

The Review button on the User Synchronization page allows you to review synchronizations that were initiated from a "push" run from the Directory Services Connector.

For option definitions, click Help in the interface.

Task
1. Select Account Management | Users.
2. Click Sync.
3. From the User Synchronization page, double-click a synchronization data set in the Sync History list.

You cannot review a failed synchronization data set because no synchronization actually occurred. But on the Directory Integration page, if you selected exception notifications to be sent to a distribution list, the notifications would provide information about the failed synchronization.

4. Review all users listed on all tabs on the User Synchronization Details page.

Download the User Synchronization History page
Download the User Synchronization History page to save the page as a .csv file.

Task
1. Click Account Management | Users | Sync.
2. If necessary, select the domain you want from the User Synchronization for drop-down list at the top of the page.
3. Click Download.

The Control Console automatically generates a .csv file which you can save or open, normally using Microsoft Excel.
How Directory Services Connector affects what you do on the Control Console

When you use Directory Services Connector, the way you can use Directory Integration on the Control Console changes.

When you select **AD Domain** in the **Logical Structure** field to enable Directory Services Connector, the following changes occur in the Control Console:

- The remaining fields of the **Directory Integration** page disappear since they do not apply. However, links from which you can download Directory Services Connector software and the **Setup Guide** are displayed.
- You can no longer manually run Directory Integration from the Control Console.
- Any previously-established schedule in the Control Console for automatically running Directory Integration is disabled.
- Exception notifications are defined and displayed in the Directory Services Connector, not in the Control Console.
- For Directory Services Connector to run synchronizations, you are required to set up a distribution list in the Control Console, if one doesn’t already exist.

With pre-3.2 versions of Directory Services Connector, though you may have run a synchronization with the Directory Services Connector, you can still review and approve the results of that synchronization in the Control Console. For Directory Services Connector Version 3.2 or later, you must approve the AD domain synchronizations through the Directory Services Connector only.

Changing back from "push" to "pull" mode

If, after you have been using Directory Services Connector, you change the **Logical Structure** field back to **Email Domain** in the **Directory Integration** page in the Control Console, Directory Services Connector will no longer be able to run a synchronization. Any schedule in the Directory Services Connector for running synchronizations is disabled.

Managing existing users one-by-one

After you have added users to the Control Console, you can manage their alias addresses and group assignments, customize spam filtering, and review their email or web activity.

Contents

- View or edit user accounts
- Managing user alias addresses
- Protect a user from automatic deletion or deactivation
- Reset user passwords
- Unlock user accounts
- Change user roles or active status
- Change display preferences and time zone for a user
- Editing multiple users at one time
- Customize spam filtering for a user
- Review email activity of a user
- Review web activity of a user
- Assign a user to a group
- Assign groups to a Group Administrator
- Deleting Users
**View or edit user accounts**

To view the basic settings for an individual user, access the **Edit User: Details** tab for that user.

**Before you begin**

Only a user with the role of Customer Administrator or higher can add, edit, or delete users.

For option definitions, click **Help** in the interface.

**Task**

1. Select **Account Management | Users**.
2. Select a user and click **Edit**.

The **Edit User: Details** tab is displayed.

3. Complete the appropriate fields, and click **Save**.
Managing user alias addresses

Add user alias email addresses to the Control Console to ensure that those addresses receive services as well as the users' primary email addresses.

Only Customer Administrators and higher-level roles can add, change, or delete another user's alias addresses.

If your company is using Intelligent Routing, you can also enter public domain addresses.

If a domain has alias domain names associated with it, alias email addresses are created automatically for all alias domain names. These additional alias email addresses cannot be edited individually and be deleted only by deleting the relevant alias domain name from the domain. For example, if you disable alias email addresses, this action does not delete any currently defined alias email addresses. Instead, it prevents any new alias email addresses from being defined.

Contents
- Add alias addresses for users
- Add public domain addresses for users
- Change a user alias address to the primary address
- Delete a user alias address

Add alias addresses for users

For each user's primary email address, add all their alias addresses. By associating these addresses, you ensure that all email and archiving services apply to aliases in the Control Console.

You are limited to a total of 500 aliases.

For option definitions, click Help in the interface.

Task
1. Select Account Management | Users.
2. Select a user and click Edit.
   The Edit User window opens.
3 Select Aliases.

4 Under the User Alias Address heading, in the blank field before the "@" sign and domain name, type the user's name portion of the alias address.

