



Getting Started Guide

Forcepoint Email Security Cloud

2020

©2020, Forcepoint

Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners.

Every effort has been made to ensure the accuracy of this document. However, Forcepoint makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Forcepoint shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Document last updated: September 11, 2020

Contents

Chapter 1	Registration and Setup	1
	Requesting an evaluation	1
	Logging on to the Forcepoint Cloud Security Gateway Portal	2
	Adding inbound and outbound connections	3
	Adding domains	3
	Setting up outbound email routing	5
	Identifying your Internet mail gateway	6
	Testing your connection	6
	Configuring your Internet mail gateway	9
	Setting up inbound email routing	9
	Restricting connections to your mail servers	10
	Setting up users and groups	11
	Where do I go from here?	11
	Frequently Asked Questions	12
Chapter 2	Setting Up End Users	15
	Introduction	15
	Sample communications	16
	Common considerations	16
Chapter 3	Technical Support	23
	Sales and Feedback	23

1

Registration and Setup

Getting Started Guide | Forcepoint Email Security Cloud

Use the following steps to get started with Forcepoint Email Security Cloud:

1. *Requesting an evaluation*
2. *Logging on to the Forcepoint Cloud Security Gateway Portal*
3. *Adding inbound and outbound connections*
4. *Adding domains*
5. *Setting up outbound email routing*
6. *Setting up inbound email routing*
7. *Restricting connections to your mail servers*
8. *Setting up users and groups*

If you are an existing Forcepoint Web Security Cloud customer or are performing a Forcepoint Web Security Cloud evaluation, you can request that Forcepoint Email Security Cloud services be added to your account by contacting Forcepoint Sales or your reseller. Forcepoint Support notifies you by email when the services are added.

Requesting an evaluation

Getting Started Guide | Forcepoint Email Security Cloud

1. Go to www.forcepoint.com and click **Products**, then select **Forcepoint Email Security Cloud**.
2. Click **Sign Up For A Free Trial** and on the **Free Trials & Demos** page, select **Forcepoint Email Security Cloud**.
3. Complete the enrollment process.

Shortly after you **Confirm** your request, you will receive a confirmation email telling you how to proceed.

If you prefer to talk to a representative, in the U.S. call 1-800-723-1166. Outside the U.S., please visit <http://www.websense.com/content/find-a-partner.aspx> to locate a reseller.

Logging on to the Forcepoint Cloud Security Gateway Portal

Getting Started Guide | Forcepoint Email Security Cloud

When you receive logon information in your confirmation email, log on to the cloud portal by clicking the provided link or by going to <https://admin.forcepoint.net/portal>.



Note

You must have port 443 open on your firewall to access the portal.

For the best experience, accept cookies from the cloud portal. The portal uses 2 cookies:

- The first determines whether the web browser is willing to accept and store cookies for the portal; it contains no information.
- The second contains temporary information about the session.

No personal information is stored in either cookie; both cookies are used only for the duration of the session.

When you connect to the cloud portal for the first time you are prompted to:

- Accept the license agreement for each Forcepoint cloud product you have purchased.
- Select a primary and backup cloud data center for storing reporting data. This is a one-time setup option. Once confirmed, the selection cannot be changed.
- Provide an administrator email address and password recovery question for use in recovering a lost administrator password.

You can now configure your Forcepoint Email Security Cloud account.

A Default email policy has been created for you. To access it, click **Email > Policy Management > Policies**. The Default policy reflects the most commonly chosen policy options.

You can change your configuration at any time. Click **Account** to enter the setup area of the portal.

See [Forcepoint Email Security Cloud Help](#) for full details of every aspect of Forcepoint Email Security Cloud administration.

Adding inbound and outbound connections

Getting Started Guide | Forcepoint Email Security Cloud

Your policy must have at least one default inbound connection and one outbound connection in order to be active on the system.

The **Default Inbound Routes** section defines where Forcepoint Email Security Cloud sends email that is not matched by an inbound routing rule after processing messages received from the Internet - these are the connections to your email servers.

