

# ENTRUST

PDF of Online Help

---

**Instant ID as a Service Software**

Software Version 5.18

July 2021

528274-001, Rev. A

## Notice

Please do not attempt to operate or repair this equipment without adequate training. Any use, operation or repair you perform that is not in accordance with the information contained in this documentation is at your own risk.

## Trademark Acknowledgments

Entrust, Sigma and the hexagon design are trademarks, registered trademarks and/or service marks of the Entrust Corporation in the United States and other countries.

Datacard is a registered trademark and service mark of Entrust Corporation in the United States and other countries.

MasterCard is a registered trademark of MasterCard International Incorporated.

Visa is a registered trademark of Visa International Service Association.

All other product names are the property of their respective owners.

## Proprietary Notice

The design and information contained in these materials are protected by US and international copyright laws.

All drawings and information herein are the property of Entrust Corporation. All unauthorized use and reproduction is prohibited.

### **Entrust Corporation**

1187 Park Place  
Minneapolis, MN 55379  
Phone: 952-933-1223  
Fax: 952-933-7971  
[www.entrust.com](http://www.entrust.com)

© 2021 Entrust Corporation. All rights reserved.

# TOC

---

<b>Welcome</b> .....	<b>9</b>
<b>User Tasks</b> .....	<b>9</b>
<b>Support</b> .....	<b>10</b>
<b>Get Started with Instant ID as a Service</b> .....	<b>10</b>
<b>Instant ID as a Service Supported languages</b> .....	<b>10</b>
<b>Accessing Instant ID as a Service Features</b> .....	<b>10</b>
<b>Session Lifetime</b> .....	<b>11</b>
<b>Logging Out</b> .....	<b>11</b>
<b>About Account Entitlements</b> .....	<b>11</b>
<b>Entitlement Bundles</b> .....	<b>12</b>
<b>How Issuance Works</b> .....	<b>12</b>
<b>Issuance Process</b> .....	<b>12</b>
<b>Issuance User Types</b> .....	<b>12</b>
<b>Issuance Administrator</b> .....	<b>12</b>
<b>Issuance Designer</b> .....	<b>13</b>
<b>Issuance Operator</b> .....	<b>13</b>
<b>Issuance Supervisor</b> .....	<b>13</b>
<b>Applicant</b> .....	<b>13</b>
<b>Objects</b> .....	<b>13</b>
<b>Credential Designs</b> .....	<b>14</b>
<b>Enrollment Design</b> .....	<b>14</b>
<b>Enrollment Forms</b> .....	<b>14</b>
<b>Enrollment Records</b> .....	<b>14</b>
<b>Credentials</b> .....	<b>15</b>
<b>Mobile Flash Passes</b> .....	<b>15</b>
<b>My Profile</b> .....	<b>15</b>
<b>My Activity</b> .....	<b>15</b>
<b>Authentication Successes / Failures past 6 months</b> .....	<b>15</b>
<b>Activity Reports Table</b> .....	<b>16</b>
<b>Set the number of rows you see</b> .....	<b>16</b>
<b>Filter the information</b> .....	<b>16</b>
<b>Export activity reports</b> .....	<b>16</b>
<b>Instant ID as a Service Dashboard</b> .....	<b>16</b>
<b>Features of the Dashboard page</b> .....	<b>17</b>
<b>View and Export Audit Logs</b> .....	<b>17</b>
<b>View Audit Events</b> .....	<b>18</b>
<b>View a Specific Audit Event</b> .....	<b>18</b>
<b>View Audit Logs for Specific Users</b> .....	<b>18</b>
<b>Filter Audit Events</b> .....	<b>19</b>
<b>Export Audit Events</b> .....	<b>19</b>
<b>Set Up Your Issuance Account</b> .....	<b>19</b>

---

<b>User Tasks</b> .....	20
<b>Issuance Administrator Tasks</b> .....	20
<b>Issuance Designer Tasks</b> .....	20
<b>Issuance Operator Tasks</b> .....	20
<b>Issuance Supervisor Tasks</b> .....	21
<b>Customize Your Account</b> .....	21
<b>Customize Your Account Appearance</b> .....	21
<b>Customize Email Templates</b> .....	22
<b>Template Fields</b> .....	23
<b>Designer</b> .....	<b>25</b>
<b>Credential Design</b> .....	25
<b>Design a Credential</b> .....	25
<b>Add and Configure Graphics</b> .....	27
<b>Add and Configure Personal Information Fields</b> .....	29
<b>Configure Photograph Capture</b> .....	31
<b>Add and Configure Signature Field</b> .....	31
<b>Enable and Configure Topcoat</b> .....	32
<b>Configure UV Printing</b> .....	33
<b>Enable and Configure Embossing</b> .....	34
<b>Enable and Configure Bar Codes</b> .....	35
<b>Enable and Configure Magnetic Stripe</b> .....	36
<b>Add and Configure the Magnetic Stripe Field</b> .....	36
<b>Connect Fields to Magnetic Stripe Tracks</b> .....	37
<b>Create a New Credential</b> .....	37
<b>Edit Credentials</b> .....	37
<b>Edit Field Properties</b> .....	38
<b>Text Field Properties</b> .....	38
<b>Static Text Properties</b> .....	38
<b>Photograph Field Properties</b> .....	39
<b>Static Graphic Properties</b> .....	40
<b>Date Field Properties</b> .....	40
<b>Signature Field Properties</b> .....	40
<b>Barcode Field Properties</b> .....	41
<b>Rectangle Properties</b> .....	42
<b>Magnetic Stripe Field Properties</b> .....	42
<b>Magnetic Stripe Track Types</b> .....	42
<b>Track Type IAT</b> .....	43
<b>Manage Layers</b> .....	44
<b>Layer Properties</b> .....	44
<b>Open Layer Properties</b> .....	44
<b>Layer Properties</b> .....	44
<b>Background Layer</b> .....	44
<b>Configure Background Layer Properties</b> .....	45
<b>Color Layer</b> .....	45

---

<b>Black Layer</b> .....	45
<b>Emboss/Indent Layer</b> .....	46
<b>Configure Emboss/Indent Layer Properties</b> .....	46
<b>Non-Printable Area Layer</b> .....	46
<b>Durability and Security</b> .....	46
<b>Laminate Layer</b> .....	<b>48</b>
<b>Topcoat/RTM Layer</b> .....	<b>49</b>
<b>UV Luster Layer</b> .....	<b>50</b>
<b>Configure Credential Settings</b> .....	50
<b>Enable Tactile Impression</b> .....	50
<b>Configure the Credential Designer</b> .....	51
<b>Print a Sample Credential</b> .....	52
<b>Enrollment Designs</b> .....	52
<b>Generate a New Enrollment Design</b> .....	52
<b>Generate an Enrollment Design</b> .....	53
<b>Copy an Enrollment Design</b> .....	53
<b>Design Enrollments</b> .....	54
<b>Enrollment Appearance</b> .....	55
<b>Add the Enrollment Design Name</b> .....	56
<b>Edit the Enrollment Design Name</b> .....	56
<b>Enrollment Design Fields</b> .....	56
<b>Add Fields</b> .....	57
<b>Edit Fields</b> .....	57
<b>Move a Field</b> .....	58
<b>Cut and Paste a Field</b> .....	58
<b>Delete Fields</b> .....	59
<b>Configure Text Fields</b> .....	59
<b>Configure Date Fields</b> .....	60
<b>Configure Photo Fields</b> .....	62
<b>Capture Options</b> .....	63
<b>Auto Crop Example</b> .....	64
<b>Configure Signature Fields</b> .....	64
<b>Add or Configure Enrollment Design Steps</b> .....	65
<b>Add Steps</b> .....	65
<b>Edit Steps</b> .....	66
<b>Reorder Steps</b> .....	66
<b>Cut and Paste a Step</b> .....	66
<b>Delete Steps</b> .....	67
<b>Configure the Job Name Identifier</b> .....	67
<b>Configure Enrollment Design Settings</b> .....	68
<b>Set or Change the Tab Order</b> .....	68
<b>Add a Description</b> .....	68
<b>Configure Enrollment Search Settings</b> .....	68
<b>Design Mobile Flash Passes</b> .....	69

---

<b>Mobile Flash Pass Process</b> .....	69
<b>Create a Mobile Flash Pass Design</b> .....	69
<b>Map Fields to Mobile Flash Pass</b> .....	71
<b>Field Connections</b> .....	72
<b>Edit Credential Design Field Connections</b> .....	72
<b>Configure Mobile Flash Pass Field Connections</b> .....	73
<b>Operator</b> .....	<b>74</b>
<b>The Enrollment Process</b> .....	74
<b>1. Enter Applicant Information</b> .....	74
<b>2. Capture a Photograph</b> .....	74
<b>3. Capture Signature</b> .....	75
<b>4. Finalize and Issue Credentials</b> .....	75
<b>Enroll Applicants</b> .....	75
<b>Enter Applicant Information</b> .....	76
<b>Capture a Photograph</b> .....	77
<b>Take a Photograph Using a Web Camera</b> .....	77
<b>Upload a Photograph of the Applicant</b> .....	78
<b>Capture a Signature</b> .....	78
<b>Capture a Signature from the Applicant</b> .....	78
<b>Upload a Signature Image</b> .....	79
<b>Issue Mobile Flash Passes</b> .....	79
<b>Requirements for the Applicants</b> .....	79
<b>Issue a Mobile Flash Pass</b> .....	80
<b>Finalize and Issue Credentials</b> .....	80
<b>Manage Enrollment Records</b> .....	80
<b>Search Enrollments</b> .....	80
<b>Edit Enrollment</b> .....	81
<b>Print From Enrollment Search</b> .....	81
<b>Print a Credential</b> .....	81
<b>Print Multiple Credentials</b> .....	82
<b>Delete Enrollment Records</b> .....	82
<b>Delete an Enrollment Record</b> .....	82
<b>Delete Multiple Enrollment Records</b> .....	82
<b>Send Mobile Flash Pass Email</b> .....	83
<b>Related links:</b> .....	83
<b>Manage the Print Queue</b> .....	83
<b>Printer Statuses</b> .....	83
<b>View Print Jobs</b> .....	84
<b>Delete Print Jobs</b> .....	84
<b>Administrator</b> .....	<b>85</b>
<b>Manage Authenticators</b> .....	85
<b>Authenticator Lockout Behavior</b> .....	85
<b>Assigning User Authenticators</b> .....	86
<b>Manage General Authenticator Settings</b> .....	86

---

Manage General Settings .....	86
Manage One Time Password (OTP) Settings .....	88
Modify OTP Authenticator Settings .....	88
Manage Temporary Access Codes .....	89
Prerequisites for Using Temporary Access Code .....	89
Modify Temporary Access Code Settings .....	90
Assign a Temporary Access Code .....	90
Manage Password Settings .....	91
Manage Password Settings .....	91
Modify the Password Settings .....	92
Set Blacklisted Passwords .....	94
Set Password Reset Settings .....	94
Assign a Password Authenticator .....	95
Self-Assign a Password Authenticator .....	96
View, Edit, Delete Password Authenticators .....	97
View, Update, and Delete a Password Authenticator .....	97
Reset a Password .....	97
Reset a Password Using a Link .....	98
Reset your User Password .....	98
Assign an Instant ID as a Service Password Authenticator .....	98
Manage Entrust Soft Token .....	99
Modify Entrust Soft Token Authenticators .....	99
Assign Entrust Soft Tokens to Users .....	100
Activate an Entrust Soft Token for a User .....	101
Add and Activate an Entrust Soft Token .....	101
Activate Using a Link in an Email .....	101
Activate Using a QR Code if You Have an Email .....	102
Activate Using a QR Code if You do not Have an Email .....	102
Activate an Entrust Soft Token Manually .....	103
Unlock and Disable a Entrust Soft Token .....	104
Unlock Your Entrust ST Authenticator .....	104
Enable or Disable a Soft Token .....	104
Manage Resources .....	105
Add an Issuance API .....	105
Add Administration API to Instant ID as a Service .....	105
Integrate Splunk SIEM with Instant ID as a Service .....	107
Add Splunk Add-on to Instant ID as a Service .....	107
Add IntelliTrust Add-on to Splunk .....	107
Manage Resource Rules .....	108
Create a Resource Rule .....	110
Edit Resource Rules .....	111
Edit a Resource Rule .....	111
Delete a Resource Rule .....	111
Enable or Disable a Resource Rule .....	111

---

<b>Manage Reports</b> .....	111
<b>View Archives and Reports</b> .....	112
<b>Filter Archives and Reports</b> .....	112
<b>Delete Reports</b> .....	112
<b>Manage Users</b> .....	113
<b>Create and Manage Groups</b> .....	113
<b>Create a Group</b> .....	113
<b>Edit a Group Name</b> .....	113
<b>Delete a Group</b> .....	114
<b>Create and Manage Roles</b> .....	114
<b>Create a Custom Role</b> .....	114
<b>Clone a Role</b> .....	115
<b>Edit a Custom Role</b> .....	116
<b>Delete a Custom Role</b> .....	116
<b>System Entities</b> .....	116
<b>Create and Manage User Attributes</b> .....	117
<b>Edit a System User Attribute Setting</b> .....	118
<b>Edit a system attribute</b> .....	118
<b>Add a Custom User Attribute</b> .....	118
<b>Edit a Custom User Attribute</b> .....	119
<b>Delete a Custom User Attribute</b> .....	119
<b>Create and Manage Users</b> .....	119
<b>Add Users</b> .....	119
<b>View, Search, and Export Users</b> .....	120
<b>View Users</b> .....	120
<b>Filter or Search for Users</b> .....	121
<b>Export a User List</b> .....	121
<b>Edit, Delete, Disable, and Unlock Users</b> .....	121
<b>Editing a User Profile</b> .....	121
<b>Edit a user profile</b> .....	122
<b>Deleting Users</b> .....	122
<b>Unlocking a User</b> .....	122
<b>Disable/Enable a User</b> .....	122
<b>Enable Password Authenticator</b> .....	123
<b>Printer Management</b> .....	123
<b>Enable Cloud Printing</b> .....	124
<b>Connect the Printer to the Internet</b> .....	124
<b>Configure CD and SD Printers for Cloud Printing</b> .....	124
<b>Enable Cloud Printing Using the LCD Menu</b> .....	125
<b>Enable Cloud Printing Using the Printer Dashboard</b> .....	125
<b>Next Steps</b> .....	126
<b>Add Printers</b> .....	126
<b>Next Steps:</b> .....	126
<b>Print a Test Card</b> .....	126



---

<b>Manage Printers</b> .....	127
<b>Edit a Printer</b> .....	127
<b>Delete a Printer</b> .....	127
<b>Open the Printer Dashboard</b> .....	127
<b>View Printers</b> .....	127
<b>Filter Printers</b> .....	128
<b>Troubleshoot Printing Issues</b> .....	128
<b>Adding the Printer Fails</b> .....	128
<b>The Printer Fails to Print a Card</b> .....	129
<b>The Printer is no Longer Visible in Instant ID as a Service</b> .....	129
<b>Enable Alexa Voice</b> .....	130
<b>Support Notes</b> .....	130
<b>Setup Alexa Voice for a Printer</b> .....	130
<b>Common Phrases</b> .....	130
<b>Check Printer Status</b> .....	130
<b>Get the Printer Serial Number</b> .....	131
<b>Check Firmware Version</b> .....	131
<b>Check Part Numbers</b> .....	131
<b>Check Cleaning Status</b> .....	131
<b>Supply Commands</b> .....	131
<b>Check Ribbon Supply Level</b> .....	131
<b>Check Laminator Supply Level</b> .....	131
<b>Maintenance Commands</b> .....	131
<b>Look Up Error Codes</b> .....	131
<b>Read the Error Code</b> .....	132
<b>Print a Cleaning Card</b> .....	132
<b>Print a Test Card</b> .....	132
<b>Manage Printer Settings</b> .....	132
<b>Open Printer Dashboard</b> .....	132
<b>Printer Information</b> .....	132
<b>Printer Status Message</b> .....	133
<b>View Device Details</b> .....	133
<b>Run a Cleaning Card</b> .....	133
<b>Manage Supplies</b> .....	134
<b>View Supply Details</b> .....	134
<b>Order Supplies</b> .....	134
<b>Printer Firmware Update</b> .....	135
<b>Check for a Firmware Update</b> .....	135
<b>Update Printer Firmware</b> .....	135
<b>Firmware Status Icon Colors</b> .....	135
<b>Change the LED Color</b> .....	135
<b>Enable Quiet Mode</b> .....	136
<b>Import Enrollment Records</b> .....	136
<b>Create an Enrollment Design</b> .....	136

---

<b>Prepare the ZIP Import File</b> .....	137
<b>Prepare Photographs</b> .....	137
<b>Prepare Signatures</b> .....	137
<b>Prepare the Import File</b> .....	138
<b>Prepare the ZIP File</b> .....	138
<b>Import Enrollment Records</b> .....	139
<b>Troubleshoot Import</b> .....	139
<b>Download and Review the Logs File</b> .....	139
<b>Solutions to Import Issues</b> .....	140
<b>The Credential Name Does Not Match</b> .....	140
<b>The Import File Does Not Contain a Credential Column</b> .....	140
<b>Columns in the Import File Do Not Match Fields on the Credential</b> <b>Design</b> .....	140
<b>The Credential Column Name is Incorrect</b> .....	141
<b>Configure and Enable Mobile Flash Pass</b> .....	141
<b>Setup Accounts for Mobile Flash Pass</b> .....	141
<b>Apple Developer Account</b> .....	141
<b>Google Developer Account</b> .....	142
<b>Enable Mobile Flash Pass</b> .....	143
<b>Enable Mobile Flash Pass for Apple Wallet</b> .....	143
<b>Enable Mobile Flash Pass for Google Pay</b> .....	144
<b>Supervisor</b> .....	<b>145</b>
<b>View the Issuance Dashboard</b> .....	145
<b>Monitor Printing</b> .....	145
<b>View Credential Designs</b> .....	146
<b>View Enrollment Records</b> .....	146
<b>Manage the Print Queue</b> .....	146
<b>Printer Statuses</b> .....	147
<b>View Print Jobs</b> .....	147
<b>Delete Print Jobs</b> .....	147

# Welcome

Welcome to the Adaptive Issuance™ Instant ID as a Service Administrator Help. Instant ID as a Service provides tools to design credentials, customize the enrollment process, enroll applicants, and print credentials. It also manages card printers and users. The following is a typical workflow for creating and issuing credentials:

1. "Manage Users" on page 113
2. "Printer Management" on page 123
3. "Design a Credential" on page 25
4. "Design Enrollments" on page 54
5. "Enroll Applicants" on page 75
6. "Manage Enrollment Records" on page 80

## User Tasks

Instant ID as a Service users perform the following tasks. Each user type performs different tasks but a user can perform the tasks of multiple user types.

User Tasks:

### Issuance Administrator

Creates additional users, manages resources, and configures printers.

- "Manage Authenticators" on page 85
- "Manage Resources" on page 105
- "Manage Reports" on page 111
- "Manage Users" on page 113
- "Printer Management" on

### Issuance Designer

Creates credential designs, manages enrollment designs, and tests the enrollment process.

- "Design a Credential" on page 25
- "Edit Credentials" on page 37
- "Print a Sample Credential" on page 52
- "Design Enrollments" on page 54
- "Design Mobile Flash Passes" on page 69

### Issuance Operator-Issuance Supervisor

Enrolls applicants and issues credentials.

- "The Enrollment Process" on page 74
- "Enroll Applicants" on page 75
- "Manage Enrollment Records" on page 80
- "Monitor Printing" on page 145

Monitors printers, reviews credential designs, and monitors enrollments.

- "View the Issuance Dashboard" on page 145
- "Monitor Printing" on page 145
- "View Credential Designs" on page 146
- "View Enrollment Records" on

Issuance Administrator

- page 123
- "Design a Credential" on page 25
- "Enroll Applicants" on page 75

Issuance Designer

Issuance Operator Issuance Supervisor

page 146

## Support

Contact your Managed Service Providers for support.

Date: March 2021

Copyright © 2021 Entrust Corporation. All rights reserved.



**ENTRUST**

SECURING A WORLD IN MOTION

## Get Started with Instant ID as a Service

Once you log in to Instant ID as a Service, your role determines the Instant ID as a Service features available to you. For more information about roles, refer to "How Issuance Works" on page 12.

### Instant ID as a Service Supported languages

Instant ID as a Service is available in English only.

### Accessing Instant ID as a Service Features

The pages and features present change based on the user type and permissions. Below is a list of the expected behavior for each user type based on the default permissions.

- Issuance Administrators view the Dashboard page after logging in and have access to all the Issuance functionality. For more information, refer to "Administrator" on page 85.
- Issuance Operators are logged in to the My Profile page and have access to the Printers, Credential Designs, and Credentials pages. For more information, refer to "Operator" on page 74.
- Issuance Designers view the Dashboard after logging in. They have access to the Dashboard, Printers, Credential Designs, and Credentials pages. For more information, refer to "Designer" on page 25.
- Issuance Supervisors view the Dashboard after logging in. They have access to the Dashboard, Printers, Credential Designs, and Credentials pages. For more information, refer to "Supervisor" on page 145.

## Session Lifetime

Once you log in, your session expires after a period of inactivity and you are automatically logged out of Instant ID as a Service. By default, Instant ID as a Service logs users out after 15 minutes. A warning appears before your session times out. If you see a Warning prompt, click **Continue** to avoid being logged out of your account. Issuance Administrators can change the default time out session. Refer to "Manage General Authenticator Settings" on page 86.

## Logging Out

You are logged out of Instant ID as a Service when one of the following occurs:

- Your session lifetime expires
- You explicitly log out
- Your web browser session ends (typically when you close the browser)

**Note:** On MacOS, quit the browser in order or the session to be terminated.

## About Account Entitlements

Entitlements are the number of users and credentials allowed for an Adaptive Issuance Instant ID as a Service Help tenant. The number of credentials and users is set by the entitlement bundle. For more information on tenants, refer to the *Service Provider Online Help*.

## Entitlement Bundles

Entitlement bundles set default entitlement settings and control access to features in Instant ID as a Service. The Essentials bundle includes limited access to features and Advanced includes access to all features.

- **Essentials:**

The Essentials bundle includes the basic level of features for designing and issuing credentials. It limits users to create 15 users and 15 credential designs.

- **Advanced:**

The Advanced bundle includes all features for designing and issuing credentials. Tenets must have the Advanced bundle to configure magnetic stripe on a credential design. It does not limit the number of credentials designs or the number of users.

## How Issuance Works

Issuance is the process by which information is gathered from an applicant and that information is presented with a credential.

### Issuance Process

The issuance includes designing and issuing credentials. Typically, credentials are used to identify members of an organization and can allow access to areas or buildings. The following is a basic description of the issuance process.

1. Administrator creates users.
2. Designer creates a credential design.
3. Designer customizes an enrollment design.
4. Operator enrolls applicants and prints credentials.

### Issuance User Types

The descriptions of the user types below are based on the default permissions assigned to the roles. Modifying the roles and permissions changes the tasks a user is allowed to perform.

#### Issuance Administrator

Administrator users are responsible for preparing Instant ID as a Service for use in production. Users with Administrator-level permissions are able to perform all tasks in Instant ID as a Service. Administrator users have the permissions to perform tasks identified as

operator, supervisor, or designer tasks. Administrator users manage users, authenticators, and resources. They also add and manage printers to enable printing credentials.

For more information and instructions, refer to "Administrator" on page 85.

### **Issuance Designer**

Designer users design credentials and design and customize enrollment designs. They ensure that the credential designs and enrollment designs contain all of the fields needed to enroll applicants.

For more information and instructions, refer to "Designer" on page 25.

### **Issuance Operator**

Operator users enroll applicants and issue credentials using enrollment forms. They work directly with the applicant to prepare them for the enrollment process. They gather all of the information needed from the applicant then enter it into the enrollment form. They also capture an image of the applicant and their signature.

For more information and instructions, refer to "Operator" on page 74.

### **Issuance Supervisor**

Supervisor users monitor the enrollment process and issued credentials to ensure that the process is working correctly.

For more information and instructions, refer to "Supervisor" on page 145.

### **Applicant**

Applicants are the people being enrolled into the system. They work with the operator to enter information into the enrollment form and produce a photograph and signature depending on the requirements of the credential design and enrollment form. After enrollment is complete, the applicant receives a credential and Instant ID as a Service creates an enrollment record for the applicant.

### **Objects**

Instant ID as a Service uses the objects described in this section to manage and issue credentials.

## **Credential Designs**

Credential designs set the appearance of a credential and configures fields. The Credential Designer provides the tools to customize and configure credential designs. Credential designs contain static fields like text and images. They also contain dynamic fields like date fields and text fields for user information. After creating a credential design, the Designer user can generate an enrollment form from the credential design, or can create an enrollment form separately and link the new enrollment form fields with a new or existing credential design (refer to "Field Connections" on page 72 for more information). For instructions on creating credential designs, refer to "Design a Credential" on page 25.

## **Enrollment Design**

After creating a credential design, an enrollment design is generated or created separately. The Enrollment designs contain fields that are connected to fields on the corresponding credential design. These fields are organized into steps. If the enrollment design is generated by Instant ID as a Service, the application links the credential design and the enrollment design fields. If an enrollment design is created separately, the fields must be manually linked (refer to "Field Connections" on page 72 for more information). Using the Enrollment Designer you can create or customize the appearance of the enrollment form, the fields, and the steps.

For instructions, refer to "Design Enrollments" on page 54.

## **Enrollment Forms**

Operators use the enrollment form to record data from the Applicant. Instant ID as a Service presents enrollment forms in the Create Enrollment wizard. Operator users enter data into the enrollment form. After completing the enrollment form and printing and saving, Instant ID as a Service issues a credential and creates an enrollment record.

For instructions on completing an enrollment form, refer to "Enroll Applicants" on page 75.