5 In the drop-down list that follows the User Alias Address field, select the domain of the user address.

6 Click New.

The address is listed in the User Alias Address section. A confirmation email is sent to the alias address and the Date Created column displays the word Pending. The user must access that email and access a link provided in the email for the alias to become active in the Control Console.

7 Click Apply.

The address is listed in the Domain Alias section for the primary domain and for any domain aliases that might be defined.

- If the address you assigned as an alias had been a primary user address, it is no longer considered a primary address.

- When a domain is deleted from the Control Console, users in that domain, including users' alias addresses, are deleted. These deletions occur even for alias addresses that have a different domain name.

Add public domain addresses for users

To allow the Control Console to apply Email Protection services to a user's public domain address (for Intelligent Routing), you must add the public domain address to the Control Console and associate it with a primary user address.

Before you begin

- Only a user with the role of Customer Administrator or higher can add, edit, or delete users.

For option definitions, click Help in the interface.
Task
1. Select Account Management | Users.
2. Select a user and select Edit | Aliases.
3. Under the Public Domain Address heading, in the blank field that is followed by the "@" sign and domain name, type the user's handle, or name, portion of the public domain address.
4. In the domain drop-down list that follows the "@" sign, select the public domain portion of the user address.
   
   ![Only public domains that are associated with the domain of the user's primary address are listed in the drop-down menu.]
5. Click New.
   The address is listed in the Public Domain Address section.
6. Click Apply.
   The address is listed in the Domain Alias section for the public domain.

Change a user alias address to the primary address
Change a user's alias address to the user's primary address so that the user can use the new primary address to receive Spam Reports, access the quarantine for the address and associated aliases, and use the email and web filtering policies assigned to that address.

Before you begin
Only a user with the role of Customer Administrator or higher can add, edit, or delete users.

If an existing primary user account is redefined as an alias email address, the user-level configurations (for example, user-level policy configurations, Allow and Deny lists, etc.) for the existing user account will be deleted after the changes are saved in this tab. Quarantine data for the existing user account will be merged into the quarantine data for the primary email address to which it is being associated as an alias email address. Thereafter, the new alias email address will use the configurations defined for the primary email address.

For option definitions, click Help in the interface.

Task
1. Select Account Management | Users.
2. Select a user and click Edit | Aliases.
3. Find the alias address you want to change, and click the Change to Primary button.
4. Click Apply.
   The address is listed in the Edit User: Details tab header. The former primary address is listed as an alias.
Delete a user alias address
Delete an alias address that is no longer available in your email server or Active Directory.

**Before you begin**

Only a user with the role of Customer Administrator or higher can add, edit, or delete users.

For option definitions, click Help in the interface.

**Task**
1. Select Account Management | Users.
2. Select a user and select Edit | Aliases.
3. Find the alias address you want to delete, and select the Delete checkbox.
4. Click Apply.

The address is removed from the list of aliases.

Protect a user from automatic deletion or deactivation
Use the Edit User: Details tab to protect a user from deletion or deactivation due to a synchronization with Active Directory or a batch update process.

**Before you begin**

A Protected - SSO (single sign-on) user has the following limitations:
- Cannot be added directly using the Control Console.
- Can be added to the Control Console only through the Application Programming Interface (API).
- Cannot be deleted by any method within the Control Console.
- Can be deleted only through the API.

For option definitions, click Help in the interface.

**Task**
1. Select Account Management | Users.
2. Select a user account, and click Edit | Edit.
3. In the Edit User: Details tab, from the Status drop-down list, select Protected.
4. Click Apply.
Reset user passwords
A user can normally retrieve the Control Console password independently by requesting the password and then answering a security question. However, if a user forgets the password, you might need to reset it.

**Before you begin**

Only a user with the role of Customer Administrator or higher can add, edit, or delete users.

Remote authentication affects password resets:
- If you use remote LDAP, IMAP, or POP3 authentication for users, the password you reset will normally be replaced the next time the Control Console synchronizes with the remote authentication server.
- If the user is a Customer Administrator or Domain Administrator, and that user is not also defined in the remote authentication server, the remote authentication synchronization will not affect the password you reset for that user.

You can also update user passwords using the **Batch Edit Users** page, which is available from the Edit drop-down menu on the **Users** tab. This page allows you to update passwords for selected users or upload a file with password updates.

For option definitions, click **Help** in the interface.

**Task**

1. Select **Account Management** | **Users**.
2. Select a user and click **Edit**.
3. At the **Password** field, click **Change**.
4. In the **Password** field, type the new password.
5. In the **Confirm Password** field, type the new password again.
6. Click **Apply**.