The **Outbound** box specifies from which connections Forcepoint Email Security Cloud is prepared to accept email for your domains (for onward delivery to the Internet).

Select the **Connections** tab on the policy to add, view, or change connections for the policy.

1. Click **Add** on the **Connections** tab to add an IP address or email server for inbound or outbound connections. Choose the button in the **Default Inbound Routes** or **Outbound** box, depending on the direction you are configuring.
2. In the **Server** field, enter a fully qualified host name or an IP address. If you enter an IP address you are asked to give this connection a name. The name you give your IP address connection is not important and can just be “inbound” and “outbound” or whatever you feel is appropriate.

If you enter an invalid IP address such as one from the reserved, private range, an error results.

3. For inbound mail, enter a **Preference** value to specify the order in which connections should be used. (Connections with preference value 1 are used before all other connections.) The preference value is ignored for outbound email.
4. If you wish to use email encryption, enter a **Security** value: Unenforced, Encrypt, Encrypt+CN, Verify, or Verify+CN. See *Encryption tab* in [Forcepoint Email Security Cloud Help](#) for further information.
5. Select an **Encryption Strength**: 128 or 256.
6. Click **Submit**.

For further details, see *Adding inbound and outbound routes* in the [Forcepoint Cloud Security Gateway Portal Help](#).

Adding domains

Getting Started Guide | Forcepoint Email Security Cloud

Each Forcepoint Email Security Cloud policy applies to a set of domains. To add domains to any policy (including the default policy), you must first set up a valid inbound connection on the **Connections** tab that will accept messages for the domain you plan to add. A valid inbound connection is one that accepts messages on port 25

for the domain. If it is behind the firewall, the firewall must allow email traffic from the IP address ranges listed on the **Service IP addresses** page. The connection is checked as part of the validation.

To add a domain or sub-domains to the policy:

1. Click **Add** on the **Domains** tab.
2. Enter the domain name in the **Domain** field.
3. To apply the policy to all sub-domains in the current domain, select **Include sub-domains**.
4. Click **Submit**.

At this stage Forcepoint Email Security Cloud checks for a valid inbound connection for this domain and displays the result on the Add Domain screen. If it cannot find or validate a connection, an error message appears.



Important

The inbound connection checking does not guarantee the correct delivery of email messages. It is strongly recommended that you run your own testing on the inbound connection that you have specified.

The Add Domain screen also displays the following options for you to verify ownership of the domain you have entered. The ownership check initially displays as **Failed**, because it cannot succeed until you have done one of the following:

- Create a CNAME record in your DNS that aliases the character string shown on the screen to autodomain.mailcontrol.com. For more information, see *CNAME records and A records* in the [Forcepoint Email Security Cloud Help](#).
- Create an A record for the character string shown on the screen, pointing to the IP address of autodomain.mailcontrol.com. For more information, see *CNAME records and A records* in the [Forcepoint Email Security Cloud Help](#).
- Add your customer-specific DNS records into your MX records in your DNS. For more information about adding and editing MX records, see *MX records* in the [Forcepoint Email Security Cloud Help](#).

Once you have made one of the above changes, click **Check Now**.



Important

If you choose to use MX record verification, the service will accept email messages for this domain as soon as the MX records are set up.

If you return to the list of domains on the Domains tab before the required record has been added or successfully propagated, the details you entered appear in the domain list with the status **Unchecked**. Once you have created the required records, click the

domain name to view the details, and then click **Check Now** again to retry the validation.



Important

Do not configure domains until you are ready to verify ownership, because all domains are marked **Rejected** after 7 days if ownership verification has not been completed. You must then call Support to edit or re-enable the domain.

Setting up outbound email routing

Getting Started Guide | Forcepoint Email Security Cloud

In order for Forcepoint Email Security Cloud to analyze your outbound email, it must be routed through the Forcepoint Email Security Cloud service using the customer-specific Domain Name System (DNS) record found on the **Service IP addresses** page in the cloud portal (the one that ends in **out.mailcontrol.com**). The way you configure your email system to achieve this depends on how the email servers are set up in your organization.

