Email Image Control

Administrator Guide

Symantec.cloud

Image Control Administrator Guide

Documentation version: 1.0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical support

If you need help on an aspect of the security services that is not covered by the online Help or administrator guides, contact your IT administrator or Support team. To find your Support team's contact details in the portal, click **Support** > **Contact us**.

Contents

Chapter 1

Introduction to Image Control

This chapter includes the following topics:

About the Image Control service

Image Control enables you to monitor and control potentially inappropriate images entering and leaving your organization - protecting your employees as well as your brand and reputation.

The Image Control service lets you do the following:

- Monitor and control images going out of your organization
- Ensure that business critical images can be sent and that potentially inappropriate images are controlled
- Detect problem areas and take the appropriate action with the employees in question
- Ensure that your brand is not tarnished

Organizations have a duty of care to protect their employees against inappropriate images and harassment. The Image Control service enables you to monitor and control the images that an employee receives. You can then take appropriate

action if the Image Control service detects an image within or attached to an email. By making the best effort to protect an employee against receiving inappropriate images, your organization protects itself against possible litigation from employees.

Image Control uses several methods to detect inappropriate images in emails and in email attachments. These methods are as follows:

- Approved sender and recipient lists enable you to specify trusted email senders and recipients. Approved senders and recipients can be internal and external email addresses or domains. In this way, a specific email address or domain can be excluded from scanning by the Image Control service.
- A local database enables your organization to maintain its own unique list of client blocked and approved images (unique signatures that identify specific images) that have been caught incorrectly. Adding the image signature to the local database provides an immediate resolution for an image that was analyzed incorrectly. Once an image's signature is added to the local database, if the image is sent or received again, it is analyzed correctly.
- The global database enables you to benefit from (and add to) a database that supports the Image Control community. Images, whether for business or social reasons, are often sent among organizations globally at great speed. If the image is misclassified, a large number of emails can be analyzed incorrectly. The global database enables organizations belonging to the Image Control community to support each other to reduce the number of emails that are triggered incorrectly.
- The ground-breaking proactive Image Composition Analysis (ICA) provides accurate detection of inappropriate images. The ICA engine is multi-layered; each layer incorporating multiple algorithms to offer an increased level of accuracy. Rather than only measuring flesh tones, the ICA heuristics technology analyzes elements of the image – face, body position, texture, and color – as well as other algorithms.

Although Image Control is a managed service requiring no additional hardware or software, it can be customized to suit your specific business requirements and company email policy. Using the portal, you can specify which detection methods to use, whether to scan within Microsoft® Office™ and PDF documents sent as attachments.

You can tune the level of sensitivity for the ICA detection method (also known as the heuristics detection method) using high, medium, and low settings. This is useful when controlling inbound and outbound scanning. For example, you may want to set sensitivity levels to high on inbound and low on outbound email traffic.

Whichever settings you choose, there will be no discernible latency in email transmission.

You can set a specific action depending on the method that detects the email. So, you can define different actions for emails detected by the approved senders and recipients lists, client and global databases, or the ICA heuristics scanner.

See "Overview of the configuration process for Image Control" on page 9.

See "Image Control best practice settings" on page 10.

Overview of the configuration process for Image Control

Use the portal to configure Image Control. Image Control can be customized to suit your specific business requirements and company email policy.

An overview of the process for configuring Image Control to your needs is presented in the following table. You do not need to complete the configuration in any particular order.

Table 1-1 Overview of the configuration process.

	Steps	For full details
1.	Define your client approved and blocked images lists	See "Frequently asked questions on Image Control" on page 39.
2.	Define your approved senders and recipients lists	See "Working with approved senders and recipients lists" on page 21.
3.	Define whether notifications are to be sent to an administrator, the sender, or the recipient when a suspect image is detected	See "Defining notifications for Image Control" on page 27.
4.	If an action is to redirect mail or copy mail to an administrator, define an administrator email address to send them to	See "Defining the administrator email address for Image Control" on page 28.
5.	Define whether the scan should look in attached Microsoft® Office™ documents (Word, Excel, and PowerPoint)	See "Scanning in Microsoft® Office™ and PDF documents for Image Control" on page 34.

Table 1-1 Overview of the configuration process. *(continued)*

	Steps	For full details
6.	Enable detection methods and define actions: ■ Define which Image Control detection methods to use for inbound and outbound mail: Client approved and blocked image lists; Global approved and blocked image lists; and Heuristics. ■ Define the required sensitivity level for the heuristics detection method, if used. ■ Define a specific action for a specific detection method. ■ If the action is to tag the subject line of a suspect mail, define the subject line tag text.	See "Defining detection methods and actions for Image Control" on page 31.

See "About the Image Control service" on page 7.

See "Image Control best practice settings" on page 10.

Locating the Image Control pages in the portal

The Image Control pages of the portal provide all of the settings you need to configure the service to your organization's needs.

To locate the Image Control pages

◆ Click **Services** > **Email Services** > **Image Control**.

If **Global settings** is selected, six tabs are displayed; **Actions**, **Notifications**, **Approved images**, **Blocked images, Approved Senders**, and **Approved recipients**.

