Embedded Web Server — Security

Administrator's Guide

C54x, C73x, C74x, C792, C925, C950, E26x, E36x, E46x, T65x, W850, X264, X36x, X46x, X54x, X65x, X73x, X74x, X79x, X86x, X925, X95x

November 2012 **www.lexmark.com**

3077716-001

Contents

Security devices covered in this guide.....5

Simple security devices.....5

Advanced security devices.....5

Using security features in the Embedded Web Server.....6

Understanding the basics.....6

Authentication and Authorization.....6

Groups.....8

Access Controls.....8

Security Templates.....8

Limiting access with Basic Security Setup.....9

Configuring building blocks.....9

Creating a password for advanced security setup.....9

Creating a password through Web Page Password Protect.....10

Creating a PIN for advanced security setup.....10

Creating a PIN through Panel PIN Protect.....11

Setting up internal accounts.....11

Connecting your printer to an Active Directory domain.....12

Using LDAP.....14

Using LDAP+GSSAPI.....16

Configuring Kerberos 5 for use with LDAP+GSSAPI.....18

Using NTLM authentication.....20

Securing access.....21

Setting a backup password.....21

Setting login restrictions.....21

Using a security template to control function access.....21

Managing certificates and other settings.....23

Installing a Certificate Authority certificate on the device.....23

Configuring the device for certificate information.....24

Creating a new certificate.....25

Viewing, downloading, and deleting a certificate.....25

Setting certificate defaults.....26

Configuring confidential printing.....26

Enabling and disabling USB devices.....27

Disk wiping.....27

Configuring security audit log settings.....28

Configuring 802.1x authentication.....30

Setting up SNMP.....31

Configuring the TCP/IP port access setting.....32

Configuring your IP security settings.....32

Enabling the security reset jumper 33
Securing the hard disk and other installed memory 34
Statement of Volatility 34
Erasing volatile memory 35
Erasing non-volatile memory 35
Completely erasing printer hard disk memory 35
Configuring printer hard disk encryption 36
Scenarios 37
Scenario: Printer in a public place 37
Scenario: Standalone or small office 38
Scenario: Network running Active Directory 39

Appendix 41

Glossary of Security Terms 50

Index 51

Security devices covered in this guide

There are two levels of security supported based on the product definition. For a complete list of available functionality, see “Authentication and Authorization” on page 6.

Simple security devices

C540, C543, C544, C546, C746, E260d, E260dn, E360d, E360dn, X264dn, X363dn, X364dn, X364dw, X543, X544, X546dtn

Advanced security devices

C73x, C748, C792, C925, C950, E460dn, E460dw, E462dtn, T650, T652, T654, T656, W850, X464de, X466, X548de, X548dte, X65x, X73x, X74x, X792, X796, X86x, X925, X950, X952, X954

Using security features in the Embedded Web Server

Lexmark Embedded Web Server represents an evolution in keeping document outputs safe and confidential in today's busy environments. With 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 that administrators can use to build secure and flexible profiles, restricting 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 to define who is allowed to use the printer, and which functions those users are allowed to access. Available components include Authentication, Authorization, and Groups.

Create a plan that identifies who the users will be and what they will need to do before configuring printer security. Items to consider might include:

- The location of the printer and whether authorized persons have access to that area
- Sensitive documents that will be sent to or stored on the printer
- Information security policies of your organization.

For additional information on business solutions security, see *http://www1.lexmark.com/en_US/solutions/business-solutions/security/index.shtml*.

Authentication and Authorization

Authentication is the method by which a system securely identifies a user.

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.”

There are two levels of security that are supported based on the product definition. The simplest level security only supports internal device authentication and authorization methods. The more advanced level security permits internal as well as external authentication and authorization as well as additional restriction capability for management, function, and solution access. Advanced security is supported for those devices that permit the installation of additional solutions to the device.

Simple security utilizes the “Panel PIN Protect” to restrict user access to the printer control panel and the “Web Page Password Protect” to restrict admin access to the device. For more information, see “Creating a PIN through Panel PIN Protect” on page 11 and “Creating a password through Web Page Password Protect” on page 10.

Advanced level security devices support PIN and password restrictions in addition to the other authentication and authorization specified. Most of this document will describe advanced security devices.

Security support summary

√ = Supported X = Not supported		
Function	**Simple security devices**	**Advanced security devices**
Panel PIN Protect	√	X
PIN Protection	X	√
Web Page Password Protect	√	X
Password Protection	X	√
Internal Accounts (Username and Username/Password)	X	√
Groups (internal)	X	√
LDAP	X	√
LDAP+GSSAPI	X	√
Kerberos 5	X	√
Active Directory	X	√
Limited access controls	√	X
Access controls (complete)	X	√
Security Templates	X	√
Basic Security Setup	X	√

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

- PIN or Panel PIN Protect
- Password or Web Page Password Protect
- Internal accounts
- LDAP
- LDAP+GSSAPI
- Kerberos 5 (used only in conjunction with LDAP+GSSAPI)
- Active Directory

To provide low-level security, you can use either PIN and Password, or Panel PIN Protect and Web Page Password Protect for some printer models, 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 if 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 cannot 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.

Note: The default settings do not contain any authentication or authorization building blocks, which means that everyone has unrestricted access to the Embedded Web Server.

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 “Appendix C: Access controls” on page 41.

Security Templates

Some scenarios call for only limited 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 for each access control.

Limiting access with Basic Security Setup

Use Basic Security Setup to limit access to the Embedded Web Server security settings and the configuration menus on the printer control panel. This selection allows the definition of simple internal device security authentication methods.

Notes:

- This feature is available only in select printer models.
- The default settings do not contain any authentication or authorization building blocks, which means that everyone has unrestricted access to the Embedded Web Server.

Applying Basic Security Setup

1. From the Embedded Web Server, click **Settings** > **Security** > **Security Setup**.
2. From the Authentication Type drop-down list, select one of the following:
   - **PIN**—Enter a PIN number. Each PIN must be 4–16 digits in length.
   - **Password**—Type a name for the password. Each password must have a unique name containing up to 128 UTF-8 characters.
   - **User ID and Password**—Type a unique user ID, and then type a name for the password. Each password must have a unique name containing up to 128 UTF-8 characters.
3. Click **Apply Basic Security Setup**.

   Note: Applying this setup may overwrite a previous configuration.

The new settings will be submitted. The next time you access Security Setup, you will be required to enter the appropriate authentication information.

Modifying or removing Basic Security Setup

1. From the Embedded Web Server, click **Settings** > **Security** > **Security Setup**.
2. Enter the appropriate authentication information to gain access to Security Setup.
3. Under Modify or Remove Basic Security Setup, enter your new authentication information.
4. Click **Modify Basic Security Setup** to enter your new authentication information to gain access to Security Setup, or click **Remove Basic Security Setup** to remove all authentication requirements.

Configuring building blocks

Creating a password for advanced security setup

Notes:

- This is available only in select printer models.
- The Embedded Web Server can store a combined total of 250 user-level and administrator-level passwords on each supported device.

1. From the Embedded Web Server, click **Settings** > **Security** > **Security Setup**.
2. Under Advanced Security Setup, click **Password**.

3 Under Manage Passwords, select **Add a Password**.

4 Type a name for the password in the Setup Name box.

Note: Each password must have a unique name containing up to 128 UTF-8 characters (example: “Copy Lockout Password”).

5 Type a password in the appropriate box, and then retype the password to confirm it.

6 If the password will be used as the Administrator password, then select **Admin Password**.

Note: Administrator-level passwords override normal passwords. If a function or setting is protected by a normal password, then 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 password through Web Page Password Protect

Notes:

- This is available only in low-level-security printers.
- The Embedded Web Server can store a combined total of 250 user-level and administrator-level passwords on each supported device.