1. *Identifying your Internet mail gateway.* The first step is to determine the route that email currently takes when intended for an Internet recipient and identify the last server in your organization. We call this your Internet mail gateway. This either routes mail directly to the recipient mail system by looking up the destination mail server(s) address using DNS Mail eXchange (MX) records, or it routes mail to a Simple Mail Transfer Protocol (SMTP) relay at your Internet Service Provider (ISP).
2. *Testing your connection.* Before you change the configuration of your Internet mail gateway, we recommend that you perform a few simple tests to check that you have connectivity through firewalls to the Forcepoint Email Security Cloud service.
3. *Configuring your Internet mail gateway.* You need to configure your Internet mail gateway to use the customer-specific DNS record found on the **Service IP addresses** page in the cloud portal.



Warning

Do not use the specific IP addresses to which these records resolve, because these could change. Should this happen and you have not used the customer-specific DNS records, you will be unable to send outbound email to the service until you make configuration changes.

Identifying your Internet mail gateway

Getting Started Guide | Forcepoint Email Security Cloud

Your Internet mail gateway is the last server in your organization through which outbound email is currently routed.

You can identify the gateway by examining network diagrams. If these are not available, we recommend sending an email message to an external account such as Hotmail or Gmail and examining the message headers of the external mail. The message headers show the route the message has taken through your organization.

For example, the text below shows the routing of a message from Forcepoint to Gmail. Ordinarily, mail systems show the routing consecutively. This routing is shown in reverse order. In this header, you can see 2 gateways in bold: the gateway for Google and the gateway for Forcepoint. The server that passes the message to the Gmail system is mail.forcepoint.com.

```
Delivered-To: anyone@gmail.com
Return-Path: <someone@forcepoint.com>
Received: from cluster-f.mailcontrol.com (cluster-
f.mailcontrol.com [85.119.2.190])
by mx.google.com with ESMTTP id
u9sil453860lmuf.12.2008.07.17.09.24.14;
Thu, 17 Jul 2008 09:24:15 -0700 (PDT)
Received-SPF: pass (google.com: domain of
someone@forcepoint.com designates 85.119.2.190 as permitted
sender) client-ip=85.119.2.190;
Authentication-Results: mx.google.com; spf=pass (google.com:
domain of someone@forcepoint.com designates 85.119.2.190 as
permitted sender) smtp.mail=someone@forcepoint.com
Received: from mail.forcepoint.com by
rly08f.srv.mailcontrol.com (MailControl) with ESMTTP id
m6HGNM80024741
for <anyone@gmail.com>; Thu, 17 Jul 2008 17:24:01 +0100
Subject: Test message
Date: Thu, 17 Jul 2008 17:23:45 +0100
From: "Doe, John" <someone@forcepoint.com>
To: <anyone@gmail.com>
```

Testing your connection

Getting Started Guide | Forcepoint Email Security Cloud

When you add a domain, Forcepoint Email Security Cloud checks for a valid inbound connection for this domain and displays the result on the **Add Domain** screen, accessed through the **Domain** tab. If it cannot find or validate a connection, an error message appears. The inbound connection checking does not guarantee the correct delivery of email messages. It is strongly recommended that you run your own testing on the inbound connection that you have specified.

We also recommend that you test your outbound connection before configuring your policies and beginning mail flow.

To test your outbound connection with the Forcepoint Email Security Cloud service, you can open a telnet session to the service IPs on port 25 using the DNS names you've been assigned, then simulate sending a message:

1. On the machine you identified as your Internet mail gateway, open a command prompt. To do so,
 - a. Select **Start > Run**
 - b. Type "cmd".
 - c. Press **Enter**.
2. Enter the following:

```
telnet custXXXX-1.out.mailcontrol.com 25
```

replacing *custXXXX-1.out.mailcontrol.com* with the first customer-specific DNS record on the Service IP Addresses page in the cloud portal. You should receive a response like this:

```
220 cluster-[x].mailcontrol.com ESMTTP MailControl
```

3. Enter:

```
helo [your server name]
```

For example:

```
HELO mail.customerdomain.com
```

Response:

```
250 cluster-g.mailcontrol.com Hello mail.customerdomain.com  
[192.168.1.1], pleased to meet you
```