## **Enrollment Records**

After completing an enrollment form, Instant ID as a Service saves an enrollment record. Enrollment records contain all of the information gathered during enrollment. Instant ID as a Service presents enrollment records in the Search Enrollment page.

For instructions on managing enrollment records, refer to "Manage Enrollment Records" on page 80.



## Credentials

After completing the enrollment form, Instant ID as a Service also creates a credential. A credential identifies the applicant possibly using an image of the applicant and personal information. Instant ID as a Service is able to issue physical credentials by printing a card using a supported printer or a digital credential called a Mobile Flash Pass.

### Mobile Flash Passes

Mobile Flash Passes are digital credentials that identify applicants using their smart phone. After creating a credential design, Instant ID as a Service provides the option to generate a Mobile Flash Pass for the applicant. The Applicant receives an email with instructions to add the Mobile Flash Pass to their Apple Wallet or Google Pay applications.

For instructions on configuring Mobile Flash Pass, refer to "Design Mobile Flash Passes" on page 69.

## My Profile

The **My Profile** page contains the following tabs, based on your administrative privileges:

- **Authenticators**

Click the **Authenticators** tab to manage the authenticators used to access your Instant ID as a Service account. For more information, refer to "Manage Authenticators" on page 85.

- **Profile**

Click the **Profile** tab to view your profile information, you cannot make changes to your profile information. If your profile information has changed contact your the Issuance Administrator. Only the Issuance Administrators can update your profile.

## My Activity

Instant ID as a Service allows you to monitor your authentication activity. There are two sections on the page: Authentication Successes/Failures past 6 months.

### Authentication Successes / Failures past 6 months

This chart shows your authentication track record over the past six months by month.

**Tip:** Hover over a graph to see the number of successes and failures for the month.

## Activity Reports Table



This table provides detailed information on all authentication transactions you have performed as a user over the past five months. You can do the following with the information in the table:

- Set the number of rows you see
- Filter the information
- Export activity reports

### Set the number of rows you see

1. Scroll to the bottom of the page.
2. From the **Rows per page** drop-down list, select the number of rows to display on the page.
3. To move to a new page, on the right-hand side of the page, do the following, as required:
  - Click > to go to the next page.
  - Click < to go to the previous page.
  - Click |< to go to the first page.
  - Click >| to go to the last page.

### Filter the information

1. Click Search  to enable filtering.
2. The **Filters** dialog box appears.
3. Select your filter options and click **Apply**. Instant ID as a Service displays the filter results.
4. To clear the filter, click Search  again.
5. On the **Filters** dialog box, click **Reset**.

### Export activity reports


Click Export  to export a report of your user activity.

Your authentication activity report is downloaded to your Downloads folder as a .CSV file.

## Instant ID as a Service Dashboard

By default, if you are an Issuance Administrator, you see the Dashboard after you log in to your Instant ID as a Service account. The Dashboard allows you to monitor account activity.

## Features of the Dashboard page

- To access the Dashboard page, select **Dashboard** from the Main Menu .
- The Dashboard includes the Getting Started area that shows the process for setting up Instant ID as a Service for issuing credentials. Click on an icon to navigate to the page containing the options to setup the issuance process.



**Step 1. Setup Printer** Click to go to the Printers page to Setup a Printer. For instructions, refer to "Printer Management" on page 123.



**Step 2. Design a Credential** Click to go to the Credential Designs page to design a credential. For instructions, refer to "Design a Credential" on page 25.

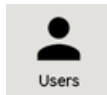


**Step 3. Enroll an Applicant** Click to go to the Credentials page to enroll applicants. For instructions, refer to "Enroll Applicants" on page 75.

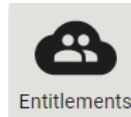


**Step 4. Issue a Credential** Click to go to the Enrollment Search page to issue a credential to an applicant. For instructions, refer to "Manage Enrollment Records" on page 80.

- The Dashboard includes the following quick access buttons:



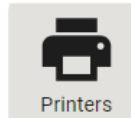
**Users** Click to go to the Users List page.



**Entitlements** Shows you the number of available Entitlements.



**Applications** Click to go to the Applications List page.



**Printers** Click to go to the Printer List page.

- The Audit Log pane lists the audit event logs. Refer to "View and Export Audit Logs" below for more information on audit logs.
- The System Alerts pane provides details of system issues, such as if a custom email server is unreachable. This pane appears only if there is a system issue.

## View and Export Audit Logs


From the **Dashboard** page you can view and export audit logs.

- **Authentication** audit logs track authentications made to your Instant ID as a Service account by location, user, and authentication type.
- **Issuance** audit logs track issuance requests, such as print requests and completion results.


- **Management** audit logs track actions performed in your Instant ID as a Service account by action and user.

Click the following options for instructions on viewing and exporting audit logs:


### **View Audit Events**

1. Click Main Menu  > **Dashboard**. The Dashboard opens.
2. Click the **Authentication**, **Issuance**, or **Management** radio button to set the type of audit log to view.
3. Set the number of audits on a page:
  - a. Scroll to the bottom of the page.
  - b. From the **Rows per page** drop-down list, select the number of rows to display on the page.
  - c. To move to a new page, on the right-hand side of the page, do the following, as required:
    - Click > to go to the next page
    - Click < to go to the previous page
    - Click |< to go to the first page
    - Click >| to go to the last page




### **View a Specific Audit Event**

1. Click Main Menu  > **Dashboard**. The Dashboard page appears.
2. Click the **Authentication**, **Issuance**, or **Management** radio button to set the type of audit log you want to view.
3. Click the row for the specific audit log you want to view. The Audit Event page opens.
4. Click **OK**.



### **View Audit Logs for Specific Users**

1. Click Main Menu  > **Members** > **Users**. The Users List page opens.
2. Click the **UserID** of the user. The User Details page opens .
3. Click the **Audits** tab. The list of audits appears.
4. Click the row for the specific audit log you want to view. The Audit Event page opens.
5. Click **OK**.

## Filter Audit Events

1. Click Main Menu  > **Dashboard**. The Dashboard page opens.
2. Click the **Authentication**, **Issuance**, or **Management** radio button to set the type of audit log you want to view.
3. Click Search  to enable filtering.
4. The **Filters** dialog box appears.
5. Select your filter options then click **Apply**. Instant ID as a Service displays the filter results.
6. To clear the filter, click Search  again.
7. On the **Filters** dialog box, click **Reset**.

## Export Audit Events

1. Click Main Menu  > **Dashboard**. The Dashboard page opens.
2. Click the **Authentication**, **Issuance**, or **Management** radio button to set the type of audit log you want to view.
3. Click Export  to export the audit log to a .CSV file. The **Export Table to CSV** dialog box appears.
4. (Optional) Enter a **Name** for the file.
5. (Optional) Enter a **Description** for the file.
6. Select the **File Delimiter** radio button: Comma (,) or Pipe (|).
7. Select attributes to include in the file. If you do not select any attributes, by default all attributes are included in the CSV file.
8. Click **Export**. The CSV file is exported to the **Reports** page (refer to "Manage Reports" on page 111).

## Set Up Your Issuance Account

To use Instant ID as a Service, you need to create users and groups and set up authenticators.

**Attention:** When creating a new Instant ID as a Service account, create another user and assign it a Super Administrator role. This safeguards against complete account lockout.

Refer to the following help topics for more information:

- "Manage Users" on page 113
- "Manage Authenticators" on page 85
- "Manage Resources" on page 105
- "Customize Your Account" on page 21

## User Tasks

Using Instant ID as a Service changes based on your user level. To get started with Instant ID as a Service, follow the steps listed in the pages for each user. The tasks listed on this page are based on the default user roles and permissions. To grant access to a function, modify the permissions for a user role. For instructions, refer to "Create and Manage Roles" on page 114.

### Issuance Administrator Tasks

Issuance Administrators are responsible for creating additional users, managing resources, and configuring printers. They are also able to perform all tasks available in Instant ID as a Service including designing credentials and enrolling applicants.

- "Manage Users" on page 113
- "Manage Resources" on page 105
- "Manage Authenticators" on page 85
- "Printer Management" on page 123
- "Manage Reports" on page 111
- "Design a Credential" on page 25
- "Enroll Applicants" on page 75

### Issuance Designer Tasks

The Designer creates credential designs, customizes enrollment designs, and tests enrollment forms. The following are some typical tasks that a Designer might perform.

- "Design a Credential" on page 25
- "Design Enrollments" on page 54
- "Print a Sample Credential" on page 52

### Issuance Operator Tasks

The Issuance Operator uses the credential enrollment forms to enroll applicants and issue credentials. The following are typical tasks performed by the Issuance Operator user:

- "Enroll Applicants" on page 75
- "Monitor Printing" on page 145
- "Manage the Print Queue" on page 146

## Issuance Supervisor Tasks

An Issuance Supervisor views the status of printers, reviews credential designs, and monitors enrollments. Refer to the following tasks:

- "View the Issuance Dashboard" on page 145
- "Monitor Printing" on page 145
- "View Credential Designs" on page 146
- "View Enrollment Records" on page 146

## Customize Your Account

Modify the appearance and notification email template settings of an Instant ID as a Service account.

- Appearance settings control the colors and logo applied to an Entrust Adaptive Issuance Instant ID as a Service account.
- Message of the Day allows you to add information to the Instant ID as a Service Login page.
- Email Templates allow you to customize the emails sent to users from an Instant ID as a Service account.

Topics in this section:


- "Customize Your Account Appearance" below
- "Customize Email Templates" on the next page

### Customize Your Account Appearance

Change the colors, company name, logo, and add a message of the day to your account login page.

**Note:** You cannot change the language setting for Instant ID as a Service accounts

1. Go to **Customization > Theme**. The **Theme** page appears.
2. Click the **Company Name** field and modify the text to change the company name.
3. To change the color settings, select a color from the color panel or enter the HEX, RGBA, or HSLA values to set a custom color.
  - Click **Primary Color** to change the primary color of the account.
  - Click **Accent Color** to change the secondary color.
  - Click **Link Color** to change the color of links.
4. To change the logo that appears in the banner of your account, go to the **Logo** section and do the following:


- a. Click **Edit**. You are prompted to upload a file.
- b. Click Upload  then select an image file.
- c. Reposition and resize your image, as required.
- d. Click **OK**.

**Tip:** JPG image format is recommended. For the best resolution, use an image no greater than 450 pixels in width and 150 pixels in height.

5. To add a message of the day to your login page, do the following:
  - a. Click **Edit** under **Message of the Day**. The **Message of the Day** dialog box appears.
  - b. Select the language from the drop-down list to add localized messages.
  - c. Enter your customized message using the HTML tags listed under **Allowed HTML tags**.  
The maximum number of characters is *2000*. A green check mark indicates that the HTML has been validated. You can also simply enter plain text.  
**Note:** Only the *target* and *href* attributes are supported on anchor tags.
  - d. Click **OK** to return to the **Theme** page.
  - e. Preview your message. If required, click **Edit** to make any changes.
6. Click **Save** to apply the changes. You are prompted to confirm the changes.  
**Note:** Click **Reset** to revert the color and logo settings back to the default settings.

## Customize Email Templates

Modify the email templates to customize emails sent from Instant ID as a Service.

1. Select Main Menu  **Administration > Customization > Email Templates**. The Email Templates page appears.
2. Select the template from **Template** drop-down list. The template options include:
  - **Common:** Standard information in all Instant ID as a Service emails.
  - **Welcome Subscriber:** Email sent to new Service Provider users. This option is only available to Service Provider accounts.
  - **Entrust Token Activation:** Email that is sent when an Entrust Soft Token has been assigned to a user. It contains instructions on how to activate the token.
  - **One Time Password:** Email that is sent that contains the user's One Time Password (OTP) to authenticate to Instant ID as a Service.
  - **Password Email:** Email sent when a user's password has been automatically generated during password reset.
  - **Mobile Flash Pass Activation:** Email sent to an applicant after issuing a Mobile Flash Pass. The email contains links to add the Mobile Flash Pass to



Apple Wallet or Google Pay. Instant ID as a Service supports only English Mobile Flash Pass email templates.

3. From the **Language** drop-down list, select the language of the template you want to edit.

**Note:** When making changes to email templates, make sure to update the templates for each language.

4. Modify the template fields, as required. Refer to the section below for instructions specific to the template type.
5. Click **Save**.

**Note:** To revert to the default settings, click **Reset**.

### Template Fields

- Common template
  - a. In the **Service Name** field, enter the name that should appear at the bottom of all emails sent.
  - b. In the **Activate Subject** field, enter the text included in the email subject. This text appears in all authenticator activation emails.
  - c. In the **Sender field**, enter the of the sender of the emails. If left blank, emails are sent under the company name of the Instant ID as a Service account.

**Note:** The Service Name and Activate Subject fields cannot contain the following:

- more than 255 characters
  - an HTML tag
  - a space as the first or last character in the string
- Welcome Subscriber template
    - a. In the **Subject** field, type the text included in the email subject.

**Note:** The Service Name and Activate Subject fields cannot contain the following:

      - more than 255 characters
      - an HTML tag
      - a space as the first or last character in the string
    - b. In the **Select Supporting Text** text box, using the allowed HTML tags, type additional information that will appear in the email.
- Entrust Soft Token Activation template
    - a. In the **Authenticator Name** field, enter the name of the authenticator.

**Note:** The Service Name and Activate Subject fields cannot contain the following:

- more than 255 characters
  - an HTML tag
  - a space as the first or last character in the string
- b. In the **Applications Links** text box, using the allowed HTML tags, enter the links where the Entrust Soft Token app can be downloaded.
- c. In the **Manual Activation Comments** text box, enter additional information required for manual activation of the authenticator.
- One Time Password template  
In the Subject field, enter the name of the account that can be accessed by OTP.  
**Note:** The Service Name and Activate Subject fields cannot contain the following:
    - more than 255 characters
    - an HTML tag
    - a space as the first or last character in the string
  - Password Email template  
In the Subject field, enter the name of the account that can be accessed by the newly-assigned password.  
**Note:** The Service Name and Activate Subject fields cannot contain the following:
    - more than 255 characters
    - an HTML tag
    - a space as the first or last character in the string

# Designer

Issuance Designers create credential designs, create and customize enrollment designs, and test the enrollment process. Refer to the following pages for more information and instructions.

- "Design a Credential" below
- "Edit Credentials" on page 37
- "Design Enrollments" on page 54
- "Print a Sample Credential" on page 52

## Credential Design

Credential designs set the appearance and functionality of the credential using customizable graphics and fields. After designing the credential and generating an enrollment, the dynamic fields on the credential design are connected to fields on the enrollment design. For more information on credential designs, refer to the following pages:


- "Design a Credential" below
- "Configure Credential Settings" on page 50
- "Edit Credentials" on page 37
- "Configure the Credential Designer" on page 51
- "Print a Sample Credential" on page 52

## Design a Credential






Follow these steps to create a new credential design. After creating a credential design Instant ID as a Service creates an enrollment design based on the fields included in the credential design.





**Note:** Separate enrollment designs can also be created manually. In this case, the enrollment design fields must be manually linked to a new or existing credential design (refer to "Field Connections" on page 72 for details). Refer to "Enrollment Designs" on page 52 for more information on creating a separate enrollment design.

1. Create a new credential design.
  - a. From the Main Menu , select **Credential Designs**. The Credential Designs page opens.

- b. Click Create New  . The Select a Credential Design Template page opens.
- c. Select a template.
  - To create a credential design using a blank template, click **Blank**.
  - To create a credential design using a template with fields, select a template.

The Credential Designer opens.

2. Configure settings for printing and card stock in the **Card Settings** pane. For more information, refer to "Configure Credential Settings" on page 50.
3. Configure the appearance of the Credential Designer. For more information, refer to "Configure the Credential Designer" on page 51.
  - Rotate the Credential in the Credential Designer using the **Rotate**  button. Before adding fields, ensure that the credential is oriented in the same direction that it is printed.
  - Set the Credential Designer view to **Front**, **Back**, or **Both**.
  - Add a grid to the credential design using the **Grid**  button.
4. Set a background image or color on the **Background** layer. For instructions, refer to "Background Layer" on page 44.
5. Add and configure fields and objects.
  - Configure the appearance of the credential. For instructions, refer to "Add and Configure Graphics" on the next page.
  - Add fields to contain personal information from the applicant. For instructions, refer to "Add and Configure Personal Information Fields" on page 29.
  - Add a **Photograph**  field to enable photograph capture step during enrollment. For instructions, refer to "Configure Photograph Capture" on page 31.
  - Add a **Signature**  field to enable the signature step during enrollment. For instructions, refer to "Add and Configure Signature Field" on page 31.
  - Add a **Barcode**  field to print a barcode on the credential that contains information from the applicant. For instructions, refer to "Enable and Configure Bar Codes" on page 35.
  - Configure the credential design for printing embossed elements on the credential. For instructions, refer to "Enable and Configure Embossing" on page 34.
  - Configure the UV layer to enable printing UV objects on the credential. For instructions, refer to "Configure UV Printing" on page 33.
  - Configure the Topcoat layer to improve the durability of the credential by printing layers of topcoat on the credential. For instructions, refer to "Enable and Configure Topcoat" on page 32.

- To duplicate fields or objects on the credential design select an element, click **Copy**  , then click **Paste**  . Instant ID as a Service pastes the field or element with the same settings on the selected side of the credential design.
6. Configure layers properties. For more information on working with layers in the Credential Designer, refer to "Layer Properties" on page 44.
  7. Click **Print Sample** to print a sample credential to verify the visual elements.
  8. Click **Save**  . Instant ID as a Service saves the credential design.
  9. Click **Generate Enrollment**  to generate an enrollment design based on the fields on the credential design. For more information on generating enrollments, refer to "Enrollment Designs" on page 52.

Next Steps:

- "Design Enrollments" on page 54
- "Edit Credentials" on page 37



## Add and Configure Graphics





Graphics are fields and objects on the credential design that add to the appearance of the credential design. Follow these steps to configure the appearance of the credential design.





Preparation:

- Prepare static images to print on the card including the background image and logos.
- Determine what text to print on all credentials printed using this credential design. This is any text that is not specific to the applicant like the name of your organization.

Steps:

1. Create a new credential design or open an existing credential design.
2. Configure the Background layer.
  - a. Select the **Background** layer from the **Layer** pane.
  - b. Click **Expand**  at the top of the Layers pane then **Expand**  next to the **Background** layer to open the Layer Properties pane.
  - c. Select **Set Background**.
  - d. To set a solid color as the background, select **Color** then select a color from the color selector.

- e. To set an image as the background, select **Image** then click **Upload**  to upload an image.
3. Add a **Static Graphic** to the credential design.
    - a. Select the **Color** or **Black** layer. Anything added to the Black layer will print in black and white.
    - b. Click on the **Static Graphic**  field then click on the credential design. Instant ID as a Service places the field on that spot and displays the Static Graphic Properties pane.
    - c. Click **Upload**  then select an image. Instant ID as a Service displays the image on the credential design.
    - d. Configure the Static Graphic properties to adjust the size, position, and opacity of the image. For more information on the Static Graphic properties, refer to "Static Graphic Properties" on page 40
  4. Add **Static Text** to the credential design.
    - a. Select the **Color** or **Black** layer. Anything added to the Black layer will print in black and white.
    - b. Click on the **Static Text** **T** field then click on the credential design. Instant ID as a Service places the field on that spot and displays the Static Text Properties pane.
    - c. Type text into the **Display Text** field in the Static Text Properties pane.
    - d. Set the position, size, color, and alignment of the text using the Static Text Properties pane. For more information on the Static Text properties, refer to "Static Text Properties" on page 38.
  5. Add a **Rectangle** field.
    - a. Select the **Color** or **Black** layer. Anything added to the Black layer will print in black and white.
    - b. Click on **Rectangle**  then click on the credential design. Instant ID as a Service places a rectangle on that spot.
    - c. Adjust the size and position of the rectangle on the credential design.
    - d. Configure the name, border, and color of the Rectangle using the **Rectangle Field Properties** pane. For more information on Rectangle properties, refer to "Rectangle Properties" on page 42.

6. To duplicate an object, select it, click **Copy** , then click **Paste** . Instant ID as a Service places a copy with the same settings on the selected side of the credential design.
7. Click **Save** .
8. To update the enrollment based on the changes made, click **Generate Enrollment** . Instant ID as a Service updates the enrollment design with the new fields on the credential design.

### **Add and Configure Personal Information Fields**



Personal information fields are dynamic fields on the credential design that contain personal information from the applicant after enrollment. The name of the field appears in the enrollment form as the name of the field.









Preparation Notes:

Before configuring personal information fields on the credential design, consider the following guidelines:

- Assess the type of information you need to acquire from the applicant.
- Determine the best name for each piece of information so that the operator understands what information is required for the field. Use this as the field label.
- If you are adding a text field for the applicants and are planning on issuing Mobile Flash Passes, ensure that the text field contains the applicant's full name. For more information on Mobile Flash Passes, refer to "Design Mobile Flash Passes" on page 69.
- To include information in the enrollment record but not include that information on the credential, place fields outside of the design area of a credential design.

Steps:

1. Create a new credential design or open an existing credential design.
2. Add and configure a **Text**  field.
  - a. Select a layer from the **Layers** pane.
  - b. Click **Text**  then click on the Credential Design. Instant ID as a Service places the Text field at that spot and displays the Text Field Properties pane.
  - c. Enter a name for the field in the **Name** field. Instant ID as a Service also uses this as the name of field on the enrollment form.
  - d. Enter text in the **Sample Data** field. This text is the placeholder for the data entered during enrollment.







- e. Set the size, position, appearance, and color using the Text Field properties. For more information on the Text Field properties, refer to "Text Field Properties" on page 38.
3. Add and configure a **Date**  field. Use a Date field to allow the operator to enter a date during enrollment.
  - a. Select a layer from the **Layers** pane.
  - b. Click **Date**  then click on the Credential Design. Instant ID as a Service places the Date field at that spot and displays the Date Field Properties pane.
  - c. Type a name for the field in the **Name** field. Instant ID as a Service also uses this as the name of the field on the enrollment form. Enter a name that indicates to the operator what information they need to enter.
  - d. (Optional) Enter a date in the **Display Text** field. By default, Instant ID as a Service uses the current date and time.
  - e. Set the size, position, alignment, and color of the Date field using the Date Field properties. For more information, refer to "Date Field Properties" on page 40.
4. Add and configure a **Signature**  field.
  - a. Select a layer from the **Layers** pane.
  - b. Click **Signature**  then click on the Credential Design. Instant ID as a Service places the Signature field at that spot and displays the Signature Field Properties pane.
  - c. Enter a name for the Signature field in the **Name** field. Instant ID as a Service also uses this as the name of field on the enrollment form.
  - d. Configure the size, position, and rotation of the Signature field. For more information on the Signature field properties, refer to "Signature Field Properties" on page 40.
5. To duplicate a field, select it, click **Copy** , then click **Paste** . Instant ID as a Service places a copy with the same settings on the selected side of the credential design.
6. Click **Save** .
7. To update the enrollment based on the changes made, click **Generate Enrollment** . Instant ID as a Service updates the enrollment design with the new fields on the credential design.



## Configure Photograph Capture

A photograph on a credential allows security officials to identify the holder of the credential visually. The Photograph field in the Credential Designer enables the Operator to capture a photograph of the applicant during enrollment.

Preparation notes:

- Determine where on the credential design the photograph will be located. The Photograph field will cover any design on the background layer.
  - Add and configure graphics on the credential design including a background color or image. For instructions, refer to "Add and Configure Graphics" on page 27.
1. Create a new credential design or open an existing credential design.
  2. Select the **Color**  or **Black** layer from the Layers pane.
  3. Click on the **Photograph**  field then click on the credential design. Instant ID as a Service places the Photograph field at that spot and display the Photograph Field Properties pane.
  4. Position the Photograph field on the credential design that is designated for the photograph.
  5. Adjust the height and width of the Photograph field to match the designated area for the photograph.
  6. Type a name in the **Name** field. Instant ID as a Service uses this name as the name of the photograph step in the enrollment form.
  7. Configure the border, opacity, and rotation. For more information on the Photograph field properties, refer to "Photograph Field Properties" on page 39.
  8. To duplicate the field, select it, click **Copy** , then click **Paste** . Instant ID as a Service pastes the field or element with the same settings on the selected side of the credential design.
  9. Click **Save** .
  10. To update the enrollment based on the changes made, click **Generate Enrollment** . Instant ID as a Service updates the enrollment design with the new fields on the credential design.






## Add and Configure Signature Field

The Signature field improves the security of the credential by allowing the signature of the holder of the credential to be cross-checked with the signature on the credential.

Preparation Notes:

- Determine if the credential requires a signature from the applicant.
- Ensure that the computer station used for enrollment is setup to obtain a signature from the applicant.

#### Steps:

1. Create a new credential design or open an existing credential design.
2. Click on the **Signature**  field then click on the credential design. Instant ID as a Service places the Signature field at that spot and display the Signature Field Properties pane.
3. Position the Signature field on the credential design.
4. Type a name for the Signature field in the **Name** field. Instant ID as a Service uses this name for the name of the Signature field in the enrollment form. Use a name that informs the operator what is data is required.
5. From the **Alignment** list, select the alignment of the signature inside of the Signature field.
  - The first word indicates the horizontal placement of the signature. Options include: **Left**, **Center**, and **Right**.
  - The second word indicates the vertical placement of the signature Options include **Top**, **Center**, and **Bottom**.
  - **Fill Entire Field** expands the signature to fill the area of the Signature field.
6. Configure the size, position and rotation. For more information, refer to "Signature Field Properties" on page 40.
7. Select **Display the signature backdrop as transparent** to set the background of the Signature field as transparent.
8. To duplicate the field, select it, click **Copy** , then click **Paste** . Instant ID as a Service places a copy with the same settings on the selected side of the credential design.
9. Click **Save** .
10. To update the enrollment based on the changes made, click **Generate Enrollment** . Instant ID as a Service updates the enrollment design with the new fields on the credential design.





