# Websense® Email RiskVision Setup Guide

v7.8.x

10240 Sorrento Valley Rd., San Diego, CA 92121, USA

Published August 2014
Printed in the United States and Ireland



### Trademarks

# Contents

# 1 Websense Email RiskVision Overview



Websense® Email RiskVision provides a way to analyze email traffic without disrupting an organization's existing email traffic flow. A Websense V-Series™ appliance-based tool, Email RiskVision monitors email traffic by connecting to the span or mirror port on a network switch and receiving a duplicate of the organization's mail flow.

- Message traffic is inspected by a robust set of analytics that detect potentially malicious attacks.
- Email data loss protection (DLP) capabilities can examine outbound messages for possible data exfiltration incidents.
- Image analysis monitors email for compliance and acceptable use purposes.
- Dashboard charts and reports provide insight into email threats confronting an organization.

Email RiskVision features include:

- Connection-level controls like real-time blacklist (RBL) options, reverse DNS lookup, and reputation service classifications
- Mail relay control options like Sender Policy Framework (SPF) record checking
- A comprehensive collection of analytics engines that examine email for viruses, spam, malicious URLs, and the characteristics of commercial bulk email
- Functionality in the Data Security manager for creating email DLP policies, including those that monitor questionable images
- Reporting tools like dashboard charts and presentation reports that allow administrators to view analysis results

You must download the following files for a Websense Email RiskVision deployment:

Appliance image file (Linux):

Websense_ERV_78x_ApplianceImage.iso

- TRITON console (Windows):

  Websense_TRITON_ERV78xSetup.exe

The installation and deployment process for Email RiskVision has 3 basic stages. Use this guide to ensure that you complete the entire process.

**Contents:**

# 2 Set Up the Appliance



Deploy Websense® Email RiskVision by setting up the V-Series™ appliance hardware and performing basic appliance configuration, as outlined below.

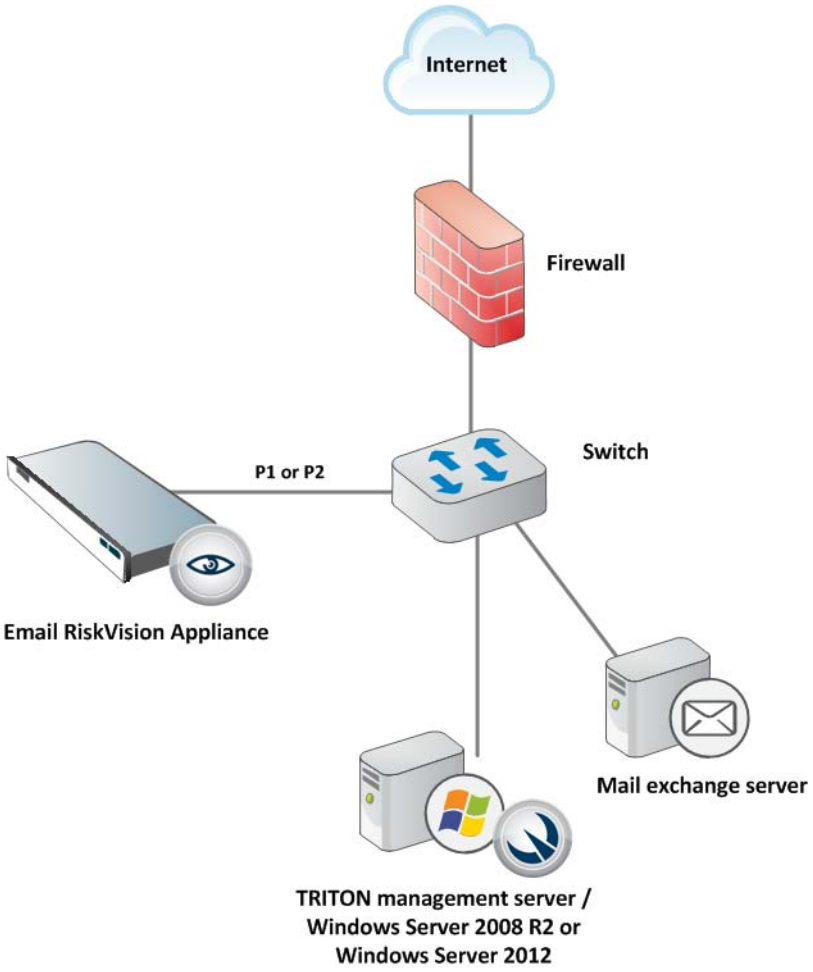
- *Step 1: Set up the appliance hardware* (rack and cable the appliance).
- *Step 2: Run the firstboot script* (activate the appliance).
- *Step 3: Configure basic appliance settings* (set date and time, and add an appliance description).

