Advanced Authentication-Proximity Card

Installation and Configuration Guide

Version 2.2
This page is intentionally left blank.
Contents

Preface ............................................................................................................................ 5
How to Use This Manual.................................................................................................. 5
Symbols Used in This Manual......................................................................................... 5
Keys and Buttons Used in This Manual ....................................................................... 6
Displays Used in This Manual....................................................................................... 7
Abbreviations Used in This Manual............................................................................... 8
Hyperlinks ..................................................................................................................... 9
Legal Notices .............................................................................................................. 10
Trademarks ................................................................................................................ 10
Copyright ................................................................................................................... 10
Disclaimers ................................................................................................................ 10

Chapter 1 Introduction ..................................................................................... 11
1.1 Overview............................................................................................................. 11
1.2 AA-PROX System Requirements .................................................................... 12
1.2.1 Operating Environment.............................................................................. 12
1.2.2 Software Requirements.............................................................................. 12
1.2.3 Hardware Requirements............................................................................. 13
1.2.3.1 Approved Proximity Card Readers..................................................... 13
1.2.3.2 Approved Cards................................................................................. 14
1.2.3.3 Optional Hardware.......................................................................... 14
1.2.4 Software Interfaces..................................................................................... 14
1.2.5 Communication Interfaces......................................................................... 15
1.2.6 LDAP Requirements............................................................................... 15
1.2.7 MEAP Application Coexistence Support................................................. 16

Chapter 2 Installing AA-PROX ........................................................................ 17
Preface

Thank you for purchasing the Advanced Authentication-Proximity Card version 2.2 software application. Please read this manual thoroughly before operating the product on your MEAP-enabled device to familiarize yourself with its capabilities, and to make the most of its many functions. After reading this manual, store it in a safe place for future reference.

How to Use This Manual

This manual assumes that the reader has a good understanding of MEAP (Multifunctional Embedded Application Platform), Canon imageRUNNER ADVANCE machines, and the AMS (Access Management System) and UM (User Management) plug-ins for iWEMC (imageWARE Enterprise Management Console). It is strongly recommended that a System Administrator with advanced knowledge of their company’s authentication servers, users, network, and use of proximity cards install and configure the Advanced Authentication-Proximity Card V2.2 software.

This manual does not include the requirements or specifications for iWEMC or any other external application or library. This manual does not provide instructions for using or operating the Advanced Authentication-Proximity Card V2.2 application. For instructions on using the Advanced Authentication-Proximity Card V2.2 application, see the Advanced Authentication-Proximity Card User’s Guide.

Symbols Used in This Manual

The following symbols are used in this manual to explain procedures, restrictions, and instructions that should be observed for safety.

〇 IMPORTANT Indicates operational requirements and restrictions. Be sure to read these items carefully to operate the product correctly, and avoid damaging the machine.

اته NOTE Indicates a clarification of an operation, or contains additional explanations for a procedure. Reading these notes is highly recommended.
Keys and Buttons Used in This Manual

Keys for using the machine’s functions are located on the Main Menu screen. To use any of the desired function’s features, you must first press the key for the desired function. If the desired function is not displayed, press [Show All] or [▼] or [▲] to scroll to the desired function.

The following key and button names are a few examples of how keys and buttons to be pressed and clicked are represented in this manual:

- **Touch Panel Display Keys:**
  - Examples: [Key Name], [Keyboard Login], [Cancel]

- **Control Panel Keys:**
  - Examples: Key Icon (Key Name), ⚪ (Power), ⌀ (Log In/Out)

- **Buttons on Computer Operation Screens:**
  - Examples: [Button Name], [Install], [OK]
Displays Used in This Manual

Most screen shots used in this manual are those taken when the Advanced Authentication-Proximity Card V2.2 software is being installed using MEAP SMS (Service Management Service), and when the Advanced Authentication-Proximity Card V2.2 software is running on the imageRUNNER ADVANCE C5045 or imageRUNNER ADVANCE 6055.

The keys/buttons you should select or click are marked with a circle, as shown below. When multiple keys/buttons can be selected on the screen, all buttons are circled.

Example:

1. Click [SWITCH] for <AA-PROX>.

![Select this button for operation.](image)

NOTE

Some operating systems and browsers may display different screens and exhibit different behaviors.
# Abbreviations Used in This Manual

The following abbreviations are used in this manual.

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA-PROX</td>
<td>Advanced Authentication-Proximity Card version 2.2</td>
</tr>
<tr>
<td>AD</td>
<td>Active Directory</td>
</tr>
<tr>
<td>AMS</td>
<td>Access Management System</td>
</tr>
<tr>
<td>CSV</td>
<td>Comma Separated Value</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>GSS-API</td>
<td>Generic Security Service-Application Programming Interface</td>
</tr>
<tr>
<td>HID</td>
<td>Human Interface Device</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>iWEMC</td>
<td>imageWARE Enterprise Management Console</td>
</tr>
<tr>
<td>iW SAM iR Agent</td>
<td>imageWARE Secure Audit Manager imageRUNNER Agent</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>ldif</td>
<td>LDAP Data Interchange Format</td>
</tr>
<tr>
<td>MEAP</td>
<td>Multifunctional Embedded Application Platform</td>
</tr>
<tr>
<td>MEAP device</td>
<td>Supported Canon imageRUNNER ADVANCE multifunctional machine that features embedded MEAP technology.</td>
</tr>
<tr>
<td>NTLM</td>
<td>NT LAN Manager</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>P2P library</td>
<td>MEAP Peer-to-Peer Configuration library</td>
</tr>
<tr>
<td>PDF</td>
<td>Portable Document Format</td>
</tr>
<tr>
<td>SASL</td>
<td>Simple Authentication and Security Layer</td>
</tr>
<tr>
<td>SMS</td>
<td>Service Management Service</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>SSO-H</td>
<td>Single Sign-On Hybrid</td>
</tr>
<tr>
<td>UI</td>
<td>User Interface</td>
</tr>
<tr>
<td>UM plug-in</td>
<td>iWEMC User Management plug-in</td>
</tr>
</tbody>
</table>

**NOTE**

When you refer to the iWEMC AMS Plug-in or UM Plug-in manuals, you will see references to SSO-H. To avoid any confusion, please substitute AA-PROX for all references to SSO-H in these manuals.
Hyperlinks

When this manual is in its native PDF form, the blue underlined text represents a hyperlink to the corresponding sections of this manual or to external Web sites.

For example: See Chapter 1, “Introduction,” on p. 11.

Likewise, all entries in the Table of Contents are hyperlinks.
Legal Notices

Trademarks

Canon, the Canon logo, imageRUNNER, imageRUNNER ADVANCE, and MEAP are registered trademarks, and the MEAP logo is a trademark, of Canon Inc. in the United States and may also be a trademark or registered trademark in other countries.

Adobe and Adobe Acrobat are trademarks of Adobe Systems Incorporated.

Microsoft, Windows, Windows Server, and Internet Explorer are registered trademarks of Microsoft Corporation in the United States and are trademarks or registered trademarks of Microsoft Corporation in other countries.

Java and all Java-based trademarks and logos are the trademarks or registered trademarks of Sun Microsystems, Inc. in the United States or other countries.

Other product and company names herein are, or may be, the trademarks of their respective owners.

Copyright

Copyright 2012 by Canon U.S.A., Inc. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or by any information storage or retrieval system without the prior written permission of Canon U.S.A., Inc.

Disclaimers

The information in this document is subject to change without notice.

CANON U.S.A., INC. MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, EITHER EXPRESS OR IMPLIED, EXCEPT AS PROVIDED HEREIN, INCLUDING WITHOUT LIMITATION, THEREOF, WARRANTIES AS TO MARKETABILITY, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE OR NON-INFRINGEMENT. CANON U.S.A., INC. SHALL NOT BE LIABLE FOR ANY DIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY NATURE, OR LOSSES OR EXPENSES RESULTING FROM THE USE OF THIS MATERIAL.
Chapter 1 Introduction

This chapter describes the overview of the AA-PROX software, the system requirements for installing, configuring, and operating the software.

1.1 Overview

The AA-PROX software is an integrated MEAP application. It should be installed and operated on a supported Canon MEAP-enabled device, and provides user authentication via user name and password or proximity card, and access to these devices.

AA-PROX can be configured for remote (Active Directory) or local user management, with optional walk-up user registration via its Configuration servlet. AA-PROX provides function restrictions, secure printing, device log on capabilities, and does not interfere with any of the MEAP device’s built-in functions, such as Copy, Print, and Scan.

AA-PROX is designed to perform the following functions once configured from the AA-PROX Configuration servlet:

- Provide support for RF IDeas pcProx Card Reader-based authentication.
- Provide support for alternative user name/password-based authentication.
- Provide authentication against an Active Directory server.
- Provide authentication against the device’s local user database.
- Support for Local User Database Management.
- Support for AMS Role Configuration.
- Support for Device Level Log-in/Function Level Log-in.
- Provide authenticated users access to device level functions.
- Ability to differentiate between non-secure and secure print jobs.
- Ability to print domain user-based print jobs via Local Device Authentication.
- Provide access to the device’s Quick Menu.
- Provide compatibility with iR ADVANCE Desktop to create the Quick Menu.
- Provide compatibility with iW SAM iR Agent, iWEMC UM and AMS plug-ins.
- Support for Local Device Authentication for Department ID Management.
- Ability to configure access to multiple Active Directory servers for user authentication.
- Ability for the user to register their proximity card ID badge.
- Ability to log debug information.
- Support for USB keyboard entry.

!! IMPORTANT
System Administrator knowledge of Microsoft Windows and Canon MEAP-enabled devices is necessary to install and configure the AA-PROX software.
1.2 AA-PROX System Requirements

The AA-PROX software requires the proper installation and configuration of all items documented in this guide. Failure to correctly install or configure the software will affect its operation.

1.2.1 Operating Environment

To authenticate a proximity card user, the MEAP device must be on the same network as an Active Directory authentication server, running MS Windows Server 2003 SP2 (32-bit), Server 2008 SP1 (32- or 64-bit), or Server 2008 R2 (64-bit).

**IMPORTANT**
- If you are using Windows Server 2008 R2 with Domain Authentication, make sure that the domain’s security policy is set to allow the DES-CBC-MD5 or AES128-HMAC-SHA1 encryption type. AA-PROX only supports the DES-CBC-MD5 and AES128-HMAC-SHA1 encryption types.
- Multi-homed domain controller environments are not supported.
- AA-PROX requires Kerberos pre-authentication. When you are configuring your Windows environment, make sure that the [Do not require Kerberos preauthentication] check box is **NOT** selected for all Active Directory accounts.

1.2.2 Software Requirements

The following software is required by AA-PROX:

- Internet Explorer 7.0 or later with JavaScript enabled is required for the Configuration servlet.
- Sun JRE (Java Runtime Environment) 5.0 or later
1.2.3 Hardware Requirements

AA-PROX is designed to operate on the following Canon MEAP-enabled devices using the minimum specified MEAP Contents version.

<table>
<thead>
<tr>
<th>Device Family</th>
<th>MEAP Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>imageRUNNER ADVANCE C9075/C9065/C7065/C7055</td>
<td>25.23</td>
</tr>
<tr>
<td>imageRUNNER ADVANCE C5051/C5045/C5035/C5030</td>
<td>20.25</td>
</tr>
<tr>
<td>imageRUNNER ADVANCE 8105/8095/8085</td>
<td>10.30</td>
</tr>
<tr>
<td>imageRUNNER ADVANCE 6075/6065/6055</td>
<td>10.30</td>
</tr>
<tr>
<td>imageRUNNER ADVANCE C2020/C2030</td>
<td>12.02 (System Software)</td>
</tr>
<tr>
<td>imageRUNNER ADVANCE 4051/4045/4035/4025</td>
<td>11.10</td>
</tr>
</tbody>
</table>

**NOTE**
The imageRUNNER ADVANCE C2020 and imageRUNNER ADVANCE C2030 support all released system software versions.

1.2.3.1 Approved Proximity Card Readers

The following USB proximity card readers have been approved:

<table>
<thead>
<tr>
<th>Name</th>
<th>Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFIdeas pcProx Plus</td>
<td>RDR-80581AKU</td>
</tr>
<tr>
<td>RFIdeas pcProx (for HID)</td>
<td>RDR-6081AKU</td>
</tr>
<tr>
<td>RFIdeas pcProx (for Casi-Rusco)</td>
<td>RDR-6281AKU</td>
</tr>
<tr>
<td>RFIdeas AIR ID Enroll for iClass</td>
<td>RDR-7081AKU</td>
</tr>
<tr>
<td>RFIdeas AIR ID Enroll for MIFARE</td>
<td>RDR-7581AKU</td>
</tr>
</tbody>
</table>

**IMPORTANT**
Card readers and cards are specific to your installation location. For more information about your specific card reader and cards, contact your local authorized Canon dealer, or see the documentation that came with your proximity card reader.
1.2.3.2 **Approved Cards**

The following proximity cards have been approved:

- HID
- HID iClass
- HID Casi-Rusco

1.2.3.3 **Optional Hardware**

<table>
<thead>
<tr>
<th>Device</th>
<th>Model</th>
<th>Vendor ID</th>
<th>Product ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB Keyboard</td>
<td>Cherry G84</td>
<td>0x046A</td>
<td>0x0001</td>
</tr>
</tbody>
</table>

1.2.4 **Software Interfaces**

The following software interfaces can be used with AA-PROX:

- iWEMC v3.0.1
- iWEMC AMS Plug-In v3.0.1
- iWEMC UM Plug-In v2.0.2 (bundled with the AMS Plug-In)
- imageRUNNER ADVANCE Desktop
- imageRUNNER ADVANCE Tracker v1.0
- AMS Printer Driver Add-In v3.0
- imageWARE Secure Audit Manager iR Agent v1.2
- PS/PCL/UFR II Printer Drivers for all supported devices. (See “Hardware Requirements,” on p. 13.)
1.2.5 Communication Interfaces

The table below shows the different communication interfaces, their specific port numbers, and descriptions used with AA-PROX.