### Enable and Configure Topcoat

The Topcoat layer prints additional layers of protective material on top of the credential. The additional layers increase the durability of the credential. It also increases the amount of topcoat material used during printing. Instant ID as a Service includes options to add up to four layers of topcoat on each side of the credential.

Preparation Notes:

- Refer to the specifications of the printer to ensure that it supports printing topcoat layers according to the setting on the credential design.
- Plan on how much topcoat to apply to the credentials taking into account the amount of topcoat material used and the required durability of the credentials.



#### Steps:








1. Create a new credential design or open an existing credential design.
2. Enable the Topcoat/RTM layer.
  - a. Click Expand  to expand the Layers pane.
  - b. Select the checkbox next to **Topcoat/RTM** to enable the layer.
3. Select the number of layers of topcoat to apply on the credential.
  - Select **Single** to apply one layers of topcoat on the credential.
  - Select **Double** to apply two layers of topcoat on the credential.
4. With the Layers pane expanded, click Expand  to open the properties for the Topcoat layer.
5. Add a Rectangle field to block topcoat from printing on that area. For more information on the Rectangle field, refer to "Rectangle Properties" on page 42.
6. Click **Save** .
7. To update the enrollment based on the changes made, click **Generate Enrollment** . Instant ID as a Service updates the enrollment design with the new fields on the credential design.

### Configure UV Printing

UV elements on a credential improves the security of the credential by adding elements that are difficult to forge. The UV layer adds elements like text fields, images, and shapes.

#### Preparation notes:

- Determine if the credential would benefit from UV security elements.
  - Design an image or text to use in UV printing.
1. Create a new credential design or open an existing credential design.
  2. Enable the UV/Luster layer.
    - a. Click **Expand**  to expand the Layers pane.
    - b. Click the checkbox next to **UV/Luster Layer** to enable the layer.
  3. With the **Layers** pane expanded, click **Expand**  to open the properties for the UV/Luster layer.

4. Add fields to the UV/Luster layer.
  - Add a **Text**  field to print text entered during enrollment onto the credential.
  - Add a **Static Text**  field to print text onto the credential.
  - Add a **Photograph**  field to print a photograph of the applicant taken during enrollment on the UV/Luster layer.
  - Add a **Static Graphic**  field to print an image on the credential design using the UV/Luster layer.
  - Add a **Signature**  field to print the signature of the application the UV/Luster layer.
5. Click **Save** .
6. To update the enrollment based on the changes made, click **Generate Enrollment** . Instant ID as a Service updates the enrollment design with the new fields on the credential design.




### Enable and Configure Embossing


Embossing imprints elevated text or numbers on the credential. Follow these steps to configure emboss printing.

Preparation notes:



- Verify that the printer supports embossing.
- Design what information will be embossed on each credential. Common examples are the applicant's name or user number.

Steps:

1. Create a new credential design or open an existing credential design.
2. Enable the Emboss layer.
  - a. Click Expand  to expand the Layers pane.
  - b. Click the checkbox next to **Emboss** to enable the layer.
3. With the Layers pane expanded, click Expand  to open the properties for the Emboss/Indent layer.
  - Select **Show the emboss and indent boundary** to highlight the area on the credential where the printer is able to emboss characters.
  - To display the emboss topping on the credential design, select **Show the emboss topping** then select a color from the color selector.
4. Add fields to the Emboss/Indent layer on the credential design.
  - Add a **Static Text**  field to emboss text on the credential. The Static Text field remains the same for all credentials.

- Add a Text  field to add text that contains information gathered from the applicant during enrollment.








For more information on configuring field properties, refer to "Edit Field Properties" on page 38.

5. Click **Save** .
6. To update the enrollment based on the changes made, click **Generate Enrollment** . Instant ID as a Service updates the enrollment design with the new fields on the credential design.

### Enable and Configure Bar Codes

The Barcode field adds a bar code to the credential design and adds a field on the enrollment form. Instant ID as a Service encodes the data entered in that field during enrollment and creates a bar code.

Preparation notes:

- Determine which bar code format to use. Ensure that the bar code reader can read that format.
  - Determine what information you want to be encoded in the bar code. A common example is the applicant's ID number.
1. Create a new credential design or open an existing credential design.
  2. Select the **Color**  or **Black**  layer from the Layers pane. Use the Black layer to produce a bar code that bar code readers can more easily read.
  3. Click the **Barcode**  field then click on the credential design. Instant ID as a Service places the Barcode field at that spot and display the Barcode Field Properties pane.
  4. In the **Name** field, type a name for the bar code field. Instant ID as a Service uses this name for the name of the field in the enrollment form. Use a name that informs the operator what information is required.
  5. Configure bar code properties in the **Barcode Field Properties** pane. For more information, refer to "Barcode Field Properties" on page 41.
  6. To duplicate the barcode, select it, click **Copy** , then click **Paste** . Instant ID as a Service places a copy with the same settings on the selected side of the credential design.
  7. Click **Save** .
  8. To update the enrollment based on the changes made, click **Generate Enrollment** . Instant ID as a Service updates the enrollment design with the new fields on the credential design.

## Enable and Configure Magnetic Stripe



The Magnetic Stripe element enables printers to encode data onto the magnetic stripe on a card. To configure magnetic stripe encoding and printer, add the Magnetic Stripe field, configure the properties, then connect fields on the enrollment form to the magnetic stripe tracks.

Preparation Notes:



- Check the magnetic stripe specifications of the card stock.
- Determine which fields on the credential you want to write to the magnetic stripe.
- Refer to "Magnetic Stripe Field Properties" on page 42 to better understand the requirements for the magnetic stripe track types.
- Configuring Magnetic Stripe requires the Advanced Entitlements Bundle. If you do not have the Advanced Entitlements Bundle, contact your Service Provider.

### Add and Configure the Magnetic Stripe Field

Follow these steps to add and configure the Magnetic Stripe field on the credential design. Then, follow the steps in "Connect Fields to Magnetic Stripe Tracks" on the next page to connect the magnetic stripe tracks to fields on the enrollment form.



1. Create a new credential design or open an existing credential design.
2. Select the Black layer .
3. Click on the **Magnetic Stripe**  field then click on the credential design.
4. Enter a name for the field in the **Name** field.
5. Adjust the **Height** of the field on the credential design to match the magnetic stripe on the card stock. The width of the field must extend the entire width of the credential design.
6. Position the Magnetic Stripe field on the credential design to match the placement of the magnetic stripe on the card stock. Enter values in the **Left** and **Top** fields or manually move the Magnetic Stripe field on the credential.
7. Configure magnetic stripe tracks for IAT track types.
  - a. Select **IAT** as the **Track Type**.
  - b. From the **Coercivity** list, select **High** or **Low**.
  - c. Select ASCII Hex Format for any track that will contain ASCII-hex characters.

For more information on the requirements for magnetic stripe tracks, refer to "Magnetic Stripe Field Properties" on page 42.

8. Click **Save** .
9. Click **Generate Enrollment**  to generate a new enrollment. Instant ID as a Service updates the enrollment design with the new fields on the credential design.



## Connect Fields to Magnetic Stripe Tracks

Connect fields on the credential design to magnetic stripe tracks. Instant ID as a Service

1. From the Main Menu , click **Credential Designs**.
2. Click **Connect Magnetic Stripe** . The Configure Magnetic Stripe Connections dialog box opens.
3. Connect the magnetic stripe tracks.
  - Select a field from the list to map the field to the magnetic stripe track.
  - Select **None** to not write any data to the track.
  - Select **New Field** to create a new field in the enrollment form for the track. Then enter a name for the new field. The data entered into the field in the enrollment form will be encoded into the magnetic stripe track.
4. Click **Save**.
5. To modify the connections after saving, click **Reset**.

## Create a New Credential

To initiate the credential design process, create a new credential design using a credential design template or a blank credential.

1. From the Main Menu , select **Credential Designer**. The Credential Designs page opens.
2. Click Create New . The Select a Credential Design Template page opens.
3. Select a template.
  - To create a credential design using a blank template, click **Blank**.
  - To create a credential design using a template with fields, select one of the other templates.The Credential Designer opens.
4. Design the credential following the instructions in "Design a Credential" on page 25.

## Edit Credentials

Edit credentials to add fields to include new information in the final credential. Editing the credential design also changes the enrollment form. To change the enrollment form, edit the credential design.

For instructions on editing credential designs, refer to the following pages:

- "Edit Field Properties" on the next page
- "Manage Layers" on page 44






## Edit Field Properties

Field properties open in the right pane after selecting a field on the credential design. Follow the steps in this section to configure field properties. Refer to the following topics for instructions specific to each field:

- "Text Field Properties" below
- "Static Text Properties" below
- "Photograph Field Properties" on the next page
- "Static Graphic Properties" on page 40
- "Date Field Properties" on page 40
- "Signature Field Properties" on page 40
- "Barcode Field Properties" on page 41
- "Rectangle Properties" on page 42

### Text Field Properties

The Text field allows text from a field in the enrollment form to appear on the credential. The Text field properties sets the location, font, and alignment of the text on the credential. Configure the following settings for the Text field on a credential design.






1. Enter a name for the Text field in the **Name** field.
2. Enter text to display in the preview of the Text field in the **Sample Data** field.
3. Modify the size of the Text field using the **Height** and **Width** fields.
4. Enter values in the **Left** and **Top** to modify the position of the Text field.
5. Enter a percent in the **Rotation** field to rotate the Text field.
6. Modify the font for the text in the Text field.
  - Enter a size in the **Font size** field.
  - Select Bold, Italic, or Underline from the **Font Style** area.
7. Select colors from the **Fill** and **Stroke** selections in the Color area.
8. Select **Left** , **Center** , **Right** , or **Justify**  from the **Alignment** area.
9. Click **Save** .

### Static Text Properties

The Static Text field places text on a credential design that remains the same for all issued credentials.


1. Type a name in the **Name** field.
2. Enter text in the **Display Text** field to display in the selected field.
3. Modify the values in the **Width** and **Height** fields to adjust the size of the field on the credential design.



4. Modify the values in the **Left** and **Top** fields to adjust the position of the field on the credential design.
5. Enter a percentage in the **Rotation** field to rotate the field on the credential design.
6. Select **Word Wrap** to allow the text in the field to wrap to
7. Select **Multiline** to allow the Static Text field to contain multiple lines of text.
8. Modify the font for the text in the field.
  - From the **Font Family** list, select a font family for the text in the field.
  - Enter a size in the **Font size** field.
  - Select Bold, Italic, or Underline from the **Font Style** area.
9. Select colors from the **Fill** and **Stroke** selections in the Color area to change the color of the field. **Fill** controls the color inside of the field and **Stroke** controls the outline of the field.
10. Select **Left** , **Center** , **Right** , or **Justify**  from the **Alignment** area.
11. Click **Save**  .



#### Photograph Field Properties

The Photograph field designates a space on the credential for a photograph of the applicant captured during enrollment. Follow these steps to configure the properties for the Photograph field.

1. Enter a name for the field in the **Name** field.
2. From the **Alignment** list, select the alignment of the photograph in the field.
3. Modify the values in the **Width** and **Height** fields to adjust the size of the field on the credential design. Size - Width and Height
4. Modify the values in the **Left** and **Top** fields to adjust the position of the field on the credential design.
5. Enter a percentage in the **Rotation** field to rotate the field on the credential design.
6. Configure the border around the photograph.
  - Select **Display Border** to enable the border.
  - From the **Weight** list, set the thickness of the border.
  - From the **Color** selector, set the color of the border.
7. In the Advanced area, set the opacity of the Photograph field - Toggle and percent opacity
  1. Select the check box under **Ghosting**.
  2. Select a percent opacity from the slider.
8. Select **Remove Backdrop** to remove the background of the photograph when previewing or printing the credential.
9. Click **Save**  .






### Static Graphic Properties

The Static Graphic places an image on the credential design. Follow these steps to configure the properties for Static Graphics.

1. Enter a name for the field in the **Name** field.
2. Click **Upload**  then select an image to upload.
3. Modify the values in the **Width** and **Height** fields to adjust the size of the field on the credential design.
4. Modify the values in the **Left** and **Top** fields to adjust the position of the field on the credential design.
5. Enter a percentage in the **Rotation** field to rotate the field on the credential design.
6. Select **Display the graphic as semi-opaque** then set the **Percent Opaque** to set the opacity of the graphic.
7. Click **Save** .


### Date Field Properties

The Date Field adds a date on the credential. During enrollment, the user selects a date.

1. Enter a name for the field in the **Name** field.
2. Enter text in the **Display Text** field to display in the selected field.
3. Modify the values in the **Width** and **Height** fields to adjust the size of the field on the credential design.
4. Modify the values in the **Left** and **Top** fields to adjust the position of the field on the credential design.
5. Enter a percentage in the **Rotation** field to rotate the field on the credential design.
6. Select **Automatically adjust font size** to allow the font size to adjust to fit the text inside the field.
7. Modify the font for the text in the field. From the **Font Family** list, select a font family for the text in the field. Enter a size in the **Font size** field. Select Bold, Italic, or Underline from the **Font Style** area.
8. Select colors from the **Fill** and **Stroke** selections in the Color area to change the color of the field. **Fill** controls the color inside of the field and **Stroke** controls the outline of the field.
9. Select **Left** , **Center** , **Right** , or **Justify**  from the **Alignment** area.
10. Click **Save** .





### Signature Field Properties

The Signature field places the signature of the applicant obtained during enrollment on the credential.

1. Enter a name for the field in the **Name** field.
2. From the **Alignment** list, select an alignment for the signature inside the field.
3. Modify the values in the **Width** and **Height** fields to adjust the size of the field on the credential design.
4. Modify the values in the **Left** and **Top** fields to adjust the position of the field on the credential design.
5. Enter a percentage in the **Rotation** field to rotate the field on the credential design.
6. Select **Display the signature backdrop as transparent** to make the background transparent.
7. Click **Save**  .

### Barcode Field Properties

The Barcode field places a bar code on the credential using data gathered from enrollment.


1. Enter a name for the field in the **Name** field.
2. Enter data in the **Sample Data** field. The Barcode field displays this data in previews and samples of the credential.
3. Select **Left**  , **Center**  , **Right**  , or **Justify**  from the **Alignment** area.
4. Modify the values in the **Width** and **Height** fields to adjust the size of the field on the credential design.
5. Modify the values in the **Left** and **Top** fields to adjust the position of the field on the credential design.
6. Enter a percentage in the **Rotation** field to rotate the field on the credential design.
7. From the **Background** color selector, select black or white to set the background of the Barcode field as black or white.
8. From the **Bar Code** type list, select a bar code format. Instant ID as a Service converts the data in the Barcode field into the selected bar code format.
9. From the **Density** list, select **High**, **Medium**, or **Low**. Density sets the width of the vertical lines in the bar code. Low sets it to four pixels, Medium sets it to two pixels, and High sets it to one pixel.
10. Under **Interpretation text**, select **On** or **Off**. Enabling Interpretation text displays the text encoded in the bar code beneath the bar code on the credential.
11. Modify the font for the text in the field.
  - From the **Font Family** list, select a font family for the text in the field.
  - Enter a size in the **Font size** field.
  - Select Bold, Italic, or Underline from the **Font Style** area.
12. From the **Alignment** list, select a alignment of the bar code inside the designated

area.

13. Click **Save**  .

### Rectangle Properties

The Rectangle field places a rectangle on the credential design. Follow these steps to configure the size, shape, and properties of a Rectangle on a credential.

1. Enter a name for the field in the **Name** field.
2. Modify the values in the **Width** and **Height** fields to adjust the size of the field on the credential design.
3. Modify the values in the **Left** and **Top** fields to adjust the position of the field on the credential design.
4. From the **Line Weight** list, select a thickness for the field.
5. From the **Line Color** selector, select a color for the border of the rectangle.
6. Select **Round Corners** to round off the corners of the rectangle element.
7. From the **Fill** selector, select a color for the body of the rectangle.
8. Click **Save**  .

### Magnetic Stripe Field Properties

The Magnetic Stripe field enables the printer to encode information on the magnetic stripe tracks on a card. Refer to this page for more information on Magnetic Stripe properties.

**Note:** Configuring Magnetic Stripe requires the Advanced Entitlements Bundle. If you do not have the Advanced Entitlements Bundle, contact your Service Provider.

1. Enter a name for the field in the **Name** field.
2. Modify the values in the **Width** and **Height** fields to adjust the size of the field on the credential design. The width is set by the width of the credential.
3. Modify the values in the **Left** and **Top** fields to adjust the position of the field on the credential design.
4. Select a **Coercivity** level to match the specifications of the printer and card stock.
  - High
  - Low
5. For IAT track types, select **ASCII Hex Format** to indicate that the data is in ASCII Hexadecimal format. This enables the printer to properly encode the data to the magnetic stripe.

### Magnetic Stripe Track Types

Instant ID as a Service supports IAT track types for magnetic stripe encoding. Instant ID as a Service uses the track type for all tracks in the magnetic stripe on the card.

## Track Type IAT

Cards with IAT magnetic stripes contain three tracks for encoding data. The three tracks together are known as "IAT" referring to the type of requirements on the data. Refer to the information below for requirement for each IAT magnetic stripe track.

### Note:

Encoding IAT track types requires an ISO magnetic stripe option in the printer.

- **Track 1:**

Track 1 is the International Air Transport Association (IATA) format. It is located at the top of the magnetic stripe. Track 1 allows up to 76 characters including ASCII characters with decimal values from 32 to 95. Valid characters are:

- Spaces
- Uppercase alphabetic characters: A-Z
- Numerals: 0-9
- Special characters: !#\$%&'()\*+,-./:;<@>=^]\[\"&\_ and (space)

- **Track 2:**

Track 2 is the American Bankers Association (ABA) format. It is located in the middle of the stripe. Track 2 allows up to 37 characters including ASCII characters with decimal values from 48 to 63. Valid characters:

- Numerals: 0-9
- Special characters: :;<=>

- **Track 3:**

Track 3 is the Thrift Third Standard (TTS) format. It is located at the bottom of the stripe. This format allows up to 104 characters (ASCII characters with decimal values from 48 to 63, inclusive). Valid characters:

- Numerals: 0-9
- Special characters: :;<=>

- **ASCII Hex Format:**

Selecting ASCII Hex Format indicates that the data provided for the magnetic stripe track is in ASCII hexadecimal format. This enables the printer to properly encode the data to the magnetic stripe. For example, select this option if the data is in ASCII hexadecimal format and you do not want to convert the data to conform to the track requirements.

## Manage Layers



The Credential Designer uses layers to organize fields and elements on the credential design into logical categories. Layers appear on the left side of the credential designer. Each field added to the credential design resides on a layer. To edit a field on a layer, you must first select that layer. Layers also contain properties that set how the layer influences and interacts with the credential design.

### Layer Properties

Layer properties configure the functionality of the layer on the credential design.

#### Open Layer Properties

Follow these steps to open the Layer Properties pane for any layer in the Credential Designer.

1. Click  above the layers to expand the Layers pane.
2. Click  next to a layer to expand the Layer Properties pane for that layer.
3. Configure the layer properties. For more information on layers and layer properties, follow one of the links below.

## Layer Properties

- "Background Layer" below
- "Color Layer" on the next page
- "Black Layer" on the next page
- "Emboss/Indent Layer" on page 46
- "Non-Printable Area Layer" on page 46
- "Durability and Security" on page 46
  - "Laminate Layer" on page 48
  - "Topcoat/RTM Layer" on page 49
  - "UV Luster Layer" on page 50

#### Background Layer



The Background layer sets a static image or color as the background of the credential. The Background layer supports the following fields:

- Static Text
- Static Graphic

- Rectangle

For more information on field properties, refer to "Edit Field Properties" on page 38.

## Configure Background Layer Properties

1. Click the arrow on the right of the layer to expand the layer properties.
2. Click **Set Background**.
  - Select **Color** then select a color from the color selector.
  - Select **Image** then click **Upload**  then upload an image for the background.
3. Click **Save** .

### Color Layer

The Color layer contains color text, images, or shapes on the credential. The Color layer supports the following fields on the credential design:

- Text
- Static Text
- Photograph
- Static Graphic
- Date
- Signature
- Barcode
- Rectangle

For more information on field properties, refer to "Edit Field Properties" on page 38.

### Black Layer

The Black layer contains objects that print without color. It is ideal for printing fields that do not require color such as barcode and signature fields. The Black layer supports the following fields:

- Text
- Static Text
- Photograph
- Static Graphic
- Date
- Signature
- Barcode

- Rectangle
- Magnetic Stripe

For more information on field properties, refer to "Edit Field Properties" on page 38.

#### Emboss/Indent Layer



The Emboss/Indent layer contains text fields that the printer will emboss on the credential. The printer imprints raised characters on the credential. The Emboss/Indent layer supports the Text and Static Text fields. The Emboss/Indent layer supports the following fields:

- Text
- Static Text

For more information on field properties, refer to "Edit Field Properties" on page 38.

## Configure Emboss/Indent Layer Properties

Follow these steps to configure the properties for the Emboss/Indent layer.

1. Click **Expand**  to the right of the layer to expand the layer properties.
2. Select **Show the emboss and indent boundary** to highlight the area on the credential where the printer is able to emboss characters.
3. To display the emboss topping on the credential design, select **Show the emboss topping** then select a color from the color selector.
4. Click **Save** .

#### Non-Printable Area Layer

Use the Non-printable area layer to define areas on the card that must not be printed over. For example, placing a rectangle in the Non-printable area layer over the manual Signature field prevents the printer from printing on top of the Signature field.

When a Rectangle is added to the Non-printable area layer, it displays red and white lines on the screen for design purposes. This Rectangle blocks the contents of all layers except for the Lamination and Topcoat/RTM layers.

#### Durability and Security



Durability and Security contains layers that apply objects and fields that improve the durability and security of the credential. Refer to the following topics for more information on the layers within Durability and Security:



- "Laminate Layer" on the next page: The Laminate layer contains options and objects that configure how the printer applies lamination to the card.
- "Topcoat/RTM Layer" on page 49: The Topcoat/RTM layer contains options to apply topcoat layers on the credential to improve durability.
- "UV Luster Layer" on page 50: The UV/Luster layer contains graphic elements printed using UV material to improve the security of the credential.

# Laminate Layer


The Laminate layer contains options that configure how the printer applies lamination to the credential. Configure the properties of the Laminate layer to set how the printer applies lamination on the credential when printing. Ensure that the printer supports the lamination settings applied on the Lamination layer.

1. Select the checkbox next to the Laminate layer to enable the layer.
2. Click Expand  to the right of the layer to expand the layer properties.
3. From the **Laminate 1** and **Laminate 2** lists select one of the following options:
  - **Do not use**: sets the laminator to print no lamination on the credential.
  - **Laminate once**: sets the laminator to print one layer or lamination on the credential.
  - **Laminate twice**: sets the laminator to print two layers of lamination on the credential.
4. Click **Save** .

# Topcoat/RTM Layer

The Topcoat/RTM layer configures how the printer applies topcoat and retransfer material (RTM) on the credential. Instant ID as a Service supports the Rectangle field on the Topcoat/RTM layer to block topcoat and RTM from printing on the credential.

Follow these steps to configure the Topcoat/RTM Layer properties.

1. Select the checkbox next to **Topcoat/RTM** layer to enable the layer.
2. Select **Single** to apply one layer on the credential.
3. Select **Double** to apply two layers on the credentials
4. Click **Save**  .

# UV Luster Layer

The UV Luster layer contains fields that prints on the credential using ultraviolet material.


The UV Luster layer supports the following fields:

- Text
- Static Text
- Photograph
- Static Graphic
- Signature

For more information on field properties, refer to "Edit Field Properties" on page 38.


## Configure Credential Settings

The credential settings in the Credential Designer set the name of the credential design, card size, and other settings related to the credential and card stock.

1. Expand the **Card Settings** pane on the right of the Credential Designer.
2. Enter a name for the credential design in the **Card Name** field.
3. (Optional) Enter a description for the credential design in the **Description** field.
4. Select a unit of measurement from the **Units** list.
5. Configure the dimensions of the card.
  - Set a card stock type from the **Dimensions** list.
  - (Optional) Modify the dimensions in the **Width** and **Height** fields.
6. Configure the options in the **Printer Actions** area.
  - Select **Rewritable** to allow the credential to be rewritten. Ensure that the card stock is rewritable.
  - Select **Tactile** to enable tactile printing on cards. For more information, refer to "Enable Tactile Impression" below.
  - Select **Front** or **Back** under **Print orientation 180 degrees** to set the print orientation for the card.
  - Select the **Ribbon optimization** options. **Auto** allows the printer to enable ribbon optimization based on the conditions of the print job and printer status.
7. Click **Save** .



## Enable Tactile Impression

Printers with a tactile impression module are able to imprint a design on the front or back of the card. Sigma printers imprint the design in one of three positions on the card. You can enable tactile impressions only on the front or back of the card not both. Follow these instructions to enable tactile imprinting on a credential design.

1. Expand the **Card Settings** pane on the right of the Credential Designer.
2. To enable tactile impression on the front of the card, select one of the following options from the **Tactile Front** list:
  - Select **True** to enable tactile impression on the front of the card. The printer imprints the design in the position on the card setup on the Tactile Impression Module. Sigma printers imprint the design in position 1.
  - Select **1** to enable the Tactile Impression Module on Sigma printers and imprint the design in position one. Position one is on the right side of the card.
  - Select **2** to enable the Tactile Impression Module on Sigma printers and imprint the design in position two. Position two is in the center of the card.
  - Select **3** to enable the Tactile Impression Module on Sigma printers and imprint the design in position three. Position three is on the left side of the card.
3. To enable tactile impression on the back of the card, select one of the following options from the **Tactile Back** list:
  - Select **True** to enable tactile impression on the back of the card. The printer imprints the design in the position on the card setup on the Tactile Impression Module. Sigma printers imprint the design in position 1.
  - Select **1** to enable the Tactile Impression Module on Sigma printers and imprint the design in position one. Position one is on the right side of the card.
  - Select **2** to enable the Tactile Impression Module on Sigma printers and imprint the design in position two in the center of the card.
  - Select **3** to enable the Tactile Impression Module on Sigma printers and imprint the design in position three on the left side of the card.
4. Click **Save** .