1 From the Embedded Web Server, click **Settings** > **Security** > **Web Page Password Protect**.

2 Under “Basic Security Setup: Create User Password,” type a password in the appropriate box, and then retype the password to confirm it.

3 Under “Basic Security Setup: Create Admin Password,” type a password in the appropriate box, and then retype the password to confirm it.

Note: Administrator-level passwords override normal passwords. If a function or setting is protected by a normal password, then any administrator-level password will also grant access.

4 Click **Modify**.

Note: To edit a password, change the password, and then click **Modify**. To delete the password, click **Delete Entry**.

Creating a PIN for advanced security setup

Note: This is available only in select printer models.

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.

1 From the Embedded Web Server, click **Settings** > **Security** > **Security Setup**.

2 Under Advanced Security Setup, click **PIN** > **Add a PIN**.

3 Type the name of the PIN configuration in the Setup Name box.

Note: Each PIN must have a unique name containing up to 128 UTF-8 characters (example: “Copy Lockout PIN”).

4 Enter a PIN in the appropriate box, and then reenter the PIN to confirm it.

To change the default PIN length:

a Click **Settings** > **Security** > **Miscellaneous Security Settings**.

b Enter a number in the Minimum PIN Length field, and then click **Submit**.

5 If the PIN will be used as the Administrator PIN, then click **Admin PIN**.

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

6 Click **Submit**.

Creating a PIN through Panel PIN Protect

Note: This is available only in select printer models with low level security.

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 enter 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.

1 From the Embedded Web Server, click **Settings** > **Security** > **Panel PIN Protect**.

2 Under “Basic Security Setup: Create User PIN,” enter a PIN in the appropriate box, and then reenter the PIN to confirm it.

3 Under “Basic Security Setup: Create Admin PIN,” enter a PIN in the appropriate box, and then reenter the PIN to confirm it.

Note: Each PIN must have a unique name containing up to 128 UTF-8 characters (example: “Copy Lockout PIN”).

4 Click **Modify**.

Notes:

- When an access control is set to User PIN, then any Admin PIN for your printer is valid for that access control.
- You can assign a user or administrator PIN to any printer function only after you complete this procedure.

Setting up internal accounts

Note: This is available only in select printer models.

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

1 From the Embedded Web Server, click **Settings** > **Security** > **Security Setup**.

2 Under Advanced Security Setup, click **Internal Accounts** > **Setup groups for use with internal accounts**.

3 Type the group name.

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

4 Click **Add**.

5 Repeat steps 3 through 4 to add more user groups.

Note: When creating groups, make a list of all users first, and then determine which device functions are needed by all users and which functions are needed only by certain users. Each group fulfills 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, click **Settings** > **Security** > **Security Setup**.

2 Under Advanced Security Setup, click **Internal Accounts** > **Add an Internal Account**.

3 Provide the information needed for each account:

- **Account Name**—Type the user's account name (example: “Jack Smith”). You can use up to 164 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 preceding field.
- **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

Internal accounts settings determine the information an administrator submits when creating a new internal account and the information a user submits when authenticating.

- **Custom Building Block Name**—Type a unique name for this building block.
- **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.

Connecting your printer to an Active Directory domain

Notes:

- This is available only in select printer models.
- Make sure to use HTTPS to protect the credentials that are used to join the printer to the domain.

- If you do not select HTTPS, then you will not be able to set up Active Directory.

1 Open a Web browser, and then type the IP address or host name of the printer.

Note: A warning with a message associated to your printer IP address or host name will appear. Click **Continue to this website (not recommended)** to continue and open the printer Web page.

2 From your printer Web page, navigate to:

Settings > **Security** > **Security Setup** > **Active Directory** > **Join an Active Directory Domain**

3 Provide the information needed for each account:

- **Realm**--Type the name of the realm that you are trying to use.
- **Domain Controllers**--Type the domain controllers that you are trying to use. Separate each domain controller with a comma.
- **User ID**--Type the user name of the network administrator or any individual that has rights to add computers to a network.
- **Password**--Type the password of the network administrator or the individual that has rights to join the domain.

  Note: Passwords are case-sensitive, but these passwords are not cached by the device.
- **Organizational Unit**--Type the name of your organizational unit, but only when necessary.

  Note: You can skip this since this is not a required field.

4 Click **Submit**.

Notes:

- After clicking the **Submit** button, the screen flashes and you may hear a clicking noise.
- A big red **X** mark will appear if the configuration is unsuccessful. A message will also appear telling you what may have gone wrong with joining the domain.

5 If there are no errors, then the setup is complete. You may click **Manage Security Templates** to use the Active Directory information to complete your security setup.

Note: If you wish to review or make some small modifications to the LDAP+GSSAPI building block, click **Return to Security Setup** and follow the process identified below.

To start reviewing and modifying the process:

a Under Advanced Security Setup, click **Kerberos 5**.

b Click **View File** to open the Kerberos Config file that was created using the Active Directory setup.

c Review the file, and then click the browser's back button to continue the review process.

Note: Do not edit or copy the Kerberos Config file to use with older devices. This can cause issues with KDC Server Affinity Service. Older devices will not recognize the special mappings associated with the KDC Server Affinity Service.

d Click **Return to Security Setup**, and then click **LDAP+GSSAPI**.

e Under LDAP+GSSAPI Setups, look for the building block that was created by the Active Directory Setup process, and then click it.

Note: By default, the building block name will be the realm name. In addition, the Server Address field was filled out using the Domain Controller name.

f Change some of the building block settings depending on your environment, including the following:

- **Server Port**--The standard port for LDAP is 389. Another common port is 3268, but this is used only for Global Catalog servers in Active Directory. When applicable, change the port to 3268 to speed up the querying process.
- **Search Base**--This tells the device where, in the directory “tree”, to start searching. Specified as a Distinguished Name, it is recommended that you at least specify the root of the directory (e.g. “dc=company,dc=com”).
- **Use Kerberos Service Ticket**--This setting is an advanced setup otherwise known as SPNEGO. This uses the session ticket that a user has when they are logged into their computer. It is recommended that you leave this setting unchecked.
- **Use Active Directory Device Credentials**--This box should normally be checked because you want to use the Service Account that was created in Active Directory. If you do not want to use this setting, because you want to utilize an existing Service Account or you want to use user credentials (advanced setup), then simply uncheck this box.

g Using the scroll bar on the right side of the page, scroll down to the following fields when necessary:

- **Group Search Base**--This field tells the device where in the directory tree to start searching for a particular group. This field does not need to be filled out if user- or group-based authorization is not required by the environment.
- **Short name for group**--This is a user-defined field that allows the user to create a name for a group and associate that name with a group identifier.
- **Group Identifier**--This field tells the device what container or organizational unit it needs to search and to validate whether an authenticated user is a member of an authorized group.

h If you have made any changes, using the scroll bar on the right side of the page, scroll down to the bottom of the page, and then click **Modify**.

Using LDAP

Note: This is available only in select printer models.

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 if an outage 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, click **Settings** > **Security** > **Security Setup**.
2. Under Advanced Security Setup, click **LDAP**.

3 Click **Add an LDAP Setup**.

The LDAP Server Setup dialog is divided into four parts:

General Information

- **Setup Name**—This name is used to identify each particular LDAP Server Setup when creating security templates.
- **Server Address**—Type the IP address or the host name of the LDAP server where the authentication will be performed.
- **Server Port**—The Embedded Web Server communicates with the LDAP server using this port. 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`.
- **Mail Attribute**—Type a maximum of 48 characters to uniquely identify e-mail addresses. The default value is "mail."
- **Full Name Attribute**—Type a maximum of 48 characters. The default value is "cn."
- **Search Base**—This 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 separated by commas, such as cn (common name), ou (organizational unit), o (organization), c (country), and dc (domain).
- **Search Timeout**—Enter a value from 5 to 30 seconds or 5 to 300 seconds depending on your printer model.
- **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. **User ID and password** is the default setting.

