Contents

Welcome to the Device Registration Service.................................................................5

Konica Minolta iOption Unified Client........................................................................6
  Overview.................................................................................................................6
  Prerequisites..........................................................................................................6
  Configure Konica Minolta OpenAPI.......................................................................6
  Configure the device to use the Authentication Application...............................7
  Configure the Konica Minolta iOption Unified Client...........................................9
    How to add an application......................................................................................9
    How to add a Konica Minolta iOption device......................................................11
    How to import device information......................................................................12
    How to register the Unified Client......................................................................14
    How to Register Unified Client Authentication..................................................14
    How to export device information......................................................................14
    How to add a device group..................................................................................15
    How to add a device to a device group...............................................................15
    How to perform device actions..........................................................................15
    How to view device information.........................................................................17
  Application navigation............................................................................................18
  Authentication.......................................................................................................20
    Card reader authentication....................................................................................21
    Touchscreen authentication..................................................................................21
  Troubleshooting the Konica Minolta iOption Unified Client..................................22

Ricoh ESA Unified Client..........................................................................................29
  Overview...............................................................................................................29
  System Requirements............................................................................................29
  Configure the Device.............................................................................................30
    Configure a device for external authentication..................................................30
    Configure a device for internal authentication..................................................33
    Single sign-on integration....................................................................................36
  Configure the Ricoh ESA Unified Client...............................................................37
    How to add an application....................................................................................37
    How to add a Ricoh ESA device..........................................................................38
    How to import device information......................................................................40
    How to export device information......................................................................43
    How to add a device group..................................................................................44
    How to add a device to a device group...............................................................44
    Ricoh authentication modes................................................................................44
    How to perform device actions..........................................................................46
    How to view device information.........................................................................47
  Configure Output Manager....................................................................................48
    How to configure the SSL port............................................................................48
    How to configure Output Manager devices.........................................................48
    How to configure copy quotas.............................................................................53
  Configure AutoStore..............................................................................................54
  How to install the Ricoh ESA Unified Client.........................................................54
Ricoh ESA Unified Client startup scenarios ..........................................................................................55
Ricoh ESA Unified Client Operations ...............................................................................................................55
Output Manager login .............................................................................................................................55
AutoStore login .......................................................................................................................................60
Ricoh ESA Unified Client screen layout ...................................................................................................60
Advanced Output Manager operations ......................................................................................................62
Logout ..................................................................................................................................................... 64
Internal login ...........................................................................................................................................65
Access control ........................................................................................................................................ 66
Accounting .............................................................................................................................................. 67
Quota management ................................................................................................................................... 67
Troubleshooting the Ricoh ESA Unified Client ..........................................................................................68

Xerox EIP Unified Client..........................................................................................................................70
Overview ............................................................................................................................................................. 70
Configure the Xerox EIP Unified Client ........................................................................................................... 70
How to add an application .......................................................................................................................... 70
How to add a Xerox EIP device .................................................................................................................... 72
How to import device information ............................................................................................................... 72
How to export device information ............................................................................................................... 73
How to add a device group .......................................................................................................................... 74
How to add a device to a device group ......................................................................................................... 74
How to perform device actions .................................................................................................................... 74
How to register the Unified Client ............................................................................................................ 75
Connect to Output Manager .......................................................................................................................... 75
How to view device information ................................................................................................................... 76
Application navigation .................................................................................................................................... 78
Log on to the Xerox Unified Client ............................................................................................................... 78
Secure Print page .......................................................................................................................................... 79
Properties page ............................................................................................................................................. 80
Settings page ................................................................................................................................................ 81
Authentication ................................................................................................................................................ 82
Card reader authentication .......................................................................................................................... 83
Touch screen authentication ......................................................................................................................... 83

Troubleshooting Device Registration Service ..........................................................................................84
Service verification ........................................................................................................................................ 86
Welcome to the Device Registration Service

The Device Registration Service web-based interface enables you to manage applications, devices, and device groups. Use the Device Registration Service to register Unified Clients on devices. A Unified Client is a component that merges AutoStore scan and Output Manager print functionality on a device. The device properties determine the scan and print functions that are available to users.

Configuring a Unified Client through Device Registration Service consists of the following high-level steps:

1. Add an application for a Unified Client type and configure the application properties.
2. Add devices and configure their properties.
3. If necessary, add device groups to organize the devices for an application.
4. Register the Unified Client on the device.

System configuration procedures vary depending on your business requirements and the Unified Client type. Refer to the section for your Unified Client for more information.
Konica Minolta iOption Unified Client

Overview

The Konica Minolta iOption Unified Client is a web-based client that merges AutoStore scan and Output Manager print functionality on Konica Minolta iOption MFP devices. The Konica Minolta iOption Unified Client has an authentication module and language interfaces for Danish, Dutch, English, Finnish, French, German, Italian, Norwegian, Portuguese (Brazilian), Spanish (Latin American), and Swedish.

When a user starts the Konica Minolta Unified Client on a device, the client connects to the embedded web server hosted by AutoStore or Output Manager. The embedded web server uses the MFP device IP address to retrieve device configuration data from Device Registration Service. This data determines how the Konica Minolta Unified Client behaves and how it contacts the AutoStore and Output Manager servers.

The following figure illustrates the architecture for a system that includes the Konica Minolta iOption Unified Client:

Prerequisites

Before you set up and register the Konica Minolta iOption Unified Client in Device Registration Service, configure the Konica Minolta OpenAPI and configure the device to use the authentication application.

Configure Konica Minolta OpenAPI

1. Log on to the MFP with the Admin password (Utility > Administrator Settings).
Configure the device to use the Authentication Application

Complete the following procedures in the order listed to configure a device for the Authentication Application:

**How to configure a device to use SSL for Web Services (OpenAPI)**

1. Create a self-signed certificate in security tab
2. Set up OpenAPI to use SSL

**Create a self-signed certificate in security tab**

1. Open a web browser and log on to the MFP as an administrator.
2. Click the Security tab and click SSL/TLS Setting.
   The following page appears if the certificate is not installed:
3. Click Setting.
4. Select Create a self-signed certificate.
5. Click OK.

![Image](image1)

6. Specify certificate values and click OK.
   Do not close the browser while the system generates the certificate.
7. Click OK.
8. If your browser indicates that the security certificate is not valid, accept the certificate to continue with Set up OpenAPI to use SSL.

**Set up OpenAPI to use SSL**
1. Click the Network tab and click OpenAPI Setting.
2. Select Use SSL/TLS and click OK.
   **Note:** This automatically uses port 50003.
3. Click OK.

**How to set up WebDAV to use SSL**
1. Open a web browser and log on to the MFP as an administrator.
2. On the Network tab, select WebDAV Settings > WebDAV Server Settings.

![Image](image2)

3. Select ON from the WebDAV Settings drop-down list.
4. Select SSL Only from the SSL Setting drop-down list and click OK.
5. Press OK.

**How to set up TCP Socket Setting to use SSL/TLS**

1. Open a web browser and log on to the MFP as an administrator.
2. Click the **Network** tab and click **TCP Socket Setting**.

![TCP Socket Setting](image)

3. Select **Use SSL/TLS Port No.(SSL)**.
4. Click **OK**.

**Configure the Konica Minolta iOption Unified Client**

**How to add an application**

This task explains how to create a Konica Minolta iOption application profile in Device Registration Service. The application profile defines the server settings for AutoStore, Output Manager, and Device Registration Service.

2. Click **Applications**.
3. Click **Add Application** on the **Applications** toolbar.
4. Type an application name.
5. Select **Konica Minolta iOption** from the **Application Type** drop-down list box.
6. Configure application properties as described in the following table:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AutoStore Server Address</strong></td>
<td>The IP address, computer name, or DNS name of the machine that hosts AutoStore Server. The default is the local IP address. You must specify an address when using AutoStore or when using both AutoStore and Output Manager. Device actions use this address. If you do not specify this address and you enable AutoStore Scan, error code 518 appears when you perform the <strong>Register Unified Client</strong> action.</td>
</tr>
<tr>
<td><strong>Output Manager Server Address</strong></td>
<td>The IP address of the machine that hosts the Output Manager server. The default is the local IP address. You must specify an address when using Output Manager or both AutoStore and Output Manager.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Device actions</strong></td>
<td>Device actions use this address if you do not enter an address for <strong>AutoStore Server Address</strong>. If you do not specify this address and you enable <strong>Print Release</strong>, error code 519 appears when you perform the <strong>Register Unified Client</strong> action.</td>
</tr>
<tr>
<td><strong>Output Manager Service URI</strong></td>
<td>The URI for the Output Manager server. The default URI is in the following format: <code>http://local_IP_address:8068</code>. You must specify a value when using Output Manager or both AutoStore and Output Manager.</td>
</tr>
<tr>
<td></td>
<td>You can specify HTTP or HTTPS protocols. If necessary, configure Output Manager for the selected protocol.</td>
</tr>
<tr>
<td><strong>Web Application Port</strong></td>
<td>The port number used by the web application. The default is 3348.</td>
</tr>
<tr>
<td></td>
<td>Verify that this port number matches the port number that you specified when configuring AutoStore or Output Manager:</td>
</tr>
<tr>
<td></td>
<td>• If you use AutoStore only, you specified the port number when configuring the component in AutoStore Process Designer.</td>
</tr>
<tr>
<td></td>
<td>• If you use AutoStore and Output Manager, you specified the port number when configuring the component in AutoStore Process Designer.</td>
</tr>
<tr>
<td></td>
<td>• If you use Output Manager only, you specified the port number when configuring <strong>Server port</strong> on the <strong>Clients</strong> tab in the <strong>Set General Preferences</strong> settings of the <strong>Administration</strong> module in Output Manager.</td>
</tr>
<tr>
<td></td>
<td>If this port does not match the <strong>Web Server Port</strong> in the AutoStore Process Designer Konica Minolta iOption component <strong>Preferences</strong> setting, <em>Connection error</em> appears on the device panel when a user presses the application button.</td>
</tr>
<tr>
<td></td>
<td>If you use Output Manager only and this port does not match the <strong>Server Port</strong> setting on the <strong>Clients</strong> tab in the <strong>Set General Preferences</strong> settings of the <strong>Administration</strong> module of Output Manager, <em>Connection error</em> appears on the device panel when a user presses the application button.</td>
</tr>
<tr>
<td><strong>Use SSL for Web Application</strong></td>
<td>Enables secure socket layer (SSL) for the web application. The default is False.</td>
</tr>
<tr>
<td></td>
<td>If this value does not match the <strong>Use SSL</strong> setting in the AutoStore Process Designer Konica Minolta iOption component <strong>Preferences</strong> settings, <em>Connection error</em> appears on the device panel when a user presses the application button.</td>
</tr>
</tbody>
</table>
**Application OpenAPI Port**

The Konica Minolta OpenAPI port number for the Konica Minolta iOption Unified Client. The default is 13351.

This port number is used to run the embedded KM Konica Minolta OpenAPI server for a web application.

**Authority OpenAPI Port**

The Konica Minolta OpenAPI port number for the Authority application. The default is 13353.

This port number is used to run the embedded Konica Minolta OpenAPI Server for an authentication application.

**Application Timeout**

The period of inactivity in seconds before the Notable Solutions Unified Client times out. The default is 60 seconds.

7. Click **Save application**.

**How to add a Konica Minolta iOption device**

This task explains how to create a device profile for the Konica Minolta iOption Unified Client. The profile enables you to manage Unified Client, AutoStore, Output Manager, and authentication settings on the device through Device Registration Service.

2. Click **Devices**.
3. Click **Add Device** on the **Devices** toolbar.
4. Type a device name.
5. Type the IP address or DNS address of the device.
   The address is specific to the device and does not appear when you configure properties for a device group.
6. Type the administrator user name for the device.
   The default is **admin**. The user name is not required to perform an action on the device.
7. Type the password for the administrator user name.
   By default, there is not a password and the field is empty.
8. Select the target application.
9. Configure device properties as described in the following table:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Functionality</td>
<td>Determines the default functionality for the client:</td>
</tr>
<tr>
<td></td>
<td>• Output Manager: The <strong>Print Release</strong> page appears when a user presses the</td>
</tr>
<tr>
<td></td>
<td>application button on the device panel.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AutoStore</td>
<td>The AutoStore page appears when a user presses the application button on the device panel.</td>
</tr>
<tr>
<td>Enable Print Release</td>
<td>Enables Output Manager print functionality. The default value is False.</td>
</tr>
<tr>
<td>Display destination specific documents only</td>
<td>Enables the user to see only printing jobs that are associated with a specific destination or with a group of destinations. The default value is False.</td>
</tr>
<tr>
<td>Enable Scan</td>
<td>Enables AutoStore scan functionality. The default value is False.</td>
</tr>
<tr>
<td>Application Name</td>
<td>The application name that appears on the device panel.</td>
</tr>
<tr>
<td>Open API Login Name</td>
<td>The login name for the Open API authentication layer. This setting is required if you use the OpenAPI authentication layer on the device. To use the OpenAPI authentication layer on a device, turn on OpenAPI authentication and configure a user name and password. The login name specified here must then match the user name specified for the OpenAPI settings on the device.</td>
</tr>
<tr>
<td>Open API Password</td>
<td>The password for the Open API authentication layer. This setting is only required if you use the OpenAPI authentication layer on the device. To use the OpenAPI authentication layer on a device, OpenAPI authentication needs to be turned on and you must configure a user name and password. The password specified here must then match the password specified for the OpenAPI settings on the device.</td>
</tr>
</tbody>
</table>

10. Click Add Device on the Add Device toolbar.

**How to import device information**

This task explains how to import device information into Device Registration Service from Output Manager or a CSV file.

2. Click Devices.
3. Click Import on the Devices toolbar and select the import method:
   - To import device information from the Output Manager server, select Import from OM.
     Type the address of the Output Manager server, select the application profile, optionally select the device group, and click Import from OM. Device Registration Service only imports devices that are marked as Unified Client devices in Output Manager.
   - To import device information from a CSV file, select Import from file.
     Browse to the CSV file and click Upload.
4. Close the Import Results window.
5. If necessary, edit the device properties:
a) Select the device in the Devices pane.
b) Click Edit on the Details toolbar.
c) Update the device properties.
d) Click Save on the Details toolbar.

Import guidelines
This topic provides guidelines for importing Konica Minolta iOption device information into Device Registration Service with a comma separated values (CSV) file.

Header information
The first row in the CSV file is the header row that contains header values for device information. Header values appear in the following order: Name, IP, ApplicationProfile, DeviceGroup, Properties, InheritPropertyFromGroup, SerialNumber, Username, Password. The subsequent rows list the corresponding values for each device separated by commas. Use the same header row when importing devices for all Unified Client types.

You can omit values other than Name, IP, and ApplicationProfile. The first row must always contain the header row because the Device Registration Service uses the headers to identify imported values. If you omit a value, make sure to insert the comma.