<table>
<thead>
<tr>
<th>Communication Interface</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTLM</td>
<td>Dynamic – Determined by AD server</td>
<td>Used for authentication between the MEAP device and the iWEMC UM/AMS Plug-ins and AMS Printer Driver Add-In v3.0.</td>
</tr>
<tr>
<td>Kerberos</td>
<td>TCP/UDP Port 88</td>
<td>Used for authentication between the MEAP device and AD domain controller.</td>
</tr>
<tr>
<td>HTTP</td>
<td>TCP Port 8000</td>
<td>Used to access the Configuration servlet.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>TCP Port 8443</td>
<td>Used to access the secure Configuration Servlet.</td>
</tr>
<tr>
<td>LDAPv3</td>
<td>TCP Port 389</td>
<td>Used for communication between the MEAP device and AD domain controller.</td>
</tr>
<tr>
<td></td>
<td>TCP Port 636</td>
<td>Used for SSL communication between the MEAP device and the AD domain controller.</td>
</tr>
</tbody>
</table>

1.2.6 LDAP Requirements

The table below describes the LDAP attributes that are required for domain authentication.

<table>
<thead>
<tr>
<th>Item</th>
<th>LDAP Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proximity Card</td>
<td>info (default)</td>
</tr>
<tr>
<td>Display Name</td>
<td>cn</td>
</tr>
<tr>
<td>E-mail Address</td>
<td>mail</td>
</tr>
<tr>
<td>Role</td>
<td>Optional. Configurable with the iWEMC AMS Plug-In. See the iWEMC AMS Plug-In User’s Guide.</td>
</tr>
</tbody>
</table>
1.2.7  MEAP Application Coexistence Support

AA-PROX V2.2 can coexist with other installed MEAP applications that have received verification by Canon U.S.A., Inc., provided that there are sufficient resources available on the MEAP device.

AA-PROX V2.2 requires the following MEAP resources:

- A maximum file space usage of 25,500 KB
- A maximum memory usages of 6,000 KB
- A maximum file descriptor usage of 35
- A maximum socket usage of 33
- A maximum thread usage of 40

AA-PROX V2.2 has been confirmed to coexist with the Authorized Send v4.5 software application.
Chapter 2 Installing AA-PROX

This chapter describes how to install and start the AA-PROX software on a MEAP-enabled machine using the MEAP SMS program.

There are three procedures to follow to use the proximity card reader with your MEAP device.

1. Install the AA-PROX software via SMS with a properly issued license file.
2. Connect the USB proximity card reader to the MEAP device.
3. Configure the AA-PROX software.

The System Administrator for the target MEAP device must install the AA-PROX software using a networked computer that is connected to the MEAP device.

MEAP SMS is the program interface used to install the AA-PROX software. You can access the SMS Login screen via a Web browser.

IMPORTANT
- Do not use the browser’s [Back] and [Forward] buttons during the installation process. Only use the clickable links in the browser’s window.
- MEAP Settings and Use HTTP settings (from the Settings/Registration screen) on the MEAP device must be enabled. (See “Activating the Use HTTP Settings,” on p. 30.)
- For more information on using SMS or uninstalling MEAP applications, see the MEAP e-Manual that came with your MEAP device.
- For more information on connecting the USB proximity card reader, see the documentation that came with your card reader.

1. Open a browser window ➔ enter the following URL:

   http://<IP>:8000/sms
   https://<IP>:8443/sms (if you are using SSL for communications)

   (Replace <IP> with the IP address of the MEAP device.)
2. Enter **MeapSmsLogin** in the [Password] text box ➞ click [Log In].

![Image of login page]

The SMS MEAP Application Management screen is displayed.

**IMPORTANT**

The default password is ‘MeapSmsLogin’ (case-sensitive). If this password was changed from the default one, you must enter the correct password to access SMS. If you forget your password, contact your local authorized Canon dealer.

3. Click [Enhanced System Application Management].

![Image of Enhanced System Application Management screen]

The Enhanced System Application Management screen is displayed.
4. Click [Browse] to the right of <Enhanced System Application File Path>.

5. Navigate to the drive or directory containing the .jar file → select the file → click [Open].

**IMPORTANT**

Make sure that you select the file that ends with the .jar extension for the enhanced system application file.

6. Verify that the correct file was selected.
7. Click [Browse] to the right of <License File Path>.

8. Navigate to the drive or directory containing the .lic file ➞ select the file ➞ click [Open].

   IMPORTANT
   Make sure that you select the file that ends with the .lic extension for the license file.

9. Verify that the correct file was selected ➞ click [Install].

The message <Preparing to install.> is displayed.
10. Click [Yes].

During installation, the message <Installing…Please wait.> is displayed.

NOTE
To cancel the installation, press [Cancel].
11. Click [SWITCH] for <AA-PROX> to change the default authentication method to AA-PROX.

The status of AA-PROX changes to <Start after Restart> if successful.
12. Restart the MEAP device.

**IMPORTANT**

If you are switching from the SSO-H Login Service to AA-PROX, or if you have trouble logging on after upgrading from SSO-H, you may need to restart the machine again to gain access to the Configuration Servlet.

Installation is complete, and AA-PROX starts.

For instructions on restarting the MEAP device, see the appropriate e-Manual that came with your machine.

13. Plug a USB proximity card reader into the USB port on the MEAP device.

This page is intentionally left blank.
Chapter 3 Configuring AA-PROX

This chapter describes how to properly configure AA-PROX.

3.1 Overview

You can configure AA-PROX to handle Local Device Authentication, Domain Authentication using an AD domain controller, or both Local Device Authentication and Domain Authentication with or without the AMS Plug-in option.

The AMS is a system for managing device usage restrictions. The table below describes the functions and their corresponding restrictions that can be managed when you use the AMS. Using AMS with AA-PROX improves security and can reduce copying/printing costs.

<table>
<thead>
<tr>
<th>Function</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Print</td>
<td>Color printing, one-sided prints, page layout printing, saving to user inboxes</td>
</tr>
<tr>
<td>Save</td>
<td>Color printing user inbox documents, one-sided prints, page layout printing</td>
</tr>
<tr>
<td>Copy</td>
<td>Color copying, one-sided copies, page layout copying</td>
</tr>
<tr>
<td>Scan</td>
<td>Color scanning</td>
</tr>
<tr>
<td>Send</td>
<td>Sending e-mail, I-faxes, faxes, sending to file servers, specifying destinations, specifying the format for sending, registering network destinations</td>
</tr>
</tbody>
</table>
If you use AA-PROX with the AMS option and configure the Login settings and Access Mode settings in the Configuration servlet, there are four options that can be used to manage the device and user authentication and usage restrictions. For more information on specifying these settings, see Chapter 4, “Role Management,” on p. 121.

1. Device-Level Log-in: When a user walks up to a MEAP device, the Log In screen is displayed. To gain access to the device, the user must authenticate by swiping their proximity card or by directly entering his/her user name and password. See Chapter 2, “Using AA-PROX,” in the Advanced Authentication-Proximity Card User’s Guide. After authentication to the device is successful, only the functions the user is permitted to access are available on the touch panel display of the MEAP device.

2. Function Level Log-in: When a user walks up to a MEAP device, the Log In screen is not displayed. However, if user information, such as user name, password, and restrictions have been registered, when the user presses a function key that is set with restrictions on the Main Menu of the touch panel display, the Log In screen appears. To gain access to the desired function, the user must be authenticated. If authentication is successful, the user is allowed to use that function.

3. Function Restrictions: If function restrictions have been configured for a user, the unavailable functions and applications for that user are either grayed out or are not displayed after the user logs on to the machine. For more information on setting function and application restrictions for a user, see “Creating Custom Roles,” on p. 123.

4. Printing from a Computer: If you want to restrict printing from computers, you must set up and install the AMS Printer Driver Add-in, and set user information for all client computers that use the MEAP device (after setting up the AMS). If client computers have been set up and the AMS Printer Driver Add-in is installed, when a user wants to print, an authentication dialog box appears. If authentication is successful, a confirmation dialog box that displays the restricted printing functions appears.

**IMPORTANT**

- It is necessary to configure AA-PROX from a Web browser on any computer that can access the network where the MEAP device is located.
- Before you configure AA-PROX, you must prepare the target MEAP device and network environment. See “Preparing the Device and Network Environment,” on p. 29.
- Before you configure AA-PROX to use the AMS, you must register a license for the AMS Kit in the target MEAP device. For more information on registering a license for the AMS, see the Access Management System Kit Administrator Guide.
- The configuration screen is password protected. A valid logon session is required to configure AA-PROX.
3.1.1 User Authentication Methods

AA-PROX enables you to configure three user authentication methods: Local Device Authentication, Domain Authentication, and Local Device + Domain Authentication. A Guest User account can also be configured to authenticate guest users to the device.

**Local Device Authentication** – Performs user information management and user authentication at the device. When a user enters a user name and password, or swipes their proximity card, user authentication is performed based on the local user information registered in the machine (via AA-PROX’s Configuration servlet).

**Domain Authentication** – Uses domain user information registered in AD to perform user authentication. When a user enters a user name and password, or swipes their proximity card, user authentication is performed by AD.

**Local Device + Domain Authentication** – Depending on how a user is configured in AA-PROX (either a local user or a domain user), access to the device is provided as described above for Local Device Authentication and Domain Authentication.

**Guest User** – When the AMS is active, designated guest users can log on to the device without using any credentials or swiping a proximity card. The Guest User account exists on the local database, but can be accessed even if AA-PROX is configured for Domain Authentication. For more information on configuring a guest user account, see “Registering Users,” on p. 137.
3.1.2 Administrator Functions

The Administrator functions listed below can be performed using AA-PROX’s Configuration servlet.

- Configure AA-PROX settings (extended under SSO-H)
- Configure User Management settings
- Configure user roles (if the AMS Kit’s license is registered and installed)
- Enable logging and upload a customized logo to the AA-PROX UI screen on the MEAP device.

3.1.3 User Functions

The user can interact with AA-PROX in the following ways:

- Authenticate to the device locally or via a domain with a proximity card.
- Authenticate to the device locally by directly entering their user name and password.
- Authenticate to the device with domain credentials (user name and password for a domain the user selects on the Log In screen).
- Select a domain to authenticate against.
- Self-register their proximity card in the device’s local database, and then authenticate to it.
- Self-register their proximity card to a domain, and then authenticate to it.
3.2 Preparing the Device and Network Environment

Before you configure AA-PROX, you must specify the following device settings to use AA-PROX for authentication:

1. Specify the Network Settings.
2. Activate the Use HTTP setting.
3. Synchronize the Date and Time Settings.
4. Specify the DNS name and DNS server settings

3.2.1 Specifying the Network Settings

Make sure that the correct IP address is set on the machine, and specify the necessary network settings by pressing (Settings/Registration) ➞ [Preferences] ➞ [Network].

⚠️ IMPORTANT

- If the device is already operating on the network (i.e., documents can already be printed or sent from a computer), this operation is not necessary.
- For more information on specifying the Network settings, see the Network e-Manual that came with your machine.
3.2.2 Activating the Use HTTP Setting

To enable access to the machine via a Web browser, or operate the AMS with AA-PROX, you must activate the Use HTTP setting.

**IMPORTANT**
You cannot connect to the machine via a proxy server. If you are using a proxy server, in the proxy server settings of your Web browser, add the IP address of the machine in the [Exceptions] (addresses that do not use a proxy server) list.

Follow the procedure below to activate Use HTTP on the MEAP device.

