Embedded Web Server — Security

Administrator's Guide

May 2016

Contents

Change history

January 2016

- Initial document release for multifunction products with a tablet-like touch-screen display

Overview

Use this document to secure the printer using the Embedded Web Server. To secure the printer, combine login methods and access controls to define users who are allowed to use the printer, and the functions they can use.

Using the Embedded Web Server you can configure the printer to reach Common Criteria Evaluation Assurance Level 2 (EAL 2). For more information, see the *Common Criteria Installation Supplement and Administrator Guide*.

Before you begin, make sure that the printer settings have been configured for e-mail. For more information, see the printer *User's Guide*.

Also, identify the following conditions:

- The login method to use
  - **Local accounts**—Use the authentication methods available on the printer. User credentials are stored in the printer memory.
  - **Lightweight Directory Access Protocol (LDAP)**
  - **with Generic Security Services Application Program Interface (LDAP+GSSAPI)**
  - **Kerberos**
  - **Active Directory**
- Other solutions that you want to include.
  - **Smart Card Authentication**—A collection of applications used to secure access to printers and their functions. The applications let you log in to a printer manually or using a smart card, and then securely send e-mails and release print jobs. You can also configure more security settings in an application, such as e-mail signing and encryption.
  - **Card Authentication**—Secure access to a printer using a card reader. When users badge in, their credentials are authenticated using a master printer, LDAP, or Identity Service Providers (ISP).

    Note: For more information, see the *Administrator's Guide* for the solution.
- The group where the users belong to. You can create groups after creating the login methods.
- The applications, functions, and printer management settings that users can access.

You may need administrative rights to configure or troubleshoot the security settings.

Supported printers

- Dell S5840cdn

Securing network connections

Accessing the Embedded Web Server

1. Obtain the printer IP address. Do either of the following:
   - Locate the IP address on the top of the printer home screen.
   - From the printer home screen, touch **Settings** > **Network/Ports** > **Network Overview**.
2. Open a Web browser, and then type the printer IP address.

Configuring TCP/IP port access settings

You can control your network device activities by configuring your device to filter out traffic on specific network connections. Protocols (such as FTP, HTTP, and Telnet) can be disabled.

Port filtering on devices disables network connections individually. When a port is closed, a device does not respond to traffic on the specified port whether the corresponding network application is enabled.

We recommend closing any ports that you do not plan to use under standard operation by clearing them.

1. From the Embedded Web Server, click **Settings** > **Network/Ports** > **TCP/IP** > **TCP/IP Port Access**.
2. Enable the access to the TCP/IP ports.
3. Click **Save**.

Note: For more information on each port, contact your system administrator.

Configuring IP Security (IPsec) settings

Apply IPsec between the printer and the workstation or server to secure traffic between the systems with a strong encryption. The printers support IPsec with preshared keys (PSK) and certificates. You can use both options simultaneously.

When using PSK authentication, printers are configured to establish a secure IPsec connection with up to seven other systems. Printers and the systems are configured with a pass phrase that is used to authenticate the systems and to encrypt the data.

When using the CA certificate authentication, printers are configured to establish a secure IPsec connection with up to five systems or subnets. Printers exchange data securely with many systems, and the process is integrated with a PKI or CA infrastructure. Certificates provide a robust and scalable solution, without configuring or managing keys and pass phrases.

1. From the Embedded Web Server, click **Settings** > **Network/Ports** > **IPSec**.
2. Select **Enable IPSec**.
3. Configure the following settings to specify the encryption and authentication methods of the printer:
   - Base Configuration
   - DH (Diffie-Hellman) Group Proposal
   - Proposed Encryption method

- Proposed Authentication Method
- IPSec Device Certificate

4 Do one or more of the following:
- From the Pre-Shared Key Authenticated Connections section, type the IP address of the client printer that you want to connect to the printer.
- From the Certificate Authenticated Connections section, type the IP address of the client printer that you want to connect to the printer.

5 Click **Save**.

Notes:

- If there are no CA certificates added, then the default certificate is used.
- If you are using PSK authentication, then type the corresponding key. Retain the key to use later when configuring client printers.

Configuring 802.1x authentication

Though normally associated with wireless devices and connectivity, 802.1x authentication supports both wired and wireless environments.

Notes:

- If using digital certificates to establish a secure connection to the authentication server, then configure the certificates on the printer before changing 802.1x authentication settings. For more information, see “Managing certificates” on page 23.
- Make sure that all printers on the same network using 802.1x are supporting the same EAP authentication type.

1 From the Embedded Web Server, click **Settings** > **Network/Ports** > **802.1x**.

2 From the 802.1x Authentication section, do the following:

a Select **Active**.

b Type the login name and password that the printer uses to log in to the authentication server.

c Select **Validate Server Certificate**.

Note: Server certificate validation is necessary when using Transport Layer Security (TLS), Protected Extensible Authentication Protocol (PEAP), and Tunneled Transport Security Layer (TTLS).

d Select **Enable Event Logging**.

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

e In the 802.1x Device Certificate list, select the digital certificate that you want to use.

Note: If only one certificate is installed, then **default** is the only option that appears.