Device Credentials

- **Use Active Directory Device Credentials**—If selected, then user credentials and group designations can be pulled from the existing network comparable to other network services.
- **Anonymous LDAP Bind**—If selected, then the Embedded Web Server binds with the LDAP server anonymously, and the Distinguished Name and MFP Password fields are unavailable.
- **Distinguished Name**—Type the distinguished name of the print server or servers.
- **MFP's Password**—Type the password for the print servers.

Search specific object classes

- **Person**—If selected, then the "person" object class will also be searched.
- **Custom Object Class**—If selected, then this custom search object class will also be searched. The administrator can define up to three custom search object classes (optional).

LDAP Group Names

- 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.

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

To edit an existing LDAP setup

1. From the Embedded Web Server, click **Settings** > **Security** > **Security Setup**.
2. Under Advanced Security Setup, click **LDAP**.
3. Click a setup from the list.
4. Make any needed changes in the LDAP Configuration dialog.
5. Click **Modify** to save the changes, or click **Cancel** to return to previous values.

To delete an existing LDAP setup

1. From the Embedded Web Server, click **Settings** > **Security** > **Security Setup**.
2. Under Advanced Security Setup, click **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, click **Settings** > **Security** > **Security Setup**.
2. Under Advanced Security Setup, click **LDAP**.
3. Click **Test LDAP Authentication Setup** next to the setup you want to test.

Using LDAP+GSSAPI

Note: This is available only in select printer models.

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 if an outage 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, click **Settings** > **Security** > **Security Setup**.

2 Under Advanced Security Setup, click **LDAP+GSSAPI**.

3 Click **Add an LDAP+GSSAPI Setup**. The 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**—Type the IP address or the host name of the LDAP server where the authentication will be performed.
- **Server Port**—This is 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`.
- **Mail Attribute**—Type a maximum of 48 characters to uniquely identify e-mail addresses. The default value is "mail."
- **Full Name Attribute**—Type a maximum of 48 characters.
- **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 separated by commas, such as cn (common name), ou (organizational unit), o (organization), c (country), and dc (domain).
- **Search Timeout**—Enter a value from 5 to 30 seconds.
- **Use Kerberos Service Ticket**—If this is selected, then a Kerberos ticket is presented to the LDAP server using the GSSAPI protocol to obtain access.

Device Credentials

- **Use Active Directory Device Credentials**—If this is selected, then user credentials and group designations can be pulled from the existing network comparable to other network services.
- **MFP Kerberos Username**—Type the distinguished name of the print server or servers.
- **MFP's Password**—Type the Kerberos password for the print servers.

Search specific object classes

- **Person**—If this is selected, then the "person" object class will also be searched.
- **Custom Object Class**—If selected, then this custom search object class will also be searched. 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.

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

To edit an existing LDAP+GSSAPI setup

1. From the Embedded Web Server, click **Settings** > **Security** > **Security Setup**.
2. Under Advanced Security Setup, click **LDAP+GSSAPI**.
3. Select a setup from the list.
4. Make any needed changes in the LDAP Configuration dialog.
5. Click **Modify** to save the changes, or **Cancel** to return to previous values.

To delete an existing LDAP+GSSAPI setup

1. From the Embedded Web Server, click **Settings** > **Security** > **Security Setup**.
2. Under Advanced Security Setup, click **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

Note: This is available only in select printer models.

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 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 resubmitting 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 if an outage 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, click **Settings** > **Security** > **Security Setup**.
2. Under Advanced Security Setup, click **Kerberos 5**.
3. Type the KDC (Key Distribution Center) address or host name in the KDC Address field.
4. Enter the number of the port (between 1 and 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, click **Settings** > **Security** > **Security Setup**.

2 Under Advanced Security Setup, click **Kerberos 5**.

3 Click **Browse**, and then 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 automatically tests 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 time stamp (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, click **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 select a time zone from the drop-down list.

Notes:

- Entering manual settings automatically disables use of NTP.
- If you select **(UTC+user) Custom** from the Time Zone list, then you will need to configure additional settings under Custom Time Zone Setup.

3 If *daylight saving time* (DST) is observed in your area, then select the **Automatically Observe DST** check box.

4 If you are located in a nonstandard time zone or an area that observes an alternate DST calendar, then adjust the Custom Time Zone Setup settings if necessary.

5 To sync to an NTP server rather than manage date and time settings manually, select the **Enable NTP** check box, and then type the IP address or host name of the NTP server.

6 If the NTP server requires authentication, then select the preferred method from the “Authentication” drop-down list, and then click the **Install MD5 key** link or **Install Autokey IFF params** link to browse to the file containing the matching NTP authentication.

7 Click **Submit** to save the changes, or **Reset Form** to restore the 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 be registered to a single NT domain only.

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 if an outage 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 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, then you will not be able to register your device with an NT domain.

2. From the Embedded Web Server, click **Settings** > **Security** > **Security Setup**.
3. Under Advanced Security Setup, click **NTLM**.
4. Type a preferred name in the Custom Building Block Name field.
5. Type the default user domain in the Default User Domain field.
6. Click **Submit**. A status screen will appear with the message ”Registering.”
   - If registration is successful, then ”Status....Registered” appears in the Manage NTLM Setup screen.
   - If registration is not successful, then ”Status....Not Registeted” appears in the Manage NTLM Setup screen.

Securing access

Setting a backup password

Note: This is available only in select printer models.

A backup password allows the Embedded Web Server administrator to access security menus regardless of the type of security assigned. It can also be helpful if other security measures become unavailable, such as when 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.

1. From the Embedded Web Server, click **Settings** > **Security** > **Security Setup**.
2. Under Additional Security Setup Options, click **Backup Password**.
3. Select the **Use Backup Password** check box, and then type and retype the password.
4. Click **Submit**.

Setting login restrictions

Note: This is available only in select printer models.

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, click **Settings** > **Security** > **Miscellaneous Security Settings** > **Login Restrictions**.
2. 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.
3. Click **Submit** to save the changes, or **Reset Form** to restore the default settings.

Using a security template to control function access

Note: This is available only in select printer models.

Each access control (or function access control), can be set to require no security (the default) or to use any of the building block selections available in the drop-down list for that function. Only one method of security can be assigned to each access control.

Step 1: Create a building block

1 From the Embedded Web Server, click **Settings** > **Security** > **Security Setup**.

2 From Step 1 under Advanced Security Setup, click the building block (or blocks) appropriate for your environment, and then configure it.

For more information on configuring a specific type of building block, see the relevant section or sections under “Configuring building blocks” on page 9.

Step 2: Create a security template

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, click **Settings** > **Security** > **Security Setup**.

2 From Step 2 under Advanced Security Setup, click **Security Template**.

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

4 In the Security Template 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 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.

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**.

Notes:

- Certain building blocks (such as Passwords and Pins) do not support separate authorization.
- For simple authorization-level security (in which individual users are not authenticated), administrators can control access to specific device functions by assigning only a password or PIN to a security template. Users will be required to enter the correct code in order to gain access to any function controlled by the password or PIN.

Step 3: Assign security templates to access controls

1 From the Embedded Web Server, click **Settings** > **Security** > **Security Setup**.

2 From Step 3 under Advanced Security Setup, click **Access Controls**.

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 the 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 “Appendix C: Access controls” on page 41.