1. On the machine’s control panel, press ☰ (Settings/Registration).
2. Press [Preferences].

If the System Manager ID and System Password have been set, press [Log In] ➔ enter the System Manager ID and System PIN using ⓪ – ⓫ (numeric keys) ➔ press [Log in].
3. Press [Network].

4. Press [TCP/IP Settings].
5. Press [Use HTTP].

![Settings/Registration](image)

*NOTE*

If the desired setting is not displayed, press [▼] or [▲] to scroll to the desired setting.

6. Press [On] ➞ [OK].

![Settings/Registration](image)


For instructions on restarting the machine, see the appropriate e-Manual.
3.2.2.1 Specifying to Use SSL Communication

If you want to use SSL (Secure Sockets Layer) communication to access AA-PROX’s Configuration servlet, you must specify the SSL Settings mode.

Follow the procedure below to specify the SSL Settings mode on the MEAP device.

**IMPORTANT**
Before you set the SSL Settings mode to ‘On’, you must set a default key in Preferences (from the Settings/Registration screen). See the Settings/Registration e-Manual.

1. On the machine’s control panel, press ☰ (Settings/Registration).

2. Press [Management Settings].

If the System Manager ID and System Password have been set, press [Log In] → enter the System Manager ID and System PIN using ⑩ – ⑪ (numeric keys) → press [Log in].
3. Press [License/Other].

4. Press [MEAP Settings].
5. Press [SSL Settings].


For instructions on restarting the machine, see the appropriate e-Manual.
3.2.3  **Synchronizing the Device and AD Server Time**

If you configure an AD server for Domain Authentication, you must ensure that the device clock and server clock are synchronized within the maximum server specified clock skew tolerance of ‘5’ minutes. If there is more than a 5 minute time difference between the device clock and server clock, a login error will occur.

To automatically synchronize the device’s system time with a public time server, set the SNTP (Simple Network Time Protocol) settings.

Follow the procedure below to synchronize the device and AD server time.

1. On the machine’s control panel, press ☰ (Settings/Registration).
2. Press [Preferences].

   ![Settings/Registration](image)

   If the System Manager ID and System Password have been set, press [Log In] ➞ enter the System Manager ID and System PIN using ☰ – ☰ (numeric keys) ➞ press [Log in].
3. Press [Network].

4. Press [TCP/IP Settings].
5. Press [SNTP Settings].

![SNTP Settings](image)

**NOTE**
If the desired setting is not displayed, press [▼] or [▲] to scroll to the desired setting.
6. Specify the SNTP settings.

<Use SNTP>: Select [On] to perform time synchronization using SNTP.

<Polling Interval>: Select the interval for performing time synchronization from ‘1’ to ‘48’ hours.

[NTP Server Address]: Enter the NTP server address or host name.
7. Press [Check NTP Server] to check the status of the NTP server.

![Image of Settings/Registration screen showing SNTP settings]

If <OK> is displayed next to [Check NTP Server], time synchronization is working correctly via SNTP.

If <Error> is displayed next to [Check NTP Server], check the settings for [NTP Server Address] set in step 6.

8. Press [OK] ➞ [Close].

The Main Menu screen appears.

**IMPORTANT**

To perform time synchronization via SNTP, it is necessary to set the time zone of the region in which you are using the machine in advance. For instructions on setting the time zone, see the appropriate e-Manual that came with your machine.
3.2.4 Specifying the DNS Server and Name Settings

Specify the DNS Server and DNS Name settings so that the domain name of the Active Directory server used for authentication (the IP address of the domain controller) can be retrieved.

Follow the procedure below to specify the DNS Server and DNS Name settings.

1. On the machine’s control panel, press (Settings/Registration).

2. Press [Preferences].

If the System Manager ID and System Password have been set, press [Log In] ➞ enter the System Manager ID and System PIN using 0 – 9 (numeric keys) ➞ press [Log in].
3. Press [Network].

4. Press [TCP/IP Settings].
5. Press [DNS Settings].

6. Press [DNS Server Address Settings].
7. Press [Primary DNS Server] ➞ enter the IP address using ① – ⑨ (numeric keys) ➞ press [OK].

8. Press [DNS Host/Domain Name Settings].
9. Under <IPv4>, press [Host Name] ➞ enter the host name ➞ press [OK].

10. Under <IPv4>, press [Domain Name] ➞ enter the name of the domain in which the machine is located ➞ press [OK].
11. Press [OK] ➔ [Close].

The Main Menu is displayed.

12. Restart the machine.

   For instructions on restarting the machine, see the appropriate e-Manual.
### 3.3 Logging On to AA-PROX

Follow the procedure below to log on to AA-PROX’s Configuration servlet.

---

1. Open a browser window ➔ enter the following URL:

   - `http://<device IP>:8000/aaprox`
   - `https://<device IP>:8443/aaprox` (if the SSL Settings are enabled)

   (Replace `<device IP>` with the IP address of the MEAP device.)

   The Login screen is displayed.

   **IMPORTANT**
   Enter `aaprox` exactly as shown, as it is case-sensitive.

2. Enter the Administrator’s user name and password ➔ select [This device] from the Login Destination drop-down list ➔ click [Log In].

   ![Login Screen](image)

   **NOTE**
   - The [Password] text box displays a solid black circle (●) for each character entered. (Note that some browsers may display asterisks or some other symbol.)
   - If authentication succeeds, the AA-PROX Configuration screen is displayed.
3.4 Configuring AA-PROX without AMS

This section describes how to configure AA-PROX for Local Device Authentication, Domain Authentication, and Domain Authentication + Local Device Authentication without the AMS Plug-In.

3.4.1 Local Device Authentication Configuration without AMS

Follow the procedure below to configure the Local Device Authentication settings without the AMS option.

1. Log on to the AA-PROX Configuration servlet.

   For instructions, see “Logging On to AA-PROX,” on p. 48.

2. Click [Configuration].

4. If you want to enable the [Keyboard Login] button on the AA-PROX Log In screen on the MEAP device, make sure the [Allow keyboard authentication] check box is selected.

5. Select the [LDAP uses SSL] check box if you want future communication with AD to be encrypted.

When the [LDAP uses SSL] check box is selected, the [LDAP Port] field is automatically set to port ‘636’. If the [LDAP uses SSL] check box is not selected, the [LDAP Port] field reverts back to its default port number ‘389’.

If you do not want to use SSL for LDAP communication, clear the [LDAP uses SSL] check box → enter the LDAP port number directly into the [LDAP Port] field.
6. If you want a user to always enter a password after they swipe their proximity card, select the [Is a password required?] check box.
7. Select the number of users to display in the User Name drop-down list on the Log In screen of the MEAP device from the Number of Login Users to Display drop-down list.

[0]: The drop-down arrow (▼) next to [User Name] on the Log In screen of the MEAP device is not displayed, and a user must enter their user name every time they log on to the machine.

[1]: Only the user name of the last user who logged on to the machine is displayed.

[Max (Maximum Number of a Device)]: The user names of the last seven users who logged on to the machine are displayed in the User Name drop-down list.
8. Click [Update] ➞ restart the machine.

**IMPORTANT**
Changes made to the AA-PROX Configuration settings only take affect after the machine is restarted. For instructions on restarting the MEAP device, see the appropriate e-Manual that came with your machine.

### 3.4.2 Domain Authentication Configuration without AMS

Follow the procedure below to configure the Domain Authentication settings without the AMS option.

**IMPORTANT**
Make sure that the network settings for AD are set up properly for the domain to which you want users to authenticate, or users will not be able to log on.
See “Preparing the Device and Network Environment,” on p. 29.

1. Log on to the AA-PROX Configuration servlet.
   
   For instructions, see “Logging On to AA-PROX,” on p. 48.

2. Click [Configuration].
3. Select [Domain Authentication] from the User Authentication System drop-down list.

![Configuration Screen]

**IMPORTANT**

If the User Authentication System was originally set to ‘Local Device Authentication’, and you are switching to ‘Domain Authentication’, click [Update] → restart the machine to display the local domains stored on the machine.
4. Click [Edit domain authentication settings] if you want to edit the configured domain credentials for users who log on to the MEAP device by using a proximity card or perform self-registration using Domain Authentication.

**IMPORTANT**

- The Edit domain authentication settings table is not displayed until an authentication attempt for the first time is successfully performed against the domain to which the machine belongs. After the first successful domain authentication attempt, the table will contain a list of domains, user names and passwords.
- AA-PROX communicates with each AD domain controller that uses a configured user name and password associated with the target domain when a user presents a proximity card to AA-PROX for authentication.
- The user name and password fields are automatically populated.
- AA-PROX stores the specified user name and password within a configuration file as clear text.
4.1 If necessary, enter the proximity card ID’s LDAP attribute name that matches the one specified in the AD domain controller.

The default attribute name is ‘info’.

**IMPORTANT**
- Make sure that before you configure the LDAP attribute, the LDAP attribute field in the AD domain controller for the configured account in the domain authentication settings table, has the ‘Write’ permission.
- It is important to configure this field so that users can perform self-registration and authenticate with a proximity card ID against an AD domain controller.
4.2 If you want to edit the configured domain credentials for users who log on to the MEAP device by using a proximity card or perform self-registration using Domain Authentication, enter a new user name and password that is associated with the target domain, or edit the current user name and password.

Press [Test] next to the desired domain to validate the user name and password. If validation is successful, [Test] changes to [OK]. If validation is not successful, [Test] changes to [NG] (No Good). If you mouse-over [NG], an error message within a tool tip box may be displayed.

**IMPORTANT**
- The domain authentication settings table is not displayed until an authentication attempt for the first time is successfully performed against the domain to which the machine belongs. After the first successful domain authentication attempt, the table will contain a list of domains.
- AA-PROX communicates with each AD domain controller that uses a configured user name and password associated with the target domain when a user presents a proximity card to AA-PROX for authentication. However, even if a user successfully authenticates to the domain via self-registration, the user’s attempt at authentication with a proximity card may fail, unless the AA-PROX Administrator sets up an appropriate domain user settings account and password for the target domain in this step.
- AA-PROX stores the specified user name and password within a configuration file as clear text.

**NOTE**
If you do not want the domain authentication settings table displayed, click the [Hide] link. [Hide] changes to [Edit domain authentication settings].
5. If you want to enable the [Keyboard Login] button on the AA-PROX Log In screen on the MEAP device, make sure the [Allow keyboard authentication] check box is selected.

6. Select the [LDAP uses SSL] check box if you want future communication with AD to be encrypted.

When the [LDAP uses SSL] check box is selected, the [LDAP Port] field is automatically set to port ‘636’. If the [LDAP uses SSL] check box is not selected, the [LDAP Port] field reverts back to its default port number ‘389’.

If you do not want to use SSL for LDAP communication, clear the [LDAP uses SSL] check box → enter the LDAP port number directly into the [LDAP Port] field.
7. If you want a user to always enter a password after they swipe their proximity card, select the [Is a password required?] check box.

8. If you want to specify a new user group for the domain administrator, enter the new group name in the [User Group Name] text box.

**NOTE**
- The default user group name is ‘Canon Peripheral Admins’. If the default user group name is changed, make sure that the domain administrator is a part of the user group specified above.
- If you change the User Group Name, the message, <Are you sure you want to change the user group name to <NAME OF DOMAIN>?> appears. Click [OK]. If you click [Cancel] instead of [OK], the message, <Restore user group name.> appears. Click [OK], and the User Group Name is restored.
9. Select the number of users to display in the User Name drop-down list on the Log In screen of the MEAP device from the Number of Login Users to Display drop-down list.

[0]: The drop-down arrow (▼) next to [User Name] on the Log In screen of the MEAP device is not displayed, and a user must enter their user name every time they log on to the machine.

[1]: Only the user name of the last user who logged on to the machine is displayed.

[Max (Maximum Number of a Device)]: The user names of the last seven users who logged on to the machine are displayed in the User Name drop-down list.
10. If multiple sites are operating in the specified domain, select the [Set access mode in sites] check box to prioritize access to the domain controller in the site to which the machine belongs, or enable access to domain controllers outside the site to which the machine belongs.

IMPORTANT

- The domain controllers are accessed in the same order as the list of domain controllers retrieved from the DNS server.
- Site information is only retrieved when you access the device (log on) directly via its UI. Site information cannot be retrieved if you log on to the machine via a Web browser.
10.1 To specify how to retrieve site information, select the [Only at First Time] or [Every time when device starts up] radio button.

[Only at First Time]:
Uses the list of domain controllers retrieved when a user logs on to the machine the first time.

[Every time when device starts up]:
Retrieves the list of domain controllers every time the machine is powered ON.

⚠️ IMPORTANT
Only a maximum of 10 domains is retrieved.
10.2 To specify the site access range, select the [Only site of device] or [Access other sites in addition to site of device] radio button.

[Only site of device]: Accesses only the domain controllers in the same site as the machine.

