VERSION 1.0
OCTOBER 2024
702P09325

Trellix® Embedded Control and Trellix® ePO

Configuration Guide

xerox™

Contents

Trellix Embedded Control....5

Trellix Embedded Control Overview....6
Setting the Security Level....7
Setting the Alert Options....8

Trellix ePO Security Event Alerts Configuration....9

Process Overview....10
Configuring for Security Event Alerts in Trellix ePO....10
Downloading and Installing the Xerox Extensions for Trellix ePO....11
Providing License Keys in Trellix ePO....12
Changing the Agent Wake-Up Communication Port in Trellix ePO....13
Changing the Maximum File Upload Size Limit on the Trellix ePO Server....14
Creating and Assigning a Policy in Trellix ePO....15
Configuring the Automated Response in Trellix ePO....16
Configuring Trellix ePolicy Orchestrator Server Settings....17
Designating Printers as Super Nodes....18
Adding DNS Entries to One or More Existing Domains....18
Adding DNS Entries to a Single New Domain....18
Ensuring that the Device is Managed in Trellix....19

Configure the Trellix ePO Proxy....21

Configure your Trellix ePO Proxy....22

Remove and Reinstall Trellix ePO Extensions....23

Removing and Reinstalling Trellix ePO Extensions....24

Trellix Embedded Control

This chapter contains:

Trellix Embedded Control Overview.....6
Setting the Security Level 7
Setting the Alert Options.....8

Note: Trellix® formerly known as McAfee®.

Trellix Embedded Control Overview

When Trellix® ePolicy Orchestrator (ePO) is installed on your server, use this guide to integrate Xerox Multifunction Printers that have the Trellix Embedded Control security feature.

Trellix Embedded Control consists of two security features:

- Enhanced Security maintains the integrity of printer software by monitoring system files and alerting you if an unauthorized change is made to a system file.
- Integrity Control is a software option that combines Enhanced Security features with the ability to monitor and prevent unauthorized executable files from running. To enable this option, you provide a feature installation key on the Feature Installation page. To obtain a Feature Installation Key, contact your Xerox representative.

You can configure the printer to send email alerts when a security event occurs. Several alert methods are available.

Email alerts can be sent directly to you or to a centralized management application, such as:

- Trellix® ePolicy Orchestrator (ePO)
- Xerox® CentreWare® Web
- Xerox® Device Manager

For details about Trellix ePO and Trellix Embedded Control, visit www.trellix.com.

Setting the Security Level

Unless you have acquired Trellix Integrity Control, Xerox recommends that you keep the security level set to the default setting, Enhanced Security.

Trellix Embedded Control has two security levels:

- Enhanced Security
- Integrity Control

Note: Only set the security level if necessary. The printer comes standard with an Enhanced Security level, which is adequate in many cases.

1. In the Embedded Web Server of the multifunction printer, click **Properties > Security**.
2. Click **Trellix Embedded Control**.
3. To enable Trellix Embedded Control features, and configure Alert Feedback options, click **Edit**.
4. To set the Security Level, under Security Level, select **Enhanced Security** or **Integrity Control**.
5. If you select Enhanced Security as the security level, click **Save**.
6. If you select Integrity Control as the security level, click **Next**, enter the software Feature Installation Key, then click **Apply**.

Note: When you change the security level setting, the printer restarts. The process takes several minutes.

Setting the Alert Options

You can configure the printer to alert you when a security event occurs.

To set the alert options:

1. In the Embedded Web Server of the multifunction printer, click **Properties > Security**.
2. Click **Trellix Embedded Control**.
3. To configure Alert Feedback options, click **Edit**.
4. To configure the printer to send email alerts:
    a. Under Locally on the Device, click **Email Alerts**, then **Save**.
    b. Next to Email Alerts, under Action, click **Edit**.
    c. Under Recipient Group Addresses, enter valid email addresses for each applicable group 1, 2, or 3.
    d. For each group with email addresses, select **Enable Group**.
    e. Under Recipient Group Preferences, for Trellix Embedded Control, select each group that you want to receive alerts: **Group 1**, **Group 2**, and **Group 3**.
    f. Click **Apply**.
    g. At the prompt, click **OK**.
5. Configure your alert feedback method.
    - To configure the printer to send alerts to Trellix ePolicy Orchestrator Server, under Trellix Remote Solutions, select **Trellix's ePolicy Orchestrator Server**.
    - If you use Xerox® CentreWare® Web to manage your printers, configure security alerts in Xerox® CentreWare® Web.
    - If Xerox manages your printers, use Xerox® Device Manager to send security alerts from registered printers.