All of the **Image Control** settings are defined within these six tabbed pages.

See "Image Control best practice settings" on page 10.

Image Control best practice settings

We recommend that initially the following settings are used for both inbound and outbound mail:

■ The action to **Copy suspected mail to...** is used for all detection methods—you can arrive at the most appropriate actions for your organization by adjusting the settings and observing the results.

- Select low or medium sensitivity for the Heuristics detection method. You can arrive at its optimum sensitivity setting by adjusting the settings and observing the results.

Image Control best- practice settings:

- Click **Services** > **Email Services** > **Image Control**.

Defining whether settings apply at global or domain level

You can apply Image Control settings to all domains (global settings), or you can apply custom settings to your individual domains.

At the individual domain level, you can customize a configuration specifically for the selected domain. On initial setup, each domain is set to use the global settings. If you select a domain from the **Global settings** list and apply custom settings using the option, you can modify the settings for the individual domain without affecting the global settings. To apply settings for a specific domain, ensure that the **Apply custom settings** option is selected. Until you select this option, all fields in these pages are inactive and cannot be edited.

The settings you can make at domain level are those in the **Actions** and **Notifications** tabs. For example, you can specify the use of the heuristics scanner at a higher sensitivity rate for a specific domain. You could also have notifications for a domain sent to a different email address than the global administrator email address.

Note: Changes to the approved images, blocked images, approved senders, and approved recipients lists can only be made at global level.

To apply global settings

1. Click **Services** > **Email Services** > **Image Control**.
2. Ensure that **Global Settings** is selected from the drop-down list:

   Six tabs are displayed; **Actions**, **Notifications**, **Approved images**, **Blocked images**, **Approved Senders**, and **Approvedrecipients**. You can apply all of the settings in these tabs at global level.

To apply settings for a specific domain

1. Click **Services** > **Email Services** > **Image Control**.
2. Select the domain from the **Global Settings** drop-down list.

   Two tabs are displayed; **Actions** and **Notifications**. If no domain-level settings have been defined yet, all fields in the **Actions** and **Notifications** pages are inactive and cannot be edited.
3. Select **Apply custom settings**.

   The fields in the **Actions** and **Notifications** pages are now editable and inherit the global settings until you make any changes. The changes you make are applied to the selected domain (provided the changes are saved).

Note: If you switch from using custom settings back to using global settings (by selecting **Use global settings**), the settings in the page display the global settings (but are inactive). But your custom settings for that domain are remembered, and when you switch back to **Use custom settings**, your custom settings are again displayed and applied.

When you select a specific domain to work with, the name of the domain is displayed as a heading.

Chapter 2

Client approved and blocked images lists

This chapter includes the following topics:

Working with client approved and blocked image lists

You can add images to your organization's own client blocked and approved image lists. If the Image Control heuristics detection method incorrectly analyzes an email, you can add it to the client approved list. Then it is not triggered incorrectly again. Likewise, if the ICA heuristics detection method does not detect an inappropriate image, you can add the image to your client blocked images list. The image is triggered the next time it is sent.

Within the portal, you can browse your directories to select and add an image to your lists. As the image is added, it is scanned and a unique signature is created for it. This signature is then saved along with a text description for the image. The image signature is then recognized correctly by the scanner if the image passes through the Image Control service again.

The actual images are not stored; the image is scanned and a signature is automatically constructed for the image. A signature is a unique identifier of an

image, and the signature is stored. Therefore, you do not need to store or distribute offensive material on your organization's network, in the process of implementing your Image Control policy. You cannot recreate an image from a signature; there is no risk of anyone reproducing a confidential or a pornographic image from a signature.

A signature is created for a specific image of a specific size. If a suspect image is cropped or changed, the existing signature no longer stops it.

You can add an image signature for any file type to your approved and blocked image lists. However, only the signatures that are created from image files are used. For example, you can scan a Microsoft Word document that contains five images and create a signature for the Word document as a whole. However, if this signature is added to the database and you send through exactly the same Word document again, the scanner is not triggered. Instead, create an individual image file for each image and upload these to the database.

Each list can contain up to 3000 image signatures. We recommend deleting images by date, if a list becomes too large. Images are distributed in phases to reflect market trends and go out of fashion fairly quickly.

You can only define client approved and blocked images at global level. The client approved and blocked image lists override the global approved and blocked image lists. For example, the Image Control service does not detect an image that is on both the global blocked image list and your client approved image list.

Once you have defined your client approved and blocked images lists, you can enable the Image Control service to use these as a detection method.

See "Viewing the client approved or blocked image list" on page 14.

See "Enabling the client approved images list" on page 35.

See "Enabling the client blocked images list" on page 35.

Viewing the client approved or blocked image list

This procedure enables you to view the images on client approved or blocked image lists.

To view approved and blocked images

1 Click **Services** > **Email Services** > **Image Control**.

2 Click the **Approved images** or **Blocked images** tab, as appropriate.

The image list is displayed. A description and image ID identify each image. The user who added the image and the date the image was added are also displayed. By default, results appear in date sequence, with the most recently added signature listed first. To change the sort order, click the column heading of the data that you want to sort.