[Access other sites in addition to site of device]: Accesses domain controllers in the same site as the machine, as well as domain controllers outside the site of the machine’s domain.

**IMPORTANT**
Even if [Only site of device] is selected, the machine may access sites outside of its domain when performing domain controller access during the startup process. However, access to the domain controllers in the same domain as the machine is prioritized.

11. Click [Update] ➞ restart the machine.

**IMPORTANT**
Changes made to the AA-PROX Configuration settings only take affect after the machine is restarted. For instructions on restarting the MEAP device, see the appropriate e-Manual that came with your machine.
3.4.3 Domain Authentication + Local Device Authentication Configuration without AMS

Follow the procedure below to configure the Domain Authentication + Local Device Authentication settings without the AMS option.

**IMPORTANT**
Make sure that the network settings for AD are set up properly for the domain to which you want users to authenticate, or users will not be able to log on.
See “Preparing the Device and Network Environment,” on p. 29.

1. Log on to the AA-PROX Configuration servlet.
   For instructions, see “Logging On to AA-PROX,” on p. 48.
2. Click [Configuration].
3. Select [Domain Authentication + Local Device Authentication] from the User Authentication System drop-down list.
4. For Domain Authentication, click [Edit domain authentication settings] if you want to edit the configured domain credentials for users who log on to the MEAP device by using a proximity card or perform self-registration using Domain Authentication.

![Image of AA-PROX interface](image)

**IMPORTANT**

- The Edit domain authentication settings table is not displayed until an authentication attempt for the first time is successfully performed against the domain to which the machine belongs. After the first successful domain authentication attempt, the table will contain a list of domains, user names and passwords.
- AA-PROX communicates with each AD domain controller that uses a configured user name and password associated with the target domain when a user presents a proximity card to AA-PROX for authentication.
- The user name and password fields are automatically populated.
- AA-PROX stores the specified user name and password within a configuration file as clear text.
4.1 If necessary, enter the proximity card ID’s LDAP attribute name that matches the one specified in the AD domain controller.

The default attribute name is ‘info’.

**IMPORTANT**
- Make sure that before you configure the LDAP attribute, the LDAP attribute field in the AD domain controller for the configured account in the domain authentication settings table, has the ‘Write’ permission.
- It is important to configure this field so that users can perform self-registration and authenticate with a proximity card ID against an AD domain controller.
4.2 If you want to edit the configured domain credentials for users who log on to the MEAP device by using a proximity card or perform self-registration using Domain Authentication, enter a new user name and password that is associated with the target domain, or edit the current user name and password.

Press [Test] next to the desired domain to validate the user name and password. If validation is successful, [Test] changes to [OK]. If validation is not successful, [Test] changes to [NG] (No Good). If you mouse-over [NG], an error message within a tool tip box may be displayed.

**IMPORTANT**

- The domain authentication settings table is not displayed until an authentication attempt for the first time is successfully performed against the domain to which the machine belongs. After the first successful domain authentication attempt, the table will contain a list of domains.
- AA-PROX communicates with each AD domain controller that uses a configured user name and password associated with the target domain when a user presents a proximity card to AA-PROX for authentication. However, even if a user successfully authenticates to the domain via self-registration, the user’s attempt at authentication with a proximity card may fail, unless the AA-PROX Administrator sets up an appropriate domain user settings account and password for the target domain in this step.
- AA-PROX stores the specified user name and password within a configuration file as clear text.

**NOTE**

If you do not want the domain authentication settings table displayed, click the [Hide] link. [Hide] changes to [Edit domain authentication settings].
5. Select the [Check local database first] check box if you want the local user database on the machine checked first for a user’s credentials the first time a user logs on to the device.

If the [Check local database first] check box is not selected, AA-PROX checks the AD server first for the user’s credentials when the user logs on to the machine the first time.

6. If you want to enable the [Keyboard Login] button on the AA-PROX Log In screen on the MEAP device, make sure the [Allow keyboard authentication] check box is selected.
7. Select the [LDAP uses SSL] check box if you want future communication with AD to be encrypted.

When the [LDAP uses SSL] check box is selected, the [LDAP Port] field is automatically set to port ‘636’. If the [LDAP uses SSL] check box is not selected, the [LDAP Port] field reverts back to its default port number ‘389’.

If you do not want to use SSL for LDAP communication, clear the [LDAP uses SSL] check box ➞ enter the LDAP port number directly into the [LDAP Port] field.

8. If you want a user to always enter a password after they swipe their proximity card, select the [Is a password required?] check box.
9. For Domain Authentication, if you want to specify a new user group for the domain administrator, enter the new group name in the [User Group Name] text box.

![Login Users Settings](image)

**NOTE**

- The default user group name is ‘Canon Peripheral Admins’. If the default user group name is changed, make sure that the domain administrator is a part of the user group specified above.
- If you change the User Group Name, the message, `<Are you sure you want to change the user group name to <NAME OF DOMAIN>?>` appears. Click [OK]. If you click [Cancel] instead of [OK], the message, `<Restore user group name.>` appears. Click [OK], and the User Group Name is restored.
10. Select the number of users to display in the User Name drop-down list on the Log In screen of the MEAP device from the Number of Login Users to Display drop-down list.

[0]: The drop-down arrow (▼) next to [User Name] on the Log In screen of the MEAP device is not displayed, and a user must enter their user name every time they log on to the machine.

[1]: Only the user name of the last user who logged on to the machine is displayed.

[Max (Maximum Number of a Device)]: The user names of the last seven users who logged on to the machine are displayed in the User Name drop-down list.
11. For Domain Authentication, if multiple sites are operating in the specified domain, select the [Set access mode in sites] check box to prioritize access to the domain controller in the site to which the machine belongs, or enable access to domain controllers outside the site to which the machine belongs.

**IMPORTANT**
- The domain controllers are accessed in the same order as the list of domain controllers retrieved from the DNS server.
- Site information is only retrieved when you access the device (log on) directly via its UI. Site information cannot be retrieved if you log on to the machine via a Web browser.
11.1 To specify how to retrieve site information, select the [Only at First Time] or [Every time when device starts up] radio button.

[Only at First Time]: Uses the list of domain controllers retrieved when a user logs on to the machine the first time.

[Every time when device starts up]: Retrieves the list of domain controllers every time the machine is powered ON.

⚠️ IMPORTANT
Only a maximum of 10 domains is retrieved.
11.2 To specify the site access range, select the [Only site of device] or [Access other sites in addition to site of device] radio button.

[Only site of device]: Accesses only the domain controllers in the same site as the machine.

[Access other sites in addition to site of device]: Accesses domain controllers in the same site as the machine, as well as domain controllers outside the site of the machine’s domain.

**IMPORTANT**
Even if [Only site of device] is selected, the machine may access sites outside of its domain when performing domain controller access during the startup process. However, access to the domain controllers in the same domain as the machine is prioritized.

12. Click [Update] → restart the machine.

**IMPORTANT**
Changes made to the AA-PROX Configuration settings only take affect after the machine is restarted. For instructions on restarting the MEAP device, see the appropriate e-Manual that came with your machine.
3.5 Configuring AA-PROX with AMS

This section describes how to configure AA-PROX for Local Device Authentication, Domain Authentication, and Domain Authentication + Local Device Authentication with the AMS Plug-In.

3.5.1 Local Device Authentication Configuration with AMS

Follow the procedure below to configure the Local Device Authentication settings with the AMS option.

1. Log on to the AA-PROX Configuration servlet.
   
   For instructions, see “Logging On to AA-PROX,” on p. 48.

2. Click [Configuration].

4. If you want to enable the [Keyboard Login] button on the AA-PROX Log In screen on the MEAP device, make sure the [Allow keyboard authentication] check box is selected.
5. Select the [LDAP uses SSL] check box if you want future communication with AD to be encrypted.

When the [LDAP uses SSL] check box is selected, the [LDAP Port] field is automatically set to port ‘636’. If the [LDAP uses SSL] check box is not selected, the [LDAP Port] field reverts back to its default port number ‘389’.

If you do not want to use SSL for LDAP communication, clear the [LDAP uses SSL] check box enter the LDAP port number directly into the [LDAP Port] field.

6. If you want a user to always enter a password after they swipe their proximity card, select the [Is a password required?] check box.
7. Select the base role to apply to users who are not associated with a role (users who do not have an assigned role in their user information) when they log on to a device from the Registered Users in Device and Device Domain drop-down list.

**IMPORTANT**

Application restrictions cannot be set for users who have their roles assigned via the Registered Users in Device and Device Domain drop-down list. If you want to assign restrictions to these users, you must create a custom role. See “Creating Custom Roles,” on p. 123.
8. Select the log in method for AA-PROX.

Select the [Display login screen when operation is started on the device] radio button if you want users to authenticate to the device using the Device Level Log-in method.

Select the [Display login screen when functions requiring authentication are selected] if you want users to have direct access to the machine, but have to authenticate themselves to access certain functions (Function Level Log-in).

**IMPORTANT**

- When you select the [Display login screen when functions requiring authentication are selected] radio button the [Allow unregistered users to log in as Guest User] check box is automatically selected, and the message <If [Display login screen when functions requiring authentication are selected] is selected, unregistered users will be allowed to log in> appears. Click [OK].
- The guest user account exists on the local database, and it can be accessed even if AA-PROX is configured for Domain Authentication.
- The guest user account cannot be deleted, but it can be edited, if necessary. See “Editing Custom Roles,” on p. 126.
9. Select the number of users to display in the User Name drop-down list on the Log In screen of the MEAP device from the Number of Login Users to Display drop-down list.

[0]: The drop-down arrow (▼) next to [User Name] on the Log In screen of the MEAP device is not displayed, and a user must enter their user name every time they log on to the machine.

[1]: Only the user name of the last user who logged on to the machine is displayed.

[Max (Maximum Number of a Device)]: The user names of the last seven users who logged on to the machine are displayed in the User Name drop-down list.
10. If the AMS Printer Driver Add-in is installed, select the [Save user authentication information] check box to save user authentication information when printing from a computer.

NOTE

If you set to save the user authentication information, you do not have to enter your user information into the AMS Printer Driver Add-in to print from a computer after the first time.
11. Specify the Job Restriction and Security Settings.

11.1 Select the [PDL print jobs not for function restrictions] check box to restrict the printing of jobs that do not support print restrictions.

**IMPORTANT**
- When the [PDL print jobs not for function restrictions] check box is selected, local users must enter their user credentials every time they print; unless, the [Save user authentication information] check box is selected in step 10.
- Make sure to select the [PDL print jobs not for function restrictions] check box and install the AMS Printer Driver Add-in to prevent printing from computers, or printing from computers in which an unknown user is logged on.
- When [PDL print jobs not for function restrictions] is selected, a security check is automatically performed if you print from a computer in which the AMS Printer Driver Add-in is installed. If a problem is found, printing is cancelled.
11.2 Select the remote jobs you want to restrict.

**IMPORTANT**
- Remote scanning is a function for using the device as a scanner and scanning documents to a computer. Optional equipment may be required. For more information, see the instruction manuals included with the device.
- Remote copying is a function for using the device as a remote copier. Optional equipment may be required. For more information, see the instruction manuals included with the device.
- Remote printing is a function for printing remotely to the machine. For more information, see the instruction manuals included with the device.

11.3 If you want to add a device signature when forwarding files from a device, select the [Add device signature to forwarding files] check box.

**IMPORTANT**
Device signatures can only be added if the optional Universal Send Digital User Signature Kit is installed in the MEAP device. For more information, see the appropriate e-Manual that came with your MEAP device.

12. Click [Update] ➔ restart the machine.

**IMPORTANT**
Changes made to the AA-PROX Configuration settings only take effect after the machine is restarted. For instructions on restarting the MEAP device, see the appropriate e-Manual that came with your machine.
3.5.2 Domain Authentication Configuration with AMS

Follow the procedure below to configure the Domain Authentication settings with the AMS option.

⚠️ IMPORTANT
Make sure that the network settings for AD are set up properly for the domain to which you want users to authenticate, or users will not be able to log on. See “Preparing the Device and Network Environment,” on p. 29.

1. Log on to the AA-PROX Configuration servlet.
   For instructions, see “Logging On to AA-PROX,” on p. 48.

2. Click [Configuration].
3. Select [Domain Authentication] from the User Authentication System drop-down list.

**IMPORTANT**
If the User Authentication System was originally set to ‘Local Device Authentication’, and you are switching to ‘Domain Authentication’, click [Update] ➞ restart the machine to enable the [Edit domain authentication settings] link.

![Image of User Authentication System settings with Domain Authentication selected]
4. Click [Edit domain authentication settings] if you want to edit the configured domain credentials for users who log on to the MEAP device by using a proximity card or perform self-registration using Domain Authentication.