4. Enter:

```
mail from: postmaster@yourdomain.com
```

For example

```
mail from: postmaster@customerdomain.com
```

Response:

```
250 2.1.0 <postmaster@customerdomain.com>... Sender ok
```

5. Enter:

```
rcpt to: Your Web mail address
```

Response:

```
250 2.1.5 <yourname@yourcompany.com>... Recipient ok
```

6. Enter:

```
data
```

Response:

```
354 Enter message, end with "." on a line by itself
```

7. Enter a sample message, ending with a period on a line by itself. For example:

```
Subject: connectivity test
```

```
This is a test.
```

```
.
```

Response:

```
250 Message accepted for delivery.
```

8. Quit the session by entering:

```
quit
```

9. Repeat for the second DNS name you've been assigned. Enter:

```
telnet custXXXX-2.out.mailcontrol.com 25
```

```
helo [your server name]
```

```
mail from: postmaster@yourdomain.com
```

```
rcpt to: Your Web email address
```

```
data
```

```
quit
```

10. Test the summary record next, the one with "-s".

```
telnet custXXXX-s.out.mailcontrol.com 25
```

```
helo [your server name]
```

```
mail from: postmaster@yourdomain.com
```

```
rcpt to: Your Web email address
```

```
data
```

```
quit
```

Any of these records can be used to route your email.

If you receive a "relaying denied" error, 1 of 2 things could be happening:

- Your firewall could be presenting its own IP address to the service IPs rather than the mail server's IP address. In this case, you should add the firewall IP address as an outbound connection in your account. To do this, go to the **Connections** tab of the cloud portal and add the firewall's IP address in the connections that you created. This is the most likely cause for this error.

- It could also be that you are using a fully-qualified domain name (FQDN) rather than an IP address for your outbound route. If this is the case, go to the **Connections** tab of the portal and change all outbound and inbound routes to IP addresses.

When you successfully connect to the service, you are ready to change the configuration of your Internet mail gateway.

Once you have changed your Internet mail gateway configuration, you can test the delivery of outbound email via Forcepoint Email Security Cloud by sending to an echo address. For example:

```
echo@uk.psi.net
```

If your email does not get through, check its progress using Message Center in the cloud portal, or contact the Forcepoint Support helpdesk.

Configuring your Internet mail gateway

Getting Started Guide | Forcepoint Email Security Cloud

There are dozens of mail servers available on the market. Some of the most popular include Microsoft Exchange, Novell GroupWise, and IBM Lotus Domino.

Search the Help system of your mail server for the terms “SMTP connector,” “SMTP relay,” or “relay host.” Look for a place where you can specify the SMTP relay host or connector for outbound messages. This is where you enter the customer-specific DNS record from the **Service IP addresses** page in the cloud portal, *custXXXX-s.out.mailcontrol.com*. If you cannot locate a place for this, contact your mail server vendor for assistance.

Setting up inbound email routing

Getting Started Guide | Forcepoint Email Security Cloud

When you add a connection or connections, you entered the IP address and name of your inbound, receiving mail server (the mail server or servers to which Forcepoint Email Security Cloud will send mail when it is received from the Internet) and verified connectivity with your inbound server.

The only thing you need to do for inbound mail is modify the Mail eXchange (MX) records in your organization’s Domain Name System (DNS).

An MX record is an entry in a DNS database that defines the host willing to accept mail for a given machine. Your MX records must route email through Forcepoint Email Security Cloud to your Internet mail gateway.

Contact your DNS manager (usually your Internet service provider (ISP)) and ask them to replace your current MX records with the customer-specific DNS records

listed on the **Service IP addresses** page in the cloud portal (the ones that end in **in.mailcontrol.com**). For example, they might change:

Change	From	To
MX Preference 1	acme.com. IN MX 50 mail.acme.com.	acme.com. IN MX 5 cust0000-1.in.mailcontrol.com .
MX Preference 2	acme.com. IN MX 51 mail.acme.com.	acme.com. IN MX 5 cust0000-2.in.mailcontrol.com .