Note: Neither the image nor the signature is displayed in the portal.

See "Defining detection methods and actions for Image Control" on page 31.

See "Working with client approved and blocked image lists" on page 13.

See "Searching for an approved or blocked image" on page 15.

See "Adding an image to your client approved or blocked image list" on page 16.

See "Deleting an image from a client blocked or approved list" on page 17.

See "Editing an image description for Image Control" on page 18.

Searching for an approved or blocked image

This procedure describes how to search for specific images in either the client approved or blocked image lists. Several criteria are available for you to use to narrow your search.

To search for a client approved or blocked image

1 Click **Services** > **Email Services** > **Image Control**.

2 Click the **Approved images** or **Blocked images** tab, as appropriate.

The **Approved images** or **Blocked images** tabs present a search feature.

3 Enter your search criteria in the **Description**, **Image ID**, **From date**, and **To date** search fields.

If you search for an image by date, we recommend that you limit the number of results in your results list by also specifying either a description or an image ID. When searching by description, you can enter any word from the description, or only a few consecutive characters from the description. Specific search criteria result in a more manageable list of results.

Note: To list all images again after a search, type * in the Description box or **0** in the Image ID box.

See "Working with client approved and blocked image lists" on page 13.

See "Viewing the client approved or blocked image list" on page 14.

See "Deleting an image from a client blocked or approved list" on page 17.

See "Editing an image description for Image Control" on page 18.

Adding an image to your client approved or blocked image list

When you add an image to your local client approved or blocked image lists, the image is scanned and a signature is constructed for the image. When adding an image to your client approved images list, you can also request that the image is added to the global approved image list if it is also relevant to the Image Control community. This option supports other organizations, and similarly, if this option is selected, images they contribute support you, resulting in fewer emails that are triggered incorrectly. Images that are specific to your organization should not be submitted to the global list.

Note: The cloud security services manually review every image that is submitted to the global list to ensure that an image is not added incorrectly.

Note: You cannot submit images to be entered on the global blocked image list, for legal reasons. The portal does not provide the functionality to do this. It is an offense to distribute certain indecent images and to save them on to a computer.

To add an image to your client approved or blocked image lists

1. Click **Services** > **Email Services** > **Image Control**.
2. In the **Approved images** or **Blocked images** tab, as appropriate, click **Add image**.

   The **Add new image** window is displayed.
3. Click **Browse** to locate the image file to add.

4 Enter a description of the image.

The description must not exceed 255 characters. We recommend that you use meaningful descriptions and avoid unacceptable language. When a suspect email is detected, the image description may be included in the notification email sent to the administrator and in statistics and reports.

5 If the offending image is appropriate to be added to the global approved image list (that is, is not specific to your organization), check **Email image to Messagelabs for analysis and inclusion within the global image community**.

The image is emailed to the cloud security services for analysis and is added to the global approved list if it is appropriate.

This option is only available for approved images.

6 Click **OK**.

The image is automatically assigned a unique ID, which is displayed in your list of client approved or blocked image lists, as appropriate.

If the image is already in your list, an error message is displayed to ensure that there is no duplication within your lists.

See "Working with global approved and blocked image lists" on page 19.

See "Defining detection methods and actions for Image Control" on page 31.

See "Viewing the client approved or blocked image list" on page 14.

See "Editing an image description for Image Control" on page 18.

See "Enabling the client approved images list" on page 35.

See "Enabling the client blocked images list" on page 35.

Deleting an image from a client blocked or approved list

You can remove an image from either a client blocked or approved images list. Confirmation of a deletion is not requested.

To delete an image from a blocked or approved list

1 Click **Services** > **Email Services** > **Image Control**.

2 In the **Approved images** or **Blocked images** tab, as appropriate, check the box to the left of the image to delete.

3 Click **Delete selected**.

4 Click **Save and exit**.

See "Working with client approved and blocked image lists" on page 13.

See "Viewing the client approved or blocked image list" on page 14.

See "Searching for an approved or blocked image" on page 15.

Editing an image description for Image Control

You can add a text description to an image in your client approved or blocked images list. The description can explain why it was approved or blocked in case other administrators need to know.

To edit an image description

1. Click **Services** > **Email Services** > **Image Control**.
2. In the **Approved images** or **Blocked images** tab, as appropriate, click on the name of the image to edit.

   The **Edit Image** window is displayed.
3. Enter the required description in the **Description** box.

   The description must not exceed 255 characters. The cloud security services recommends that you use meaningful descriptions and avoid unacceptable language. When a suspect email is detected, the image description may be included in the notification email that is sent to the administrator and in statistics and reports.
4. Click **OK**.

See "Working with client approved and blocked image lists" on page 13.

See "Viewing the client approved or blocked image list" on page 14.

See "Searching for an approved or blocked image" on page 15.

See "Adding an image to your client approved or blocked image list" on page 16.

See "Enabling the client approved images list" on page 35.

See "Enabling the client blocked images list" on page 35.