**IMPORTANT**

- The Edit domain authentication settings table is not displayed until an authentication attempt for the first time is successfully performed against the domain to which the machine belongs. After the first successful domain authentication attempt, the table will contain a list of domains, user names and passwords.
- AA-PROX communicates with each AD domain controller that uses a configured user name and password associated with the target domain when a user presents a proximity card to AA-PROX for authentication.
- The user name and password fields are automatically populated.
- AA-PROX stores the specified user name and password within a configuration file as clear text.
4.1 If necessary, enter the proximity card ID’s LDAP attribute name that matches the one specified in the AD domain controller.

The default attribute name is ‘info’.

**IMPORTANT**

- Make sure that before you configure the LDAP attribute, the LDAP attribute field in the AD domain controller for the configured account in the domain authentication settings table, has the ‘Write’ permission.
- It is important to configure this field so that users can perform self-registration and authenticate with a proximity card ID against an AD domain controller.
4.2 If you want to edit the configured domain credentials for users who log on to the MEAP device by using a proximity card or perform self-registration using Domain Authentication, enter a new user name and password that is associated with the target domain, or edit the current user name and password.

Press [Test] next to the desired domain to validate the user name and password. If validation is successful, [Test] changes to [OK]. If validation is not successful, [Test] changes to [NG] (No Good). If you mouse-over [NG], an error message within a tool tip box may be displayed.

**IMPORTANT**
- The domain authentication settings table is not displayed until an authentication attempt for the first time is successfully performed against the domain to which the machine belongs. After the first successful domain authentication attempt, the table will contain a list of domains.
- AA-PROX communicates with each AD domain controller that uses a configured user name and password associated with the target domain when a user presents a proximity card to AA-PROX for authentication. However, even if a user successfully authenticates to the domain via self-registration, the user’s attempt at authentication with a proximity card may fail, unless the AA-PROX Administrator sets up an appropriate domain user settings account and password for the target domain in this step.
- AA-PROX stores the specified user name and password within a configuration file as clear text.

**NOTE**
If you do not want the domain authentication settings table displayed, click the [Hide] link. [Hide] changes to [Edit domain authentication settings].
5. If you want to enable the [Keyboard Login] button on the AA-PROX Log In screen on the MEAP device, make sure the [Allow keyboard authentication] check box is selected.

6. Select the [LDAP uses SSL] check box if you want future communication with AD to be encrypted.

When the [LDAP uses SSL] check box is selected, the [LDAP Port] field is automatically set to port ‘636’. If the [LDAP uses SSL] check box is not selected, the [LDAP Port] field reverts back to its default port number ‘389’.

If you do not want to use SSL for LDAP communication, clear the [LDAP uses SSL] check box ➞ enter the LDAP port number directly into the [LDAP Port] field.
7. If you want a user to always enter a password after they swipe their proximity card, select the [Is a password required?] check box.

8. Select the base role to apply to users who are not associated with a role (users who do not have an assigned role in their user information) when they log on to a device from the Registered Users in Device and Device Domain drop-down list.

**IMPORTANT**

Application restrictions cannot be set for users who have their roles assigned via the Registered Users in Device and Device Domain drop-down list. If you want to assign restrictions to these users, you must create a custom role. See “Creating Custom Roles,” on p. 123.
9. Select the default role of users who are registered in a trusted domain from the Registered Users in Trusted Domains drop-down list.
10. Select the log in method for AA-PROX.

Select the [Display login screen when operation is started on the device] radio button if you want users to authenticate to the device using the Device Level Log-in method.

Select the [Display login screen when functions requiring authentication are selected] if you want users to have direct access to the machine, but have to authenticate themselves to access certain functions (Function Level Log-in).

**IMPORTANT**

- When you select the [Display login screen when functions requiring authentication are selected] radio button the [Allow unregistered users to log in as Guest User] check box is automatically selected, and the message <If [Display login screen when functions requiring authentication are selected] is selected, unregistered users will be allowed to log in> appears. Click [OK].
- The guest user account exists on the local database, and it can be accessed even if AA-PROX is configured for Domain Authentication.
- The guest user account cannot be deleted, but it can be edited, if necessary. See “Editing Custom Roles,” on p. 126.
11. If you want to specify a new user group for the domain administrator, enter the new group name in the [User Group Name] text box.

NOTE
- The default user group name is ‘Canon Peripheral Admins’. If the default user group name is changed, make sure that the domain administrator is a part of the user group specified above.
- If you change the User Group Name, the message, <Are you sure you want to change the user group name to <NAME OF DOMAIN>?> appears. Click [OK]. If you click [Cancel] instead of [OK], the message, <Restore user group name.> appears. Click [OK], and the User Group Name is restored.

12. Select the number of users to display in the User Name drop-down list on the Log In screen of the MEAP device from the Number of Login Users to Display drop-down list.

- [0]: The drop-down arrow (▼) next to [User Name] on the Log In screen of the MEAP device is not displayed, and a user must enter their user name every time they log on to the machine.
- [1]: Only the user name of the last user who logged on to the machine is displayed.
- [Max (Maximum Number of a Device)]: The user names of the last seven users who logged on to the machine are displayed in the User Name drop-down list.
13. Make sure that the [Save user authentication information] check box is not selected.

The AMS Printer Driver Add-in [Save user authentication information] setting only supports local user authentication information.

14. Specify the Job Restriction and Security Settings.
14.1 Select the [PDL print jobs not for function restrictions] check box to restrict the printing of jobs that do not support print restrictions.

**IMPORTANT**
- When the [PDL print jobs not for function restrictions] check box is selected, users must enter their user credentials to print.
- Make sure to select the [PDL print jobs not for function restrictions] check box and install the AMS Printer Driver Add-in to prevent printing from computers, or printing from computers in which an unknown user is logged on.
- When [PDL print jobs not for function restrictions] is selected, a security check is automatically performed if you print from a computer in which the AMS Printer Driver Add-in is installed. If a problem is found, printing is cancelled.

14.2 Select the remote jobs you want to restrict.

**IMPORTANT**
- Remote scanning is a function for using the device as a scanner and scanning documents to a computer. Optional equipment may be required. For more information, see the instruction manuals included with the device.
- Remote copying is a function for using the device as a remote copier. Optional equipment may be required. For more information, see the instruction manuals included with the device.
- Remote printing is a function for printing remotely to the machine. For more information, see the instruction manuals included with the device.
14.3 If you want to add a device signature when forwarding files from a device, select the [Add device signature to forwarding files] check box.

**IMPORTANT**

Device signatures can only be added if the optional Universal Send Digital User Signature Kit is installed in the MEAP device. For more information, see the appropriate e-Manual that came with your MEAP device.
15. If multiple sites are operating in the specified domain, select the [Set access mode in sites] check box to prioritize access to the domain controller in the site to which the machine belongs, or enable access to domain controllers outside the site to which the machine belongs.

**IMPORTANT**

- The domain controllers are accessed in the same order as the list of domain controllers retrieved from the DNS server.
- Site information is only retrieved when you access the device (log on) directly via its UI. Site information cannot be retrieved if you log on to the machine via a Web browser.
15.1 To specify how to retrieve site information, select the [Only at First Time] or [Every time when device starts up] radio button.

**[Only at First Time]:** Uses the list of domain controllers retrieved when a user logs on to the machine the first time.

**[Every time when device starts up]:** Retrieves the list of domain controllers every time the machine is powered ON.

**IMPORTANT**
Only a maximum of 10 domains is retrieved.
15.2 To specify the site access range, select the [Only site of device] or [Access other sites in addition to site of device] radio button.

[Only site of device]: Accesses only the domain controllers in the same site as the machine.

[Access other sites in addition to site of device]: Accesses domain controllers in the same site as the machine, as well as domain controllers outside the site of the machine’s domain.

**IMPORTANT**
Even if [Only site of device] is selected, the machine may access sites outside of its domain when performing domain controller access during the startup process. However, access to the domain controllers in the same domain as the machine is prioritized.

16. Click [Update] ➔ restart the machine.

**IMPORTANT**
Changes made to the AA-PROX Configuration settings only take affect after the machine is restarted. For instructions on restarting the MEAP device, see the appropriate e-Manual that came with your machine.
3.5.3 Domain Authentication + Local Device Authentication Configuration with AMS

Follow the procedure below to configure the Domain Authentication + Local Device Authentication settings with the AMS option.

**IMPORTANT**

Make sure that the network settings for AD are set up properly for the domain to which you want users to authenticate, or users will not be able to log on. See “Preparing the Device and Network Environment,” on p. 29.

1. Log on to the AA-PROX Configuration servlet.
   For instructions, see “Logging On to AA-PROX,” on p. 48.

2. Click [Configuration].

3. Select [Domain Authentication + Local Device Authentication] from the User Authentication System drop-down list.
4. For Domain Authentication, click [Edit domain authentication settings] if you want to edit the configured domain credentials for users who log on to the MEAP device by using a proximity card or perform self-registration using Domain Authentication.

![Image of AA-PROX configuration settings]

**IMPORTANT**

- The Edit domain authentication settings table is not displayed until an authentication attempt for the first time is successfully performed against the domain to which the machine belongs. After the first successful domain authentication attempt, the table will contain a list of domains, user names and passwords.
- AA-PROX communicates with each AD domain controller that uses a configured user name and password associated with the target domain when a user presents a proximity card to AA-PROX for authentication.
- The user name and password fields are automatically populated.
- AA-PROX stores the specified user name and password within a configuration file as clear text.
4.1 If necessary, enter the proximity card ID’s LDAP attribute name that matches the one specified in the AD domain controller.

The default attribute name is ‘info’.

**IMPORTANT**

- Make sure that before you configure the LDAP attribute, the LDAP attribute field in the AD domain controller for the configured account in the domain authentication settings table, has the ‘Write’ permission.
- It is important to configure this field so that users can perform self-registration and authenticate with a proximity card ID against an AD domain controller.
4.2 If you want to edit the configured domain credentials for users who log on to the MEAP device by using a proximity card or perform self-registration using Domain Authentication, enter a new user name and password that is associated with the target domain, or edit the current user name and password.

Press [Test] next to the desired domain to validate the user name and password. If validation is successful, [Test] changes to [OK]. If validation is not successful, [Test] changes to [NG] (No Good). If you mouse-over [NG], an error message within a tool tip box may be displayed.

**IMPORTANT**
- The domain authentication settings table is not displayed until an authentication attempt for the first time is successfully performed against the domain to which the machine belongs. After the first successful domain authentication attempt, the table will contain a list of domains.
- AA-PROX communicates with each AD domain controller that uses a configured user name and password associated with the target domain when a user presents a proximity card to AA-PROX for authentication. However, even if a user successfully authenticates to the domain via self-registration, the user’s attempt at authentication with a proximity card may fail, unless the AA-PROX Administrator sets up an appropriate domain user settings account and password for the target domain in this step.
- AA-PROX stores the specified user name and password within a configuration file as clear text.

**NOTE**
If you do not want the domain authentication settings table displayed, click the [Hide] link. [Hide] changes to [Edit domain authentication settings].
5. Select the [Check local database first] check box if you want the local user database on the machine checked first for a user’s credentials the first time a user logs on to the device.

If the [Check local database first] check box is not selected, AA-PROX checks the AD server first for the user’s credentials when the user logs on to the machine the first time.

6. If you want to enable the [Keyboard Login] button on the AA-PROX Log In screen on the MEAP device, make sure the [Allow keyboard authentication] check box is selected.
7. Select the [LDAP uses SSL] check box if you want future communication with AD to be encrypted.

When the [LDAP uses SSL] check box is selected, the [LDAP Port] field is automatically set to port ‘636’. If the [LDAP uses SSL] check box is not selected, the [LDAP Port] field reverts back to its default port number ‘389’.

If you do not want to use SSL for LDAP communication, clear the [LDAP uses SSL] check box ➞ enter the LDAP port number directly into the [LDAP Port] field.

8. If you want a user to always enter a password after they swipe their proximity card, select the [Is a password required?] check box.
9. Select the base role to apply to users who are not associated with a role (users who do not have an assigned role in their user information) when they log on to a device from the Registered Users in Device and Device Domain drop-down list.

**IMPORTANT**
Application restrictions cannot be set for users who have their roles assigned via the Registered Users in Device and Device Domain drop-down list. If you want to assign restrictions to these users, you must create a custom role. See “Creating Custom Roles,” on p. 123.

10. Select the default role of users who are registered in a trusted domain from the Registered Users in Trusted Domains drop-down list.
11. Select the log in method for AA-PROX.

Select the [Display login screen when operation is started on the device] radio button if you want users to authenticate to the device using the Device Level Log-in method.

Select the [Display login screen when functions requiring authentication are selected] if you want users to have direct access to the machine, but have to authenticate themselves to access certain functions (Function Level Log-in).