Konica Minolta iOption properties
When you add a property to the file, do not include a space in the property name. The following table describes the properties that you can include in the file:

Note: An asterisk indicates a required property.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| DefaultFunctionality (*)| Determines the default functionality for the Unified Client. This is specified by one of the following options:  
  • Output Manager: The Print Release page appears when the user presses the application button on the device panel.  
  • AutoStore: The AutoStore page appears when the user presses the application button on the device panel. |
| EnablePrintRelease (*)  | Enables Output Manager print functionality. The default value is False.       |
| EnableScan (*)          | Enables AutoStore scan functionality. The default value is False.            |
| ApplicationName         | The default application name that appears on the device panel.               |
| OpenApiUser             | The user name for Open API.                                                  |
| OpenApiPassword         | The password for the Open API user name.                                    |

Sample import file
The following example shows Konica Minolta iOption import file entries:
How to register the Unified Client

This task explains how to register the Konica Minolta iOption Unified Client on the MFD.

2. Click Devices and select the device.
3. On the Details toolbar, select Register Unified Client from the drop-down list box.
4. Click Perform selected action.
5. Optional: To view registrations for a device, select the device and click Refresh status on the Details toolbar.

The following example shows registrations for a device:

After registration, a button with the application name appears in the APP section on the device.

How to Register Unified Client Authentication

This task explains how to use Device Registration Service to register Konica Minolta iOption Unified Client authentication on the device.

1. Verify that you configured the device for authentication as described in Configure the device to use the Authentication Application on page 7.
3. Click Devices and select the device.
4. On the Details toolbar, select Register Authentication from the drop-down list box.
5. Click Perform selected action.

How to export device information

This task explains how to export Konica Minolta iOption device information to a CSV file.

1. Click Devices.
2. On the Devices toolbar, click Export.

Device Registration Service exports the device information to a CSV file in the following format:

Name, IP, ApplicationProfile, Device Group, Properties, InheritPropertyFromGroup, SerialNumber, Username, Password

Tip: You can use the exported CSV file as a template to import device information.
How to add a device group
This task explains how to create a group to organize devices in Device Registration Service. The device group is a single configuration point for managing multiple devices for an application.

1. Click Devices.
3. Enter the Name, Username and Password for the device group.
4. From the drop-down list box, select the target application.
5. Configure device group properties.

How to add a Konica Minolta iOption device on page 11 provides more information on the properties that you can configure.


How to add a device to a device group
This task explains how to add a device to a device group.

1. Click Devices.
   To add an existing device to a group, highlight the device and drag it to the device group.
2. Select the device group.
3. Click Add Device.
4. Type a device name and the device address.
5. Specify the property inheritance value:
   • To inherit properties from the device group, select True for Inherit Properties from Group.
   • To configure specific device properties, select False and configure the properties.

How to add a Konica Minolta iOption device on page 11 provides more information on configuring device properties.

6. Click Add Device.

How to perform device actions

2. Click Devices.
3. Select a device.
4. On the Details toolbar, select an action as described in the following table:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Register Unified Client | Registers the Konica Minolta iOption Unified Client on the device. Registration adds a button with the application name to the APP section on the device.  
  Note: Because devices are registered while the server is running, it is not necessary to restart the server after adding and registering new devices. |
| Unregister Unified Client | Deregisters the Unified Client from the device. The button with the application name is removed from the application software section on the device. |
| Register Authentication | Registers Unified Client authentication on the device. After you register authentication, the authentication |
application controls access to the device. End users cannot view the device menus and the application software section until authentication is complete.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unregister Authentication</td>
<td>Deregisters authentication on the device. After you deregister authentication, the device shows the normal menu screen.</td>
</tr>
</tbody>
</table>

5. **Click Perform selected action.**

**Konica Minolta iOption return codes**
The following table describes the return codes that can appear in the Device Registration Service **Action History** pane for a Konica Minolta iOption device or device group.

<table>
<thead>
<tr>
<th>Return Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>101</td>
<td>Successful Konica Minolta iOption Unified Client registration.</td>
</tr>
<tr>
<td>102</td>
<td>Successful authentication registration.</td>
</tr>
<tr>
<td>104</td>
<td>Successful Unified Client deregistration.</td>
</tr>
<tr>
<td>105</td>
<td>Successful authentication deregistration.</td>
</tr>
<tr>
<td>301</td>
<td>Device is offline.</td>
</tr>
<tr>
<td>302</td>
<td>Device is online.</td>
</tr>
<tr>
<td>303</td>
<td>Device is online and one of three applications is registered.</td>
</tr>
<tr>
<td>304</td>
<td>Device is online and two of three applications are registered.</td>
</tr>
<tr>
<td>305</td>
<td>Device is online and all three applications are registered.</td>
</tr>
<tr>
<td>500</td>
<td>Konica Minolta iOption device registration failed.</td>
</tr>
<tr>
<td>501</td>
<td>Konica Minolta iOption device deregistration failed.</td>
</tr>
<tr>
<td>502</td>
<td>Unable to proceed. Please restart device.</td>
</tr>
<tr>
<td>503</td>
<td>Invalid password. Please retry login.</td>
</tr>
<tr>
<td>504</td>
<td>Unable to connect to device. Please restart device.</td>
</tr>
<tr>
<td>505</td>
<td>Maximum registered applications exceeded. Remove unused applications and retry.</td>
</tr>
<tr>
<td>506</td>
<td>Device is locked. Retry later.</td>
</tr>
<tr>
<td>Return Code</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>507</td>
<td>Logo icon file does not exist. Contact Notable Solutions Support.</td>
</tr>
<tr>
<td>508</td>
<td>The device solution key file not found. Contact Notable Solutions Support.</td>
</tr>
<tr>
<td>509</td>
<td>Invalid Output Manager server address. Enter correct server address and retry.</td>
</tr>
<tr>
<td>510</td>
<td>Registration was unsuccessful on the device.</td>
</tr>
<tr>
<td>511</td>
<td>Device does not support iOption. Add iOption or use the Native Scan connector.</td>
</tr>
<tr>
<td>512</td>
<td>Invalid password. Enter the valid password and retry.</td>
</tr>
<tr>
<td>513</td>
<td>Deregistration failed because Unified Client is not registered.</td>
</tr>
<tr>
<td>515</td>
<td>OpenAPI SSL is not enabled on the device. Authority registration requires OpenAPI SSL. See Device Registration Service Help to enable OpenAPI SSL.</td>
</tr>
<tr>
<td>517</td>
<td>Registration failed due to insufficient device memory.</td>
</tr>
<tr>
<td>518</td>
<td>Invalid AutoStore server address. Enter the valid address and retry.</td>
</tr>
<tr>
<td>519</td>
<td>Invalid web application port number. Enter the valid port number and retry.</td>
</tr>
</tbody>
</table>

### How to view device information

1. Browse to the Device Registration Service (for example, [http://10.16.37.51:9000/device](http://10.16.37.51:9000/device)).
2. Click **Devices**.
3. To filter device and device group information that appears in the **Devices** pane, type or select criteria in the **Filter** pane and click **Apply**.
4. To view action history for a device or device group, select the device or device group in the **Details** pane.

The **Action History** pane shows the following information:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Time stamp of when the action was attempted.</td>
</tr>
<tr>
<td>Action</td>
<td>Attempted action.</td>
</tr>
<tr>
<td>Message</td>
<td>Action taken and the result.</td>
</tr>
<tr>
<td>Status</td>
<td>Status for the action.</td>
</tr>
<tr>
<td>Success</td>
<td>Indicates if the action was successful.</td>
</tr>
</tbody>
</table>
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Name of the device.</td>
</tr>
<tr>
<td>Address</td>
<td>IP address of the device.</td>
</tr>
<tr>
<td>Return code</td>
<td>Return code returned by the device. The values shown on the device type.</td>
</tr>
</tbody>
</table>

### Application navigation

This topic provides general information on navigating the Unified Client application on the Konica Minolta iOption device panel.

The device properties that you configured determine if AutoStore, Output Manager, or both AutoStore and Output Manager options appear on the device panel. If you configured the Unified Client for both AutoStore and Output Manager functionality, you can toggle between them on the device.

The Konica Minolta iOption Unified Client initially shows an authentication screen unless authentication has been registered for the device, in which case single sign-on is attempted.

The initial screen that appears depends on the default functionality that is set for the device and the settings on the AutoStore or Output Manager server. You can configure AutoStore to not require a login. Output Manager always requires user identification.

If Output Manager is the default application, the **Start Print Release** screen appears and shows the print jobs that are waiting to be printed.
You can select documents and then press **Print, Print All, Delete, Change Settings** or **Info**.

The following table describes the options available through the interface:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Printed Jobs</td>
<td>Toggles the view to show documents for the current user that have been printed.</td>
</tr>
<tr>
<td></td>
<td>Documents in the printed jobs list are in a retained state, which may be configured by an administrator to have an expiration period.</td>
</tr>
<tr>
<td>View Unprinted Jobs</td>
<td>Toggles the view to show documents for the current user that are unprinted.</td>
</tr>
<tr>
<td>Print</td>
<td>Routes selected documents to the device and releases them for printing.</td>
</tr>
<tr>
<td>Print All</td>
<td>Routes all documents in the list to the device and releases them for printing.</td>
</tr>
<tr>
<td>Delete</td>
<td>Prompt to confirm deletion and then permanently deletes the selected documents.</td>
</tr>
<tr>
<td>Change Settings</td>
<td>Adjusts print preferences of the selected documents. Press <strong>Done</strong> to return to the documents view. Any changes are submitted to Output Manager.</td>
</tr>
<tr>
<td>Info</td>
<td>View document details.</td>
</tr>
</tbody>
</table>

The **Info** button shows information about the selected document.
If you configured the Unified Client for both Output Manager and AutoStore, toggle between the applications by pressing the AutoStore scanner button or the Output Manager printer button.

In the following example, Output Manager is the active application. Pressing the scanner button switches to AutoStore.

In the following example, AutoStore is the active application. Pressing the printer button switches to Output Manager.

**Authentication**

The Konica Minolta iOption Unified Client provides an authentication service for Konica Minolta MFPs. The service enables authentication through card readers and a touch screen. The credentials obtained from the MFP are available
to the Unified Client and other applications running on the device. You can also apply access control by restricting specific users from features on the MFP.

**Card reader authentication**

Most Konica Minolta MFPs support USB-attached card readers. Contact Konica Minolta Support to determine which card readers are compatible with your MFP and if any firmware upgrades are required.

When the user authenticates through a card reader, the MFP sends the card ID to Output Manager. If a match is found, the authentication service grants access based on the ACL configured for the user for that MFP. The service also provides information about the user, such as the user name and email address. If a match is not found, the MFP enables the user to associate the card to the user name. Subsequent use of the card results in user authentication.

Use the Output Manager Console to configure card login settings. In the Administration application, select Set General Preferences and select the Security tab. Click Help when the Security tab is active for more information on configuring security settings.

During two-phase authentication, the user provides a Personal Identification Number (PIN) after swiping a card. When you configure Output Manager to require two-phase authentication, the MFP prompts the user for the PIN after swiping the card.

**Touchscreen authentication**

An end user can authenticate through the MFP touchscreen. If no user is logged on at the MFP, the console shows the Output Manager log on screen. Depending on the Output Manager configuration, the end user can log in by entering a card ID, by entering a card ID and a PIN, or by entering a user name and password.

![Figure 1: Prompt to enter domain user name and password](image)

Copyright © 2014 Notable Solutions, Inc.
Troubleshooting the Konica Minolta iOption Unified Client

- **Authentication connection errors** on page 22
- **Unified Client application connection errors** on page 23
- **Unified Client resets too quickly** on page 23
- **Unified client registration error messages** on page 25
- **Authentication registration error messages** on page 26
- **Unified Client deregistration error messages** on page 26
- **Orphan Unified Client button on the device** on page 27

**Authentication connection errors**

Follow these steps to resolve an authentication connection error on a device:

- Verify that the AutoStore and Output Manager servers are started.
- Verify that the port specified in the application settings for a device in the Device Registration Service matches the port specified in AutoStore or Output Manager:
  - If you are using AutoStore or both AutoStore and Output Manager, confirm the **Web Application Port** value in the application settings matches the AutoStore component port setting
  - If you are only using Output Manager, confirm the **Web Application Port** value in the application settings matches the **Server Port** value on the **Clients** tab in the Output Manager Administration application.

  How to add an application on page 9 provides more information on application settings.

- Verify that the **Use SSL for Web Application** setting specified in the application settings for the device in the Device Registration Service matches the **Use SSL** setting in AutoStore or Output Manager:
  - If you are using AutoStore or both AutoStore and Output Manager, confirm the **Use SSL for Web Application** setting in the application settings matches the **Use SSL** setting for the AutoStore component.
  - If you are only using Output Manager, confirm the **Use SSL for Web Application** setting in the application settings matches **Use SSL** on the **Clients** tab in the Administration module of Output Manager.

  How to add an application on page 9 provides more information on application settings.

- Test the Authority Application by creating a dummy device without registering it on an actual device in Device Registration Service and then typing the following address in a web browser:

  `http://server_IP_address:3348/Authority`

  This assumes that Device Registration Service uses default web application port 3348 and the **Use SSL** value is **False**.
• Test the OpenAPI Authority by typing the following address in a web browser:

   http://server_IP_address:13353

   This assumes the OpenAPI authentication uses default port 13353 and the Use SSL value is set to False.

• Restart the device and the AutoStore or Output Manager service.

• Verify that there is no firewall software or hardware blocking the specified port and that IP routing has been set up to enable communication on this port.

**Unified Client application connection errors**

• Verify that the AutoStore and Output Manager servers are started.

• Verify that the port specified in the application settings for a device in the Device Registration Service matches the port specified in AutoStore or Output Manager:
  • If you are using AutoStore or both AutoStore and Output Manager, confirm the port used by the device in Device Registration Service matches the Web Server Port setting in the Preferences for the Konica Minolta iOption component in AutoStore Process Designer.
  • If you are only using Output Manager, confirm the Web Server Port setting in the application settings matches the Server Port setting on the Clients tab in the Output Manager Administration application.

   *How to add an application* on page 9 provides more information on application settings.

• Verify that the Use SSL for Web Application setting specified in the application settings for the device in the Device Registration Service matches the Use SSL setting in AutoStore or Output Manager:
  • If you are using AutoStore or both AutoStore and Output Manager, confirm the Use SSL for Web Application setting in the application settings matches the Use SSL setting for the AutoStore component.
  • If you are only using Output Manager, confirm the Use SSL for Web Application setting in the application settings matches Use SSL on the Clients tab in the Output Manager Administration application.

   *How to add an application* on page 9 provides more information on application settings.