Note: When Trellix Embedded Control features are enabled, the printer also records security events in the audit log.

Trellix ePO Security Event Alerts Configuration

This chapter contains:

Process Overview....10
Downloading and Installing the Xerox Extensions for Trellix ePO....11
Providing License Keys in Trellix ePO....12
Changing the Agent Wake-Up Communication Port in Trellix ePO....13
Changing the Maximum File Upload Size Limit on the Trellix ePO Server....14
Creating and Assigning a Policy in Trellix ePO....15
Configuring the Automated Response in Trellix ePO....16
Configuring Trellix ePolicy Orchestrator Server Settings....17
Designating Printers as Super Nodes....18
Ensuring that the Device is Managed in Trellix....19

Process Overview

This overview provides the procedures, in the specific order required, to configure for security alerts in Trellix ePO.

CONFIGURING FOR SECURITY EVENT ALERTS IN TRELLIX EPO

To configure for security alerts in Trellix ePO, complete each procedure in the order provided:

1. Purchase and install the Trellix ePO server software. For details, contact a Trellix representative or visit www.trellix.com.
2. The Xerox® extensions for Trellix ePO require the Microsoft .NET Framework. Download and install the Microsoft .NET Framework, version 4.0 or later. For details, visit www.microsoft.com.

   Note: The .NET version required depends on the SQL server used in your ePO server.

   Note: If you do not complete this procedure, it results in an Error-2 message when you open the Xerox MFP extension.
3. Download and install the Xerox® extensions for Trellix ePO. For details, refer to Downloading and Installing the Xerox Extensions for Trellix ePO.
4. Provide license keys in Trellix ePO. For details, refer to Providing License Keys in Trellix ePO.
5. To ensure that the printer can communicate with your Trellix ePO server, change the default agent wake-up communication port in Trellix ePO. For details, refer to Changing the Agent Wake-Up Communication Port in Trellix ePO.
6. To allow printer software updates, change the maximum file size upload limit on the Trellix ePO server. The maximum file size upload limit must be larger than the Xerox® printer software update file size. For details, refer to Changing the Maximum File Upload Size Limit on the Trellix ePO Server.
7. Ensure that security event alerts are sent when they occur rather than at regular intervals. Create a security policy, then associate the policy with your Xerox® printers in Trellix ePO. For details, refer to Creating and Assigning a Policy in Trellix ePO.
8. To ensure that you receive emails automatically in the event of a security alert, configure the Automated Response in Trellix ePO. For details, refer to Configuring the Automated Response in Trellix ePO.
9. In the Embedded Web Server of the multifunction printer, on the Trellix Embedded Control page, provide details about your Trellix ePO server. For details, refer to Configuring Trellix ePolicy Orchestrator Server Settings.
10. Designate printers as Super Nodes on your network. For details, refer to Designating Printers as Super Nodes.
11. Ensure that the device is managed within Trellix ePO. For details, refer to Ensuring that the Device is Managed in Trellix ePO.
12. Configure your Trellix ePO Proxy. For details, refer to Configuring Your Trellix ePO Proxy.

Downloading and Installing the Xerox Extensions for Trellix ePO

1. Locate then download the Xerox® extensions. The extensions are contained in a .zip file.
   a. To go to the Xerox® Support website, open a Web browser, then type www.xerox.com/office/support.
   b. To navigate to the support page for your specific device, in the Search field, type your device model, then press **Enter**.
   c. From the list of results that appear for your device, click **Drivers and Downloads**.
   d. From the Operating System drop-down menu, select the operating system for your server.

   Note: Ensure that you select the operating system for your server, not the operating system of your computer.

   e. Under Utilities and Applications, click **Xerox Extension for Trellix ePolicy Orchestrator (ePO)**.
   f. Read the End User License Agreement, then click **Accept**.
2. Open the .zip file, then move the two compressed extension files to a temporary folder. Do not open the .zip extension files.
3. In Trellix ePO, install the .zip extension files.
   a. Access the Trellix ePO web interface at https://servername.domain:8443.
   b. Navigate to **Menu > Software > Extensions**.
   c. In the upper left corner, click **Install Extension**.
   d. Browse to the temporary folder, select a .zip extension file, then open it.
   e. Click **OK**.

   Note: If a message appears during installation indicating that the Solidcore extension is installed already, remove the existing Solidcore extension. After the installation completes, reinstall the software provided by Xerox and update the Solidcore extension. For details, refer to Removing and Reinstalling Trellix ePO Extensions.

   f. Install the other .zip extension file.
4. To continue configuring your security alerts, proceed to Providing License Keys in Trellix ePO.