**IMPORTANT**
- When you select the [Display login screen when functions requiring authentication are selected] radio button the [Allow unregistered users to log in as Guest User] check box is automatically selected, and the message <If [Display login screen when functions requiring authentication are selected] is selected, unregistered users will be allowed to log in> appears. Click [OK].
- The guest user account exists on the local database, and it can be accessed even if AA-PROX is configured for Domain Authentication.
- The guest user account cannot be deleted, but it can be edited, if necessary. See "Editing Custom Roles,” on p. 126.
12. For Domain Authentication, if you want to specify a new user group for the domain administrator, enter the new group name in the [User Group Name] text box.

<table>
<thead>
<tr>
<th>Set Default Role</th>
<th>General User</th>
<th>Effective attribute of domain authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registered Users in Device and Device Group</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registered Users in Trusted Domain</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NOTE**

- The default user group name is ‘Canon Peripheral Admins’. If the default user group name is changed, make sure that the domain administrator is a part of the user group specified above.
- If you change the User Group Name, the message, <Are you sure you want to change the user group name to <NAME OF DOMAIN>?> appears. Click [OK]. If you click [Cancel] instead of [OK], the message, <Restore user group name.> appears. Click [OK], and the User Group Name is restored.

NOTE
13. Select the number of users to display in the User Name drop-down list on the Log In screen of the MEAP device from the Number of Login Users to Display drop-down list.

- **[0]**: The drop-down arrow (▼) next to [User Name] on the Log In screen of the MEAP device is not displayed, and a user must enter their user name every time they log on to the machine.

- **[1]**: Only the user name of the last user who logged on to the machine is displayed.

- **[Max (Maximum Number of a Device)]**: The user names of the last seven users who logged on to the machine are displayed in the User Name drop-down list.
14. If most users are going to log on to the machine using Domain Authentication, make sure that the [Save user authentication information] check box is not selected. The AMS Printer Driver Add-in [Save user authentication information] setting only supports local user authentication information.
15. Specify the Job Restriction and Security Settings.

<table>
<thead>
<tr>
<th>Login</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>[PDL print jobs not for function restrictions] check box</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

15.1 Select the [PDL print jobs not for function restrictions] check box to restrict the printing of jobs that do not support print restrictions.

**IMPORTANT**
- When the [PDL print jobs not for function restrictions] check box is selected, users must enter their user credentials to print.
- Make sure to select the [PDL print jobs not for function restrictions] check box and install the AMS Printer Driver Add-in to prevent printing from computers, or printing from computers in which an unknown user is logged on.
- When [PDL print jobs not for function restrictions] is selected, a security check is automatically performed if you print from a computer in which the AMS Printer Driver Add-in is installed. If a problem is found, printing is cancelled.

15.2 Select the remote jobs you want to restrict.

**IMPORTANT**
- Remote scanning is a function for using the device as a scanner and scanning documents to a computer. Optional equipment may be required. For more information, see the instruction manuals included with the device.
- Remote copying is a function for using the device as a remote copier. Optional equipment may be required. For more information, see the instruction manuals included with the device.
- Remote printing is a function for printing remotely to the machine. For more information, see the instruction manuals included with the device.
15.3 If you want to add a device signature when forwarding files from a device, select the [Add device signature to forwarding files] check box.

**IMPORTANT**

Device signatures can only be added if the optional Universal Send Digital User Signature Kit is installed in the MEAP device. For more information, see the appropriate e-Manual that came with your MEAP device.
16. For Domain Authentication, if multiple sites are operating in the specified domain, select the [Set access mode in sites] check box to prioritize access to the domain controller in the site to which the machine belongs, or enable access to domain controllers outside the site to which the machine belongs.

**IMPORTANT**

- The domain controllers are accessed in the same order as the list of domain controllers retrieved from the DNS server.
- Site information is only retrieved when you access the device (log on) directly via its U1. Site information cannot be retrieved if you log on to the machine via a Web browser.
16.1 To specify how to retrieve site information, select the [Only at First Time] or [Every time when device starts up] radio button.

[Only at First Time]: Uses the list of domain controllers retrieved when a user logs on to the machine the first time.

[Every time when device starts up]: Retrieves the list of domain controllers every time the machine is powered ON.

**IMPORTANT**
Only a maximum of 10 domains is retrieved.
16.2 To specify the site access range, select the [Only site of device] or [Access other sites in addition to site of device] radio button.

[Only site of device]: Accesses only the domain controllers in the same site as the machine.

[Access other sites in addition to site of device]: Accesses domain controllers in the same site as the machine, as well as domain controllers outside the site of the machine’s domain.

**IMPORTANT**  
Even if [Only site of device] is selected, the machine may access sites outside of its domain when performing domain controller access during the startup process. However, access to the domain controllers in the same domain as the machine is prioritized.

17. Click [Update] ➞ restart the machine.

**IMPORTANT**  
Changes made to the AA-PROX Configuration settings only take affect after the machine is restarted. For instructions on restarting the MEAP device, see the appropriate e-Manual that came with your machine.
3.6 Configuring the Other Settings

This section describes how to specify the custom logo settings and how to enable the Debug logging mode under the <Other Settings> heading on the Configuration servlet’s Configuration screen.

1. Log on to the AA-PROX Configuration servlet.
   
   For instructions, see “Logging On to AA-PROX,” on p. 48.

2. Click [Configuration].
3. If you want to upload a custom logo to the MEAP device’s Log In screen, select the [Enable custom logo] check box → click [Browse] → follow the directions on the screen to locate the logo’s image file.

![Screenshot of the Enable custom logo settings](image)

**IMPORTANT**
- [Browse] is grayed out until the [Enable custom logo] check box is selected.
- The logo’s image dimensions must be 800 pixels wide by 340 pixels high for devices with 800 x 600 screens, and 640 pixels wide by 272 pixels high for devices with 640 x 480 screens. The image format must be PNG, JPEG, or GIF.
- Any logo that is not within the specifications above is discarded without notice.

4. Click [Update].

![Screenshot of the Custom logo settings](image)

If the image file contains the correct specifications, the logo is uploaded and displayed on the MEAP device’s Log In screen.
5. If you want debug information logged in a log file, select the [Enable debug mode] check box.

![Image of Advanced Authentication-Proximity Card V2.2 Installation and Configuration Guide]

**IMPORTANT**

Enabling the Debug mode, may slow down AA-PROX’s performance.

6. To view the log file, click [Download Log].

The log file is downloaded to your PC with the name ‘log.zip’. The zip file contains up to two log files which are named with a random number plus the extension “.log”.

The maximum size of each log file is 5 MB. If the log files are about to exceed this limit, the older log file is deleted, and a new log file is created.
3.7 Logging Off

Follow the procedure below to log off the AA-PROX Configuration servlet.


The Login screen is displayed.
Chapter 4  Role Management

This chapter describes how to configure AMS role permissions, import/export roles, create and delete custom roles.

There are three basic methods to manage users/roles:

• Local administration using the iWEMC UM and AMS Plug-ins
• Local administration using the Configuration servlet
• Active Directory administration using the AD Administrator Console of supported Windows servers in conjunction with the iWEMC UM and AMS Plug-ins

Local administration is used when AA-PROX is configured to be used in the Local Device Authentication mode. This mode enables user account information to be managed and retained distinctly on each MEAP device.

Active Directory administration is used when AA-PROX is configured to be used in the Domain Authentication mode or Domain Authentication + Local Device Authentication mode. These modes enable user account information to be centrally managed and retained in AD domain controllers.

IMPORTANT

This chapter only describes how to manage roles and users from AA-PROX with the AMS. Although, you can manage roles and users from iWEMC, the functions and features of iWEMC is beyond the scope of this document. For more information on managing users and roles using iWEMC, see the imageWARE Enterprise Management Console User Management Plug-In User’s Guide and the AMS Administrator’s Guide.
4.1 Managing Roles

There are two types of roles for setting device restriction information: Base roles and Custom roles.

Base roles are roles that are provided by the AMS, and which have usage restriction information set by default.

Custom roles are user-defined roles that are created by adding or editing usage restriction information from a base role.

There are five default base roles and two default custom roles. For more information on these default roles and their device function restrictions and device management privileges, see the Access Management System V3.0 Individual Management Configuration Administrator Guide.

Base Roles: Administrator, Power User, General User, Limited User, Guest User
Custom Roles: DeviceAdmin, NetworkAdmin

IMPORTANT
- You can register a maximum of 100 roles (base and custom).
- To access the Role Management screen, AMS must be installed and activated on the MEAP device.
- For the default base roles and custom roles, you cannot edit the device function restrictions and device management privileges, or set application restrictions.
- For the Guest User role, you can set device function and application restrictions; however, you cannot edit the device management privileges.
4.2 Creating Custom Roles

This section describes how to create custom roles with AA-PROX.

**IMPORTANT**

- The restrictions for settings that are not supported by a device cannot be selected from the Add Custom Role screen. For example, if you are configuring role settings for a user on a black-and-white device, the Color Print drop-down list is not displayed in the <Function Category Restriction Details> section of the Add Custom Role screen.
- It is recommended that you export created custom role information to a server or computer for backup purposes. This also enables these roles to be imported and registered in multiple devices. For instructions on exporting roles, see “Exporting Roles,” on p. 134. For instructions on importing roles, see “Importing Roles,” on p. 131.

---

1. Log on to the AA-PROX Configuration servlet.

   For instructions, see “Logging On to AA-PROX,” on p. 48.

2. Click [Role Management].
3. Under <Custom Roles>, click [Add Role].
4. Specify a name for the custom role, enter any comments, if necessary, and select the base role on which the custom role will be based.

You can specify up to 32 characters for the Role Name. A space and the following symbols cannot be entered as part of the Role Name: * ? | <> ] ; , = + @ " &

5. Specify the device, function, and application restrictions for the custom role ➞ click [Add].

For more information on the Add Custom Role settings and their descriptions, see the *Access Management System V3.0 Individual Management Configuration Administrator Guide*. 
4.3 Editing Custom Roles

This section describes how to edit custom roles.

**IMPORTANT**
- Only the [Comments] field can be edited for base roles and custom (administrator) roles. However, restriction information can also be edited for the Guest User role.
- To change the name of a custom role, you must delete the role, and then add it as a new role. (You can also export the role information, and then edit it with a text editor. However, take care not to edit the control characters.)
- To change the Base Role setting to change the role’s device management privileges, you must delete the role, and then add it as a new role.
- The edited role information is enabled from the next time the user logs on to the machine.
- If a guest role is registered using the AMS Plug-in and a task for distributing restriction information is executed in the AMS Plug-in, the base Guest User role in AA-PROX is overwritten. In this case, it is best to export the user information in AA-PROX to back it up.
- It is recommended that you export created custom role information to a server or computer for backup purposes. This also enables these roles to be imported and registered in multiple devices. For instructions on exporting roles, see “Exporting Roles,” on p. 134. For instructions on importing roles, see “Importing Roles,” on p. 131.

1. Log on to the AA-PROX Configuration servlet.
   For instructions, see “Logging On to AA-PROX,” on p. 48.

2. Click [Role Management].

![Screen capture of the AA-PROX Configuration servlet with Role Management selected.](image-url)
3. Click [Edit] next to the role you want to edit.
4. Edit the required settings ➞ click [Update].

**NOTE**

The Device Management Restriction settings can only be edited if the Administrator role is set as the base role.
4.4 Deleting Custom Roles

This section describes how to delete a custom role.

**IMPORTANT**
Base roles and custom (administrator) roles cannot be deleted.

1. Log on to the AA-PROX Configuration servlet.
   
   For instructions, see “Logging On to AA-PROX,” on p. 48.

2. Click [Role Management].
3. Select the custom role you want to delete ➔ click [Delete].

The message <Are you sure you want to delete the selected roles?> is displayed. Click [OK].

The selected roles are deleted.

**NOTE**
- If you want to select all of the custom roles, click [Select All].
- If you want to clear all the check marks from the selected custom role check boxes, click [Clear All].
4.5 Importing Roles

This section describes how to import roles that are registered in another device from a file saved on a computer.

**IMPORTANT**
- If a role in AA-PROX is named the same as a role that is imported, the role in AA-PROX is overwritten with the imported role's information. However, only comments are overwritten for base roles other than the Guest User role and custom (administrator) roles.
- If <Device Settings> and <Network Settings> under <Device Management Restriction> are set to ‘Not Allowed’ and <All Settings> is set to ‘No Restrictions’, the role information is deemed invalid, and is not imported.
- Roles that have already been registered in the device are not deleted when roles are imported. The imported roles are added to the device.

1. Log on to the AA-PROX Configuration servlet.

   For instructions, see “Logging On to AA-PROX,” on p. 48.

2. Click [Role Management].
3. Click [Import].

4. Click [Browse] ➞ select the xml file to import ➞ click [Open].
5. Click [Start Import].

The message <Importing…> is displayed while AA-PROX is importing the selected role information.