Make sure they include the trailing period, and ask them to set both of these records to the lowest preference value.

Because Forcepoint Email Security Cloud has a guaranteed 99.999 percent uptime with a geographically distributed network and multiple layers of resilience, you do not need any fallback MX records in addition to the customer-specific DNS records we have provided you. Please ask your DNS manager to remove any fallback MX records.

Fallback routes are susceptible to spammers, anyway. They often deliberately send junk email through fallback routes to evade or reduce the effectiveness of filters on the primary route. Such abuse of fallback routes affects network performance, because the fallback servers are flooded with junk mail. Perhaps most importantly of all, the benefits of network-related filtering techniques on the primary route are severely reduced or lost altogether. You may find that you receive spam or viruses that would otherwise have been blocked by Forcepoint Email Security Cloud's filters.

It normally takes up to 24 hours to propagate changes to your MX records across the Internet.

To view your MX records, you can use the tool on our website:

<http://www.websense.com/content/mxrecordchecker.aspx>

Enter your domain name, for example acme.com, and click **Check MX record**.

Restricting connections to your mail servers

Getting Started Guide | Forcepoint Email Security Cloud

We strongly recommend that you prevent servers on the Internet from sending email directly to your mail servers, ignoring your MX records. If this is not prevented then email can be maliciously routed directly to your mail servers, bypassing Forcepoint Email Security Cloud. You may be able to do this at your corporate firewall or on your Internet mail gateway by restricting incoming SMTP traffic from any source other than Forcepoint Email Security Cloud. We recommend that you block all SMTP traffic except that from all IP address ranges that Forcepoint Email Security Cloud uses. These can be found on the **Email > Settings > Service IP addresses** page in the cloud portal.

In addition, you should enforce outbound mail routing to be via Forcepoint Email Security Cloud to ensure that it is analyzed for viruses and other security issues.

As a general security measure, we also recommend restricting the use of external Web mail systems such as Hotmail, because they offer another possible avenue for virus infection. Where possible, you should also block IMAP and POP3 access from your network to external mail servers. Email arriving from such servers has not been processed by Forcepoint Email Security Cloud.

Setting up users and groups

Getting Started Guide | Forcepoint Email Security Cloud

Click **Account** on the cloud portal main menu bar to define users and groups of people who will use the service. See the [Forcepoint Email Security Cloud Help](#) for instructions.

If you are a large organization with an LDAP-compliant directory such as Active Directory, you can set up users and groups automatically by synchronizing your directory to the cloud service. This is described in the [Forcepoint Email Security Cloud Help](#).

Note that you do not need to add or synchronize groups just because users are members of them. You need groups only if you intend to use them for policy assignment or exceptions.

Before you synchronize any data, we strongly recommend that you review your current directory structure and plan how your data structure will work within the cloud portal. Here are some questions to consider:

- Do you have sites or departments with different filtering requirements?
- Are there exceptions to rules within a group? If so, what are they?
- How often does the directory change?
- How often should you synchronize?

Refer to Appendix A of the [Forcepoint Email Security Cloud Help](#) for guidelines on setting up directory synchronization for your email service.

Where do I go from here?

Getting Started Guide | Forcepoint Email Security Cloud

Now that you've set up inbound and outbound mail routing, you can send and receive mail using the default policy that's been established for you. We recommend that you notify end users that you are evaluating this service so that they are aware there may be changes to the email they receive. (See the next section of this guide for considerations and sample notification messages.)

If you would like to customize the default policy, set up white and black lists, change attachment rules, or perform other administrative functions, refer to the [Forcepoint Email Security Cloud Help](#) for instructions. It explains how to use the various sections of the manager to set up your account and policies. Online assistance is also available. Just click **Help** in the manager to access it.

In addition, there are a number of FAQs in the [Knowledge Base](#). Some of the most common questions are included in the next section.

Frequently Asked Questions

Getting Started Guide | Forcepoint Email Security Cloud

Can I have different annotations for different parts of my business?