Editing or deleting an existing security template

1. From the Embedded Web Server, click **Settings** > **Security** > **Security Setup**.
2. From Step 2 under Advanced Security Setup, click **Security Template**.
3. Select a security template from the list.
4. Edit the fields as necessary.
5. Click **Modify** to save the changes, or **Cancel** to retain previously configured values.

Notes:

- Clicking **Delete Entry** will delete the selected security template. To delete all security templates on the device, click **Delete List** in the Manage Security Templates screen.
- You can delete a security template only if it is not in use; however, security templates currently in use can be edited.

Managing certificates and other settings

Note: This is available only in select printer models.

The Certificate Management menu is used for configuring printers to utilize certificates for establishing SSL, PSec, and 802.1x connections. Additionally, MFPs utilize certificates for LDA over SSL authentication and address book look-ups.

The process for configuring devices consists of the following activities:

- Loading of the CA (Certificate Authority) certificate for a certificate authority into the device
- Creating a device certificate or using of the device default certificate
- Creating a CA-signed certificate using the device certificate data
- Loading of the CA-signed certificate into the device

Installing a Certificate Authority certificate on the device

Note: This feature is available only in network printers or printers connected to print servers.

The Certificate Authority (CA) is needed so that the printer can trust and validate the credentials of another system on the network. Without a CA certificate, the printer has no other means to determine whether to trust the certificate that has been presented by the system that would like to create the secure connection.

Start with the certificate file (.pem format) for the CA that is to be utilized. An example of how to create this file is provided in “Appendix A: CA file creation” on page 41.

1. Open a Web browser, and then type the IP address or host name of the printer.
2. From your printer Web page, click **Settings** > **Security** > **Certificate Management** > **Certificate Authority Management**.

   Notes:

   - This window allows the device administrator the ability to initiate a request for a new CA certificate, delete all CA certificates, and view previously installed CA certificates. To view more details of an installed CA

certificate or delete a particular CA certificate, simply click on the certificate common name link listed under the Certificate Authority Common Name heading.

- There is no installed CA certificates to view on this page if this a new, out-of-the-box device.

3 Click **New** to display the Certificate Authority Installation screen.

4 Click **Browse** to select the .pem format certificate authority file, and then select **Submit**. This completed the process of installing a CA certificate.

Configuring the device for certificate information

Note: This is available only in select printer models.

The printer has a self-generated certificate. For some operations (e.g. 802.1x, IPSec, etc.), the printer certificate needs to be upgraded to a certificate that has been signed by a certificate authority.

The printer includes a certificate signing request that can be viewed or downloaded, which greatly facilitates the process of obtaining the signed certificate for the printer.

1 Open a Web browser, and then type the IP address or host name of the printer.

2 From your printer Web page, click **Settings** > **Security** > **Certificate Management** > **Set Certificate Defaults**.

Note: The Set Certificates Defaults menu allows you to update the out-of-the-box information on the device with information including those that fit your organization's certificate requirements.

3 After updating all the fields that fit your organization, click **Submit**. For more information, see "Setting certificate defaults" on page 26.

Note: The Web page refreshes and returns to the Certificate Management page.

4 Click the **Device Certificate Management** link.

Notes:

- This window allows the device administrator the ability to initiate a request for a new device certificate, delete all device certificates, and view previously installed device certificates. To view more details of an installed device certificate or delete a particular device certificate, simply click on the certificate common name link listed under the Friendly Name heading.
- If this is for a new, out-of-the-box device, then there will be a default self-signed certificate to view on this page.

5 Select the link for the preferred device certificate to obtain the certificate signing request information.

Notes:

- You may use the default certificate link to use the default certificate created in step 2 or another named certificate. The certificate information is displayed.
- Other certificates are created by selecting **New**, which will open a Certificate Generation Parameters page. For more information, see "Creating a new certificate" on page 25.

6 Click **Download Signing Request**, and then save and open the .csr file with a notepad or any other text editor.

Note: The file data is displayed in a standard format that includes the base-64 representation in the application window. Highlight and copy that information for later usage by a paste operation.

7 Leave your current printer Web page open while you open a new Web browser to the Certificate Authority Web site.

8 Follow the CA certificate request process as defined for the Certificate Authority. A sample request is shown in “Appendix B: CA-Signed Device Certificate creation” on page 41.

Note: The result of this process will be a new CA Signed Device Certificate file (in .pem format). Save this file on your computer since it will be required for the next steps.

9 In your printer Web page, return to the “default” Device Certificate Management page, and then click **Install Signed Certificate**.

10 Click **Browse**, and then select the CA Signed Device Certificate file that was created in step 8.

11 Click **Submit**.

Note: This completes the process of creating and installing a signed printer certificate. The printer can now present a valid certificate to systems to which it attempts to negotiate an SSL or IPSec connection.

Creating a new certificate

1 From the Embedded Web Server, click **Settings** > **Security** > **Certificate Management**.

2 Click **Device Certificate Management** > **New**.

3 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 host name 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/Region**—Type the country or region where the company or organization issuing the certificate is located (2-character maximum).
- **Province Name**—Type the name of the province or state 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, type 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).

4 Click **Generate New Certificate**.

Viewing, downloading, and deleting a certificate

1 From the Embedded Web Server, click **Settings** > **Security** > **Certificate Management** > **Device Certificate Management**.

2 Select a certificate from the list.

The details of the certificate appear in the Device Certificate Management window.

3 Click any of the following:
- **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 the screen.

1 From the Embedded Web Server, click **Settings** > **Security** > **Certificate Management** > **Set Certificate Defaults**.

2 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/Region**—Type the country or region where the company or organization issuing the certificate is located (2-character maximum).
- **Province Name**—Type the name of the province or state 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, type 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.

3 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, click **Settings** > **Security** > **Confidential Print Setup**.

2 Enter an option for Max Invalid PIN:
- Enter **0** to allow users to enter an incorrect PIN as many times as they choose.
- Enter a value 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 the changes, or **Reset Form** to reset both fields.

Enabling and disabling USB devices

Note: This is available only in select printer models.

1 From the Embedded Web Server, click **Settings** > **Security** > **Schedule USB Devices**.
2 From the Disable Devices menu, select to disable printing from any USB device or from flash drives only.

   Note: All scheduled “Disable” actions will be affected by this setting.
3 Click **Submit**.
4 Enable or disable the use of USB devices on certain days or during certain hours. To create a schedule:
   a From the Action menu, select **Enable** or **Disable** to specify which action should occur at the specified time.
   b From the Time menu, select the hour at which the selected action should begin (example: “06:00,” to start at 6:00 AM).
   c From the Day(s) menu, select which day or days the schedule should run (example: “Weekdays (Mon-Fri)”).
   d Click **Add** to save the action to 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 the 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.

Notes:

- Not all printers have a hard disk installed. If you do not see Disk Wiping in the main Security menu, then it is not supported on your device.
- Disk wiping can take one or more hours, during which time the printer will be unavailable for other tasks.

Setting up disk wiping

1 From the Embedded Web Server, click **Settings** > **Security** > **Disk Wiping**.
2 For Wiping Mode, select one of the following:
   - **Off**—Use this to disable disk wiping.
   - **Auto**—Use this to automatically wipe data following each use (can increase the time between jobs).

- **Manual**—Use this to set up a schedule for disk wiping.

3 Click **Submit**.

Notes:

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

Modifying scheduled disk wiping

1 If you have enabled the Manual Wiping mode to set a schedule for disk wiping, then click **Scheduled Disk Wiping** and do the following:

   a Use the Time and Day(s) lists to designate when disk wiping should occur, and then click **Add**.

   b If necessary, repeat the step to schedule additional times for disk wiping.