• Test the Authority Application by creating a dummy device without registering it on an actual device in Device Registration Service and then typing the following address in a web browser:

   http://server_IP_address:3348/Authority

   This assumes the Device Registration Service uses default web application port 3348 and the Use SSL setting is False.

• Test the OpenAPI application by typing the following address in a web browser:

   http://server_IP_address:13351

   This assumes the OpenAPI application port uses default port 13351 and the Use SSL setting is False.

• Restart the device and the AutoStore or Output Manager service.

• Verify that there is no firewall software or hardware blocking the specified port and that IP routing has been set up to enable communication on this port.

**Unified Client resets too quickly**

**Problem description**

When the user is working on the Konica Minolta iOption Unified Client screen, the screen resets after one minute, even if the user pressed buttons on the screen within the last minute.

**Cause**

The Auto Reset System setting in the MFP is set to 1 minute.

The **Auto Reset Setting** controls the timeout for the MFP client. This timeout is not reset when buttons are pressed in a browser-based application such as the Konica Minolta iOption Unified Client.

**Solution**
Increase the device timeout interval to 3 minutes.

Complete these steps to increase the device timeout interval:

**Note:** The MFP administrator password is required to access the Administrator Settings menu.

1. Change **System Auto Reset Time** to 3 minutes in the MFP control panel:

   Press **Utility > Administrator Settings > System Settings > Reset Settings > System Auto Reset > System Auto Reset Time**.

   ![System Auto Reset Settings](image)

2. Find the **Priority Mode** used when the MFP resets:

   Press **Utility > Administrator Settings > System Settings > Reset Settings > System Auto Reset > Priority Mode**.

3. Make a note of this setting (the default is Copy) and then change the **Auto Reset** setting for the function:

   Press **Utility > Administrator Settings > System Settings > Reset Settings > Auto Reset**.

   ![Auto Reset Settings](image)

4. Change the value for the appropriate function to 3 minutes:

   - If priority function was Main Menu or Copy, change the value for the **Copy** reset.
   - If priority function was **Scan**, change the value for the **Scan/Fax** reset.
   - If priority function was **User Box**, change the value for the **User Box** reset.
   - If priority function was **Web Browser**, change the value for the **Web Browser** reset.
## Unified client registration error messages

<table>
<thead>
<tr>
<th>Code</th>
<th>Message</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>502</td>
<td>Unable to proceed. Please restart device.</td>
<td>The device may be in faulted state or the device does not support OpenAPI. If the device is started and this error still occurs, contact Notable Solutions Support.</td>
</tr>
<tr>
<td>503</td>
<td>Invalid password. Please retry login.</td>
<td>Verify that you enter the correct device admin password in the device Details pane in Device Registration Service.</td>
</tr>
<tr>
<td>504</td>
<td>Unable to connect to device. Please restart device.</td>
<td></td>
</tr>
<tr>
<td>505</td>
<td>Maximum registered applications exceeded. Please remove unused applications and retry.</td>
<td></td>
</tr>
<tr>
<td>506</td>
<td>Device is locked. Please retry later.</td>
<td>Verify that the device is not in authentication mode or application mode.</td>
</tr>
<tr>
<td>507</td>
<td>Logo icon file does not exist. Contact Notable Solutions Support.</td>
<td></td>
</tr>
<tr>
<td>508</td>
<td>Device solution key file not found. Contact Notable Solutions Support.</td>
<td></td>
</tr>
<tr>
<td>509</td>
<td>Invalid Output Manager server address. Enter correct server address and retry.</td>
<td>The Output Manager server address is blank. Enter the Output Manager server on the Applications tab in Device Registration Service or set Enable Print Release as False in the device Details pane.</td>
</tr>
<tr>
<td>511</td>
<td>iOption not supported on device. Add iOption or use the Native Scan connector.</td>
<td></td>
</tr>
<tr>
<td>512</td>
<td>Invalid password. Enter the valid password and retry.</td>
<td>Reenter your credentials using a valid password.</td>
</tr>
<tr>
<td>518</td>
<td>Invalid AutoStore server address. Enter the valid address and retry.</td>
<td>The AutoStore server address is blank. Enter the AutoStore server on the Applications tab of Device Registration Service or set Enable</td>
</tr>
<tr>
<td>Code</td>
<td>Message</td>
<td>Comments</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>----------</td>
</tr>
<tr>
<td>519</td>
<td>Invalid Web application port number. Enter the valid port number and retry.</td>
<td>The Web Application Port setting is blank or contains a negative number. Enter a valid port number for Web Application Port on the Application tab of Device Registration Service.</td>
</tr>
</tbody>
</table>

**Authentication registration error messages**

Registration requires that the device is on and functioning normally. Ping the device or access PageScape to verify that the device is communicating with the network. The AutoStore and Output Manager services do not have to be running when you perform the registration.

<table>
<thead>
<tr>
<th>Code</th>
<th>Message</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>502</td>
<td>Unable to proceed. Please restart device.</td>
<td>The device may be in a faulted state or the device does not support OpenAPI. If the device is started and this error still occurs, contact Notable Solutions Support.</td>
</tr>
<tr>
<td>503</td>
<td>Invalid password. Please retry login.</td>
<td>Verify that you enter the correct device administrator password.</td>
</tr>
<tr>
<td>504</td>
<td>Unable to connect to device. Please restart device.</td>
<td></td>
</tr>
<tr>
<td>506</td>
<td>Device is locked. Please retry later.</td>
<td>Verify that the device is not in authentication mode or application mode.</td>
</tr>
<tr>
<td>509</td>
<td>Invalid Output Manager server address. Enter correct server address and retry.</td>
<td>The Output Manager server address is blank. Either enter the Output Manager server address on Applications tab of DRS or set Enable Print Release as False on Devices tab of the Device Registration Service.</td>
</tr>
</tbody>
</table>

**Unified Client deregistration error messages**

Un-registration requires that the device is on and functioning normally. Ping the device or access PageScape to verify that the device is communicating with the network.

<table>
<thead>
<tr>
<th>Code</th>
<th>Message</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>502</td>
<td>Unable to proceed. Please restart device.</td>
<td>The device may be in a faulted state or the device does not support OpenAPI. If the device is started</td>
</tr>
<tr>
<td>Code</td>
<td>Message</td>
<td>Comments</td>
</tr>
<tr>
<td>------</td>
<td>----------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and this still occurs, contact Notable Solutions Support.</td>
</tr>
<tr>
<td>503</td>
<td>Invalid password. Please retry login.</td>
<td>Verify that you enter the correct device administrator password.</td>
</tr>
<tr>
<td>504</td>
<td>Unable to connect to device. Please restart device.</td>
<td></td>
</tr>
<tr>
<td>506</td>
<td>Device is locked. Please retry later.</td>
<td>Verify that the device is not in authentication mode or application mode.</td>
</tr>
<tr>
<td>513</td>
<td>Unregistration failed because no unified client has been registered.</td>
<td>There is no registered Unified Client application.</td>
</tr>
</tbody>
</table>

**Orphan Unified Client button on the device**

Use the Konica Minolta MFP component to remove the button:

1. Open the Konica Minolta MFP component **Properties** dialog box.
2. Click **Device Manager**.
3. Enter values for **IP Address** and **Admin password** and click the **Application list** button.
4. Select the Unified Client application and click **Delete**.
<table>
<thead>
<tr>
<th>App No</th>
<th>Name</th>
<th>Type</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>AutoStorm:UC1</td>
<td>Browser (Scan)</td>
<td>3.5</td>
</tr>
</tbody>
</table>
Ricoh ESA Unified Client

Overview

The Ricoh ESA Unified Client merges Output Manager print and AutoStore scan functionality on a Ricoh Multi-Function Device (MFD) or Multi-Function Printer (MFP). Use Device Registration Service to install the Ricoh Unified Client on the device and to configure the device with Output Manager server and AutoStore server settings. Your business requirements determine if your environment uses Output Manager or AutoStore or if your environment uses both Output Manager and AutoStore.

The Ricoh ESA Unified Client supports Output Manager and AutoStore authentication through user name and password, card identification (ID) with an optional personal identification number (PIN), and card swipe with an optional PIN.

The Ricoh ESA Unified Client supports single sign-on (SSO) for the following systems:
- Adaptable Authentication API (AAA): Ricoh SSO infrastructure.
- Internal authentication: built-in MFD logon mechanism.

The Ricoh ESA Unified Client can collect accounting data to enable you to track usage for up to three billing accounts.

System Requirements

This topic describes system requirements for the Ricoh ESA Unified Client.

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoStore</td>
<td>Version 6.0 SP1</td>
</tr>
<tr>
<td>Output Manager</td>
<td>Version 3.2.27.29</td>
</tr>
</tbody>
</table>
| Java           | The Ricoh Unified Client supports devices with the following versions of the Java platform:  
|                | • 4.x                                              |
|                | • 5.x                                              |
|                | • 7.x, except for 4-line LCD devices               |
|                | • 10.x                                             |
|                | • 11.x                                             |
|                | • 12.x                                             |
|                | Refer to the Ricoh brand matrix to determine the Java platform version on a device. |
| Languages      | The Ricoh Unified Client provides localization support for the following languages:  
<p>|                | • Spanish (Latin American)                         |
|                | • German                                           |
|                | • Italian                                          |
|                | • Dutch                                            |
|                | • Danish                                           |</p>
<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Swedish</td>
</tr>
<tr>
<td></td>
<td>• French</td>
</tr>
<tr>
<td></td>
<td>• Portuguese (Brazilian)</td>
</tr>
<tr>
<td></td>
<td>• Norwegian</td>
</tr>
<tr>
<td></td>
<td>• Finnish</td>
</tr>
</tbody>
</table>

Card readers

The Ricoh Unified Client has been tested for the following card readers:

• RFIDeas, MS3-00M1AKU, pcSwipe, Card: magnetic stripe.
• RFIDeas, RDR-6081APU pcProx. Card: HID.
• RFIDeas, RDR-7581APU pcProx. Card:
  • MIFARE® CSN
  • MIFARE® DesFire CSN
  • ISO 14443A/15693 CSN

For RFIDeas readers, the second to last character in the model number indicates the device color (P=Pearl, K=Black, and W=White). Differences in this character do not affect device compatibility.

CAC Authentication

To run the Ricoh Unified Client with the CAC solution, ensure compliance with the following before installing the Ricoh Unified Client:

• CAC Authentication application is set to have first priority.
• Device heap stack is set to a minimum of 45 MB.

Configure the Device

Configure a device for external authentication

Complete the procedures in this section to use external authentication to control user access to device functions. You configure access control settings through Enhanced External Charge Unit Management in Output Manager.

How to turn off internal authentication

Turn off internal authentication before turning on Enhanced External Charge Unit Management.

1. On the MFP console, press the User Tools hard key or soft key on the Smart Operation Panel.
2. Press System Settings > Administrator Tools.
4. Press **User Authentication Management** > **Off** > **OK**.

5. On the **Administrator Tools** tab, press **Administrator Authentication Management** > **User Management** > **Off** > **OK**.

**How to turn on Enhanced External Charge Unit Management**

Turn on Enhanced External Charge Unit Management to activate the settings that control user access to device functions.

1. On the MFP console, go to a function other than **User Tools**. For example, go to the **Copy** function.

2. Enter one of the following key sequences depending on the Java platform version on the device:

<table>
<thead>
<tr>
<th>Java platform</th>
<th>Key sequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.x or earlier</td>
<td>Press <strong>Clear Modes</strong>, type 107 on the numeric keypad, and press and hold <strong>Clear/Stop</strong> for 5 seconds.</td>
</tr>
<tr>
<td>10.x</td>
<td>Press <strong>Reset</strong>, type 107 on the numeric keypad, press and hold <strong>C</strong> for 5 seconds.</td>
</tr>
<tr>
<td>11.x</td>
<td>Press <strong>Reset</strong>, type 806182 on the numeric keypad, press and hold <strong>C</strong> for 5 seconds.</td>
</tr>
</tbody>
</table>

The SP mode options appear.

3. Press **System Sp**.

   The SP mode service options appear.
4. Press SP-5XXX and page down until 5113 appears.
5. Press 5113 > 2 to show the COPY : SP-5-113-002 page.
6. Press 1: Expansion Device 1 > OK.
7. Press Exit.
8. Restart the device.

**How to configure user access to device functions**

Use Enhanced External Charge Unit Management to configure user access to device functions.

1. On the MFP console, press the User Tools hard key or soft key on the Smart Operation Panel.
2. Press System Settings > Administrator Tools.
4. Press the category functions for which you want to restrict user access.

   For example, if you press Full Color, Single Color, and Two-color and you do not press Black & White for the Copier category, users can only make black and white copies of documents.

   Do not restrict access to the Printer category options and do not restrict access to JavaTM/X in the Other Functions category. The following figure shows sample settings:

5. Press OK.
Configure a device for internal authentication

To enable authentication through the built-in login screen of the device, enable Internal Authentication at the device or partially through the Web Image Monitor application.

How to configure LDAP and user authentication at a device

This task explains how to configure LDAP and user authentication at the device.

1. Verify that external authentication is turned off as described in Select functions for access control.
2. Verify that Enhanced External Charge Unit Management functions are not selected.
   For information about configuring these functions, see Select functions for access control.
3. Configure the LDAP server required for authentication:
   a) On the MFP console, press the User Tools hard key or soft key on the Smart Operation Panel.
   b) Press System Settings > Administrator Tools.
   c) Page down and press Program / Change / Delete LDAP Server.
   d) Press Program > Change and press the LDAP server that you want to configure.
   e) Configure LDAP server settings.
   Contact your system administrator for the server settings for your environment.
   f) Press OK to return to Administrator Tools.
4. Set user authentication to the LDAP server:
   a) Press Administrator Tools.
   b) Page down and press Administrator Authentication Management.
   c) Press Administrator Authentication Management, press On next to Admin. Authentication, and press OK.
d) On the Administrator tab, press User Authentication Management > LDAP Auth.
e) Next to LDAP Servers, select the LDAP server that you configured and press Next.
f) For Copier, press None > Next.
g) Next to Other Functions, turn off Document Server, Facsimile, and Scanner, and press OK.

   This setting affects the device logon screen but not the operation of Output Manager.

6. Restart the device.

**How to configure LDAP and user authentication**

This task explains how to configure LDAP and user authentication on a workstation using the Ricoh Web Image Monitor application.

1. Log on to the Web Image Monitor.
2. Browse to the Configuration page.
3. Click LDAP Server under Device Settings.
   Internal authentication requires LDAP authentication.
4. Select the LDAP server and click Change.

5. Configure LDAP server settings.
   Contact your system administrator for the server settings for your environment.
6. Click OK and then click OK to return to the Configuration page.
7. Click Administrator Authentication Management under Device Settings.
8. For User Administrator Authentication, select On.
9. Click OK to return to the Configuration page.