3 From the Allowable Authentication Mechanisms section, select one or more authentication protocols.
- EAP-MD5, EAP-MSCHAPv2, and LEAP require a login name and password.
- PEAP, and EAP-TTLS require a login name and password and a CA certificate.
- EAP-TLS requires a login name and password, a CA certificate, and a signed printer certificate.

4 In the TTLS Authentication Method menu, select the authentication method to use.

5 Click **Save**.

Setting the restricted server list

You can configure printers to connect only from a list of specified TCP/IP addresses. This action blocks all TCP connections from other addresses, protecting the printer against unauthorized printing and configuring.

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

2 In the Restricted Server List field, type up to 10 IP addresses, separated by commas, that are allowed to make TCP connections.

3 Click **Save**.

Managing devices remotely

Using HTTPS for printer management

To restrict the access of the printer Embedded Web Server to HTTPS only, turn off the HTTP port, leaving the HTTPS port (443) active. This action ensures that all communication with the printer using the Embedded Web Server is encrypted.

1. From the Embedded Web Server, click **Settings** > **Network/Ports** > **TCP/IP** > **TCP/IP Port Access**.
2. Clear **TCP 8000 (HTTP)** and **TCP 80 (HTTP)**.
3. Click **Save**.

Setting up SNMP

Configuring SNMP versions 1 or 2c settings

1. From the Embedded Web Server, click **Settings** > **Network/Ports** > **SNMP**.
2. From the “SNMP Versions 1 and 2c” section, select **Enabled** > **Allow SNMP Set**.
3. In the SNMP Community field, type a name for the SNMP Community identifier. The default community name is **`public`**.
4. Select **Enable PPM Mib** (Printer Port Monitor MIB) to facilitate the automatic installation of printer drivers and other printing applications.
5. Click **Save**.

Configuring SNMP version 3 settings

Before you begin, disable SNMP versions 1 and 2c.

1. From the Embedded Web Server, click **Settings** > **Network/Ports** > **SNMP**.
2. From the SNMP Version 3 section, select **Enabled**.
3. If necessary, configure the following by providing your authentication credentials:
   - **Set Read/Write Credentials**—Allow remote installation and configuration changes and printer monitoring.
   - **Set Read-only Credentials**—Allow only printer monitoring.
4. In the Authentication Hash menu, select the hash function of your SNMP server.
5. In the Minimum Authentication Level, select **Authentication, Privacy**.
6. In the Privacy Algorithm menu, select the strongest setting supported by your network environment.
7. Click **Save**.

Configuring SNMP traps

After configuring SNMP settings, you can customize which alerts are sent to the network management system by designating events (SNMP traps) that trigger an alert message.

1. From the Embedded Web Server, click **Settings** > **Network/Ports** > **SNMP** > **Set SNMP Traps**.
2. In one of the IP Address fields, type the IP address of the network management server or monitoring station.
3. Select the conditions for which you want to generate an alert.
4. Click **Save**.

Configuring security audit log settings

The security audit log lets administrators monitor security-related events on a device, including failed user authorization, successful administrator authentication, and Kerberos file uploads to a device. By default, security logs are stored on the device, but may also be transmitted to a network system log (syslog) server for further processing or storage.

We recommend enabling audit in secure environments.

1. From the Embedded Web Server, click **Settings** > **Security** > **Security Audit Log**.
2. Do one or more of the following:

Activate security audit logging

Select **Enable Audit**.

Configure transmission to a network syslog server

This option lets you use both the remote syslog server and the internal logging.

a. Select **Enable Remote Syslog**.

b. Configure the Remote Syslog settings.

- **Remote Syslog Server**—Type the IP address or host name of the server.
- **Remote Syslog Port**—Type the port number used for the destination server. The default value is 514.
- **Remote Syslog Method**—Select **Normal UDP** to send log messages and events using a lower-priority transmission protocol. Otherwise, select **Stunnel**.
- **Remote Syslog Facility**—Select a facility code for events logged to the destination server. All events sent from the device are tagged with the same code to aid in sorting and filtering by network monitor or intrusion detection software.
- **Severity of Events to Log**—Select the priority level cutoff for logging messages and events. The highest severity is 0, and the lowest is 7. The selected severity level and anything higher are logged. For example, if you select **4 - Warning**, then severity levels 0–4 are logged.
- **Remote Syslog Non-Logged Events**—Send all events regardless of severity to the remote server.

Configure e-mail notification

Before you begin, make sure that the printer settings have been configured properly for e-mail.

a In the Admin's E-mail Address field, type one or more e-mail addresses, separated by commas.

b Configure the notification settings.

- **E-mail Log Cleared Alert**—Send a notification when the Delete Log button is clicked.
- **E-mail Log Wrapped Alert**—Send a notification when the log becomes full and begins to overwrite the oldest entries.
- **Log Full Behavior**—Wrap over oldest entries or e-mail the log and then delete all entries.
- **E-mail % Full Alert**—Send a notification when log storage space reaches a certain percentage of capacity.
- **% Full Alert Level**—Specify how full the log must be before an alert is triggered.
- **E-mail Log Exported Alert**—Send a notification when the log file is exported.
- **E-mail Log Settings Changed Alert**—Send a notification when the log settings are changed.
- **Log Line Endings**—Specify how the log file terminates the end of each line.
- **Digitally Sign Exports**—Add a digital signature to each exported log file.