2 Set the Disk Wiping method (Automatic, Manual, or Scheduled) that matches the selected Wiping Mode:

   - **Single Pass**—This lets you overwrite the printer hard disk in a single pass with a repeating bit pattern.
   - **Multi-pass**—This lets you overwrite the printer hard disk with random bit patterns several times, followed by a verification pass. A secure overwrite is compliant with the DoD 5220.22-M standard for securely erasing data from a hard disk. Highly confidential information should be wiped using this method.

3 Click **Submit**.

Configuring security audit log settings

Note: This is available only in select printer models.

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, click **Settings** > **Security** > **Security Audit Log**.

2 Select **Enable Audit** to activate security audit logging (syslog).

3 Type the IP address or host name of the Remote Syslog Server, and then select the **Enable Remote Syslog** check box to transmit log events to a network syslog server.

   Note: The Enable Remote Syslog check box is unavailable until an IP address or host name is entered.

4 Enter the Remote Syslog Port number used on the destination server. The default value is 514.

5 From the Remote Syslog Method menu, select one of the following:

   - Normal UDP—To send log messages and events using a lower-priority transmission protocol.
   - Stunnel—If implemented on the destination server.

6 From the Remote Syslog Facility menu, 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” menu, select the priority level cutoff (0–7) for logging messages and events.

Note: The highest severity is 0, and the lowest is 7. The selected severity level and anything higher will be logged. For example, if level **4 - Warning** is selected, then severity levels 0–4 will be logged.

8 Select **Remote Syslog non-logged events** to send all events regardless of severity to the remote server.

9 In the “Admin's e-mail address” field, type one or more e-mail addresses (separated by commas) to automatically notify administrators of certain log events, and then select from the following options:

- **E-mail log cleared alert**—This indicates when the **Delete Log** button is clicked.
- **E-mail log wrapped alert**—This indicates when the log becomes full and begins to overwrite the oldest entries.
- **Log full behavior**—This provides a drop list with two options:
  - “Wrap over oldest entries”
  - “E-mail log then delete all entries”
- **E-mail % full alert**—This indicates when log storage space reaches a certain percentage of capacity.
- **% full alert level (1-99%)**—This sets how full the log must be before an alert is triggered.
- **E-mail log exported alert**—This indicates when the log file is exported.
- **E-mail log settings changed alert**—This indicates when the log settings are changed.
- **Log line endings**—This sets how the log file terminates the end of each line. Select a line ending option from the drop-down menu.
- **Digitally sign exports**—This adds a digital signature to each exported log file.

Note: To use e-mail alerts, click **Submit** to save the changes, and then follow the **Setup E-mail Server** link to configure SMTP settings.

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

E-mail server setup

1 From the Security Audit Log main screen, click **Setup E-mail Server**.

2 Under SMTP Setup, type the IP address or host name of the Primary SMTP Gateway the device will use for sending e-mail.

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

4 If you are using a secondary or backup SMTP server, then type the IP address/host name and SMTP port for that server.

5 For SMTP Timeout, enter the number of seconds (5–30) the device will wait for a response from the SMTP server before timing out. The default value 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/TLS 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, then select an authentication method from the SMTP Server Authentication list. The default setting 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** if authentication is required.

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

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

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 devices and connectivity, 802.1x authentication supports both wired and wireless environments.

The following network authentication mechanisms can be included in the 802.1x protocol negotiation:

- EAP-MD5
- EAP-TLS
- EAP-TTLS with the following methods:
  - CHAP
  - MSCHAP
  - MSCHAPv2
  - PAP
- EAP_MSCHAPV2
- PEAP
- LEAP

EAP Type	Needs on MFP or Printer
EAP-MD5	Device login name and password
EAP-TLS	Device login name and password, CA certificate, signed device certificate
EAP-TTLS	Device login name and password, CA certificate
PEAP (PEAP-MSCHAPV2)	Device login name and password, CA certificate
PEAP (TLS)	Device login name and password, CA certificate, signed device certificate
LEAP	Device login name and password

Note: It is important to make sure that all of the devices participating in the 802.1x process support the same EAP authentication type.

1 From the Embedded Web Server, click **Settings** > **Security** > **802.1x**.

2 Under 802.1x Authentication, do the following:

   a Select the **Active** check box to enable 802.1x authentication.

   b Type the login name and password the printer will use to log in to the authentication server.

   c Select the **Validate Server Certificate** check box to require verification of the security certificate on the authenticating server.

Notes:

- If you are using digital certificates to establish a secure connection to the authentication server, then you must configure them on the printer before changing 802.1x authentication settings.
- Server certificate validation is integral to TLS (Transport Layer Security), PEAP (Protected Extensible Authentication Protocol), and TTLS (Tunneled Transport Security Layer).

d Select the **Enable Event Logging** check box to log 802.1x authentication-related activity.

Warning—Potential Damage: To reduce FLASH part wear, only use this feature when necessary.

e From the 802.1x Device Certificate list, select the digital certificate you want to use. If only one certificate has been installed, then **default** will be the only choice listed.

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

4 From the TTLS Authentication Method list, select the authentication method to accept 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-connected 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, click **Settings** > **Security** > **SNMP**.

2 Under SNMP Version 1, 2c, select **Enabled**.

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

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 **Enable PPM Mib** (Printer Port Monitor MIB).

6 Click **Submit** to save the changes, or click **Reset Form** to restore the default values.

SNMP Version 3

1 From the Embedded Web Server, click **Settings** > **Security** > **SNMP**.

2 Under SNMP Version 3, select **Enabled**.

3 To allow remote installation and configuration changes as well as device monitoring, type a user name in the SNMPPv3 Read/Write User field and a password in the SNMPPv3 Read/Write Password field.

4 To allow device monitoring only, type a user name in the SNMPPv3 Read Only User field and a password in the SNMPPv3 Read Only Password field.

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 the changes or click **Reset Form** to restore the 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, click **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, enter 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 the changes, or click **Reset Form** to clear all fields.

Configuring the TCP/IP port access setting

Note: This is available only in select printer models.

This feature allows you to set access settings on the different TCP/IP ports of the device.

1 From the Embedded Web Server, click **Settings** > **Security** > **TCP/IP Port Access**.

Note: The page displays a list of TCP/IP ports. All ports, except TCP 10000 (Telnet), are enabled by default.

2 Click the check box of the TCP/IP port to change its access setting.

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

Configuring your IP security settings

Note: This is available only in select printer models.

1 From the Embedded Web Server, click **Settings** > **Network/Ports** > **IPSec**.

2 From the IPSec menu page, configure the following settings:

Setting	Description
IPSec Enable On Off	To enable or disable the printer's IP security settings. **Note:** On is the factory default setting.
* This is the factory default setting.	

Setting	Description
Connections Pre-Shared Key Authenticated Connections Host 1–5 Certificate Authenticated Connections Host 1–5	To configure the printer's authenticated connections. • The following pre-shared key settings can be configured: – **Address**—You can type a maximum of 45 bytes of characters. – **Key**—You can type a maximum of 256 bytes of characters. • The following certificate setting can be configured: – **Address[/subnet]**—You can type a maximum of 59 bytes of characters.
Settings DH Group DH (Diffie-Hellman) Group Proposal modp768 (1) modp1024 (2)* modp1536 (5) modp2048 (14) Encryption Proposed Encryption Method DES 3DES* AES Authentication Proposed Authentication Method MD5 SHA 1 Certificate Validation Validate Peer Certificate On* Off Select Device Certificate IPSec Device Certificate default*	To specify your printer's encryption and authentication methods.
* This is the factory default setting.	

3 Click **Submit** to save the changes, or click **Reset Form** to restore the default values.

Enabling the security reset jumper

Note: This is available only in select printer models.

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, click **Settings** > **Security** > **Miscellaneous Security Settings**.