Providing License Keys in Trellix ePO

1. Access the Trellix ePO web interface at https://servername.domain:8443.
2. Navigate to **Menu > Configuration > Server Settings**.
3. Click **Solidcore**.
4. In the bottom right corner, click **Edit**.
5. Enter the following license keys:
   - Change Control: `XL17-ZCWK-K7E2-9PZY-OT6V`
   - Application Control: `ZM7H-FX52-3SFL-TR5Z-MAG3`
   - Integrity Control: `K5DA-AG51-5AR3-OB99-WTDG`
6. Click **Save**.
7. To continue configuring your security alerts, proceed to Changing the Agent Wake-Up Communication Port in Trellix ePO.

Changing the Agent Wake-Up Communication Port in Trellix ePO

1. Access the Trellix ePO web interface at https://servername.domain:8443.
2. Navigate to **Menu > Configuration > Server Settings**.
3. Click **Ports**.
4. In the bottom right corner, click **Edit**.
5. Next to Agent wake-up communication port, type 8083, or any unused port other than the default, 8081.
6. Click **Save**.
7. To continue configuring your security alerts, proceed to Changing the Maximum File Upload Size Limit on the Trellix ePO Server.

Changing the Maximum File Upload Size Limit on the Trellix ePO Server

1. Access the Trellix ePO server, then navigate to `C:\Program Files (x86)\Trellix\ePolicy Orchestrator\Server\conf\orion`.
2. Using a text editor application, open the file **orion.properties**.
3. Change the text `orion.upload.max.size=90000000` to `orion.upload.max.size=500000000`.
4. Save the text file.
5. Restart the ePO server.
6. To continue configuring your security alerts, proceed to Creating and Assigning a Policy in Trellix ePO.

Creating and Assigning a Policy in Trellix ePO

1. Access the Trellix ePO web interface at https://servername.domain:8443.
2. Navigate to **Menu > Policy > Policy Catalog**.
3. Next to Product, select **Trellix Agent**.
4. Next toCategory, select **General**.
5. To create the policy, next to My Default, under the Actions column, click **Duplicate**.
   a. Next to Name, type `MFP Agent`.
   b. Next to Notes, type `For Xerox endpoints`.
   c. Click **OK**.
6. To edit the policy, under Name, click **MFP Agent**.
7. Click the **Events** tab.
   a. If not previously selected, select **Enable priority event forwarding**.
   b. Next to Forward events with a priority equal or greater than, select **Informational**.
   c. Next to Interval between uploads, type `1`.
   d. Next to Maximum number of events per upload, type `20`.
   e. Click **Save**.
8. Navigate to **Menu > Policy > Policy Assignment Rules**.
9. Click **New Assignment Rule**.
   a. Next to Name, type `MFP Agent`.
   b. Click **Next**.
   c. Click **Add Policy**.
   d. Under Product, select **Trellix Agent**, under Category, select **General**, then under Policy select your new policy, **MFP Agent**.
   e. Click **Next**.
   f. Under Available Properties, click **Tag**.
   g. Under Comparison, click **Has tag**.
   h. Under Value, select **Xerox MFP**.
   i. Click **OK**.
   j. Click **Next**.
10. Click **Save**.
11. To continue configuring your security alerts, proceed to Configuring the Automated Response in Trellix ePO.

Configuring the Automated Response in Trellix ePO

To provide security administrators the ability to receive automatic email notifications, install the Automated Response feature. These notifications are sent whenever Trellix Embedded Control detects a security event on a Xerox device. When installed, this response system applies to all devices currently provisioned by the ePO server. The events that trigger a Xerox MFP Alerts Automated Response are File Read Denied, File Write Denied, or Execution Denied.

By default, the Automated Response is disabled. To enable it, a security administrator must include a valid email address.

To add an email address and enable the response:

1. In Trellix ePO, select **Menu > Automation > Automatic Responses**.
2. Click **New Response**.
    a. Next to Name, type `Xerox MFP Alerts`.
    b. Next to Description, type `Threat Events`.
    c. For Event Group, select **Solidcore Events**.
    d. For Event Type, select **Client Events**.
    e. For Status, select **Enabled**.
    f. Click **Next**.
3. Click **Event**.
    a. Under Value, select **File Created**, **File Deleted**, **File Modified**, **Execution Denied**, and **File Read Denied**, then click the plus icon (**+**) to create a row.
    b. Under Recipients, type email addresses.
    c. Click **Next**, then click **Save**.
4. Under Aggregation, for Throttling, select **Trigger this response if multiple events occur every 1 hour**.
5. Under the Actions tab, select **Send Email**.
6. Click **Next**, then click **Save**.
7. To continue configuring your security alerts, proceed to Configuring Trellix ePolicy Orchestrator Server Settings.