Chapter 3

Global approved and blocked image lists

This chapter includes the following topics:

Working with global approved and blocked image lists

The global blocked images list is a database of images (image signatures) that have been confirmed as being inappropriate, manually. The global approved images list is a database of signatures of images that are clean but that have been incorrectly identified as suspect by the Image Control service.

The cloud security services manages and monitors the databases, which provide an ever-expanding resource to improve the success rate for detecting suspect images for Image Control service users. The Image Control community comprises The cloud security services and other organizations globally who subscribe to the Image Control service. Organizations can submit images for the approved images list that have been analyzed incorrectly for them and that other organizations may be likely to see. The images are analyzed manually and if they are definitely clean, they are added to the global database for use within the community. Organizations from around the world submit images to the Image Control community. Therefore, many images that are analyzed incorrectly will be added to the approved list before your organization sees them.

The global blocked images list does not contain any images that are borderline with respect to their level of offense. If it did contain such images, there is a risk of desired images being blocked incorrectly for other organizations. For example, images of swimwear or lingerie being modeled are not added to the global blocked

database. However, your client blocked images list overrides the global list. The global blocked images list only contains images (image signatures) that are undeniably pornographic and images sometimes found in offensive joke emails.

You can request that an image is added to a global approved image list to support the Image Control community. Remember that the interpretation of images is subjective. An image is not added to the global lists if it is only of interest to an individual organization.

Note: You cannot submit images to be entered on the global blocked images list, for legal reasons. It is an offense to save, make copies of, or distribute certain inappropriate images. The portal does not provide this functionality.

You can enable the Image Control service to use the global approved and blocked image lists as a detection method.

See "Adding an image to your client approved or blocked image list" on page 16.

See "Enabling the global approved image list" on page 36.

See "Enabling the global blocked image list" on page 36.

Adding an image to the global approved image list

You can send an image to the cloud security services to add to the global approved image list. You do so when you save it to your client approved list.

If the image is not accepted for the global database, it is still saved to your local client list.

Note: You cannot send an image to be added to the global blocked image list. This is to avoid contravening legislation that prohibits storing and distributing illegal images.

See "Adding an image to your client approved or blocked image list" on page 16.

See "Working with global approved and blocked image lists" on page 19.

See "Enabling the global blocked image list" on page 36.

Chapter 4

Approved senders and recipients lists

This chapter includes the following topics:

Working with approved senders and recipients lists

You can define your own lists of approved senders and recipients, thereby excluding a specific email address or domain from an Image Control service scan. For example, if business-critical images sent regularly from a specific user are incorrectly analyzed, the email address can be added to the approved senders list, ensuring that these emails are not delayed. Likewise, if a user is authorized to receive images and a number of them are analyzed incorrectly, you can add the recipient's address to the approved recipients list. For example, if images of medical wounds are received often, they are typically from the same source, so the sender can be added to the approved sender list. As another example, the marketing personnel of a modeling agency may be trusted to send and receive images, while all other employees are not.

The settings for approved senders and recipients are only active for your organization. So if you add an external email address to your approved recipient list, an email you send to it may not reach its destination if the external domain has its own email security policy that rejects your email.

Within the portal, you can browse the approved senders and recipients lists, and manage the email addresses and domains in them. You can add, delete, and edit entries individually. Or you can download your existing lists, edit them offline, and upload them back to the portal.

Each list can contain up to 1500 entries. If a list becomes too large, we recommend that you delete entries by date.

Note: You can only define approved senders and recipients at global level.

Note: No functionality exists within the portal to define blocked senders or recipients.

Once you have defined your approved senders and recipients lists, the Image Control service uses these automatically. No further steps are needed to enable the use of these lists.

Viewing your approved senders and recipients

You can view the email addresses and domains of those senders and recipients that are listed as approved.

To view your approved senders and recipients

1. Click **Services** > **Email Services** > **Image Control**.
2. Click the **Approved senders** or **Approved recipients** tab, as appropriate.

   The email addresses and domains in your list are displayed. Each entry comprises the domain name or email address, the entry type, and a description. The user who added the entry and the date it was added are also displayed.

The **Approved senders** or **Approved recipients** tabs also present a keyword search feature. You can search your list by entering a keyword to search for. The search is performed on the **Domain/Email** and **Description** fields.

You can use wildcards for partial matching. The wildcard * is interpreted as 0 or more unknown characters. For example, *W*d* finds words including *Wild* and *W*ithhel*d*.

Adding approved senders and recipients

You can add an entry to your approved sender or recipient lists by the portal interface., You can also download an existing list, edit it offline, and upload it back into the portal. Alternatively you can create your list offline and upload it to the portal.

To add individual email addresses or domains

1. Click **Services** > **Email Services** > **Image Control**.
2. In the **Approved senders** or **Approved recipients** tab, as appropriate, click **Add Entry**.

   The **Add Entry** window is displayed.
3. Enter the email address or domain and a description.

   The description can contain a maximum of 255 characters.

   The description field is useful for any additional comments that help you identify your list entry.
4. Click **OK**.

Downloading an approved senders or recipients list

You can download a CSV file of approved senders or recipients. Then you can edit existing entries and insert new entries into the list and then upload it back to the portal. When you save the list, ensure that it is saved as a .csv (comma-separated values) file.