Annotations are added to messages as they pass through the service. By default, they are set up for entire policies; however, you can also set up more specific annotations. Refer to [Forcepoint Cloud Security Gateway Portal Help](#) for instructions.

Examples of annotations that you might add to inbound messages are, “Click [here](#) to report this message as spam,” and “This message has been analyzed for malware by Forcepoint Email Security Cloud.”

For inbound email, you can create annotations specific to each domain in your policy. For outbound email, you can create annotations specific to an arbitrary list of domains, email addresses, or groups.

Can I allow certain addresses to receive an encrypted message while blocking it for everyone else?

Yes, but this requires a custom rule. See “Content Filtering” in [Forcepoint Email Security Cloud Help](#) for more information.

Can I have per-user/group message-size limits?

Not at this time. This is under consideration for a future release. For now, message-size limits are configured at the account level.

Why is my whitelisted message blocked?

A whitelist entry for an address may appear not to work if there is a conflict between black listing and white listing or between policy-level exceptions and account-level exceptions. Whitelists apply only to messages identified as spam. Other security analyses still apply to whitelisted messages, so the message could have been blocked because it contains a virus. It could also be blocked if it breaks other rules established for your account.

I've just set up the service and I can't send any outbound mail. It's all

denied with a “relaying denied” message.

Your firewall could be presenting its own IP address to the service IPs rather than the mail server’s IP address. In this case, you should add the firewall IP as an outbound connection in your account. To do this, go to the **Connections** tab of your policy and add the firewall’s IP address in the connections that you created. This is the most likely cause for this error.

It could also be that you are using a fully-qualified domain names (FQDN) rather than an IP address for your outbound route. If this is the case, go to the **Connections** tab of your policy and change all outbound and inbound routes to IP addresses.

2

Setting Up End Users

Introduction

Getting Started Guide | Forcepoint Email Security Cloud

You can set up Forcepoint Email Security Cloud services quickly and easily with minimum disruption to email users. Depending on the services you have licensed, however, users may experience some changes to the email they receive. This document advises you how to best communicate these changes to your end-user community.

What you need to communicate depends on the services you have licensed and your policy configuration. It is not unusual for organizations to change their policy configuration following an initial evaluation stage. Whenever a change affects the end-user community, it is good practice to inform the community in advance.

This document outlines the main policy configuration areas that affect the end user. Also included is sample text that can be pasted directly into a communication to your end users or used as a template.

Please read this document in conjunction with the [Forcepoint Email Security Cloud Help](#). The sample text is intended to supplement, not replace the *End User Guide* and *End User Quick Start Guide*.

Sample communications

Below is an introduction to the Forcepoint Email Security Cloud services that you can use with your own end users. Some of this text may not be relevant depending upon the services you have chosen.

Dear user,

We are introducing a new email analysis service, called Forcepoint Email Security Cloud, to filter out spam (junk email), computer viruses, phishing attacks, and email with inappropriate content.

Forcepoint Email Security Cloud uses a highly advanced spam detection engine to block email at the Internet level, before it reaches our network. All your email will continue to be delivered as normal, but you should notice a reduction in the volume of junk email you receive. We have also implemented a content filtering service to protect you and the business. By analyzing the content of email, we can ensure that those containing inappropriate words or file attachments do not enter or leave the organization.

In general, you won't be aware that Forcepoint Email Security Cloud is running. However, one of the reasons we chose Forcepoint Email Security Cloud is that it gives you, the end user, some control over the way the service operates. Details of how to use this functionality are contained in the attached End User Guide.

No spam detection engine is foolproof, however we believe Forcepoint Email Security Cloud will block over 98% of all our spam email.

The service will go live on XXXX. If anyone has any questions please contact the helpdesk.

Common considerations

Each Forcepoint Email Security Cloud service has a number of configurable options that can have a direct impact on end users' experience. The main areas that may need to be communicated are discussed in the following sections. Sample text that you can edit and paste into your communications is provided for each option.

Antivirus

1. When inbound email is quarantined because it contains a virus, users receive a notification by default. The user may call the helpdesk to find out the contents of the email. It is unlikely that a virus-infected message contains useful information and therefore you may not achieve anything by enabling notifications. Users subscribing to a personal message report are made aware of email that is quarantined because it contained a virus. Note that notifications on quarantining inbound email may be required for content filtering rules.