## Configure the Credential Designer

The Credential Designer includes options to configure the appearance and functions of the Credential Designer. Follow the instructions below to enable the options.

- **Grid:** Click  to enable the Grid. The Grid places horizontal and vertical lines on the selected side of the card in increments of 1 cm or 1 in.
- **Rotate:** Click  to rotate the credential in the Credential Designer. It rotates the selected side of the credential 90 degrees clockwise. Rotate the credential to match the orientation of the final credential.
- **Front, Back, and Both:** Select the side of the credential to display in the Credential Designer.

## Print a Sample Credential

Print a sample of a credential design to view how the credential design will appear on a printed card. The sample credential contains place-holder data in the place of data typically gathered from the applicant.

1. Click **Print Sample**  . The Print Sample dialog box opens.
2. From the **Select sides to print** list, select a side of the card to print. Options include Both sides, Front, or Back.
3. From the **Printer** list, select a printer.
4. From the **Hopper** list, select a hopper on the printer that contains card stock for the credential.
5. Click **Print**. The selected printer prints a sample credential with placeholder information and graphics.

## Enrollment Designs

Enrollment designs control the appearance and functionality of the enrollment form used to enroll Applicants.

Generating an enrollment from a credential design creates an enrollment design (refer to "Generate an Enrollment Design" on the next page). Alternatively, enrollment designs can be created independently of credential designs if needed, although a credential design must also still be created (refer to "Generate a New Enrollment Design" below).

Using the enrollment designer you can add or reorganize fields and steps, customize field and step properties, link enrollment design fields to a credential design via the "Field Connections" on page 72 page, and customize the appearance of the enrollment form. Configure the enrollment design to customize the enrollment process.

Entire enrollment designs can also be copied and re-used via the Save As feature (refer to "Copy an Enrollment Design" on the next page).



- "Generate a New Enrollment Design" below
- "Generate an Enrollment Design" on the next page
- "Copy an Enrollment Design" on the next page
- "Design Enrollments" on page 54

## Generate a New Enrollment Design

Generate a separate enrollment design without automatically generating the enrollment design from a credential design.

**Important:** If a separate enrollment design is created, the fields in the new enrollment design must be linked to a new or existing credential design (refer to "Field Connections" on page 72 for more information).

After generating the new enrollment design, customize it using the Enrollment Designer.



1. From the Main Menu , select **Enrollment Designs**. The Enrollment Designs page opens.
2. Select **Create New** . The Enrollment Designer page opens.
3. Set up the new enrollment design by formatting the available fields in the Enrollment Designer page. Refer to "Design Enrollments" on the next page for details.

Next Steps:

"Design Enrollments" on the next page

## Generate an Enrollment Design

Generate an enrollment from an existing credential design to create an enrollment form and enrollment design. After generating an enrollment design, customize it using the Enrollment Designer.




1. From the Main Menu , select **Credential Designs**. The Credentials pages opens.
2. Select a credential design from the table. The Credential Designer opens.
3. Review the credential design to ensure that it appears correct. For instructions on using the Credential Designer, refer to "Design a Credential" on page 25.
4. Click **Generate Enrollment** . A confirmation dialog box opens.  
**Note:** Generating an enrollment from a credential design that already has enrollment records deletes all existing enrollment records for that credential design.
5. Click **Generate**. Instant ID as a Service generates an enrollment form based on the credential design.

Next Steps:

"Design Enrollments" on the next page

## Copy an Enrollment Design

Copy an existing enrollment design and re-use it as the basis for a new design via the Save As feature.

1. Open an existing enrollment design:
  - a. From the Main Menu , select **Enrollment Designs**. The Enrollment Designs page opens.
  - b. Click on an enrollment design name. The enrollment design opens in the Enrollment Designer.
2. Click **Save As** . The Save as a New Enrollment Design page opens.
  - a. Enter a unique name for the copied enrollment design.
  - b. Click **Save**.
3. Modify the appearance of the copied enrollment design by adding or updating fields and the name of the Enrollment Design. For instructions, refer to "Enrollment Appearance" on the next page.
4. Configure field properties to meet the needs of the enrollment process. For instructions, refer to the following pages:
  - "Enrollment Design Fields" on page 56
  - "Configure Text Fields" on page 59
  - "Configure Date Fields" on page 60
  - "Configure Photo Fields" on page 62
  - "Signature Field Properties" on page 40
  - For information on Mobile Flash Pass, refer to "Design Mobile Flash Passes" on page 69
5. Configure steps in the enrollment design to meet the needs of the enrollment process. This includes creating, renaming, moving, or deleting steps. For instructions, refer to "Add or Configure Enrollment Design Steps" on page 65.
6. Edit the enrollment design settings to add a description or change the tab order. For instructions, refer to "Configure Enrollment Design Settings" on page 68.
7. Edit the enrollment search settings to customize the fields displayed when searching for enrollments. For instructions, refer to "Configure Enrollment Search Settings" on page 68.
8. Link any unlinked fields created to a new or existing credential design. For instructions, refer to "Field Connections" on page 72.
9. Click **Save** .


## Design Enrollments

Enrollment designs control the fields and pages that the Operator user uses to enroll applicants.

The enrollment designer provides tools to create or modify the appearance of steps and fields, change the settings for steps and fields, and change the order of steps, fields, and pages on the enrollment form.



Entire enrollment designs can also be copied and re-used via the Save As feature (refer to "Copy an Enrollment Design" on page 53).

1. Either generate an enrollment from a Credential Design (refer to "Generate an Enrollment Design" on page 53) or create a separate enrollment design (refer to "Generate a New Enrollment Design" on page 52).
2. Open the enrollment design, or continue to edit the newly created separate enrollment design. To open an existing design:
  - a. From the Main Menu , select **Enrollment Designs**. The Enrollment Designs page opens.
  - b. Click on an enrollment design name. The enrollment design opens in the Enrollment Designer.
3. Modify the appearance of the enrollment design by adding or updating fields and the name of the Enrollment Design. For instructions, refer to "Enrollment Appearance" below.
4. Configure field properties to meet the needs of the enrollment process. For instructions, refer to the following pages:
  - "Enrollment Design Fields" on the next page
  - "Configure Text Fields" on page 59
  - "Configure Date Fields" on page 60
  - "Configure Photo Fields" on page 62
  - "Signature Field Properties" on page 40
  - For information on Mobile Flash Pass, refer to "Design Mobile Flash Passes" on page 69
5. Configure steps in the enrollment design to meet the needs of the enrollment process. This includes creating, renaming, moving, or deleting steps. For instructions, refer to "Add or Configure Enrollment Design Steps" on page 65.
6. Edit the enrollment design settings to add a description or change the tab order. For instructions, refer to "Configure Enrollment Design Settings" on page 68.
7. Edit the enrollment search settings to customize the fields displayed when searching for enrollments. For instructions, refer to "Configure Enrollment Search Settings" on page 68.
8. For separate enrollment designs that have been manually generated, link the fields created to a new or existing credential design. For instructions, refer to "Field Connections" on page 72.




## **Enrollment Appearance**

The enrollment design sets the appearance of the enrollment form that Operators use to enroll applicants. The Enrollment Designer allows the user to create or edit the name of the enrollment design, add or modify the name of steps, and add, rearrange, or edit the steps. Refer to "Add or Configure Enrollment Design Steps" on page 65 for more

information on steps. Use the instructions on this page to add or edit the enrollment design name.




### Add the Enrollment Design Name

The enrollment design name appears above the enrollment form during the enrollment process. The name of the enrollment design must be unique. Follow these steps to add the enrollment design name.

1. Click the **Settings**  icon in the left pane.
2. Type a new Enrollment Design Name.
3. Click **Save**  to save or **Close**  to exit without saving.

### Edit the Enrollment Design Name

The enrollment design name appears above the enrollment form during the enrollment process. The name of the enrollment design must be unique. Follow these steps to edit the enrollment design name.

1. Click **Edit**  next to the Enrollment Design name.
2. Type a new Enrollment Design Name.
3. Click **Save**  to save or **Close**  to exit without saving.

### Enrollment Design Fields

The fields in an enrollment design are connected to fields on the corresponding credential design. Every field on the credential design is connected to a field on the enrollment design.

Refer to the following pages for instructions on setting up fields on the enrollment design:










- "Configure Text Fields" on page 59
- "Configure Photo Fields" on page 62
- "Configure Date Fields" on page 60
- "Configure Signature Fields" on page 64
- For information on Mobile Flash Pass, refer to "Design Mobile Flash Passes" on page 69

Once added or configured, enrollment fields can also be edited, moved, copied and pasted, or deleted.

**Note:** Separate enrollment designs created manually and not generated from a credential design must have their fields linked manually to a new or existing credential design. Refer to "Field Connections" on page 72 for more information on the process.




### Add Fields

To add fields to a step:

1. Click the **Enrollment Design**  icon in the left pane.
2. Click the arrow icon to expand the pane (if necessary).
3. Click the arrow icon next to Enrollment Design to expand the menu. The current steps for the enrollment design display.
4. Click to select a step.
5. Click in the main pane to the right and the pane becomes active. Any existing fields in the step display.
6. Click the **Add**  icon next to any of the steps to add that step to the sequence and start configuring the step. Note that default steps will have some information pre-populated. To configure the step:
  - a. Click in the main pane to the right and the pane becomes active.
  - b. Click in the field for the step name and enter the name.
  - c. Add specific step fields by clicking the icon for the type needed and the clicking again in the location where the field should be placed. Note that fields can be clicked-and-dragged to specific locations.
    - i. **Text**  : Adds a text field.
    - ii. **Photo**  : Adds a photo field.
    - iii. **Date**  : Adds a date field.
    - iv. **Signature**  : Adds a signature field.
    - v. **Auto Sequence**  : Adds an auto-sequence field.
7. Click each field and the field's Properties pane displays. Edit the properties for the field as needed.
8. Click **Save**  to save or **Close**  to exit without saving.
9. For separate enrollment designs that have been manually generated, link the fields created to a new or existing credential design. For instructions, refer to "Field Connections" on page 72.




### Edit Fields

To edit existing fields:

1. Click the **Enrollment Design**  icon in the left pane.
2. Click the arrow icon to expand the pane (if necessary).
3. Click the arrow icon next to Enrollment Design to expand the menu. The current steps for the enrollment design display.
4. Click to select a step.
5. Click in the main pane to the right and the pane becomes active. The fields in the step display.
6. Click the field to be edited and the field's Properties pane displays. Edit the properties for the field as needed.
7. Link any unlinked fields created to a new or existing credential design. For instructions, refer to "Field Connections" on page 72.
8. Click **Save**  to save or **Close**  to exit without saving.





### Move a Field

Move a field from one location to another.

1. Click the **Enrollment Design**  icon in the left pane.
2. Click the arrow icon to expand the pane (if necessary).
3. Click the arrow icon next to Enrollment Design to expand the menu. The current steps for the enrollment design display.
4. Click a step to select it.
5. Click in the main pane to the right and the pane becomes active. Any existing fields in the step display.
6. Click and drag a field to a new location in the step.
7. Click **Save**  to save or **Close**  to exit without saving.




### Cut and Paste a Field

Cut a field and use it again in another location.

1. Select a field.
2. Click **Cut** .
3. Select a different location to reuse the field.
4. Click **Paste** .
5. Link any unlinked fields created to a new or existing credential design. For instructions, refer to "Field Connections" on page 72.
6. Click **Save**  to save or **Close**  to exit without saving.



## Delete Fields



Delete fields in the Enrollment Designer to possibly simplify the enrollment form.

1. Select a field.
2. Click Delete  next to the field name. Instant ID as a Service deletes the field.
3. Click **Save**  to save or **Close**  to exit without saving.

## Configure Text Fields

Text fields contain information about the Applicant, such as their name and an identification number. Follow these steps to configure Text fields on the enrollment design.

1. Select a Text field from steps in the enrollment design. The Text Field Properties pane opens.
2. Configure the General properties.
  - a. Enter a name for the field in the **Name** field.
  - b. Enter text to display in the field as an example in the **Sample Data** field.
  - c. To set the alignment of text in the field, select an option from the **Alignment** field.
  - d. To change the character limit of the field, modify the value in the **Input Length** field.
  - e. To move the field, modify the values in the **Left** and **Top** fields. The value in those fields represents the distance in pixels from the top-left corner of the enrollment design to the top-left corner of the field.
  - f. To adjust the width of the field, modify the value in the **Width** field.
  - g. To require a value in the field during enrollment, select **Mandatory**.
  - h. To prevent the field from being altered during enrollment, select **Read Only**.
  - i. To hide the field during enrollment, select **Hidden**. Instant ID as a Service will not show this field during enrollment.
3. Configure the Appearance properties.
  - a. To change the font family of the text in the field, select a font family from the **Font Family** list.
  - b. To change the size of the text in the field, modify the value in the **Font Size** field.
  - c. To set the text to bold, select Bold .
  - d. To set the text to italic, select Italic .

- e. To change the color surrounding the text, select a color from the **Fill** color selector.
  - f. To change the color of the text, select a color from the **Stroke** color selector.
4. Configure the Operator Prompt properties.
- a. To remove the operator prompt, clear the **Display an operator prompt** checkbox.
  - b. Enter text to identify the field in the **Operator Prompt** field.
  - c. To change the font family, select a font family from the **Font Family** list.
  - d. To change the size of the text, enter a new value in the **Font Size** field.
  - e. To set the text to bold, select Bold **B** .
  - f. To set the text to italic, select Italic **I** .
  - g. To change the color surrounding the text, select a color from the **Fill** color selector.
  - h. To change the color of the text, select a color from the **Stroke** color selector.
5. Click **Save**  to save or **Close**  to exit without saving.

### Configure Date Fields

Date fields gather dates from the enrollment process and ensure the date follows a selected date format. Configure Date fields to set the appearance and the date format for the field.

1. Select a Date field from the enrollment design. The Date Field Properties pane opens.
2. Configure the General properties.
  - a. Enter a name for the field in the **Name** field.
  - b. To set the alignment of text in the field, select an option from the **Alignment** field.
  - c. To change the character limit of the field, modify the value in the **Input Length** field.
  - d. To move the field, modify the values in the **Left** and **Top** fields. The value in those fields represents the distance in pixels from the top-left corner of the enrollment design to the top-left corner of the field.
  - e. To adjust the width of the field, modify the value in the **Width** field.
  - f. To require a value in the field during enrollment, select **Mandatory**.
  - g. To prevent the field from being altered during enrollment, select **Read Only**.

- h. To hide the field during enrollment, select **Hidden**. Instant ID as a Service will not show this field during enrollment.
3. Configure the Appearance properties.
    - a. To change the font family of the text in the field, select a font family from the **Font Family** list.
    - b. To change the size of the text in the field, modify the value in the **Font Size** field.
    - c. To set the text to bold, select Bold **B** .
    - d. To set the text to italic, select Italic **I** .
    - e. To change the color surrounding the text, select a color from the **Fill** color selector.
    - f. To change the color of the text, select a color from the **Stroke** color selector.
  4. Configure the Operator Prompt properties.
    - a. To remove the operator prompt, clear the **Display an operator prompt** checkbox.
    - b. Enter text to identify the field in the **Operator Prompt** field.
    - c. To change the font family, select a font family from the **Font Family** list.
    - d. To change the size of the text, enter a new value in the **Font Size** field.
    - e. To set the text to bold, select Bold **B** .
    - f. To set the text to italic, select Italic **I** .
    - g. To change the color surrounding the text, select a color from the **Fill** color selector.
    - h. To change the color of the text, select a color from the **Stroke** color selector.
  5. Configure the Advanced properties for the Date field.
    1. Select **Enforce input mask** to modify the date format for the field.
    2. From the **Date Format** list, select a format for the Date field. A wide variety of date formats are supported.

**Note:** If you are bulk importing enrollment records, only one date format is supported for the import process: yyyy-mm-dd hh:mm:ss. During the import, dates must be provided in this format. The dates are then automatically changed to reflect the format selected above when displayed on the user interface.
    3. From the **Time Format** list, select **None**, **12 hour format**, or **24 hour format**. Selecting **None** removes the time from the Date field.

6. Click **Save**  to save or **Close**  to exit without saving.

### Configure Photo Fields

Photo fields allow images of the user to be captured or uploaded. Follow these steps to configure Photo Fields.

1. Configure the General properties.
  - a. Enter a name for the field in the **Name** field.
  - b. To set the alignment of the photograph in the field, select an option from the **Alignment** field.
  - c. To move the field, modify the values in the **Left** and **Top** fields. The value in those fields represents the distance in pixels from the top-left corner of the Enrollment Design to the top-left corner of the field.
  - d. To adjust the size of the field, modify the values in the **Height** and **Width** fields.
  - e. To require a value in the field during enrollment, select **Mandatory**.
  - f. To prevent the field from being altered during enrollment, select **Read Only**.
  - g. To hide the field during enrollment, select **Hidden**. Instant ID as a Service will not show this field during enrollment.
2. Configure the Operator Prompt properties.
  - a. To remove the operator prompt, clear the **Display an operator prompt** checkbox.
  - b. Enter text to identify the field in the **Operator Prompt** field.
  - c. To change the font family, select a font family from the **Font Family** list.
  - d. To change the size of the text, enter a new value in the **Font Size** field.
  - e. To set the text to bold, select Bold **B** .
  - f. To set the text to italic, select Italic **I** .
  - g. To change the color surrounding the text, select a color from the **Fill** color selector.
  - h. To change the color of the text, select a color from the **Stroke** color selector.
3. Configure the Capture Options
  - a. Select **Enable Capture from File** to allow Operators to upload a photograph of the Applicant.



- b. Select **Enable Capture from Device** to allow Operators to capture a photograph of the Applicant using a web camera.
3. Select one of the Cropping options for the photograph field:
  - **No Crop Box**: After capturing a photograph, Instant ID as a Service does not apply a crop box with a set size. The Operator can draw a crop box on the photograph.
  - **Crop Box with Shape of this Field**: Sets the crop box to the same height and width as the Photo field. This ensures that the photograph fits in the field while maintaining the aspect ratio of the field.
  - **Crop Box With Shape**: Sets the crop box to a specific height and width. Enter values in the **Height** and **Width** fields to set the size of the crop box.
4. To enable Auto Crop, select **Auto Crop** then enter a value in the **Crop Area** field.

**Note:** For more information on the Capture Options, refer to "Capture Options" below.

4. Click **Save**  to save or **Close**  to exit without saving.

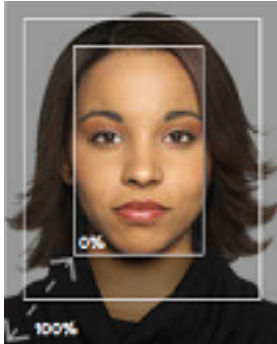
#### Capture Options

The Capture Options set how photographs are captured during enrollment. The options also set which options are available to the Operator when capturing a photograph.

- **Enable Capture from File**: Allows the Operator to upload a photograph of the Applicant from the local file system.
- **Enable Capture from Device**: Allows the Operator to capture a photograph of the Applicant using a camera.
- **Image Rotation**: Automatically rotates the photograph clockwise after capture. Options include 0, 90, 180, and 270 degrees.
- **Cropping**: Options in this area set the cropping options available to the Operator.
  - **No Crop Box**: Instant ID as a Service does not automatically apply a crop box over the photograph. The Operator must draw a crop box over the image to crop it.
  - **Crop Box with Shape of this Field**: Sets the height and width of the crop box to match the height and width of the Photo field. This ensures that the photograph will properly fit in the field.
  - **Crop Box with Shape**: Sets the height and width of the crop box to the values in the **Width** and **Height** fields.
  - **Auto Crop**: Instant ID as a Service automatically crops the image around the Applicant's face. For more information, refer to "Auto Crop Example" on the next page.

## Auto Crop Example



After capturing a photograph, Instant ID as a Service detects the Applicant's face then crops the photograph to include the Applicant's face and some of the surrounding area. The Crop Area value sets amount of surrounding area included in the photograph. For example, a value of 0 includes only the Applicant's face. A value of 100 includes the Applicant's face and some of the surrounding area including the Applicant's hair. Refer to the image below for an example.



### Configure Signature Fields

Signature fields provide options to upload or capture a signature from the Applicant. Follow these steps to customize the Signature field for the enrollment process.

1. Select the step that contains the Signature field. By default, the step is called **Capture a Signature**.
2. Select the Signature field. The Signature Field Properties pane opens.
3. Configure the General properties.
  - a. Enter a name in the **Name** field to change the name of the Signature field.
  - b. To change where in the field the signature appears, select an alignment from the **Alignment** field.
  - c. To adjust the size of the field, modify the values in the **Height** and **Width** fields.
  - d. To move the field, modify the values in the **Left** and **Top** fields. The value in those fields represents the distance in pixels from the top-left corner of the Enrollment Design to the top-left corner of the field.
  - e. To require a value in the field during enrollment, select **Mandatory**.
  - f. To prevent the field from being altered during enrollment, select **Read Only**.
  - g. To hide the field during enrollment, select **Hidden**. Instant ID as a Service will not show this field during enrollment.



4. Configure the Operator Prompt properties.
  - a. To remove the operator prompt, clear the **Display an operator prompt** checkbox.
  - b. Enter text to identify the field in the **Operator Prompt** field.
  - c. To change the font family, select a font family from the **Font Family** list.
  - d. To change the size of the text, enter a new value in the **Font Size** field.
  - e. To set the text to bold, select Bold **B** .
  - f. To set the text to italic, select Italic **I** .
  - g. To change the color surrounding the text, select a color from the **Fill** color selector.
  - h. To change the color of the text, select a color from the **Stroke** color selector.
5. Configure the Capture Options.
  - Select **Enable Capture from File** to allow Operators to upload an image of the Applicant's signature.
  - Select **Enable Capture from Device** to allow Operators to capture the Applicant's signature using a mouse or touch screen.
6. Click **Save**  to save or **Close**  to exit without saving.

### Add or Configure Enrollment Design Steps








The enrollment designer includes options to name or change the name of steps, move steps, copy and paste steps, delete steps, and configure the Job name identifier.

#### Add Steps

To add steps:




1. Click the **Enrollment Design**  icon in the left pane.
2. Click the arrow icon to expand the pane (if necessary).
3. Click the arrow icon next to Enrollment Design to expand the menu. The default steps for the enrollment design display, including a step called "Blank."
4. Click the **Add**  icon next to any of the steps to add that step to the sequence and start configuring the step. Note that default steps will have some information pre-populated. To configure the step:
  - a. Click in the main pane to the right and the pane becomes active.
  - b. Click in the field for the step name and enter the name.
  - c. Add specific step fields by clicking the icon for the type needed and the clicking again in the location where the field should be placed. Note that fields can

be clicked-and-dragged to specific locations.

- i. **Text**  : Adds a text field.
  - ii. **Photo**  : Adds a photo field.
  - iii. **Date**  : Adds a date field.
  - iv. **Signature**  : Adds a signature field.
  - v. **Auto Sequence**  : Adds an auto-sequence field.
- d. Click each field and the field's Properties pane displays. Edit the properties for the field as needed.
5. Click **Save**  to save or **Close**  to exit without saving.




### Edit Steps

To edit steps:

1. Click the **Enrollment Design**  icon in the left pane.
2. Click the arrow icon to expand the pane (if necessary).
3. Click the arrow icon next to Enrollment Design to expand the menu. The current steps for the enrollment design display.
4. Click to select a step.
5. Click in the main pane to the right and the pane becomes active. The fields in the step display.
6. Edit the properties for the step as needed.
7. Click **Save**  to save or **Close**  to exit without saving.





### Reorder Steps

Reorder the steps on the enrollment form.

1. Click the **Enrollment Design**  icon in the left pane.
2. Click the arrow icon to expand the pane (if necessary).
3. Click the arrow icon next to Enrollment Design to expand the menu. The current steps for the enrollment design display.
4. Click and drag a step to a new location in the sequence.
5. Click **Save**  to save or **Close**  to exit without saving.






### Cut and Paste a Step

Cut a step and use it again in another location.

1. Select a step.
2. Click **Cut** .
3. Select a different location to reuse the step.
4. Click **Paste** .
5. Click **Save**  to save or **Close**  to exit without saving.



### Delete Steps

Delete steps in the Enrollment Designer to possibly simplify the enrollment form. Instant ID as a Service prevents steps with fields to be deleted. Before deleting a step, you must move all fields on the step to a different step.

1. Move all fields on the step to another step.
  - a. Select a field on the step.
  - b. Click **Cut** .
  - c. Select a different step in the Enrollment Design.
  - d. Click **Paste** . Instant ID as a Service places the field on the step.
  - e. Move the field on the step.
2. Click Delete  next to the step name. Instant ID as a Service deletes the step.
3. Click **Save**  to save or **Close**  to exit without saving.

### Configure the Job Name Identifier

The Job Name Identifier is the name displayed for print jobs initiated using the enrollment. Instant ID as a Service includes options to use the enrollment design name or a value from a field on the enrollment design.



1. Select the **Preview and Print** step or, if the name has changed, the last step in the Enrollment Design.
2. To use the Enrollment Design name as the Job Name Identifier, select **Enrollment Name and Timestamp**.
3. To use a value from a field as the Job Name Identifier, select **Enrollment Fields** then select a field from the list.
4. Click **Save**  to save or **Close**  to exit without saving.

## Configure Enrollment Design Settings

The enrollment design settings set the description for the enrollment design and the tab order for the fields during enrollment.



### Set or Change the Tab Order

Tab order determines which field is selected after pressing the Tab key.

