Lexmark™

Mobile Print

Integration Guide for Microsoft Intune

August 2018

www.lexmark.com

Contents

Change history

August 2018

- Initial document release

Overview

Lexmark^{TM} Mobile Print (LMP) lets you send documents and images directly to network-connected Lexmark printers and servers from your mobile device. It also lets you scan documents, and then save them to your mobile device.

To control the user access to the company resources and protect corporate data, use Lexmark Mobile Print with Microsoft Intune.

Microsoft Intune enables your organization to do the following:

- Manage the application deployment.
- Set the configuration and data protection policies for LMP.
- Provide different types of mobile device management profiles, such as VPN or tunneling profile.

This document provides instructions on how to integrate and configure Lexmark Mobile Print for Microsoft Intune.

System requirements

- Intune Company Portal v5.0 or later
- Either of the following platforms:
  - For mobile devices with the Android^{TM} platform:
    - Lexmark Mobile Print v2.7 or later
    - Android 5.0 or later
  - For mobile devices with iOS operating system:
    - Lexmark Mobile Print Intune v2.7 or later
    - iOS 10.0 or later

Integrating the application

Before you begin, make sure that your organization has an administrator account to the Microsoft Azure portal.

Adding the LMP application to Microsoft Intune

1. From your browser, go to https://portal.azure.com.
2. Click **Microsoft Intune** > **Mobile apps** > **Apps** > **Add**.
3. Do either of the following:

   ### For LMP for Android

   a. In the "App type" drop-down menu, click **Android**.
   b. Click **App information**.
   c. In the Name field, type **`Lexmark Mobile Print for Intune`**.
   d. In the Description field, type the application description.
   e. In the Publisher field, type **`Lexmark International, Inc`**.
   f. In the Appstore URL field, type the Google Play^{TM} store URL for Lexmark Mobile Print.
   g. In the "Minimum operating system" drop-down menu, click **Android 5.0 (Lollipop)**.
   h. Click **OK**.

   ### For LMP for iOS

   a. In the "App type" drop-down menu, click **iOS**.
   b. Click **Search the App Store**.
   c. Search for Lexmark Mobile Print Intune, and then click **Select**.

4. Click **Add**.

Adding users to Microsoft Intune

1. From your browser, go to https://portal.azure.com.
2. Click **Microsoft Intune** > **Users** > **New user**.
3. In the Name field, type the name.
4. In the "User name" field, type the e-mail address.
5. If necessary, configure the user profile or role.
6. Click **Create**.

   Note: The portal generates the user password automatically.

Adding groups

1. From your browser, go to **https://portal.azure.com**.
2. Click **Microsoft Intune** > **Groups** > **New group**.
3. In the “Group type” drop-down menu, click **Security**.
4. In the “Group name” field, type a unique group name.
5. In the “Membership type” drop-down menu, depending on your organization requirement, select whether the membership type is assigned or dynamic.
6. If necessary, type a group description.
7. Click **Create**.

Adding the LMP application to a group

1. From your browser, go to **https://portal.azure.com**.
2. Click **Microsoft Intune** > **Mobile apps** > **Apps**.
3. Select **Lexmark Mobile Print** or **Lexmark Mobile Print Intune**.
4. Click **Assignments** > **Add group**.
5. In the “Assignment type" drop-down menu, depending on your configuration, click **Available for enrolled devices**, **Available with or without enrollment**, or **Required**.
6. Click **Included Groups** > **Select groups to include**.
7. In the Select field, type the group name.

   Note: You can also select a group from the list.
8. Click **Select**.

Adding users to a group

To assign an application protection policy to a user, the user must be added to a group.

1. From your browser, go to **https://portal.azure.com**.
2. Click **Microsoft Intune** > **Groups**, and then select a group.
3. Click **Members** > **Add members**.
4. In the “Select member or invite an external user" menu, select a user.
5. Click **Select**.

Configuring the application

Adding an application protection policy

To configure the data relocation, application access, and data loss prevention settings, add an application protection policy.

1. From your browser, go to **https://portal.azure.com**.
2. Click **Microsoft Intune** > **Mobile apps** > **App protection policies** > **Add a policy**.
3. In the Name field, type the policy name.
4. In the Platform drop-down menu, select an operating system.