10. Click User Authentication Management under Device Settings.
   - For User Authentication Management, select LDAP Authentication from the drop-down list box.
   - For LDAP authentication, select the LDAP server you configured.

11. Click OK to return to the Configuration page.

12. Restart the device.

Internal authentication and Address Book

Use the settings configured in this section as a template to create an entry in the device Address Book. A user has access to a function if it is enabled by internal authentication through the Output Manager server at login or the user
settings in the Address Book. It is recommended that you turn off the functions in the Address Book so only the server settings are active.

For existing users in the Address Book, it is recommended that you turn off the functions locally or remotely through the Web Image Monitor application. You can also delete user accounts so new accounts with correct settings are created the next time the users log in.

**Single sign-on integration**

An application participates in single sign-on (SSO) in an authority role or listener role.

In the authority role, the application provides the original login for a user and sends login information to other SSO listener applications. In the listener role, the application receives login information through SSO from the authority application.

The Ricoh ESA Unified Client can function in the authority role for the following authentication modes:

- Output Manager Authentication with Device Access Control
- OM Authentication
- Device Authentication.

As the authority, the Ricoh ESA Unified Client notifies its listeners for login and logout events.

The Ricoh ESA Unified Client can function in the listener role for the following authentication modes:

- External AAA Provider
- CAP

As a listener, the Ricoh ESA Unified Client shows a not-logged-in message rather than a login screen when no user is logged in.

**Single sign-on under AAA**

The AAA infrastructure requires a provider that can broadcast the authority login information to listeners.

![Figure 3: AAA infrastructure for single sign-on](image)

To configure the Ricoh ESA Unified Client as the AAA authority, follow these steps:

1. In Device Registration Service, select the device in the Devices pane.
2. In the Details pane, set Authentication to OM Authentication with Device Access Control or OM Authentication.
3. Set OM Enable SSO Provider to True.
4. Install the Ricoh Unified Client as described in Install the Unified Client.

When the above flag is turned on, both the Unified Client Xlet and the SSO provider servlet are installed on the device. Device actions such as Start and Stop apply to both applications.

To configure the Unified Client as a AAA listener, set Authentication to External AAA Provider. The Unified Client listens to AAA login and logout events through Output Manager or AutoStore depending on whether Enable Print Release is set to True or False.
**Single sign-on under internal authentication**

Internal authentication allows applications to participate in SSO by registering a login plug-in for the SSO authority or an event listener for a SSO listener.

![Diagram](image)

**Figure 4: Internal authentication infrastructure for single sign-on**

To configure the Ricoh ESA Unified Client as the internal login authority, set **Authentication** to **Device Authentication** in the device **Details** pane in Device Registration Service.

To configure the Ricoh ESA Unified Client as an internal listener, set **Authentication** to **CAP**.

**Configure the Ricoh ESA Unified Client**

**How to add an application**

This task explains how to create a Ricoh ESA application profile in Device Registration Service. The application profile defines the server settings for AutoStore, Output Manager, and Device Registration Service.

2. Click **Applications**.
3. Click **Add Application** on the **Applications** toolbar.
4. Type an application name. For example: **Ricoh Production**
5. Select **Ricoh ESA** from the **Application Type** drop-down list box.
6. Configure application properties as described in the following table:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AutoStore Server Address</strong></td>
<td>IP address, computer name, or DNS name of the AutoStore server.</td>
</tr>
<tr>
<td><strong>AutoStore Server Port</strong></td>
<td>Port number that the AutoStore server uses to communicate with clients. Verify that this port number matches the port that is set for the AutoStore server. The default is 8084.</td>
</tr>
<tr>
<td><strong>Output Manager Server Address</strong></td>
<td>IP address of the Output Manager database management server.</td>
</tr>
<tr>
<td><strong>Output Manager Server Port</strong></td>
<td>Port number that the Output Manager database management server uses to communicate with clients. Verify that this port number matches the port that is set for the Output Manager database management server. The default is 8068 for HTTP and 8069 for HTTPS.</td>
</tr>
<tr>
<td><strong>DRS Server Address</strong></td>
<td>IP address of the server that hosts Device Registration Service.</td>
</tr>
</tbody>
</table>
How to add a Ricoh ESA device

This task explains how to create a device profile for the Ricoh ESA Unified Client. The profile enables you to manage the Ricoh ESA Unified Client, AutoStore, Output Manager, and authentication settings on the device through Device Registration Service.

2. Click Devices.
3. Click Add Device on the Devices toolbar.
4. Type a device name.
5. Type the IP address or DNS address of the device.
   The address is specific to the device and does not appear when you configure properties for a device group.
6. Type the administrator user name for the device.
   The default is admin. The user name is not required to perform an action on the device.
7. Type the password for the administrator user name.
   By default, there is not a password and the field is empty.
8. Select the target application.
9. Configure device properties as described in the following table:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Install Password</td>
<td>Remote password for the device. Use this password to upload the Ricoh ESA</td>
</tr>
<tr>
<td></td>
<td>Unified Client Xlet to the Ricoh ESA device. The default password is ricoh.</td>
</tr>
<tr>
<td>Enable Print Release</td>
<td>Set to True to enable users to release Output Manager print jobs after logging in to the device.</td>
</tr>
<tr>
<td>Enable Scan</td>
<td>Set to True to enable users to scan documents through AutoStore.</td>
</tr>
<tr>
<td>Default Functionality</td>
<td>Select if Output Manager or AutoStore settings appear by default after users log in to the device.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Select the authentication mode that controls how users log in to the device.</td>
</tr>
<tr>
<td></td>
<td>Ricoh authentication modes provides more information on authentication modes.</td>
</tr>
<tr>
<td></td>
<td>If you select OM Authentication with Device Access Control, OM Authentication, or AutoStore Authentication and the device has a Smart Operation Panel, set SmartPanel Compatibility Mode to True.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Secure Communication</td>
<td>Set to <strong>True</strong> to enable secure socket layer (SSL) communication through HTTPS. Set to <strong>False</strong> to use unsecure communication through HTTP.</td>
</tr>
<tr>
<td>Log Level</td>
<td>Set the log level as follows:</td>
</tr>
<tr>
<td></td>
<td>• Error: Errors appear in the log file.</td>
</tr>
<tr>
<td></td>
<td>• Warning: Errors and warnings appear in the log file.</td>
</tr>
<tr>
<td></td>
<td>• Information: Errors, warnings, and information messages appear in the log file.</td>
</tr>
<tr>
<td></td>
<td>• Debug: All message types and debugging messages appear in the log file.</td>
</tr>
<tr>
<td>OM Date Format</td>
<td>Specify the format that Output Manager uses to show the date.</td>
</tr>
<tr>
<td>OM Date Time Format</td>
<td>Specify the format that Output Manager uses to show the date and time.</td>
</tr>
<tr>
<td>AS Application Name</td>
<td>Specify the name of the application that appears on the device panel.</td>
</tr>
<tr>
<td>AS Status Refresh Interval</td>
<td>Specify the refresh interval for AutoStore in seconds. The default is 60 seconds.</td>
</tr>
<tr>
<td>AS Batch Scan Timeout</td>
<td>When batch scanning mode is enabled, specifies the period of inactivity in seconds at the device panel before the Ricoh ESA Unified Client</td>
</tr>
<tr>
<td></td>
<td>sends the batch scan job to AutoStore. For example, you use the default of 60 seconds.</td>
</tr>
<tr>
<td></td>
<td>If a user scans a batch of 12 documents and leaves the device, the Ricoh ESA Unified Client sends the job to AutoStore 60 seconds after the</td>
</tr>
<tr>
<td></td>
<td>last document enters the scanner.</td>
</tr>
<tr>
<td>OM Application Timeout</td>
<td>Specify the period of inactivity in seconds at the device panel before the Ricoh ESA Unified Client automatically logs a user off the</td>
</tr>
<tr>
<td></td>
<td>device.</td>
</tr>
<tr>
<td></td>
<td>On a device that operates with a Java platform version older than 10.x, the period of inactivity starts with a key or button click when the</td>
</tr>
<tr>
<td></td>
<td>Ricoh ESA Unified Client is active on the panel.</td>
</tr>
<tr>
<td></td>
<td>On a device that operates with Java platform version 10.x or newer, the period of inactivity starts with a key or button click from any</td>
</tr>
<tr>
<td></td>
<td>application.</td>
</tr>
<tr>
<td>Display Destination Specific</td>
<td>Set to <strong>True</strong> to show print jobs for only the device that you are configuring. For example, you set the value to <strong>True</strong> for device A.</td>
</tr>
<tr>
<td>Documents Only</td>
<td>When users view print jobs at the device A panel, they see only the print jobs that they have submitted to device A. If the value is</td>
</tr>
<tr>
<td></td>
<td><strong>False</strong>, users see the print jobs that they have submitted to device A and to other destinations.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| OM Enable SSO Provider         | Set to **True** to enable single-sign-on (SSO) through a provider if users log in and log out through a device configured for Output Manager functionality. Verify that the following requirements are satisfied to enable SSO:  
  • A third-party application wants SSO through the Ricoh ESA Unified Client login.  
  • A Notable Solutions SSO provider is installed. |
| SmartPanel Compatibility Mode  | Enables authentication compatibility between the Ricoh ESA Unified Client and Ricoh devices that have a Smart Operation Panel.  
  Set the value to **True** if the device has a Smart Operation Panel and the **Authentication** value is OM Authentication with Device Access Control, OM Authentication, or AutoStore Authentication. The Ricoh ESA Unified Client shows a graphical **Logout** button because the Smart Operation Panel does not have a Logout key.  
  Set the value to **False** for Ricoh devices that do not have a Smart Operation Panel. Users log out by pressing the Logout key on the standard device panel. |

10. Click **Add Device** on the **Add Device** toolbar.

### How to import device information

This task explains how to import device information into Device Registration Service from Output Manager or a CSV file.

1. Browse to the Device Registration Service (for example, [http://10.16.37.51:9000/device](http://10.16.37.51:9000/device)).
2. Click **Devices**.
3. Click **Import** on the **Devices** toolbar and select the import method:
   
   • To import device information from the Output Manager server, select **Import from OM**.  
     Type the address of the Output Manager server, select the application profile, optionally select the device group, and click **Import from OM**. Device Registration Service only imports devices that are marked as Unified Client devices in Output Manager.  
   
   • To import device information from a CSV file, select **Import from file**.  
     Browse to the CSV file and click **Upload**.  

4. Close the **Import Results** window.
5. If necessary, edit the device properties:
   
   a) Select the device in the **Devices** pane.  
   b) Click **Edit** on the **Details** toolbar.  
   c) Update the device properties.  
   d) Click **Save** on the **Details** toolbar.
Import guidelines
This topic provides guidelines for importing Ricoh ESA device information into Device Registration Service with a comma separated values (CSV) file.

Header information
The first row in the CSV file is the header row that contains header values for device information. Header values appear in the following order: Name, IP, ApplicationProfile, DeviceGroup, Properties, InheritPropertyFromGroup, SerialNumber, Username, Password. The subsequent rows list the corresponding values for each device separated by commas. Use the same header row when importing devices for all Unified Client types.

You can omit values other than Name, IP, and ApplicationProfile. The first row must always contain the header row because the Device Registration Service uses the headers to identify imported values. If you omit a value, make sure to insert the comma.

Ricoh ESA properties
When you add a property to the file, do not include a space in the property name. The following table describes the properties that you can include in the file:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EnablePrintRelease (*)</td>
<td>Set to True to enable users to release Output Manager print jobs after logging in to the device. The default value is True.</td>
</tr>
<tr>
<td>EnableScan (*)</td>
<td>Set to True to enable users to scan documents through AutoStore. The default value is True.</td>
</tr>
<tr>
<td>DefaultFunctionality (*)</td>
<td>Specifies the default functionality for the client. Options are:</td>
</tr>
<tr>
<td></td>
<td>• Output Manager</td>
</tr>
<tr>
<td></td>
<td>• AutoStore</td>
</tr>
<tr>
<td>Authentication (*)</td>
<td>Determines the authentication mode. Options are:</td>
</tr>
<tr>
<td></td>
<td>• OM Authentication with Device Access Control</td>
</tr>
<tr>
<td></td>
<td>• OM Authentication</td>
</tr>
<tr>
<td></td>
<td>• Device Authentication</td>
</tr>
<tr>
<td></td>
<td>• AutoStore Authentication</td>
</tr>
<tr>
<td></td>
<td>• External AAA Provider</td>
</tr>
<tr>
<td></td>
<td>• CAP</td>
</tr>
</tbody>
</table>

*Ricoh authentication modes* provides more information on authentication modes.

If you select OM Authentication with Device Access Control, OM Authentication, or AutoStore Authentication and the device has a Smart Operation Panel, set SmartPanel Compatibility Mode to True.