The message <Import was completed.> is displayed if the import process was successful. Click [Back] to return to the Role Management main screen.

The imported roles are displayed on the Role Management main screen.

If the import process fails, the role information is restored to what it was before the import.
4.6  Exporting Roles

This section describes how to export role information that is registered in the device as a file. This is useful for backup purposes, or for using the registered role information in another device.

NOTE

The exported role information is saved as an .xml file, and the default file name is ‘roleData.xml’.

1. Log on to the AA-PROX Configuration servlet.

   For instructions, see “Logging On to AA-PROX,” on p. 48.

2. Click [Role Management].
3. Click [Export].

4. Click [Start Export].

5. Follow the instructions on the screen to specify the location to save the file.

   The file is downloaded, and the role information can be imported into the machine.
This page is intentionally left blank.
Chapter 5  User Management

This chapter describes how to manage user information that is used for local device authentication, and how to import and export user information in batches.

IMPORTANT
- Only users that are associated with the Administrator role (except for users that are associated with a custom role based on the Administrator role, such as ‘DeviceAdmin’ or ‘NetworkAdmin’), can manage users.
- When the AMS is active, designated guest users can log on to the device without using any credentials or swiping a proximity card. The Guest User account exists on the local database, but can be accessed even if AA-PROX is configured for Domain Authentication.
- To register a user for Domain Authentication, you must add the user to the Administrator Group on the Active Directory server using the Active Directory Management Tool. For more information, see the MEAP e-Manual that came with your machine.
- If the domain administrator disables a domain user’s account, make sure that you manually remove the Card ID from the LDAP field of the user’s AD account properties in the Edit domain authentication settings section of AA-PROX’s Configuration screen. Otherwise, the user can still log on to the machine. For more information, see “Configuring AA-PROX without AMS,” on p. 49, or “Configuring AA-PROX with AMS,” on p. 75.

5.1  Registering Users

This section describes how to register user information for Local Device Authentication using AA-PROX.

IMPORTANT
- You can register a maximum of 5,000 users.
- A user that is associated with the Administrator role has an asterisk (*) displayed to the left of the user name on the User Management screen.
- By default, the Guest User account has a user name and display name of “Guest,” no password, no Department ID credentials, no e-mail address, and the role of “Limited User.”
- It is recommended that you export the user information after registering it for backup purposes. This enables the user information to be imported and registered in multiple devices. For instructions on exporting user information, see “Exporting User Information,” on p. 150. For instructions on importing user information, see “Importing User Information,” on p. 145.

1. Log on to the AA-PROX Configuration servlet.

   For instructions, see “Logging On to AA-PROX,” on p. 48.
2. Click [User Management].

3. Click [Add User].

4. Enter the User Name, Password, Department ID, PIN, Displayed As, and E-Mail Address information.
# User Management Setting Table

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Setting Conditions</th>
</tr>
</thead>
</table>
| **User Name** | Set the user name to use when performing user authentication in the Local Device Authentication mode.                                             | • User-defined string of 32 characters. However, spaces and the following characters cannot be used: \/: * ? | < > [ ] ; , = + @ “.  
• Case-sensitive.  
• You cannot register a user name that already exists. |
| **Password** | Set the password to use when performing user authentication in the Local Device Authentication mode.                                             | • User-defined string of 0 to 32 characters.  
• Case-sensitive. |
| **Confirm** | Enter the same password entered in [Password].                                                                                                 | • User-defined string of 0 to 32 characters.  
• Case-sensitive. |
| **Department ID** | To use Department ID Management with the AMS and when Local Device Authentication is set as the user authentication system, enter the Department ID. | • Seven-digit number (if the entered number is not seven digits, zeros are appended to the start of the number).  
• If not using Department ID Management, leave the Department ID field blank. |
| **PIN** | To use Department ID Management with the AMS and when Local Device Authentication is set as the user authentication system, enter the PIN that corresponds to the Department ID entered in [Department ID]. | • Seven-digit number (if the entered number is not seven digits, zeros are appended to the start of the number).  
• If not using Department ID Management, leave the PIN field blank. |
| **Confirm** | Enter the same PIN entered in [PIN] under [Department ID].                                                                                     | • Seven-digit number (if the entered number is not seven digits, zeros are appended to the start of the number).  
• If not using Department ID Management, leave the Confirm (PIN) field blank. |
| **Displayed As** | Set how the user name is displayed.                                                                                                            | User-defined string of 0 to 32 characters. |
| **E-Mail Address** | Set the user’s e-mail address.                                                                                                                 | • Enter up to 256 alphanumeric characters.  
The following symbols can also be used: @ . "_.  
• An e-mail address format check is not performed. |
**IMPORTANT**

- If the AMS is operating in an individual management configuration and the Local Device Authentication mode is being used, it can be used with the Department ID Management function. However, the [Department ID] and [PIN] user information registered in AA-PROX must match the Department ID and PIN registered for the user on the machine. If the Department ID and PIN have been changed due to the delivery of device information, make sure to change the user information in AA-PROX accordingly.
- If [E-Mail Address] is left blank, the specified user cannot use the e-mail sending function on the device.
- If an e-mail address is specified, the Displayed As name and e-mail address of the logged in user are displayed in the [From] field in an e-mail message that is sent from the machine.
- If an e-mail address is specified, the logged on user’s e-mail address is displayed in the Sender field to the recipient of an I-fax.

5. Select the role with which to associate the user from the Select Role to Set drop-down list ➔ click [Add].

![Image of user interface](image1.png)

The new user information is registered.

**NOTE**

If you do not select a role from the Select Role to Set drop-down list, the role selected from the Registered Users in Device and Device Domain drop-down list on the Configuration screen is applied. See “Local Device Authentication Configuration with AMS,” on p. 75.
5.2 Editing User Information

This section describes how to edit registered user information.

**IMPORTANT**
- User names cannot be edited. To change a user name, you must delete the user information, and then register it again as a new user. (You can also export the user information, and then edit it with a text editor. However, take care not to edit the control characters.)
- The changed user information is only enabled from the next time the user logs on to the machine.
- It is recommended that you export the user information after editing it for backup purposes. For more information, see “Exporting User Information,” on p. 150.

1. Log on to the AA-PROX Configuration servlet.
   
   For instructions, see “Logging On to AA-PROX,” on p. 48.

2. Click [User Management].

   ![User Management]

3. Click [Edit] next to the user you want to edit.

   ![Edit User]
4. To change the user’s password, select the [Change password] check box → enter the new password in [New Password] → enter the same password in [Confirm].

5. If necessary, enter a different or new Department ID in the Department ID text box.

6. To change the Department ID’s PIN, select the [Change PIN] check box → enter the PIN in [PIN] → enter the same PIN in [Confirm].

7. If necessary, edit the Displayed As, E-Mail Address, and Select Role to Set information → click [Update].

The user information is changed.
5.3 Deleting User Information

This section describes how to delete registered user information.

**IMPORTANT**
You can only delete the user information of users who are not currently logged on to a machine.

1. Log on to the AA-PROX Configuration servlet.
   For instructions, see “Logging On to AA-PROX,” on p. 48.

2. Click [User Management].
3. Select the check box next to the user information you want to delete → click [Delete].

![User Management Screen]

The message <Are you sure you want to delete the selected user?> is displayed. Click [OK].

The selected users are deleted.

📝 NOTE
- If you want to select all users, click [Select All].
- If you want to clear all the check marks from the selected user check boxes, click [Clear All].
5.4 Importing User Information

This section describes how to import user information that is registered in another device from a file saved on a computer.

**IMPORTANT**
- If a user in AA-PROX is named the same as a user that is imported, the user information in AA-PROX is overwritten with the imported user’s information.
- If an imported user does not have a role associated with them, the role selected from the Registered Users in Device and Device Domain drop-down list on the Settings screen is applied. See “Local Device Authentication Configuration with AMS,” on p. 75.
- It is recommended that you import user information in the SDL (Specification and Design Language) format.
- In AA-PROX, if the AMS Kit is activated, only user information in the SDL format with the “.ldif” extension can be imported. However, if you use the UM Plug-in, you can also import user information created in the CSV format. For more information, see the imageWARE Enterprise Management Console User Management Plug-In Online Help.

**NOTE**
For more information on the file formats that can be used for importing user information files, see the MEAP e-Manual that came with your machine.

1. Log on to the AA-PROX Configuration servlet.
   
   For instructions, see “Logging On to AA-PROX,” on p. 48.

2. Click [User Management].
3. Click [Import].

![Image of the AA-PROX interface showing a user management page with options for adding or deleting users.]

4. Click [Browse] ➞ select the file to import.

![Image of the AA-PROX interface showing the option to import user information with specified file format and file path.]

5. Select the file format from the File Format drop-down list.

5.1 If the AMS Kit is activated and installed, select [SDL Format] ➞ proceed to step 6.

![Image of the AA-PROX interface showing the import user information page with file path and format options.]
5.2 If the AMS Kit is not activated and installed, select [SDL Format], [NetSpot Accountant 3.x Format], or [NetSpot Accountant 4.x Format].

[SDL Format]: Select this file format if you are importing user data created in the file format used for SDL and Local Device Authentication. (File extension: .ldif)

[NetSpot Accountant 3.x Format]: Select this file format if you are importing user data created in the NetSpot Accountant 3.x format. (File extension: .csv)

[NetSpot Accountant 4.x Format]: Select this file format if you are importing user data created in the NetSpot Accountant 4.x or imageWARE Accounting Manager format. (File extension: .csv)
5.2.1 If you selected [NetSpot Accountant 3.x Format] or [NetSpot Accountant 4.x Format] as the file format, specify the character code for importing the user information from the Encoding drop-down list.

- [Windows Latin-1 (CP1252)]: Select this option to import a file that is written in the Windows Latin (a European character code) format.

- [Windows Japanese (CP932)]: Select this option to import a file that is written in the Windows Japanese (a Japanese character code) format.

5.2.2 If you selected [NetSpot Accountant 3.x Format] or [NetSpot Accountant 4.x Format] as the file format, select the type of user name used when logging on to the machine from the User Name Type drop-down list.

- [User ID]: Uses the User ID as the user name when importing the user information.

- [Windows User Name]: Uses the Windows user name when importing the user information.
6. Click [Start Import].

The message <Importing…> is displayed while AA-PROX is importing the selected user information.

The message <Import was completed.> is displayed if the import process was successful. Click [Back] to return to the User Management main screen.

The imported roles are displayed on the User Management main screen.

![User Management Screen]

**IMPORTANT**
If user data with the same name is already registered, the imported user data overwrites the existing data.
5.5 Exporting User Information

This section describes how to export user information that is registered in the device as a file. This is useful for backup purposes, or for using the registered user information in another device.

⚠️ IMPORTANT
- It is recommended that you export user information in the SDL format.
- Only the information for users that have a Department ID assigned to them is exported in the NetSpot Accountant format. If no users have Department IDs assigned, a 0 byte file is exported.

💡 NOTE
- The exported user information is saved as an .ldif file, and the default file name is ‘sdlData.ldif’.
- For more information on the file formats that can be used for exporting user information files, see the MEAP e-Manual that came with your machine.

1. Log on to the AA-PROX Configuration servlet.
   
   For instructions, see “Logging On to AA-PROX,” on p. 48.

2. Click [User Management].
3. Click [Export].

4. Select the file format from the File Format drop-down list.

4.1 If the AMS Kit is activated and installed, select [SDL Format].
4.2 If the AMS Kit is not activated and installed, select [SDL Format], [NetSpot Accountant 3.x Format], or [NetSpot Accountant 4.x Format].

[SDL Format]: Select this file format to export user data created in the file format used for SDL and Local Device Authentication. (File extension: .ldif)

[NetSpot Accountant 3.x Format]: Select this file format to export user data created in the NetSpot Accountant 3.x format. (File extension: .csv)

[NetSpot Accountant 4.x Format]: Select this file format to export user data created in the NetSpot Accountant 4.x or imageWARE Accounting Manager format. (File extension: .csv)

4.2.1 If you selected [NetSpot Accountant 3.x Format] or [NetSpot Accountant 4.x Format] as the file format, specify the character code for exporting the user information from the Encoding drop-down list.

[Windows Latin-1 (CP1252)]: Select this option to export the file in the Windows Latin (a European character code) format.

[Windows Japanese (CP932)]: Select this option to export the file in the Windows Japanese (a Japanese character code) format.
5. Click [Start Export] ➔ follow the instructions on the screen to specify the location to save the file.

The exported user information file is saved to the specified location.
Chapter 6 Appendix

This chapter explains the various issues that may arise when configuring AA-PROX, and the various messages that may appear on the Configuration servlet screen, along with their possible causes and remedies.

6.1 List of Error Messages

This section explains the various messages that may appear on the AA-PROX Configuration servlet screen, along with their possible causes and remedies.