- By default, notifications are sent to the sender when Forcepoint Email Security Cloud receives a virus-infected outbound email. This ensures that the user knows they have been infected with a virus. You may want to inform users of this:

Example text

The Antivirus service informs you by email notification if you send an email that contains a virus. If you receive such a notification, you should immediately contact the helpdesk. You are not notified if an email sent to you contains a virus. This is because most virus-infected email is not purposely sent, so it is unlikely that there is any useful content in it.

If you want an IT staff member to be notified as well, you can configure the service to notify an administrator.

- By default, the service blocks executable file attachments. You should inform end users of this:

Example text

To minimize the possibility of an unknown virus infecting your computer, Forcepoint Email Security Cloud has been configured to block executable file attachments. If you must receive such attachments, please contact the helpdesk.

Antispam

The **Tag and Deliver** option is often used during an evaluation or initial roll-out phase to gain end user confidence. End users should be informed how long this will last, when the switch to quarantine will occur, and what to do if they receive email tagged as spam that they believe is not.

Example message 1

For the first XXXXX, we will not quarantine spam but will tag it as such and deliver it to you. Note that what you consider to be spam may not be what others consider spam; some of the messages that you receive may be borderline. See the End User Guide for information about black lists and white lists that help you manage how you classify spam.

Example message 2:

We have now successfully completed the evaluation of the Forcepoint Email Security Cloud service. Going forward, spam messages will be quarantined rather than tagged.

- If you are not going to grant access to personal (end-user) message reports, we recommend that the end users are not given the End User Guide. This guide contains information to allow end users to manage their quarantined email.
- If end users are not allowed to release a copy of quarantined spam, they should be informed of this.

Example text

All quarantined email will be managed by the IT department. If you believe that an email may have been quarantined by mistake, please contact the helpdesk.

3. If end users are not allowed to populate individual allow and block lists, they should be informed of this.

Example text

All allow lists and block lists will be managed by the IT department.

4. By default, we include the “Report this email as spam” link in your inbound annotation. See the *Forcepoint Email Security Cloud Help* for more details.

Example text

If you receive an email that you think is spam and it has a link on the bottom for reporting spam, click the link. See the End User Guide for more information.

Content Filtering

1. Forcepoint Email Security Cloud allows you to block or mask file attachments with extensions that you specify. This allows you to control what types of file attachments are allowed into the organization.

Example text

For additional protection, we have configured Forcepoint Email Security Cloud to disable file extensions for the following attachment file types: XXXX. This prevents attachments from automatically running when you open the email or double-click the attachment. If you need to access an attachment, contact the helpdesk.

2. Forcepoint Email Security Cloud provides bandwidth-saving features that allow messages over certain sizes to be non-delivered, quarantined, or delayed until outside of business hours.

Example text

Large email messages take up bandwidth and slow down our Internet connection, therefore we have implemented the following restrictions:

- *Inbound email messages over XXMB will not be delivered.*
- *Inbound and outbound email messages over XXMB will be quarantined, and you will receive a notification email. If this happens and you need to release the email, contact the helpdesk.*

Emails bigger than XXMB will be delayed and delivered overnight when their affect on our Internet connection will not be noticed.

3. The attachment parking feature allows you to strip attachments over a defined size from email and park them in a secure quarantine store for collection by the recipient over HTTPS.

Example text

People are often sent large file attachments that take up bandwidth and slow down our Internet connection. Often these are not needed or can be discarded once read. We have therefore implemented a feature within our Forcepoint Email Security Cloud email service that will strip attachments over XXMB in size from your email and park them in a secure store for you for up to XX days. You will receive an email when this happens, with an annotation (text at the bottom) followed by a link. Click this link and you will be given the option to save the file or open it.

4. Enforcing controls using lexical rules could be contentious. Forcepoint recommends that you communicate that they have been implemented.