To download a list from the portal

1. Click **Services** > **Email Services** > **Image Control**.
2. Click the **Approved senders** or **Approved recipients** tab, as appropriate.
3. Click **Download**.

   A dialog box asks you whether to open or save the file. The CSV file is named ImageControlApprovedSenders.csv.

   The first column lists the email address or domain entry and the second column lists an associated description, if required.

   The download operation may take some time to complete depending on the size of the list.

Uploading an approved senders or recipients list

You can create or edit a list of approved senders or recipients offline and upload the list to the portal. Two options are available for uploading lists into the portal:

Delete existing addresses and replace with uploaded addresses	By selecting this option the uploaded list replaces the existing list. Any entries in the existing list that are not in the uploaded list are lost.
Merge existing addresses with uploaded addresses	By selecting this option the uploaded list merges into the existing list. This is a useful way to add new entries to an existing list.

The file to upload must be a CSV file. You can upload a maximum of 1500 addresses.

To upload email addresses and domains

1. Click **Services** > **Email Services** > **Image Control**.
2. In the **Approved senders** or **Approved recipients** tab, as appropriate, click **Upload**.

   The **Upload File** window is displayed.
3. Enter the file path and name to upload or click **Browse** to locate the file.
4. Select whether to **Delete existing entries and replace with uploaded entries** or **Merge existing entries with uploaded entries**.
5. Click **Upload**.

   If the file contains invalid entries, an error message displays the first 100 invalid addresses and asks if you want to continue to upload the valid addresses.
6. Click **Save and Exit**.

   A confirmation message is displayed. New list entries are added to the list that is displayed in the **Approved senders** or **Approved recipients** tab.

Deleting entries from approved senders and recipients lists

These procedures explain how to remove entries (individual or all) from Approved Senders or Recipients lists.

Note: When you delete an entry, you are not asked to confirm the deletion. Make sure that you definitely want to delete the entry before you click **Save and exit**.

To delete an entry from approved senders or recipients lists

1. Click **Services** > **Email Services** > **Image Control**.
2. In the **Approved senders** or **Approved recipients** tab as required, check the box to the left of the entry to delete.
3. Click **Delete selected**.
4. Click **Save and exit**.

To delete all entries from approved senders or recipients lists

1. Click **Services** > **Email Services** > **Image Control**.
2. In the **Approved senders** or **Approved recipients** tab as required, check the box in the heading of the left-hand column to select all images.
3. Click **Delete selected**.
4. Click **Save and exit**.

Editing an entry in the approved senders or recipients list

You can edit the email addresses and text descriptions of entries in your approved senders and recipients lists.

To edit an entry in the approved senders or recipients list

1. Click **Services** > **Email Services** > **Image Control**.
2. In the **Approved senders** or **Approved recipients** tab, as appropriate, click on the name of the entry to edit.

   The **Edit Entry** window is displayed.
3. Edit the email address or domain as required.
4. Enter the required description in the **Description** box.

   The description can contain a maximum of 255 characters.
5. Click **OK**.

Chapter 5

Defining notifications

This chapter includes the following topics:

Defining notifications for Image Control

You can specify whether to send a notification to the sender or recipient of an inappropriate email. You can also specify a notification to be sent to an administrator when a user sends or receives an inappropriate email.

- For inbound emails, notifications can be sent to email recipients within your organization when the **Block and delete** or **Redirect to administrator** action is applied
- For outbound emails, notifications can be sent to email senders within your organization when the **Block and delete** or **Redirect to administrator** action is applied.
- For both inbound and outbound emails, notifications can be sent to administrators when the **Block and delete** action is applied.

To enable notifications to be sent

1. Click **Services** > **Email Services** > **Image Control**.
2. Click the **Notifications** tab.
3. In the **Notifications** section, click the checkbox next to the option(s) you require.

   The text of the notifications is as follows:

   - **Send notification if users receive an inappropriate email**:

The Email Security service has identified a file attachment in an e-mail sent to you that has been deemed to be potentially unacceptable by your Domain Administrator.
The subject title of the e-mail was:- %t
The sender address of the e-mail was:- %e
The recipient address of the e-mail was:- %r
The attachment filename was %y

- **Send notifications if users send an inappropriate email**:
  The Email Security service has identified a file attachment in an e-mail sent by you that has been deemed to be potentially unacceptable by either your Domain Administrator or the Recipient's domain administrator .
  The subject title of the e-mail was:- %t
  The sender address of the e-mail was:- %e
  The recipient address of the e-mail was:- %r
  The attachment filename was %y
- **Send notifications to administrator if one of your users send or receives an inappropriate email**:
  The Email Security service has identified a file attachment in an e-mail sent to/from one of your users that you have deemed to be potentially unacceptable.
  The subject title of the e-mail was:- %t
  The sender address of the e-mail was:- %e
  The recipient address of the e-mail was:- %r
  The attachment filename was %y

If a suspect email contains multiple attachments, the notification provides the name of the specific attachment that triggered Image Control.