2 From the Security Reset Jumper list, select one of the following:
- **No Effect**—This removes access to *all* security menus and should be used with caution.
- **Access controls = "No security"**—This removes security only from the function access controls.

- **Reset factory security defaults**—This restores all security settings to the default values.

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

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

Securing the hard disk and other installed memory

Statement of Volatility

Your printer contains various types of memory that are capable of storing device and network settings, information from embedded solutions, and user data. The types of memory—along with the types of data stored by each—are described as follows:

- **Volatile memory**—Your device utilizes standard random access memory (RAM) to temporarily buffer user data during simple print and copy jobs.
- **Non-volatile memory**—Your device may utilize two forms of non-volatile memory: EEPROM and NAND (flash memory). Both types are used to store the operating system, device settings, network information, scanner and bookmark settings, and embedded solutions.
- **Hard disk memory**—Some devices have a hard disk drive installed. The printer hard disk is designed for device-specific functionality and cannot be used for long term storage for data that is not print-related. The hard disk does not provide the capability for users to extract information, create folders, create disk or network file shares, or FTP information directly from a client device. The hard disk can retain buffered user data from complex scan, print, copy, and fax jobs, as well as form data, and font data.

You may want to erase the contents of the memory devices installed in your printer when:

- The printer is being decommissioned.
- The printer hard drive is being replaced.
- The printer is being moved to a different department or location.
- The printer is being serviced by someone from outside your organization.
- The printer is being removed from your premises for service.

Disposing of a hard drive

Note: Not all printers have a hard disk installed.

In high-security environments, it may be necessary to take additional steps to ensure that confidential data stored on the printer hard disk cannot be accessed once the printer or its hard disk is removed from your premises. While most data can be erased electronically, you may want to consider one or more of the following actions before disposing of a printer or hard disk:

- **Degaussing**—This flushes the hard drive with a magnetic field that erases stored data.
- **Crushing**—This physically compresses the hard disk to break component parts and render them unreadable.
- **Milling**—This physically shreds the hard disk into small metal bits.

Note: While most data can be erased electronically, the only way to guarantee that all data is completely erased is to physically destroy each memory device on which data could have been stored.

Erasing volatile memory

The volatile memory (RAM) installed on your printer requires a power source to retain information. To erase the buffered data, simply turn off the device.

Erasing non-volatile memory

There are several methods available for erasing data stored in non-volatile memory, depending on the type of memory device installed and the type of data stored by that device.

- **Individual settings**—You can erase individual printer settings using the printer control panel or the printer Embedded Web Server. For more information, see the *User's Guide*.
- **Device and network settings**—You can erase device and network settings and restore factory defaults by resetting the NVRAM using the printer Config menu.
- **Security settings**—You can restore factory defaults or erase security settings by selecting a behavior for the Security Reset Jumper in the Embedded Web Server, and then moving a hardware jumper located on the motherboard.
- **Fax data**—If your printer does not contain a hard disk, or if you have chosen NAND for fax storage, then you can erase fax settings and data by resetting the NVRAM using the printer Config menu.

  Note: If your printer has a hard disk that has been partitioned for fax storage, then you must reformat that partition to erase fax data and settings.
- **Embedded solutions**—You can erase information and settings associated with embedded solutions by uninstalling the solutions, or by restoring factory defaults using the printer Config menu.

Completely erasing printer hard disk memory

Configuring Disk Wiping in the printer menus enables you to remove confidential material left by scan, print, copy, and fax jobs, by securely overwriting files that have been marked for deletion.

For information on erasing the remaining job information stored in printer hard disk memory using the Embedded Web Server, see "Disk wiping" on page 27.

Using the printer control panel

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 device back on. It takes approximately a minute to boot into the Configuration menu.

   Once the MFP is ready, the touch screen shows a list of functions instead of standard home screen icons such as Copy and Fax.
3. Release the buttons when the screen with the progress bar appears. The printer undergoes a power-on reset, and then the Configuration menu appears.
4. Touch **Wipe Disk**, and then touch one of the following:
   - **Wipe disk (fast)**—This lets you overwrite the disk with all zeroes in a single pass.
   - **Wipe disk (secure)**—This lets you overwrite the disk with random bit patterns several times, followed by a verification pass. A secure overwrite is compliant with the DoD 5220.22-M standard for securely erasing data from a hard disk. Highly confidential information should be wiped using this method.

5 Touch **Yes** to proceed with disk wiping. A status bar will indicate the progress of the disk wiping task.

Note: Disk wiping can take from several minutes to more than an hour, during which the printer will be unavailable for other user tasks.

6 Touch **Back**, then touch **Exit Config Menu**.

The printer undergoes a power-on reset and then returns to normal operating mode.

Configuring printer hard disk encryption

Enable hard disk encryption to prevent loss of sensitive data in the event the printer or its hard disk is stolen.

Note: Some printer models may not have a printer hard disk installed.

Using the Embedded Web Server

1 Open a Web browser, and then type the printer IP address in the address field.

Notes:

- View the printer IP address on the printer home screen. The IP address appears as four sets of numbers separated by periods, such as 123.123.123.123.
- If you are using a proxy server, then temporarily disable it to load the Web page correctly.

2 Click **Settings** > **Security** > **Disk Encryption**.

Note: Disk Encryption appears in the Security Menu only when a formatted, non-defective printer hard disk is installed.

3 From the Disk Encryption menu, select either of the following:

- **Disable**—Use this to disable disk encryption.
- **Enable**—Use this to enable disk encryption.

  Notes:

  - Disable is the factory default setting.
  - Changing this setting will cause the printer to undergo a power-on reset.

  Warning—Potential Damage: Changing the setting for disk encryption will erase the contents of the hard disk.

4 Click **Submit** to proceed with disk wiping and encryption.

Note: Encryption takes approximately two minutes.

Warning—Potential Damage: Do not turn off the printer during the encryption process.

5 Click **Refresh** to return to the Embedded Web Server.

Using the printer control panel

1 Turn off the printer.

2 Hold down **2** and **6** while turning the printer on. Release the buttons only when the screen with the progress bar appears.

The printer performs a power-on sequence, and then the Configuration menu appears. When the printer is fully turned on, a list of functions appears on the printer display.

3 Touch **Disk Encryption** > **Enable**.

4 Touch **Yes** to proceed with disk encryption.

Notes:

- Do not turn off the printer during the encryption process. Doing so may result in loss of data.
- Encryption takes approximately two minutes.
- A status bar will indicate the progress of the disk wiping task. After the disk has been encrypted, the printer will return to the Enable/Disable screen.

5 Touch **Back** > **Exit Config Menu**.

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

Scenarios

Scenario: Printer in a public place

If your printer is located in a public space such as a lobby, and you want to prevent the general public from using it, then 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 1: Create a password or PIN

1 From the Embedded Web Server, click **Settings** > **Security** > **Security Setup**.

2 Under Advanced Security Setup, click either **PIN** or **Password**, and then configure it.

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

For more information on configuring a PIN or password, see the relevant section or sections under “Configuring building blocks” on page 9.

Step 2: Create a security template

1 From the Embedded Web Server, click **Settings** > **Security** > **Security Setup**.

2 Under Advanced Security Setup, click **Security Template**.

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

4 In the Security Template 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 drop-down list, select the PIN or password created in Step 1.

6 Click **Save Template**.

Step 3: Assign security templates to access controls

1 From the Embedded Web Server, click **Settings** > **Security** > **Security Setup**.

2 Under Advanced Security Setup, click **Access Controls**.

3 If necessary, click **Expand All** or click a specific folder to view a list of available functions.

4 From the drop-down list next to the name of each function you want to protect, select the security template created in Step 2.

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

In order to gain access to any function controlled by this security template, users will now be required to enter the appropriate PIN or password.