Websense Email RiskVision is not supported on a virtual appliance. An Email RiskVision appliance may not run in dual security mode with Websense Web Security, Web Security Gateway, or TRITON® RiskVision (for Web).

# Step 1: Set up the appliance hardware

The diagram below gives a simple overview of a Websense Email RiskVision deployment. In addition to the appliance, a Windows Server 2008 R2 or Windows Server 2012 machine is required to host management and reporting components. The management and reporting components must be configured to connect to a Microsoft SQL Server 2008, 2008 R2, or 2012 installation within your network.

A switch should be configured to send a duplicate of the organization's email traffic flow to the RiskVision appliance. Use the P1 or P2 network interface to connect to a span or mirror port on the switch. Cat 5E cables (or better) are required. Do not use crossover network cables.




For a V10000 appliance, network **interface C** provides communication for appliance modules and handles database downloads. Network **interface P1** serves this purpose on a V5000 appliance.

The communication interface:

- Must be able to access a DNS server

- Should have continuous access to the Internet

Ensure that the communication interface is able to access the download servers at **download.websense.com**. This URL must be permitted by all firewalls, routers, or host files controlling the URLs that the communication interface can access.

## Step 2: Run the firstboot script

You must re-image the appliance before you set up the machine and run the firstboot script. Click here to download the **Websense_ERV_78x_ApplianceImage.iso** image file. This file may be used for both the V10000 G3 and V5000 G2 appliances.

Install the image on the appliance in one of two ways:

- As a virtual DVD, via a Dell Remote Access Controller (DRAC)
- Copied to a physical DVD and run in the appliance DVD drive

After hardware setup, connect directly to the Email RiskVision appliance through the serial port or the monitor and keyboard ports.

V10000 G3 appliance:

V5000 G2R2 appliance:


An activation script, called **firstboot**, runs when you start the appliance. The firstboot script prompts you to:

- Supply settings for the network interface labeled C.
- Enter a few other general items, such as hostname and password.

You are given the opportunity to review and change these settings before you exit the **firstboot** script. After you approve the settings, initial appliance configuration occurs.

Later, if you want to change settings, you can do so through the Appliance manager, a graphical management interface accessed through a web browser.

Gather the following information before running the **firstboot** script.

| | |
|---|---|
| Security mode | **Email** |
| Which subscription? | **RiskVision** |
| Hostname (example: appliance.domain.com)<br><br>1 - 60 characters long.<br>The first character must be a letter.<br>Allowed: letters, numbers, dashes, or periods.<br>The name cannot end with a period. | |
| IPv4 address for network interface C | |
| Subnet mask for network interface C | |
| Default gateway for network interface C (IP address) | |
| Primary DNS server for network interface C (IP address) | |
| Secondary DNS server for network interface C (IP address) *Optional* | |
| Tertiary DNS server for network interface C (IP address) *Optional* | |
| Password (8 to 15 characters, at least 1 letter and 1 number)<br>This password is for the **admin** account used to access the Appliance manager. | |
| Send usage statistics? | Usage statistics from appliance modules can optionally be sent to Websense to help improve the accuracy of email traffic analysis. |

Run the initial command-line configuration script (**firstboot**) as follows.

1. Access the appliance through a USB keyboard and monitor, or a serial port connection.

   **Note**

   For serial port activation, use:

   - 9600 baud rate
   - 8 data bits
   - no parity

2. Accept the subscription agreement when prompted.
3. When asked if you want to begin, enter **yes** to launch the **firstboot** activation script.

To rerun the script manually, enter the following command:

```
firstboot
```

4. Follow the on-screen instructions to provide the information collected in the table above.

After the script finishes running, continue with the next step.

