# Embedded Web Server

## Administrator's Guide

**February 2009** **www.lexmark.com**


740 West New Circle Road
Lexington, Kentucky 40550

**Edition notice**

February 2009



For Lexmark technical support, visit **support.lexmark.com**.

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

If you don't have access to the Internet, you can contact Lexmark by mail:

Lexmark International, Inc.
Bldg 004-2/CSC
740 New Circle Road NW
Lexington, KY 40550

# Contents

# Using security features in the Embedded Web Server

The latest suite of security features available in the Lexmark Embedded Web Server represents an evolution in keeping document outputs safe and confidential in today's busy environments. Incorporating traditional components such as authentication and group permissions, administrators can use Embedded Web Server Security Templates to control access to the devices that produce, store, and transmit sensitive documents. Security templates are an innovative new tool developed by Lexmark to enable administrators to build secure, flexible profiles that provide end users the functionality they require, while limiting access to sensitive printer functions or outputs to only those users holding appropriate credentials. Utilizing soft configuration features alone or in conjunction with physical security such as Common Access Cards, the printer will no longer be a weak link in the document security chain.

# Understanding the basics

Securing a printer through the Embedded Web Server involves combining one or more components—Authentication, Authorization, and Groups—to define who is allowed to use the printer, and which functions those users are allowed to access.

Before configuring printer security, it can be helpful to create a plan that identifies who the users will be and what they will need to do. Items to consider might include the location of the printer and whether non-authorized persons have access to that area, sensitive documents that will be sent to or stored on the printer, and the information security policies of your organization.

## Authentication and Authorization

*Authentication* is the method by which a system securely identifies a user (that is, who you are).

*Authorization* specifies which functions are available to a user who has been authenticated by the system. This set of authorized functions is also referred to as "permissions."

The Embedded Web Server handles authentication and authorization using one or more of the following, also referred to as *Building Blocks*:

- PIN
- Password
- Internal accounts
- LDAP
- LDAP+GSSAPI
- Kerberos 5 (used only in conjunction with LDAP+GSSAPI)
- NTLM

Some Building Blocks, such as Password or PIN, can be used alone to provide low-level security, by simply limiting access to a printer—or specific functions of a printer—to anyone who knows the correct code. This type of security might be appropriate in a situation in which a printer is located in the lobby or other public area of a business, so that only employees who know the password or PIN are able to use the printer. Because anyone who enters the correct password or PIN receives the same privileges and users can not be individually identified, passwords and PINs are considered less secure than other building blocks that require a user to be identified, or both identified and authorized.

## Groups

Administrators can designate up to 32 groups to be used in association with either the Internal accounts or LDAP/LDAP+GSSAPI building blocks. For the purposes of Embedded Web Server security, groups are used to identify sets of users needing access to similar functions. For example, in Company A, employees in the warehouse do not need to print in color, but those in sales and marketing use color every day. In this scenario, it makes sense to create a "Warehouse" group, and a "Sales and Marketing" group.

## Access Controls

By default, all device menus, settings, and functions come with no security enabled. Access Controls (also referred to in some devices as "Function Access Controls"), are used to manage access to specific menus and functions or to disable them entirely. Access controls can be set using a password, PIN, or security template. The number of functions that can be controlled varies depending on the type of device, but in some multifunction printers, over 40 individual menus and functions can be protected.

**Note:** For a list of individual Access Controls and what they do, see "Menu of Access Controls" on page 29.

## Security Templates

Some scenarios call for only basic security such as PIN-protected access to common device functions, while others require tighter security and role-based restrictions. Individually, building blocks, groups, and access controls may not meet the needs of a complex security environment. In order to accommodate users in different groups needing access to a common set of functions such as printing, copying, and faxing, administrators must be able to combine these components in ways that give all users the functions they need, while restricting other functions to only authorized users.

A *Security Template* is a profile constructed using a building block, or certain building blocks paired with one or more groups. How they are combined determines the type of security created:

| **Building block** | **Type of security** |
|---|---|
| Internal Accounts | Authentication only |
| Internal Accounts with Groups | Authentication and authorization |
| Kerberos 5 | Authentication only |
| LDAP | Authentication only |
| LDAP with Groups | Authentication and authorization |
| LDAP + GSSAPI | Authentication only |
| LDAP + GSSAPI with Groups | Authentication and authorization |
| Password | Authorization only |
| PIN | Authorization only |

Each device can support up to 140 security templates, allowing administrators to create very specific profiles—or roles—for each access control.

# Configuring building blocks

## Creating a password

The Embedded Web Server can store a combined total of 250 user-level and administrator-level passwords on each supported device.

### To create a password

1. From the Embedded Web Server Home screen, browse to **Settings → Security → Edit Security Setups**.
2. Under Edit Building Blocks, select **Password**.
3. Under Manage Passwords, select **Add a Password**.
4. Type a name for the password in the Setup Name box. Each password must have a unique name consisting of 1-128 UTF-8 characters (example: "Copy Lockout Password").
5. Type a password in the appropriate box, and then re-enter the password to confirm it.
6. Select **Admin Password** if the password will be used as the Administrator password.

   **Note:** Selecting the **Admin Password** box sets the password as administrator-level. Administrator-level passwords override normal passwords. If a function or setting is protected by a normal password, any administrator-level password will also grant access.
7. Click **Submit**.

**Notes:**

- To edit a password, select a password from the list, and then modify the settings.
- To delete a password, select a password from the list and then click **Delete Entry**. Clicking **Delete List** will delete all passwords on the list, whether they are selected or not.

## Creating a PIN

Typically, *Personal Identification Numbers* (PINs) are used to control access to specific device menus or to a device itself. PINs can also be used to control access to document outputs, by requiring a user to type a correct PIN to retrieve a held print, copy, or fax job. The Embedded Web Server can store a combined total of 250 user-level and administrator-level PINs.

### To create a PIN

1. From the Embedded Web Server Home screen, browse to **Settings → Security → Edit Security Setups**.
2. Under Edit Building Blocks, select **PIN**.
3. Select **Add a PIN**.
4. Type the name of the PIN configuration in the Setup Name box. Each PIN must have a unique name consisting of 1-128 UTF-8 characters (example: "Copy Lockout PIN").
5. Type a PIN in the appropriate box, and then re-enter the PIN to confirm it.

   **Note:** The default PIN length is four digits, which may be changed by modifying the Minimum PIN length field under **Settings → Security → Miscellaneous Security Settings**.

6 Select **Admin PIN** if the PIN will be used as the Administrator PIN.

**Note:** If an activity is secured by a specific Administrator PIN, then only that PIN will grant access to it.

7 Click **Submit**.

# Setting up internal accounts

Embedded Web Server administrators can configure one internal account building block per supported device. Each internal account building block can include a maximum of 250 user accounts, and 32 user groups.

The internal accounts building block can be used by itself in a security template to provide authentication-level security, or in conjunction with one or more groups to provide both authentication and authorization.

## Defining user groups

If using groups for authorization, define them prior to creating new internal accounts.

1 From the Embedded Web Server Home screen, browse to **Settings → Security → Edit Security Setups**.

2 Under Edit Building Blocks, select **Internal Accounts**.

3 Select **Setup groups for use with internal accounts**.

4 Type the Group Name.

**Note:** Group names can contain up to 128 UTF-8 characters.

5 Click **Add**.

6 Repeat steps 4 through 5 to add additional user groups.

**Note:** When creating groups, it is helpful to first make a list of all users, and then determine which device functions —such as printing, scanning, and copying—will be needed by all users, and which functions will be needed only by certain users. Each group will fulfill a *role* once combined into a security template, and users can be assigned to more than one group (or role), in order to grant them access to all needed functions.

## Creating user accounts

1 From the Embedded Web Server Home screen, browse to **Settings → Security → Edit Security Setups**.

2 Under Edit Building Blocks, select **Internal Accounts**.

3 Select **Add an Internal Account**, and then provide the information needed for each account:

- **Account Name**—Type the user's account name (example: "Jack Smith"). You can use up to 128 UTF-8 characters.
- **User ID**—Type an ID for the account (example: "jsmith"). You can use up to 128 UTF-8 characters.
- **Password**—Type a password of between 8 and 128 characters.
- **Re-enter Password**—Type the password entered in the field above.
- **E-mail**—Type the user's E-mail address (example: "jsmith@company.com").
- **Groups**—Select the groups to which the account belongs. Hold down the Ctrl key to select multiple groups for the account.

4 Click **Submit** to save the new account, or **Cancel** to return to the Manage Internal Accounts menu without storing the new account.