SecureCommunication | Set to True to enable secure socket layer (SSL) communication through HTTPS. Set to False to use
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>unsecure communication through HTTP. The default value is False.</td>
<td></td>
</tr>
<tr>
<td><strong>LogLevel (</strong>)**</td>
<td>The level of logging. There are four options:</td>
</tr>
<tr>
<td></td>
<td>• Error: Errors appear in the log file.</td>
</tr>
<tr>
<td></td>
<td>• Warning: Errors and warnings appear in the log file.</td>
</tr>
<tr>
<td></td>
<td>• Information: Errors, warnings, and information messages appear in the log file.</td>
</tr>
<tr>
<td></td>
<td>• Debug: All message types and debugging messages appear in the log file.</td>
</tr>
<tr>
<td></td>
<td>The default is Debug and provides for the most detailed logging.</td>
</tr>
<tr>
<td><strong>OMDateFormat</strong></td>
<td>Specify the format that Output Manager uses to show the date.</td>
</tr>
<tr>
<td><strong>OMDateTimeFormat</strong></td>
<td>Specify the format that Output Manager uses to show the date and time.</td>
</tr>
<tr>
<td><strong>ASApplicationName</strong></td>
<td>Specify the name of the application that appears on the device panel.</td>
</tr>
<tr>
<td><strong>ASStatusRefreshInterval</strong></td>
<td>Specify the refresh interval for AutoStore in seconds. The default is 60 seconds.</td>
</tr>
<tr>
<td><strong>ASBatchScanTimeout</strong></td>
<td>When batch scanning mode is enabled, specifies the period of inactivity in seconds at the device panel before the Ricoh ESA Unified Client sends the batch scan job to AutoStore. For example, you use the default of 60 seconds. If a user scans a batch of 12 documents and leaves the device, the Ricoh ESA Unified Client sends the job to AutoStore 60 seconds after the last document enters the scanner.</td>
</tr>
<tr>
<td><strong>OMApplicationTimeout</strong></td>
<td>Specify the period of inactivity in seconds at the device panel before the Ricoh ESA Unified Client automatically logs a user off the device. The default is 300 seconds. On a device that operates with a Java platform version older than 10.x, the period of inactivity starts with a key or button click when the Ricoh ESA Unified Client is active on the panel. On a device that operates with Java platform version 10.x or newer, the period of inactivity starts with a key or button click from any application.</td>
</tr>
<tr>
<td><strong>DisplayDestinationSpecificDocumentsOnly</strong></td>
<td>Set to True to show print jobs for only the device that you are configuring. For example, you set the value to True for device A. When users view print jobs at the device A panel, they see only the print jobs that they have submitted to device A. If the value is False, users see the print jobs that they have submitted to device A and to other destinations.</td>
</tr>
</tbody>
</table>
### Property Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| **OMEnableSSOProvider** | Set to True to enable single-sign-on (SSO) through a provider if users log in and log out through a device configured for Output Manager functionality. Verify that the following requirements are satisfied to enable SSO:  
1. A third-party application wants SSO through the Ricoh Unified Client login.  
2. A Notable Solutions SSO provider is installed.  
The default is False. |
| **SmartPanelCompatibilityMode** | Enables authentication compatibility between the Ricoh ESA Unified Client and Ricoh devices that have a Smart Operation Panel.  
Set the value to True if the device has a Smart Operation Panel and the Authentication value is OM Authentication with Device Access Control, OM Authentication, or AutoStore Authentication. The Ricoh ESA Unified Client shows a graphical Logout button because the Smart Operation Panel does not have a Logout key.  
Set the value to False for Ricoh devices that do not have a Smart Operation Panel. Users log out by pressing the Logout key on the standard device panel. |

### Sample import file

The following example shows Ricoh import file entries:

<table>
<thead>
<tr>
<th>Name,</th>
<th>IP,</th>
<th>ApplicationProfile,</th>
<th>Device Group,</th>
<th>Properties,</th>
<th>InheritPropertyFromGroup,</th>
<th>SerialNumber,</th>
<th>Username,</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ricoh, 191.211.13.5, Ricoh Profile, Ricoh Group, EnablePrint Release=true~EnableScan=true, TRUE, E153M310024, admin, ricoh</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ricoh, 191.211.13.9, Ricoh Profile, Ricoh Group, EnablePrint Release=true~EnableScan=true, TRUE, E264M302574, admin, ricoh</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### How to export device information

This task explains how to export Ricoh ESA device information to a CSV file.

1. Click Devices.
2. On the Devices toolbar, click Export.

Device Registration Service exports the device information to a CSV file in the following format:

Name, IP, Application, Device Group, Property Name=Property Value, Inherit Property From Group, Serial Number, Username, Password
How to add a device group
This task explains how to create a group to organize devices in Device Registration Service. The device group is a single configuration point for managing multiple devices for an application.

1. Click Devices.
3. Enter the Name, Username and Password for the device group.
4. From the drop-down list box, select the target application.
5. Configure device group properties.
   Devices and device groups share properties. How to add a Ricoh ESA device on page 38 provides more information on the properties that you can configure.

How to add a device to a device group
This task explains how to add a device to a device group.

1. Click Devices.
   To add an existing device to a group, highlight the device and drag it to the device group.
2. Select the device group.
3. Click Add Device.
4. Type a device name and the device address.
5. Specify the property inheritance value:
   • To inherit properties from the device group, select True for Inherit Properties from Group.
   • To configure specific device properties, select False and configure the properties.

   How to add a Ricoh ESA device on page 38 provides more information on configuring device properties.
6. Click Add Device.

Ricoh authentication modes
The following table describes the authentication modes that you can use for a Ricoh ESA device or Ricoh ESA device group.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OM Authentication with Device Access Control</td>
<td>Output Manager manages authentication. Output Manager controls login and logout protocols on the device for the Notable Solutions Unified Client. All device functions such as copying and faxing are made available only after the user logs into the device. Login at the device will be by user name and password credentials or a card used that can be swiped at the device. Accounting which encompasses the tracking of the number of printing, copying, scanning and faxing jobs is enabled. Once logged in, the user can toggle between Output Manager and AutoStore if AutoStore has been installed. However, the initial application that will display upon</td>
</tr>
<tr>
<td>Mode</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>OM Authentication</strong></td>
<td>Output Manager manages authentication. Output Manager controls login and logout protocols on the device for the Ricoh ESA Unified Client only. Other device functions such as copying and faxing are not affected. The user provides user name and password login credentials at the device or swipes a card at the device. Once logged in, the user can toggle between Output Manager and AutoStore if AutoStore has been installed. The initial application that appears after login is controlled by the Default Functionality property.</td>
</tr>
<tr>
<td><strong>Device Authentication</strong></td>
<td>The device manages authentication. The internal authentication component of a device controls login and logout protocols. Output Manager controls access to the Ricoh ESA Unified Client. The user provides user name and password login credentials at the device or swipes a card at the device. Once logged in, the user can toggle between Output Manager and AutoStore. The initial application that appears after login is controlled by the Default Functionality property.</td>
</tr>
<tr>
<td><strong>AutoStore Authentication</strong></td>
<td>AutoStore manages authentication. The Ricoh ESA component in AutoStore supports Microsoft Windows, Active Directory, NetWare, and custom scripting authentication types. Once logged in, the user can toggle between AutoStore and Output Manager if Output Manager has been installed. The initial application that appears after login is controlled by the Default Functionality property. To complete AutoStore Authentication, refer to the Ricoh ESA component Help for more information.</td>
</tr>
<tr>
<td><strong>External AAA Provider</strong></td>
<td>Adaptable Authentication API (AAA) is a sign-on (SSO) infrastructure used by Ricoh to manage authentication. Output Manager or AutoStore can control access to the Ricoh ESA Unified Client. If the Enable Print Release and Enable Scan values are True and the Default Functionality value is AutoStore, AutoStore controls access to the Ricoh ESA Unified Client. If the Enable Print Release and Enable Scan values are True and the</td>
</tr>
</tbody>
</table>
© 2014 Notable Solutions, Inc.

**Mode** | **Description**
--- | ---

**Default Functionality** value is Output Manager. Output Manager controls access to the Ricoh ESA Unified Client.

Users log in at the device with a common access card (CAC). For AutoStore, other options can include third-party applications, such as Equitrac. These applications must be installed prior to using this option.

Once logged in, a user can toggle between AutoStore and Output Manager if both applications have been installed.

**CAP**

Card Authentication Package (CAP) is a card login product used by Ricoh to manage card authentication.

Output Manager or AutoStore can control access to the Ricoh ESA Unified Client. If the **Enable Print Release** and **Enable Scan** values are **True** and the **Default Functionality** value is AutoStore, AutoStore controls access to the Ricoh ESA Unified Client. If the **Enable Print Release** and **Enable Scan** values are **True** and the **Default Functionality** value is Output Manager, Output Manager controls access to the Ricoh ESA Unified Client.

Users log in at the device with CAP. CAP must be installed prior to using this mode of authentication.

Once logged in, the user can toggle between AutoStore and Output Manager if both applications have been installed.

---

**Note:** The Output Manager detailed history by device report shows entries for native copy, Output Manager print, and AutoStore scan jobs. The report does not show entries for native scan and fax jobs.

**How to perform device actions**

1. On the Device Registration Service web client, click **Devices**.
2. Select a device.
3. On the **Details** toolbar, select an action as described in the following table:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install</td>
<td>Installs the Ricoh ESA Unified Client Xlet on the device.</td>
</tr>
<tr>
<td>Uninstall</td>
<td>Uninstalls the Ricoh ESA Unified Client Xlet on the device.</td>
</tr>
<tr>
<td>Start</td>
<td>Starts the Ricoh ESA Unified Client Xlet on the device.</td>
</tr>
<tr>
<td>Stop</td>
<td>Stops the Ricoh ESA Unified Client Xlet on the device.</td>
</tr>
<tr>
<td>Install and Start</td>
<td>Installs the Ricoh ESA Unified Client Xlet on the device and then starts the Ricoh ESA Unified Client.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Update Menus</td>
<td>Updates device registration configuration and menus for the AutoStore application on the device.</td>
</tr>
<tr>
<td>Reboot</td>
<td>Reboots the device.</td>
</tr>
<tr>
<td>Install and Reboot</td>
<td>Install the Ricoh ESA Unified Client Xlet on the device and then reboots the device.</td>
</tr>
</tbody>
</table>

4. Click Perform selected action.

**How to view device information**

2. Click Devices.
3. To filter device and device group information that appears in the Devices pane, type or select criteria in the Filter pane and click Apply.
4. To view action history for a device or device group, select the device or device group in the Details pane.

The Action History pane shows the following information:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Time stamp of when the action was attempted.</td>
</tr>
<tr>
<td>Action</td>
<td>Attempted action.</td>
</tr>
<tr>
<td>Message</td>
<td>Action taken and the result.</td>
</tr>
<tr>
<td>Status</td>
<td>Status for the action.</td>
</tr>
<tr>
<td>Success</td>
<td>Indicates if the action was successful.</td>
</tr>
<tr>
<td>Device</td>
<td>Name of the device.</td>
</tr>
<tr>
<td>Address</td>
<td>IP address of the device.</td>
</tr>
<tr>
<td>Return code</td>
<td>Return code returned by the device. The values shown on the device type.</td>
</tr>
</tbody>
</table>

**Ricoh ESA return codes**

Ricoh ESA return codes appear for device actions that you perform through Device Registration Service.

The following return codes appear in the Action History.

<table>
<thead>
<tr>
<th>Return Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Xlet is not installed.</td>
</tr>
<tr>
<td>100</td>
<td>Xlet is installed.</td>
</tr>
<tr>
<td>200</td>
<td>Xlet is initializing.</td>
</tr>
<tr>
<td>300</td>
<td>Xlet has started.</td>
</tr>
</tbody>
</table>
## Configure Output Manager

This procedure provides the high-level steps for configuring Output Manager server settings for the Ricoh ESA Unified Client.

Complete the following procedure if the device **Authentication** property is set to **OM Authentication** or **OM Authentication with Device Access Control**.

1. Start the **Output Manager Console** application and log in.
2. Configure SSL settings as described in **Configure the SSL port**.
3. Configure devices as described in **Configure Output Manager devices**.
4. Configure copy quota settings as described in **Configure copy quota for users**.

### How to configure the SSL port

Follow the steps in this procedure to configure the Output Manager SSL port for the Ricoh ESA Unified Client.

1. On the Output Manager machine, select **Start > All Programs > NSi > NSi Output Manager Server > OM Server Configuration**.
2. Click the **SSL Certificate Manager** tab and configure the port for DdmInterface.

   ![SSL Certificate Manager](image)

   Click **Help** for more information on configuring SSL settings.

### How to configure Output Manager devices

This topic describes how to configure devices in the Output Manager Console.

1. On the Output Manager server, select **Start > All Programs > NSi > NSi Output Manager Console** and connect to the Output Manager server.
2. In the **Devices** application, right-click the device and select **Configure**.
3. Click the **Device Details** tab.
4. For **Embedded client type**, verify that Ricoh is selected.
5. **Configure devices for accounting**.
   If a device is configured for accounting, complete the following tasks:
   - Configure the device for external authentication.
     
     *Configure a device for external authentication* provides more information.
   - Enable Output Manager login for the Unified Client.
   - Set **Manage login** in Output Manager to External.
6. **Configure devices for access control**.
7. **Configure devices for accounting**.

**How to configure device for accounting**
This procedure describes how to configure a device for accounting.

If the **Device Configuration** dialog box for the device is not open already, follow the instructions in *Configure Output Manager devices* before continuing with this procedure.

*Note:* Accounting data for Output Manager print jobs and Ricoh ESA Unified Client scan jobs is always recorded, regardless of settings configured with this procedure.

1. In the **Device Configuration** dialog box, click the **Device Details** tab.
2. For **Cost Management**, select **Prints** or **Copies** depending on your business requirements.
3. If you selected **Copies**, specify the cost per page.

If the Ricoh ESA Unified Client is already started, restart it to implement the changes.

**How to configure device for access control**
This procedure shows how to create access control profiles for users, groups, and departments.

If **Device Configuration** dialog box for the device is not open already, follow instructions in *Configure Output Manager devices* before continuing with this procedure.

Perform these steps only if access control is required.

Access control can be configured for users, groups, and departments. If access control is not configured, a default profile with full access is provided for new users.

1. In the **Device Configuration** dialog box, click the **Device Details** tab.
2. Select **Unified client**.
3. In the **Unified Client** box, click **Configure access control**.
4. Click the appropriate tab to configure access control for **Users**, **Groups**, or **Departments**.
5. Click the browse button (…) for the user, group, or department that you want to configure.
6. In the **Manage MFP ACL Profiles** dialog box, you can create or edit ACL profiles for the selected user, group, or department.

7. Click **New** to create an MFP ACL profile.
   You do not need to restart the Unified Client to implement the changes. The changes take effect the next time users log in to the Unified Client.

**How to configure device for print preferences**

MFP Kiosk Preferences profiles make print preference available to users.

If **Device Configuration** dialog box for the device is not open already, follow instructions in *Configure Output Manager devices* before continuing with this procedure.

Perform these steps only if you want users to adjust print preferences before printing.

1. In the **Device Configuration** dialog box, click the **Device Details** tab.
2. Select **Unified client**.
3. In the **Unified Client** box, click **New**.
4. Type a name for the profile in the **Name** field.
5. Optional: Type a profile description in the **Description** field.
6. Click the arrow next to any item to expand an option group.
7. Select the check box next to a print option to add it to the **Selected items** list.

8. Click **OK**.

If the Unified Client is already started, restart it to implement the changes.

**How to configure login methods**

This procedure describes how to configure the login methods for Output Manager users.

1. Start the Output Manager console and connect to the server.
   To start the console, select **Start > NSi > NSi Output Manager Console > Output Manager Console**.
2. Click the **Administration** application.
3. In the **Administration** options, click **Set General Preferences**.
4. In the **Administration - Set General Preferences** settings, click the **Security** tab.
5. Select options in the External client login section as described in the following table:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow user name / password</td>
<td>The user can log in by entering user name, password, and selecting a domain.</td>
</tr>
<tr>
<td>Allow card swipe</td>
<td>The user can log in through a card swipe. The user must also enter a PIN if Require PIN with card swipe is selected.</td>
</tr>
<tr>
<td>Allow manual card ID entry</td>
<td>The user can log in by entering an ID. The user must also enter a pin if Require PIN with manual entry is also selected.</td>
</tr>
<tr>
<td>Allow unmasked card ID</td>
<td>The card ID will be readable as it is entered. If you clear this check box, the card ID will be masked.</td>
</tr>
<tr>
<td>Default manual login method</td>
<td>Select the default user login method:</td>
</tr>
<tr>
<td></td>
<td>• Card ID Entry</td>
</tr>
<tr>
<td></td>
<td>• User Name/Password</td>
</tr>
<tr>
<td>Require PIN with card swipe</td>
<td>Users must also enter a pin when using a card swipe.</td>
</tr>
<tr>
<td>Require PIN with card ID entry</td>
<td>Users also enter a PIN when using manual card ID entry.</td>
</tr>
</tbody>
</table>

6. Click Apply.

7. Restart Output Manager.

How to configure billing accounts
This procedure describes how to configure billing accounts and scan properties for Output Manager users.