# Step 3: Configure basic appliance settings

The Email RiskVision appliance settings are configured in the Appliance manager, a web-based interface. Use the Appliance manager to view system status, configure network and communication settings, and perform general appliance administration.

To configure the basic settings needed to get started with Email RiskVision:

1. Open a supported browser (Internet Explorer 8, 9, and 11 and Microsoft Internet Explorer 10 in Desktop mode, Mozilla Firefox 5 and later, or Google Chrome 13 and later), and enter the following URL in the address bar:

   ```
   https://<IP-address-of-C-interface>:9447/appmng
   ```

2. Log on with the user name **admin** and the password set during initial appliance configuration (**firstboot**).
3. Use the left navigation pane to navigate to the **Configuration** > **System** page.
4. Under **Time and Date**, use the **Time zone** list to select the time zone to be used on this system.

   GMT (Greenwich Mean Time), the default, is also known as UTC (Universal Time, Coordinated). Other time zones are calculated by adding or subtracting from GMT. GMT is sometimes chosen to provide a common time stamp for geographically distributed systems.
5. Use the **Time and date** radio buttons to indicate how you want to set the date.

   Time is set and displayed using 24-hour notation. Make sure that the time and date are synchronized on the Email RiskVision appliance and any machine hosting Email RiskVision components.

   - To synchronize with an Internet Network Time Protocol (NTP) server (www.ntp.org.), select the **Automatically synchronize** option and enter the address of a primary NTP server. The secondary and tertiary fields are optional.

**Important**

If you synchronize the system clock with an NTP server, NTP protocol packets and their response packets must be allowed on any firewall or NAT device between the appliance and the NTP server. Ensure that you have outbound connectivity to the NTP servers. Add a firewall rule that allows outbound traffic to UDP port 123 for the NTP server.

- To set the time yourself, select the **Manually set** option and change the value in the Date and Time fields. Use the format indicated below the entry field.

6. Create or edit a unique appliance **Description** to help you identify and manage the system.

   The description is displayed in the appliance list in the TRITON Unified Security Center when the appliance is added there.

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

> **Note**
>
> In the **Configuration > Network Interfaces** page, the C interface information you entered during firstboot appears by default. Information for network interfaces E1 and E2 (P1 and P2 on a V5000 appliance) do not appear on this page.

When you are finished deploying your RiskVision appliance, continue with the next topic: *Create a Management Server*, page 9.

# 3 Create a Management Server



After performing initial appliance configuration, install management and reporting components on a Windows Server 2008 R2 or Windows Server 2012 machine, as described in the sections that follow.



Before you begin:

- Make sure that Microsoft SQL Server 2008, 2008 R2, or 2012 is installed and running in your network, and that the network is configured to allow the Email RiskVision management server machine to connect to the SQL Server machine.
- Make sure that Windows Server 2008 R2 or Windows Server 2012 machine that will become the management server has at least 4 CPU cores (2.5 GHz), 8 GB RAM, and 146 GB of disk space available.
- Make sure all Microsoft updates have been applied on the management server machine. There should be no pending updates, especially any requiring a restart of the system.
- The Microsoft .NET Framework is required to run the Windows installer:
  - On Windows Server 2008 R2 machines, .NET Framework 2.0 is required.
  - On Windows Server 2012, .NET Framework 2.0 and 3.5 are both required.

  You can install the required version or versions of .NET Framework via the Server Manager, or download it from www.microsoft.com.
- Disable any antivirus software on the machine prior to installing Email RiskVision components. Be sure to re-enable the antivirus software after installation.
- Synchronize the clocks on the Email RiskVision appliance and any machine where Email RiskVision components are installed. It is a good practice to point the machines to the same Network Time Protocol server.

# Step 1: Download the installer and start installation

1. Download the **TRITON RiskVision Installer** from here.
   - The file name is **Websense_TRITON_ERV78xSetup.exe**.
   - When extracted, the installation files occupy about 2 GB of disk space.
2. Double-click the installer executable to launch the **Websense TRITON Setup** program.