## Specifying settings for internal accounts

Settings selected in the Internal Accounts Settings section will determine the information an administrator must submit when creating a new internal account, as well as the information a user must submit when authenticating.

- **Require e-mail address**—Select this box to make the E-mail address a required field when creating new internal accounts.
- **Required user credentials**—Select either **User ID** or **User ID and Password** to specify the information a user must submit when authenticating.

# Using LDAP

*Lightweight Directory Access Protocol* (LDAP) is a standards-based, cross-platform, extensible protocol that runs directly on top of the TCP/IP layer, and is used to access information stored in a specially organized information directory. One of the strengths of LDAP is that it can interact with many different kinds of databases without special integration, making it more flexible than other authentication methods.

**Notes:**

- Supported devices can store a maximum of five unique LDAP configurations. Each configuration must have a unique name.
- Administrators can create up to 32 user-defined groups that apply to each unique LDAP configuration.
- As with any form of authentication that relies on an external server, users will not be able to access protected device functions in the event of an outage that prevents the printer from communicating with the authenticating server.
- To help prevent unauthorized access, users are encouraged to securely end each session by selecting **Log out** on the printer control panel.

## To add a new LDAP setup

1. From the Embedded Web Server Home screen, browse to **Settings → Security → Edit Security Setups**.
2. Under Edit Building Blocks, select **LDAP**.
3. Click **Add an LDAP Setup**.
4. The LDAP Server Setup dialog is divided into four parts:

### General Information

- **Setup Name**—This name will be used to identify each particular LDAP Server Setup when creating security templates.
- **Server Address**—Enter the IP Address or the Host Name of the LDAP server where the authentication will be performed.
- **Server Port**—The port used by the Embedded Web Server to communicate with the LDAP server. The default LDAP port is 389.
- **Use SSL/TLS**—From the drop-down menu select **None**, **SSL/TLS** (Secure Sockets Layer/Transport Layer Security), or **TLS**.
- **Userid Attribute**—Type either **`cn`** (common name), **`uid`**, **`userid`**, or **`user-defined`**.
- **Search Base**—The Search Base is the node in the LDAP server where user accounts reside. Multiple search bases may be entered, separated by commas.

  **Note:** A Search Base consists of multiple attributes—such as cn (common name), ou (organizational unit), o (organization), c (country), or dc (domain)—separated by commas.

- **Search Timeout**—Enter a value of from 5 to 30 seconds.
- **Required User Input**—Select either **User ID and Password** or **User ID** to specify which credentials a user must provide when attempting to access a function protected by the LDAP building block.

### Device Credentials

- **Anonymous LDAP Bind**—If selected, the Embedded Web Server will bind with the LDAP server anonymously, and the Distinguished Name and MFP Password fields will be grayed out.
- **Distinguished Name**—Enter the distinguished name of the print server(s).
- **MFP Password**—Enter the password for the print server(s).

### Search specific object classes

- **Person**—Click to select or clear; this specifies that the "person" object class will also be searched.
- **Custom Object Class**—Click to select or clear; the administrator can define up to three custom search object classes (optional).

### LDAP Group Names

- **Configure Groups**—Administrators can associate as many as 32 named groups stored on the LDAP server, by entering identifiers for those groups under the Group Search Base list. Both the Short name for group, and Group Identifier must be provided.
- When creating Security Templates, the administrator can pick groups from this setup for controlling access to device functions.

5 Click **Submit** to save changes, or **Cancel** to return to previous values.

## To edit an existing LDAP setup

1 From the Embedded Web Server Home screen, browse to **Settings → Security → Edit Security Setups**.

2 Under Edit Building Blocks, select **LDAP**.

3 Click a setup from the list.

4 Make any needed changes in the LDAP Configuration dialog.

5 Click **Modify** to save changes, or click **Cancel** to return to previous values.

## To delete an existing LDAP setup

1 From the Embedded Web Server Home screen, browse to **Settings → Security → Edit Security Setups**.

2 Under Edit Building Blocks, select **LDAP**.

3 Select a setup from the list.

4 Click **Delete Entry** to remove the profile, or **Cancel** to return to previous values.

**Notes:**

- Click **Delete List** to delete all LDAP setups in the list.
- An LDAP building block cannot be deleted if it is being used as part of a security template.

## To validate an existing LDAP setup

1. From the Embedded Web Server Home screen, browse to **Settings → Security → Edit Security Setups**.
2. Under Edit Building Blocks, select **LDAP**.
3. Click **Test LDAP Authentication Setup** next to the setup you want to test.

# Using LDAP+GSSAPI

Some administrators prefer authenticating to an LDAP server using *Generic Security Services Application Programming Interface* (GSSAPI) instead of simple LDAP authentication because the transmission is always secure. Instead of authenticating directly with the LDAP server, the user will first authenticate with a Kerberos server to obtain a Kerberos "ticket." This ticket is then presented to the LDAP server using the GSSAPI protocol for access. LDAP+GSSAPI is typically used for networks running Active Directory.

**Notes:**

- LDAP+GSSAPI requires that Kerberos 5 also be configured.
- Supported devices can store a maximum of five unique LDAP + GSSAPI configurations. Each configuration must have a unique name.
- As with any form of authentication that relies on an external server, users will not be able to access protected device functions in the event of an outage that prevents the printer from communicating with the authenticating server.
- To help prevent unauthorized access, users are encouraged to securely end each session by selecting **Log out** on the printer control panel.

## To add a new LDAP+GSSAPI setup

1. From the Embedded Web Server Home screen, browse to **Settings → Security → Edit Security Setups**.
2. Under Edit Building Blocks, select **LDAP+GSSAPI**.
3. Click **Add an LDAP+GSSAPI Setup**.
4. The LDAP+GSSAPI Server Setup dialog is divided into four parts:

### General Information

- **Setup Name**—This name will be used to identify each particular LDAP+GSSAPI Server Setup when creating security templates.
- **Server Address**—Enter the IP Address or the Host Name of the LDAP server where the authentication will be performed.
- **Server Port**—The port used by the Embedded Web Server to communicate with the LDAP server. The default LDAP port is 389.
- **Use SSL/TLS**—From the drop-down menu select **None**, **SSL/TLS** (Secure Sockets Layer/Transport Layer Security), or **TLS**.
- **Userid Attribute**—Enter either **`cn`** (common name), **`uid`**, **`userid`**, or **`user-defined`**.
- **Search Base**—The Search Base is the node in the LDAP server where user accounts reside. Multiple search bases may be entered, separated by commas.

  **Note:** A Search Base consists of multiple attributes—such as cn (common name), ou (organizational unit), o (organization), c (country), or dc (domain)—separated by commas.

- **Search Timeout**—Enter a value of from 5 to 30 seconds.
- **Required User Input**—Select either **User ID and Password** or **User ID** to specify which credentials a user must provide when attempting to access a function protected by the LDAP building block.

### Device Credentials

- **MFP Kerberos Username**—Enter the distinguished name of the print server(s).
- **MFP Password**—Enter the Kerberos password for the print server(s).

### Search specific object classes

- **Person**—Click to select or clear; this specifies that the "person" object class will also be searched.
- **Custom Object Class**—Click to select or clear; the administrator can define up to three custom search object classes (optional).

### LDAP Group Names

- **Configure Groups**—Administrators can associate as many as 32 named groups stored on the LDAP server, by entering identifiers for those groups under the **Group Search Base** list. Both the Short name for group, and Group Identifier must be provided.
- When creating Security Templates, the administrator can pick groups from this setup for controlling access to device functions.

5 Click **Submit** to save changes, or **Cancel** to return to previous values.

## To edit an existing LDAP+GSSAPI setup

1 From the Embedded Web Server Home screen, browse to **Settings → Security → Edit Security Setups**.

2 Under Edit Building Blocks, select **LDAP+GSSAPI**.

3 Select a setup from the list.

4 Make any needed changes in the LDAP Configuration dialog.

5 Click **Modify** to save changes, or **Cancel** to return to previous values.

## To delete an existing LDAP+GSSAPI setup

1 From the Embedded Web Server Home screen, browse to **Settings → Security → Edit Security Setups**.

2 Under Edit Building Blocks, select **LDAP+GSSAPI**.

3 Select a setup from the list.

4 Click **Delete Entry** to remove the profile, or **Cancel** to return to previous values.

**Notes:**

- Click **Delete List** to delete all LDAP+GSSAPI setups in the list.
- An LDAP+GSSAPI building block cannot be deleted if it is being used as part of a security template.

