Mobile DLP Quick Start

(Email Synchronization)

Forcepoint™ TRITON® AP-DATA lets you define what content can and cannot be sent to mobile devices—such as phones and i-pads—from network email systems. Most organizations employ such a policy to protect their data in case an employee's mobile devices is lost or stolen.

The system analyzes content when users synchronize their mobile devices to their organization's Exchange server. If content being pushed to the device breaches the organization's mobile DLP policy, it is quarantined or permitted accordingly, whether that content is part of an email message, calendar item, or task.

Mobile policies are set for user directory entries (users and groups), business units, or custom users, not individual mobile devices.

To get started with mobile DLP

1. Define *user directories* for TRITON AP-DATA users and other policy resources such as networks and domains.
2. Set up *email properties* for alerts and notifications.
3. *Connect* the mobile agent to your Microsoft Exchange server and mobile devices.
4. Optionally, configure *settings* for mobile devices, such as which email components to analyze and which devices to trust.
5. Configure the mobile *quick-start policy*. Select and enable the mobile attributes to monitor—for example message size. Configure properties for those attributes.
6. *Deploy* your settings.

Note

You can't delete or rename your mobile DLP policy, but you can enable or disable its attributes.

Configuring user directory server settings

To resolve user details during analysis and enhance the details displayed in reporting, you need to first configure user directory server settings.

In the TRITON Manager, define the LDAP user directory to use *when adding and authenticating TRITON administrators* with network accounts. (Select **TRITON Settings** from the TRITON toolbar, then select **General** > **User Directory**.)

In the Data module of the TRITON Manager, you define the user directory to use *for TRITON AP-DATA users and other policy resources* such as devices and networks.

1. Select **Settings > General > User Directories**.
2. Click **New** in the toolbar.
3. In the Add User Directory Server screen, complete the following fields:

Field	Description
Name	Enter a name for the user directory server.
Type	Select the type of directory from the pull-down menu: Active Directory, Domino, or CSV file.
Connection Settings	
IP address or host name	Enter the IP address or host name of the user directory server.
Port	Enter the port number of the user directory server.
User distinguished name	Enter a user name that has access to the directory server.
Password	Enter the password for this user name.
Root naming context	Optionally, enter the root naming context that TRITON AP-DATA should use to search for user information. If you supply a value, it must be a valid context in your domain. If the **Root naming context** field is left blank, the system begins searching at the top level of the directory service.
Use SSL encryption	Select this box if you want to connect to the directory server using Secure Sockets Layer (SSL) encryption.
Follow referrals	Select **Follow referrals** if you want TRITON AP-DATA to follow server referrals should they exist. A server referral is when one server refers to another for programs or data.
Test Connection	Click this button to test your connection to the user-directory server.
Directory usage	
Get user attributes	Select this box if you want to retrieve user attributes from the directory server.
Attributes to retrieve	Enter the user attributes that you want the Data Security manager to collect for all users (comma separated).

Field	Description
Photo attributes to retrieve	Enter the valid photo attributes, thumbnailPhoto (default), to display a photo of the user (comma separated). • If you do not want to display a photo of the user, leave this field blank. • If a photo does not exist for the user, an empty image displays.
Sample email address	Enter a valid email address with which you can perform a test.
Test Attributes	Click **Test Attributes** to retrieve user information, such as the user's attributes and email address you supplied.

4. Click **OK** to save your changes.

Note

If you select CSV as the file type in the Add User Directory Server, you won't see the IP address, port, and SSL fields. You need to supply the full path for the CSV files, along with a user name and password. The Test Connection functionality is the same.

There are no Directory usage fields associated with CSV files.

Setting up email properties

Set up the email properties, such as SMTP mail server, to be used for system alerts.

1. Select **Settings > General > Alerts**.
2. On the **General** tab select the conditions on which you want to trigger alerts.
3. On the **Email Properties** tab, complete the fields as follows:

Field	Description
Sender name	When an alert is sent to administrators, from whom should it be coming?
Sender email address	Enter the email address of the person from whom the alert is coming.

4. To define or edit the **Outgoing mail server**, click Edit (the pencil icon). Complete the fields as follows:

Field	Description
IP address or host name	Enter the IP address or host name of the outgoing SMTP mail server to use for scheduled alerts and notifications.
Port	Enter the port number of the mail server to use.

5. Complete the remaining fields as follows:

Field	Description
Subject	Enter a subject for alerts. Click the right-arrow to select a variable to include in the subject, such as %Severity%.
Recipients	Click **Edit** to select the recipients to whom alerts should be sent.