   A progress dialog box is displayed as files are extracted. This may take a few minutes.
3. On the **Welcome** screen, click **Start**.
4. On the **Subscription Agreement** screen, select **I accept this agreement** and then click **Next**.
5. On the **Installation Type** screen, select **TRITON Unified Security Center**, then mark the **Email Security** check box. When you select Email Security, the **Data Security** check box is marked automatically.

   **Note**

   You must use a dedicated TRITON® console machine to manage Email RiskVision. Email RiskVision cannot share a TRITON console with the Websense® Web Security module.

   When you are finished, click **Next**.
6. On the **Summary** screen, click **Next** to continue the installation.

   The TRITON Infrastructure Setup program launches. Continue with the next section.

# Step 2: Install TRITON Infrastructure

TRITON Infrastructure is the platform on which Websense TRITON management components are built. When the infrastructure components have been installed, the Data Security installer launches automatically to install the Data Security management components. The Email Security installer launches after Data Security installation is complete.

1. On the TRITON Infrastructure Setup **Welcome** screen, click **Next**.

2. On the **Installation Directory** screen, specify the location where you want TRITON Infrastructure to be installed and then click **Next**.

   > **Important**
   > The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

3. On the **SQL Server** screen, select **Use existing SQL Server on another machine** to specify the location and connection credentials for a database server located elsewhere in the network.

   Enter the **Hostname or IP address** of the SQL Server machine, including the instance name, if any.

   - If you are using a named instance, the instance must already exist.
   - If you are using SQL Server clustering, enter the virtual IP address of the cluster.

     Also provide the **Port** used to connect to the database (1433, by default).

4. Select the **Authentication** method to use for database connections: **SQL Server Authentication** (to use a SQL Server account) or **Windows Authentication** (to use a Windows trusted connection).

   a. Provide the **User Name** or **Account** and **Password** for a database account with system administrator rights in SQL Server, then click **Next**.

   b. If your SQL Server installation is already configured to use SSL encryption to secure communication with the database, mark **Encrypt connection**.

   When you are finished, click **Next** to verify the connection to the database.

   - If the connection test is successful, the next installer screen appears.
   - If the test is unsuccessful, the following message appears:

     ```
     Unable to connect to SQL
     Make sure the SQL Server you specified is currently
     running. If it is running, verify the access
     credentials you supplied.
     ```

   Click **OK** to dismiss the message, verify the information you entered, and click **Next** to try again.

5. On the **Server & Credentials** screen, select the IP address of this machine and specify network credentials to be used by TRITON Unified Security Center.

   - Select an **IP address** for this machine. If this machine has a single network interface card (NIC), only one address is listed.
   - Specify the **Server or domain** of the user account that you want to use to run the TRITON Infrastructure and TRITON Unified Security Center services. The server/host name cannot exceed 15 characters.
   - Specify the **User name** of the account that you want to use to run the TRITON Unified Security Center services.
   - Enter the **Password** for the specified account.

6. On the **Administrator Account** screen, enter an email address and password for the default TRITON console administration account: **admin**. When you are finished, click **Next**.
7. Entering information on the **Email Settings** screen is not required for Email RiskVision. Unmark the **Configure email settings** check box and then click **Next**.
8. On the **Pre-Installation Summary** screen, verify the information and then click **Next** to begin the installation.
9. Next, the **Installation** screen appears. Wait until all files have been installed.

   If the following message appears, check whether port 9443 is already in use on this machine:

   ```
   Error 1920. Server 'Websense TRITON Central Access'
   (EIPManagerProxy) failed to start. Verify that you have
   sufficient privileges to start system services.
   ```

   If port 9443 is in use, release it and then click **Retry** to continue installation.
10. On the **Installation Complete** screen, click **Finish**.

The TRITON Infrastructure Setup program closes and the Data Security component installer launches. Continue with the next section.

## Step 3: Install Data Security components

All Email RiskVision subscriptions include email DLP, used for data loss monitoring. Data loss monitoring is performed by Data Security components installed on the management server, and configured in the Data Security module of the TRITON console.