# Configuring Kerberos 5 for use with LDAP+GSSAPI

Though it can be used by itself for user authentication, Kerberos 5 is most often used in conjunction with the LDAP +GSSAPI building block. While only one Kerberos configuration file (krb5.conf) can be stored on a supported device, that krb5.conf file can apply to multiple realms and Kerberos Domain Controllers (KDCs). An administrator must thus anticipate the different types of authentication requests the Kerberos server might receive, and configure the krb5.conf file to handle all such requests.

**Notes:**

- Because only one krb5.conf file is used, uploading or re-submitting a simple Kerberos file will overwrite the configuration file.
- The krb5.conf file can specify a default realm. However, if a realm is not specified in the configuration file, then the first realm specified will be used as the default realm for authentication.
- As with any form of authentication that relies on an external server, users will not be able to access protected device functions in the event of an outage that prevents the printer from communicating with the authenticating server.
- To help prevent unauthorized access, users are encouraged to securely end each session by selecting **Log out** on the printer control panel.

## Creating a simple Kerberos configuration file

1. From the Embedded Web Server Home screen, browse to **Settings → Security → Edit Security Setups**.
2. Under Edit Building Blocks, select **Kerberos 5**.
3. Type the KDC (Key Distribution Center) address or hostname in the **KDC Address** field.
4. Type the number of the port (between 1-88) used by the Kerberos server in the **KDC Port** field.
5. Type the realm (or domain) used by the Kerberos server in the **Realm** field
6. Click **Submit** to save the information as a krb5.conf file on the selected device, or **Reset Form** to reset the fields and start again.

## Uploading a Kerberos configuration file

1. From the Embedded Web Server Home screen, browse to **Settings → Security → Edit Security Setups**.
2. Under Edit Building Blocks, select **Kerberos 5**.
3. Click **Browse** to find and select the krb5.conf file.
4. Click **Submit** to upload the krb5.conf file to the selected device, or **Reset Form** to reset the field and search for a new configuration file.

   **Note:** After you click **Submit**, the Embedded Web Server will automatically test the krb5.conf file to verify that it is functional.

   **Notes:**

   - Click **Delete File** to remove the Kerberos configuration file from the selected device.
   - Click **View File** to view the Kerberos configuration file for the selected device.
   - Click **Test Setup** to verify that the Kerberos configuration file for the selected device is functional.

## Setting date and time

Because Kerberos servers require that key requests bear a recent timestamp (usually within 300 seconds), the printer clock must be in sync or closely aligned with the KDC system clock. Printer clock settings can be updated manually, or set to use *Network Time Protocol* (NTP), to automatically sync with a trusted clock—typically the same one used by the Kerberos server.

1. From the Embedded Web Server Home screen, browse to **Settings → Security → Set Date and Time**.
2. To manage the settings manually, type the correct date and time in **`YYYY-MM-DD HH:MM`** format, and then choose from the Time Zone drop-down list.

   **Notes:**

   - Entering manual settings automatically disables use of NTP.
   - Choosing "(UTC+user) Custom" from the Time Zone list will require configuration of additional settings under Custom Time Zone Setup.
3. If *Daylight Saving Time* (DST) is observed in your area, click the **Automatically Observe DST** check box.
4. If you are located in a non-standard time zone or an area that observes an alternate DST calendar, adjust the Custom Time Zone Setup settings as needed.
5. To sync to an NTP server rather than manage date and time settings manually, click the **Enable NTP** check box, and then type the IP address or hostname of the NTP Server.
6. If the NTP server requires authentication, click the **Enable Authentication** check box, and then use the "Install auth keys" link to browse to the file containing the NTP authentication credentials.
7. Click **Submit** to save changes, or **Reset Form** to restore default values.

# Using NTLM authentication

*NTLM* (Windows NT LAN Manager) is Microsoft's solution for enabling authentication without requiring the transmission of a user's password across a network in clear text. Instead of comparing the user's actual password, the NTLM server and the client generate and compare three encrypted strings based on the user's password.

An administrator can store only one NTLM configuration on a supported device because each device can only be registered to a single NT domain.

**Notes:**

- The NTLM building block can be used in a security template only after a supported device has registered with the NTLM domain.
- The NTLM building block cannot be deleted or unregistered if it is being used as part of a security template.
- As with any form of authentication that relies on an external server, users will not be able to access protected device functions in the event of an outage that prevents the printer from communicating with the authenticating server.
- To help prevent unauthorized access, users are encouraged to securely end each session by selecting **Log out** on the printer control panel.

### Specifying the default user domain for the NTLM server

1. Open the Embedded Web Server home screen using the secure version of the page (with the URL beginning "https://"), rather than an unsecured browsing window.

   **Note:** If you do not connect to the Embedded Web Server using HTTPS, you will not be able to register your device with an NT domain.

2. From the Embedded Web Server Home screen, browse to **Settings → Security → Edit Security Setups**.
3. Under Edit Building Blocks, select **NTLM**.
4. Type the default user domain in the **Default User Domain** field, and then click **Register Domain** to access additional configuration settings.
5. On the Settings screen under Register Domain, provide the credentials appropriate to your NT domain:
   - Domain Name
   - Domain PDC Name (the server name of the Primary Domain Controller)
   - User ID
   - Password
6. Click **Submit**. A status screen will appear with the message "Registering."
   - If registration is successful, the **Manage NTLM Setup** screen will display "Status....Registered."
   - If registration is not successful, the **Manage NTLM Setup** screen will display "Status....Not Registeted."

# Securing access

## Setting a backup password

The Backup Password allows Embedded Web Server administrators to access security menus regardless of the type of security assigned. A backup password can be helpful if other security measures become unavailable, for example, if there is a network communication problem, or an authentication server fails.

**Note:** In some organizations, security policies prohibit the use of "back door" measures such as a backup password. Consult your organization's policies before deploying any security method that might compromise those policies.

### To create a backup password

1. From the Embedded Web Server Home screen, browse to **Settings → Security → Edit Security Setups**.
2. Under Edit Backup Password, select **Backup Password**.
3. Select the **Use Backup Password** box, and then type and re-enter the password.
4. Click **Submit**.

# Setting login restrictions

Many organizations establish login restrictions for information assets such as workstations and servers. Embedded Web Server administrators should verify that printer login restrictions also comply with organizational security policies.

1. From the Embedded Web Server Home screen, browse to **Settings → Security → Miscellaneous Security Settings**.
2. Select **Login Restrictions**.
3. Enter the appropriate login restrictions:
   - **Login failures**—Specify the number of times a user can attempt login before being locked out.
   - **Failure time frame**—Specify the amount of time before lockout takes place.
   - **Lockout time**—Specify the duration of lockout.
   - **Panel Login Timeout**—Specify how long a user may be logged in before being automatically logged off.
   - **Remote Login Timeout**—Specify how long a user may be logged in remotely before being automatically logged off.
4. Click **Submit** to save changes, or **Reset Form** to restore default values.

# Using a password or PIN to control function access

Each Access Control (or Function Access Control), can be set to require No Security (the default), or to use any of the selections available in the drop-down list for that function. For simple authorization-level security (in which individual users are not authenticated), administrators can control access to specific device functions using a password or PIN. Only one method of security can be assigned to each Access Control.

**Note:** To help prevent unauthorized access, users are encouraged to securely end each session by selecting **Log out** on the printer control panel.

1. From the Embedded Web Server Home screen, select **Settings → Security → Edit Security Setups**.
2. Under Edit Access Controls, select **Access Controls**.
3. For each function you want to protect, select a password or PIN from the drop-down list next to the name of that function.
4. Click **Submit** to save changes, or **Reset Form** to cancel all changes.

   Users will now be required to enter the correct code in order to gain access to any function controlled by a password or PIN.

# Using a security template to control function access

## Step 1: Create a building block

1. From the Embedded Web Server Home screen, browse to **Settings → Security → Edit Security Setups**.
2. Under Edit Building Blocks, select the building block (or blocks), appropriate for your environment, and configure as needed.

   For more information on configuring a specific type of building block, see the relevant section(s) under "Configuring building blocks" on page 7.

## Step 2: Create a security template

Once configured, one or two building blocks can be combined with a unique name of up to 128 characters to create a security template. Each device can support up to 140 security templates. Though the names of security templates must be different from one another, building blocks and security templates can share a name.

