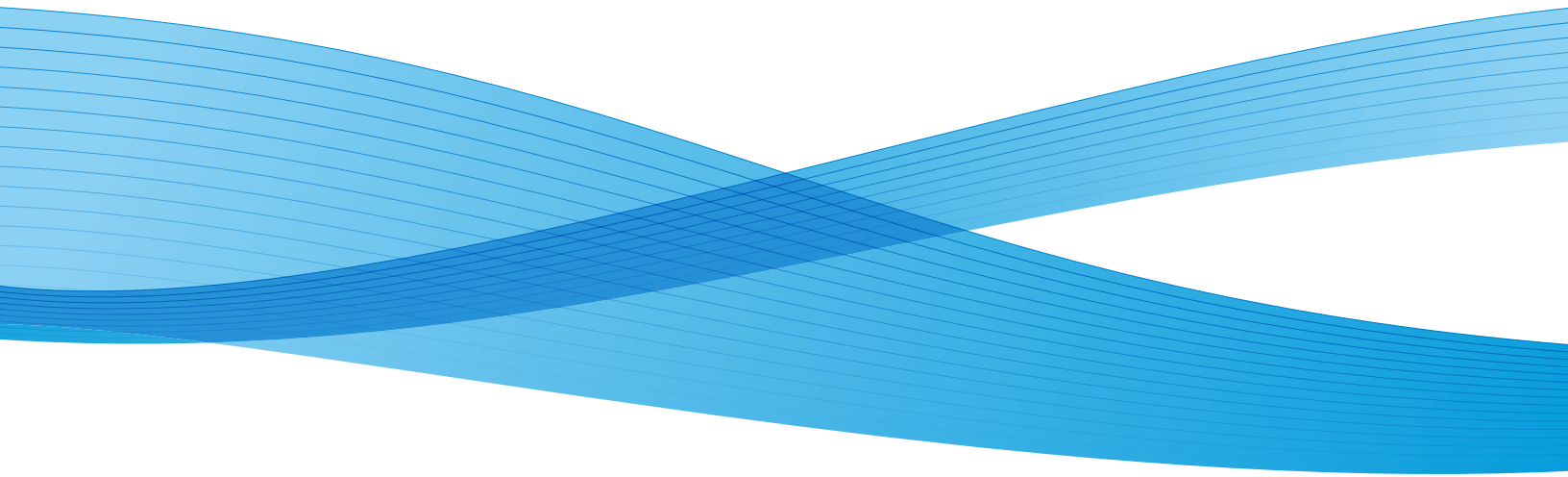


McAfee® Embedded Control

Configuration Guide for McAfee® ePO



© 2013 Xerox Corporation. All rights reserved. Unpublished rights reserved under the copyright laws of the United States. Contents of this publication may not be reproduced in any form without permission of Xerox Corporation.

Copyright protection claimed includes all forms of matters of copyrightable materials and information now allowed by statutory or judicial law or hereinafter granted, including without limitation, material generated from the software programs which are displayed on the screen such as styles, templates, icons, screen displays, looks, and so on.

Xerox® and Xerox and Design®, Phaser®, PhaserSMART®, PhaserMatch®, PhaserCal®, PhaserMeter™, CentreWare®, PagePack®, eClick®, PrintingScout®, Walk-Up®, WorkCentre®, FreeFlow®, SMARTsend®, Scan to PC Desktop®, MeterAssistant®, SuppliesAssistant®, Xerox Secure Access Unified ID System®, Xerox Extensible Interface Platform®, ColorQube®, Global Print Driver®, and Mobile Express Driver® are trademarks of Xerox Corporation in the United States and/or other countries.

Adobe® Reader®, Adobe® Type Manager®, ATM™, Flash®, Macromedia®, Photoshop®, and PostScript® are trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Apple, Bonjour, EtherTalk, TrueType, iPad, iPhone, iPod, iPod touch, Mac and Mac OS are trademarks of Apple Inc., registered in the U.S. and other countries. AirPrint and the AirPrint logo are trademarks of Apple Inc.

