McAfee® Embedded Control
McAfee ePolicy Orchestrator®
Configuration Guide

Contents

Contents

McAfee Embedded Control

When McAfee ePO is installed on your server, use this guide to integrate Xerox MFPs that have the McAfee Embedded Control security feature.

McAfee 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:

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

For details about McAfee ePO and McAfee Embedded Control, visit www.mcafee.com.

Setting the Security Level

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

McAfee Embedded Control has three security levels:

- Enhanced Security
- Integrity Control
- Disabled

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, click **Properties > Security**.
2. Click **McAfee Embedded Control**.
3. To enable McAfee 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**.
   To turn off McAfee Embedded Control security features, select **Disable McAfee Embedded Control**.

   Note: Xerox recommends that you do not disable this feature.

5. If you selected Enhanced Security as the security level, click **Save**.
6. If you selected 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, click **Properties > Security**.
2. Click **McAfee 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 E-mail 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 McAfee 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 McAfee ePolicy Orchestrator Server, under McAfee Remote Solutions, select **McAfee'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 McAfee Embedded Control features are enabled, the printer also records security events in the audit log.

Configuring for Security Event Alerts in McAfee ePO

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

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

1. Purchase and install the McAfee ePO server software. For details, contact a McAfee representative or visit www.mcafee.com.

2. The Xerox® extensions for McAfee 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: 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 McAfee ePO. For details, refer to Downloading and Installing the Xerox Extensions for McAfee ePO on page 8.

4. Provide license keys in McAfee ePO. For details, refer to Providing License Keys in McAfee ePO on page 8.

5. To ensure that the printer can communicate with your McAfee ePO server, change the default agent wake-up communication port in McAfee ePO. For details, refer to Changing the Agent Wake Up Communication Port in McAfee ePO on page 9.

6. To allow printer software updates, change the maximum file size upload limit on the McAfee 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 McAfee ePO Server on page 9.

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 McAfee ePO. For details, refer to Creating and Assigning a Policy in McAfee ePO on page 10.

8. To ensure that you receive emails automatically in the event of a security alert, configure the Automated Response in McAfee ePO. For details, refer to Configuring the Automated Response in McAfee ePO on page 10.

9. In the Embedded Web Server, on the McAfee Embedded Control page, provide details about your McAfee ePO server. For details, refer to Configuring McAfee ePolicy Orchestrator Server Setting on page 12.

10. Designate printers as Super Nodes on your network. For details, refer to Designating Printers as Super Nodes on page 12.

11. Ensure that the device is managed within McAfee ePO. For details, refer to Ensuring that the Device is Managed in McAfee ePO on page 13.

12. Configure your McAfee ePO Proxy. For details, refer to Configuring Your McAfee ePO Proxy on page 14.

Downloading and Installing the Xerox Extensions for McAfee 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. For Utilities and Applications, click **Xerox Extension for McAfee 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 McAfee ePO, install the **.zip** extension files.
   a. Access the McAfee 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 or the McAfee Agent extension is installed already, remove the existing software. After the installation completes, reinstall the software provided by Xerox and update the Solidcore or the McAfee Agent extension. For details, refer to Removing and Reinstalling McAfee ePO on page 15.

   f. Install the other .**zip** extension file.
4. To continue configuring your security alerts, proceed to Providing License Keys in McAfee ePO on page 8.

Providing License Keys in McAfee ePO

1. Access the McAfee 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**
6. Click **Save**.
7. To continue configuring your security alerts, proceed to Changing the Agent Wake Up Communication Port in McAfee ePO on page 9.

Changing the Agent Wake-Up Communication Port in McAfee ePO

1. Access the McAfee 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 McAfee ePO Serve on page 9.

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

1. Access the McAfee ePO server, then navigate to **C:\Program Files (x86)\McAfee\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 McAfee ePO on page 10.

Creating and Assigning a Policy in McAfee ePO

1. Access the McAfee ePO Web interface at https://servername.domain:8443.
2. Navigate to **Menu** > **Policy** > **Policy Catalog**.
3. Next to Product, select **McAfee Agent**.
4. Next to Category, 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 **McAfee 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 McAfee ePO on page 10.

Configuring the Automated Response in McAfee ePO

To provide security administrators the ability to receive automatic email notifications, install the Automated Response feature. These notifications are sent whenever McAfee 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 McAfee 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**.
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 McAfee ePolicy Orchestrator Server Setting on page 12.

Configuring McAfee ePolicy Orchestrator Server Settings

1. In the Embedded Web Server, click **Properties** > **Security**.
2. Click **McAfee Embedded Control**.
3. On the McAfee Embedded Control page, next to Device Security Levels, click **Edit**.
4. Select **McAfee ePolicy Orchestrator Server**, then click **Edit**.
5. Select **McAfee ePolicy Orchestrator Server**, then click **Save**.
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 McAfee 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 on page 12.

Designating Printers as Super Nodes

The Xerox® extension for McAfee 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, McAfee ePO can use the other supernodes to communicate with other printers. You designate printers as supernodes by adding specific entries to your DNS server.

> Notes:
> - Your Xerox® printers and your McAfee ePO server must use the same DNS server.
> - Complete the following procedures on the DNS server, not the McAfee 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
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 McAfee ePO on page 13.

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 McAfee ePO looks for a domain with this name.
2. For Xerox.local, add entries for each supernode, then name them:
    -   XeroxDiscoverySuperNode1
    -   XeroxDiscoverySuperNode2
3. XeroxDiscoverySuperNode3
4. To continue configuring your security alerts, proceed to Ensuring that the Device is Managed in McAfee ePO on page 13.

Ensuring that the Device is Managed in McAfee ePO

1. In McAfee 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 McAfee ePO window, under Menu, select **Third Party**, then click the **Xerox MFP** extension.
7. For convenient McAfee ePO access, drag and drop the **Xerox MFP** extension icon to the top banner.
8. To continue configuring your security alerts, proceed to Configuring Your McAfee ePO Proxy on page 14.

Configuring Your McAfee ePO Proxy

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

1. In McAfee 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**.

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

Removing and Reinstalling McAfee ePO Extensions

If a message appears during installation indicating that the Solidcore or the McAfee Agent extension is installed already, remove the existing software. After the installation completes, reinstall the software provided by Xerox and update the Solidcore or the McAfee Agent 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.