6. Click **OK** to save your changes.

Note

The same outgoing mail server is used for alerts, notifications, scheduled tasks, and email workflow. The settings you use here apply to the other cases, and if you change the settings for one, it affects the others.

Configuring the mobile agent

After you install the mobile agent in your network, you must connect it to your Microsoft Exchange Server and mobile devices. To do so:

1. Select **Settings > Deployment > System Modules**.
2. Click the mobile agent module.
3. On the **Connections** tab, complete the fields as follows:

Field	Description
Exchange Connection	
Use secure connection (SSL)	Select this box if you want to use Secure Sockets Layer (SSL) to provide communication security when connecting the mobile agent to your Microsoft Exchange server.
Host name or IP address	Enter the IP address of your Microsoft Exchange server. The mobile appliance connects to this server to access email resources. The appliance acts as a reverse proxy to the Exchange server, making mobile devices unaware of the server.

Field	Description
Port	The port number for the Microsoft Exchange server depends on whether you are using a secure connection: • If you select the **Use secure connection (SSL)** check box, the Exchange server must connect on port 443. • If you do not select the **Use secure connection (SSL)** check box, the Exchange server must connect on port 80.
Domain	Optionally, enter the domain used to identify users in your organization.
Mobile Devices Connection	
Use secure connection (SSL)	Select this box if you want to use Secure Sockets Layer (SSL) to provide communication security when connecting the mobile agent to your users' mobile devices.
IP address	Select the IP address of the network interface card (NIC) that mobile devices should use to connect to this agent. This is a NIC on the mobile appliance or machine hosting the mobile agent. It is the IP address that the mobile agent will listen on. The list reflects all of the NICs found on the mobile appliance. Select **All IP addresses** to allow the agent to listen and accept connections from all available network interface IPs. **Note:** To modify the IP addresses available on the mobile agent machine, re-install and re-register the mobile agent. If you enter a user name in the installation wizard, the system resolves it to the correct IP address.
Port	The port number for the Microsoft Exchange server depends on whether you are using a secure connection: • If you select the **Use secure connection (SSL)** check box, the Exchange server must connect on port 443. • If you do not select the **Use secure connection (SSL)** check box, the Exchange server must connect on port 80.
Use Forcepoint default security certificate	To secure connection, users must set up their mobile devices to accept security certificates from the server. Select this option to use the default security certificate provided by Forcepoint. The default security certificate is a self-signed certificate automatically generated by Forcepoint. It enables SSL encryption to secure the ActiveSync public channel that is used by the mobile agent when communicating with mobile devices, but it does not rely on a well known Root CA for authentication. If you use this option, users may need to configure their mobile devices to accept all SSL certificates. Some devices, such as those using Windows Mobile 7, do not support this.

Field	Description
Use the following certificates	Select this option to secure the ActiveSync public channel using your own signed certificates, then upload the certificates to use. This option enables SSL encryption and CA authentication, so it is seamlessly accepted by all mobile devices. You must upload both a public certificate and its associated private key. ● **Public certificate** - Upload the public certificate that the agent should use to identify itself to mobile devices. The signing CA can be a self-signed Root CA or subordinated (possibly untrusted) CA. If your certificate is signed by a subordinated CA, you must also upload its associated certificate chain file. (See **Add chained certificate** below.) ● **Private key** - Upload the private key that was used to generate the public certificate. The certificate files must conform to these requirements: ● All files should be in .PEM file format. ● The .PEM files for the public certificate and private key must be separate. Concatenaton is not supported. ● The files should not be encrypted or passphrase protected. ● You must follow a Certificate Signing Request (CSR) procedure when creating the files. Instructions are readily available online.
Add chained certificate	Select this option if your public certificate is signed by a subordinated certificate. The certificate chain, also known as the certification path, should be a list of all of the CA certificates between (but not including) the server certificate and the Root CA stored in the mobile devices. Each certificate in the list should be signed by the entity identified by the next. For example, the chained certificate should include numbers 2, 3, and 4 below, but not numbers 1 or 2. 1. Server certificate, signed by 2. Issuing CA 1, signed by 3. Intermediate CA 2, signed by 4. Intermediate CA 3, signed by 5. Root CA The SSLCertificateChainFile file is the concatenation of the various PEM-encoded CA certificate files, usually in certificate chain order. In most cases, the CA organization you work with provides this file.