   Note: If your organization uses two or more platforms, then add a protection policy for each platform.
5. Navigate to **Apps** > select the LMP application > **Select**.
6. Click **Settings**, and then configure the supported Access Actions settings.

   Notes:

   - Lexmark Mobile Print does not claim support for the “Data relocation” settings.
   - For more information on supported Access Actions settings, see “Understanding the supported Access Actions settings” on page 8.
7. Click **OK** > **Create**.

Understanding the supported Access Actions settings

Setting	Description
Recheck the access requirements after (minutes)—Timeout	Enter the time before the access requirements for the application are rechecked after launching it. **Note:** We recommend setting the value to 5. The default value is 30.
Block screen capture and Android Assistant (Android only)	• Click **Yes** to prevent the mobile device from running a personal assistant application and making a screen capture. • Click **No** to allow the device to run a personal assistant application and enable the screen capture capability. **Notes:** • This setting is available only for mobile devices running on Android 6.0 or later. • The default value is Yes.

Setting	Description
Min OS version	To configure the setting, do the following: 1 In the VALUE field, type the minimum supported OS version of the mobile device. 2 In the ACTION drop-down menu, do one of the following: • Click **Block access** to prevent the application from running when the OS version of the mobile device is less than the set minimum. • Click **Wipe data** to delete the application data when the OS version of the mobile device is less than the set minimum. • Click **Warn** to receive a warning when the OS version of the mobile device is less than the set minimum.

Assigning an application protection policy to a group

1. From your browser, go to **https://portal.azure.com**.
2. Click **Microsoft Intune** > **Mobile apps** > **App protection policies**.
3. Select a policy, and then click **Assignments**.
4. From the Include section, click **Select groups to include**.
5. In the Select field, type the group name.

   Note: You can also select a group from the list.
6. Click **Select**.

Adding an application configuration policy

1. From your browser, go to **https://portal.azure.com**.
2. Click **Microsoft Intune** > **Mobile apps** > **App configuration policies** > **Add**.
3. In the Name field, type a policy name.
4. In the “Device enrollment type” drop-down menu, select either **Managed apps** or **Managed devices**.
5. Navigate to **Associated app** > select an application > **OK**.
6. Click **Configuration settings**, and then type the key and value.

   Note: For more information, see “Understanding the application-specific configurations” on page 10.
7. Click **OK** > **Add**.

Understanding the application-specific configurations

Key	Value	Description
`type-`*`name`* where ***`name`*** is the provider type name	Provider type - **`printer`** - **`server`** - **`server-premise`**	In the Name field, assign a name for the provider type, and then in the Value field, type the value for the provider type. For example, type **`type-`*`LexmarkColorMFP`*** in the Key field, and then type **`printer`** in the Value field.
`address-`*`name`* where ***`name`*** is the provider type name	Network address	In the Name field, assign a name for the printer or server, and then in the Value field, type the network address. For example, type **`address-`*`LexmarkColorMFP`*** in the Key field, and then type ***`255.255.255.255`*** in the Value field. **Note:** Make sure that the name used in **`address-`*`name`*** is the same with the name used in **`type-`*`name`***.
`auto-discover-`*`name`* where ***`name`*** is the provider type name	- **`true`** - **`false`**	Type **`true`** to discover the printer automatically after importing the configuration file. Make sure that the value for **`type-`*`name`*** is set to **`printer`**. **Note:** Make sure that the name used in **`auto-discover-`*`name`*** is the same with the name used in **`type-`*`name`***.
`add-providers`	- **`true`** - **`false`**	Type **`true`** to allow adding printers or servers from the application. **Note:** If the key is not configured, then the default value is used. The default value is **`true`**.
`delete-providers`	- **`true`** - **`false`**	Type **`true`** to allow deleting printers or servers from the application. **Note:** If the key is not configured, then the default value is used. The default value is **`true`**.
`supports-clipboard`	- **`true`** - **`false`**	Type **`true`** to allow printing from the clipboard. **Note:** If the key is not configured, then the default value is used. The default value is **`true`**.
`supports-photos`	- **`true`** - **`false`**	Type **`true`** to allow printing photos or starting a scan from the gallery. **Note:** If the key is not configured, then the default value is used. The default value is **`true`**.
`supports-web`	- **`true`** - **`false`**	Type **`true`** to allow printing web pages from the application. **Note:** If the key is not configured, then the default value is used. The default value is **`true`**.
`supports-jobs`	- **`true`** - **`false`**	Type **`true`** to allow access to job queues. **Note:** If the key is not configured, then the default value is used. The default value is **`true`**.