1. From the Embedded Web Server Home screen, browse to **Settings → Security → Edit Security Setups**.
2. Under Edit Security Templates, select **Security Templates**.
3. Under Manage Security Templates, select **Add a Security Template**.
4. In the Security Templates Name field, type a unique name containing up to 128 characters. It can be helpful to use a descriptive name, such as "Administrator _ Only", or "Common _ Functions _ Template."
5. From the Authentication list, select a method for authenticating users. This list will be populated with the authentication building blocks that have been configured on the device.
6. To use authorization, click **Add authorization**, and then select a building block from the Authorization Setup list. This list will be populated with the authorization building blocks available on the device.

   **Note:** Certain building blocks—such as Passwords and Pins—do not support separate authorization.
7. To use groups, click **Modify Groups**, and then select one or more groups to include in the security template. Hold down the Ctrl key to select multiple groups.
8. Click **Save Template**.

## Step 3: Assign security templates to access controls

1. From the Embedded Web Server Home screen, browse to **Settings → Security → Edit Security Setups**.
2. Select **Access Control**.
3. For each function you want to protect, select the newly created security template from the drop-down list next to the name of that function.
4. Click **Submit** to save changes, or **Reset Form** to cancel all changes.

   Users will now be required to enter the appropriate credentials in order to gain access to any function controlled by the security template.

   **Notes:**

   - To help prevent unauthorized access, users are encouraged to securely end each session by selecting **Log out** on the printer control panel.
   - For a list of individual Access Controls and what they do, see "Menu of Access Controls" on page 29.

## Editing or deleting an existing security template

1. From the Embedded Web Server Home screen, browse to **Settings → Security → Edit Security Setups**.
2. Under Edit Security Templates, select **Security Templates**.
3. Select a security template from the list.
4. Edit the fields as necessary.
5. Click **Modify** to save changes, or **Cancel** to retain previously configured values.

**Notes:**

- Clicking **Delete List** will delete all security templates on the device, regardless of which one is selected. To delete an individual security template, select it from the list, and then click **Delete Entry** in the Settings screen for that template.
- You can only delete a security template if it is not in use; however, security templates currently in use can be edited.

# Scenarios

## Scenario: Printer in a public place

If your printer is located in a public space such as a lobby, and you wish to prevent the general public from using it, a password or PIN can provide simple protection right at the device. Administrators can assign a single password or PIN for all authorized users of the device, or separate codes to protect individual functions. The key to remember is that anyone who knows a password or PIN can access any functions protected by that code.

### Step One: Create a password or PIN

1. From the Embedded Web Server Home screen, browse to **Settings → Security → Edit Security Setups**.
2. Under Edit Building Blocks, select either **Password** or **PIN**, and configure as needed.

For more information on configuring a password or PIN, see the relevant section(s) under "Configuring building blocks" on page 7.

### Step Two: Assign a password or PIN to each access control

After creating one or more codes, determine which device functions need to be protected, and then:

1. From the Embedded Web Server Home screen, browse to **Settings → Security → Edit Security Setups**.
2. Select **Access Control**.
3. For each function you want to protect, select a password or PIN from the drop-down list next to the name of that function, and then click **Submit**.

   Users will now be required to enter the correct code in order to gain access to a function controlled by that code.

## Scenario: Standalone or small office

If your printer is not connected to a network, or you do not use an authentication server to grant users access to devices, Internal Accounts can be created and stored within the Embedded Web Server for authentication, authorization, or both.

### Step One: Set up individual user accounts

1. From the Embedded Web Server Home screen, browse to **Settings → Security → Edit Security Setups**.
2. Under Edit Building Blocks, select **Internal Accounts**, and configure as needed.

   For more information on configuring individual user accounts, see "Setting up internal accounts" on page 8.

### Step 2: Create a security template

1. From the Embedded Web Server Home screen, browse to **Settings → Security → Edit Security Setups**.
2. Under Edit Security Templates, select **Security Templates**.
3. Under Manage Security Templates, select **Add a Security Template**.
4. In the Security Templates Name field, type a unique name containing up to 128 characters. It can be helpful to use a descriptive name, such as "Administrator _ Only", or "Common _ Functions _ Template."
5. From the Authentication list, select a method for authenticating users. This list will be populated with the authentication building blocks which have been configured on the device.
6. To use authorization, click **Add authorization**, and then select a building block from the Authorization Setup list. This list will be populated with the authorization building blocks available on the device.

   **Note:** Certain building blocks—such as PINs and Passwords—do not support separate authorization.
7. To use groups, click **Modify Groups**, and then select one or more groups to include in the security template. Hold down the Ctrl key to select multiple groups.
8. Click **Save Template**.

### Step 3: Assign security templates to access controls

1. From the Embedded Web Server Home screen, browse to **Settings → Security → Edit Security Setups**.
2. Select **Access Control**.
3. For each function you want to protect, select a security template from the drop-down list next to the name of that function.
4. Click **Submit** to save changes, or **Reset Form** to cancel all changes.

   Users will now be required to enter the appropriate credentials in order to gain access to any function controlled by a security template.

## Scenario: Network running Active Directory

On networks running Active Directory, administrators can use the LDAP+GSSAPI capabilities of the Embedded Web Server to take advantage of authentication and authorization services already deployed on the network. User credentials and group designations can be pulled from the existing network, making access to the printer as seamless as other network services.

### Step 1: Collect information about the network

Before configuring the Embedded Web Server to integrate with Active Directory, you will need to know the following:

1. Kerberos configuration information
   - Character encoding (used for passwords)
   - Location of the Kerberos file on the network (if importing a krb5.conf file)
   - If creating a Simple Kerberos Setup:
     - The IP address or hostname of the *Key Distribution Center* (KDC)
     - The KDC port
     - The name of the Realm (or domain) where the KDC is located
   - The Kerberos username (distinguished name) and password assigned to the printer

2 LDAP server information
   - The IP address or hostname of the LDAP server
   - The LDAP server port (the default is 389)
   - A list of up to three object classes stored on the LDAP server, which will be searched for user credentials during authentication (optional)
   - A list of up to 32 groups stored on the LDAP server which will be used to authorize user for access to printer functions

## Step 2: Configure Kerberos setup

1 From the Embedded Web Server Home screen, browse to **Settings → Security → Edit Security Setups**.

2 Under Edit Building Blocks, select **Kerberos 5**.

3 Configure Kerberos settings using the information gathered in step 1.

   For more information on configuring Kerberos, see "Configuring Kerberos 5 for use with LDAP+GSSAPI" on page 13.

## Step 3: Configure LDAP+GSSAPI Settings

1 From the Embedded Web Server Home screen, browse to **Settings → Security → Edit Security Setups**.

2 Under Edit Building Blocks, select **LDAP+GSSAPI**.

3 Click **Add an LDAP+GSSAPI Setup**.

4 Configure LDAP+GSSAPI settings using the information gathered in step 1.

   For more information on configuring LDAP+GSSAPI, see"Using LDAP+GSSAPI" on page 11

## Step 4: Create a security template

1 From the Embedded Web Server Home screen, browse to **Settings → Security → Edit Security Setups**.

2 Under Edit Security Templates, select **Security Templates**.

3 Under Manage Security Templates, select **Add a Security Template**.

4 In the Security Templates Name field, type a unique name containing up to 128 characters. It can be helpful to use a descriptive name, such as "Administrator _ Only", or "Common _ Functions _ Template."

5 From the Authentication Setup list, select the name given to your LDAP+GSSAPI setup.

6 Click **Add authorization**, and then select the name given to your LDAP+GSSAPI setup.

7 To use groups, click **Modify Groups**, and then select one or more of the groups listed in your LDAP+GSSAPI Group Names list. Hold down the Ctrl key to select multiple groups.

8 Click **Save Template**.

## Step 5: Assign security templates to access controls

1 From the Embedded Web Server Home screen, browse to **Settings → Security → Edit Security Setups**.

2 Select **Access Control**.

3 For each function you want to protect, select the newly created security template from the drop-down list next to the name of that function.

4 Click **Submit** to save changes, or **Reset Form** to cancel all changes.

Users will now be required to enter the appropriate credentials in order to gain access to any function controlled by the security template.

# Managing certificates and other settings

## Managing certificates

The Embedded Web Server supports the use of digital certificates to help ensure the integrity of information transmitted to and from your printer, including authentication and group information, as well as document outputs.

### Creating a new certificate

1 From the Embedded Web Server Home screen, browse to **Settings → Security → Certificate Management**.

2 Select **Device Certificate Management**.

3 Click **New**.

4 Enter values in the appropriate fields:

- **Friendly Name**—Type a name for the certificate (64-character maximum).
- **Common Name**—Type a name for the device (128-character maximum).