1. Click Settings  in the left pane. The Enrollment Design settings page opens.
2. From the Tab Order list, select one of the following options:
  1. **Horizontal**: Pressing Tab selects the field to the right of the currently selected field. If the selected field is at the right end of a row, pressing Tab selects the first field in the next row.
  2. **Vertical**: Pressing tab selects the field below the currently selected field. If the selected field is at the bottom of a column, pressing Tab selects the first field in the column to the right.
3. Click **Save** .





### Add a Description

Add a description to the enrollment design to provide more information about the enrollment design.

1. Click Settings . The Enrollment Design settings page opens.
2. Add a description to the **Description** field.
3. Click **Save** .

## Configure Enrollment Search Settings

The enrollment search settings control the fields displayed as columns when searching for enrollments. It also sets the order of the columns. By default, Instant ID as a Service displays all fields.

1. Click Search Settings . The Search Settings page opens.
2. To remove a field, select it from the **Configured fields** list then click **Remove**.
3. To add a field, select it from the **Supported fields** list then click **Add**.
4. To change the order of fields, select a field from the **Configured fields** list then click Up  to move it up or click Down  to move it down the order.
5. Click **Save** .

# Design Mobile Flash Passes

Mobile Flash Passes are digital credentials that contain information about the applicant to identifying the applicant or gaining access to an area. Mobile Flash Passes require the use of either Google Pay or Apple Wallet.



## Mobile Flash Pass Process



Follow this process to configure, enable, and issue Mobile Flash Passes:

1. Enable Mobile Flash Passes. This task is performed by an Administrator-level user. For instructions, refer to "Configure and Enable Mobile Flash Pass" on page 141.
2. Create a Credential Design and generate an enrollment form. For instructions, refer to "Design a Credential" on page 25.  
**Note:** The credential design must have a single field containing the full name of the applicant. This allows the full name of the applicant to map to a field on the Mobile Flash Pass.
3. Create a Mobile Flash Pass Design. Mobile Flash Pass Designs set the appearance and functionality of Mobile Flash Passes. For instructions, refer to "Create a Mobile Flash Pass Design" below.
4. Map fields from the Credential Design to the Mobile Flash Pass Design. For instructions, refer to "Map Fields to Mobile Flash Pass" on page 71.
5. Customize the Mobile Flash Pass email template with information that assist the applicant to add the Mobile Flash Pass to their Google Pay or Apple Wallet accounts. For instructions, refer to "Customize Email Templates" on page 22.
6. Enroll an applicant and issue a Mobile Flash Pass. For instructions, refer to "Enroll Applicants" on page 75.




## Create a Mobile Flash Pass Design

A Mobile Flash Pass design sets the appearance and functionality of Mobile Flash Passes. Follow these steps to create a Mobile Flash Pass design.

1. From the Main Menu , select **Mobile Flash Pass Designs**. The Mobile Flash Pass Designs page opens.
2. Click Add . The Add Mobile Flash Pass Design page opens.
3. In the **Name** field, type a name for the Mobile Flash Pass Design. This name identifies the Mobile Flash Pass Design in Instant ID as a Service.
4. In the **Mobile Flash Pass Title** field, type a title for the Mobile Flash Pass. This title will display on the Mobile Flash Pass.



5. From the **Barcode Type** list, select a barcode format. This sets the format of the barcode that displays on the Mobile Flash Pass.
6. Select a color from the color selector in the **Background Color** area. This color displays as the background color of the Mobile Flash Pass.
7. Upload a logo to display on the Mobile Flash Pass.
  - a. Click Add . The Upload Logo dialog box opens.
  - b. Click Upload . A file browser opens.
  - c. Open an image. The Upload Logo dialog box previews the logo.
  - d. (Optional) Use the zoom slider to adjust the size logo inside the frame.
  - e. Click **OK**. The Add Mobile Flash Pass page displays the logo as it will appear in Google Pay and Apple Wallet.
  - f. Review the image. If it appears incorrect, correct the image or upload a new image.
8. Enter information on the company issuing the Mobile Flash Pass.
  - a. In the **Company Name** field, type the name of the company or organization issuing the Mobile Flash Pass.
  - b. In the **Company Address** field, type the address of the company or organization.
  - c. In the **Support Email** field, type an email address for the applicant to contact in case of an issue.
  - d. In the **Support Phone** field, type a phone number that the applicant to contact in case of an issue.
  - e. In the **Website** field, type the website address for the company. Use an address where the user can find support information.
  - f. In the **Legal Information** field, type a message that provides instructional information in case of an issue.
9. (Optional) Apply a security watermark to add an watermark image over the applicant photograph. Including a watermark makes it more difficult to counterfeit the Mobile Flash Pass.
  - a. Select **Apply Security Watermark**. Security watermark settings display.
  - b. Upload a watermark image. Select an image that is 200 by 200 pixels and has a transparent background.



- i. Click Add . The Upload Image dialog box opens.
  - ii. Click Upload  then select an image. The image displays in the preview frame.
  - iii. Adjust the image by clicking and dragging the image and adjusting the zoom slider.
  - iv. Click **OK**.
- c. From the **Watermark Position** list, select the position of the watermark on the applicant photograph.
  - d. From the **Watermark Size** list, select the size of the watermark. The percent shown represents the width of the watermark in relation to the width of the applicant photograph.
  - e. From the **Opacity Strength** list, select the opacity of the watermark.
  - f. Select **Overlap Background** to extend the watermark on to the background of the Mobile Flash Pass. This makes it more difficult to counterfeit the Mobile Flash Pass.
10. Click **Save**.
  11. To test the Mobile Flash Pass Design, click **Send Email**  on the Mobile Flash Pass Designs page. Instant ID as a Service sends a test email containing a test version of the Mobile Flash Pass.

## Map Fields to Mobile Flash Pass

To add information gathered during enrollment to a Mobile Flash Pass, map fields on the Credential Design to fields on the Mobile Flash Pass. After enrolling the applicant, Instant ID as a Service adds the information from the enrollment form to the Mobile Flash Pass.

1. From the Main Menu , select **Credential Designer**. The Credential Designs page opens.
2. Click **Setup**  next to a Credential Design. The Configure Mobile Flash Pass dialog box opens.
3. From the **Mobile Flash Pass Design** list, select a Mobile Flash Pass Design.
4. From the **Full Name** list, select a field on the Credential Design that contains the applicant's full name.
5. From the **Email Address** list, select a field on the Credential Design that contains the applicant's email address.
  - To select an email address on the credential design, select that field from the **Email Address** list.



- To create a new field for the email address, select **<Auto Generate Field>**.
6. Map other fields to the Mobile Flash Pass.
    - a. From the **User Photo** list, select a photograph field that contains a photograph of the applicant.
    - b. From the **User Role** list, select a field that contains the role of the applicant in the organization.
    - c. From the **User Number** list, select a field that contains the ID number of the applicant.
    - d. From the **Barcode Value** list, select a field that contains data that will be converted to a barcode on the Mobile Flash Pass.
    - e. From the **Since Date** list, select a date field that contains the date when the applicant was added to the organization. This field must map to a Date field on the credential design.
    - f. From the **Expiry Date** list, select a date field that contains the date when the credential or the applicant's membership in the organization expires. This field must map to a Date field on the credential design.
  7. Click **Submit**.

## Field Connections

Field connections connect fields in a credential design or mobile flash pass design to fields in the enrollment design. Data entered during enrollment populates the connected field on the credential design or mobile flash pass.

### Edit Credential Design Field Connections



Instant ID as a Service connects fields on a credential design to fields on an enrollment design when the user generates an enrollment design from a credential design. Instant ID as a Service supports connecting only one credential design to one enrollment design. To modify the fields connections between a credential design and an enrollment design, follow these steps.

1. From the Main Menu , select **Enrollment Designs**. The Enrollment Designs page opens.
2. Select **Field Connections**  to edit the field connections for that enrollment design. The Field Connections page opens.
3. From the **Source** list, select **Credential Design**.
4. From the **Credential Design** list, select a credential design.

5. For each field in the **Credential Design** column, select a field from the **Enrollment Design** column.
6. Click **Save**.

## Configure Mobile Flash Pass Field Connections

Use field connections to connect fields on a mobile flash pass to fields on an enrollment design. When completing enrollment, the operator will enter data in the fields. That data populates the connected field on the mobile flash pass. Instant ID as a Service supports connecting only one mobile flash pass to one enrollment design.

1. From the Main Menu , select **Enrollment Designs**. The Enrollment Designs page opens.
2. Select **Field Connections**  to edit the field connections for that enrollment design. The Field Connections page opens.
3. From the **Source** list, select **Mobile Flash Pass Design**.
4. From the **Mobile Flash Pass Design** list, select a mobile flash pass.
5. For each field in the **Mobile Flash Pass Design** column, select a field from the **Enrollment Design** column.
6. Click **Save**.

# Operator

Issuance Operators use enrollment forms to enroll applicants and issue credentials. The following are typical tasks performed by the Issuance Operator user:

- "The Enrollment Process" below
- "Enroll Applicants" on the next page
- "Monitor Printing" on page 145

## The Enrollment Process

Follow the enrollment process to gather information from the applicant, enter the information in an enrollment form, then issue a credential. The steps included in the enrollment process are dependent on the fields on the credentials design. For example, if the credential design contains a photograph field the enrollment will contain the Capture a Photograph step. If the credential design does not contain a photograph field, the enrollment will not contain the Capture a Photograph step. This page describes the enrollment process for a credential design that contains personal information, Photograph, and Signature fields.

### 1. Enter Applicant Information

The Personal Information page of the Create Enrollment wizard contains fields that correspond to dynamic fields on the credential design. This can be text fields that contain any text information such as the name of the applicant or their department. It also contains date fields for possibly entering the birth date of the applicant or the issue date of the credential.

For instructions, refer to "Enter Applicant Information" on page 76.

### 2. Capture a Photograph

The Photograph field displays an image of the applicant on the credential. Instant ID as a Service uses a web camera configured on the browser to capture the photograph.

For instructions, refer to "Capture a Photograph" on page 77.

### 3. Capture Signature

The Signature field allows the signature of the applicant to appear on the credential and reside, for the record, in the Instant ID as a Service database. The applicant uses a mouse to draw their signature into the Create Enrollment wizard.

For instructions, refer to "Capture a Signature" on page 78.





### 4. Finalize and Issue Credentials

After gathering information, capturing photographs, and capturing signatures, Instant ID as a Service shows a preview of the final credential. Review the credential to ensure that it contains all of the information that is required for the credential.

For instructions, refer to "Finalize and Issue Credentials" on page 80.

## Enroll Applicants



The steps required to enroll an applicant change depending on the fields on the credential used to enroll an applicant.

1. Select Main Menu  > **Credentials**. The Credentials page opens displaying the credentials available for enrolling an applicant.
2. Click Enroll  for a credential. The Create Enrollment page opens to the Personal Information tab.
3. Enter information specific to the applicant in the fields. For more information on personal information fields, refer to "Enter Applicant Information" on the next page.
4. Click **Next**. The Capture a Photograph tab opens if the credential design contains a Photograph field.
5. Capture a photograph of the applicant.
  - Click **Capture**  then capture a photograph of the applicant using a web camera.
  - Click **Upload**  then select a photograph of the applicant.

For more information on capturing a photograph, refer to "Capture a Photograph" on page 77.

6. Click **Next**. The Capture a Signature tab opens if the credential contains a signature field.

7. Capture a signature.

- Click Capture  then instruct the applicant to sign in the signature field using the mouse.
- Click Upload  then select a signature image file.


For more information, refer to "Capture a Signature" on page 78.

8. Click **Next**. The Preview and Print tab opens.
9. Review the credential. Ensure that the applicant information appears correctly on the credential.
10. To save the enrollment to the database, click **Save**.
11. To print the credential and save the enrollment to the database, click **Save and Print**.

## Enter Applicant Information

The Personal Information page of the Create Enrollment wizard contains fields that correspond to fields on the credential design that contain information about the applicant. This can be text fields that contain any text information such as the name of the applicant or the department of the applicant. It also contains the date fields for possibly entering the birth date of the applicant or the issue date of the credential.

With the Personal Information tab open in the Create Enrollment wizard follow these steps to enter information specific to the applicant.

1. Type information into text fields. Text fields might include: Name, Last Name, Department, or Role.
2. Enter a date into Date fields. Date fields might include: Date of Birth, Issuance Date, or Start Date.
  - a. Click **Enter Date**  . The Calendar widget opens.
  - b. To change the month, click on the right or left arrows next to the current month.
  - c. To change the year, click the current year at the top of the calendar widget.
  - d. Select a date from the Calendar widget. The Calendar widget closes and the Create Enrollment wizard displays the selected date in the field.
3. Click **Next**.

Next step: "Capture a Photograph" on the next page

## Capture a Photograph

The Photograph field displays an image of the applicant on the credential. Instant ID as a Service uses a web camera through the browser to capture the photograph. With the Capture a Photograph tab open, follow these steps to capture a photograph of the applicant.

### Take a Photograph Using a Web Camera

Follow these steps to capture a photograph of the applicant using a web camera configured on the browser.

1. To enable automatic cropping of the photograph, select **Auto Crop**.

2. Click Capture . The Capture Photograph dialog box opens.

**Note:** For the first capture, you might need to grant the browser access to the camera.

3. Tap Capture . The Capture Photograph dialog box opens.


**Note:** The browser might request access to the camera on the mobile device. Allow the browser to access your camera to continue.

4. Adjust the web camera to position the applicant in the frame. Or, instruct the applicant to move within the frame so that the applicant's image covers most of the frame.
5. Click **Capture**. Instant ID as a Service takes a photograph of the applicant.

**Note:**

If Auto Crop is enabled, Instant ID as a Service detects the face of the applicant in the photograph and crops the image. If Instant ID as a Service cannot locate a face in the photograph, it instructs you to manually crop the photograph.

6. Manually crop the photograph.

- a. Click Edit .
- b. Position the cropping frame on the photograph. If Auto Crop is disabled, click and drag on the image to position the cropping frame.
- c. Click **Crop**.


**Note:** The photograph field on the credential design sets the aspect ratio of the photograph on the credential.

7. Click **Next**.

## Upload a Photograph of the Applicant

Follow these steps to upload an existing photograph of the applicant.

1. To enable automatic cropping of the photograph, select **Auto Crop**.

2. Click Upload . The Open dialog box opens.

3. Tap Upload .

**Note:** The browser might request access to the file system on the mobile device.

Allow the browser to access the file system on the mobile device to proceed.

4. Select an image file from the file system.
5. Click **Open**. Instant ID as a Service loads the image file into the photograph field.

**Note:**

If Auto Crop is enabled, Instant ID as a Service detects the face of the applicant in the photograph and crops the image. If Instant ID as a Service cannot locate a face in the photograph, it instructs you to manually crop the photograph.

6. Manually crop the photograph.

- a. Click Edit .

- b. Position the cropping frame on the photograph. If Auto Crop is disabled, click and drag on the image to position the cropping frame.

- c. Click **Crop**.

**Note:** The photograph field on the credential design sets the aspect ratio of the photograph on the credential.

7. Click **Next**.


Next Step: "Capture a Signature" below

## Capture a Signature

The Signature field allows the signature of the applicant to appear on the credential. The applicant uses a mouse to draw their signature into the Create Enrollment wizard. Follow these steps to capture a signature from the applicant.

### Capture a Signature from the Applicant

Follow these steps to capture a signature from the applicant.

1. Click Capture . The Capture Signature dialog box opens.
2. Instruct the applicant to sign in the signature box using the mouse.



3. Instruct the applicant to sign in the signature box using their finger.
4. Click **Capture**. The signature displays on the Create Enrollment wizard.
5. Click **Next**.

### Upload a Signature Image

Follow these steps to upload an image containing the applicant's signature.

1. Click Upload . The Open dialog box opens.

2. Tap Upload .

**Note:** The browser might request access to the file system on the mobile device.

Allow the browser to access the file system on the mobile device to proceed.

3. Select an image file that contains the signature.
4. Click **Open**. Instant ID as a Service loads the image file.
5. Click **Next**.

Next Step: "Finalize and Issue Credentials" on the next page

### Issue Mobile Flash Passes

Mobile Flash Passes are digital credentials that contain all information for the applicant and a barcode for identifying the user and gaining access to an area. Flash Passes require the use of either Google Pay or Apple Wallet. Follow these steps to issue a Mobile Flash Pass.

To enable Mobile Flash Passes, enable and configure Mobile Flash Passes then Design and Map Mobile Flash Passes. Refer to the following pages for instructions:

- "Configure and Enable Mobile Flash Pass" on page 141
- "Design Mobile Flash Passes" on page 69

### Requirements for the Applicants

Ensure that the applicant is familiar with the requirements and is able to add the Mobile Flash Pass to their device. The applicant must have a device that meets the following requirements:

- Apple or Google account
- Apple Wallet or Google Pay installed

## Issue a Mobile Flash Pass

Follow these steps to complete the Mobile Flash Pass tab to issue a Mobile Flash Pass to the Applicant.

1. In the **Email Address** field, enter the email address for the applicant. Instant ID as a Service sends the Mobile Flash Pass email to this address.
2. Instruct the applicant of the process for adding the Mobile Flash Pass to their device.
3. Click **Send Mobile Flash Pass**. Instant ID as a Service sends the Mobile Flash Pass to the applicant.

## Finalize and Issue Credentials

After gathering information, capturing photographs, and capturing signatures, Instant ID as a Service shows a preview of the final credential. Review the credential to ensure that it contains all of the information that is required for the credential. If the credential is incorrect, follow these steps to correct the enrollment or to correct the credential design.

1. Review the preview of the credential displayed on the Preview and Print tab.
2. To correct any errors in the data entered during enrollment, navigate back to the previous tabs in the Create Enrollment wizard and correct the information.
3. Click **Save** to save the enrollment to Instant ID as a Service.
4. Click **Save and Print** to save the enrollment and print the credential.




## Manage Enrollment Records

Enrollment records contain all the information gathered during enrollment. The Search Enrollments page provides the tools to view and edit enrollment records. It also include the option to print a credential from an existing enrollment record allowing the operator to reprint a credential for an applicant. Refer to the following pages for more information:

- "Search Enrollments" below
- "Edit Enrollment" on the next page
- "Print From Enrollment Search" on the next page
- "Delete Enrollment Records" on page 82
- "Send Mobile Flash Pass Email" on page 83



## Search Enrollments

The Credentials page includes the option to search for enrollments created for a credential.

1. Select Main Menu  > **Credentials**. The Credentials page opens.
2. Click **Search**  in the area for a credential. The Search Enrollment page opens and lists all of the enrollments for the credential.
3. Click **Filter Search** . The Search Panel dialog box opens. The Search Panel dialog box contains fields for each text field on the credential.
4. Enter text in a field to search the enrollments for text in the matching field on the credential.  
For example, enter a name in the **Name** field to search the enrollments for that name.
5. Click **Search**. Instant ID as a Service searches for enrollments that match the search criteria.

## Edit Enrollment

After enrolling an applicant, Instant ID as a Service saves the enrollment information. Instant ID as a Service includes options to edit the information for enrollment after the issuing a credential to the applicant. Do this to update applicant information, correct information, or add missing information. Follow these steps to edit an enrollment.




1. Select **Main Menu**  > **Credentials**. The Credentials page opens.
2. Click **Search**  in the area for a credential. The Search Enrollment page opens and lists all of the enrollments for the credential.
3. (Optional) Filter the enrollment list using search terms. For more information, refer to "Search Enrollments" on the previous page.
4. Click on a row to open the enrollment in the Create Enrollment wizard.
5. Modify the information in the enrollment. For more instructions on using the Create Enrollment wizard, refer to "Enroll Applicants" on page 75.
6. Click **Save** to save the changes to Instant ID as a Service.
7. Click **Print** to print a new credential and save the changes to Instant ID as a Service.

## Print From Enrollment Search

The Search Enrollment page includes options to print a credential. Print a new credential for an applicant if they require a new credential for any reason.




### Print a Credential

Follow these steps to print individual credentials.

1. Select Main Menu  > **Credentials**. The Credentials page opens.
2. Click **Search**  in the area for a credential. The Search Enrollment page opens and lists all of the enrollments for the credential.
3. (Optional) Filter the enrollment list using search terms. For more information, refer to "Search Enrollments" on page 80.
4. Click **Print**  in a row for a credential. The Printers dialog box opens.
5. Select a printer from the **Printers** list.
6. Select a hopper from the **Hoppers** list.
7. Click **Print**. Instant ID as a Service prints the credential.

### Print Multiple Credentials

Follow these steps to print multiple credentials.




1. Select Main Menu  > **Credentials**. The Credentials page opens.
2. Click **Search**  in the area for a credential. The Search Enrollment page opens and lists all of the enrollments for the credential.
3. (Optional) Filter the enrollment list using search terms. For more information, refer to "Search Enrollments" on page 80.
4. Select the check box next to the credentials to print.
5. Click **Print**  at the top of the table. The Printers dialog box opens.
6. Select a printer from the **Printers** list.
7. Select a hopper from the **Hoppers** list.
8. Click **Print**. Instant ID as a Service prints the credentials.

### Delete Enrollment Records

Delete enrollment records if they are no longer needed or are incorrect.




#### Delete an Enrollment Record

Follow these steps to delete a single enrollment record.

1. Select **Main Menu**  > **Credentials**. The Credentials page opens.
2. Click **Search**  in the area for a credential. The Search Enrollment page opens and lists all of the enrollments for the credential.
3. Click **Delete** . The Delete Enrollment confirmation opens.
4. Click **Delete**. Instant ID as a Service deletes the enrollment record.




#### Delete Multiple Enrollment Records

Follow these steps to delete multiple enrollment records.

1. Select **Main Menu**  > **Credentials**. The Credentials page opens.
2. Click **Search**  in the area for a credential. The Search Enrollment page opens and lists all of the enrollments for the credential.
3. Select the check box next to all enrollments to be deleted.
4. Click **Delete**  above the enrollment record table. The Delete Enrollment confirmation opens.
5. Click **Delete**. Instant ID as a Service deletes the enrollment records.

## Send Mobile Flash Pass Email

After enrolling an applicant using an enrollment with mobile flash pass enabled, Instant ID as a Service sends an email to the applicant that contains a link to retrieve their mobile flash pass. Send the mobile flash pass email to any users with an email address from Search Enrollment page.

1. Select Main Menu  > **Credentials**. The Credentials page opens.
2. Click **Search**  in the area for a credential. The Search Enrollment page opens and lists all of the enrollments for the credential.
3. (Optional) Filter the enrollment list using search terms. For more information, refer to "Search Enrollments" on page 80.
4. Select the check box for each enrollment record to be sent a mobile flash pass email.
5. Click **Send Mobile Flash Pass** . The Send Mobile Flash Pass dialog box opens.
6. Click **Send**. Instant ID as a Service sends the mobile flash pass email to the applicants.

### Related links:

- "Customize Email Templates" on page 22
- "Configure and Enable Mobile Flash Pass" on page 141

## Manage the Print Queue

The Print Queue displays print jobs for all printers visible to the current user.

### Printer Statuses




After submitting a print job, the Print Queue page displays the print job and its status. The status of the print job indicates the current state of the print job. Below is a list of the

possible print job statuses.

- **Queued:** Instant ID as a Service sent the print job to the printer.
- **In Progress:** The printer is preparing and printing the credential.
- **Failed:** The printer encountered an error causing the print job to fail.
- **Waiting for Smartcard:** The printer is waiting on information provided by the smart car reader.

## View Print Jobs

The Print Queue displays print jobs for all printers visible to the current user. Follow these steps to view the Print Queue page to monitor print jobs.

1. From the Main Menu , click **Print Queue**. The Print Queue page opens.
2. Click on a column title to sort the column in descending or ascending order.
3. To filter print jobs:
  - a. Click **Filter** . The Filter print jobs dialog box opens.
  - b. In the **Printer name** field, enter the name of a printer name to filter the print job list based on the printer.
  - c. In the **Print job name** field, enter text to filter the print job list based on the print job name.
  - d. Click **Search**. Instant ID as a Service filters the print job list based on the criteria.
4. Click **Reset**  to reset the filters applied the list of print jobs to the default filters.

## Delete Print Jobs

Delete a print job to clear it from the list of print jobs. Instant ID as a Service allows only print jobs with Waiting or Stopped statuses to be deleted.

To delete a print job, click **Delete** .

# Administrator

Issuance Administrators create additional users, manage resources, and setup printers. They are also able to perform all other tasks available in Instant ID as a Service including designing credentials and enrolling applicants.

- "Manage Authenticators" below
- "Manage Resources" on page 105
- "Manage Reports" on page 111
- "Manage Users" on page 113
- "Printer Management" on page 123
- "Design a Credential" on page 25
- "Enroll Applicants" on page 75

## Manage Authenticators

An authenticator is a security measure that protects an application from unauthorized access. Authenticators require that a user respond to a challenge in order to gain access to the application. You assign authenticators to users to allow them to access applications protected by Instant ID as a Service.

Consider the following when assigning authenticators to users:

- A user can be assigned multiple authenticators.
- A user must have at least one authenticator assigned to them in order to log in to Instant ID as a Service.
- A user can choose to receive their OTP by voice, email, or SMS if they have a phone number, email address, or mobile device registered to their account.
- Assigned Entrust Soft Token must have a token state (either Active or Inactive). Only Entrust Soft Tokens in an Active state can be used for authentication.
- The resource rule associated with an application determine which authenticators can be used to log in to an application.

## Authenticator Lockout Behavior

The authenticators allowed to access applications are set by the resource rules (see Create resource rules). If a user enters an incorrect authenticator response more times than the value set in the **Lockout Count** (Refer to "Manage General Authenticator Settings" on the next page), the authenticator is locked and the user cannot access the application using that authenticator.