**Unlock user accounts**
If a user attempts to sign in unsuccessfully five times within a 30 minute period, the user’s account is locked for 30 minutes. You can unlock the user’s account right away on the Control Console.

**Task**

1. Select **Account Management** | **Users**.
2. Select a user and click **Edit** | **Edit**.
3. Click **Unlock**.

**Change user roles or active status**
You can change or remove a user’s administrative role and change a user's active/inactive status.
For option definitions, click **Help** in the interface.
Task
1 Select Account Management | Users.
2 Select a user and click Edit | Edit.
3 From the Status drop-down list, select the user status you want to give the user.
4 From the Role drop-down list, select the role you want to give the user.
5 Click Apply.

Change display preferences and time zone for a user
You can set up a user’s preferences, which include display settings and the time zone in which messages are stamped.

Before you begin
This procedure describes how you set display preferences for another user. As an administrator, you can set your own user preferences by clicking My Account | Preferences. A user, if given permissions to do so, can set his or her own display preferences by clicking Preferences.

For option definitions, click Help in the interface.

Task
1 Select Account Management | Users.
2 Select a user and click Edit | Edit.
3 From the Time Zone, Language, and Entries per page drop-down menus, select the option you want to give the user.
4 Click Apply.

Editing multiple users at one time
The Batch Edit Users page allows you to edit a list of user accounts by displaying and changing multiple accounts in a single page or by uploading a predefined text file containing a list of email addresses with revised user names, time zones, and/or languages.

The Batch Edit Users page is a convenient tool for adding McAfee Client Proxy user IDs for Web Protection because these Client Proxy user IDs are added as user names on the Batch Edit Users page.

Contents
- Edit users in a list
- Edit multiple users with a batch file

Edit users in a list
You can edit a list of user accounts for some commonly changed characteristics by displaying and changing those accounts in the Batch Edit Users page. On this page, you can change user names, time zones, languages, and several other attributes.
You cannot edit a user with a Protected - SSO status. A Protected - SSO user can be added, changed, or deleted only through the Application Programming Interface (API). For option definitions, click Help in the interface.
Task
1 Select Account Management | Users.
2 In the User Accounts List, select the users you want to edit.
3 Click Edit and select Batch Edit.
   
   The Batch Edit Users page is displayed.
4 To display or hide any columns of data for editing:
   a Click the heading of a column
      
      A down arrow appears in the right of the column heading.
   b Click the down arrow, and select Columns.
   c Select the checkbox for each type of data you want to edit.
5 For any user listed in the Batch Edit Users page, doubleclick on any of the following fields to change the information:
   • **Time Zone** — From the drop-down list, select a new time zone.
   • **Username** — Enter a new user name.
   • **Language** — From the drop-down list, select a new language.
   • **Status** — From the drop-down list, select a new status.
   • **Password** — (Available only for Customer Administrators) Enter a new password.

   If you use remote LDAP, IMAP, or POP3 authentication for users, the password you reset will normally be replaced the next time the Control Console synchronizes with the remote authentication server.

   • **First Name** — Enter the user's first name.
   • **Last Name** — Enter the user's last name.
   • **Display Name** — Enter the user's display name.
   • **Mobile Phone** — Enter the user's mobile phone number.
   • **Title** — Enter the user's title.
   • **Department** — Enter the user's department.

   Though you can change the Target User address, only do so if you are adding a batch file and the address is in error.

   To remove data for a user once it is uploaded into the Batch Edit User page, doubleclick the data field and select Unset Value from the drop-down menu in the field. To leave the data for a field as it was prior to uploading the file, select No Change from the drop-down menu in the field.
6 Click Save.
Edit multiple users with a batch file

The Batch Edit Users page allows you to upload user changes in a predefined .csv (Excel) or text file. Typically, the file contains a list of revised email addresses, user names, time zones, languages, and other attributes. Entries in the list must have the exact format.

Customer administrators can also use this task to change passwords.

For option definitions, click Help in the interface.

Task
1. Open Excel or a text editor, for example, Notepad, to create your file of addresses.
2. On the first line of the file, type the column headers for the data you want to upload, starting in the left-most column with Target User. In a text file, separate each heading with a comma. The other data headings can include:
   - Time Zone
   - Username
   - Language
   - Status
   - First Name
   - Last Name
   - Display Name
   - Mobile Phone
   - Title
   - Department

In addition, as a Customer Administrator, you can view and change passwords, so you can also include the heading Password.