  **Note:** Leave this field blank to use the hostname for the device.
- **Organization Name**—Type the name of the company or organization issuing the certificate (128-character maximum).
- **Unit Name**—Type the name of the unit within the company or organization issuing the certificate (128-character maximum).
- **Country Name**—Type the country location for the company or organization issuing the certificate (2-character maximum).
- **Province Name**—Type the name of the province where the company or organization issuing the certificate is located (128-character maximum).
- **City Name**—Type the name of the city where the company or organization issuing the certificate is located (128-character maximum).
- **Subject Alternate Name**—Type the alternate name and prefix that conforms to RFC 2459. For example, enter an IP address using the format IP:1.2.3.4, or a DNS address using the format DNS:ldap.company.com. Leave this field blank to use the IPv4 address (128-character maximum).

5 Click **Generate New Certificate** .

### Viewing, downloading, and deleting a certificate

1 From the Embedded Web Server Home screen, browse to **Settings → Security → Certificate Management**.

2 Select **Device Certificate Management**.

3 Select a certificate from the list.

The details of the certificate are displayed in the Device Certificate Management window.

4 From here, you can:

- **Delete**—Remove a previously stored certificate.
- **Download to File**—Download or save the certificate as a .pem file.
- **Download Signing Request**—Download or save the signing request as a .csr file.
- **Install Signed Certificate**—Upload a previously signed certificate.

## Setting certificate defaults

Administrators can set default values for certificates generated for a supported device. The values entered here will be present in all new certificates generated in the Certificate Management task, even though those fields will remain blank on-screen.

1 From the Embedded Web Server Home screen, browse to **Settings → Security → Certificate Management**.

2 Select **Set Certificate Defaults**.

3 Enter values in the appropriate fields:

- **Common Name**—Type a name for the device (128-character maximum).

  **Note:** Leave this field blank to use the domain name for the device.
- **Organization Name**—Type the name of the company or organization issuing the certificate.
- **Unit Name**—Type the name of the unit within the company or organization issuing the certificate.
- **Country Name**—Type the country location for the company or organization issuing the certificate (2-character maximum).
- **Province Name**—Type the name of the province where the company or organization issuing the certificate is located.
- **City Name**—Type the name of the city where the company or organization issuing the certificate is located.
- **Subject Alternate Name**—Type the alternate name and prefix that conforms to RFC 2459. For example, enter an IP address using the format IP:1.2.3.4, or a DNS address using the format DNS:ldap.company.com. Leave this field blank to use the IPv4 address.

  **Note:** All fields accept a maximum of 128 characters, except where noted.

4 Click **Submit**.

## Configuring confidential printing

Users printing confidential or sensitive information may opt to use the confidential print option, which allows print jobs to be PIN-protected so that they remain in the print queue until the user enters a PIN on the operator panel of the device.

1 From the Embedded Web Server Home screen, browse to **Settings → Security → Confidential Print Setup**.

2 Select an option for Max Invalid PIN:

- Select **0** to allow users to enter an incorrect PIN as many times as they choose.
- Select a value of between 2 and 10 to specify the number of times users can enter an incorrect PIN before being locked out.

3 Select an option for Job Expiration:
   - Select **Off** to allow unprinted confidential print jobs to remain in the print queue indefinitely.
   - Select a value of 1 hour, 4 hours, 24 hours, or 1 week to specify the amount of time that an unprinted confidential print job will remain in the print queue before being automatically deleted.

4 Click **Submit** to save changes or **Reset Form** to reset both fields.

# Enabling and disabling USB devices

1 From the Embedded Web Server Home screen, browse to **Settings → Security → Schedule USB Devices**.

2 Under Schedule USB Devices, choose whether to disable all USB devices or Flash drives only.

   **Note:** All scheduled Disable actions will be affected by this setting.

3 Click **Submit**.

4 Use Schedules to enable or disable use of USB devices on certain days or during certain hours. To create a schedule:
   - From the Action list, select Enable or Disable to specify which action should occur at the specified time.
   - From the Time list, select the hour at which the selected action should begin (example: `06:00`, to start at 6 AM).
   - From the Day(s) list, select which day (or days) the schedule should run (example: Weekdays (Mon-Fri)).
   - Click **Add** to save the action to the schedule.
   - Repeat as needed to complete the schedule.

   **Notes:**

   – Use of USB devices is enabled by default.
   – For each Disable schedule entry, you must also create an Enable schedule entry to reactivate use of USB devices.

# Disk wiping

On certain devices, administrators can use disk wiping to remove residual confidential material from the device and free up memory space. Disk wiping uses random data patterns to securely overwrite files stored on the hard drive that have been marked for deletion. Overwriting can be accomplished with a single pass—for a quick wipe—or with multiple passes for greater security. Multi-pass wiping is compliant with the DoD 5220.22-M standard for securely erasing data from a hard disk. Disk wiping can be performed manually, automatically, or on a scheduled basis.

## Setting up disk wiping

1 From the Embedded Web Server Home screen, browse to **Settings → Security → Disk Wiping**.

   **Note:** If you do not see Disk Wiping in the main Security menu, it is not supported on your device.

2 From the Wiping Mode list, select **Off** (for no wiping), **Auto** (for automatic wiping), or **Manual** (for either scheduled or ad-hoc wiping).

   **Notes:**

   - The Scheduled Disk Wiping option will not appear until Manual mode has been selected and submitted.
   - Clicking **Submit** after choosing a Wiping Mode will return you to the main Security menu, where you must again select **Disk Wiping** to make further configuration changes.

3 If you have enabled Manual mode and wish to set up a schedule for disk wiping, select **Scheduled Disk Wiping**.

4 Use the Time and Day(s) lists to designate when disk wiping should occur, and then click **Add**. Repeat as needed to schedule additional times for disk wiping. When finished, use the browser Back button to return to the Disk Wiping setup screen, or use the menu on the left to browse back to **Settings → Security → Disk Wiping**

5 Back on the main Settings screen for Disk Wiping, choose **Single Pass**, or **Multi-pass** for each method of disk wiping (Automatic, Manual, and Scheduled).

6 Click **Submit** to finalize changes.

### Changing or deleting scheduled disk wiping

1 From the Embedded Web Server Home screen, browse to **Settings → Security → Disk Wiping**.

2 Select **Scheduled Disk Wiping**.

3 Choose an existing Start value (the scheduled time and day will appear in the drop-down menus).

- To change scheduled settings, modify the time and day as needed, and then click **Modify** to save changes.
- To delete a scheduled disk wiping, click **Delete Entry**, and on the following screen click **Delete Entry** again to confirm.

## Encrypting the hard disk

Hard disk encryption helps prevent loss of sensitive data in the event your printer—or its hard disk—is stolen. Disk encryption can be turned on only at the device (not through the Embedded Web Server).

1 Turn off the printer using the power switch.

2 Simultaneously press and hold the "2" and "6" keys on the numeric keypad while turning the printer back on. Continue pressing 2 and 6 until the printer status bar reaches %100. This takes approximately one minute.

Once the printer is fully powered up, the printer touch screen should display a list of functions, instead of standard home screen icons such as Copy or Fax.

3 Verify that the printer is in Configuration mode by locating the Exit Configuration button in the lower right corner of the touch screen.

**Note:** On some devices the button will appear as "Exit Config Menu."

4 Press the down arrow to scroll through the configuration menus until you see the Disk Encryption menu selection.

5 Select **Disk Encryption**.

6 From the Disk Encryption menu, select **Enable** to turn on disk encryption, or **Disable** to deactivate it.

**Warning—Potential Damage:** Enabling or disabling disk encryption will erase the contents of the hard disk.

7 A message will appear asking you to confirm the action: `Contents will be lost. Continue?`

- Select **Yes** to proceed with disk wiping and encryption. Encryption takes approximately two minutes, and a status bar will indicate the progress of the encryption task.

  After the disk has been encrypted, you will be returned to the Enable/Disable screen.

  **Warning—Potential Damage:** Do not power off the printer during the encryption process.
- Select **No** to cancel and return to the Enable/Disable screen.

8 To finish, press **Back**, and then **Exit Configuration** (or Exit Config Menu).

The printer will power-on reset, and then return to normal operating mode.

# Configuring security audit log settings

The security audit log allows administrators to monitor security-related events on a device including, among others, user authorization failures, successful administrator authentication, or Kerberos files being uploaded to a device. By default, security logs are stored on the device, but may also be transmitted to a network syslog server for further processing or storage.