Example text

To protect you and the business, we have implemented a number of rules that analyze email for inappropriate content and words. Please see the company computer use policy for further detail about what is deemed inappropriate use of email. If you receive or send email that contravenes our email policy, Forcepoint Email Security Cloud will send you a notification email.

We suggest you include a link to your computer or email use policy in this message.

Encryption

1. If you are implementing email encryption, you should inform your users that you have an encryption policy in place.

Example text

To ensure the privacy and integrity of our email communications, we have implemented policy-based email encryption.

2. The TLS part of email encryption requires no intervention from your users, but you may want to communicate to them which organizations you have configured within the encryption policy, especially to those users to whom you are making ad hoc encryption available (see below).

Example text

Our policy is set up to encrypt data that is sent to or from organizations with whom we communicate sensitive information on a regular basis. The organizations affected are XX / a list of the organizations affected can be found here: XX.

3. Standard (ad hoc) encryption rules can affect users and/or a rule can require user intervention to trigger it. Your communication may be user or group specific and will depend on the rules configured. Below are some examples of what you could communicate for each rule.

Example text

Our policy allows individual messages to be encrypted according to a set of rules configured within our Forcepoint Forcepoint Email Security Cloud service. When an outbound email meets the criteria in a rule, it is saved into a secure quarantine area for collection by the recipient using a secure Web browser session. The recipient will receive a notification with a link to the email. They also need a password to allow them to access it. It is your responsibility to communicate this password to the recipient.

Email that meet ALL of the following criteria will trigger rule XX:

- *Email from XX*
- *Email sent to XX*
- *Email that is marked as sensitive*
- *Email with the prefix XX at the beginning of the subject line, followed by a space, before the subject.*

When using automatic password generation, you should communicate this.

Example text

You will receive a notification email confirming that the email that you sent has been encrypted. This will contain the password that recipients need to access this email.

If you are allowing a user-specified password and are using a prefix to trigger the ad hoc encryption process, you should communicate the format.

Example text

You must specify the prefix trigger word XX at the beginning of the email subject. Follow the trigger word by a space, the password that you want the recipient to use to access the email in parentheses, another space, and the subject itself. For example:

XX (password) Subject

If you are allowing a user-specified password and are not using a prefix to trigger the ad hoc encryption process, you should communicate the format.

Example text

You must specify a password that you want the recipient to use to collect the email in the subject line. This must be indicated by a prefix XX followed by a space, the password in parentheses, another space, and the subject itself. For example:

XX (password) Subject

If you have the Forcepoint Email Security Encryption Module, you can set up advanced encryption rules in a similar manner to standard encryption, but the message retrieval process is different. You should communicate something similar to the following:

Example text

Our policy allows individual messages to be encrypted according to a set of rules configured within our Forcepoint Email Security Cloud service. When an outbound email meets the criteria in a rule, it is saved into a secure quarantine area for collection by the recipient using a secure Web browser session. The recipient will receive a notification with a link to the email. They will need to enter their email address and create a password to allow them to access it. The recipient then uses this password to access all subsequent encrypted messages sent to their email address.

Email that meet one or all of the following criteria will trigger rule XX:

- *Email from XX*
- *Email sent to XX*
- *Email that is marked as sensitive*
- *Email with the keyword(s) XX in the subject line or body of the message.*

3

Technical Support

Forcepoint provides technical information about Forcepoint products online 24 hours a day, including:

- Latest release information
- Searchable Knowledge Base
- Show-me tutorials
- Product documents
- Tips
- In-depth technical papers

Access support on the website at:

support.forcepoint.com

It is highly recommended that you create an account at the Forcepoint [My Account](#) page when you first set up your Forcepoint Email Security Cloud account.

When you do, you are prompted to enter your Forcepoint subscription keys. This helps to ensure ready access to information, alerts, and help relevant to your chosen Forcepoint products and versions whenever you need support or updates.

If you need additional help, please fill out the online support form at:

support.forcepoint.com/ContactSupport

Make a note of your case number.

Sales and Feedback

For product and pricing information, or to place an order, contact Forcepoint. To find your nearest Forcepoint office, please visit our web site: www.forcepoint.com.