3 Click **Save**.

Managing security audit logs

- To delete the syslog, in the Clear Log menu, click **Clear**.
- To view or save the syslog, in the Export Log menu, select the file type, and then click **Export**.

Updating firmware

Automated firmware updates can be done simultaneously over a network of printers. For security, the ability to perform this update can be restricted to authorized administrators by using access control.

Printers inspect all downloaded firmware packages for some required attributes before adopting and executing the packages. The firmware is packaged in a proprietary format and encrypted with a symmetric encryption algorithm through an embedded key that is known only to the manufacturer. However, the strongest security measure comes from requiring all firmware packages to include multiple digital 2048-bit RSA signatures from the manufacturer. If these signatures are not valid, or if the message logs indicate a change in firmware after the signatures were applied, then the firmware is discarded.

1 From the Embedded Web Server, click **Settings** > **Device** > **Update Firmware**.

2 Browse to the firmware file.

3 Click **Upload**.

Managing login methods

Restricting public access to functions, applications, printer management, and security options

The guest account can use the printer without logging in. To control the access of guest account users, restrict the functions, applications, printer management, and security options for the guest account.

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
2. From the Public section, click **Manage Permissions**.
3. Select the access controls that the guest account can access. For more information, see “Understanding access controls” on page 21.
4. Click **Save**.

Using local accounts

Local accounts are stored in the printer memory and provides authentication-level security.

Creating local accounts

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
2. From the Local Accounts section, click **Add User**.
3. Select the type of authentication method that you want the account to use when logging in to the printer.
   - **User Name/Password**—Add an account with a user name and password.
   - **User Name**—Add an account with a user name only.
   - **Password**—Add an account with a password only.
   - **PIN**—Add an account with a personal identification number (PIN) only.
4. From the User Information section, type the user information and authentication credentials.
5. From the Permission Groups section, select one or more groups.

   Note: To create a group for the user, select **Add New Group**. For more information, see “Creating local account groups” on page 13.
6. Click **Save**.

Editing and deleting local accounts

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
2. From the Local Accounts section, click the authentication method where the user account belongs to.
3. Click the user account that you want to edit or delete.

4 Do either of the following:
   - To edit the user account, update the user information, and then click **Save**.
   - To delete the user account, click **Delete User**.

Note: To delete multiple user accounts, select the account, and then click **Delete**.

Creating local account groups

Use groups to customize users’ access to applications and printer functions.

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

2 Do either of the following:

Add a group when managing permissions

a From the Local Accounts section, click **Manage Groups/Permissions**.

b Click **Add Group**.

Add a group when creating or editing a user account

a Create or edit a user account.

b From the Permission Groups section, select **Add New Group**.

3 Type a unique group name.

4 From the Access Controls section, select the functions, menus, and applications the group can access.

5 Click **Save**.

Notes:

- To import access controls from another group, click **Import Access Controls**, and then select a group.
- For more information on access controls, see “Understanding access controls” on page 21.

Editing or deleting local account groups

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

2 From the Local Accounts section, click **Manage Groups/Permissions**.

3 Click the group, and then do either of the following:
   - Configure the access controls, and then click **Save**.
   - Click **Delete Group**.

Notes:

- To import access controls from another group, click **Import Access Controls**, and then select a group.
- To delete multiple groups, select the groups, and then click **Delete**.
- For more information on access controls, see “Understanding access controls” on page 21.

Using LDAP or LDAP+GSSAPI

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

LDAP+GSSAPI is used when you want your transmission to be always secure. Instead of authenticating directly with the LDAP server, the user is first authenticated with a Kerberos to obtain a Kerberos ticket. This ticket is 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 a Kerberos network account. For more information, see “Creating a Kerberos login method” on page 16.
- Supported printers can store a maximum of five unique LDAP or LDAP+GSSAPI login methods. Each method must have a unique name.
- Administrators can create up to 32 user-defined groups that apply to each unique login method.
- LDAP and LDAP+GSSAPI relies on an external server for authentication. If the server is down, then users are not able to access the printer using LDAP or LDAP+GSSAPI.
- To help prevent unauthorized access, log out from the printer after each session.

Creating an LDAP or LDAP+GSSAPI login method

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
2. From the Network Accounts section, click **Add Login Method** > **LDAP**.
3. Select the authentication type.
   - LDAP
   - LDAP+GSSAPI
4. Configure the settings.

   ### General Information

   - **Setup Name**—Type a unique name for the LDAP network account.
   - **Server Address**—Type the IP address or the host name of the LDAP server.
   - **Server Port**—Enter the port where LDAP queries are sent.

     Note: If you are using SSL, then use port **636**. Otherwise, use port **389**.
   - **Required User Input**—Select the required LDAP authentication credentials used when logging in to the printer. This setting is available only in the LDAP setup.
   - **Use Integrated Windows Authentication**—Select one of the following:
     - **Do not use**
     - **Use if available**—Use Windows® operating system authentication credentials, if available.
     - **Require**—Use only Windows operating system authentication credentials.

     Note: This setting is available only in the LDAP+GSSAPI setup.