Configuring Trellix ePolicy Orchestrator Server Settings

1. In the Embedded Web Server of the multifunction printer, click **Properties > Security**.
2. Click **Trellix Embedded Control**.
3. On the Trellix Embedded Control page, next to Device Security Levels, click **Edit**.
4. Select **Trellix ePolicy Orchestrator Server**, then click **Save**.
5. Select **Trellix ePolicy Orchestrator Server**, then click **Edit**.
6. Select an address type. Type the appropriately formatted address or host name of your server and change the default port number as needed.
7. Under User Name, type the name that the printer uses to access the Trellix ePO server application.
8. Type the password, then type the password again to verify.
9. Click **Save**.
10. To continue configuring your security alerts, proceed to Designating Printers as Super Nodes.

Designating Printers as Super Nodes

The Xerox® extension for Trellix ePO uses up to three Xerox® printers as supernodes to communicate with the other Xerox® printers that it monitors. Xerox recommends that you designate more than one Xerox® printer as a supernode. If one supernode is not functioning or is offline, Trellix ePO can use the other supernodes to communicate with other printers. You designate printers as supernodes by adding specific entries to your DNS server.

Note:

- Your Xerox® printers and your Trellix ePO server must use the same DNS server.
- Complete the following procedures on the DNS server, not the Trellix ePO server.

To add a DNS entry, do one of the following:

ADDING DNS ENTRIES TO ONE OR MORE EXISTING DOMAINS

If you have a small number of domains in your network, use this method to add DNS entries to each domain.

1. On your DNS server, find the domain of each printer that you want to designate as a supernode.
2. For each domain, add entries for all supernodes, then name them:
   - XeroxDiscoverySuperNode1
   - XeroxDiscoverySuperNode2
   - XeroxDiscoverySuperNode3

   Note: The entries for all supernodes are not case sensitive.
3. If your network uses more than one DNS server, repeat the previous step for all other DNS servers.
4. To continue configuring your security alerts, proceed to Ensuring that the Device is Managed in Trellix ePO.

ADDING DNS ENTRIES TO A SINGLE NEW DOMAIN

If you have a large number of domains in your network, use this method to add DNS entries to a single domain.

1. On your DNS server, create a domain named Xerox.local. The Xerox extension for Trellix ePO looks for a domain with this name.
2. For Xerox.local, add entries for each supernode, then name them:
   - XeroxDiscoverySuperNode1
   - XeroxDiscoverySuperNode2
   - XeroxDiscoverySuperNode3
3. To continue configuring your security alerts, proceed to Ensuring that the Device is Managed in Trellix ePO.

Ensuring that the Device is Managed in Trellix

1. In Trellix ePO, click **System Tree**.
2. Click **Lost & Found**.
3. Under Preset, select **This Group and all Subgroups**.
4. Verify that your Xerox device appears.
5. Verify that the Xerox device appears as Managed under the Managed State.
6. In the Trellix ePO window, under Menu, select **Third Party**, then click the **Xerox MFP** extension.
7. For convenient Trellix ePO access, drag and drop the **Xerox MFP** extension icon to the top.
8. To continue configuring your security alerts, proceed to Configuring Your Trellix ePO Proxy.

Configure the Trellix ePO Proxy

This chapter contains:

Configure your Trellix ePO Proxy 22

Configure your Trellix ePO Proxy

If a proxy is used, it must be configured with Trellix ePO.

1. In Trellix ePO, under Menu, select **Configuration**.
2. Select **Server Settings**.
3. Select **Proxy Settings**.
4. In the bottom right corner, click **Edit**.
5. Under Type, select **Configure the proxy settings manually**.
6. Under Proxy server settings, manually configure to match the unique settings for your site.
7. Click **Save**.
8. Restart the ePO server.

Note: If you do not complete this procedure, it results in an Error-2 message when you open the Xerox MFP extension.

Remove and Reinstall Trellix ePO Extensions

This chapter contains:

Removing and Reinstalling Trellix ePO Extensions.....24

Removing and Reinstalling Trellix ePO Extensions

If a message appears during installation indicating that the Solidcore extension is installed already, remove the existing Solidcore extension. After the installation completes, reinstall the software provided by Xerox and update the Solidcore extension. Performing these two steps establishes the necessary foundation to update the software to a more recent version.

1. Remove the current software.
2. Install the software provided by Xerox.
3. Complete the entire setup procedure using the software version just installed.
4. If available, upgrade to a more current version.