1. Start the Output Manager Console and connect to the server.
   To start the console, click Start > NSi > NSi Output Manager Console > Output Manager Console.
2. Click the Administration application.
3. In the Administration options, click Manage Billing Accounts.
4. In the **Administration - Manage Billing Accounts** settings, you can create or edit a billing list and its billing accounts.

5. You can create secondary billing accounts under the main accounts.

6. Click the **Administration** application again, and in the **Administration** options, click **Manage Users**.

7. In **Administration - Manage Users**, select a user and click the **Device Profile** column to select or edit an existing profile or to create a new profile.

8. In a profile, you can create a single billing list, two billing lists, or one primary list and one secondary list.
How to configure copy quotas

This procedure describes how to configure the copy quota for a user.

1. Start the Output Manager Console and connect to the server.
   To start the console, click Start > NSi > NSi Output Manager Console > Output Manager Console.
2. Click the Administration application button.
3. In the Administration options, click Manage Users.
4. In the Administration - Manage Users pane, click the Balances tab.

5. For a user, select the check box in the Set Balance column, and click the browse button (...) in the Allowances Profile column to create or edit profiles.

6. Click New or Edit to set allowances for print and copy.
7. Click **OK** to save changes to the profile and then click **Close**.

8. Click the profile list the **Allowances Profile** column to assign the allowances profile to the user.

You do not need to restart the Ricoh ESA Unified Client. Users see the changes after their next login.

**Configure AutoStore**

Configure the authentication for the Ricoh ESA component to work with AutoStore or Output Manager authentication.

1. In **AutoStore Process Designer**, add the Ricoh ESA capture component to a task.
2. Double-click the component.
3. On the **Authentication** tab, select the **Authentication type** value as follows:
   - For authentication through Output Manager, select **None**.
   - For authentication through AutoStore:
     - If **Authentication** is set to **OM Authentication** in the device **Details** pane in Device Registration Service, select an authentication type that resolves login information to user names on the Output Manager server. Do not select **None**.
     - If **Authentication** is set to **AutoStore Authentication**, select any authentication type.
4. Configure settings for the selected authentication type.
   Refer to the Ricoh ESA component Help for more information.
5. Optional: Configure options required by the workflow on the other tabs.
6. Click **OK**.

**How to install the Ricoh ESA Unified Client**

Use Device Registration Service to send configuration settings to the MFD.

Before performing this procedure, configure an application profile on the **Applications** tab and specify it in a device profile on the **Devices** tab.

2. Click Devices and select the device.
3. In the Details pane, select Install or Install Start from the drop-down list box.
4. Click Perform selected action.
5. Install the Ricoh Xlet:
   a) Go to the Device Registration Service installation directory (for example, C:\Program Files (x86)\NSi\Device Registration Service\Service\Plugins\) and copy the 33956099.zip file to the desktop.
   b) Unzip the file to a temporary folder on the desktop and open the UnifiedESAXlet.dalp file in a text editor.
   c) At the bottom of the file, modify the deviceRegServer and deviceRegPort arguments for your Device Registration Service instance as shown in the following example:

   
   <argument>deviceRegServer=15.166.37.151</argument>
   <argument>deviceRegPort=8353</argument>

   d) Save the file and create an updated 33956099.zip file from the temporary folder.
   e) Replace the original 33956099.zip file in the Device Registration Service installation directory (for example, C:\Program Files (x86)\NSi\Device Registration Service\Service \Plugins\) with the updated file.

   If the arguments have the correct connection information, the Ricoh ESA Unified Client starts. Ricoh ESA Unified Client startup scenarios on page 55 contains more information on factors that may affect how the Ricoh ESA Unified Client starts.
6. Install the SSO Xlet:
   a) In the Device Registration Service Devices pane, select the device.
   b) Click Edit on the Details toolbar.
   c) Select True for OM Enable SSO Provider.
   d) Click Save.

   The system adds the 34084353.zip SSO Xlet file to the Device Registration Service installation directory (for example, C:\Program Files (x86)\NSi\Device Registration Service\Service\Plugins\). How to add a Ricoh ESA device on page 38 provides more information on the OM Enable SSO Provider option.
7. Optional: To view registrations for a device, select the device and click Refresh status on the Details toolbar.

Ricoh ESA Unified Client startup scenarios
Startup scenarios depend on the login application and if Output Manager and AutoStore are enabled and licensed.

Startup behavior depends on the following:
  • Output Manager — Licensed or unlicensed
  • AutoStore — Licensed or unlicensed
  • Output Manager — Enabled or disabled
  • AutoStore — Enabled or disabled
  • Login application — Output Manager or AutoStore
  • Default application — Output Manager or AutoStore

Ricoh ESA Unified Client Operations

Output Manager login
This section describes how to configure login settings and how to log on to Output Manager through the Ricoh ESA Unified Client.
Login settings
This topic describes settings that control the Ricoh ESA Unified Client login to Output Manager.

The Ricoh ESA Unified Client login is configured in the Output Manager Console by the External client login options (see Configure logon methods).

<table>
<thead>
<tr>
<th>External client login</th>
<th>Allow user name / password</th>
<th>Allow card swipe</th>
<th>Require PIN with card swipe</th>
<th>Allow manual card ID entry</th>
<th>Require PIN with card ID entry</th>
<th>Allow unmasked card ID</th>
<th>Default manual login method: User Name / Password</th>
</tr>
</thead>
</table>

The External client login The settings define three login methods and two PIN options:

- User name and password login.
- Card swipe login, with optional PIN.
  
  A PIN can be treated as password for a card ID.
- Manual card ID entry login, with option for a PIN.

After you change login settings on the Output Manager server, restart the Ricoh ESA Unified Client to implement the changes. Depending on the selections in the External client login settings, users see different login options at the Ricoh ESA Unified Client.

Typically, all three login methods are enabled. Depending on the default login method selected at the Output Manager server, the user sees either the user name and password login or the manual card ID entry login.

![Figure 5: User name/password login screen](image)

![Figure 6: Manual ID entry login screen](image)

A user can press Switch to switch between these to methods. If one of the methods is not enabled, the switch button does not appear. For example:
Figure 7: Manual ID entry disabled

Since the Card Swipe Login is always available, there is no need to switch to it and it cannot be specified as a default login method in the Output Manager server. When Card Swipe Login is the only method enabled, the screen prompts to swipe a card.

Figure 8: Card Swipe login only

The following screen shows when no login method is available.

Figure 9: No login method available

The user name, password, and card ID or PIN are entered using a soft keyboard.

Figure 10: Soft keyboard
When the **Allow unmasked card ID** check box is cleared, the entry is obscured as the user types characters.

**Figure 11: Soft keyboard with mask**

**User name and password entry**
This section describes options when supplying a user name and password to log in.

User name and password entry supports the following user types:

- Microsoft Windows domain
- Output Manager
- LDAP realm

The domain, Output Manager, or realm is selected in the **Domain** list box:

If the login fails, an error message shows **Invalid user name or password**:

**Manual ID entry**
This section describes options for the manual ID entry login.

Manual ID entry login prompts for both ID or server or registers an unrecognized user. By default, the manual ID login provides fields for both card ID and PIN for logging onto the server. If the PIN option is disabled, the Ricoh ESA Unified Client shows the login screen without the PIN field.
If a login fails, the Ricoh ESA Unified Client prompts the user to register an ID or PIN.

If the user presses Yes, the Ricoh ESA Unified Client prompts the user to log in to assign an ID or PIN.

If the assignment is successful, the user can use the card ID or PIN for future logins.

**Card swipe**

This topic describes options for the card swipe login.

This login type supports the following features:

- Card can be swiped when the Ricoh ESA Unified Client is not the active application on the device panel. The Ricoh ESA Unified Client performs a login in the background. This is very helpful when the Unified Client is providing SSO to other applications. The active application could log in the user after receiving the SSO notification.
- Card can be swiped when the device is in energy-saving sleep mode. The Ricoh ESA Unified Client wakes up the device and logs in the user.

If the Require PIN with card swipe option is not selected, the card swipe logs in a user with a registered card ID. If the Require PIN with card swipe option is selected, the user enters a PIN.
If a login fails, the Ricoh ESA Unified Client prompts the user to register an ID or PIN.

If the user presses **Yes**, the Ricoh ESA Unified Client prompts the user to log in to assign an ID or PIN.

If the assignment is successful, the user can use the card ID or PIN for future logins.

**AutoStore login**

The Ricoh ESA Unified Client shows an AutoStore login screen when it is configured to use the AutoStore login. The following figure shows a sample screen for the Active Directory login on AutoStore.

**Ricoh ESA Unified Client screen layout**

After a user logs in, the Ricoh ESA Unified Client shows the **AutoStore workflow** or the **Output Manager** screen. The Ricoh ESA Unified Client screen that appears depends on the settings that you configure in *How to add a Ricoh ESA device* on page 38.
Figure 12: AutoStore workflow screen (large panel)

Figure 13: AutoStore workflow screen (small panel)

Figure 14: Output Manager screen (large panel)
Figure 15: Output Manager screen (small panel)

Notes:

- The Release my print button in AutoStore does not appear if only scanning is enabled.
- The Home button in Output Manager does not appear if only printing is enabled.
- The number of jobs retrieved from the Output Manager server is limited to 40.
- Some buttons are disabled when no jobs are selected.

Advanced Output Manager operations

Billing accounts

The user can configure a billing account for each print at login or at each release.

The login billing accounts list is called Default Billing Accounts. They are recorded as part of the accounting data for Copy, Scan, Print, and Fax operations.

Figure 16: Default billing accounts

The Billing Accounts button is enabled only if Prompt for billing accounts at login is selected at the Output Manager server. This selection allows a logged in user to change the default billing accounts during a login session.

Print settings

The Ricoh ESA Unified Client can be configured to let users press the Settings on the console before releasing selected jobs.

The Ricoh ESA Unified Client shows the settings that are available and in the order they are set up in the Output Manager server.
There are three commands in the Settings screen.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save</td>
<td>Set the preferences for the jobs on the Output Manager server.</td>
</tr>
<tr>
<td>Print</td>
<td>Set the preferences and then release the jobs according to the preferences. If billing lists are assigned, the Ricoh ESA Unified Client prompts the user with billing account options as described in Billing Accounts.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Cancel the print operation.</td>
</tr>
</tbody>
</table>

**Job information**

The job information screen shows job details.

The user can select one or more jobs and press Info to view information about each job.
When multiple jobs are selected, the user can press Previous and Next to navigate the information screens for the jobs.

**Printed jobs**

The printed jobs lists show information about completed print jobs.

The user can view previously printed jobs by pressing Print Jobs.

The number of jobs retrieved is limited to 40. When the user presses Print Jobs, it changes to Unprinted Jobs. This allows users to switch from one list to the other.

**Logout**

The Ricoh ESA Unified Client supports the following logout options at the MFD:

- **Logout button**
- **Logout by card swipe**
- **Auto logout**
- **Energy Saving Mode logout**
- **Powered off logout**

**Logout button**

The user logs out by pressing Login/Logout on the device panel. The Ricoh ESA Unified Client shows the login screen after the user logs out. For 10.x and later devices, the user can press Login/Logout to log out even when the application is not the current application on the device panel.
If the Ricoh ESA Unified Client is configured for compatibility with Smart Operation Panel devices, the user can log out by pressing the graphical **Logout** button on the Smart Operation Panel display.

**Logout by card swipe**

While logged in, the user can swipe a card again to log out. This is a convenient way to log out when the application is not the current application on the panel, even for pre-10.x devices.

**Auto logout**

If the user forgets to log out, the Ricoh ESA Unified Client automatically logs out the user after the user has not been active on the MFD control panel for a specified timeout interval. The time period is specified as the number of seconds through the **OM Application Timeout** property in the device **Details** pane in Device Registration Service.

**Energy Saving Mode logout**

When the device enters Energy Saving Mode while the user is logged in, the Ricoh ESA Unified Client logs out the user before the device shuts down.

**Powered off logout**

When the device is powered off manually or through auto-power off timer, the Ricoh ESA Unified Client logs out the user before the device shuts down.

**Internal login**

When you configure the Ricoh ESA Unified Client to do internal login, it is integrated with the built-in login of a device.

**Login**

Depending on the setting for Enhanced Authentication Management, the user sees either of the following two login screens:

![Login Screen](image)

*Figure 21: Enhanced Authentication Management set to On*
In either case, the Ricoh ESA Unified Client supports both user name and password and card swipe login for a card ID already registered. A card swipe is ignored if the card ID is not already registered.

**Logout**

The user can log out by pressing **Login/Logout** on the device panel at any time, even when the Ricoh ESA Unified Client is not the active application. The device shows its login screen again after the user has logged out.

There is no automatic logout when the Ricoh ESA Unified Client is configure for internal login. The **autoLogoutTime** setting is ignored.

**Access control**

The Ricoh ESA Unified Client controls device access for the following scenarios:

- **Authentication** is set to OM Authentication with Device Access Control or Device Authentication.
- **Access control profiles** have been configured for users on the device.

**Access control under external authentication**

When external authentication is enabled, a user who is not logged in sees a screen like the following:

If the user is logged in but not permitted access in any profile, the Ricoh ESA Unified Client notifies the user of insufficient permissions.
Access control under internal authentication

When internal authentication is enabled, a user who is not logged in sees the device login screen. If the user logs in but lacks permissions to a feature, the Ricoh ESA Unified Client notifies the user of insufficient permissions.

Accounting

The Ricoh ESA Unified Client uses accounting flags to perform accounting operations. Collecting accounting data is achieved through the following actions:

- Output Manager server tracks print activity.
- Output Manager server tracks AutoStore scan activity.
- Print and native copy activities are tracked according to the accounting flags. AutoStore scan activities are also tracked.

The Ricoh ESA Unified Client records accounting data for color and black and white content as follows:

- When a user logs in at a device, the Ricoh ESA Unified Client reads the device print and copy counters. When the user logs out, the Ricoh ESA Unified Client reads the counters and records the differences since the start of the session.
- The Ricoh ESA Unified Client records data for configured billing accounts. When the user changes the billing accounts while logged in, the Ricoh ESA Unified Client records the counter differences before each change.
- For an Output Manager print job, the Output Manager server records its accounting data at the end of the job regardless of the accounting settings. The Output Manager server uses the recorded print counters to reconcile the accounting data.
- For an AutoStore scan job, the Ricoh ESA Unified Client records its accounting data at the end of the job regardless of the accounting settings.