For a list of the error messages that may appear, along with their causes and remedies when installing AA-PROX using the MEAP SMS, see the MEAP e-Manual that came with your machine.

Any words that appear italicized are variables, and are replaced with their corresponding values on the actual application screen.

6.1.1 MEAP Device Login Screen Error Messages

This section explains the Log In screen error messages that may appear on the MEAP device’s UI, along with possible causes and remedies.

<table>
<thead>
<tr>
<th>Message</th>
<th>Cause</th>
<th>Remedy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login failed. Check the user name and password.</td>
<td>• You entered an incorrect user name and password.</td>
<td>• Make sure that your user name and password are correct, and try to log on again.</td>
</tr>
<tr>
<td></td>
<td>• The user name and password that are set for domain authentication are invalid.</td>
<td>• Check the domain user’s credentials, and make sure they are valid.</td>
</tr>
<tr>
<td>Login failed due to an authentication error in Dept. ID/Management. Contact system manager.</td>
<td>The Department ID configured for the user who is trying to log on is incorrect.</td>
<td>Make sure that the user account is configured with the proper Department ID, and that the user is logging on to the machine using their local authentication credentials. See Chapter 5, “User Management,” on p. 137.</td>
</tr>
<tr>
<td>Login failed. You are not authorized to use these functions.</td>
<td>The user does not have permission to use the selected function.</td>
<td>If the user should have permission to use the selected function, grant the user account access privileges. See Chapter 4, “Role Management,” on p. 121.</td>
</tr>
<tr>
<td>Message</td>
<td>Cause</td>
<td>Remedy</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
<td>--------</td>
</tr>
<tr>
<td><strong>Login failed. Timer settings for this device and the auth. server may be skewed. Contact system manager, or check the user name and password.</strong></td>
<td>The time on the device is not synchronized with the time on the authentication server.</td>
<td>Make sure that the time on the device is synchronized within the 5 minute clock skew tolerance of the authentication server. See “Synchronizing the Device and AD Server Time,” on p. 37.</td>
</tr>
<tr>
<td><strong>Domain Authentication configuration is not yet complete. Contact system manager.</strong></td>
<td>You cannot log on to the selected domain because Domain Authentication configuration information is missing.</td>
<td>Make sure that all Domain Authentication information is configured correctly in the AA-PROX Configuration servlet, restart the machine, and try to log on to the domain again. See “Domain Authentication Configuration without AMS,” on p. 53, or “Domain Authentication Configuration with AMS,” on p. 84.</td>
</tr>
<tr>
<td><strong>Configuration for the domain you selected is not yet complete. Contact system manager.</strong></td>
<td>You cannot log on to the selected domain because Domain Authentication configuration has not been completed.</td>
<td>Make sure that all Domain Authentication information is configured correctly in the AA-PROX Configuration servlet, restart the machine, and try to log on to the domain again. See “Domain Authentication Configuration without AMS,” on p. 53, or “Domain Authentication Configuration with AMS,” on p. 84.</td>
</tr>
<tr>
<td><strong>A password is not set on the authentication server side. Contact system manager.</strong></td>
<td>• The DES (Data Encryption Standard) key required for Domain Authentication has not been generated for the user in Active Directory. • You are using AA-PROX in a Windows 2008 R2 environment with Domain Authentication and the domain’s security policy is not set to allow the DES-CBC-MD5 encryption type.</td>
<td>• Reset the password for the intended user on the AD server. • Make sure that the domain’s security policy is modified to allow the DES-CBC-MD5 encryption type.</td>
</tr>
</tbody>
</table>
### Message | Cause | Remedy
---|---|---
**The machine will not operate normally because Dept. ID Management is set to On. Contact system manager.** | Department ID Management is set to ‘On’ on the MEAP device, and there is a conflict between the MEAP device and AA-PROX. | Set Department ID Management on the MEAP device to ‘Off’. See the Security e-Manual that came with your machine. |
**Card reader is not ready. Please make sure the card reader connection at USB port.** | The device cannot communicate with the card reader. | Make sure that the proximity card reader is attached to the machine correctly. |
**Main menu is unavailable because Department ID is not set for guest user. Please contact system manager.** | You are logged on to the machine as a Guest User, and you cannot access the Main Menu of the machine because the Guest User account requires a Department ID to be set. | Configure a Department ID for the Guest User account. See Chapter 5, “User Management,” on p. 137. |

### 6.1.2 Configuration Servlet Log In Error Messages

This section explains AA-PROX’s Configuration Servlet’s Log In screen error messages, along with possible causes and remedies.

<table>
<thead>
<tr>
<th>Message</th>
<th>Cause</th>
<th>Remedy</th>
</tr>
</thead>
</table>
**The account expiration date has passed. Please contact your system administrator.** | • The user account expired.  
• The user account is disabled. | • Reset the user account in Active Directory.  
• Enable the user account in Active Directory. |
**A password is not set on the authentication server side. Contact system manager.** | • The DES (Data Encryption Standard) key required for Domain Authentication has not been generated for the user in Active Directory.  
• You are using AA-PROX in a Windows 2008 R2 environment with Domain Authentication and the domain’s security policy is not set to allow the DES-CBC-MD5 encryption type. | • Reset the password for the intended user on the AD server.  
• Make sure that the domain’s security policy is modified to allow the DES-CBC-MD5 encryption type. |
**The password expiration date has passed. Contact system manager.** | • The password for the authenticated user has expired.  
• The user account is set to ‘Require Change of Password Next Login’ in Active Directory. | • Reset the password of the user account that expired in Active Directory.  
• Clear the check mark in the [Require Change of Password Next Login] check box in Active Directory. |
<table>
<thead>
<tr>
<th>Message</th>
<th>Cause</th>
<th>Remedy</th>
</tr>
</thead>
<tbody>
<tr>
<td>To log in, JRE (Java 2 Runtime Environment) is required. Install a version of JRE that supports this MEAP login application, and set the browser to use Java.</td>
<td>JRE is not installed on the computer that is trying to access AA-PROX’s Configuration servlet.</td>
<td>Install a version of JRE that supports AA-PROX, and set your Web browser to use Java.</td>
</tr>
<tr>
<td>You do not have privileges to display the specified page. Contact the system manager for details.</td>
<td>You are trying to access a page to which your account does not have access privileges.</td>
<td>Have an administrator grant you access privileges to the page you are trying to access.</td>
</tr>
<tr>
<td>The number of connections to access the login page has exceeded the limit. Please wait a moment and try to access the page again.</td>
<td>The maximum number of users is connected, and you cannot access the login page.</td>
<td>Wait until some users disconnect, and try to access the login page again.</td>
</tr>
</tbody>
</table>
| The authentication server is not running. Contact system manager. | • The LAN (Local Area Network) cable is not connected.  
• The Active Directory server is not started.  
• The KDC (Key Distribution Center) service of Active Directory stopped. | • Connect the LAN cable.  
• Start the Active Directory server.  
• Start the “Services” management tool on the Active Directory server, and then check whether the AD server is operating normally. |
| Could not obtain log in information. Contact system manager. | The port number specified in the ‘_ldap’ SRV record (part of the DNS information of the domain specified as the login destination) is incorrect. | Follow the procedure below to confirm the settings.  
1. Start the DNS server management tool.  
2. Double-click [Forward Lookup Zones] ➞ [<domain specified as the login destination>] ➞ [_.tcp].  
3. Right-click the ‘_ldap’ SRV record ➞ select [Properties].  
4. Select the [Service Location (SRV)] tab ➞ confirm the value in [Port Number]. If the port number is different from the port number of the LDAP service, enter the correct port number ➞ click [OK]. |
<table>
<thead>
<tr>
<th>Message</th>
<th>Cause</th>
<th>Remedy</th>
</tr>
</thead>
</table>
| **Authentication server not found. Contact system manager.** | • The LAN cable is not connected.  
• The primary/secondary DNS server settings in the machine are incorrect or not specified.  
• The DNS server specified in the machine is not started, or the service has been stopped.  
• Domain resolution could not be performed with the DNS server. | • Connect the LAN cable.  
• Confirm the DNS server settings on the machine, and specify the correct values. See “Specifying the DNS Server and Name Settings,” on p. 42.  
• Confirm the DNS server specified on the machine, and start the server if it has not been started.  
• Confirm that the host record exists on the DNS server, and that the forwarding settings are correct. |
| **Could not obtain authentication server information. Contact system manager.** | AA-PROX is unable to communicate with the authentication server. | Confirm the authentication server configuration, and make sure that all settings are specified correctly. |
| **Could not obtain restriction information. Contact system manager.** | The user’s role configuration settings are invalid. | Import the correct role information from iWEMC. See “Importing Roles,” on p. 131. |
| **The machine will not operate normally because Dept. ID Management is set to On. Contact system manager.** | Department ID Management is set to ‘On’ on the MEAP device, and there is a conflict between the MEAP device and AA-PROX. | Set Department ID Management on the MEAP device to ‘Off’. See the Security e-Manual that came with your machine. |
### 6.1.3 Configuration Screen Error Messages

This section explains the Configuration screen error messages, along with possible causes and remedies.

<table>
<thead>
<tr>
<th>Message</th>
<th>Cause</th>
<th>Remedy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain authentication setting is mandatorily required for proximity card authentication. Please configure a user name and password for each domain first. Otherwise, any user may not log in using proximity card.</td>
<td>No user names and passwords are configured for domain authentication.</td>
<td>Add the appropriate user names and passwords for each configured domain. See “Domain Authentication Configuration without AMS,” on p. 53, or “Domain Authentication Configuration with AMS,” on p. 84.</td>
</tr>
<tr>
<td>In order to get back to this configuration page with domain user, the domain user needs to join the user group specified below.</td>
<td>The user trying to access the configuration page is not a member of the necessary Domain user group.</td>
<td>Add the user to the appropriate user group, and have them try to access the configuration page again.</td>
</tr>
<tr>
<td>The Active Directory site information is invalid. Contact system manager.</td>
<td>The configured Active Directory site information is incorrect, and you cannot configure AA-PROX for Domain Authentication.</td>
<td>Make sure that the Active Directory site information is correct, and try to configure AA-PROX for Domain Authentication again.</td>
</tr>
<tr>
<td>System is under maintenance. Please try later.</td>
<td>The AA-PROX application is not started in MEAP SMS.</td>
<td>Check the device’s status, and make sure that the AA-PROX application fully starts. See Chapter 2, “Installing AA-PROX,” on p.17.</td>
</tr>
<tr>
<td>Cannot select Domain Authentication together with Department Management mode. Please disable Department Management mode on the device.</td>
<td>You tried to select [Domain Authentication] as the User Authentication System, and the Department ID Management mode is only supported with Local Device Authentication.</td>
<td>Set the Department ID Management mode to ‘Off’ on the machine before you configure AA-PROX for Domain Authentication. See the Security e-Manual that came with your machine.</td>
</tr>
<tr>
<td>Logo image must be 800x340 GIF/JPEG/PNG image. Otherwise, the uploaded image is disposed without notice.</td>
<td>The logo you are trying to upload is not within the specifications.</td>
<td>Make sure the logo you are trying to upload is 800 x 340 pixels and in the GIF, JPEG, or PNG format. See “Configuring the Other Settings,” on p. 116.</td>
</tr>
<tr>
<td>Message</td>
<td>Cause</td>
<td>Remedy</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Logo image must be 640x272 GIF/JPEG/PNG image. Otherwise, the uploaded image is disposed without notice.</td>
<td>The logo you are trying to upload is not within the specifications.</td>
<td>Make sure the logo you are trying to upload is 640 x 272 pixels and in the GIF, JPEG, or PNG format. See “Configuring the Other Settings,” on p. 116.</td>
</tr>
<tr>
<td>Default logo image is displayed if this option is disabled or incorrect image file has been uploaded.</td>
<td>The default logo image is displayed if the [Enable custom logo] check box is not selected, or if an incorrect image file is uploaded.</td>
<td>Select the [Enable custom logo] check box, and make sure to upload an image file within the specifications mentioned on the screen. See “Configuring the Other Settings,” on p. 116.</td>
</tr>
<tr>
<td>No domain to be configured. Please restart the device after the device and application settings correctly updated.</td>
<td>Domain information has been entered incorrectly on the device.</td>
<td>Enter the correct domain information on the device, and restart the machine. See “Specifying the DNS Server and Name Settings,” on p. 42.</td>
</tr>
<tr>
<td>Enabling debug mode may cause less performance.</td>
<td>Excessive debug logs may affect system performance.</td>
<td>Switch to a different logging filter, and then check the system’s performance.</td>
</tr>
<tr>
<td>Unable to update user account on Active Directory with registration data.</td>
<td>The user does not have permission to change the LDAP attributes.</td>
<td>Give the user proper permissions on the AD side.</td>
</tr>
</tbody>
</table>
This page is intentionally left blank.