Device Credentials

- **Anonymous LDAP Bind**—Bind the printer with the LDAP server anonymously. This option is applicable only if your LDAP server allows anonymous binding. Enabling this option does not require you to provide authentication credentials. This setting is available only in the LDAP setup.
- **Use Active Directory Device Credentials**—Use user credentials and group designations that are pulled from the existing network comparable to other network services. This option is available only in the LDAP +GSSAPI setup.
- If **Anonymous LDAP Bind** or **Use Active Directory Device Credentials** is disabled, then provide the authentication credentials used to bind the printer with the LDAP server.
  - **Device Username**
    - For LDAP setup, type the fully qualified distinguished name (DN) of a user registered to the LDAP server.
    - For LDAP+GSSAPI setup, type the DN of a user registered to the Kerberos server.
  - **Device Realm**—The realm used for the Kerberos server. This setting is available only in the LDAP +GSSAPI setup.
  - **Device Password**—Type the password for the user.

Advanced Options

- **Use SSL/TLS**—If the LDAP server requires SSL, then select **SSL/TLS**.
- **Userid Attribute**—Type the LDAP attribute to search for when authenticating users' credentials. The default value is **`sAMAccountName`**, which is common in a Windows operating system environment. For other directories you can type **`uid`**, **`cn`**, or a user-defined attribute. For more information, contact your system administrator.
- **Mail Attribute**—Type the LDAP attribute that contains the users' e-mail addresses. The default value is **`mail`**.
- **Full Name Attribute**—Type the LDAP attribute that contains the users' full names. The default value is **`cn`**.
- **Search Base**—The node in the LDAP server where user accounts reside. You can type multiple search bases, 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.
- **Follow LDAP Referrals**—Search the different servers in the domain for the logged-in user account.

Search Specific Object Classes

- **person**—Search the "person" object class.
- **Custom Object Classes**—Type the name of the custom object class to search.

  Note: A maximum of three custom object classes can be searched. Type the other object class in the other Custom Object Class field.

Address Book Setup

The following settings are used to configure the address book used when scanning to an e-mail address.

- **Displayed Name**—Select the LDAP attribute you want displayed on the address book.
- **Max Search Results**—Type the maximum search results displayed on the address book.
- **Use user credentials**—Use the logged-in user credentials to connect to the LDAP server.

- **Search Attributes**—Select LDAP attributes used as search filters.
- **Custom Attributes**—Type LDAP custom attributes used as search filters.

5 Click **Save and Verify**.

Editing or deleting LDAP or LDAP+GSSAPI login methods

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

2 From the Network Accounts section, click the LDAP or LDAP+GSSAPI login method.

3 Do either of the following:

- To edit the login method, update the LDAP or LDAP+GSSAPI settings, and then click **Save and Verify**.
- To delete login method, click **Delete LDAP**.

Using Kerberos

You can use this login method by itself or in conjunction with the LDAP+GSSAPI login method.

Notes:

- Only one Kerberos configuration file can be saved on the printer memory. This configuration file can apply to multiple realms and Kerberos Domain Controllers.
- Uploading another configuration file or updating the Kerberos settings overwrites the saved configuration file.
- If you want to delete a Kerberos file, then delete first the LDAP+GSSAPI login method that is using the file.
- Administrators must anticipate the different types of authentication requests the Kerberos server might receive, and configure the configuration file to handle the requests.
- Kerberos relies on an external server for authentication. If the server is down, then users are not able to access the printer using LDAP.
- To help prevent unauthorized access, log out from the printer after each session.

Creating a Kerberos login method

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

2 From the Network Accounts section, click **Add Login Method** > **Kerberos**.

3 Do one of the following:

Create a simple Kerberos configuration file

From the Generate Simple Kerberos File section, configure the following:

- **KDC Address**—Type the IP address or host name of the KDC IP.
- **KDC Port**—Enter the port number used by the Kerberos server.
- **Realm**—Type the realm used by the Kerberos server. The realm must be typed in uppercase.

Import a Kerberos configuration file

In the Import Kerberos File field, browse to the krb5.conf file.

4 If necessary, from the Miscellaneous Settings section, configure the following settings:

- **Character Encoding**—Select the character encoding used for the configuration file.
- **Disable Reverse IP Lookups**

5 Click **Save and Verify**.

Setting the date and time

When using Kerberos authentication, make sure that the time difference between the printer and the domain controller does not exceed five minutes. You can manually update the date and time settings or use the *Network Time Protocol* (NTP) to sync the time with the domain controller automatically.

1 From the Embedded Web Server, click **Settings** > **Device** > **Preferences** > **Date and Time**.

Using manual settings

Note: Configuring the manual settings disables NTP.

a From the Configure section, in the Manually Set Date & Time field, enter the appropriate date and time.

b Select the appropriate date format, time format, and time zone.

Note: If you select **(UTC+user) Custom**, then specify the offset values for UTC (GMT) and DST.

Using NTP

a From the Network Time Protocol section, select **Enable NTP**, and then type the IP address or host name of the NTP server.

b If the NTP server requires authentication, then select **MD5 key** in the Enable Authentication menu.

c In the Install MD5 key field, browse to the file containing the NTP authentication credentials.