Quota management

This topic describes how to enable quota management on a device.

Configure the following to have Output Manager to use quota management:
Enable external authentication  See *Configure a device for external authentication*
Set manageLogin to external
Set the allowance profile  See *Configure copy quota for users*

**Note:** Output Manager cannot do quota management on 2.x devices, as they do not support external authentication.

Quota is checked at login time, and during and after a copy session. After the limit is reached, the Ricoh ESA Unified Client issues a command to stop copy. The command turns off all device functions, including copy, scan, and fax. Depending on the device capabilities, it may continue copying pages before its functions are turned off. The Ricoh ESA Unified Client shows the following screen on the device:

Output Manager also issues error beeps and shows a quota reached message:

---

**Troubleshooting the Ricoh ESA Unified Client**

This topic provides information for troubleshooting problems with the Ricoh ESA Unified Client application.

**Error codes**

**Table 1: Ricoh ESA Unified Client error codes**

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>J201, J301</td>
<td>Failed security check due to:</td>
</tr>
<tr>
<td></td>
<td>• A demo signature expired.</td>
</tr>
<tr>
<td></td>
<td>• Corrupted device registry information when a device was not shut down properly.</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| J204 | Disk out of space for one of the following reasons:  
  • Failed to copy application zip file to the install directory.  
  • Cannot start in standard time due to missing file, wrong `.dalp` file format, or thread takes too long. |
| J522 | Java class reference missing for one of the following reasons:  
  • Missing library.  
  • An application exception.  
  • For a 10.x device, this can occur when installing with Web Image Monitor. You can use RxopGuiClient instead of Web Image Monitor. |

**A4 small panel scanner settings**

Typically, the MFP device automatically detects the scan settings that you configure. If the MFP device does not detect the scan settings and the device panel shows an error, map the device model code to the scanner bed value:

1. Locate the `33956099.zip` file on the server (for example, `C:\Program Files (x86)\NSi\Device Registration Service \Service\Plugins\33956099.zip`).
2. Extract the `modelinfo.properties` file from the ZIP file and open it in a text editor.
3. Configure the `modelinfo.properties` file by adding an entry for your device in the following format:
   ```properties
   Modelcode=ScanSize
   ```
4. Save your changes to the file and reinstall the Xlet.
Xerox EIP Unified Client

Overview

The Xerox Extensible Interface Platform (EIP) Unified Client is a web-based client that uses a subset of the Xerox Extensible Interface EIP Application Programming Interface (API) to merge AutoStore scan and Output Manager print functionality on Xerox MFDs.

The Xerox Unified Client consists of a web client and authentication module on the AutoStore server. A Xerox MFD connects over the network to the web client using HTTP or HTTPS.

The following figure illustrates the architecture for a system that includes the Xerox EIP Unified Client:

Web client

The web client for the Xerox Unified Client is a web site hosted by the web server embedded in either the AutoStore or Output Manager server. The ANT Galio browser navigates to this web site based on the URL that was provided during registration. The embedded web server uses the configuration settings to show and order pages. Business requirements determine if your environment uses AutoStore or Output Manager. The client provides language interfaces for Danish, Dutch, English, Finnish, French, German, Italian, Norwegian, Portuguese (Brazilian), Spanish (Latin American), and Swedish.

Configure the Xerox EIP Unified Client

How to add an application

This task explains how to create a Xerox EIP Connect application profile in Device Registration Service. The application profile defines the server settings for AutoStore, Output Manager, and Device Registration Service.

2. Click Applications.
3. Click Add Application on the Applications toolbar.
4. Type an application name.
5. Select Xerox EIP Connect from the Application Type drop-down list box.
6. Configure application properties as described in the following table:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoStore Server Address</td>
<td>The IP address, computer name, or DNS name of the machine where the AutoStore server is installed. The default is the local IP address. Important: An entry must be made when using AutoStore or both AutoStore and Output Manager.</td>
</tr>
<tr>
<td>Output Manager Server Address</td>
<td>The IP address of the machine where Output Manager server is installed. The default is the local IP address. Important: An entry must be made when using Output Manager or both AutoStore and Output Manager.</td>
</tr>
<tr>
<td>Output Manager Web Service URI</td>
<td>The URI for the Output Manager server in the following format: http://&lt;LOCAL IP ADDRESS&gt;:8068. You can specify HTTP, Net.TCP, or HTTPS protocols. Output Manager settings should be configured to support the selected protocol. Important: An entry must be made when using Output Manager or both AutoStore and Output Manager.</td>
</tr>
</tbody>
</table>
| Web Application Port           | The port number used by the web application. The default is 3241. Verify that this port number matches the port number that you specified when configuring AutoStore or Output Manager:  
  - If you use AutoStore only, you specified the port number when configuring the component in AutoStore Process Designer.  
  - If you use AutoStore and Output Manager, you specified the port number when configuring the component in AutoStore Process Designer.  
  - If you use Output Manager only, you specified the port number when configuring Server port on the Clients tab in the Set General Preferences settings of the Administration module in Output Manager. |
| Use SSL for Web Application     | Enables secure socket layer (SSL) for the web application. The default is True.                                                                                                                                 |
| Application Timeout             | The time after which the Unified Client will timeout. The default is 60 seconds.                                                                                                                                 |

7. Click Save application.
How to add a Xerox EIP device

This task explains how to create a device profile for the Xerox EIP Unified Client. The profile enables you to manage Unified Client, AutoStore, Output Manager, and authentication settings on the device through Device Registration Service.

2. Click Devices.
3. Click Add Device on the Devices toolbar.
4. Type a device name.
5. Type the IP address or DNS address of the device.
The address is specific to the device and does not appear when you configure properties for a device group.
6. Type the administrator user name for the device.
The default is admin. The user name is not required to perform an action on the device.
7. Type the password for the administrator user name.
By default, there is not a password and the field is empty.
8. Select the target application.
9. Configure device properties as described in the following table:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Name</td>
<td>The application name that appears on the device for the default application.</td>
</tr>
<tr>
<td>Enable Print</td>
<td>Enables Output Manager print functionality. The default value is False.</td>
</tr>
<tr>
<td>Display destination specific documents only</td>
<td>Enables the user to see only printing jobs that are associated with a specific destination or with a group of destinations. The default value is False.</td>
</tr>
<tr>
<td>Enable Scan</td>
<td>Enables AutoStore scan functionality. The default value is False.</td>
</tr>
<tr>
<td>SNMP GET community name</td>
<td>This is the GET community name SNMP configuration value specified on the device. Enter either public or private. The default is “public.”</td>
</tr>
<tr>
<td>SNMP SET community name</td>
<td>This is the SET community name SNMP configuration value specified on the device. Enter either public or private. The default is “private.”</td>
</tr>
<tr>
<td>Default Functionality</td>
<td>The default functionality for the client:</td>
</tr>
<tr>
<td></td>
<td>• Output Manager</td>
</tr>
<tr>
<td></td>
<td>• AutoStore</td>
</tr>
</tbody>
</table>

10. Click Add Device on the Add Device toolbar.

How to import device information

This task explains how to import device information into Device Registration Service from Output Manager or a CSV file.

2. Click Devices.
3. Click **Import** on the **Devices** toolbar and select the import method:
   - To import device information from the Output Manager server, select **Import from OM**.
     Type the address of the Output Manager server, select the application profile, optionally select the device group, and click **Import from OM**. Device Registration Service only imports devices that are marked as Unified Client devices in Output Manager.
   - To import device information from a CSV file, select **Import from file**.
     Browse to the CSV file and click **Upload**.

4. Close the **Import Results** window.

5. If necessary, edit the device properties:
   a) Select the device in the **Devices** pane.
   b) Click **Edit** on the **Details** toolbar.
   c) Update the device properties.
   d) Click **Save** on the **Details** toolbar.

**Xerox EIP import properties**

Properties that can be included in a CSV import file for a Xerox device.

- **Note:** When you select a property, the property name should not include a space in the property name. For example, **Default Functionality** should be **DefaultFunctionality**.

- **Note:** The properties marked with a * are required.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ApplicationName (*)</td>
<td>The name that appears on the device for the default application.</td>
</tr>
<tr>
<td>EnablePrintRelease (*)</td>
<td>Enables Output Manager print functionality. The default value is <strong>False</strong>.</td>
</tr>
<tr>
<td>EnableTrace (*)</td>
<td>Enables trace logging. The default value is <strong>False</strong>.</td>
</tr>
<tr>
<td>SNMPGET (*)</td>
<td>This is the GET community name SNMP configuration value specified on the device. Enter either <strong>public</strong> or <strong>private</strong>. The default is <strong>public</strong>.</td>
</tr>
<tr>
<td>SNMPSET (*)</td>
<td>This is the SET community name SNMP configuration value specified on the device. Enter either <strong>public</strong> or <strong>private</strong>. The default is <strong>private</strong>.</td>
</tr>
</tbody>
</table>

**How to export device information**

This task explains how to export Xerox EIP device information to a CSV file.

1. Click **Devices**.
2. On the **Devices** toolbar, click **Export**.

Device Registration Service exports the device information to a CSV file in the following format:

```
Name, IP, Application, Device Group, Property Name=Property Value, Inherit Property From Group, Serial Number, Username, Password
```

- **Tip:** You can use the exported CSV file as a template to import device information.
How to add a device group
This task explains how to create a group to organize devices in Device Registration Service. The device group is a single configuration point for managing multiple devices for an application.

1. Click Devices.
3. Enter the Name, Username and Password for the device group.
4. From the drop-down list box, select the target application.
5. Configure device group properties.
   Devices and device groups share properties. How to add a Xerox EIP device on page 72 provides more information on properties that you can configure.

How to add a device to a device group
This task explains how to add a device to a device group.

1. Click Devices.
   To add an existing device to a group, highlight the device and drag it to the device group.
2. Select the device group.
3. Click Add Device.
4. Type a device name and the device address.
5. Specify the property inheritance value:
   • To inherit properties from the device group, select True for Inherit Properties from Group.
   • To configure specific device properties, select False and configure the properties.
   How to add a Xerox EIP device on page 72 provides more information on configuring device properties.
6. Click Add Device.

How to perform device actions
2. Click Devices.
3. Select a device.
4. On the Details toolbar, select an action as described in the following table:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Register Unified Client</td>
<td>Registers the Unified Client on the device.</td>
</tr>
<tr>
<td>Register Authentication</td>
<td>Registers Authentication on the device.</td>
</tr>
<tr>
<td>Register Accounting</td>
<td>Registers Accounting on the device.</td>
</tr>
<tr>
<td>Unregister Unified Client</td>
<td>Deregisters the Unified Client on the device.</td>
</tr>
<tr>
<td>Unregister Authentication</td>
<td>Deregisters Authentication on the device.</td>
</tr>
<tr>
<td>Unregister Accounting</td>
<td>Deregisters Accounting on the device.</td>
</tr>
<tr>
<td>Restart</td>
<td>Restarts the device.</td>
</tr>
</tbody>
</table>

5. Click Perform selected action.
How to register the Unified Client

This task explains how to register the Xerox EIP Unified Client on the MFD.

2. Click Devices and select the device.
3. On the Details toolbar, select Register Unified Client from the drop-down list box.
4. Click Perform selected action.

Connect to Output Manager

You can configure Output Manager to use HTTP, HTTPS, or Net.TCP to connect to clients. The default is HTTP. The procedures in this section describe how to change settings to use HTTPS or Net.CFG.

How to use Net.TCP to connect to Output Manager

Follow the steps in this procedure to use Net.TCP to connect to Output Manager.

1. Browse to the Xerox web.config file (for example, C:\Program Files (x86)\NSi\AutoStore Workflow 6\ASXeroxEIPWeb20) and open it in a text editor.
2. Enclose the HTTP section in XML comment tags, which is the default protocol.
   These are the <endpoint address="http://DBMSERVER ... />
   endpoints near the end of the <client>
   element, which is usually at the end of the web.config file.
   
   Tip: Insert <!-- before the first endpoint in the section and --> after the last endpoint in the section.
3. Remove the XML comment tags from the Net.TCP section, which are the <endpoint address="net.tcp://DBMSERVER ... />
   endpoints, usually the last ones in <client>
   element.
   
   Tip: Add --> to the end of the comment line (which starts with that starts with <!-- ) before the first endpoint in the section, and remove --> from the end of the section.

   This specifies Net.TCP connections to NSi Output Manager, so now there are three ways to connect: HTTP (default), HTTPS, and Net.TCP.
4. Save the web.config file.
5. Change the URI setting for the Device Registration Service to https://IP_address:8070, where the IP_address is the IP address for the Output Manager server, and 8070 is the Net.TCP port on the server.
   To do this, change the URI section on the Applications tab of the Device Registration Service web client.
   For example, if the default setting is http://10.16.37.56:8068 (where 10.16.37.56 is the IP address of the Output Manager server and 8068 is the port used for HTTP), then for Net.TCP change it to net.tcp://10.16.37.56:8070 to specify the port for Net.TCP.

How to use HTTPS to connect to Output Manager

Follow the steps in this procedure to use HTTPS to connect to Output Manager.

1. Browse to the Xerox web.config file (for example, C:\Program Files (x86)\NSi\AutoStore Workflow 6\ASXeroxEIPWeb20) and open it in a text editor.
2. Enclose the HTTP section in XML comment tags, which is the default protocol.
   These are the <endpoint address="http://DBMSERVER ... />
   endpoints near the end of the <client>
   element, which is usually at the end of the web.config file.
   
   Tip: Insert <!-- before the first endpoint in the section and --> after the last endpoint in the section.
3. Remove the XML comment tags from the HTTPS section, which are the <endpoint address="https://DBMSERVER ... />
   elements, near the end of the <client>
   element.
   
   Tip: Add --> to the end of the comment line at the beginning of the section so it appears as <!-- use the following endpoints for HTTPS connections to Output Manager -->. Remove --> after the last element in the section.
This specifies HTTPS connections to Output Manager, so now there are two ways to connect: HTTP (default), and HTTPS.

4. Save the web.config file.

5. Change the URI setting for the Device Registration Service to https://IP_address:8069, where the IP_address is the IP address for the Output Manager server, and 8069 is the HTTPS port on the server.

   To do this, change the URI section on the Applications tab of the Device Registration Service web client.

   For example, if the default setting is http://10.16.37.56:8068 (where 10.16.37.56 is the IP address of the Output Manager server and 8068 is the port used for HTTP), then for HTTPS change it to net.tcp://10.16.37.56:8069 to specify the port for HTTPS.

6. Bind port 8069 to HTTPS connections in the Output Manager server settings.

How to view device information


2. Click Devices.

3. To filter device and device group information that appears in the Devices pane, type or select criteria in the Filter pane and click Apply.