4 Click **Save and exit**.

Note: If you would like to customize these notifications, contact the support team. Click **Support** > **Contact Us** for details.

Defining the administrator email address for Image Control

The Image Control administrator is the person that suspect mail is sent to if the action to either redirect or copy suspected mail is selected. Only one administrator email address can be set up for each domain. This address is used for both inbound and outbound email when enabled for that domain.

Note: This setting must be defined if an action for a suspected email is to redirect or copy it to the Image Control administrator.

To define an administrator's email address

1. Click **Services** > **Email Services** > **Image Control**.
2. Click the **Notifications** tab.
3. In the **Image Control Administrator Email Address** section, enter the required email address.
4. Click **Save and exit**.

Chapter 6

Enabling detection methods and defining actions

This chapter includes the following topics:

Defining detection methods and actions for Image Control

You can specify the Image Control detection methods you want to use to find suspect emails. You can also specify the action for the emails that are detected by each method. Each detection method has a checkbox to enable the detection method and a drop-down list of actions to choose.

Define each detection method to your requirements for inbound and outbound mail.

Table 6-1 Image Control detection methods

Detection method	Description	More information
Scan Microsoft® Office™ & PDF documents	You can choose to scan the images in Microsoft® Office™ and PDF file attachments.	See "Scanning in Microsoft® Office™ and PDF documents for Image Control" on page 34.
Use client approved image list	Allows the images on your own approved images list through the Image Control filters.	See "Enabling the client approved images list" on page 35.
Use client blocked image list	Detects the images on your own blocked images list.	See "Enabling the client blocked images list" on page 35.
Use global approved image list	Allows the globally approved images to pass through the Image Control filters.	See "Enabling the global approved image list" on page 36.
Use global blocked image list	You can block all images that are defined as inappropriate by our global client base.	See "Enabling the global blocked image list" on page 36.
Use heuristics	Use Image Composition Analysis (ICA) for accurate detection of inappropriate images.	See "Enabling the heuristics detection for Image Control" on page 37.

See "Available actions for Image Control" on page 32.

See "Defining whether settings apply at global or domain level" on page 11.

Available actions for Image Control

Options exist for dealing with the email that is suspected of containing unacceptable images, both inbound, or outbound. You can set an action depending on whether the client approved and blocked images lists, the global database, or the ICA heuristics scanner detects the email. So, you can apply a more severe action like **Block and delete** for the methods that you have a high level of

confidence in. Examples include the global and local blocked image list. This flexibility reduces the analysis overhead.

The available actions for detected email are:

Block and delete suspected mail	The email is prevented from reaching the intended recipients. It is permanently deleted. The scanning process is terminated for this email.
Redirect suspected mail to the Image Control administrator	The email is redirected so that it does not continue to the intended recipients, but is sent to an administrator of the Image Control service. Scanning is terminated for this email.
Copy suspected mail to the Image Control administrator	The email is flagged to be copied to a nominated Image Control administrator once scanning is completed. The scanning process continues and the email is delivered to the intended recipient.
Tag suspected mail within header	A comment is added into the email X-Header to indicate that this email triggered an Image Control rule. The scanning process continues. (See below for more information.) The action is available for inbound emails only.
Tag subject line but allow mail through	A tag is added to the subject line. You define the text for the tag. Tagging the subject line provides the benefit of warning a user before they open it that the email may contain inappropriate content. The action is available for inbound emails only. See "Defining the subject line tag text" on page 38.
Log only	The portal statistics record that a rule has been triggered. No other action is taken. The scanning process continues.

The action to **Tag suspected email within the header** adds a string to the email header. The string identifies that an email contains an image that the Image Control service flags. Because the tag identifies such emails, you can take further action as required, when they enter your organization's mail system or your end-users' email client. The format for the string is:

`X-PornInfo: found (level 0)`	This tag is added to the header if an image is detected that matches one in your blocked images list, or in the global blocked images list

`X-PornInfo: found (level n))`	*n* is either 1, 2, or 3 depending on the heuristic level that the image triggered: ■ Images with a classification of 1 and above are detected if the sensitivity level is set to **High sensitivity**. ■ Images with a classification of 2 and above are detected if the sensitivity level is set to **Medium sensitivity**. ■ Images with a classification of 2 and above are detected if the sensitivity level is set to **Low sensitivity**.

We recommend that on initial configuration you set the actions to **Tag suspected email within the header**, rather than to block or redirect suspected emails. The tagging action allows emails containing images to be received as normal, while the portal statistics and reports let you observe activity. You can then determine the optimum sensitivity level for your needs.

See "Enabling the client approved images list" on page 35.

Scanning in Microsoft® Office™ and PDF documents for Image Control

When defining the scanning of your inbound and outbound mail, you can choose whether to scan the images that have been inserted into Microsoft® Office™ and PDF file attachments. Using images within Microsoft® Office™ and PDF documents is a common method of getting around an organization's IT security policy.

To enable scanning in Microsoft Office documents

1. Click **Services** > **Email Services** > **Image Control**.
2. Click the **Actions** tab.
3. In the **Inbound mail** or **Outbound mail** sections (as required), check **Scan Microsoft® Office™ documents & PDF**.
4. Click **Save and Exit**.