Scenario: Standalone or small office

Note: This is available only in select printer models.

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

Step 1: Set up individual user accounts

1 From the Embedded Web Server, click **Settings** > **Security** > **Security Setup**.

2 Under Advanced Security Setup, click **Internal Accounts**, and then configure it.

For more information on configuring individual user accounts, see “Setting up internal accounts” on page 11.

Step 2: Create a security template

1 From the Embedded Web Server, click **Settings** > **Security** > **Security Setup**.

2 Under Advanced Security Setup, click **Security Template**.

3 Under Manage Security Templates, click **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 menu, 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 menu. 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, click **Settings** > **Security** > **Security Setup**.

2 Under Advanced Security Setup, click **Access Controls**.

3 If necessary, click **Expand All** or click a specific folder to view a list of available functions.

4 For each function you want to protect, select a security template from the drop-down menu next to the name of that function.

5 Click **Submit** to save the 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

Note: This is available only in select printer models.

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 need to know the following:

- Realm
- Domain Controllers
- User ID (for the domain)
- Password (for the User ID)
- The IP address or host name of the specific server

Step 2: Create a security template

1 From the Embedded Web Server, click **Settings** > **Security** > **Security Setup**.

2 Under Advanced Security Setup, click **Security Template**.

3 Under Manage Security Templates, click **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 3: Assign security templates to access controls

1 From the Embedded Web Server, click **Settings** > **Security** > **Security Setup**.

2 Under Advanced Security Setup, click **Access Controls**.

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 the 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.

Appendix

Appendix A: CA file creation

Note: This example of generation of a CA file for the Certificate Authority assumes usage of a Windows Certificate Authority server.

1. Point the browser window to the CA. Make sure to use the URL, http//<CA's address>/CertSrv, where **CA's address** is the IP address or host name of the CA server.

   Note: Before the CA Web page opens, a Windows login window may pop up and request user credentials to verify that you have access to the CA Web page.

2. Click **Download a CA certificate, certificate chain, or CRL**.
3. Click **Base 64 encoded**, and then click **Download CA Certificate**.

   Note: DER encoding is not supported.

4. Save the certificate that is offered in a file. The file name is arbitrary, but the extension should be ".pem".

Appendix B: CA-Signed Device Certificate creation

Note: This example of generation of a CA file for the Certificate Authority assumes usage of a Windows Certificate Authority server.

1. Point the browser window to the CA. Make sure to use the URL, http//<CA's address>/CertSrv, where **CA's address** is the IP address or host name of the CA server.
2. Click **Request a certificate**.
3. Click **advanced certificate request**.
4. Click **Submit a certificate request by using a base-64-encoded**.
5. Paste the (.csr prompted) information copied from the device into the Saved Request field, and then select a Web Server-type certificate template.
6. Click **Submit**.

   Note: The server takes a moment or two to process the request, and then presents a dialog window.

7. Select **Base 64 encoded**, and then click **Download Certificate**.

   Note: DER encoding is not supported.

8. Save the certificate that is offered in a file. The file name is arbitrary, but the extension should be ".pem".

Appendix C: Access controls

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

Administrative Menus

Function access control	What it does
Configuration Menu	This protects access to the Configuration Menu.
Manage Shortcuts at the Device	This protects access to the Manage Shortcuts section of the Settings menu from the printer control panel.
Manage Shortcuts Remotely	This protects access to the Manage Shortcuts section of the Settings menu from the Embedded Web Server.
Network/Ports Menu at the Device	This protects access to the Network/Ports section of the Settings menu from the printer control panel.
Network/Ports Menu Remotely	This 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 adapter NPA settings change commands are ignored.
Option Card Configuration at the Device	This 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 on the device.
Option Card Configuration Remotely	This controls access to the Option Card Configuration section of the Settings menu from the Embedded Web Server. This applies only when an Option Card with configuration options is installed on the device.
Paper Menu at the Device	This protects access to the Paper menu from the printer control panel.
Paper Menu Remotely	This protects access to the Paper menu from the Embedded Web Server.
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.
Reports Menu at the Device	This protects access to the Reports menu from the printer control panel.
Reports Menu Remotely	This protects access to the Reports menu from the Embedded Web Server.
Security Menu at the Device	This protects access to the Security menu from the printer control panel.
Security Menu Remotely	This protects access to the Security menu from the Embedded Web Server.
Service Engineer Menus at the Device	This protects access to the Service Engineer menu from the printer control panel.
Service Engineer Menus Remotely	This protects access to the Service Engineer menu from the Embedded Web Server.
Settings Menu at the Device	This protects access to the General and Print Settings sections of the Settings menu from the printer control panel.
Settings Menu Remotely	This protects access to the General and Print Settings sections of the Settings menu from the Embedded Web Server.
Supplies Menu at the Device	This protects access to the Supplies menu from the printer control panel.
Supplies Menu Remotely	This protects access to the Supplies menu from the Embedded Web Server.

Management

Function access control	What it does
Firmware Updates	This controls the ability to update firmware from any source other than a flash drive. Firmware files that are received through FTP, the Embedded Web Server, etc., will be ignored (flushed) when this function is protected.
Operator Panel Lock	This protects access to the locking function of the printer control panel. If this is enabled, then users with appropriate credentials can lock and unlock the printer touch screen. In a locked state, the touch screen displays only the "Unlock Device" icon, and no further operations can be performed at the device until appropriate credentials are entered. Once unlocked, the touch screen will remain in an unlocked state even if the user logs out of the device. To enable the control panel lock, the user must select the "Lock Device" icon, and then enter the appropriate credentials.
PJL Device Setting Changes	When disabled, all device settings changes requested by incoming print jobs are ignored.
Remote Management	This controls access to printer settings and functions by remote management tools such as MarkVision™. When protected, no printer configuration settings can be altered except through a secured communication channel (such as that provided by a properly configured installation of MarkVision).
Solutions Configuration or eSF Configuration	This controls access to the configuration of any installed solutions.
Web Import/Export Settings	This controls the ability to import and export printer settings files (UCF files) from the Embedded Web Server.

Function Access

Function access control	What it does
Address Book	This controls the ability to perform address book searches in the Scan to Fax and Scan to E-mail functions.
Cancel Jobs at the Device	This controls the ability to cancel jobs from the printer control panel.
Change Language from Home Screen	This controls access to the Change Language feature from the printer control panel.
Color Dropout	This controls the ability to use the Color Dropout feature for scan and copy functions.
Copy Color Printing	This controls the ability to perform color copy functions. Users who are denied will have their copy jobs printed in black and white.
Copy Function	This controls the ability to use the Copy function.
Create Bookmarks at the Device	This controls the ability to create new bookmarks from the printer control panel.
Create Bookmarks Remotely	This controls the ability to create new bookmarks from the Bookmark Setup section of the Settings menu on the Embedded Web Server.
Create Profiles	This controls the ability to create new profiles.
E-mail Function	This controls access to the Scan to E-mail function.
Fax Function	This controls access to the Scan to Fax function.
Flash Drive Color Printing	This controls the ability to print color from a flash drive. Users who are denied will have their print jobs printed in black and white.
Flash Drive Firmware Updates	This controls the ability to update firmware from a flash drive.

Function access control	What it does
Flash Drive Print	This controls the ability to print from a flash drive.
Flash Drive Scan	This controls the ability to scan documents to a flash drive.
FTP Function	This controls access to the Scan to FTP function.
Held Jobs Access	This protects access to the Held Jobs function.
PictBridge Printing	This controls the ability to print from an attached PictBridge-enabled digital camera. **Note:** Selected devices only.
Release Held Faxes	This controls the ability to release (print) held faxes.
Use Profiles	This controls access to profiles, such as scanning shortcuts, workflows, and eSF applications.