For example, the first line might include the following data: Target User, Time Zone, Username, Language. Commas separate each header from the other headers.

3. On the second line of the file, type the primary email address for a user, followed by the other data you want to include for the user. The data must match the order you used for the first-line headings.

   `<primary email address>,<time zone name>,<username>,<language>`

Rules regarding batch file entries:

- Enter a primary email address. Other entries are optional. However, in a text file, enter commas to indicate an entry's position even if you don't want to change it. For example, for `jsmith@acme.com`, you might want to change the language to Italian, but not the time zone or user name. Enter `jsmith@acme.com,,Italian`.

- Email addresses must be unique.

- If the local name, or handle, portion of an email address contains commas, enclose that portion of the address in double-double quotes (" "), for example: ""smith,j""@acme.com.

- Enter a time zone name exactly as listed in the Time Zone drop-down list in the New User page. The exact names are also listed online. http://www.mcafee.com/us/resources/misc/mcafee-saas-time-zones-languages.pdf

- The user name can include a domain name with the format `<domain>\<username>`, for example: `jsmith@acme.com,America/Denver,acme\joesmith,en_US`

The domain portion can contain 1–15 alphanumeric characters as well as the following symbols (no spaces):

`! @ # $ % ^ & ( ) ~`
• If you are changing the language, enter the language in English exactly as listed in the Language drop-down list. The exact names are also listed online.

• You cannot change the data for a user that has the status Protected - SSO. You also cannot change a user to the status Protected - SSO. A Protected - SSO can be added, changed, or deleted only through the Application Programming Interface (API).

• If you are adding a password, the password must follow the same rules as if you are changing your own password. For example, you cannot use the user's email address as the password.

4 Press Enter or an equivalent key to create a hard return and start a new line in the file.

5 Create one line of addresses per user.
   The maximum number of users you can upload at one time is 10000.

6 Save the file to your computer's hard drive with a file name of your choice, using the following guidelines:
   A .CSV file for batch edit users can be encoded in any of the following formats:
   • UTF-8 without Byte Order Mark (BOM)
   • UTF-8 with BOM
   • UCS2 - Big Endian
   • UCS2 - Little Endian

   These formats apply to both single byte (such as French or Russian) and double-byte (such as Traditional Chinese, Japanese) characters. By default, Notepad and Microsoft Excel support single-byte ANSI formats only. As a result, double-byte characters might not be saved correctly in ANSI using these editors. Therefore, if you are creating a .csv file in Notepad or Excel and are including multibyte characters, save the file in UTF-8 without BOM encoding.

7 Select Account Management | Users.

8 Click Edit.

9 From the Edit drop-down list, select Batch Edit.

   A blank Batch Edit Users page is displayed.

10 Click Browse. Search for and select the file you created.
11 Click Upload.

The data is displayed in the page. If you leave a value blank, the field for that value displays No Change.

12 Review the entries for errors. If there are errors, you can correct them in the page by double-clicking the field and changing the information. If you want to change a password, you can select the Show passwords in clear text when editing to see the password as you are changing it.

13 Click Save.

**Customize spam filtering for a user**

You can view, set or change how spam is reported in the user's Spam Report. These changes override settings on the Anti-Spam: Reporting tab in the user's Email Protection policy.

**Before you begin**

Only a user with the role of Customer Administrator or higher can add, edit, or delete users.

For option definitions, click Help in the interface.
**Task**

1. Select **Account Management | Users**.
2. Select a user and click **Edit | Email Protection**.

   The **Edit User: Email Protection** tab is displayed.

3. Complete the fields as required.
4. Click **Apply**.

   Changes take effect immediately.

**Review email activity of a user**

You can review the number of messages a user received in the last week and the average size of those messages.

**Before you begin**

The domain must be assigned a package of Email Protection features for the **Email Activity** tab to be available.
**Task**

1. Select **Account Management | Users**.

2. Select a user and select **Edit | Email Protection | Email Activity**.

3. Review the number of incoming messages the user received in the last seven days and the average size of a message, including attachments.

4. Click **User Details** to return to the **Edit User: Email Protection** tab for the user.

**Review web activity of a user**

You can review a user’s web traffic for the last week, including volume in and out, the number and type of threats encountered, and the number of blocked/allowed content requests.

---

**Before you begin**

The domain must be assigned a package of Web Protection features for the **Web Activity** tab to be available.