To install the Data Security management components:

1. When the Data Security component installer launches, and the **Welcome** screen is displayed, click **Next**.
2. On the **Select Components** screen, all required components are selected by default and the selections cannot be changed. Click **Next**.
3. If prompted, click **OK** to accept that services such as ASP.NET and SMTP will be enabled.
4. On the **Fingerprinting Database** screen, accept the default location or click **Browse** to specify a different location (local path only).
5. Use the **Temporary Folder Location** screen to provide the name of a folder to use for temporary files created during archive processing and system backup and restore. Also indicate:
   - Whether to **Enable incident archiving and system backup** to archive old or aging incidents and perform system backup or restore.
   - Use the **From SQL Server** field to enter the UNC path that the SQL Server should use to access the temporary folder. Make sure the account used to run SQL Server has write access to this folder.

- Use the **From TRITON Management Server** field to enter the UNC path the management server should use to access the temporary folder. Enter a user name and password for a user who is authorized to access this location.

6. If the **Local Administrator** screen appears, provide credentials for a local administrator account for email DLP components to use, then click **Next**.
7. In the **Installation Confirmation** screen, click **Install** to begin installing Data Security components.
8. If the following message appears, click **Yes** to continue the installation:

   ```
   Data Security needs port 80 free.
   In order to proceed with this installation, DSS will free
   up this port.
   Click Yes to proceed OR click No to preserve your
   settings.
   ```

   A similar message for port 443 may appear. Click **Yes** to continue.
9. The **Installation Progress** screen appears. Wait for the installation to complete.

   When the **Installation Complete** screen appears, click **Finish** to close the Data Security installer.

The Data Security component installer closes, and the Email Security component installer launches. Continue with the next section.

## Step 4: Install Email Security components

To install the Email Security management components:

1. When the Email Security component installer launches, and the **Introduction** screen appears, click **Next**.
2. On the **Select Components** screen, choose whether to install Email Security Log Server on this machine and then click **Next**.

   Email Security manager is installed automatically.

   To install Email Security Log Server, SQL Server must already be installed and running in your network.
3. On the **Email Security Database** screen, specify the IP address or IP address and instance name (format: IP address\instance) for the Email Security database.

   Designate the login type for the database, either Windows authentication or SQL authentication.
4. On the **Email Security Database File Location** screen, specify where Email Security database files should be located and then click **Next**.
5. On the **Email Security Gateway** screen, specify the Email Security Gateway appliance to be managed by this installation of the TRITON Unified Security Center and then click **Next**.

   Enter the IP address of the C interface of the Email RiskVision appliance. You must specify an IP address only. Do not use a fully-qualified domain name (FQDN).

When you click **Next**, communication with the specified appliance will be verified.

6. On the **Installation Folder** screen, specify the location to which you want to install Email Security components and then click **Next**.
7. On the **Pre-Installation Summary** screen, review your settings for the components to be installed. If they are correct, click **Install**.

   Click **Back** to return to any screen on which you want to modify settings.
8. The **Installing Websense Email Security** screen appears as components are being installed.
9. Wait until the **Installation Complete** screen appears, and then click **Done**.

You have completed installation of the TRITON management server. Continue with the next section.

## Step 5: Change update service configuration

Before you enter your Email RiskVision subscription key in the Email Security manager, you need to modify the appliance update service for RiskVision operation.

Use the following steps to modify the **sig_update.conf** file:

1. Log on to the appliance as user root.
2. Execute the following command:

   ```
   ssh esg
   ```
3. Locate the **sig_update.conf** file in the **/usr/local/etc/** directory.
4. Change the network interface from:

   ```
   nic = eth0
   ```

   to:

   ```
   nic = internal
   ```
5. Restart the update service using the following command:

   ```
   svc -du /service/update_daemon/
   ```

You are now ready to enter a subscription key and activate Websense Email RiskVision. Continue with the next section

## Step 6: Enter a subscription key

To log on to the TRITON console and enter your Email RiskVision subscription key:

1. Open a preferred browser (Mozilla Firefox 5 and later or Google Chrome 13 and later), and enter the following URL in the address bar:

   ```
   https://<IP-address-of-management server>:9443/triton/
   ```

   Internet Explorer 8, 9, 10 (not Compatibility View), and 11 are also supported.