HP-GL®, HP-UX®, and PCL® are trademarks of Hewlett-Packard Corporation in the United States and/or other countries.

IBM® and AIX® are trademarks of International Business Machines Corporation in the United States and/or other countries.

Microsoft®, Windows Vista®, Windows®, and Windows Server® are trademarks of Microsoft Corporation in the United States and other countries.

Novell®, NetWare®, NDPS®, NDS®, IPX™, and Novell Distributed Print Services™ are trademarks of Novell, Inc. in the United States and other countries.

SGI® and IRIX® are trademarks of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

Sun, Sun Microsystems, and Solaris are trademarks or registered trademarks of Oracle and/or its affiliates in the United States and other countries.

McAfee®, ePolicy Orchestrator®, and McAfee ePO™ are trademarks or registered trademarks of McAfee, Inc. in the United States and other countries.

UNIX® is a trademark in the United States and other countries, licensed exclusively through X/ Open Company Limited.

PANTONE® and other Pantone, Inc. trademarks are the property of Pantone, Inc.

Document version 1.0: August 2013

BR7883_en-us

Contents

McAfee Embedded Control	5
Setting the Security Level.....	5
Setting the Alert Options	6
Configuring for Security Event Alerts in McAfee ePO	6
Downloading and Installing the Xerox® Extensions for McAfee ePO.....	7
Providing License Keys in McAfee ePO	8
Changing the Agent Wake Up Communication Port in McAfee ePO.....	8
Changing the Maximum File Upload Size Limit on the McAfee ePO Server.....	8
Creating and Assigning a Policy in McAfee ePO	8
Configuring the Xerox Automated Response in McAfee ePO.....	9
Configuring McAfee ePolicy Orchestrator Server Settings.....	10
Designating Printers as Super Nodes.....	10
Adding DNS Entries to One or More Existing Domains	10
Adding DNS Entries to a Single New Domain.....	10
Ensuring the Device is Managed in McAfee ePO.....	11
Configuring Your McAfee ePO Proxy	11
Removing and Reinstalling McAfee ePO Extensions	11

[This page left intentionally blank]

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. Enable this option by providing a feature installation key on the Feature Installation page. To get 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. They can also be sent 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 Xerox® CentreWare® Internet Services, 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**. 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 Xerox® CentreWare® Internet Services, 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

To configure security alerts in McAfee, the procedures must be completed in a specific order. This overview includes references to each procedure.

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 Microsoft .NET Framework 4.0 or later. For details, visit www.microsoft.com.

Note: Not completing this procedure results in an "error-2" message when opening the Xerox® MFP extension.

3. Download and install the Xerox® extensions for McAfee ePO. For details, see [Downloading and Installing the Xerox® Extensions for McAfee ePO](#) on page 7.
4. Provide license keys in McAfee ePO. For details, see [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, see [Changing the Agent Wake Up Communication Port in McAfee ePO](#) on page 8.

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, see [Changing the Maximum File Upload Size Limit on the McAfee ePO Server](#) on page 8.
7. Ensure that security event alerts are sent when they occur rather than at regular intervals. Create a security policy, and associate the policy with your Xerox® printers in McAfee ePO. For details, see [Creating and Assigning a Policy in McAfee ePO](#) on page 8.
8. To ensure that you automatically receive emails in the event of a security alert, configure the Xerox Automated Response in McAfee ePO. For details, see [Configuring the Xerox Automated Response in McAfee ePO](#) on page 9.
9. On the McAfee Embedded Control page in Xerox® CentreWare® Internet Services, provide details about your McAfee ePO server. For details, see [Configuring McAfee ePolicy Orchestrator Server Setting](#) on page 10.
10. Designate printers as Super Nodes on your network. For details, see [Designating Printers as Super Nodes](#) on page 10.
11. Ensure that the device is managed within McAfee ePO. For details, see [Ensuring That the Device is Managed](#) on page 11.
12. Configure your McAfee ePO Proxy. For details, see [Configuring Your McAfee ePO Proxy](#) on page 11.