---

**Task**

1. Select **Account Management | Users**.

2. Select a user and select **Edit | Web Protection | Web Activity**.

3. Review the data.

4. Click **User Details** to return to the **Web Protection** tab for the user.

**Assign a user to a group**

You can assign a user to one or more predefined groups.

Follow these guidelines:

- If a user is assigned to only one group, the policy to which the group is assigned will be used for the user account.

- If an Email Protection user is assigned to more than one group and the groups have different policies, then the policy with the highest priority is applied to the user.

- If a Web Protection user is assigned to more than one group and the groups have different policies, then a merged version of the policies is applied to the user.

**Note:** A Group Administrator can change the group a user belongs to only if the Group Administrator is assigned to that group.

For option definitions, click **Help** in the interface.

---

**Task**

1. Select **Account Management | Users**.

2. Select a user and click **Edit | Edit**.
3 In the Edit User page, click Group Membership.

The list of available groups and selected groups is displayed. If you are a Group Administrator, the lists include only groups for which you are an administrator.

4 If there are multiple pages of groups available:
   - Use the forward and backward buttons at the bottom of the page to navigate.
   - If the list is too large, filter the list in the following way:
     1. Place your cursor on the Available Groups column heading.
     2. Click the column's down arrow to display the first menu.
     3. Use your cursor to highlight Filters.
4 From the Filter submenu, click the checkbox for the specific filtering option you want.

5 Enter a value for which to search for matching group names.

5 From the Available Groups list, select the group or groups you want to assign to the user. You can also select the Available Groups checkbox at the top of the column to add all groups listed on the page at once.

6 To add the groups you selected on the page, click Add. To add all groups on all pages of your filtered search, click Add All.

   The groups are added to the Selected Groups list.

7 Click Apply.

Tasks
• **Remove a user from a group on page 77**
   You can remove a user from one or more groups.

Remove a user from a group
You can remove a user from one or more groups.

   A Group Administrator can remove the group a user belongs to only if the Group Administrator is assigned to that group.

For option definitions, click Help in the interface.

Task
1 Select Account Management | Users.

2 Select a user and click Edit | Edit.

3 In the Edit User page, click Group Membership.

   The list of selected groups is displayed. If you are a Group Administrator, the Selected Group list includes groups for which you are not an administrator and therefore cannot remove.

4 From the Selected Group list, select the group or groups you want to unassign to the user. You can also select the Selected Group checkbox at the top of the column to add all groups listed on the page at once.

5 To remove the groups you selected on the page, click Remove. To remove all groups on all pages, click Remove All.

   The groups are removed from the Selected Groups list.

6 Click Apply.
Assign groups to a Group Administrator

You must assign groups to a Group Administrator to allow the Group Administrator to administer those groups. The user does not need to be a member of the group to be its Group Administrator.

Before you begin

When the Group Administration tab is clicked, a list of groups available for the administrator is displayed. If there are multiple pages of groups available, the page number of the group list, along with page forward and page backward buttons, are shown.

A Group Administrator can access the Group Administration tab to view the administrator's own list of assigned groups or the assigned groups of other Group Administrators. However, a Group Administrator cannot change the group or groups to which the administrator is assigned.

Task

1. Select Account Management | Users.
2. Select a user and click Edit | Edit.
3. Click Group Administration.

The Edit User: Group Administration tab is displayed.

4. If there are multiple pages of groups available:
   - Use the forward and backward buttons at the bottom of the page to navigate.
   - If the list is too large, filter the list in the following way:
     1. Place your cursor on the Available Groups column heading.
     2. Click the column's down arrow to display the first menu.
     3. Use your cursor to highlight Filters.
4 From the Filter submenu, click the checkbox for the specific filtering option you want.

5 Enter a value for which to search for matching group names.

5 Select the name of a group you want to add to the user, or select the Available Groups checkbox to add all groups listed on the page at once.

6 To add the groups you selected on the page, click Add. To add all groups on all pages of your filtered search, click Add All.

   The groups are added to the Selected Groups list. The selected groups are displayed under Selected Groups.

7 Click Apply.

Deleting Users
You can delete one or more user accounts from the Users List or from the Delete Batch Users page in the Control Console.

You can delete only user accounts whose roles are at a lower level than your role (for example, Domain Administrators can delete Report Managers, Quarantine Managers, and User, but cannot delete Partner Administrators or Customer Administrators). Only those user accounts that can be deleted by your role will be listed in this page. You should also consider the following guidelines:

• Users with the status Protected - SSO cannot be deleted from this page. Protected - SSO users can be deleted only from the API.