Consider this example:

1. A user has access to two applications, Application 1 and Application 2.
2. The resource rule for Application 1 requires password + OTP or Entrust Soft Token.
3. The resource rule for Application 2 allows Entrust Soft Token only.
4. The Lockout Count is set to 5.
5. The user accesses Application 1 and enters a valid password, but enters in incorrect Entrust Soft Token response 5 times, which locks the Entrust Soft Token authenticator.
6. The user can still access Application 1 using the correct password and a valid OTP.
7. The user cannot access Application 2 because it requires Entrust Soft Token authentication but the user has locked their Entrust Soft Token authenticator.

## Assigning User Authenticators

This section describes how to set up and assign user authenticators. and how to authenticate with them.

Topics in this section:

- "Manage General Authenticator Settings" below
- "Manage One Time Password (OTP) Settings" on page 88
- "Manage Temporary Access Codes" on page 89
- "Manage Password Settings" on page 91
- "Manage Entrust Soft Token" on page 99

## Manage General Authenticator Settings

After you create a user, you must assign the user authenticators. The user respond to authentication challenges to access Instant ID as a Service. The General settings set the conditions for authenticators and whether a user is automatically assigned certain authenticators when their account is created. While you can modify the General Settings at any time, you may want to configure the settings before you create new users or assign users additional authenticators. For example, you can set the General Settings to automatically assign an Entrust Soft Token to a user or automatically create a password for the user.

**Note:** If you are configuring Instant ID as a Service to synchronize users from Active Directory (AD), configure the Lockout Count and Lockout Lifetime settings to match the values used in your AD configuration.

### Manage General Settings

Follow these steps to configure general settings for the user currently logged on.

1. Click Main Menu  **Administration > Settings > General**. The **General** page appears.



2. Set **Lockout Count** to the number of times a user can fail an authentication challenge before being locked out of their account.
3. From the **Lockout Mode** list, select how Instant ID as a Service locks out an account.
  - Select **Authenticator** to lockout just the authenticator type used when the lockout happened. After a lockout, the user can use another authenticator type to log in.
  - Select **User** to lock out the user. That user will not be able to log in using any authenticator type.
4. Set **Lockout Lifetime** to the number of seconds before the lockout expires. After the Lockout Lifetime expires, a user can attempt to authenticate again. A value of 0 means the account remains locked until unlocked by an administrator.
5. Enter the **Authentication Session Lifetime** to set the time limit before an authenticated user needs to reauthenticate. The maximum value is 3600 (1 hour). The default is 900 seconds.
6. Enter the **Push Authentication Lifetime** to set the time limit a user has to respond to a soft token challenge notification by selecting **Confirm**, or **Cancel**.
7. From the **Automatic Authenticator** drop-down list, select the type of authenticator that is automatically assigned to a newly-created user.
8. Select **Entrust Soft Token** if you want your users to activate by email.
9. Select **None** if you require your users to register, you are manually assigning authenticators to your users, or you have email system attributes enabled for OTP authentication.
10. Set **Maximum Tokens Per User** to the maximum number of tokens a user can have. The maximum value is 10.
11. Select **Create Password** to automatically create a password for new users.
12. Enable Cross-Origin Resource Sharing (CORS) to allow other origins to make API calls to your account:
  - a. Select **Enable CORS**.
  - b. Click **Add**. Enter the allowed origin. Origins have the following options and limitations:
    - The origin must be in the following format: <http | https> "://" <host-name> [ ":" <port> ]
    - Origins must begin with HTTP or HTTPS
    - You can use the localhost for development purposes; however, Entrust does not recommend using it for production environments.
    - HTTP is the only supported protocol for localhost.Limitations:
    - The hostname value cannot include a wildcard (for example, https://\*mydomain.com)
    - The port supports the \* wildcard (for example, https://www.test.com:\*)

- If a port value is not provided, the default ports are used: port 80 for HTTP and port 443 for HTTPS.
- c. Repeat step b to add more allowed origins.

**Note:** When you add CORS values, it automatically adds the CORS Redirect URI to OIDC applications.

13. Click **Save**.


## Manage One Time Password (OTP) Settings

A one time password (OTP) authenticator is a random series of characters that are sent to the mobile device number or email address of a user during authentication. For OTP to be available, a user must have a value set for at least one of the following system attributes:

- Email
- Mobile
- Phone

Refer to "Create and Manage User Attributes" on page 117 for more information on user attributes.

### Modify OTP Authenticator Settings

1. Click Main Menu  > **Settings** > **Authenticators**. The **Authenticators** page appears.
2. Select **One Time Password** from the drop-down list. The **One Time Password** settings page appears.
3. From the **OTP Type** drop-down list, select one of the following:
  - Random—creates a random OTP
  - MemoPasscode™—creates an easier to remember OTP using a combination of letters and numbers
4. In the **OTP Alphabet** field, enter the characters that can appear in the OTP. You can enter specific letters, numbers, and special characters. For example, if you set it to **a3#** then the OTP will always include those characters.

**Note:** Using VOICE over OTP with characters as the OTP values (instead of just numbers) is not easy for users to understand. Numeric characters only are recommended if using VOICE as the OTP delivery method.
5. From the **OTP Default Delivery** drop-down list, select the **OTP Default Delivery** method used to send the OTP to the user (**Voice**, **Email**, or **SMS**). If the method selected is not available, another delivery method is used.

6. Enter the **OTP Length**. For example, if you enter **4**, the OTP is always four characters in length.
7. Enter the **OTP Lifetime** for the amount of time in seconds a user can use an OTP to authenticate after it is generated.
8. Click **Save**.

## Manage Temporary Access Codes

Temporary Access Codes can be used to log in when a user cannot access their one-time passcode (OTP) or Entrust Soft Token authenticator (for example, if a user has misplaced the mobile device containing their Entrust Soft Token mobile application).

**Note:** Temporary Access Codes can also be used as a standalone authenticator rather than as a substitute, but Entrust Datacard recommends using temporary access codes only for interim authentication.

You can limit the Temporary Access Code to a number of uses or a period of time. For example, you can limit the use of the Temporary Access Code to a single use or a 24-hour period.

Temporary Access Codes are different from one-time passwords (OTP) authenticators. A Temporary Access Code can be used multiple times over a configurable period. An OTP is a single-use authentication code sent to a user's phone, mobile device, or email address during authentication. Temporary Access Codes are not sent to users during authentication.

A user cannot see the Temporary Access Code they have been assigned on the user portal. Administrators must provide the Temporary Access Code to the user. A user is assigned only one Temporary Access Code. If a temporary access code has expired, you must delete it before you can assign a new one to a user.

### Prerequisites for Using Temporary Access Code

A Temporary Access Code can only be used for authentication if:


- It has been assigned to the user
- It has not expired
- It has not reached the maximum number of uses allowed
- The resource rule controlling access to the account allows Temporary Access Codes to be used for authentication.

## Modify Temporary Access Code Settings


If a Temporary Access Code has expired or is about to expire, you can modify the expiry information so that a user can still authenticate with it. Modify the Temporary Access Code if the user still does not have a new authenticator (a token, for example) when the Temporary Access Code expires.




Any changes made to temporary access codes take effect the next time they are used for authentication.



**Tip:** You can click **Undo** to reverse any modified settings that have not been saved. Clicking **Undo** does not revert these settings to their default value.

1. Click Main Menu  > **Settings** > **Authenticators**. The **Authenticators** page opens.
2. Select **Temporary Access Code** from the drop-down list. The **Temporary Access Code** settings open.
3. Modify the following settings as required:
  - a. Set **Length** to the number of characters or digits that can be included in a user's Temporary Access Code.
  - b. Set **Alphabet** to the number and characters that can be included in each user's Temporary Access Code. The alphabet characters must be unique. No white spaces can be included.
  - c. Select **Case Sensitive** to make the values entered in the Alphabet sensitive to whether the letters included are upper or lower case. When **Case Sensitive** is not selected, the Alphabet must contain either upper or lower case letters but not both.
  - d. Select **Replace Similar Characters** if you want to replace similar looking characters in a response. For example, replace O with 0 and I with 1.
  - e. Set **Maximum Uses** to the number of times the Temporary Access Code can be used to complete an authenticate challenge. Setting the field to **0** allows the authenticator to be used an infinite number of times.
  - f. Set **Lifetime (secs.)** to the amount of time in seconds before a Temporary Access Code expires.
4. Click **Save** to confirm changes to the **Temporary Access Code** settings.

## Assign a Temporary Access Code

1. Click Main Menu  > **Members** > **Users**. The **Users List** page opens.
2. Click the **User ID** of the user to whom you want to assign the temporary access code. The **User Details** page appears.

3. Click the **Authenticators** tab. The **Authenticators** page opens showing a list of authenticators assigned to the user.
4. Click Add . A drop-down list of authenticators opens.
5. Select **Temporary Access Code**. The Temporary Access Code is added to the user's list of authenticators. You need to send the code to the user.
6. To get the temporary access code, on the user's **Authenticators** page, click  and select  **Details**. The Temporary Access Code Details page appear.
7. Copy the text in the **Code** field. This is the temporary access code. Share the code to the user.
8. Click **OK** to close the Temporary Access Code Details page.

**Note:** You cannot create more than one Temporary Access Code for each user. To create a new Temporary Access Code, you must first delete the user's current Temporary Access Code, if there is one. If you need to delete the temporary access code, click  and select  **Delete** and click **Delete** on the confirmation prompt.


## Manage Password Settings

Password settings determine the requirements for Instant ID as a Service passwords, including password reset. Passwords are manually or automatically assigned to users on Instant ID as a Service. Passwords must meet the restrictions set in the Password Authenticator settings.

Additional topics in this section:

- "Manage Entrust Soft Token" on page 99
- "Assign Entrust Soft Tokens to Users" on page 100
- "Add and Activate an Entrust Soft Token" on page 101

### Manage Password Settings

1. Select Main Menu  > **Settings** > **Authenticators**. The **Authenticators** page opens.
2. Select **Password** from the drop-down list. The **Password** settings page appears.
3. Perform the following tasks, as required:
  - "Modify the Password Settings" on the next page
  - "Set Blacklisted Passwords" on page 94
  - "Set Password Reset Settings" on page 94
4. Click **Save** to save your changes. The changes apply to all passwords.

## Modify the Password Settings

In the Password Settings section, do the following:

1. Set **Minimum Length** to the minimum number of characters a password must contain. The maximum password length is 255 characters.
2. Set **Lifetime Days** to the number of a days a password is valid.  
This setting defines the value of the **Default Password Lifetime** set for a user's password authenticator (see "Assign a Password Authenticator" on page 95). A value of 0 sets the password to never expire. The default password lifetime is 90 days. The maximum is 36,500 days. The value cannot be less than the setting for the **Minimum Lifetime**.
3. Set **Minimum Lifetime** to the number of days a user must wait between creating and changing their password.
4. Set **Password Kept in History** to the number of previous passwords stored in the account password history. This setting prevents users from reusing recent passwords.  
The maximum number of passwords is 255. Enter a value of 0 to disable the password history.
5. Select the **Minimum Password Strength** from the drop-down list. A number of factors, such as common passwords, names, phrases, and character repetition determine the strength of a password. The default setting is **Good**.
6. Select Active Directory Complexity Requirements to require that any password entered during password reset meets the password requirements included in the user's Active Directory.

The following table provides a mapping of AD password settings to Instant ID as a Service password settings.

AD Password Setting	Instant ID as a Service password setting
Minimum password length	Minimum length
Maximum password age	Lifetime Days
Minimum password age	Minimum Lifetime
Enforce password history	Number of passwords kept in the History List
Password must meet complexity requirements	There is no direct mapping of AD complexity requirements to Instant ID as a Service.

**Note:** The Active Directory settings enforce the Lifetime Days, Maximum Lifetime, and Passwords Kept in History setting values. The Active Directory Password

complexity requirements are also enforced when resetting an Active Directory password.


7. Set **Protection Type** to either **Hashed** or **Encrypted Supports CHAP/MSCHAP authentication**. You must select **Encrypted (Supports CHAP/MSCHAP authentication)** to use a CHAP/MSCHAP authentication protocol.  
**Note:** This setting only applies to new passwords. The password must be changed on Instant ID as a Service for changes to the **Protection Type** to be applied to the password.
8. From the **Include Number** drop-down list, select the number is requirements.  
Tip: To create a password that is all numerals, such as for ATM access, set this option to **Required**, and set the options for letters and special characters to **Not allowed**.
9. Set **Number of Numeric Characters if Required** to the minimum number of numerals the password must contain when **Required** is set for **Include Number**. The **Required** value cannot exceed 255.
10. From the **Include Uppercase Letter** drop-down list, select the uppercase letter requirements.
11. Set **Number of Uppercase Characters if Required** to the minimum number of uppercase letters the password must contain when **Required** is set for **Include Uppercase Letter**. The **Required** value cannot exceed 255.
12. From the **Include Lowercase Letter** drop-down list, select the lowercase letter requirements.
13. Set **Number of Lowercase Characters if Required** to the minimum number of lowercase letters the password must contain when **REQUIRED** is set for **Include Lowercase Letter**. The **REQUIRED** value cannot exceed 255.
14. From the **Include Nonalphanumeric Character** drop-down list, select the non-alphanumeric requirements. Permitted special characters are: ! @ # \$ % ^ \* + ? /
15. Set **Number of Nonalphanumeric Characters if Required** to the minimum number of lowercase letters the password must contain when **Required** is set for **Include Lowercase Letter**. The **Required** value cannot exceed 255.
16. Set **Maximum Repeated Characters** to the maximum number of times a character can appear in the password.
17. Set **Maximum Change Time (Minutes)** to the amount of time, in minutes, that a password change must be made.  
When Instant ID as a Service flags a password for changing, you can choose a time period in which that change must be made. If the time period expires, an attempt to change the password fails and the administrator must reset the password. Enter a positive integer that represents the number of seconds, minutes, hour or days.

**Note:** Setting **Maximum Change Time (Minutes)** to 0 does not cause any already-expired passwords to be unexpired.

### Set Blacklisted Passwords


Blacklisted passwords are a list of words disallowed as user passwords.

In the **Blacklisted Passwords** section, do the following:

1. Click **Add**. The **Add Blacklisted Passwords** dialog box appears.
2. In the text box, enter the **Blacklisted Password Values**.  
**Note:** You cannot add duplicate words and strings in the **Blacklisted Password Values** list. For example, if you add *password* to the blacklisted password list, users are restricted from using the word *password* anywhere in your password.
3. Press **<return>** to enter each new blacklisted password on a new line.
4. When done, click **Add** to return to the Password setting page.
5. To delete a blacklisted password, click .

### Set Password Reset Settings

To enable users to reset their password during authentication, do the following:

1. Select **Enable Forgot Password** to enable users to reset their password during authentication. The setting is disabled by default. Additional **Password Reset Settings** appear.  
**Note:** You must also modify your Instant ID as a Service resource rules to enable password reset. See "Reset a Password" on page 97 for more information.
2. Select the **Groups Allowed to perform a Password Reset**.  
**Tip:** Click  to filter your group list.
3. From the Second Factor Authenticators Allowed to perform a Password Reset list, select the second factor authentication methods. Note the following when selecting second factor authenticators:
  1. Drag and drop the selected authentication methods in order of preference.
  2. Users resetting their password are prompted to complete the authentication challenge at the top of the list before being able to reset their password.
  3. If the user does not have that type of authenticator, they are prompted to use the next authenticator on the list.
  4. If they do not have any of the authenticators on the Second Factor Authenticators Allowed to perform a Password Reset list they cannot reset their password.  
**Note:** Selecting **Temporary Access Code** as an allowed authenticator only enables completing a Temporary Access Code authentication challenge to perform a password reset. Temporary Access Codes cannot be used to



complete a Grid Card, OTP, or Token challenge that is required before resetting a password.

4. (Optional) Select **Additional Second Factor**.

If selected, users are required to complete a second-factor authentication before being able to reset their password. When enabled the user must complete two of the second factor authentication challenges in the **Second Factor** list.

5. Select **Unlock User Account** to unlock the user account after they reset their password. The setting is enabled by default.

6. Review the **Knowledge-based Authentication Settings**. These settings only apply if **Knowledge-based Authenticator** is selected in the **Second Factor** list.

### Assign a Password Authenticator


You can assign passwords to users. Before assigning passwords to users, "Manage Password Settings" on page 91 as required.

**Note:** If **Create Default Password** is selected in the "Manage General Authenticator Settings" on page 86, a new user is automatically assigned a password authenticator by default.

1. Click Main Menu  > **Members** > **Users**. The **Users List** page appears.

2. Click the **UserID**. The **User Details** page appears.

3. Click the **Authenticators** tab. The **Authenticators** page appears.

4. Click Add  and select **Password** from the drop-down list. The **Edit Password Settings** dialog box appears.

5. Set the new password using one of the following methods:

- Select **Automatic Password Generation** to have a random, computer-generated password assigned to the user.


**Note:** Automatic Password Generation is disabled if the user does not have an email address.

6. In the **Enter the user password** field, enter the password to assign to the user and **Confirm Password** the password.

**Note:** The password must meet the **Password Rules**.




7. Set **Password Lifetime**. The options are:

- Default Password Lifetime Password expires based on the Lifetime Days setting in Authenticator Password Settings (Refer to "Manage Password Settings" on page 91)
- Password Never Expires
- Set Password Expiry Date Set the password to expire on a specific date.
- Use Existing Expiry Date If you do not select one of the other Password Lifetime options, the default password Expiry Date is used.

8. If you select **Set Password Expiry Date**, complete the following steps:
  - a. Click **Expiry Date**. A calendar pop-up appears.
  - b. Select the date that you want the password to expire. The user is prompted to enter a new password the next time they log in after the password expires.
  - c. Click **OK**. The date appears in the **Expiry Date** field.
9. (Optional) Select **Change Is Required on First Usage** to prompt the user to change their password at first login.
10. (Optional) If the user has an email address, select **Email Password to User** to send the password to the user by email. You cannot disable this option if you select **Automatic Password Generation**.
11. Click **Save**.
12. (Optional) Edit the Resource Rules for the Administrator user group to use the password as the first factor authenticator.
  - a. From the Main Menu , select **Administration > Resources > Resource Rules**. The Resource Rules page opens.
  - b. Click on a portal under Identity as a Service Portal Applications. The Edit Resource Rules page opens.
  - c. From the **First Factor** list, select **Password**.
  - d. To use Password as the only authenticator, clear the check boxes next to all of the authenticators under Second Factors.
  - e. Click **Submit**.

### Self-Assign a Password Authenticator

Follow these steps to self-assign an Instant ID as a Service password authenticator

1. Click Main Menu  > **My Profile**. The My Profile page opens.
2. Click the **Authenticators** tab. The Authenticators page opens.
3. Click Add .
4. Select **Password** from the authenticators list. The Password Settings page appears.
5. In the **New Password** field, enter your password.
6. Enter the same password in the **Confirm Password** field.
7. Review each item in the **Password Rules** box to confirm your password meets all of the requirements. A  should appear to the left of each rule if the requirement has been met.
8. Click **Save**.









## View, Edit, Delete Password Authenticators

After you assign a user a password authenticator, you can manage the following features of a user's password authenticator:

- View the password details
- Set the expiry time
- Force a password update
- Clear password history
- Delete a password

You can also reset a password. Refer to "Reset a Password" below for instructions.

### View, Update, and Delete a Password Authenticator

1. Click Main Menu  > **Members** > **Users**. The **Users List** page opens.
2. Click the **UserID**. The **User Details** page opens.
3. Click the **Authenticators** tab. The **Authenticators** page opens.
4. Click  next to the Password authenticator.
5. Do the following, as required:
  - Click  **Reset** to edit the password settings. (Refer to "Assign a Password Authenticator" on page 95 for more details.)
  - Click  **Details**. The Password Details page appear. Click **OK** to close.
  - Click  **Set Expiry Time** to set the password lifetime. (See "Assign a Password Authenticator" on page 95 for more details.)
  - Click  **Force Password Update** to force the user to change their password and then click **Force Password** on the prompt.
  - Click  **Clear Password History** and then click **Clear** on the prompt.
  - Click  **Delete** to delete the password authenticator. Click **Delete** on the prompt.

### Reset a Password

By default, if users forget their password used to access Instant ID as a Service account, they must contact an account administrator to have it reset.

You can enable password reset to allow users to reset their password without contacting the administrator. When set, a **Forgot your password?** link appears on the login page.

When a user clicks this link, they are asked for their user name and second-factor credentials. If both are valid, the user is prompted to create a new password.

- Enable Forgot Password — Refer to "Manage Password Settings" on page 91
- Set Authentication Decisions — Set **First Factor** to **password** in the Resource Rule **Allowed Authenticators** (see Create a resource rule).

- Assign password reset groups to users — If you have configured the Password Reset Settings of your account to require users to be part of specific groups (see the instructions to *Set Password Reset Settings* in "Manage Password Settings" on page 91, assign those groups to users accordingly (refer to "Add Users" on page 119).
- Assign required second factor authenticators to users — If configured Additional Second Factor to require users resetting their password to use a second factor authenticator before they can reset their password, assign at least one of the Second Factor Authenticators Allowed to perform a Password Reset to users (refer to "Manage Authenticators" on page 85).

#### Reset a Password Using a Link

A password reset URL is available at `##/reset/<userID>` where **userID** is optional.




For example, if the User ID is *aliceg*, then the password reset link would be *mycorp.<region>.trustedauth.com/##/reset/aliceg*

- If set, **userID** allows a user to skip entering their username and enter directly into the password reset flow.
- If a user navigates directly to the reset URL when they are already logged in, the user will be logged out and they will go into the password reset flow.
- If an invalid user ID is passed, an error message appears and the user is prompted to enter their user ID.
- If the user clicks **Cancel** while in the password reset flow then they will be redirected to `##/reset`.
- If during the password reset flow it is determined that the user is unable to reset their password then they will be redirected to the login page.

#### Reset your User Password

You can reset your Instant ID as a Service password, You can only have one Instant ID as a Service password at a time.

#### Assign an Instant ID as a Service Password Authenticator

1. Click Main Menu  > **My Profile**. The **My Profile** page appears.
2. Click the **Authenticators** tab. The **Authenticators** page appears.
3. Click  next to the Password authenticator.
4. Select **Change Password**. The **Edit Password** page appears.
5. In the **New Password** field, enter your password.
6. Enter the same password in the **Confirm Password** field.
7. Review each item in the **Password Rules** box to confirm your password meets all of the requirements. A  should appear to the left of each rule if the requirement has

- been met.
8. Click **Save**.

## Manage Entrust Soft Token

An Entrust Soft Token is an authentication token provided by Entrust Datacard for authentication. When assigned to a user, Instant ID as a Service requires that users who have been assigned this authenticator provide a specific challenge response generated by the Entrust Soft Token application. A user using a mobile device with an Internet connection can also leverage an enhanced Entrust ST feature called "Push Notification." Push Notification automatically prompts the user to authenticate on their mobile device when they authenticate on Instant ID as a Service.

A user can have multiple Entrust Soft Tokens. For example, if a user with multiple mobile devices might want to add an Entrust Soft Token to each one.


Administrators can assign Entrust Soft Tokens to users using the following methods:

- Automatically assign users an Entrust Soft Token. If the user has an email address, the user receives an email with instructions to activate their Entrust ST tokens. Refer to "Manage General Authenticator Settings" on page 86 for information on automatically assigning Entrust Soft Tokens to users.
- Add an Entrust Soft Token to a user's profile

Users can also add Entrust Soft Tokens to their accounts

**Note:** Before assigning authenticators to users, review the authenticator settings and change them as required.

### Modify Entrust Soft Token Authenticators

1. Click Main Menu  **Administration > Settings > Authenticators**. The **Authenticators** page appears.
2. Select **Entrust Soft Token** from the drop-down list. The **Entrust Soft Token** settings page appears.
3. Select **6** or **8** as the number of digits in the OTP generated by the token.
4. (Optional) Select **PIN Required** if you want users to enter a PIN to access the OTP.
5. Set the **Max. Time Steps** to the amount of time (in 30 second intervals) that the token response is valid. The default is 10 (5 minutes).
6. Set the **Max. Reset Time Steps** to the amount of time (in 30 second intervals) for a token reset. The default is 120 (60 minutes), which is the allowable time difference between the soft token and the server clocks.



**Note:** If the token reset does not work, try increasing the **Max. Time Steps** and then try to reset the token again. If the problem continues, contact the Entrust Datacard Support Team.


7. Enter the Activation Password Length to set number of characters that can be included in the password assigned to a user.
8. Enter the **Activation Lifetime** to set the amount of time in seconds that a user has to activate their Entrust Soft Token.
9. Select **Allow Unsecure Device** to allow the Entrust Soft Token to run on an unsecured device (such as custom ROM Androids or jail-broken iOS devices).
10. Select **Soft Token Facial Recognition Allowed** to allow authentication using the mobile Soft Token facial recognition.
11. Select the activation methods to include in the Entrust Soft Token Activation Email. You must select at least one option.
12. Click **Save**.

Next you need to assign, add, and activate Entrust Soft Tokens. Refer to the following topics:

- "Assign Entrust Soft Tokens to Users" below
- "Add and Activate an Entrust Soft Token" on the next page
- "Unlock and Disable a Entrust Soft Token" on page 104




### Assign Entrust Soft Tokens to Users

1. Click Main Menu  > **Members** > **Users**. The Users List page opens.
2. Click the User ID of the user. The **User Details** page appears.
3. Click the **Authenticators** tab. The **Authenticators** page appears.
4. Click Add  . A drop-down list of authenticators appears.
5. Select **Entrust Soft Token** from the drop-down list. Entrust Soft Token appears the user's list of authenticators.
  - If the user has an email, the user is sent an email with instructions on how to activate their Entrust Soft Token.
  - If the user does not have an email, the user must activate the Entrust Soft Token from their **My Profile** page. Refer to "Add and Activate an Entrust Soft Token" on the next page.

**Note:** Click  next to the Entrust Soft Token and select **Re-Activate** from the drop-down list to send another email if the first email was not received or the Entrust Soft Token was not activated before the activation expiry.