4. On the **Analysis** tab, complete the fields as follows:

Field	Description
Mode	Select the mode in which you want to deploy the module: • **Monitoring** - Monitor traffic through the mobile agent but not block it. • **Blocking** - Block actions that breach policy.
When an unspecified error occurs	Only available in blocking mode. Select what action to take when an unspecified error occurs during data analysis and traffic cannot be analyzed: • **Permit traffic** - Allow traffic routed through the mobile agent to continue unprotected. • **Block traffic** - Stop all traffic through the mobile agent until the problem is resolved.
Notify users of breach	Only available in blocking mode. Select this option if you want to notify users when an email message, task, appointment, or other item was blocked by the agent. You can enter the text to include in the email subject line and body, or you can click the right arrows and select from variables such as %From%, %Attachments%, and %Type%. **Note:** Before users can be notified of breaches, you must configure an outgoing mail server and sender details. To do so, navigate to **Settings > General > Alerts**, and then select the Email Properties tab.
Minimum transaction size	Select the smallest email transaction to analyze, in bytes.

5. Click **OK**.

Configuring mobile device settings

If desired, you can customize the default settings configured for mobile devices—settings such as how long to keep released messages (14 days), how often to send status updates (every 5 minutes), which email components to monitor (all), and which devices to trust (none).

To do so:

1. Select **Settings > General > Mobile**.

2. Complete the fields as follows:

Field	Description
Keep released messages for	When the mobile agent accepts a release operation for a specific message, it stores it for 2 main purposes: • To wait for the user's device to sync, which triggers the actual release sequence in Exchange. • To avoid any subsequent analysis for the same message by the same user syncing to a second device. Indicate how long the mobile agent should preserve a release operation. You can select between 3 and 30 days. By default, released messages are stored for 14 days. This number affects the size of your incident database. A large number requires more storage space than a small one.
Update status every	Indicate how often you want device status sent to the management server. Status includes the device owner and type, date of the last synchronization, date of incident detection, and more. You can update status every minute, hourly, or any interval in between. By default, status is sent every 5 minutes. Status from all registered devices is sent to the management server in a single batch operation.

Field	Description
Analyze the following components	Indicate which Exchange server components you want the mobile agent to analyze: • **Email messages** - Select this to analyze all parts of an email message (Subject, Body, To, From, Attachments, etc.) • **Calendar events** - Select this to analyze calendar items, including Subject, Location, Attendees, and Description. • **Tasks** - Select this to analyze content in To-Do lists. By default, all message types are analyzed.
Trusted Devices	Trusted devices are those you feel you don't need to monitor. Trusted devices do not get analyzed by TRITON AP-DATA. If you have devices that you do not want enforced: 1. Select **Enable trusted devices**. 2. One by one, enter a user name and user agent for each trusted device, and then click **Add**. ▪ **User name** - The name of the device user, case insensitive. Do not include the domain name. For example, enter jdoe rather than mydomain\jdoe. If you leave this field blank, all people who use the device specified in the User agent field are trusted. ▪ **User agent** - a case-sensitive identifier used to identify the device operating system and email client software. Similar devices share the same identifier. If you leave this field blank, all devices for the specified users are trusted—for example, all mobile devices used by jdoe. If the device is connected to an Exchange server, you can find the user agent string using an interface such as Outlook Web App (OWA). Click **Remove** to remove a device from the trusted device list.

3. Click **OK**.

Configuring the mobile quick-start policy

A quick-start mobile data loss prevention (DLP) policy is provided with TRITON AP-DATA. You just need to configure it.

1. In the Data Security manager, select **Main > Policy Management > DLP Policies > Mobile DLP Policy**.

2. On the **Attributes** tab, select one or more web attributes to include in the policy, then define parameters for those attributes in the right pane. When the system detects a match for an attribute, it triggers the policy. (Refer to the following table for a description of each attribute.)

   a. If you want to send notifications when there is a violation of a particular attribute setting, select the **Send the following notification:** check box. You can configure who receives the notifications by clicking the name of the notification, "Web policy violation." Click this option to define the mail server, email subject, and message body, as well as other required properties. Policy owners receive notifications by default.

   b. For each attribute, indicate how severe a breach would be (low, medium, or high severity), and what action should be taken if a breach is detected. The default severity levels and available actions are shown below for each attribute.