Key	Value	Description
supports-manual-add	• **true** • **false**	Type **true** to allow adding printers manually. Make sure that **<add-providers>** is set to **true**. **Note:** If the key is not configured, then the default value is used. The default value is **true**.
supports-qrcode	• **true** • **false**	Type **true** to allow adding printers by using a QR code. Make sure that **<add-providers>** is set to **true**. **Note:** If the key is not configured, then the default value is used. The default value is **true**.
supports-network-search	• **true** • **false**	Type **true** to allow adding printers by searching the network. Make sure that **<add-providers>** is set to **true**. **Note:** If the key is not configured, then the default value is used. The default value is **true**.
supports-nfc	• **true** • **false**	Type **true** to allow printing by using NFC. **Note:** If the key is not configured, then the default value is used. The default value is **true**.
easy-saas	• **true** • **false**	Type **true** to enable **Access to Lexmark Print Management Cloud**. This setting automatically adds **lsp.lexmark.com/lexmark** to the list of LPM servers. **Note:** If the key is not configured, then the default value is used. The default value is **false**.
quick-print-release	• **true** • **false**	Type **true** to allow releasing of LPM On-Premises print jobs using Quick Print. **Note:** If the key is not configured, then the default value is used. The default value is **false**.
quick-print-release-type	• **QR** • **IP**	Type **QR** to release the print job using the QR code. Type **IP** to release the print job using the printer IP address. Make sure that **quick-print-release** is set to **true**. **Note:** To make both options available, leave the value blank.
direct-printing-port	Port number	Type the port number to use for printing directly from the mobile device. **Note:** If the key is not configured, then the default value is used. The default value is **631**.
secure-print-release-port	Port number	Type the port number to use for secure connection with the servers. **Note:** If the key is not configured, then the default value is used. The default value is **443**.

Key	Value	Description
web-port	Port number	Type the port number to use for web communications. **Note:** If the key is not configured, then the default value is used. The default value is **80**.
printer-capabilities-data-port	Port number	Type the port number to use for sending data to the printer. **Note:** If the key is not configured, then the default value is used. The default value is **9100**.
premise-server-ssl-port	Port number	Type the port number to use for releasing print jobs in the servers. **Note:** If the key is not configured, then the default value is used. The default value is **9743**.
import-configList	• **use_config** • **merge** • **reset_all**	Define how the providers in the configuration file are managed when importing. Type **use_config** to do the following: • Delete the printers and servers from the application that are not in the configuration file. • Add the printers and servers that are in the configuration file and not in the application. • Update the nicknames of the printers and servers that are in the configuration file and in the application. Type **merge** to do the following: • Keep the existing printers and servers from the application. • Add the printers and servers that are in the configuration file, but are not in the application. • Update the nicknames of the printers and servers that are in the configuration file and in the application. Type **reset_all** to do the following: • Delete all the printers and servers that are in the application. • Add the printers and servers that are in the configuration file.

Assigning an application configuration policy to a group

1. From your browser, go to https://portal.azure.com.
2. Click **Microsoft Intune** > **Mobile apps** > **App configuration policies**.
3. Select a configuration policy, and then click **Assignments**.
4. From the Include section, click **Select groups to include**.

5. In the Select field, type a group name.

   Note: You can also select a group from the list.

6. Click **Select**.

Creating a VPN profile

Virtual private networks (VPN) let users access your company network remotely and securely.

1. From your browser, go to **https://portal.azure.com**.
2. Click **Microsoft Intune** > **Device configuration** > **Profiles** > **Create profile**.
3. In the Name field, type a profile name.
4. If necessary, type a description.
5. In the Platform drop-down menu, select the operating system of the mobile devices used in your organization.

   Note: If your organization uses two or more platforms, then create a separate VPN profile for each platform.

6. In the “Profile type” drop-down menu, click **VPN**.
7. Click **Settings**, and then configure the VPN and proxy settings for your organization.
8. Click **OK** > **OK** > **Create**.