### Activate an Entrust Soft Token for a User

If the user cannot activate their Entrust Soft Token, for example, the user does not have connectivity to complete the activation, an administrator can complete the activation for the user. The user needs to provide the administrator with the activation code.

1. Click Main Menu  > **Members > Users**. The **Users List** page appears.
2. Click the User ID of the user. The **User Details** page appears.
3. Click the **Authenticators** tab. The **Authenticators** page appears.
4. Click  next to the Entrust Soft Token and select  Complete. A **Complete token activation** window appears.
5. In the **Enter Registration Code** field, enter 10-digit registration code that appears on your Entrust Soft Token.
6. Click **Complete** to register the authenticator with Instant ID as a Service.

### Add and Activate an Entrust Soft Token

An administrator can add Entrust Soft Tokens to your account. You can also add Entrust Soft tokens to your Instant ID as a Service account. You can have multiple Entrust Soft Tokens. For example, if you have multiple mobile devices, you might want to add an Entrust Soft Token to each one.

1. Click Main Menu  > **My Profile**. The My Profile page appears.
2. Click the **Authenticators** tab. The Authenticators page opens.
3. Click Add . A drop-down list of authenticators appears.
4. Select **Entrust Soft Token**. The **Activate Token** dialog box opens.
5. Use one of the tasks on this page to activate your Entrust Soft Token.

**Note:** To send an email with activation information, click **Send Email**. Click **OK** on the Activate Token dialog box to close it.

### Activate Using a Link in an Email

Use this procedure to activate your soft token from a link in an email. You must be able to access the email account that receives the email on your mobile device.


1. Open the authentication email on your mobile device.
2. Click the activation link, for example, **Click here to activate your mobile soft token**.
3. Tap either **Click here if this text is displayed as a link** or **Alternatively, click here if the above text is not displayed as a link**, depending on which link is available. The Entrust ST mobile application opens.

4. Enter the PIN required to open your Entrust ST mobile application. The application displays the **Activate Identity** page, with activation details entered automatically.
5. (Optional) Enter your name into the **Name** field if it has not already been entered.
6. Select **Activate**. A **Success** window appears when the soft token is activated.
7. Press **OK** to close the message. A new page opens displaying a 6 or 8-digit security code. The code updates every 30 seconds. This is the code that you must use to authenticate to Instant ID as a Service.

#### Activate Using a QR Code if You Have an Email

1. Open the email sent to you from Instant ID as a Service on your computer or your mobile device. The email is sent from [noreply@trustedauth.com](mailto:noreply@trustedauth.com). The email contains a QR code and password that you need to complete the assignment of the authenticator.
2. Open your Entrust ST application on your mobile device.
3. Enter the PIN required to access your application. If this is your first time accessing the application, enter a new PIN. The PIN gives you access to the mobile application.
4. Tap the QR code symbol. The QR Scanner feature opens within the application.  
**Tip:** The location of the QR code icon may vary. You can also go through your Entrust ST app to select the Scan QR code icon.
5. Scan the QR code located near the bottom of your email using the Entrust ST mobile application. A Password Required window appears requesting the 8-digit password.
6. In the **Password Required** field, enter the 8-digit password that was provided in the email.
7. Click **OK**. The Activate Identity window appears on your mobile application.
8. If it has not already been entered automatically, enter your user ID into the **Identity Provider Name** field. Press **Done**.
9. Press **Activate** to register the authenticator with Instant ID as a Service and complete the assignment of the authenticator to your profile. A message appears on your mobile application confirming the successful registration of the authenticator.
10. Press **OK**. A new window with a 6 or 8-digit security code appears. This is the code that you must use to access Instant ID as a Service or another application.


#### Activate Using a QR Code if You do not Have an Email

1. On your **Authenticators** page, click  in the **Actions** column for the Entrust Soft Token.
2. Select **Activate** from the drop-down list. The Activate Selected Token dialog box opens.
3. Click **Activate**. The **Activate Selected Token** dialog appears. Keep this dialog box open.



4. Scan the QR code that appears on the **Activate Selected Token** dialog box. A **Password Required** window appears requesting the 8-digit password.
5. In the **Password Required** field, enter the 8-digit password that appears in the **Activation Code** field on the **Activate Selected Token** dialog box.
6. Click **OK**. The **Activate Identity** window appears on your mobile application.
7. If it has not already been entered automatically, enter your user ID into the **Identity Provider Name** field. Press **Done**.
8. Press **Activate** to register the authenticator with Instant ID as a Service and complete the assignment of the authenticator to your profile. A message appears on your mobile application confirming the successful registration of the authenticator.
9. Press **OK**. A new window with a 6 or 8-digit security code appears. This is the code that you must use to access Instant ID as a Service or another application.





#### **Activate an Entrust Soft Token Manually**

1. Open the email on your computer (not your mobile device). The email is sent from **noreply@trustedauth.com**. It contains the address, serial number, and activation code information needed to complete the activation of the authenticator.
2. Open your Entrust ST application on your mobile device.
3. Enter the PIN required to access your application. If this is your first time accessing the application, enter a new PIN. This gives you access to the mobile application.
4. Tap **Add New Identity** or **+**. A new window appears for you to enter the information contained in your activation email.
5. Enter the address, serial number, and activation code information included in the activation email you previously received.
6. (Optional) Enter the name of your identity provider into the **Name** field if it was not automatically imported after you enter the **Address** information.
7. Press **Save** or **Activate**(depending on which version of Entrust Soft Token you are using). A window with a registration code appears.
8. Return to your **Authenticators** page in Instant ID as a Service.
9. Click  to the right of the **Entrust Soft Token** that you want to activate. A drop-down list appears.
10. Select **Complete** from the drop-down list. The Complete token activation window opens.
11. In the **Enter Registration Code** field, enter 10-digit registration code that appears on your Entrust Soft Token.
12. Click **Complete** to register the authenticator with Instant ID as a Service.
13. Press **OK** on your Entrust Soft Token mobile application.
14. Press **Yes**. A window with a 6 to 8-digit security code appears. This is the code that you must use when accessing Instant ID as a Service or another application.






## Unlock and Disable a Entrust Soft Token

If you enter an incorrect login PIN in your Entrust ST application too many times, you are locked out of Instant ID as a Service. You can also disable or enable a soft token authenticator after it has been activated. You may want to disable a soft token if you lost the mobile device that contains the soft token. Similarly, you can enable the soft token if the device containing the soft token is found.

### Unlock Your Entrust ST Authenticator

1. Select Main Menu  > **My Profile**. The My Profile page appears.
2. Click the **Authenticators** tab. Your list of assigned authenticators appears.
3. Open your Entrust ST mobile application.
4. Select . A window appears that displays a PIN Reset Code.
5. On the Instant ID as a Service page, click  to the right of the soft token authenticator that you want to unlock. A drop-down list appears.
6. Select  **Unlock**. The Unlock token dialog box opens.
7. Enter the **PIN Reset Code** that appears on the Entrust Soft Token application.
8. Click **Unlock**. The Unlock token window displays an Unlock code.
9. Enter the **Unlock code** in the Entrust ST mobile application.
10. Select **Unlock**. You are prompted to enter a new PIN.
11. Enter a new 4-digit PIN.
12. Re-enter the same 4-digit PIN.
13. Enable or disable a soft token

### Enable or Disable a Soft Token

1. Select Main Menu  > **My Profile**. The My Profile page opens.
2. Click the **Authenticators** tab. Your list of assigned authenticators appears.
3. Click  to the right of the soft token authenticator that you want to enable or disable. A drop-down list appears.
4. Do one of the following:
  - Click  **Disable** to disable the Entrust Soft Token (for example, if the mobile device containing the Entrust Soft Token is lost or being repaired).
  - Click  **Enable** to enable the Entrust Soft Token.
  - Click  to delete the Entrust Soft Token.
5. Click **Confirm** on the confirmation prompt.

# Manage Resources

This section describes how to add a Splunk IEM add-on, integrate an Issuance API to manage your printers and print jobs, add printers to your account, and create resource rules to protect access to Instant ID as a Service.

Topics in this section:




- "Add an Issuance API" below
- "Integrate Splunk SIEM with Instant ID as a Service" on page 107
- "Manage Resource Rules" on page 108
- "Add Printers" on page 126

## Add an Issuance API

You can add an Issuance API to manage printers and submit print jobs. Instant ID as a Service provides a JSON file that contains the credentials needed for the API integration to authenticate to Instant ID as a Service.

See the *IntelliTrust Administration API Guide* for more information.

### Add Administration API to Instant ID as a Service

1. Click Main Menu  > **Resources** > **Applications**. The **Applications** page appears.
2. Click **Add**. The **Add Applications** page appears.
3. Click **Issuance API**. The **Add Issuance API** page appears.
4. In the **Application Name** field, type a name for your application.
5. In the **Application Description** field, type a description for your application.
6. (Optional) Add a custom application logo as follows:
  - a. Click Add  next to **Application Logo**. The **Upload Logo** dialog box appears.
  - b. Click Upload  to select an image file to upload.
  - c. Browse to select your file and click **Open**. The **Upload Logo** dialog box reappears showing your selected image.
  - d. If required, resize your image.
  - e. Click **OK**.
7. Click **Next**. The **General Settings** page appears.
8. The **Application ID** is generated automatically once you submit the application. You do not need to enter a value for this field.

9. From the **Select Role** drop-down list, select to the role you want to assign to the API application. The role defines the operations that can be performed using this API application. You can select one of the system-defined roles or a custom role. You cannot select **No Role Assigned**.

System-defined roles include:

- **Auditor:** This role grants view-only access to users, authenticators, roles, and tokens on the integrated Entrust Adaptive Issuance Instant ID as a Service account.
  - **Help Desk Administrators:** This role allows you to add or remove users and their authenticators.
  - **SIEM Add-on:** This role provides full access to all SIEM management functions in view-only mode.
  - **Super Administrator:** This role allows you to add or remove users and their authenticators, and query your Entrust Adaptive Issuance Instant ID as a Service account roles.
  - **Issuance Administrator:** This role manages printers, print jobs, and Issuance administration.
  - **Issuance Operator:** Creates an Issuance API application that is used to issue print jobs.
10. If the account is a Service Provider, from the **Select Service Provider Role** drop-down list, select to the Service Provider role you want to assign to the API application. The role defines the operations that can be performed using this API application.

Available roles:

- **Super Account Manager:** Users with this role have full access to the Service Provider portal. These users can perform all the tasks assigned to On-boarding Administrators as well as:
    - Make changes to Service Provider settings.
    - Manage the Service Provider roles assigned to other users.
    - Remove Tenant accounts (this applies to regular Tenants only. Service Provider Tenants cannot be removed)
    - Unlock the administrators of a Tenant
  - **Audit:** Users with this role have view-only access to the Service Provider portal. Auditors cannot make any changes to Service Provider settings.
  - **On-boarding Administrator:** Users with this role can view, create, lock, and unlock Tenant accounts as well as promote Tenants to Service Providers
11. Click **Submit**. The **Complete** page appears. This page contains the parameters that your application must pass to the Administrator API.
  12. Do one of the following:
    - Click **Copy to Clipboard** to copy the applicationId, hostname and sharedSecret. You need these values to set up your Administration API.
    - Click **Credentials** to download a JSON file that contains the API credentials for this application.




13. Click **Done**.

## Integrate Splunk SIEM with Instant ID as a Service

Use the Splunk Add-on to Instant ID as a Service to automatically forward audit logs from your IntelliTrust account to your Splunk SIEM.

The IntelliTrust Splunk Add-On is located at <https://splunkbase.splunk.com/app/4204>.

### Add Splunk Add-on to Instant ID as a Service

1. Select Main Menu  > **Resources** > **Applications**. The **Applications** page appears.
2. Click **Add**. The **Add Applications** page appears.
3. Click **Splunk Add-on**. The **Add Splunk Add-on** page appears.
4. In the **Application Name** field, type a name for your application.
5. (Optional) In the **Application Description** field, type a description for your application.
6. (Optional) Add a custom application logo as follows:
  - a. Click Add  next to **Application Logo**. The **Upload Logo** dialog box appears.
  - b. Click Upload  to select an image file to upload.
  - c. Browse to select your file and click **Open**. The **Upload Logo** dialog box reappears showing your selected image.
  - d. If required, resize your image.
  - e. Click **OK**.
7. Click **Submit**. The **Complete** page opens.
8. Do one of the following:
  - Click **Copy to Clipboard** to copy the credentials.
  - Click **Credentials** to download a JSON file that contains the credentials

**Attention:** Once you leave this page the credentials are no longer available. If you do not copy or download the data then you will need to recreate the application.
9. Click **Done**.

### Add IntelliTrust Add-on to Splunk

1. Log in to Splunk.
2. Click **Find More Apps**.
3. In the **Browse More Apps** field, search for **IntelliTrust**. The Entrust Datacard IntelliTrust Add-on for Splunk dialog box opens.

4. Click **Install**.
5. In the **Login**, page enter your Splunk.com username and password.
6. Accept the terms of agreement.
7. Click **Login and Install**.
8. Click **Restart Now** on the Restart Splunk prompt.
9. Click **OK**.
10. Log in to Splunk as an administrator. The IntelliTrust Add-on appears in the **Apps** list.
11. Click **IntelliTrust Add-on**. The Inputs page opens.
12. Click **Configuration**. The Configuration page opens.
13. Click **Add-on Settings**.
14. In the **IntelliTrust Splunk App Secret** field, paste the credentials that you generated in *Add Splunk add-on to Instant ID as a Service*.
15. Click **Save**.
16. On the **Inputs** page, click **Create New Input**.
17. In the **Interval** box enter the interval period, in seconds, that Splunk queries IntelliTrust for new audit events.
18. In the **Include** field select the type of audits to include. Options include:
  - Authentication Events Only
  - Management Events Only
  - Both
19. Click **Add**.

## Manage Resource Rules

Resource rules protect access to applications by setting access restrictions. In an Instant ID as a Service account, the only application available is the Administration portal. When a user attempts to authenticate to the application, the resource rule determines how a user must authenticate to gain access. For example, You must configure First Factor and Second Factors. These settings allow administrators to clearly define the authenticators users are prompted to use when they authenticate to Instant ID as a Service.

You might set multiple resource rules to access the application. For example:

- Resource rule 1 allows some groups to access the application and some not
- Resource rule 2 forces some groups of users to have different authentication

You must configure First Factor and Second Factors settings. These settings define the authenticators users are prompted to use when they authenticate to an application.

- The selected **First Factor** authenticator determines whether a user must authenticate using their password or whether they skip directly to second factor authentication. If the first factor is set to **Skip Password**, a user must respond to a **Second**

**Factor** authenticator.

**Note:** Before setting Password as the first factor authenticator, ensure that the administrator user has a password configured. For instructions, refer to "Enable Password Authenticator" on page 123.

- The **Second Factors** list is ordered by preference from top to bottom.
  - Only selected authenticators in that list can be used to complete a second factor authentication challenge.
  - During authentication, the resource rule prompts the user to complete the **First Factor** authentication.
  - Once the user completes the first factor challenge, the user is prompted with the most preferred second-factor authentication challenge. If a user does not have a specific authenticator, they are prompted to log in using the next-most preferred authenticator on the list.  
For example, if Entrust Soft Token appears at the top of the list of second factor authenticators, the user is prompted to authenticate using Entrust Soft Token. If the user does not have an Entrust Soft Token, the user is prompted to authenticate using the next second factor authenticator in the list, and so on.

Consider these examples:

- **Example 1:** First Factor is set to **Skip Password**. Second Factors are set to **Entrust Soft Token** and **One Time Password**, in that order. The user logs in to Instant ID as a Service using Entrust Soft Token Push. If the user does not have Entrust Soft Token push, the user selects **Use an alternative authenticator** on the log in screen, and selects OTP from the list.
- **Example 2:** First Factor is set to **Password**. Second Factors is set to **Temporary Access Code**. The user logs in to Instant ID as a Service using their Instant ID as a Service password.. If the user does not have Entrust Soft Token push, the user selects **Use an alternative authenticator** on the log in screen, and selects OTP from the list.
- **Example 3:** You want to create multiple resource rules for different users of your account. For example,
  - Resource rule A for Group A is set to **Skip First Factor** and second factor set to **OTP** and **Entrust ST**.
  - Resource rule B for Group B is set to First Factor **Password** with no second factors selected. Users authenticate using password only.
  - Resource rule C for Group C is set to **Skip First Factor** and Second Factor set to all four options (For example, some users only have Temporary Access Code. When logging in, they select Alternate Authentication on the second

factor authentication page to be able to authenticate using their Temporary Access Code).

- Resource rule for no group selected (all groups) is set to **Skip First Factor** and second factor **OTP**. Users must authenticate by OTP. There are no other options.

If an application has multiple resource rules, Instant ID as a Service selects the resource rule to be used as follows:

- Ignores the resource rules for which the user's group does not match
- Selects from the remaining resource rules alphabetically based on name


Topics in this section:

- "Create a Resource Rule" below
- "Edit Resource Rules" on the next page

## Create a Resource Rule

You must add a resource rule to allow users to access Instant ID as a Service. Be sure to review the information in "Manage Resource Rules" on page 108 before you begin.

Create a resource rule to protect access to your application.

1. Select Main Menu  > **Resources** > **Resource Rule**. The **Resource Rules List** page appears.
2. Enter a **Rule Name**. Resource rules are applied alphabetically. For example, a resource rule name "Administration Portal - Administrators" is considered first if a second resource rule is named Operators.
3. Enter a **Rule Description**.
4. Select the **Groups** for which the resource rule applies. If you do not select any groups, then all groups are selected by default.
5. Select the First Factor from the drop-down list.
  - If you select **Skip Password**, then a user must authenticate using a second factor. You must select at least one second factor if you select Skip Password.
  - If you select **Password**, then a user must authenticate first using their Instant ID as a Service password and then respond to the second factor authentication challenge. If you select first factor **password** and do not select any second factor authenticators, users authenticate using their password only.
6. Select the **Second Factors**.
  - **OTP**: Users respond to a one-time password authentication.
  - **Entrust Soft Token Push**: Users respond to a push notification on their mobile device by pressing **Confirm** on their Entrust Soft Token.
  - **Software Token**: Users enter a token passcode generated on their Entrust Soft Token.
  - **Temporary Access Code**: Users enter their temporary access code.




7. Drag and drop the order of second factors. This is the order in which a user is presented second factor authentication.
8. Click **Submit**.



### **Edit Resource Rules**

After you create a resource rule, you can do the following:




#### **Edit a Resource Rule**

1. Select Main Menu  > **Resources** > **Resource Rule**. The **Resource Rules List** page appears.
2. Click the Rule Name of the resource rule you want to modify. The **Edit Resource Rules** page appears.
3. Modify your resource rule as required.
4. Click **Submit** to save your changes.

#### **Delete a Resource Rule**

1. Select Main Menu  > **Resources** > **Resource Rule**. The **Resource Rules List** page appears.
2. Click  next to the resource rule you want to delete. You are prompted to delete the rule.
3. Click **Delete**.

#### **Enable or Disable a Resource Rule**

1. Click Main Menu  > **Resources** > **Resource Rule**. The **Resource Rules List** page appears.
2. If the resource rule is enabled and you want to disable it, click .
3. If the resource rule is disabled and you want to enable it, click .

## **Manage Reports**

You can create reports and export data from the following tables:


- Audit events (refer to "View and Export Audit Logs" on page 17)
- Users (refer to "View, Search, and Export Users" on page 120)
- Archives of audit events from recent weeks

When you export users and audit events, they are downloaded to the **Reports** page. You can view and export activity reports. Reports remain on the Reports page for one week.




Archives contain audit events from recent weeks that are ready to download in CSV format. Audits are available for download for a period of six months. Archive audits are saved for a period of three years.

**Note:** You can export a maximum of 100,000 records.

## View Archives and Reports

1. Select Main Menu  **Administration > Reports > Reports**. The Reports page appears.
2. Click the **Reports** or **Archives** radio button to set the type of reports you want to view.
3. Set the number of reports on a page:
  - a. Scroll to the bottom of the page.
  - b. From the **Rows per page** drop-down list, select the number of rows to display on the page.
  - c. To move to a new page, on the right-hand side of the page, do the following, as required:
    - Click > to go to the next page.
    - Click < to go to the previous page.
    - Click |< to go to the first page.
    - Click >| to go to the last page.

## Filter Archives and Reports

1. Click Main Menu  **Administration > Reports > Reports**. The Reports page appears.
2. Click the **Reports** or **Archives** radio button to set the type of reports you want to filter.
3. Click  to enable filtering.
4. The **Filters** dialog box appears.
5. Select your filter options and click **Apply**.
6. You are returned to the **Reports** page. The page displays your filter results.
7. To clear the filter, click  again.
8. On the **Filters** dialog box, click **Reset**.

## Delete Reports

1. Click Main Menu  **Administration > Reports > Reports**. The Reports page appears.
2. Click the **Reports** radio button.
3. To delete an individual report, click  to delete the desired report.

4. To delete multiple reports, click the check boxes next to the reports you want to delete.  
If you want to delete all the reports, click the check box next to **State** to select all the reports.
5. Click **Delete** on the Delete Report confirmation prompt.

## Manage Users

This section provides instructions on how to add users, create custom user attributes, assign and create user roles, and assign users to groups. Before adding users, set up your groups, roles, and user attributes.

Topics in this section:

- [Create and manage groups](#)
- [Create and manage roles](#)
- [Create and manage user attributes](#)
- [Add users](#)



### Create and Manage Groups

A group is a collection of users. You can assign or remove groups by modifying a user's profile information.


You can create as many groups needed to control which users can access Instant ID as a Service.

This section explains how to create, edit, and delete groups.



#### Create a Group

1. Click  > **Members** > **Groups**. The **Groups** page displays.
2. Click . The **Add Group** dialog box appears.
3. Enter a **Name** for your group.
4. Click **Add**. The group is added to your groups list.

#### Edit a Group Name

1. Click  > **Members** > **Groups**. The **Groups** page displays.
2. Click the group name. The **Edit Group** dialog box appears.
3. Edit the **Group Name** as required.
4. Click **Save**.

## Delete a Group

1. Click  > **Members > Groups**. The **Groups** page displays.
2. Click  for the group you want to delete.
3. Click **Delete** on the confirmation prompt.



## Create and Manage Roles

Roles control the operations that a user can perform in their Instant ID as a Service account. A role defines a list of system entities and the permissions for those entities. There are six system-defined roles. Administrators can also create custom roles. Changes to a role take effect the next time the user logs in. System-defined roles cannot be changed.

System-defined roles include:

- **Auditor**: This role gives view-only access to the features available on the administrator portal. It has the **Manage All Roles** permission setting enabled by default. This setting allows administrators with this role to manage all user and role settings. This includes being able to assign a role to a user.
- **Super Administrator**: This role provides full access to the features available on the administrator portal. It has the **Manage All Roles** setting enabled by default.
- **Help Desk Administrator**: The Help Desk Administrator role can manage other user accounts with the Auditor and Help Desk Administrator roles and those without a role (end users). They cannot manage users with Super Administrator or custom roles. The **Manage All Roles** setting cannot be modified for this role.
- **SIEM Add-on**: This role provides full access to all SIEM management functions in view-only mode
- **Issuance Administrator**: Manages printers, print jobs, and Issuance administration.
- **Issuance Operator**: Creates an Issuance API application that is used to issue print jobs.

## Create a Custom Role

1. Select Main Menu  > **Members > Roles**. The **Roles List** page opens.
2. Click Add . The **Add Role** page appears.
3. Enter a **Name** for your custom role.
4. Enter a **Description** for your custom role.
5. Choose one of the following options:
  - Select **Manage All Roles** to allow those assigned this role to manage all users. Or:
  - Do not select **Manage All Roles** and from the Select **Roles to Manage** drop-down list, select the roles that you want the users assigned this role to




manage.

When you select a role, it appears in the **Administrator is allowed to manage these roles** list. To add more roles, select the next role from the drop-down list.

6. Select the **System Entities** and permissions for the custom role.  
The system entities define the functionality the role can access. For example, if you create a custom role called *Marketing* and want to only allow users with the Marketing role to have access to the Theme page, you would set the **Account Branding Customization** system entity to **All** to allow users with the Marketing role access and edit the Theme page.
7. Click **Add** to create the role.

### Clone a Role

You can create a copy of an existing role.


1. Select **Main Menu**  > **Members** > **Roles**. The **Roles List** page appears.
2. Click **Clone**  next to the role you want to clone.
3. Click **Add** . The **Add Role** page appears. By default, **Copy** is appended to the name of the role you are cloning.
4. Change the role **Name**, as required.
5. Edit the role **Description**, as required.
6. Choose one of the following options:
  - Select **Manage All Roles** to allow those assigned this role to manage all users.
  - or–
  - Do not select **Manage All Roles** and from the select **Roles to Manage** drop-down list, select the roles that you want the users assigned this role to manage.
  - For example, if you want to create a custom role called *Super Auditor* that allows the role to manage all users assigned the Auditor role, select *Auditor* from the drop-down list.

**Note:** You can select more than one role to manage.



7. Edit the **System Entities**, as required.  
System entities define the functionality the role can access. For example, if you create a custom role called *Marketing* and want to only allow users with the Marketing role to have access to the Theme page, you would set the **Account Branding Customization** system entity to **All** to allow users with the Marketing role access and edit the Theme page.

8. Click **Add**.

### **Edit a Custom Role**

1. Click Main Menu  > **Members** > **Roles**. The **Roles List** page appears.
2. Click the name of the custom role you want to edit. The **Add Role** page appears.
3. Modify the settings as required.
4. Click **Add**.

### **Delete a Custom Role**

1. Select Main Menu  > **Members** > **Roles**. The **Role List** page appears.
2. Click Delete  next to the role you want to delete.
3. Click **Delete** on the confirmation prompt.

### **System Entities**

A system entity is the functionality available to the assigned role in Instant ID as a Service. Click the system entity for more details about its function.