1. From the Embedded Web Server Home screen, select **Settings → Security → Security Audit Log**.
2. Select **Enable Audit** to activate security audit logging (syslog).
3. To transmit log events to a network syslog server, type the IP address or hostname of the Remote Syslog Server, and then select the **Enable Remote Syslog** check box.

   **Note:** The Enable Remote Syslog check box will be grayed out until an IP address or hostname is entered.
4. Type the Remote Syslog Port number used on the destination server. The default value is port 514.
5. From the Remote Syslog Method list, select **Normal UDP** (to send log messages and events using a lower-priority transmission protocol) or **Stunnel** (if implemented on the destination server).
6. From the Remote Syslog Facility list, select a facility code for events to be logged to on the destination server. All events sent from the device will be tagged with the same facility code to aid in sorting and filtering by network monitoring or intrusion detection software.

   **Note:** Steps 4 through 6 are valid only if Remote Syslog is enabled.
7. From the **Severity of events to log** list, select the priority level cutoff (0-7) for logging messages and events. 0 is the highest severity, and 7 is the lowest. The chosen severity level and anything higher will be logged (e.g. if level "4 - Warning" is chosen, severity levels 0-4 will be logged).
8. To send all events regardless of severity to the remote server, select the **Remote Syslog non-logged events** check box.
9. To have administrators automatically notified of certain log events, type one or more E-mail addresses (separated by commas) in the Admin's e-mail address field, and then choose from the following options:

   **E-mail log cleared alert**—When the **Delete Log** button is clicked

   **E-mail log wrapped alert**—When the log becomes full and begins to overwrite the oldest entries

   **Log full behavior**—Wrap over oldest entries, or E-mail log then delete

   **E-mail % full alert**—When log storage space reaches a certain percentage of capacity

   **% full alert level (1-99%)**—How full the log must be before an alert is triggered

   **E-mail log exported alert**—When the log file is exported

   **E-mail log settings changed alert**—When log settings are changed

   **Note:** In order to use E-mail alerts, you must click **Submit** to save changes, and then follow the **Setup E-mail Server** link to configure SMTP settings.
10. Click **Submit** to save changes, or **Reset Form** to restore default values.

## E-mail server setup

1. From the Security Audit Log main screen, select **Setup E-mail Server**.
2. Under SMTP Setup, type the IP address or hostname of the Primary SMTP Gateway the device will use for sending E-mail.

3 Type the Primary SMTP Gateway Port number of the destination server. The default value is port 25.

4 If using a secondary or backup SMTP server, enter the IP address/hostname and SMTP port for that server.

5 For SMTP Timeout, type the number of seconds (5-30) the device will wait for a response from the SMTP server before timing out. The default is 30 seconds.

6 To receive responses to messages sent from the printer (in case of failed or bounced messages), type the Reply Address .

7 From the Use SSL list, select **Disabled**, **Negotiate**, or **Required** to specify whether E-mail will be sent using an encrypted link.

8 If your SMTP server requires user credentials, select an authentication method from the SMTP Server Authentication list. The default is "No authentication required."

9 From the Device-Initiated E-mail list, select **None** for no authentication, or **Use Device SMTP Credentials** if authentication is required.

10 From the User-Initiated E-mail list, select **None** for no authentication, or **Use Device SMTP Credentials**, **Use Session User ID and Password**, **Use Session E-mail address and Password**, or **Prompt user** if authentication is required.

11 If the device must provide credentials in order to send E-mail, enter the information appropriate for your network under Device Credentials.

### Viewing or deleting the security audit log

- To view or save a text file of the current syslog, click **Export Log**.
- To delete the current syslog, click **Delete Log**.

## Configuring 802.1x authentication

Though normally associated with wireless network connections, 802.1x authentication is also used on wired networks to create port-based connections.

**Note:** If using digital certificates to establish a secure connection to the authentication server, you must configure them on the printer before changing 802.1x authentication settings. For more information on configuring digital certificates, see "Managing certificates" on page 21.

1 From the Embedded Web Server Home screen, browse to **Settings → Security → 802.1x**.

2 Under 802.1x Authentication:
   - Select the **Active** check box to enable 802.1x authentication.
   - Type the login name and password the printer will use to log in to the authentication server.
   - Select the **Validate Server Certificate** check box to require verification of the security certificate on the authenticating server.

     **Note:** Server certificate validation is integral to TLS (Transport Layer Security), PEAP (Protected Extensible Authentication Protocol), and TTLS (Tunneled Transport Security Layer).
   - Select the **Enable Event Logging** check box to log 802.1x authentication-related activity.
   - From the **802.1x Device Certificate** list, choose the digital certificate you want to use. If only one certificate has been installed, **default** will be the only choice listed.

3 Under Allowable Authentication Mechanisms, choose which authentication protocols the printer will recognize by clicking the check box next to each applicable protocol.

4 From the **TTLS Authentication Method** list, choose which authentication method will be accepted through the secure tunnel created between the authentication server and the printer.

5 Click **Submit** to save the changes, or **Reset Form** to restore the default settings.

**Note:** Changes made to settings marked with an asterisk (*) will cause the print server to reset.

# Setting up SNMP

*Simple Network Management Protocol* (SNMP) is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. The Embedded Web server allows administrators to configure settings for SNMP versions 1 through 3.

## SNMP Version 1, 2c

1 From the Embedded Web Server Home screen, browse to **Settings → Security → SNMP**.

2 Under SNMP Version 1, 2c, select the **Enabled** check box.

3 To allow SNMP variables to be set, select the **Allow SNMP Set** check box.

4 Type a name to be used for the SNMP Community identifier (the default community name is **`public`**).

5 To facilitate the automatic installation of device drivers and other printing applications, select the **Enable PPM Mib** (Printer Port Monitor MIB) check box.

6 Click **Submit** to finalize changes, or **Reset Form** to restore default values.

## SNMP Version 3

1 From the Embedded Web Server Home screen, browse to **Settings → Security → SNMP**.

2 Under SNMP Version 3, select the **Enabled** check box.

3 To allow remote installation and configuration changes as well as device monitoring, type an SNMPPv3 Read/Write User name and Password in the appropriate fields.

4 To allow device monitoring only, type an SNMPv3 Read Only User name and Password in the appropriate fields.

5 From the SNMPv3 Minimum Authentication Level list, select **No Authentication, No Privacy**, **Authentication, No Privacy**, or **Authentication, Privacy**.

6 From the SNMPv3 Authentication Hash list, select **MD5** or **SHA1**.

7 From the SNMPv3 Privacy Algorithm list, select **DES**, **AES-128**, **AES-192**, or **AES-256**.

8 Click **Submit** to save changes, or **Reset Form** to restore default values.

## Setting SNMP Traps

After configuring SNMP Version 1, 2c or SNMP Version 3, you can further customize which alerts are sent to the network management system by designating SNMP “traps”, or events that trigger an alert message.

1 From the Embedded Web Server Home screen, browse to **Settings → Security → SNMP**.

2 Click **Set SNMP Traps**.

3 From the IP Address list, click one of the blank IP address entries (shown as **0.0.0.0**).

4 Under Trap Destination, type the IP address of the network management server or monitoring station, and then click the check box next to each condition that should generate an alert.

5 Click **Submit** to save changes, or **Reset Form** to clear all fields.

## Enabling the security reset jumper

The Security Reset Jumper is a hardware jumper located on the motherboard. Administrators can use the Embedded Web Server to specify the effect of using this jumper.

1 From the Embedded Web Server Home screen, browse to **Settings → Security → Miscellaneous Security Settings**.

2 From the Security Reset Jumper list , select **No Effect** (to remove access to *all* security menus—use with caution), **Access controls = "No security"** (to remove security only from function access controls), or **Reset factory security defaults** (to return all security settings to default values).

3 Click **Submit** to save the changes.

**Warning—Potential Damage:** If "No Effect" is chosen and the password (or other applicable credential) is lost, you will not be able to access the security menus. To regain access to the security menus, a service call will be required to replace the device RIP card (motherboard).