Assigning a VPN profile

1. From your browser, go to **https://portal.azure.com**.
2. Click **Microsoft Intune** > **Device configuration** > **Profiles**.
3. Select a VPN profile, and then click **Assignments**.
4. Do either of the following:

To all users or devices

a. In the “Assign to” drop-down menu, depending on your organization requirement, click **All Users & All Devices**, **All Devices**, or **All Users**.

b. Click **Save**.

To a group

a. In the “Assign to” drop-down menu, click **Selected Groups**.

b. In the Select field, type the group name.

   Note: You can also select a group from the list.

c. Click **Select** > **Save**.

Connecting a mobile device to VPN

Before you begin, depending on the network infrastructure of your organization, download one of the following:

- Cisco AnyConnect

  Note: For Cisco AnyConnect, make sure that the External Control setting is enabled to let third-party applications control it.

- Cisco Legacy AnyConnect (iOS only)
- Check Point Capsule Connect
- SonicWall Mobile Connect
- F5 Access for iOS or F5 Access 2018
- Citrix® VPN

1. From your mobile device, launch the VPN application.
2. Depending on the application, touch **Settings** or **Connections**.
3. Configure the VPN settings or add a VPN connection.
4. Enable the VPN connection.

Configuring the Intune Company Portal application

Before you begin, make sure that you have downloaded the Intune Company Portal application.

Note: You may need to connect to a VPN network before configuring the Intune Company Portal application. For more information, see "Connecting a mobile device to VPN" on page 14.

1. From your mobile device, launch the Intune Company Portal application.
2. Log in using your company credentials, and then follow the instructions on the screen.
3. Do either of the following:

   ### For Android devices

   a. From the Company Portal screen, touch **Activate**.

   b. If prompted, grant permissions.

   Note: For Samsung devices, you may need to read and agree to the Samsung Knox Privacy Policy.

   ### For iOS devices

   a. If prompted, allow the application to access the settings.

   b. From the Install Profile dialog box, touch **Install**.

   Notes:

   - The device may ask for your password.
   - The device may prompt a mobile device management warning. If prompted, touch **Install**.

   c. From the Remote Management dialog box, touch **Trust**.

4. Touch **Done**.

Deploying the LMP application to a mobile device

1. From your mobile device, launch the Intune Company Portal application, and then log in using your corporate credentials.
2. From the application home screen, touch **App**.

   Note: For iOS devices, you may need to click **View** to access the list of applications.
3. Depending on your mobile device, touch **Lexmark Mobile Print Intune** or **Lexmark Mobile Print for Intune**.
4. Touch **Install**.
5. From the App Installation dialog box, touch **Install**.

Updating the LMP application

In the Microsoft Intune web portal

1. Add the latest version of the Lexmark Mobile Print application to Microsoft Intune. For more information, see “Adding the LMP application to Microsoft Intune” on page 6.
2. Click the application, and then click **Assignments** > **Add Group**.
3. From the “Assignment type” drop-down menu, click **Available for enrolled devices**.
4. From the “Selected groups” section, click **Select groups to include**.
5. In the Select field, type the group name.

   Note: You can also select a group from the list.
6. Click **Select**.

On the mobile device

1. From your mobile device, launch the Intune Company Portal application, and then log in.
2. From the application home screen, touch **App**.

   Note: For iOS devices, you may need to click **View** to access the list of applications.
3. Depending on your mobile device, touch **Lexmark Mobile Print Intune** or **Lexmark Mobile Print for Intune**, and then touch **Update**.

   Note: For iOS devices, the App Installation dialog box may appear. If prompted, touch **Update**.

Disabling access to the App Store online store or the Google Play store

To restrict third-party applications that are not approved for use in your organization, disable access to the App Store online store or the Google Play store.

1. From your browser, go to **https://portal.azure.com**.
2. Click **Microsoft Intune** > **Device configuration** > **Profiles** > **Create profile**.

3 In the Name field, type a profile name.

4 Do either of the following:

For Android devices

Note: This setting applies only to Samsung mobile devices with KNOX Standard 4.0+ enabled.

a In the Platform drop-down menu, click **Android**.

b In the “Profile type” drop-down menu, click **Device restrictions**.

c Click **Settings** > **Google Play Store**.

d Click **Block** beside the “Google Play store (Samsung KNOX only)” setting.