Downloading and Installing the Xerox® Extensions for McAfee ePO

1. Locate and download the Xerox® extensions. The extensions are contained in a **.zip** file.
 - a. Using a Web browser, go to the Xerox Support website at www.xerox.com/office/support.
 - b. Navigate to the support page for your specific device. For example, type WorkCentre 7830 in the Search box, then press **Enter**.
 - c. In the results listed for your device, click **Drivers and Downloads**.
 - d. From the **Operating System** drop-down menu, select the operating system for your server.

Note: Ensure you select the operating system for your server, not the operating system of your computer.
 - e. Under 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 three 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 lower 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 that the Solidcore or the McAfee Agent extension is installed already, remove the existing software. Then reinstall the software provided by Xerox and update the Solidcore or the McAfee Agent extension. For details, see [Removing and Reinstalling McAfee ePO](#) on page 11.
 - f. Install the other two **.zip** extension files.
4. To continue configuring your security alerts, proceed to step 4 of [Configuring for Security Event Alerts in McAfee ePO](#) on page 6.

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:
 - Integrity Monitor: **A5G2-XBVN-49YT-SDL5-K835**
6. Click **Save**.
7. To continue configuring your security alerts, proceed to step 5 of [Configuring for Security Event Alerts in McAfee ePO](#) on page 6.

Note: This is Integrity Control in ePO 5.0.

- Change Control: **XL17-ZCWK-K7E2-9PZY-OT6V**
- Application Control: **ZM7H-FX52-3SFL-TR5Z-MAG3**

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 step 6 of [Configuring for Security Event Alerts in McAfee ePO](#) on page 6.

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\Policy 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 step 7 of [Configuring for Security Event Alerts in McAfee ePO](#) on page 6.

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. 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. On the bottom tray, 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, select **Has Tag**.
 - h. Under Value, select **Xerox MFP**.
 - i. Click **Next**.
10. Click **Save**.
11. To continue configuring your security alerts, proceed to step 8 of [Configuring for Security Event Alerts in McAfee ePO](#) on page 6.

Configuring the Xerox Automated Response in McAfee ePO

The Xerox Automated Response comes with the Xerox[®] Extension. Install the Xerox Automated Response to provide key operators the ability to receive automatic email notifications. 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 Xerox Automated Response is disabled. To enable it, a key operator 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. Locate Xerox MFP Alerts, then click **Edit**.
3. Click **4. Actions**.
4. For Recipients, add your preferred email address, then click **Save**.
5. Under Responses, select **Xerox MFP**.
6. Click **Actions**, then click **Enable Responses**.

Note: To view Xerox[®] MFP security events with McAfee ePO, select **Menu > Reporting > Threat Event Log**.

7. To continue configuring your security alerts, proceed to step 9 of [Configuring for Security Event Alerts in McAfee ePO](#) on page 6.

Configuring McAfee ePolicy Orchestrator Server Settings

1. In Xerox® CentreWare® Internet Services, 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 step 10 of [Configuring for Security Event Alerts in McAfee ePO](#) on page 6.

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 step 11 of [Configuring for Security Event Alerts in McAfee ePO](#) on page 6.

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 step 11 of [Configuring for Security Event Alerts in McAfee ePO](#) on page 6.

Ensuring 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 is displaying 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 step 12 of [Configuring for Security Event Alerts in McAfee ePO](#) on page 6.

Configuring Your McAfee ePO Proxy

A proxy, if used, 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: Not completing this procedure results in an "error-2" message when opening the Xerox® MFP extension.

Removing and Reinstalling McAfee ePO Extensions

If a message appears during installation that the Solidcore or the McAfee Agent extension is installed already, remove the existing software. Then 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. Using the version provided, complete the entire setup procedure.
4. If available, upgrade to a more current version.