4. To view action history for a device or device group, select the device or device group in the Details pane.

   The Action History pane shows the following information:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Time stamp of when the action was attempted.</td>
</tr>
<tr>
<td>Action</td>
<td>Attempted action.</td>
</tr>
<tr>
<td>Message</td>
<td>Action taken and the result.</td>
</tr>
<tr>
<td>Status</td>
<td>Status for the action.</td>
</tr>
<tr>
<td>Success</td>
<td>Indicates if the action was successful.</td>
</tr>
<tr>
<td>Device</td>
<td>Name of the device.</td>
</tr>
<tr>
<td>Address</td>
<td>IP address of the device.</td>
</tr>
<tr>
<td>Return code</td>
<td>Return code returned by the device. The values shown on the device type.</td>
</tr>
</tbody>
</table>

Xerox EIP return codes

Xerox EIP return codes displayed for actions that are performed in the Device Registration Service.

<table>
<thead>
<tr>
<th>Return Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>Unified Client is already registered.</td>
</tr>
<tr>
<td>101</td>
<td>Unified Client registration succeeded.</td>
</tr>
<tr>
<td>102</td>
<td>Accounting registration succeeded.</td>
</tr>
<tr>
<td>103</td>
<td>Authentication registration succeeded.</td>
</tr>
<tr>
<td>Return Code</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>104</td>
<td>Unified Client deregistration succeeded.</td>
</tr>
<tr>
<td>105</td>
<td>Accounting deregistration succeeded.</td>
</tr>
<tr>
<td>106</td>
<td>Authentication deregistration succeeded.</td>
</tr>
<tr>
<td>107</td>
<td>The device is already configured for authentication.</td>
</tr>
<tr>
<td>108</td>
<td>Unified Client, Authentication and Accounting are not registered.</td>
</tr>
<tr>
<td>109</td>
<td>Unified Client and Accounting are not registered, Authentication is registered.</td>
</tr>
<tr>
<td>110</td>
<td>Authentication and Accounting are not registered, Unified Client is registered.</td>
</tr>
<tr>
<td>111</td>
<td>Unified Client and Authentication are not registered, Accounting is registered.</td>
</tr>
<tr>
<td>112</td>
<td>Unified Client and Accounting are registered, Authentication is not registered.</td>
</tr>
<tr>
<td>113</td>
<td>Unified Client and Authentication are registered, Accounting is not registered.</td>
</tr>
<tr>
<td>114</td>
<td>Authentication and Accounting are registered, Unified Client is not registered.</td>
</tr>
<tr>
<td>115</td>
<td>Unified Client, Authentication and Accounting are registered.</td>
</tr>
<tr>
<td>500</td>
<td>Unsupported action.</td>
</tr>
<tr>
<td>501</td>
<td>Unable to get device status.</td>
</tr>
<tr>
<td>502</td>
<td>Registration failed. Enable Scan, Print or both.</td>
</tr>
<tr>
<td>503</td>
<td>Unified Client registration failed.</td>
</tr>
<tr>
<td>504</td>
<td>An exception was encountered. Please review the error log for additional details.</td>
</tr>
<tr>
<td>505</td>
<td>Accounting registration failed.</td>
</tr>
<tr>
<td>506</td>
<td>Authentication registration failed.</td>
</tr>
<tr>
<td>507</td>
<td>Authentication is not registered on this device.</td>
</tr>
<tr>
<td>508</td>
<td>Accounting deregistration failed.</td>
</tr>
<tr>
<td>509</td>
<td>Authentication deregistration failed.</td>
</tr>
<tr>
<td>Return Code</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>510</td>
<td>Unable to connect to device.</td>
</tr>
<tr>
<td>511</td>
<td>Unable to initialize communications with device.</td>
</tr>
<tr>
<td>512</td>
<td>SSL is required for authentication.</td>
</tr>
</tbody>
</table>

### Application navigation

The web client for the Xerox Unified Client is a web site hosted by the web server embedded in either the AutoStore or Output Manager server. The ANT Galio browser navigates to this web site based on the URL that was provided during registration. The embedded web server uses the configuration settings to show and order pages. Possible scenarios include configurations where either AutoStore or Output Manager is present.

### Log on to the Xerox Unified Client

You can configure AutoStore to allow users to either require or not require users to log in to the Xerox Unified Client. Output Manager always requires user credentials. The AutoStore and Output Manager documentation describes login requirements. Typically, a user enters the appropriate web address in a browser and then enters credentials on the login page.

![Output Manager login page](image)

**Figure 23: Output Manager login page**

![AutoStore login page](image)

**Figure 24: AutoStore login page**
After the user logs in, the Xerox Unified Client initially shows unprinted documents in table format. **Secure Print page** provides more information.

![Figure 25: Initial view in the Xerox Unified Client](image)

**Secure Print page**

This page first appears after a user logs in to the Xerox Unified Client.

The page initially shows unprinted print jobs for the current user. Press **View Printed Jobs** to view a list of released print jobs.

![Figure 25: Initial view in the Xerox Unified Client](image)

**Commands**

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>View Printed Jobs</strong></td>
<td>Shows a list of printed documents. The documents are in a <em>retained</em> state and may have an expiration period as configured by the Output Manager administrator.</td>
</tr>
<tr>
<td><strong>View Job Info</strong></td>
<td>Switches to a page that shows more information about selected documents. Press <strong>Done</strong> to return to the documents view.</td>
</tr>
</tbody>
</table>
### Command buttons

<table>
<thead>
<tr>
<th>Button</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Scan image" /></td>
<td>Scan image</td>
<td>Switches to the AutoStore capture component. Output Manager passes the login credentials for the current user to AutoStore. Depending on AutoStore settings, AutoStore accepts or rejects the credentials.</td>
</tr>
<tr>
<td><img src="image" alt="Print" /></td>
<td>Print</td>
<td>Switches to Output Manager.</td>
</tr>
<tr>
<td><img src="image" alt="Logout" /></td>
<td>Logout</td>
<td>Ends the Unified Client session and returns to the login screen.</td>
</tr>
<tr>
<td><img src="image" alt="Exit" /></td>
<td>Exit</td>
<td>Closes the Xerox Unified Client application.</td>
</tr>
</tbody>
</table>

### Properties page

This page shows properties for a selected print job.

Access the page by selecting print jobs on the **Secure Print** page and pressing **View Printed Jobs**. Press **Done** to return to the print jobs list.
Command buttons

<table>
<thead>
<tr>
<th>Button</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Scan image icon]</td>
<td>Scan image</td>
<td>Switches to the AutoStore capture component. Output Manager passes the login credentials for the current user to AutoStore. Depending on AutoStore settings, AutoStore accepts or rejects the credentials.</td>
</tr>
<tr>
<td>![Print icon]</td>
<td>Print</td>
<td>Switches to Output Manager.</td>
</tr>
<tr>
<td>![Logout icon]</td>
<td>Logout</td>
<td>Ends the Unified Client session and returns to the login screen.</td>
</tr>
<tr>
<td>![Exit icon]</td>
<td>Exit</td>
<td>Closes the Xerox Unified Client application.</td>
</tr>
</tbody>
</table>

Settings page

Use this page to adjust print preferences for selected documents.

Access the page by selecting print jobs on the Secure Print page and pressing Settings. Press Done to save changes and return to the print jobs list. Press Cancel to discard changes and return to the print jobs list.
Command buttons

<table>
<thead>
<tr>
<th>Button</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Scan image" /></td>
<td>Scan image</td>
<td>Switches to the AutoStore capture component. Output Manager passes the login credentials for the current user to AutoStore. Depending on AutoStore settings, AutoStore accepts or rejects the credentials.</td>
</tr>
<tr>
<td><img src="image" alt="Print" /></td>
<td>Print</td>
<td>Switches to Output Manager.</td>
</tr>
<tr>
<td><img src="image" alt="Logout" /></td>
<td>Logout</td>
<td>Ends the Unified Client session and returns to the login screen.</td>
</tr>
<tr>
<td><img src="image" alt="Exit" /></td>
<td>Exit</td>
<td>Closes the Xerox Unified Client application.</td>
</tr>
</tbody>
</table>

Authentication

The Xerox Unified Client can provide a Convenience Authentication (CA) service for Xerox MFDs. This is implemented as a web service hosted by the EWS. It allows for card reader and touch screen authentication. The credentials obtained are available to the Xerox Unified Client and other applications running on the device. On MFDs that support the Xerox Job Limits API, functional access control can also be enforced. This is where a user can be restricted from using features or functions of the MFD.
Card reader authentication

The Xerox EIP Unified Client component supports card reader authentication.

If the MFD supports card readers, you can configure card reader authentication for the Xerox EIP Unified Client. The primary reader types are proximity card readers and magnetic stripe card readers. Contact Xerox Support to determine which card readers are compatible with the MFD and if firmware upgrades are required.

You configure card reader authentication through the Administration application in the Output Manager Console. Select Set General Preferences and select the Security tab. Select Allow card swipe to enable the feature. Click Help on the Security tab for more information.


Proximity card readers require the user to pass a proximity card to initiate the authentication process. The event is communicated to the authentication service on the embedded web server along with the card ID. If a match is found, the authentication service grants access and provides information about the user such as user name and email address. If a match is not found, the user is given the opportunity to provide additional authentication data to enable a new proximity card for future use.

Magnetic stripe cards typically contain more information than a proximity card. They store data in different formats. The Xerox EIP Unified Client includes a financial card parser that allows Output Manager to identify the user or give the user the option to register the card.

Touch screen authentication

A user can authenticate at an MFD device through its touch screen console. The user presses the button on the top right of the MFD touch screen.

Press Alternate Login to continue the process manually. Depending on the Output Manager settings, the MFD might prompt the user to log in with a card ID and PIN, or with a user name and password.
## Troubleshooting Device Registration Service

The following table provides troubleshooting information for the Device Registration Service and the Device Registration Service web client:

<table>
<thead>
<tr>
<th>Description</th>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows service does not start.</td>
<td>One or more configuration settings may be invalid.</td>
<td>If the Windows service has been set to run under a network account, ensure the account has local administrator permissions. If connecting to SQL Server, click Verify under Properties to ensure the connection information is valid.</td>
</tr>
<tr>
<td>Web client reports service is down.</td>
<td>The Windows service that hosts the Web service may not have been started or was unable to start.</td>
<td>Use the NSi Device Management Configuration Tool to ensure that the Web service has been started. If the service fails to start, verify the database connection by clicking Verify in database properties. Ensure the Service Port number set in the Service tab of the NSi Device Management Configuration Tool is not in use elsewhere.</td>
</tr>
<tr>
<td>Web client reports access is denied.</td>
<td>The user does not belong to the Access Group set in the NSi Device Management Configuration Tool.</td>
<td>Add the user to the Window group set with the Access Group field on the Service tab of the configuration tool, or clear the Access Group field to allow all users.</td>
</tr>
<tr>
<td>Application does not appear in the Application drop-down list box when creating a device.</td>
<td>The application for the specific device type has not been created.</td>
<td>Create an application in the Application section of the Web client. When prompted for Application Type, select the option that matches the type of device you want to create a device for.</td>
</tr>
<tr>
<td>Importing devices reports Application Profile was not found for all rows.</td>
<td>Imported file is not in CSV format, or does not follow the expected import format.</td>
<td>Verify that the imported file is a text file in comma separated value (CSV) format with the .csv extension. If you are using Microsoft Excel, use the Save As option to save the file as a CSV file. Import headers should appear in the following order: Name, IP, ApplicationProfile, DeviceType, DeviceGroup, Properties, InheritPropertyFromGroup, SerialNumber, Username, Password. Refer to the import guidelines</td>
</tr>
<tr>
<td>Description</td>
<td>Cause</td>
<td>Solution</td>
</tr>
<tr>
<td>-------------</td>
<td>-------</td>
<td>----------</td>
</tr>
<tr>
<td>Web client does not connect to service when SSL is enabled.</td>
<td>File path to certificate is invalid, or the password is incorrect.</td>
<td>Use the NSi Device Management Configuration Tool to verify the Certificate Path and Certificate Password settings on the Security tab. Ensure that the <code>httpCfg.exe</code> utility has not been removed from under the Service folder of the Device Registration Service installation folder. <strong>Advanced</strong> With the Windows service stated, verify the certificate has been installed in the local Windows certificate store. A self-signed certificate should be found under Personal Certificates on the local machine.</td>
</tr>
<tr>
<td>Cannot connect to Web client when SSL is enabled.</td>
<td>File path to certificate is invalid, or the password is incorrect.</td>
<td>See <strong>Web client does not connect to service when SSL is enabled</strong> in this table for more information.</td>
</tr>
<tr>
<td>Web client does not load in the browser.</td>
<td>One or more configuration settings may be invalid, or the service is not started.</td>
<td>Use the NSi Device Management Configuration Tool to verify that the Client Port number set on the Service tab is not in use elsewhere. Verify that the service has been started, then use the Web client link at the bottom of the Service tab in the NSi Device Management Configuration Tool to launch the Web client.</td>
</tr>
<tr>
<td>Get an Error in Opening Window error message when starting Device Configuration Manager.</td>
<td>FIPS was enabled without clearing the SSL settings.</td>
<td>Close Device Configuration Manager and then disable FIPS. Start Device Configuration Manager, select the Security tab, clear the Enable SSL on Web Service and Enable SSL on Web Client options, and then enable FIPS.</td>
</tr>
</tbody>
</table>
Service verification

You can verify the Device Registration Service Web Service by using the DRS Service Tester utility (NSi.DeviceManagement.ServiceTester) located in the Service subfolder of the Device Registration Service installation folder (for example, C:\Program Files\NSi\Device Registration Service\Service\).

![Service Tester dialog box](image)

Figure 26: Service Tester dialog box

The utility requires the service address to verify the presence of the web server. Entering a service address and clicking the Get Device Configurations returns an Object not found error message. If the service is not available at the specified address, a communication error appears.

The Device Registration Service Web Service address for the Unified Client is:

```
http://server name or IP address:port number/DeviceManagementService/transfer
```

The Device Registration Service Web Client address formula for the Device Registration Service Web Client is:

```
http://server name, or IP address:port number/DeviceManagementService/
```

**Note:** The default port for the Device Registration Service Web Service is port 8753. You can use the Device Registration Service Configuration Tool to change the default port.

To verify the presence of the Web Service and a registered device, enter the Service Address and Device Address, and then click Get Device Configurations. A device address in this instance may be either an IP address or a server name. You can specify the host computer name for the Web Service in the Optional Device Host box. The utility uses the host name to look up the device in the Device Registration Service repository if the specified Device Address is not found. If the device is not found in the Device Registration Service repository, an Object not found message appears. If the device is found, its properties appear.