2. Enter the user name **admin** and the password set during installation, then click **Log On**. You are logged on to the TRITON console.
3. Click the Email Security tab in the TRITON console module tray to display a pop-up box that allows you to enter your Email Security subscription key.
4. Enter **TSTB24RCUKGJ75BA** in the **Subscription Key** entry field.
5. Log off the TRITON console and continue with the next section of this document.

The next time you log on to the TRITON console, you are connected to the Email RiskVision manager, instead of the Email Security manager. A new **RiskVision** tab appears in the **Main > Status > Dashboard** screen.

**Note**

When you log on to the Email RiskVision manager, Data Security is automatically registered using the C network interface. You cannot change the settings in the **Settings > General > Data Security** page.

Continue with the next section to configure the Email RiskVision manager.

# 4 Configure Email RiskVision



After setting up the Websense® Email RiskVision appliance and creating a TRITON® management server, you must provide some additional settings to enable email traffic monitoring. You may also want to refine other Email RiskVision monitoring functions using some additional RiskVision manager settings.

Post-installation configuration involves the following procedures:



See the Email Security Manager Help (accessed from the Help menu in the Email RiskVision manager) for more information about enabled Email RiskVision manager components. Some functions described in the Email Security Manager Help are disabled in RiskVision and not available to Email RiskVision users.

## Step 1: Define protected domains

You must specify all the domains that the organization owns and needs Email Security Gateway to protect. Use the Protected Domain group to define the domains that Email RiskVision monitors.

To add domains to the Protected Domain group:

1. Click the **Protected Domain** link on the **Settings > Users > Domain Groups** page to open the Edit Domain Group page.
2. You may define your protected domain group in one of two ways:
   - To import a predefined set of protected domains:
     a. Click **Browse** next to the **Domain address file** field.

b. Navigate to the desired text file.

c. Click **Open**.

The file format should be 1 domain address per line, and its maximum size is 10 MB. If a file contains any invalid entries, Email RiskVision accepts only the valid entries. Invalid entries are rejected.

- To specify individual domains:

a. Enter an individual domain address in the **Domain Address** field.

b. Click the arrow button to add the information to the **Added Domains** box on the right.

Use wildcards to include subdomain entries (e.g., *.domain.com).

3. Click **OK**.

## Step 2: Configure Log Server

The Email RiskVision Log Server receives records of system event and email filtering activity, which the Log Database uses to generate reports. You must enter Log Server settings for proper Email RiskVision operation.

If you installed Log Server during TRITON manager installation, the information you entered there appears in the Log Server page by default.

To configure the Log Server:

1. On the **Settings** > **Reporting** > **Log Server** page, enter the Log Server IP address in the **Log Server** entry field
2. Enter the port number in the **Port** entry field.
3. Click **OK**.

## Configure RiskVision dashboard charts (optional)

When you log on to the TRITON console after having completed the appliance setup and management server installation, you access the Email RiskVision manager by clicking the Email Security tab. A new **RiskVision** tab is displayed with a set of default charts:

- 24-Hour Business Value
- 30-Day Blocked Message Value
- Connections Summary
- Inbound Volume by Message Type.

You can modify the RiskVision dashboard tab by adding or removing charts, or by customizing existing dashboard charts to suit your needs.

To add new charts to the RiskVision dashboard:

1. Click **Add Charts** at the top of the screen to open the Add Charts screen.
2. Ensure that **RiskVision** is selected in the **Add elements to tab** drop-down list.
3. Select a chart to add in the **Dashboard Elements** list. Elements currently displayed on the selected tab are marked by a blue circle icon.
4. The selected chart appears in a **Preview** pane, where you can make changes to the chart Name and, if applicable, Chart type, Time period, and Top value (for example, top 1-5 categories, or top 16-20 users).

   You can add multiple copies of the same element to a tab (for example, each might show a different time period).
5. Click **Add** when you are finished.

To edit an existing chart:

1. Click the **Options** icon in the chart title bar and then select **Edit**.
2. Perform the following edit operations:
   - Change:
     - Chart name
     - Chart type
     - Time period
     - Top numerical designation
   - Restore default chart settings
   - Copy chart

## Create an email DLP policy (optional)

Default email policies (inbound, outbound, and internal) apply to all senders and recipients and cannot be modified in Email RiskVision. However, you can configure an email DLP policy if desired, to detect data loss via email.