Field	Description
Message size	Select the size of email messages to monitor. For example, choose 25 MB if you want the systemto analyze and enforce messages exceeding 25 MB, but you're not concerned about messages smaller than 25 MB, even if there is a match. The default size is 10 MB. Default severity: **low**. Available actions: **quarantine** (default), **permit**.
Regulatory & compliance	Select the regulatory and compliance laws you need to enforce. These are applied to the regions you selected with the regulatory & compliance option. • Personally Identifiable Information (PII) • Protected Health Information (PHI) • Payment Card Industry (PCI DSS) If you have not selected regions, an error pops up. Click "Select regions" to fix this. Once you've selected a law, click its name to view or edit the specific policies to enforce. For example, in the PCI category, both Europe and US credit card policies are enforced by default. You might exclude the US credit card policy if you do not do business in the US. Applying only the policies you need improves performance and reduces resource consumption. Select a sensitivity for each policy. • **Wide** is highly sensitive and errs on the restrictive side. To avoid leaking sensitive data, it is more likely to produce a false positive (unintended match) than a false negative (content that is not detected). • **Default** balances the number of false positives and false negatives. • **Narrow** is the least restrictive. It is more likely to let content through than to produce an unintended match. Default severity: **high**. Available actions: **quarantine** (default), **permit**.

Field	Description
Attachment name	One by one, enter the names of the exact files that should be monitored when they're attached to an email message. Include the filename and extension. Click **Add** after each entry. For example, add the file named **confidential.docx**. When that file is attached to an email message, the system detects it and either permits or quarantines the message. Default severity: **low**. Available actions: **quarantine** (default), **permit**
Attachment type	Click **Add** to specify the types of files that should be monitored when attached to an email message, for example Microsoft Excel files. From the resulting dialog box, select the type or types of files to monitor. If there are more file types than can appear on the page, enter search criteria to find the file type you want. The system searches in the file type group, description, and file type for the data you enter. If the file type does not exist, specify exact files of this type using the **Attachment name** attribute instead. Default severity: **low**. Available actions: **quarantine** (default), **permit**.
Patterns & phrases	Click **Add** to define key phrases or regular expression (RegEx) patterns that should be monitored. RegEx patterns are used to identify alphanumeric strings of a certain format. On the resulting dialog box, enter the precise phrase (for example "Internal Only") or RegEx pattern (for example ~ m/H.?e/) to include. Select how many phrase matches must be made for the policy to trigger. The default number of matches is 1. Define whether to search for the phrase or RegEx pattern in all email fields, or in one or more specific fields. For example, you may want to search only in an attachment, or skip searching in To and CC fields. Default severity: **medium**. Available actions: **quarantine** (default), **permit**. **Note:** Although you do not define whether to search only for unique strings, the system will use the following defaults: Key phrase: non-unique - all matches will be reported. Regular expression: unique - only unique matches will be reported as triggered values.

Field	Description
Acceptable use	Select the dictionaries that define unacceptable use in your organization. For example, if you want to prevent adult language from being exchanged by email, select Adult. TRITON AP-DATA includes dictionaries in 9 languages. Select the languages to enforce. Only terms in these languages are considered a match. For example, if you select the Adult dictionary in Hebrew, then adult terms in English are not considered an incident. Note that false positives (unintended matches) are more likely to occur when you select multiple languages. For this reason, exercise caution when selecting the languages to enforce. You cannot add or delete terms from predefined dictionaries, but you can exclude them from detection if you are getting unintended matches. Select **Main > Policy Management > Content Classifiers > Patterns & Phrases**, select the dictionary to edit, then enter the phrases to exclude. By default the policy is triggered by a single match from the dictionary or dictionaries you select. Default severity: **medium**. Available actions: **quarantine** (default), **permit**.
Questionable images	Select this attribute to prevent pornographic images from entering your organization. (This feature requires a special TRITON AP-DATA Image Analysis subscription). Pornographic images pose a legal liability to organizations in many countries. The system judges images based on the amount of flesh tone they contain. Default severity: **low**. Available actions: **quarantine** (default), **permit**.

3. Indicate which users to trust. Policies are not enforced for trusted users.
4. On the **Policy Owners** tab, define an owner or owners for this Mobile DLP policy. Policy owners can modify a policy and, if configured, receive notifications of breaches. Notifications must be enabled in one or more of the policy's attributes for notifications to be sent.
5. Click **OK**.
6. If you would like notifications to be sent to policy owners:
   a. Select **Main > Policy Management > Resources**.
   b. Click **Notifications** in the Remediation section of the page.
   c. Select an existing notification or click **New** to create a new one.
   d. Under Recipients, select **Additional email addresses**.
   e. Click the right arrow then select the variable, %Policy Owners%.
   f. Click **OK**.

Deploying your settings

The settings you configured in this chapter must be deployed to the mobile agent appliance and other system components to begin monitoring your mobile devices.

To deploy settings, click **Deploy** in the Data Security manager toolbar.

Your mobile DLP policy is now functioning!