2 Click **Save**.

Using Active Directory

You can use this login method by itself or in conjunction with the LDAP+GSSAPI login method.

Notes:

- Only one Kerberos configuration file can be saved on the printer memory. This configuration file can apply to multiple realms and Kerberos Domain Controllers.
- Administrators must anticipate the different types of authentication requests the Kerberos server might receive, and configure the configuration file to handle the requests.
- Uploading another configuration file or updating the Kerberos settings overwrites the saved configuration file.
- Kerberos relies on an external server for authentication. If the server is down, then users are not able to access the printer using LDAP.
- To help prevent unauthorized access, log out from the printer after each session.

Creating an Active Directory login method

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
2. From the Network Accounts section, click **Add Login Method** > **Active Directory**.
3. Configure the settings.
   - **Domain**—Type the realm or domain name of the Active Directory server.
   - **User Name**—Type the name of the user that can authenticate to the Active Directory.
   - **Password**—Type the password of the user.
   - **Organizational Unit**—Type the organizational unit attribute the user belongs to.
4. Click **Join Domain**.

Editing or deleting an Active Directory login method

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
2. From the Network Accounts section, click the Active Directory login method.
3. Do either of the following:
   - To delete the login method, click **Unjoin Domain**.
   - Configure the following settings, and then click **Save and Verify**.

     General Information

     - **Setup Name**—Type a unique name for the Active Directory login method.
     - **Server Address**—Type the IP address or the host name of the LDAP server.
     - **Server Port**—Enter the port where queries are sent.
     - **Required User Input**—Select the required authentication credentials when logging in to the printer.
     - **Use Integrated Windows Authentication**—Select one of the following:
       - **Do not use**
       - **Use if available**—Use Windows operating system authentication credentials, if available.

  - **Require**—Use only Windows operating system authentication credentials.

Device Credentials

- **Use Active Directory Device Credentials**—Use user credentials and group designations that are pulled from the existing network comparable to other network services.
- If **Use Active Directory Device Credentials** is disabled, then provide the authentication credentials used to bind the printer with the Active Directory server.
  - **Device Username**—Type the fully qualified DN of a user registered to the Active Directory server.
  - **Device Realm**—The Active Directory domain name.
  - **Device Password**—Type the password for the user.

Advanced Options

- **Use SSL/TLS**—If the LDAP server requires SSL, then select **SSL/TLS**.
- **Userid Attribute**—Type the LDAP attribute to search for when authenticating users' credentials. The default value is **`sAMAccountName`**, which is common in a Windows environment. For other directories you can type **`uid`**, **`cn`**, or a user-defined attribute. For more information, contact your system administrator.
- **Mail Attribute**—Type the LDAP attribute that contains the users' e-mail addresses. The default value is **`mail`**.
- **Full Name Attribute**—Type the LDAP attribute that contains the users' full names. The default value is **`cn`**.
- **Search Base**—The node in the LDAP server where user accounts reside. You can type multiple search bases, 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.
- **Follow LDAP Referrals**—Search the different servers in the domain for the logged-in user account.

Search Specific Object Classes

- **person**—Search the "person" object class.
- **Custom Object Classes**—Type the name of the custom object class to search.

  Note: A maximum of three custom object classes can be searched. Type the other object class in the other Custom Object Class field.

Address Book Setup

The following settings are used to configure the address book used when scanning to an e-mail address:

- **Displayed Name**—Select the LDAP attribute you want displayed on the address book.
- **Max Search Results**—Type the maximum search results displayed on the address book.
- **Use user credentials**—Use the logged-in user credentials to connect to the LDAP server.
- **Search Attributes**—Select LDAP attributes used as search filters.
- **Custom Attributes**—Type LDAP custom attributes used as search filters.

Creating LDAP, LDAP+GSSAPI, or Active Directory groups

Use groups to customize user access to applications and printer functions.

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
2. From the Network Account section, click the LDAP, LDAP+GSSAPI, or Active Directory login method.
3. Click **Manage Groups** > **Add Group**.
4. Do either of the following:

Search for the group name or user name

a. Select how you want to search for the group in your LDAP server.
b. Depending on the search scope selected, type the group name or user name.
c. Click **Search**.
d. Select the group you want to add.
e. Click **Add Selected**.

Add a group manually

a. Click **Manual Add**.
b. In the Group Name field, type the name of the group.
c. In the Group Identifier field, type the LDAP identifier for the group.
d. Click **Submit**.

5. Select the group, and then from the Access Controls section, select the functions, menus, and applications the group can access.
6. Click **Save**.

Notes:

- To import access controls from another group, click **Import Access Controls**, and then select a group.
- For more information on access controls, see “Understanding access controls” on page 21.

Editing or deleting LDAP, LDAP+GSSAPI, or Active Directory groups

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
2. Click the LDAP, LDAP+GSSAPI, or Active Directory login method, and then click **Manage Groups**.
3. Click the group, and then do either of the following:
   - Configure the access controls, and then click **Save**.
   - Click **Delete Group**.

Notes:

- To import access controls from another group, click **Import Access Controls**, and then select a group.
- To delete multiple groups, select the groups, and then click **Delete**.

- For more information on access controls, see “Understanding access controls” on page 21.

Understanding access controls

Access controls let you limit users’ access to functions, applications, and printer management.