For iOS devices

a In the Platform drop-down menu, click **iOS**.

b In the “Profile type” drop-down menu, click **Device restrictions**.

c Click **Settings** > **App Store, Doc Viewing, Gaming**.

d Click **Block** beside the “App store” setting.

5 Click **OK** > **OK** > **Create**.

Increasing the device enrollment limit

1 From your browser, go to **https://portal.azure.com**.

2 Click **Microsoft Intune** > **Device Enrollment** > **Enrollment restrictions**.

3 From the Device Limit Restrictions section, click the default restriction.

4 From the Device Limit section, click the device limit counter.

5 In the Device Limit drop-down menu, select the number of devices.

Note: You can set up to 15 devices.

6 Click **Save**.

Appendix

Dual-mode support

LMP for Android

- The Intune Company Portal application is required to enforce the configurations and policies to the Lexmark Mobile Print application.
- To use the Lexmark Mobile Print with Microsoft Intune, add the application in the Intune portal. Do not download the application directly from the Google Play store.
- If the device enrollment limit is exceeded, then remove unused devices or increase the device limit to enroll a new device. For more information, see "Increasing the device enrollment limit" on page 16.

LMP for iOS

- The Intune Company Portal application is not required to enforce the configurations and policies to the Lexmark Mobile Print Intune application. You can launch the application without the portal. For administrative purposes, we recommend installing the Intune Company Portal application.
- Lexmark Mobile Print and Lexmark Mobile Print Intune are both available in the App Store online store. The Intune configurations and policies work only with Lexmark Mobile Print Intune.
- If the device enrollment limit is exceeded, then remove the unused devices or increase the device limit to enroll a new device. For more information, see "Increasing the device enrollment limit" on page 16.
- If a user logs in to the Intune Company Portal, then the user is paired with the application. To remove the pairing, reset the mobile device to factory defaults or disable the account.

Unsupported features

Some LMP features are not available in the Intune version.

LMP for Android

- Sharing from external applications is not supported.
- Reading the mobile device storage contents is not supported.
- The Capture From feature is not supported.
- Camera images taken from the application dashboard are not saved to the mobile device gallery.
- The Print plug-in is not supported.
- The LMP widgets are not supported.

LMP for iOS

- Sharing from external applications is not supported.
- Reading the mobile device storage contents is not supported.
- The Capture From feature is not supported.
- If the **`Transfer Apps`** policy is set to **`None`**, then the widget does not open the correct screen, and the Action Not Allowed dialog box appears. Closing the dialog box lets you use the application.

- If the application configuration setting includes the **`supports-jobs=true`** code, then the bottom tool bar of the application dashboard does not update.
- From the About screen, tapping the application name five times opens a dialog box with the debug information.

Application limitations

- For the unsupported protection policies, enabling or disabling a key may not take effect. For example, if you disable printing in the policy setting, the LMP application allows users to print.
- The application configuration policy in JSON, XML, or custom format is not supported.

Notices

Edition notice

August 2018

The following paragraph does not apply to any country where such provisions are inconsistent with local law: LEXMARK INTERNATIONAL, INC., PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in later editions. Improvements or changes in the products or the programs described may be made at any time.

References in this publication to products, programs, or services do not imply that the manufacturer intends to make these available in all countries in which it operates. Any reference to a product, program, or service is not intended to state or imply that only that product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any existing intellectual property right may be used instead. Evaluation and verification of operation in conjunction with other products, programs, or services, except those expressly designated by the manufacturer, are the user’s responsibility.

For Lexmark technical support, visit **http://support.lexmark.com**.

For information on supplies and downloads, visit **www.lexmark.com**.

GOVERNMENT END USERS

The Software Program and any related documentation are "Commercial Items," as that term is defined in 48 C.F.R. 2.101, "Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. 12.212 or 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. 12.212 or 48 C.F.R. 227.7202-1 through 227.7207-4, as applicable, the Commercial Computer Software and Commercial Software Documentation are licensed to the U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein.

Trademarks

Lexmark and the Lexmark logo are trademarks or registered trademarks of Lexmark International, Inc. in the United States and/or other countries.

Android and Google Play are trademarks of Google Inc.

App Store is a trademark of Apple Inc.

Citrix is a trademark of Citrix Systems, Inc., and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

All other trademarks are the property of their respective owners.

Index