Use the Data Security manager to configure an email DLP policy:

1. Select the **Data Security** module of the TRITON console.
2. On the Main tab, navigate to the **Policy Management** > **DLP Policies** > **Email DLP Policy** page.
3. On the Attributes tab for inbound or outbound email, select and enable the email attributes to monitor, such as:
   - Regulatory and compliance attributes, like protected health information
   - Custom patterns and phrases appropriate to your organization or industry
   - Email attachment name or type
   - Questionable images

   When the settings you configure are matched, the policy is triggered.
4. Select the **Policy Owners** tab, then identify an administrator as the owner for the policy.

5. Click **OK**, then click **Deploy**.

When you click **Deploy**, the Data Security components activate the policies that you configured.

Ensure that Data Security policies are enabled in the Email RiskVision manager (**Main > Policy Management > Policies**).

See the Data Security Manager Help (accessed from the Help menu in the Data Security manager) for more information about email DLP policies.

## Configure a user directory (optional)

You can create a user directory if you want to enable user-based reporting on email DLP policy application.

To add a user directory to Email RiskVision:

1. Click Add in the **Settings > Users > User Directories** page.
2. Enter a name in the **User directory name** entry field.

   Note that a new user directory has a status of **Not referenced**, because it is not yet being used by an email policy.
3. Select a user directory type from the drop-down list. Supported user directories include:
   - Microsoft Active Directory
   - IBM LDAP Server Directory
   - Generic LDAP Server Directory
   - Recipient List
   - ESMTP Server Directory
4. Create the selected directory type by specifying its associated properties.

   See Email Security Manager Help (accessed from the Help menu in the Email RiskVision manager) for user directory details.

## Establish global Always Block/Always Permit lists (optional)

Use lists of IP and email addresses that are either always blocked or always permitted to refine your RiskVision monitoring. Maintain global Always Block and Always Permit lists in the **Main > Policy Management > Always Block/Permit** page.

You can add an IP or email address directly into the Always Block or Always Permit list or you can add a predefined IP or email address list.

To add IP addresses to a list:

1. Click the **Always Block** or **Always Permit** tab, depending on which list you want to modify.
2. Enter IP addresses in one of two ways:
   - In the IP Address Block List section of the page, add a predefined IP address list by clicking **Browse** and navigating to the desired text file.

     The file format should be 1 IP address per line, and its maximum size is 10 MB.
   - Enter an individual IP/subnet address in the **IP/Subnet address** field, and then click the right arrow button to add the individual entry to the IP Address List on the right.
3. Click **OK**.

To add an email address to a list:

1. Click the **Always Block** or **Always Permit** tab, depending on which list you want to modify.
2. Enter email addresses in one of two ways:
   - In the Email Address Block List section, add a predefined email address list by clicking **Browse** and navigating to the desired text file.

     The file format should be 1 email address per line, and its maximum size is 10 MB.
   - Enter an individual email address in the **Email address** field. Click the right arrow button to add the individual entry to the Email Address List on the right.
3. Click **OK**.

# Troubleshooting tips

This section includes a few suggestions for troubleshooting issues in Email RiskVision.

You can use the following general steps when you determine that an appliance service is down to determine the cause of the problem:

1. Identify the service that is down.
2. Collect its log file.
3. Restart the affected service:

   ```
   esg_rv.sh restart
   ```

To enable debugging for the traffic collection server (log file: **/var/log/tserver.log)**:

1. Locate the configuration file **/usr/local/etc/tserver_log.conf**.
2. Enable the debug log by changing the following configuration file item from:

   ```
   log_level=log_msg_err
   ```

   to:

```
log_level=log_msg_all
```

To enable debugging for the resend service (log file: **/var/log/sender.log**):

1. Locate the configuration file **/usr/local/sbin/sender.conf**.
2. Enable the debug log by changing the following configuration file item from:

   ```
   #default log level
   root_level=error
   ```

   to:

   ```
   root_level=debug
   ```
3. Change the following item from:

   ```
   #debug level of individual modules
   smtpdialog_level=warn
   ```

   to:

   ```
   smtpdialog_level=debug
   ```

You must restart any service you modify in order to apply your changes.