See "Defining detection methods and actions for Image Control" on page 31.

Enabling the client approved images list

The client approved images list enables you to specify images to allow through the Image Control filters.

No action needs to be set for this detection method; an image that is detected but is approved is sent directly to the recipient.

To enable use of the approved images list

1. Click **Services** > **Email Services** > **Image Control**.
2. Select the **Actions** tab.
3. In the **Inbound mail** or **Outbound mail** sections (as required), check **Use client approved image list**.
4. Click **Save and exit**.

See "Defining detection methods and actions for Image Control" on page 31.

See "Working with client approved and blocked image lists" on page 13.

See "Viewing the client approved or blocked image list" on page 14.

See "Searching for an approved or blocked image" on page 15.

See "Adding an image to your client approved or blocked image list" on page 16.

Enabling the client blocked images list

You can define a list of images that should be blocked by Image Control whether or not the images would be detected by the filters.

To enable use of the blocked images list

1. Click **Services** > **Email Services** > **Image Control**.
2. Click the **Actions** tab.
3. In the **Inbound mail** or **Outbound mail** sections (as required), check **Use client blocked image list**.
4. From the drop-down list, select an action for emails that are detected by this method.
5. Click **Save and exit**.

See "Defining detection methods and actions for Image Control" on page 31.

See "Working with client approved and blocked image lists" on page 13.

See "Viewing the client approved or blocked image list" on page 14.

See "Adding an image to your client approved or blocked image list" on page 16.

Enabling the global approved image list

The global approved image list enables you to permit globally approved images to pass through the Image Control filters. Global settings apply to all users of the service.

To enable use of the global approved image list

1. Click **Services** > **Email Services** > **Image Control**.
2. Select the **Actions** tab.
3. In the **Inbound mail** or **Outbound mail** sections (as required), check **Use global approved image list**.
4. Click **Save and Exit**.

No action needs to be set for this detection method, because an image that is detected but is approved is sent directly to the recipient.

See "Defining detection methods and actions for Image Control" on page 31.

See "Working with global approved and blocked image lists" on page 19.

See "Adding an image to the global approved image list" on page 20.

Enabling the global blocked image list

You can block all images that are defined as inappropriate by our global client base.

To enable use of the global blocked image list

1. Click **Services** > **Email Services** > **Image Control**.
2. Select the **Actions** tab.
3. In the **Inbound mail** or **Outbound mail** sections (as required), check **Use global blocked image list**.
4. From the drop-down list, select an action for that emails that this method detects.
5. Click **Save and Exit**.

See "Defining detection methods and actions for Image Control" on page 31.

See "Working with global approved and blocked image lists" on page 19.

See "About the Image Control service" on page 7.

Enabling the heuristics detection for Image Control

The ground-breaking proactive Image Composition Analysis (ICA) provides accurate detection of inappropriate images. The ICA engine is multi-layered; each layer incorporating multiple algorithms to offer an increased level of accuracy. Rather than only measuring flesh tones, the ICA heuristics technology analyzes elements of the image – face, body position, texture, and color – as well as other algorithms.

To define the predictive (heuristics) settings

1. Click **Services** > **Email Services** > **Image Control**.
2. Click the **Actions** tab
3. In the **Inbound mail** or **Outbound mail** sections (as required), check **Use heuristics**.
4. Select the sensitivity level you require for your inbound or outbound mail. The options are as follows:

Low	Detects images marked as level 3
Medium	Detects images within levels 2 or 3
High	Detects images within 1,2 and 3

   Low detects fewer images than **High**. **Low** detects images that are clearly pornographic. **Medium** and **High** detect a wider range of images.
5. From the drop-down list, select an action for emails that are detected by this method.
6. Click **Save and Exit**.

See "Working with ICA (heuristics detection method)" on page 37.

See "Defining detection methods and actions for Image Control" on page 31.

Working with ICA (heuristics detection method)

The heuristics detection method uses ICA to read and analyze image content and intercept suspect material. For example, the heuristics detection method can determine the following: whether the image contains any faces, whether it is a portrait photograph, if a body is near the face, the position of that body in relation to the face, and much more. Because ICA has knowledge of anatomy, Image Control is able to calculate the position and suspect nature of the bodies in the image.

When dealing with inbound and outbound emails, you can set the sensitivity of the ICA to low, medium, or high. By adjusting the sensitivity setting, you adjust the tolerance threshold at which an image is declared to be inappropriate. That is, a low sensitivity setting detects fewer inappropriate images than a high sensitivity setting. The low sensitivity setting detects those images that are analyzed as clearly pornographic. The medium and high sensitivity settings detect a wider range of images based on the results of the ICA algorithms.

The sensitivity settings are determined by many scanning algorithms used by the ICA technology to judge an image against specific criteria. The outputs of these algorithms combine to provide a composite score for an image.