• This action is irreversible. All data for the user accounts are deleted once this action is completed, including quarantine data, configurations, etc. Be very sure that you want to complete this action.

• A user account might be auto-created after deletion of the user account, depending on the domain's configurations.

Contents

▪ Delete users you select from the Users List
▪ Delete multiple users with a batch file

Delete users you select from the Users List
You can delete users you select from the Users List with the Delete button. Use the following guidelines:

• If you delete a primary address, all associated alias addresses are also automatically deleted, even if you did not include those alias addresses in the batch file.

• If you delete an alias address, its associated primary address is not automatically deleted.
**Task**

1. Select **Account Management | Users**.

2. Select one or more users on the list.

   You can select users on different pages of the **User List** and clicking **Delete** deletes all users you selected.

3. Click **Delete**.

   A confirmation page appears.

4. Click **Delete**.

   If you cannot delete a user, for example because the user is protected, an error message is displayed in the status bar.

**Delete multiple users with a batch file**

The **Batch Delete Users** page allows you to upload a batch file that contains a list of users that you can then delete.

**Task**

1. Open a text editor, for example Notepad, to create your file of addresses. You can also use a .csv (Excel) file.

2. On the first line of the file, type the column header **Target User**.

3. On the second line of the file, type the email address for a user.

   Rules regarding batch file entries:
   - You can enter a primary email address or an alias address.
   - Email addresses must be unique.
   - If the local name, or handle, portion of an email address contains commas, enclose that portion of the address in double-double quotes (""""), for example: """"""smith,j""""@acme.com.

4. Press the **Enter** key or an equivalent key to create a hard return and start a new line in the file.

5. Create one line of addresses per user.

   The maximum number of users you can upload at one time is 10000. If you delete a primary address, all associated alias addresses are also automatically deleted, even if you did not include those alias addresses in the batch file. If you delete an alias address, its associated primary address is not automatically deleted.

6. Save the file to your computer’s hard drive with a file name of your choice.

7. Select **Account Management | Users**.
8  Click the Delete link at the top of the page.

The Batch Delete Users page is displayed.

<table>
<thead>
<tr>
<th>Target User</th>
<th>Primary/Alias</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:mat@denver-acme.com">mat@denver-acme.com</a></td>
<td>Primary</td>
</tr>
<tr>
<td><a href="mailto:user100@denver-acme.com">user100@denver-acme.com</a></td>
<td>Primary</td>
</tr>
<tr>
<td><a href="mailto:marc@denver-acme.com">marc@denver-acme.com</a></td>
<td>Primary</td>
</tr>
<tr>
<td><a href="mailto:dave@denver-acme.com">dave@denver-acme.com</a></td>
<td>Primary</td>
</tr>
<tr>
<td><a href="mailto:nick@acme.com">nick@acme.com</a></td>
<td>Primary</td>
</tr>
</tbody>
</table>

9  Click Browse next to the Users field. Search for and select the file you created.

10 Click Upload.

The list of users is displayed in the Target User list in the Delete User page. The Primary/Alias column identifies whether the address is a primary or alias address.

11 Click Delete.
Adding and managing users
Managing existing users one-by-one
Managing groups

Use and manage groups when there are users in the organization whose email you want to filter according to a policy other than the default policy. You create and manage groups only if you are using Email Protection or Web Protection and you are an enterprise customer.

A user that you do not assign to a group receives treatment according to the policy of the users' domain, normally the default policy.

Contents

- Determine who needs separate filtering
- Assigning a user to multiple groups
- Create a group
- Change a group name or description
- Add users to a group
- Move a user to a different group
- Assign a Group Administrator
- View the Email Protection policies for a group

Determine who needs separate filtering

Groups are used when there are users in the organization whose email should be filtered according to a policy other than the default policy.

For example, you might have a support group that needs to receive email from a wide variety of customers, some of whom might send many advertisements via email. In this case, email from those customers might be blocked periodically by the default policy. You can create a group within Email Protection for technical support, then create a new policy just for Support.

Creating and applying groups is a three step process.

- Create a new group.
- Assign individual user accounts to the group.
- Create a new policy with special email filtering rules and associate the group to the policy.

When the groups are completed, the users in the group will have their email filtered according to the newly created policy, instead of the email filtering rules in the default policy.

All users who are not assigned a group continue to receive email according to the default Email Protection policy. Also, users from up to three different domains can be assigned to the same group.
Assigning a user to multiple groups

You can assign a user to multiple groups to match how the user is administered within the Active Directory.