Device Solutions

Function access control	What it does
New Solutions	This controls the initial security profile of each solution-specific access control installed on the printer.
Solution 1–10	The Solution 1 through Solution 10 access controls can be assigned to installed eSF applications and profiles created by LDSS. The access control for each solution is assigned in the creation or configuration of the application or profile.

Note: Depending on the solutions you have installed, additional solution-specific access controls may be listed below solutions 1–10. Use these additional access controls if they are available for your installed solutions. If no additional solution-specific access controls are available, then assign one of the ten numbered access controls to each solution you want to protect.

Notices

Edition notice

November 2012

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

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

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

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

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

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
USA

©2012 Lexmark International, Inc.

All rights reserved.

Trademarks

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

Mac and the Mac logo are trademarks of Apple Inc., registered in the U.S. and other countries.

All other trademarks are the property of their respective owners.

GOVERNMENT END USERS

The Software Program and any related documentation are "Commercial Items," as that term is defined in 48 C.F.R. 2.101, "Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. 12.212 or 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. 12.212 or 48 C.F.R. 227.7202-1 through 227.7207-4,

as applicable, the Commercial Computer Software and Commercial Software Documentation are licensed to the U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein.

GifEncoder

GifEncoder - writes out an image as a GIF. Transparency handling and variable bit size courtesy of Jack Palevich. Copyright (C) 1996 by Jef Poskanzer * <jef@acme.com>. All rights reserved. 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. THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS 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 AUTHOR OR 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. Visit the ACME Labs Java page for up-to-date versions of this and other fine Java utilities: http://www.acme.com/java/

ZXing 1.7

This project consists of contributions from several people, recognized here for convenience, in alphabetical order.

Agustín Delgado (Servinform S.A.), Aitor Almeida (University of Deusto), Alasdair Mackintosh (Google), Alexander Martin (Haase & Martin GmbH), Andreas Pillath, Andrew Walbran (Google), Andrey Sitnik, Androida.hu / http://www.androida.hu/, Antonio Manuel Benjumea (Servinform S.A.), Brian Brown (Google), Chang Hyun Park, Christian Brunschen (Google), crowdin.net, Daniel Switkin (Google), Dave MacLachlan (Google), David Phillip Oster (Google), David Albert (Bug Labs), David Olivier, Diego Pierotto, drejc83, Eduardo Castillejo (University of Deusto), Emanuele Aina, Eric Kobrin (Velocitude), Erik Barbara, Fred Lin (Anobiit), gcstang, Hannes Erven, hypest (Barcorama project), Isaac Potoczny-Jones, Jeff Breidenbach (Google), John Connolly (Bug Labs), Jonas Petersson (Prisjakt), Joseph Wain (Google), Juho Mikkonen, jwicks, Kevin O'Sullivan (SITA), Kevin Xue (NetDragon Websoft Inc., China), Lachezar Dobrev, Luiz Silva, Luka Finžgar, Marcelo, Mateusz Jędrasik, Matrix44, Matthew Schulkind (Google), Matt York (LifeMarks), Mohamad Fairol, Morgan Courbet, Nikolaos Ftylitakis, Pablo Orduña (University of Deusto), Paul Hackenberger, Ralf Kistner, Randy Shen (Acer), Rasmus Schrøder Sørensen, Richard Hřivňák, Romain Pechayre, Roman Nurik (Google), Ryan Alford, Sanford Squires, Sean Owen (Google), Shiyuan Guo / 郭世元, Simon Flannery (Ericsson), Steven Parkes, Suraj Supekar, Sven Klinkhamer, Thomas Gerbet, Vince Francis (LifeMarks), Wolfgang Jung, Yakov Okshtein (Google)

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.

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

Numerics
802.1x authentication 30

A
access controls
  list of 41
  managing with PIN or
    password 21
  managing with security
    templates 21
  understanding 8
Active Directory
  printer, connecting 12
advanced security setup
  password 9
Appendix A
  CA file creation 41
Appendix A: CA file creation 41
Appendix B
  CA-Signed Device Certificate
    creation 41
Appendix B: CA-Signed Device
Certificate creation 41
authenticating
  using Kerberos 18
  using LDAP 14
  using LDAP+GSSAPI 16
  using NTLM authentication 20
authentication
  understanding 6
authorization
  understanding 6

B
backup password
  creating 21
  using 21
basic security
  applying basic security setup 9
  authentication type 9
  limiting access 9
  modifying or removing access 9
building blocks
  adding to security templates 21
  internal accounts 11
  Kerberos 5 18
  LDAP 14
  LDAP+GSSAPI 16
  NTLM authentication 20

C
CA file creation
  Appendix A 41
CA-Signed Device Certificate
creation
  Appendix B 41
certificate
  creating 25
  deleting 25
  downloading 25
  viewing 25
Certificate Authority certificate
  installing 23
certificate defaults
  setting 26
certificate information
  device, configuring 24
certificates
  setting defaults 26
confidential printing
  configuring 26
configuring
  IP security settings 32
  TCP/IP port access setting 32
configuring device
  certificate information 24
creating
  certificate 25
creating a new certificate 25
creating internal accounts 11

D
deleting
  certificate 25
device, configuring
  certificate information 24
disk wiping 35
  modifying 27
  scheduling 27
disposing of printer hard disk 34
downloading
  certificate 25

E
encrypting the printer hard disk 36
erasing hard disk memory 35
erasing non-volatile memory 35
erasing volatile memory 35

F
Function Access Controls 8
function access controls
  list of 41

G
groups
  understanding 8

H
hard disk
  wiping 35
hard disk memory
  erasing 35

I
installing
  Certificate Authority certificate 23
Installing a Certificate Authority
certificate on the device 23
internal accounts
  creating 11
  using 11
IP security settings
  configuring 32
IPSec
  IP security settings 32

K
Kerberos
  configuring 18
  LDAP+GSSAPI and 18
  setting date and time for 18

L
LDAP
  using 14
LDAP+GSSAPI
  Kerberos and 18
  using 16

lockout 21
login
  failure 21
  restrictions 21

M

memory
  types installed on printer 34

N

non-volatile memory 34
  erasing 35
notices 45
NTLM authentication
  HTTPS and 20
  using 20

P

Panel PIN Protect 11
password
  advanced security setup 9
  creating or editing 9
password, creating
  security 10
  Web Page Password Protect 10
personal identification number (PIN) 10, 11
PIN
  advanced security setup 10
  creating or editing 10, 11
  Panel PIN Protect 11
printer hard disk
  disposing of 34
  encrypting 36
printer hard disk encryption 36
printer, connecting
  Active Directory 12

S

scenario
  Active Directory networks 39
  assigning security templates 38
  creating passwords and PINs 37
  creating security templates 37
  printer in a public place 37
  standalone or small office 38
security
  802.1x authentication 30
  Active Directory domain 12
  authentication 6
  authorization 6
  backup password 21
  confidential printing 26
  disk wiping 27
  groups 8
  internal accounts 11
  Kerberos authentication 18
  LDAP authentication 14
  LDAP+GSSAPI authentication 16
  login restrictions 21
  NTLM authentication 20
  password 9
  PIN 10, 11
  reset jumper on motherboard 33
  security audit log 28
  security templates 21
  SNMP 31
  USB devices 27
security audit log
  configuring 28
security devices
  advanced 5
  simple 5
security reset jumper
  enabling 33
security templates
  understanding 8
  using to control function access 21
SNMP 31
statement of volatility 34

T

TCP/IP Port Access
  configuring 32

U

USB devices
  disabling 27
  enabling 27

V

viewing
  certificate 25
volatile memory 34
  erasing 35
volatility
  statement of 34

W

Web Page Password Protect 10
wiping the hard disk 35