Note: Some access controls are available only on some printer models.

Function Access

The following access controls allow users to access printer functions:

- **Search Address Book**
- **Create Profiles**—Create profiles for printing, copying, scanning, e-mailing, or faxing.
- **Manage Bookmarks**
- **Flash Drive Print**—Print from a flash drive.
- **Flash Drive Color Printing**—Print in color from a flash drive.
- **Flash Drive Scan**—Scan to a flash drive.
- **Copy Function**
- **Copy Color Printing**—Use the color copy function.
- **Color Dropout**—Use this feature when scanning or copying.
- **E-mail Function**
- **Fax Function**
- **FTP Function**—Scan to an FTP network folder.
- **Release Held Faxes**
- **Held Jobs Access**
- **Use Profiles**—Access profiles for scan shortcuts, workflows, and eSF applications.
- **Cancel Jobs at the Device**—Cancel jobs from the printer home screen.
- **Change Language from Home Screen**
- **Internal Printing Protocol (IPP)**—Configure and use IPP.
- **B/W Print**—Print in black and white.
- **Color Print**

Administrative Menus

The following access controls allow users to access the menus in the Embedded Web Server that are used to manage functions, applications, and security:

- **Security Menu**—Manage login methods and configure other security options.
- **Network/Ports Menu**—Configure network connections.
- **Paper Menu**—Configure the paper settings.
- **Reports Menu**—View reports.
- **Function Configuration Menus**—Configure the settings for the functions available in the printer.
- **Supplies Menu**—Manage printer supplies.
- **Option Card Menu**—Configure the option cards installed in the printer. This control is available only when an option card is installed.

- **SE Menu**—View diagnostic logs.
- **Manage Shortcuts**—Manage shortcuts available on the printer.
- **Address Book**—Manage the address book.
- **Device Menu**—Configure the printer firmware settings.

Device Management

The following access controls allow users to use printer management options:

- **Remote Management**—Access the printer remotely.
- **Firmware Updates**
- **Apps Configuration**—Configure the installed applications.
- **Operator Panel Lock**—Configure the locking function of the printer home screen. If this control is enabled, then users can lock and unlock the printer home screen.
- **Import / Export Settings**—Import or export a printer settings file (.ucf) from the Embedded Web Server.
- **Out of Service Erase**—Clear all settings, applications, and pending jobs stored in the printer memory, or erase all data in the printer hard disk.

Apps

Applications with access control are added in the function access group. Users are allowed to use the application when the application access control is selected.

Managing certificates

Certificates are used when you want the printer to establish an SSL, IPSec, and 802.1x connection and to identify securely other devices on the network. Printers can also use these certificates for LDAP over SSL authentication and address book look-ups.

Certificate Authorities (CA) are trusted locations established on the network that are required in secure environments. Otherwise, the default printer certificate is used to identify devices on the network.

Configuring printer certificate defaults

1. From the Embedded Web Server, click **Settings** > **Security** > **Certificate Management**.
2. From the Device Certificates section, click **Configure Certificate Defaults**.
3. Configure the settings.
   - **Friendly Name**—Type a unique name for the certificate.
   - **Common Name**—Type the name for the printer.

     Note: If you want to use the printer host name, then leave this field blank.
   - **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.
   - **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`**.

     Note: If your printer is using an IPv4 address, then leave this field blank.
4. Click **Save**.

Creating a printer certificate

1. From the Embedded Web Server, click **Settings** > **Security** > **Certificate Management**.
2. From the Device Certificates section, click **Generate**.
3. Configure the settings. For more information, see "Configuring printer certificate defaults" on page 23.
4. Click **Generate** or **Generate and Download**.

Installing certificates manually

Note: To download the CA certificate automatically, see “Installing certificates automatically” on page 24.

Before configuring Kerberos or domain controller settings, make sure to install the CA certificate used for domain controller validation. If you want to use chain validation for the domain controller certificate, then make sure to install the entire certificate chain. Each certificate must be in a separate PEM (.cer) file.

1. From the Embedded Web Server, click **Settings** > **Security** > **Certificate Management**.
2. From the Manage CA Certificates section, click **Upload CA**, and then browse to the PEM (.cer) file.

   Sample certificate:

   ```
   -----BEGIN CERTIFICATE-----
   MIIE1jCCA76gAwIBAgIQY6sV0KL3tIhBtlr4gHG85zANBgkqhkiG9w0BAQUFADBs
   …
   l3DTbPe0mnIbTq0iWqKEaVne1vvaDt52iSpEQyevwgUcHD16rFy+sOnCaQ==
   -----END CERTIFICATE-----
   ```
3. Click **Save**.

Installing certificates automatically

1. From the Embedded Web Server, click **Settings** > **Security** > **Certificate Management** > **Configure Certificate Auto Update**.
2. If you are prompted to join an Active Directory domain, then click **Join Domain**, and then type the domain information.
3. Select **Enable Auto Update**.

   Note: If you want to install the CA certificate without waiting for the scheduled run time, then select **Fetch Immediately**.
4. Click **Save**.