When a user is assigned to multiple groups, the way in which policies are applied to the user differs depending on the application, Email Protection or Web Protection, in which the policies reside.

- **Email Protection** — Filtering policies available to assign to groups are ranked in order of priority on the Email Protection policies list page. As a result, when you assign a user to more than one group, the user receives policy filtering from whichever group is assigned the highest-priority policy.
  
  For example, a person who manages a customer support group and is included in that group might also be included in a management group. In this case, if the management group is assigned a policy that is a higher priority than the policy for the customer support group, the manager would receive policy treatment assigned to the management group.

- **Web Protection** — Policies are merged. For a given time of day, all policies attached to groups to which a user belongs are combined. The resulting policy for a given time of day is the most restrictive. A category that is blocked in any of the group policies will be blocked in the combined policy. Hosts that exist on a category bypass and a block list are blocked.

Create a group

Create a new group so you can assign a policy specific to that group's needs. The new group will be automatically subscribed to the default inbound and default outbound policy sets defined in the Policy Configuration: Group Subscriptions pages for Email Protection.

Before you begin

Groups are available only to enterprise customers. Only a Customer Administrator or higher role can add a group.

For option definitions, click Help in the interface.

**Task**

1. Select Account Management | Groups.
   
   The Groups List is displayed.
2 Click **New**.

The **New Group** page is displayed.

3 Complete the fields in the page as necessary.

4 Click **Save**.

The group is added to the **Groups List**.

You can remove a group by selecting the group from the **Groups List**, clicking **Delete**, and then clicking **Delete** again. The group is also removed from assignment to the policy it was assigned to. Users in the group immediately begin having their email processed by the default policy for domains.

**Tasks**

- **Filter the Group List on page 85**
  You can filter the list of groups on the **Group List** page based on one or more criteria you specify. To filter the **Group List** page so that only groups that match criteria you select are listed:

- **Download Groups List data on page 86**
  From the **Groups List** page, you can create a .csv file of group data to save data included on the **Groups List** page to use for other purposes.

**Filter the Group List**

You can filter the list of groups on the **Group List** page based on one or more criteria you specify. To filter the **Group List** page so that only groups that match criteria you select are listed:

**Task**

1 Select **Account Management | Groups**.

The **Groups List** page is displayed.
2. In the Group List page, place your cursor on the column heading whose criteria you want to use for filtering. Filter criteria are available on the following columns:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>List only groups whose names start with, contain, or equal the characters you enter.</td>
</tr>
<tr>
<td>Description</td>
<td>List only groups whose descriptions start with, contain, or equal the characters you enter.</td>
</tr>
<tr>
<td>Date Created</td>
<td>List only groups that were created before, after, or on a specific date. You can also create a range of time based on the use of a &quot;before&quot; date and an &quot;after&quot; date together.</td>
</tr>
</tbody>
</table>

3. Click the column's down arrow to display the first menu.

4. Use your cursor to highlight Filters.

5. From the Filter submenu, click the checkbox for the specific filtering option you want. You might also have to enter a value with which to select data as, for example, when filtering by Group Name.

**Download Groups List data**

From the Groups List page, you can create a .csv file of group data to save data included on the Groups List page to use for other purposes.

Additional group attributes that may exist on the Group Details page for any particular group are also included in the downloaded file.

For option definitions, click Help in the interface.
**Task**

1. Select Account Management | Groups.

2. Use display options in the column headers to display or hide the columns of data you want to include in the file.

3. Click Download.

   An Excel dialog box appears to guide to completion of the .csv download.

---

### Change a group name or description

Change a group’s name or description, for example, if you want to reflect changes due to a reorganization.

For option definitions, click Help in the interface.

**Task**

1. Select Account Management | Groups.

   The Groups List page is displayed.

2. Select the appropriate group, then click Edit.

   The Group Details page is displayed.

3. Change the fields as necessary, and click Apply.
Add users to a group

This task allows you to assign users to a group so each user's account receives treatment from the policy associated with the group.

Task

1. Select Account Management | Groups.
   
   The Groups List page is displayed.

2. Select the appropriate group, and click Edit.
   
   The Group Details page is displayed.

3. Click Members.
   
   A list of users available for the group is displayed. The AD domain of each user, if any, is displayed. In addition, the Group Count column displays how many groups, if any, the user is already a member of.

4. If there are multiple pages of users available:
   
   - Use the forward and backward buttons at the bottom of the page to navigate.
   