# Appendix

## Menu of Access Controls

Depending on device type and installed options, some Access Controls (referred to on some devices as Function Access Controls) may not be available for your printer.

| Function Access Control | What it does |
|---|---|
| Address Book | Controls the ability to perform address book searches in the Scan to Fax and Scan to Email functions |
| Change Language from Home Screen | Controls access to the Change Language feature from the printer control panel |
| Color Dropout | Controls the ability to use the Color Dropout feature for scan and copy functions |
| Configuration Menu | Protects access to the Configuration Menu |
| Copy Color Printing | Controls the ability to perform color copy functions. Users who are denied will have their copy jobs output in black and white |
| Copy Function | Controls the ability to use the Copy function |
| Create Bookmarks at the Device | Controls the ability to create new bookmarks from the printer control panel |
| Create Bookmarks Remotely | Controls the ability to create new bookmarks from the Bookmark Setup section of the Settings menu in the Embedded Web Server |
| Create Profiles | Controls the ability to create new profiles |
| E-mail Function | Controls access to the Scan to Email function |
| eSF Configuration | Controls access to the configuration of any installed eSF applications |
| Fax Function | Controls access to the Scan to Fax function |
| Firmware Updates | Controls the ability to update firmware from any source other than a flash drive. Firmware files which are received via FTP, the Embedded Web Server, etc., will be ignored (flushed) when this function is protected. |
| Flash Drive Color Printing | Controls the ability to print color from a flash drive. Users who are denied will have their print jobs output in black and white. |
| Flash Drive Firmware Updates | Controls the ability to update firmware from a flash drive |
| Flash Drive Print | Controls the ability to print from a flash drive |
| Flash Drive Scan | Controls the ability to scan documents to a flash drive |
| FTP Function | Controls access to the Scan to FTP function |
| Held Jobs Access | Protects access to the Held Jobs function |
| Manage Shortcuts at the Device | Protects access to the Manage Shortcuts section of the Settings menu on the printer control panel |
| Manage Shortcuts Remotely | Protects access to the Manage Shortcuts item of the Settings menu from the Embedded Web Server |

| Function Access Control | What it does |
|---|---|
| Network Ports/Menu at the Device | Protects access to the Network/Ports section of the Settings menu from the printer control panel |
| Network Ports/Menu Remotely | Protects access to the Network/Ports section of the Settings menu from the Embedded Web Server |
| NPA Network Adapter Setting Changes | When disabled, all network adaptor NPA settings change commands are ignored |
| Operator Panel Lock | Protects access to the Operator Panel Lock. Users who are denied access cannot enable or disable the printer control panel lock. |
| Option Card Configuration at the Device | Controls access to the Option Card Configuration section of the Settings menu from the printer control panel. This applies only when an Option Card with configuration options is installed in the device. |
| Option Card Configuration Remotely | Controls access to the Option Card Configuration item of the Settings menu from the Embedded Web Server. This applies only when an Option Card with configuration options is installed in the device. |
| Paper Menu at the Device | Protects access to the Paper menu from the printer control panel. |
| Paper Menu Remotely | Protects access to the Paper menu from the Embedded Web Server. |
| PictBridge Printing | Controls ability to print from an attached PictBridge capable digital camera. |
| PJL Device Setting Changes | When disabled, all device settings changes requested by incoming print jobs are ignored. |
| Release Held Faxes | Controls the ability to release (print) Held Faxes. |
| Remote Certificate Management | When disabled, it is no longer possible to manage certificates using remote management tools. Certificate Management is limited to the operations available from the printer control panel and Embedded Web Server. |
| Remote Management | Controls access to printer settings and functions by remote management tools such as MarkVision™ Professional. When protected, no printer configuration setting can be altered except through a secured communication channel (such as that provided by a properly configured installation of MarkVision Professional). |
| Reports Menu at the Device | Protects access to the Reports menu from the printer control panel |
| Reports Menu Remotely | Protects access to the Reports menu from the Embedded Web Server |
| Security Menu at the Device | Protects access to the Security menu from the printer control panel |
| Security Menu Remotely | Protects access to the Security menu from the Embedded Web Server |
| Service Engineer Menus at the Device | Protects access to the Sevice Engineer menu from the printer control panel |
| Service Engineer Menus Remotely | Protects access to the Service Engineer menu from the Embedded Web Server |
| Settings Menu at the Device | Protects access to the General and Print Settings sections of the Settings menu from the printer control panel |
| Settings Menu Remotely | Protects access to the General and Print Settings items of the Settings menu from the Embedded Web Server |
| Solution 1–10 | The Solution 1 through Solution 10 Access Controls can be assigned to installed eSF applications and/or profiles created by LDSS. The Access Control for each Solution is assigned in the creation or configuration of the application or profile. |

| Function Access Control | What it does |
|---|---|
| Supplies Menu at the Device | Protects access to the Supplies menu from the printer control panel |
| Supplies Menu Remotely | Protects access to the Supplies menu from the Embedded Web Server |
| User Profiles | Controls access to Profiles, such as scanning shortcuts, workflows, or eSF applications |
| Web Import/Export Settings | Controls the ability to import and export printer settings files (UCF files) from the Embedded Web Server |

# Notices

This product includes software developed by the Apache Software Foundation (**http://www.apache.org**).

## The Apache Software License, Version 1.1



Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment:

   "This product includes software developed by the Apache Software Foundation (http://www.apache.org/)."

   Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
4. The names "Apache" and "Apache Software Foundation", "Jakarta-Oro" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.
5. Products derived from this software may not be called "Apache" or "Jakarta-Oro", nor may "Apache" or "Jakarta-Oro" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see **http://www.apache.org/**

## Apache License Version 2.0, January 2004

**http://www.apache.org/licenses/**

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

**1** Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

**2** Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

**3** Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:
   a. (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
   b. (b) You must cause any modified files to carry prominent notices stating that You changed the files; and
   c. (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
   d. (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

   You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.
5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.
6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.
7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.
8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.
9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

### APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

**http://www.apache.org/licenses/LICENSE-2.0**

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

## GNU Lesser General Public License

View the GNU Lesser General Public License online at **http://www.gnu.org/licenses/lgpl.html**.

## LEXMARK SOFTWARE LICENSE AGREEMENT

PLEASE READ CAREFULLY BEFORE INSTALLING AND/OR USING THIS SOFTWARE: This Software License Agreement ("License Agreement") is a legal agreement between you (either an individual or a single entity) and Lexmark International, Inc. ("Lexmark") that, to the extent your Lexmark product or Software Program is not otherwise subject to a written software license agreement between you and Lexmark or its suppliers, governs your use of any Software Program installed on or provided by Lexmark for use in connection with your Lexmark product. The term "Software Program" includes machine-readable instructions, audio/visual content (such as images and recordings), and associated media, printed materials and electronic documentation.

BY USING AND/OR INSTALLING THIS SOFTWARE, YOU AGREE TO BE BOUND BY ALL THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. IF YOU DO NOT SO AGREE, DO NOT INSTALL, COPY, DOWNLOAD, OR OTHERWISE USE THE SOFTWARE PROGRAM. IF YOU DO NOT AGREE WITH THE TERMS OF THIS LICENSE AGREEMENT, PROMPTLY RETURN THE PRODUCT UNUSED AND REQUEST A REFUND OF THE AMOUNT YOU PAID. IF YOU ARE INSTALLING THIS SOFTWARE PROGRAM FOR USE BY OTHER PARTIES, YOU AGREE TO INFORM THE USERS THAT USE OF THE SOFTWARE PROGRAM INDICATES ACCEPTANCE OF THESE TERMS.

**1** STATEMENT OF LIMITED WARRANTY. Lexmark warrants that the media (e.g., diskette or compact disk) on which the Software Program (if any) is furnished is free from defects in materials and workmanship under normal use during the warranty period. The warranty period is ninety (90) days and commences on the date the Software Program is delivered to the original end-user. This limited warranty applies only to Software Program media purchased new from Lexmark or an Authorized Lexmark Reseller or Distributor. Lexmark will replace the Software Program should it be determined that the media does not conform to this limited warranty.

**2** DISCLAIMER AND LIMITATION OF WARRANTIES. EXCEPT AS PROVIDED IN THIS LICENSE AGREEMENT AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, LEXMARK AND ITS SUPPLIERS PROVIDE THE SOFTWARE PROGRAM "AS IS" AND HEREBY DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, TITLE, NON-INFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND ABSENCE OF VIRUSES, ALL WITH REGARD TO THE SOFTWARE PROGRAM. This Agreement is to be read in conjunction with certain statutory provisions, as that may be in force from time to time, that imply warranties or conditions or impose obligations on Lexmark that cannot be excluded or modified. If any such provisions apply, then to the extent Lexmark is able, Lexmark hereby limits its liability for breach of those provisions to one of the following: replacement of the Software Program or reimbursement of the price paid for the Software Program.