Viewing, downloading, and deleting a certificate

1. From the Embedded Web Server, click **Settings** > **Security** > **Certificate Management**.
2. Select a certificate from the list.
3. Click one or more of the following:
   - **Delete**—Remove a previously stored certificate.
   - **Download To File**—Download or save the certificate as a PEM (.cer) file.
   - **Download Signing Request**—Download or save the signing request as a .csr file.
   - **Install Signed Certificate**—Upload a previously signed certificate.

Note: To delete multiple certificates, select the certificates, and then click **Delete**.

Managing other access functions

Scheduling access to USB devices

In secure environments, devices can be configured to limit or disable the capabilities of USB host ports.

You can disable the front USB port using access control restrictions. Devices also have a rear USB port designed for card readers and human interface devices, such as a keyboard.

1. From the Embedded Web Server, click **Settings** > **Security** > **Schedule USB Devices**.
2. Select a device action, and then specify when the device performs the action.
3. Click **Save**.

Notes:

- For each Disable schedule entry, create an Enable schedule entry to reactivate use of the USB host ports.
- You can create multiple schedules.

Setting login restrictions

To prevent malicious access to a device, restrict the number of invalid login attempts and require a lockout time before letting users retry logging in.

Many organizations establish login restrictions for information assets such as workstations and servers. Make sure that device login restrictions also comply with organizational security policies.

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Restrictions**.
2. Set the login restrictions.
   - **Login failures**—Specify the number of times a user can attempt to log in before being locked out.
   - **Failure time frame**—Specify how long a user can attempt to log in before lockout takes place.
   - **Lockout time**—Specify how long the lockout lasts.
   - **Web Login Timeout**—Specify how long a user may be logged in remotely before being logged out automatically.
3. Click **Save**.

Configuring confidential printing

Users printing confidential or sensitive information may use the confidential print option. This option allows print jobs to remain in the print queue until the user enters a PIN on the printer control panel.

Note: This feature is available only in printer models that allow PIN selection from the control panel.

1. From the Embedded Web Server, click **Settings** > **Security** > **Confidential Print Setup**.
2. Enter an option for the following:
   - **Range**—Specify how many times an invalid PIN can be entered before being locked out.

Notes:

- When the limit is reached, the print jobs for that user name and PIN are deleted.
- This setting appears only when a formatted, working printer hard disk is installed.
- To turn off this setting, enter **0**.

- **Confidential Job Expiration**—Specify how long the printer stores confidential print jobs.

  Notes:

  - Changes in this setting do not affect the expiration time for confidential print jobs that are already in the printer memory or hard disk.
  - If the printer is turned off, then all confidential jobs held in the printer memory are deleted.
- **Repeat Job Expiration**—Specify how long the printer stores print jobs.
- **Verify Job Expiration**—Specify how long the printer stores print jobs needing verification.
- **Reserve Job Expiration**—Specify how long the printer stores print jobs for printing at a later time.
- **Require All Jobs to be Held**—Keep all jobs remain on the printer until released by an authorized user or until they expire.

3 Click **Save**.

Enabling solutions LDAP settings

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

2 Select one or more of the following:

- **Follow LDAP Referrals**—Search the different servers in the domain for the logged-in user account.
- **LDAP Certificate Verification**

  Note: You need to restart the device for the changes to take effect.

3 Click **Save**.

Showing secured applications or functions on the home screen

By default, the secured applications or functions are hidden from the printer home screen.

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

2 In the Protected Features menu, select **Show**.

3 Click **Save**.

Enabling print permission

Use this feature for cost control. Whether users are allowed to print (color or black and white) or not depends on the user's permission configuration. For more information, see "Managing login methods" on page 12.

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

2 Select **Print Permission**.

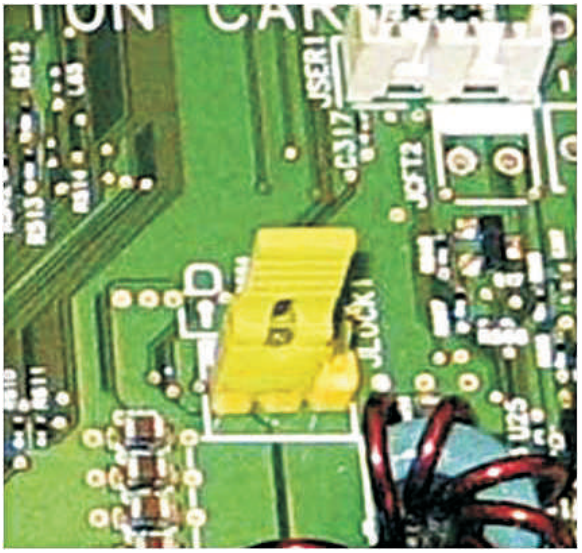
3 Click **Save**.

Enabling the security reset jumper

If the device is locked down due to a forgotten administrator password or lost network connectivity, then you can recover the device by resetting it. Access the controller board and move the reset jumper to cover the middle and unexposed prongs.

Using a cable lock to secure access to the controller board ensures that the device is not maliciously reset.

Warning—Potential Damage: Resetting the device deletes all customer data.



The secure reset feature requires specifying in the Embedded Web Server the effect of using the *security reset jumper*, which is on the controller board.