   - If the list is too large, filter the list in the following way:
     1. Place your cursor on the Available Users column heading.
     2. Click the column's down arrow to display the first menu.
3 Use your cursor to highlight Filters.

4 From the Filter submenu, click the checkbox for the specific filtering option you want.

5 Enter a value for which to search for matching email addresses.

5 Perform these steps for all users you want to add to the group.
   a Select the user or users you want to add to the group. You can also select the Available Users checkbox at the top of the column to add all users listed on the page at once.
   b To add selected users on the page, click Add. To add all user on all pages of your filtered search, click Add All.

The users you selected are added to the Selected Users list.

6 Click Apply.

The number in the Group Count column can differ from the number of groups to which a user is actually assigned within the customer's Active Directory (AD), even when Directory Integration synchronizes user data by AD domain. This difference can result for various reasons. For example, users can be manually added to groups in the Control Console and not added in the Active Directory. Also, in the Control Console, groups that contain other groups are included in the user's group count.

---

**Move a user to a different group**

You can move a user to a different group so that the filtering policy for that user is a better match.

**Task**

1 Select Account Management | Groups.

   The Groups List page is displayed.

2 Select the appropriate group, and click Edit.

   The Group Details page is displayed.

3 Click Members.

4 In the Available Users list, select the name of a user you want to add to the group. You can also select multiple users to add at one time.

5 Click Add.
6 Click Apply.
   The user is added to the new group.

7 From the **Groups List**, select the group from which you want to remove users.
   A list of users for the current group is displayed.

8 Select **Members**.

9 In the **Selected Users** list, select the name of a user you want to remove from the group. You can also select multiple users to remove at one time.

10 Click **Remove**.

11 Click **Apply**.
   The user is removed from the user's old group.

**Assign a Group Administrator**

Assign one or more Group Administrators to a group to enable others to manage the members and policies assigned to the group.

**Before you begin**

Use the following guidelines:

- You must have the role of Customer Administrator or higher in order to perform this task. A Group Administrator can view the **Administrators** page, but cannot make changes.

- A Group Administrator can perform the following tasks for a group to which the administrator is assigned:
  - Add and remove members of the group.
  - Create, edit, and assign Email Protection policies to a group.
  - View policies that have been created at the customer level, and assign those policies to the group.
  - Create, edit, and delete policies specifically for a group. When a policy has been created specifically for a group, the group is said to own the policy.
  - Assign policies that were created for one group to another group. To perform this task, the Group Administrator must be assigned to both groups.

- A Group Administrator does not need to be a member of a group in order to be able to perform Group Administrator tasks for that group. As a result, a Group Administrator can administer multiple groups, including those groups in which the Group Administrator is not a member. However, a Group Administrator cannot add or remove a group.

- A group can also have multiple Group Administrators assigned to it.

For option definitions, click **Help** in the interface.

**Task**

1 Select **Account Management | Groups**.
   The **Groups List** page is displayed.
2 Select the appropriate group, and click **Edit**.

The **Group Details** page is displayed.

3 Click **Administrators**.

The **Administrators** page is displayed.

4 Select the administrator you want to add. To add all the available administrators, select the **Available Group Administrators** checkbox.

5 If there are multiple pages of group administrators available:
   - Use the forward and backward buttons at the bottom of the page to navigate.
   - If the list is too large, filter the list in the following way:
     1. Place your cursor on the **Available Group Administrators** column heading.
     2. Click the column's down arrow to display the first menu.

     - Use your cursor to highlight **Filters**.
4. From the Filter submenu, click the checkbox for the specific filtering option you want.

5. Enter a value for which to search for matching email addresses.

6. To add selected administrators on the page, click Add. To add all administrators on all pages of your filtered search, click Add All.

   The selected administrators are displayed under Selected Group Administrators.

7. Click Apply.

---

**View the Email Protection policies for a group**

Use the Email Protection Policies page to review the Email Protection policies that have been assigned to a group.

Both an inbound and outbound policy can be assigned to the group. If no policy has been assigned, the fields are blank.

To see the details of a policy, you must access the Email Protection | Policies page, then select the policy name you want to review.

For option definitions, click Help in the interface.

**Task**

1. Select Account Management | Groups.

   The Groups List page is displayed.

2. Select the appropriate group, and click Edit.

   The Group Details page is displayed.
3 Select Email Protection Policies.

The names of the Inbound Policy and Outbound Policy are displayed.

Inbound Policy: Test Inbound Policy
Outbound Policy: Test Outbound Policy
Managing groups
View the Email Protection policies for a group