**3** LICENSE GRANT. Lexmark grants you the following rights provided you comply with all terms and conditions of this License Agreement:

**a** Use. You may Use one copy of the Software Program. The term "Use" means storing, loading, installing, executing, or displaying the Software Program. If Lexmark has licensed the Software Program to you for concurrent use, you must limit the number of authorized users to the number specified in your agreement with Lexmark. You may not separate the components of the Software Program for use on more than one computer. You agree that you will not Use the Software Program, in whole or in part, in any manner that has the effect of overriding, modifying, eliminating, obscuring, altering or de-emphasizing the visual appearance of any trademark, trade name, trade dress or intellectual property notice that appears on any computer display screens normally generated by, or as a result of, the Software Program.

**b** Copying. You may make one (1) copy of the Software Program solely for purposes of backup, archiving, or installation, provided the copy contains all of the original Software Program's proprietary notices. You may not copy the Software Program to any public or distributed network.

**c** Reservation of Rights. The Software Program, including all fonts, is copyrighted and owned by Lexmark International, Inc. and/or its suppliers. Lexmark reserves all rights not expressly granted to you in this License Agreement.

**d** Freeware. Notwithstanding the terms and conditions of this License Agreement, all or any portion of the Software Program that constitutes software provided under public license by third parties ("Freeware") is licensed to you subject to the terms and conditions of the software license agreement accompanying such Freeware, whether in the form of a discrete agreement, shrink-wrap license, or electronic license terms at the time of download. Use of the Freeware by you shall be governed entirely by the terms and conditions of such license.

**4** TRANSFER. You may transfer the Software Program to another end-user. Any transfer must include all software components, media, printed materials, and this License Agreement and you may not retain copies of the Software Program or components thereof. The transfer may not be an indirect transfer, such as a consignment. Prior to the transfer, the end-user receiving the transferred Software Program must agree to all these License Agreement terms. Upon transfer of the Software Program, your license is automatically terminated. You may not rent, sublicense, or assign the Software Program except to the extent provided in this License Agreement.

**5** UPGRADES. To Use a Software Program identified as an upgrade, you must first be licensed to the original Software Program identified by Lexmark as eligible for the upgrade. After upgrading, you may no longer use the original Software Program that formed the basis for your upgrade eligibility.

**6** LIMITATION ON REVERSE ENGINEERING. You may not alter, reverse engineer, reverse assemble, reverse compile or otherwise translate the Software Program, except as and to the extent expressly permitted to do so by applicable law for the purposes of inter-operability, error correction, and security testing. If you have such statutory rights, you will notify Lexmark in writing of any intended reverse engineering, reverse assembly, or reverse compilation. You may not decrypt the Software Program unless necessary for the legitimate Use of the Software Program.

**7** ADDITIONAL SOFTWARE. This License Agreement applies to updates or supplements to the original Software Program provided by Lexmark unless Lexmark provides other terms along with the update or supplement.

**8** LIMITATION OF REMEDIES. To the maximum extent permitted by applicable law, the entire liability of Lexmark, its suppliers, affiliates, and resellers, and your exclusive remedy shall be as follows: Lexmark will provide the express limited warranty described above. If Lexmark does not remedy defective media as warranted, you may terminate your license and your money will be refunded upon the return of all of your copies of the Software Program.

**9** LIMITATION OF LIABILITY. To the maximum extent permitted by applicable law, for any claim arising out of Lexmark's limited warranty, or for any other claim whatsoever related to the subject matter of this Agreement, Lexmark's liability for all types of damages, regardless of the form of action or basis (including contract, breach, estoppel, negligence, misrepresentation, or tort), shall be limited to the greater of $5,000 or the money paid to Lexmark or its authorized remarketers for the license hereunder for the Software Program that caused the damages or that is the subject matter of, or is directly related to, the cause of action.

IN NO EVENT WILL LEXMARK, ITS SUPPLIERS, SUBSIDIARIES, OR RESELLERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, EXEMPLARY, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING BUT NOT LIMITED TO LOST PROFITS OR REVENUES, LOST SAVINGS, INTERRUPTION OF USE OR ANY LOSS OF, INACCURACY IN, OR DAMAGE TO, DATA OR RECORDS, FOR CLAIMS OF THIRD PARTIES, OR DAMAGE TO REAL OR TANGIBLE PROPERTY, FOR LOSS OF PRIVACY ARISING OUT OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE PROGRAM, OR OTHERWISE IN CONNECTION WITH ANY PROVISION OF THIS LICENCE AGREEMENT), REGARDLESS OF THE NATURE OF THE CLAIM, INCLUDING BUT NOT LIMITED TO BREACH OF WARRANTY OR CONTRACT, TORT (INCLUDING NEGLIGENCE OR STRICT LIABILITY), AND EVEN IF LEXMARK, OR ITS SUPPLIERS, AFFILIATES, OR REMARKETERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR FOR ANY CLAIM BY YOU BASED ON A THIRD-PARTY CLAIM, EXCEPT TO THE EXTENT THIS EXCLUSION OF DAMAGES IS DETERMINED LEGALLY INVALID. THE FOREGOING LIMITATIONS APPLY EVEN IF THE ABOVE-STATED REMEDIES FAIL OF THEIR ESSENTIAL PURPOSE.

**10** TERM. This License Agreement is effective unless terminated or rejected. You may reject or terminate this license at any time by destroying all copies of the Software Program, together with all modifications, documentation, and merged portions in any form, or as otherwise described herein. Lexmark may terminate your license upon notice if you fail to comply with any of the terms of this License Agreement. Upon such termination, you agree to destroy all copies of the Software Program together with all modifications, documentation, and merged portions in any form.

**11** TAXES. You agree that you are responsible for payment of any taxes including, without limitation, any goods and services and personal property taxes, resulting from this Agreement or your Use of the Software Program.

**12** LIMITATION ON ACTIONS. No action, regardless of form, arising out of this Agreement may be brought by either party more than two years after the cause of action has arisen, except as provided under applicable law.

**13** APPLICABLE LAW. This Agreement is governed non-exclusively by the laws of the country in which you acquired the Software Program (or, if that country has a federal system of government, then this Agreement will be governed by the laws of the political subdivision in which you acquired the Software). If you acquired the Software in the United States, the laws of the Commonwealth of Kentucky shall govern. No choice of law rules in any jurisdiction will apply.

**14** UNITED STATES GOVERNMENT RESTRICTED RIGHTS. The Software has been developed entirely at private expense and is provided with RESTRICTED RIGHTS. Use, duplication and disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and in similar FAR provisions (or any equivalent agency regulation or contract clause).

**15** CONSENT TO USE OF DATA. You agree that Lexmark, its affiliates, and agents may collect and use information you provide in relation to support services performed with respect to the Software Program and requested by you. Lexmark agrees not to use this information in a form that personally identifies you except to the extent necessary to provide such services.

**16** EXPORT RESTRICTIONS. You may not (a) acquire, ship, transfer, or reexport, directly or indirectly, the Software Program or any direct product therefrom, in violation of any applicable export laws or (b) permit the Software Program to be used for any purpose prohibited by such export laws, including, without limitation, nuclear, chemical, or biological weapons proliferation.

**17** CAPACITY AND AUTHORITY TO CONTRACT. You represent that you are of the legal age of majority in the place you sign this License Agreement and, if applicable, you are duly authorized by your employer or principal to enter into this contract.

**18** ENTIRE AGREEMENT. This License Agreement (including any addendum or amendment to this License Agreement that is included with the Software Program) is the entire agreement between you and Lexmark relating to the Software Program. Except as otherwise provided for herein, these terms and conditions supersede all prior or contemporaneous oral or written communications, proposals, and representations with respect to the Software Program or any other subject matter covered by this License Agreement (except to the extent such extraneous terms do not conflict with the terms of this License Agreement, any other written agreement signed by you and Lexmark relating to your Use of the Software Program). To the extent any Lexmark policies or programs for support services conflict with the terms of this License Agreement, the terms of this License Agreement shall control.

# Glossary of Security Terms

| | |
|---|---|
| **Access Controls** | Settings that control whether individual device menus, functions, and settings are available, and to whom. Also referred to as Function Access Controls on some devices. |
| **Authentication** | A method for securely ientifying a user. |
| **Authorization** | A method for specifying which functions are available to a user, i.e. what the user is allowed to do. |
| **Building Block** | Authentication and Authorization tools used in the Embedded Web Server. They include: password, PIN, Internal accounts, LDAP, LDAP+GSSAPI, Kerberos 5, and NTLM. |
| **Group** | A collection of users sharing common characteristics. |
| **Security Template** | A profile created and stored in the Embedded Web Server, used in conjunction with Access Controls to manage device functions. |

# Index