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

2 In the Security Reset Jumper menu, select either of the following:

- **Enable “Guest” access**—Provide guests with full access control.
- **No Effect**—All protected access controls remain protected.

  Warning—Potential Damage: If this option is selected, then the device is locked down and you cannot access the security menus. To replace the device controller board and regain access to the security menus, a service call is required.

3 Click **Save**.

Securing data

Erasing printer memory

To erase volatile memory or buffered data in your printer, turn off the printer.

To erase non-volatile memory or individual settings, printer and network settings, security settings, and embedded solutions, do the following:

1. From the Embedded Web Server, click **Settings** > **Device** > **Maintenance**.
2. From the Erase Printer Memory section, select **Sanitize all information on nonvolatile memory**.
3. If necessary, select either **Start initial setup wizard** or **Leave printer offline** after erasing the printer memory.
4. Click **Start**.

Erasing printer hard disk memory

Note: This process can take from several minutes to more than an hour, making the printer unavailable for other tasks.

1. From the Embedded Web Server, click **Settings** > **Device** > **Maintenance**.
2. From the Erase Hard Disk section, select **Sanitize all information on hard disk**.
3. Click **Start**.

Configuring printer hard disk encryption

Notes:

- Enabling disk encryption erases the contents of the hard disk. If necessary, back up important data from the printer before starting the encryption.
- Do not turn off the printer during the encryption process. Loss of data can occur.
- Disk encryption can take from several minutes to more than an hour, making the printer unavailable for other tasks.

1. From the Embedded Web Server, click **Settings** > **Security** > **Disk Encryption**.
2. Click **Start encryption**.

Restoring factory default settings

1. From the Embedded Web Server, click **Settings** > **Device** > **Restore Factory Defaults**.
2. Select **Restore all settings**.
3. Click **Start**.

Statement of Volatility

Your printer contains various types of memory that can store printer and network settings and user data.

Type of memory	Description
Volatile memory	Your printer uses standard *random access memory* (RAM) to buffer user data temporarily during simple print jobs.
Non-volatile memory	Your printer may use two forms of non-volatile memory: EEPROM and NAND (flash memory). Both types are used to store the operating system, printer settings, network information and bookmark settings, and embedded solutions.
Hard disk memory	Some printers have a hard disk drive installed. The printer hard disk is designed for printer-specific functionality. The hard disk lets the printer retain buffered user data from complex print jobs, form data, and font data.

Erase the content of any installed printer memory in the following circumstances:

- The printer is being decommissioned.
- The printer hard disk 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.
- The printer is being sold to another organization.

Disposing of a printer hard disk

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

In high-security environments, extra steps are needed to make sure that confidential data stored in the printer hard disk cannot be accessed. This precaution is necessary when the printer—or its hard disk—is removed from your premises.

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

Note: Most data can be erased electronically, but the only way to guarantee that all data are completely erased is to destroy physically each hard disk where data is stored.

Troubleshooting

User is locked out

Try one or more of the following:

Update the allowed number of login failures and lockout time

Note: This solution is applicable only in some printer models.

The user may have reached the allowed number of login failures.

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Restrictions**.
2. Update the allowed number of login failures and the lockout time.
3. Click **Save**.

   Note: Wait for the lockout time to pass before the new settings take effect.

Reset or replace the smart card

Check whether the type of smart card that you are using can be reset. If the card cannot be reset, then replace the card.

User is logged out automatically

Increase the Screen Timeout value

1. From the Embedded Web Server, click **Settings** > **Device** > **Preferences**.
2. Increase the Screen Timeout value.
3. Click **Save**.

User cannot access applications or functions

Make sure that the user is assigned to a group that has access to the applications and functions

For more information, see “Managing login methods” on page 12.

KDC and MFP clocks are out of sync

Make sure that the date and time settings on the printer are correct

For more information, see “Setting the date and time” on page 17.

Domain controller certificate is not installed

Make sure that the correct certificate is installed on the printer

For more information, see “Managing certificates” on page 23.

KDC is not responding within the required time

Try one or more of the following:

Make sure that the IP address or host name of the KDC is correct

Make sure that the KDC is available in the configuration file

You can add multiple KDCs in the configuration file.

Make sure that the server and firewall settings are configured to allow communication between the printer and the KDC server on port 88

LDAP lookups fail

Try one or more of the following:

Make sure that the server and firewall settings are configured to allow communication between the printer and the LDAP server on port 389 and port 636

The default ports are port 389 and port 636.

If reverse DNS lookup is not used in your network, then disable it in the Kerberos settings

1. From the Embedded Web Server, click **Settings** > **Security**.
2. From the Network Accounts section, click **Kerberos**.
3. From the Miscellaneous Settings section, select **Disable Reverse IP Lookups**.
4. Click **Save and Verify**.

If the LDAP server requires SSL, then enable SSL for LDAP lookups

Some solutions that provide authentication may require you to enable SSL for LDAP lookups. For more information, see the administrator’s guide for the solution.

Narrow the LDAP search base to the lowest possible scope that includes all necessary users

Make sure that all LDAP attributes that are being searched for are correct

Notices

Edition notice

May 2016

The following paragraph does not apply to any country where such provisions are inconsistent with local law: THIS PUBLICATION IS PROVIDED “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.

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

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.

Index