Pornography is a very subjective topic, which makes it difficult to declare absolute threshold values for what does and does not constitute pornography. For example, images that are perceived as pornographic by one person may be viewed as art or fashion by another. Also, the use of email within an organization and the culture of that organization has a bearing on how the sensitivity should be set. A marketing business may be more likely to email greater quantities and a wider range of image files than a manufacturing business. With Image Control, the marketing business can use a lower sensitivity setting than the manufacturing business to minimize disruption to normal business email while still catching pornographic material. An organization can arrive at its optimum sensitivity setting by adjusting the settings and observing the results.

False positives are images that are incorrectly identified as pornographic by the Image Control service. False negatives are images that are pornographic but bypass the system without detection. False negatives are not visible from the system statistics. Tests indicate that very few images bypass the scan in this way. If you experience consistent false negatives or false positives, contact the support team. Click **Support** > **Contact Us** for details.

Note: Conditions such as poor lighting or image clarity may cause images to fall outside a given sensitivity band.

See "Enabling the heuristics detection for Image Control" on page 37.

Defining the subject line tag text

If you select an action to **Tag subject line but allow mail through** for any detected inbound email, you must define the text to use in the subject line. Tagging the subject provides the benefit of warning a user that the email may contain an unacceptable image before they open it.

To define a subject line tag

1. Click **Services** > **Email Services** > **Image Control**.
2. Click the **Actions** tab.
3. In the **Inbound mail** section, enter the text to use in the **Enter text** box.

   The default text for the subject line tag is “inappropriate image.” The maximum number of characters that the tag can contain depends on the language that you use. The tag text can contain non-Western characters.
4. Select an option depending on whether to put the text before or after the existing subject line text.
5. Click **Save and exit**.

Frequently asked questions on Image Control

Table 6-2 General

Question	Answer
How does the Image Control service work?	Four components are included within the Image Control service as follows: ■ Heuristics scanner (ICA). Uses a combination of algorithms and heuristics to determine whether an image is inappropriate or not ■ Client approved and blocked image lists. You can add incorrectly classified images to a blocked or approved image list. ■ Global approved and blocked image lists for the Image Control community. The cloud security services adds incorrectly classified images to a global database to take effect for all organizations that have selected this detection method ■ Approved sender and recipient lists. You approve a sender or recipient (internal or external) to send or receive images This multilevel approach ensures increased accuracy and reduced false positives.
Does Image Control scan within Microsoft® Office™ documents as well as the email?	Yes. You can configure the Image Control service to scan within Microsoft® Office™ attachments (Word, Excel, and PowerPoint.

Table 6-2 General *(continued)*

Question	Answer
Does Image Control scan within PDF files as well as the email?	Yes. You can configure the Image Control service to scan within PDF files.
Are email addresses case-sensitive?	Yes. If you want to search for an email address you must type it as it is recorded. Most email addresses are stored in lowercase.
Do you scan within archive files like .zip files?	The Image Control service unpacks attached archive files and scans the image attachments or images within Microsoft Office documents that are archived within them.
If I activate all of the components for my organization, which order do they scan in?	The scan order is as follows: ■ Approved sender and recipient lists ■ Client approved and blocked image lists ■ Global approved and blocked image lists ■ Image Control heuristics scanner This means, for example, that an image that appears in a local approved list overrides the heuristics scanner.
What should I do if a business image has triggered the Image Control service incorrectly?	It depends on what the image is. If the image is likely to be seen again and is company-specific, add it to your client approved images list. If the image is likely to be seen again and is more generic, add the image to your local approved list and send it for analysis to add value to the Image Control community. If a specific user receives a large number of images that are analyzed incorrectly but change frequently, add the individual to the approved recipient list.
How accurate is the ICA scanner?	The ICA (Image Composition Analysis) heuristics scanner should always be used to help monitor and control problem areas, thus enforcing your organization's email security policy. However, ICA cannot be 100 percent accurate due to the objectivity of image analysis. The ICA scanner has different levels of accuracy depending the selected sensitivity setting and the nature of your email. False positives are more likely in a modeling agency than in an IT organization, due to the nature of email that is sent and received.

Table 6-3 Client approved and blocked images lists

Question	Answer
If I add an image to my client approved or blocked images list, how long does it take to update and take effect?	All signatures that are added to your client approved and blocked images lists are collected and distributed to the cloud security services infrastructure.

Table 6-4 Approved senders and recipients

Question	Answer
What happens if I add an approved sender or recipient to my list?	The Image Control service does not scan email communication from approved senders or to approved recipients. These individuals or domains are removed from the Image Control scanning process. **Note:** Your approved senders and recipients are only approved within your organization's Email Security system. The recipient or sender of the email may have their own local scanners set up.

Table 6-5 Global approved and blocked image lists

Question	Answer
What benefit does the global approved and blocked image lists provide to my organization?	Organizations from around the world submit images to the Image Control community. Therefore, many images that are analyzed incorrectly will be added before your organization sees them.
What is the Image Control community? And how can I benefit from it?	The Image Control community comprises The cloud security services and other organizations globally who subscribe to the Image Control service. These organizations submit images that have been analyzed incorrectly for them and that other organizations may be likely to see. The images are analyzed manually, and if they are definitely "good" or "bad" they are added to the global database for use within the community.