- **Account and Authenticator Settings:** Controls the settings of the different authenticators available on Entrust Adaptive Issuance Instant ID as a Service.
- **Account Branding Customization:** Allows users to customize the appearance of their Entrust Adaptive Issuance Instant ID as a Service account and email templates.
- **Account Entitlement Status:** Allows users to see the number of entitlements assigned to their account. Account entitlements define how many users can be created within an account.
- **Account Reports:** Allows users to monitor their account activity. Users can generate reports on specific account metrics.
- **Application Template Management:** Allows access to the configuration settings needed to add an application to your Instant ID as a Service account.
- **Applications Management:** Allows users to configure their application accounts so that they are accessible after authenticating to Entrust Adaptive Issuance Instant ID as a Service.
- **Bulk Enrollments:** Allows users to perform bulk import of enrollment records into Entrust Adaptive Issuance Instant ID as a Service.
- **Credential Design Management:** Allows users to create and manage credential designs.
- **Enrollments:** Allows users to manage enrollment records.
- **Export Reports:** Allows users to export user, grid card, and audit reports.
- **Groups Management:** Controls the groups available on an account. A group is a collection of users given access to applications based on the resource rules assigned to them.

- **Issue Credentials:** Allows users to enroll applicants and issue credentials.
- **Printer Management:** Allows you to manage printers (create, delete, update, and view printers).
- **Resource Rules Management:** Controls the resource rules that define the application access restrictions.
- **Roles Management:** Controls the level of access each user has to the features on their Entrust Adaptive Issuance Instant ID as a Service account.  
**Note:** Selecting the Role Management system entity automatically enables the Manage All Roles setting.
- **Scheduled Task Management:** Allows users to manage and schedule tasks.
- **User Attribute Management:** Controls the information fields available in the user profile information.
- **User Management:** This feature controls the user accounts listed in your Entrust Adaptive Issuance Instant ID as a Service account.
- **User Password Authenticator Management:** Controls access to the password assigned to users.
- **User Role Management:** Facilitates the assignment of a role to a user.
- **User Temporary Access Code Management:** Provides access to view or create a temporary access code for a user. The temporary access code information can be seen except for the code itself (a character string). Accessing the code value requires a role with the **User Temporary Access Code View Value**.
- **User Token Authenticator Management:** Allows users to control the hardware and soft token authenticators assigned to other users in their account.

## Create and Manage User Attributes

User attributes are the information fields in a User Profile. There are two types of attributes in Instant ID as a Service:

- **System user attributes** are set by Instant ID as a Service and can be modified but cannot be deleted. You cannot leave mandatory user attributes blank.
- **Custom user attributes** are additional user attributes that an administrator can add to a user profile.

**Note:** All custom user attributes and some system-defined attributes can be set to mandatory or optional.

You can change the settings of some system attributes, create new user attributes, and edit existing custom user attributes. See the following options for instructions:

## Edit a System User Attribute Setting

You can configure the following system attributes to be optional or mandatory:


- Email
- First name
- Last name
- Mobile
- Phone

**Note:** For OTP to be available, a user must have a value set for at least one of the following system attributes:



- phone
- email
- mobile

If no values are provided for all of those system attributes, then OTP will not be available.

### Edit a system attribute


1. Select Main Menu  > **Members** > **Attributes**. The **User Attributes List** page appears.
2. Under **System User Attributes**, click the user attribute. For example, click **First Name**. The **Edit User Attribute** dialog box appears.
3. Do one of the following:
  - Check **Required** if you want the attribute to be mandatory.
  - Clear **Required** to make the attribute optional.
4. Click **Save**.

### Add a Custom User Attribute



1. Select Main Menu  > **Members** > **Attributes**. The **User Attributes List** page appears.
2. Under **Custom User Attributes**, click Add . The **Add User Attribute** dialog box opens.
3. Enter a **User Attribute Name** for the custom user attribute. For example, `Sales-force`.
4. Select **Required** to set the attribute as mandatory.
5. Click **Add** to create the attribute. The attribute now appears in the user's profile.



## Edit a Custom User Attribute

1. Select Main Menu  > **Members** > **Attributes**. The **Attributes List** page appears.
2. Click the name of the custom user attribute. The **Edit User Attribute** dialog box appears.
3. Edit the **User Attribute Name** as required.
4. Check or clear **Required** to make the attribute mandatory or optional.
5. Click **Save**.

## Delete a Custom User Attribute

1. Click  > **Members** > **Attributes**. The **Attributes List** page appears.
2. Click  for the custom user attribute that you want to delete.
3. Click **Delete** on the confirmation prompt.



## Create and Manage Users

Users set the credentials used to access Instant ID as a Service. They also contain personal information used to identify the user. Use the following pages to create and manage users:

- "Add Users" below
- "View, Search, and Export Users" on the next page
- "Edit, Delete, Disable, and Unlock Users" on page 121
- "Enable Password Authenticator" on page 123

### Add Users

Add users to your Instant ID as a Service account. The role you assign to your users determines the functionality available to them. For more information on roles, refer to "Create and Manage Roles" on page 114.

1. Click Main Menu  > **Members** > **Users**. The **Users List** page appears.
2. Click Add  . The **Add User** page opens.
3. Enter the following attributes, as required:
  - a. Enter the **First Name** of the user.
  - b. Enter the **Last Name** of the user.
  - c. Enter the **Email** address of the user. The email address is used to send authenticator and account information emails.
  - d. Enter the **Mobile** number of the user.

- e. Enter the **Phone** number of the user.

**Note:** By default, First Name, Last Name, and Email are set as mandatory.

For information on changing them, refer to "Edit a system attribute" in the section, "Create and Manage User Attributes" on page 117.

1. Enter the **User ID** of the user. This system attribute is mandatory.
2. Under **Permissions**, do the following:
  - a. From the **Select Group to add** drop-down list, assign the user to the required group. You can add a user to multiple groups.

**Note:** If no groups are selected, the user is assigned to the **All Instant ID as a Service Users** group by default.
  - b. From the **Select Role** drop-down list, select the user role. The role determines which features the user can access in Instant ID as a Service. For more information, see "Create and Manage Roles" on page 114.
3. By default, the user **State** is **Active**. You can toggle this setting to **Inactive** if you do not want the user to have access to their Instant ID as a Service account.
4. If applicable, under **Required Attributes**, on the line below each required attribute, enter the value for the attribute. For more information on attributes, see "Create and Manage User Attributes" on page 117.
5. (Optional) Add a user alias to allow the user to log in using their User ID or an alias. Note the following when adding aliases:
  - All aliases must be unique in the system.
  - An alias must not be the same as a User ID in the system.
  - You can add up to 10 aliases.

Add an alias as follows:

- a. Under **Aliases**, click **Add**. The **Add Alias** dialog box opens.
  - b. In the **Add Alias** field, enter the alias.
  - c. Click **OK**.
  - d. Repeat steps a to c to add another alias.
4. Click **Save**.

### **View, Search, and Export Users**




You can set the number of users listed on a page, filter your user list to display only users in an active, inactive, or locked state, and export your user list to a custom CSV file.

#### **View Users**



1. Click Main Menu  > **Members** > **Users**. The **Users List** page appears.
2. Scroll to the bottom of the page.

3. From the **Rows per page** drop-down list, select the number of rows to display on the page.
4. To move to a new page, on the right-hand side of the page, do the following, as required:
  - Click **>** to go to the next page.
  - Click **<** to go to the previous page.
  - Click **|<** to go to the first page.

#### **Filter or Search for Users**

1. Click Main Menu  **> Members > Users**. The **Users List** page appears.
2. On the **Users List** page, click  to enable filtering.
3. The **Filters** dialog box appears.
4. Select your filter options and click **Apply**.
5. You are returned to the **Users List** page. The page displays your filter results.
6. To clear the filter, click  again.
7. On the **Filters** dialog box, click **Reset**.

#### **Export a User List**

1. Click Main Menu  **> Members > Users**. The **Users List** page appears.
2. Click **Export**  to export the user list to a .CSV file. The **Export Table to CSV** dialog box appears.
3. (Optional) Enter a **Name** for the file.
4. (Optional) Enter a **Description** for the file.
5. Select the **File Delimiter** radio button, Comma (,) or Vertical bar (|).
6. Select the attributes you want to include in the file.
7. If you do not select any attributes, by default only the User ID is included in the CSV file.
8. Click **Export**. The CSV file is exported to the Reports page (see [Manage reports](#)).

**Note:** You can export a maximum of 100,000 records.

#### **Edit, Delete, Disable, and Unlock Users**

Delete users, modify user profiles, disable and enable users, and unlock users.


**Note:** If a user is locked and you also disable the user, the user's state shows as disabled. If you re-enable the user, the user remains in a locked state until you unlock the user.

#### **Editing a User Profile**

You can edit the user profile of users, as follows:



- Only users with a Super Administrator role can change the role assigned to another account.
- Super Administrators can only be deleted by other Super Administrators.
- Super administrators cannot be disabled.
- A Unique User ID attribute is added once a user has been added to Instant ID as a Service. You cannot modify this attribute.

#### Edit a user profile

1. Click Main Menu  > **Members > Users**. The **Users List** page opens.
2. Click the **User ID** for the profile you want to edit. The **User Profile** page appears.
3. Make the required changes and click **Save**.

#### Deleting Users





You can only delete Instant ID as a Service users one at a time.

1. Click Main Menu  > **Members > Users**. The **Users List** page appears.
2. Click  for the user you want to delete.
3. Click Delete on the Delete User prompt.

#### Unlocking a User




Users can lock their authenticators by failing an authentication attempt too many times (refer to "Manage General Authenticator Settings" on page 86).

The **User List** page shows users with locked authenticators.

1. Click Main Menu  > **Members > Users**. The **Users List** page appears. A  appears beside users with locked authenticators.
2. Click  Unlock in the **Actions** column. The **Unlock User** dialog box appears showing a list of locked authenticators.
3. Click **Confirm** on the Unlock User prompt to unlock the locked authenticators. The  disappears and all the user's authenticators are now unlocked.

#### Disable/Enable a User




If you want to prevent a user from logging in to their Instant ID as a Service account, you can disable the user.

1. Click Main Menu  > **Members > Users**. The **Users List** page appears.
2. Click  next to the user you want to disable. The **Disable User** dialog box appears.
3. Click **Confirm**.
4. To enable a user, click . The Enable User dialog box appears.
5. Click **Confirm**.

## Enable Password Authenticator

By default, the first factor authenticator is set to skip the password authenticator. This makes the second-factor authenticator the only authenticator used to log into Instant ID as a Service.

**Note:** Configure a password for the user before configuring the resource rules to use a password authenticator. If you do not, Instant ID as a Service might lock the account.

1. Configure a password for the current Administrator user.
  - a. From the Main Menu , select **Administration > Members > Users**. The Users List page opens.
  - b. Click on a user name from the **Users** List. The User Details page opens.
  - c. Select the **Authenticators** tab.
  - d. Select Add  > **Password**. The Edit Password Settings dialog box opens.
  - e. Complete the fields on the Edit Password Settings dialog box then click **Save**.
2. Edit the Resource Rules for the Administrator user group to use the password as the first factor authenticator.
  - a. From the Main Menu , select **Administration > Resources > Resource Rules**. The Resource Rules page opens.
  - b. Click on a portal under Identity as a Service Portal Applications. The Edit Resource Rules page opens.
  - c. From the **First Factor** list, select **Password**.
  - d. To use Password as the only authenticator, clear the check boxes next to all of the authenticators under Second Factors.
  - e. Click **Submit**.

## Printer Management

Follow the instructions in the following topics to configure a new cloud-printer:

- "Enable Cloud Printing" on the next page
- "Add Printers" on page 126

Use the instructions in the following topics to manage printers and resolve printing issues:

- "Print a Test Card" on page 126
- "Manage Printers" on page 127
- "Troubleshoot Printing Issues" on page 128

## **Enable Cloud Printing**

Instant ID as a Service prints to cloud-enabled printers over the internet. To enable printing, configure the printer to communicate over the internet with the Instant ID as a Service server. Follow the instructions on this page to enable cloud printing on supported Entrust printers.

Instant ID as a Service supports printing to the following printers:

- Sigma DS1
- Sigma DS2
- Sigma DS3
- CD800
- CD812
- CD820
- CD870
- CD880
- SD260L
- SD360
- SD460

### **Connect the Printer to the Internet**

To enable communication between Instant ID as a Service and the printer, connect the printer to the internet using the Ethernet port. Before following these instructions, follow the instructions in the Quick Install Guide to connect the printer to the power and insert the print ribbon.

1. Connect an Ethernet cable from a network-connected port to the Ethernet port on the printer.
2. Note the IP Address. Connecting to the Printer Dashboard requires the IP address of the printer.

### **Configure CD and SD Printers for Cloud Printing**

Use the EDC Cloud Ready Utility to verify that a CD or SD printer is compatible with cloud printing and configure the printer for cloud printing.

1. Request the EDC Cloud Ready Utility from your service provider.
2. Install then open the Utility.

3. In the **IP** field, enter the IP address of a printer then click **Connect**. The Utility connects to the printer and displays the printer network information.
4. Click **Check Setup**. The Utility verifies the cloud status on the printer.
5. Click **Setup Cloud** if the printer is not configured for cloud. The Cloud Location dialog box opens.
6. Select a cloud location from the list then click **Select**. The Utility configures the printer for cloud printing and displays **Passed**.


### Enable Cloud Printing Using the LCD Menu

After connecting the printer to the network, configure it to communicate over the internet with Instant ID as a Service to print credentials. To enable cloud printing on the printer enable cloud then select the region in which you are using the printer.

1. Enable cloud printing.
  - a. Using the LCD menu, select **Configuration > Network Cloud > Cloud Connection**.
  - b. Select **Enabled**.
2. Select a region. Selecting the region determines which Instant ID as a Service server the printer will use for receiving print jobs and other printer communications. This is the same region that you are connected to Instant ID as a Service software.
  - a. Select **Configuration > Network Cloud > Cloud Region**.
  - b. Select the region in which the printer resides.
    - United States
    - Ireland
    - Germany
    - CustomUse Custom only for financial printing.

### Enable Cloud Printing Using the Printer Dashboard

Use the Printer Dashboard to configure the printer for cloud printing. Before connecting to the Printer Dashboard, connect the printer to the internet.

1. In a browser, enter the following URL to open the Printer Dashboard.  
`https://[Printer IP Address]/`
2. From the Main Menu , select **Configuration > Settings**.
3. From the drop-down menu, select **Behavior**.
  - a. Expand the drop-down menu for the **CloudConnection** offset.
    - i. Select **Enable**.

- b. Expand the drop-down menu for **CloudLocation**.
  - i. Select the cloud region that matches the cloud region used by your Instant ID as a Service tenant.
4. Click **Save**.

**Note:**


Ensure that TCP port 8883 is open on the network hosting the printer.

### **Next Steps**

- Add the printer to Instant ID as a Service. For instructions refer to "Add Printers" below.
- Resolve any issues encountered while managing a printer. Refer to "Troubleshoot Printing Issues" on page 128 for guidance on resolving printer issues.
- Manage the printers configured in Instant ID as a Service. For instructions, refer to "Manage Printers" on the next page.

## **Add Printers**

Add a printer to enable Instant ID as a Service to print to the printer, manage the printer, and access Printer Dashboard.

1. Click Main Menu  > **Resources > Printers**. The **Printers List** page appears.
2. Click **Add**. The **Add Printer** dialog box appears.
3. Enter the **Printer Name**.
4. Enter the 16-digit **Printer Device id**.
5. Enter the printer **Location**.
6. Click **Add**. The Printer is added to the Printers List page.

**Note**

If a printer is duplicated by adding it more than once or by adding the same printer with a different name, an error message reading "Your printer is already registered" displays. In this case, both printer registrations must be deleted from existing tenants and the printer must be re-onboarded or re-registered one time by following the steps above.

### **Next Steps:**

- "Manage Printers" on the next page
- "Print a Test Card" below

## **Print a Test Card**

Print a test card from a printer on the Printers page to test the connectivity of the printer, the printing supplies, and quality of the printer.




## Manage Printers

Follow the instructions on this page to modify the settings of a printer managed by Instant ID as a Service.


### Edit a Printer

Follow these settings to modify the settings of a printer managed by Instant ID as a Service.

1. If you need to edit the name or location, on the **Printer List** page, click  next to the printer. The **Update Printer** dialog box appears.
2. Modify the settings.
3. Click **Save**.

### Delete a Printer

Follow these steps to remove a printer from Instant ID as a Service management.

1. To delete a printer, on the **Printer List** page, click  next to the printer. The **Delete Printer** dialog box appears.
2. Click **Delete**. A confirmation dialog box opens.
3. Click **Delete**.

### Open the Printer Dashboard

Use the Printer Dashboard to manage settings on the printer. The printer hosts the Printer Dashboard. To access the Printer Dashboard, ensure that the printer is powered on and connected to the internet.

### View Printers



The Printer List page displays all of the printers managed by Instant ID as a Service. Follow these steps to modify how the Printers List page displays printers.

1. On the **Printer List** page, scroll to the bottom of the page.
2. From the **Rows per page** drop-down list, select the number of rows to display on the page.
3. To move to a new page, on the right-hand side of the page, do the following, as required:
  - Click **>** to go to the next page.
  - Click **<** to go to the previous page.

- Click |< to go to the first page.
- Click >| to go to the last page.

### Filter Printers

Filter printers to change which printers the Printer List page displays.

1. On the **Printer List** page, click  to enable filtering.
2. The **Filters** dialog box appears.
3. Select your filter options and click **Apply**.
4. You are returned to the **Printer List** page. The page displays your filter results.
5. To clear the filter, click  again.
6. On the **Filters** dialog box, click **Reset**.

### Troubleshoot Printing Issues

If you experience issues connecting your printer to Instant ID as a Service, refer to the topics on this page to help resolve the issue. If you experience an issue that is not described on this page or the content here does not help resolve the issue, contact Entrust Technical Support.

#### Adding the Printer Fails

When adding the printer to Instant ID as a Service for management fails. The Add Printer function displays an error indicating that Instant ID as a Service failed to add the printer.

Cause	Solutions
The Device ID is incorrect.	Using the LCD menu or Printer Dashboard, verify that the Device ID entered in Instant ID as a Service matches.
The Printer is not configured for cloud printing.	Follow the instructions in "Enable Cloud Printing" on page 124 to configure the printer for cloud printing.
The printer is not connected to the internet.	<ul style="list-style-type: none"> <li>• Check the internet connection of the printer. Follow the instructions in "Enable Cloud Printing" on page 124 to connect the printer to the internet.</li> <li>• Verify that the internet connection to the printer location is viable.</li> </ul>
The user is connected to the wrong Instant ID as	Use the Printer Dashboard or LCD menu to verify that the printer is configured to the same Instant ID as a Service region that you are connected to.

Cause	Solutions
a Service region.	
Duplicate printers have been added.	If a printer is duplicated by adding it more than once or by adding the same printer with a different name, an error message reading "Your printer is already registered" displays. In this case, both printer registrations must be deleted from existing tenants and the printer must be re-onboarded or re-registered one time. Refer to "Add Printers" on page 126 for details.

### The Printer Fails to Print a Card

When printing a test card or credential from enrollment and the printer fails to produce a credential, there are many possible causes for this issue.

Cause	Solutions
The printer is off.	<ul style="list-style-type: none"> <li>• Turn on the printer.</li> <li>• Ensure that the printer is in a "Ready" state.</li> </ul>
A print ribbon is not installed in the printer.	<ul style="list-style-type: none"> <li>• Install a print ribbon.</li> <li>• Ensure that the printer is in a "Ready" state.</li> </ul>
The connection between the printer and Instant ID as a Service is broken.	<ul style="list-style-type: none"> <li>• Ensure that the printer is connected to the internet.</li> <li>• Ensure that the printer is on, in the "Ready" state, and the cloud icon shows that the printer is cloud-ready. Non-Sigma printers show a plus icon.</li> <li>• Ensure that the printer is connected to the same region that you are connected to Instant ID as a Service.</li> <li>• Ensure that TCP port 8883 is open on the network hosting the printer.</li> </ul>

### The Printer is no Longer Visible in Instant ID as a Service

If a printer previously managed by Instant ID as a Service is no longer visible to you, follow these steps to resolve the issue.

Cause	Solutions
The current user no longer has access to that printer.	<ul style="list-style-type: none"> <li>• Work with your Instant ID as a Service administrator to grant your user access.</li> <li>• Grant your user access to the printer.</li> </ul>
A user deleted the printer from Instant ID as a Service.	Add the printer back to Instant ID as a Service. For instructions, refer to "Add Printers" on page 126.

## Enable Alexa Voice

After enabling the Alexa Voice feature, use an Alexa Device to check the status of the printer, print a test card, and many other things. The Alexa Voice feature supports only English commands.


### Support Notes

The Amazon Alexa devices, Amazon account, and Entrust Printer must meet the requirements in this section to use the Alexa Voice feature.

- Supports all Amazon Alexa Voice devices and Amazon Alexa applications on iPhone and Android
- Supports only English commands
- An Alexa Device must be registered to the Amazon account used to configure Alexa Voice

### Setup Alexa Voice for a Printer

Setup the Alexa Voice feature on a printer to enable your Alexa devices to monitor and control the printer.

1. From the Main Menu , select **Printers**. The Printers page opens.
2. Select **> Register with Amazon Alexa**. The Amazon Sign-in dialog box opens.
3. Log in using your Amazon credentials.
4. Click **Allow** to allow your Alexa Devices to access the printer. The Alexa Device responds to indicate that it discovered the printer.

### Common Phrases

Using Amazon Alexa with Entrust Printers supports many commands with different syntax. Below are a list of some examples of commands to use with your Alexa Device.

#### Check Printer Status

The printer state is the current status of the printer. Use this to check if the printer is in an error state or to check if the printer is ready to print cards.

**Command:** Alexa, what is the printer state?

### **Get the Printer Serial Number**

Speak this command to have Alexa speak the serial number of the printer.

**Command:** Alexa, what is the Serial Number?

### **Check Firmware Version**

Speak this command and Alexa will read the current version of firmware on the printer.

**Command:** Alexa, what is the firmware version?

### **Check Part Numbers**

Speak this command to have Alexa read the part numbers for the printer ribbon.

**Command:** Alexa, what are the part numbers?

### **Check Cleaning Status**

Speak this command to check on how many cards can be printed before a cleaning card must be run.

**Command:** Alexa, what is the cards before cleaning?

### **Supply Commands**

Use the commands in this section to check on the status of the supplies in the printer.

#### **Check Ribbon Supply Level**

Speak this command to check the status of the ribbon supply in the printer.

**Command:** Alexa, what is the ribbon supply level?

#### **Check Laminator Supply Level**

Speak this command to check the status of laminator supply in the printer.

**Command:** Alexa, what is the laminator L1 supply level?

### **Maintenance Commands**

#### **Look Up Error Codes**

When an Entrust printer encounters an error, it presents an error code. You can use your Alexa device to learn more information on the error code including the cause of the error and possible solutions.

**Command:** Alexa, ask Entrust printer what is error code [error code number].

#### Read the Error Code

Speak this command to have Alexa read the error code of an error the printer is experiencing.

**Command:** Alexa, what is the error code?

#### Print a Cleaning Card

Cleaning cards clean debris from the internal mechanisms in the printer. Run a cleaning card to maintain the printer or when the printer is not printing correctly.

Before commanding the printer to print a cleaning card, place a cleaning card in the printer hopper.

**Command:** Alexa, set printer maintenance to run a cleaning card.

#### Print a Test Card

Speak this command to print a test card on the printer.

**Command:** Alexa, set printer maintenance to print test card.

## Manage Printer Settings

Instant ID as a Service connects to cloud-enabled printers to manage printer settings, monitor the printer status, and view firmware updates using the Printer Dashboard.

### Open Printer Dashboard

Follow these steps to open Printer Dashboard. Ensure that the printer supports Printer Dashboard.

1. From the Main Menu , select **Printers**. The Printers page opens.
2. Click on the printer name. The Printer Dashboard opens.

### Printer Information

The areas of the Printer Dashboard below describe the status and details of the printer.

- **Summary:** The Summary area provides information on the status of the printer, the model, and the connection type. For more information, refer to "View Device Details" on the next page.
- **Supplies:** The Supplies area provides information on the printer supplies. For more information, refer to "Manage Supplies" on page 134.


- **Cleaning Card:** The Cleaning Card area shows the number of cards after which you must run a cleaning card. For more information, refer to "Run a Cleaning Card" below.
- **Device Activity:** The Device Activity area shows the status of print jobs.
- **Hoppers:** The Hoppers area shows the status of the hoppers on the printer.
- **Firmware:** The Firmware area displays the current firmware version. The color of the square indicates the status of the firmware.

### Printer Status Message

When the printer is in a state that might require service or attention, Printer Dashboard displays a message with information about the issue at the bottom of the page. Use this information to help diagnose and resolve the issue or to communicate the issue to customer service.

### View Device Details

The Device Details page displays information about the printer including product information, networking information, and software versions.

1. From the Main Menu , select **Printers**. The Printers page opens.
2. Click on the printer name. The Printer Dashboard opens.
3. Click **Device Details**. The Device Details page opens and displays the following information about the printer:
  - **Product Data:** Displays information about the printer including the serial number, name, and manufacturer.
  - **Network:** Information for each networking interface including the IP address, netmask, and gateway for both IPv4 and IPv6 (if configured).
  - **Serial Numbers:** Shows the serial numbers and names used to identify the printer.
  - **Versions:** Displays the version of the hardware, firmware, and software used in the printer.
  - **Options:** Shows all of the features and options on the printer in alphabetical order.

### Run a Cleaning Card

Run a cleaning card to clean debris from the internal mechanisms in the printer. The Cleaning Card page shows the number of cards after which you must run a cleaning card, cleaning best practices, and a video tutorial about running a cleaning card.

To run a cleaning card:

1. Open the printer cover.
2. Remove the spent print ribbon and cleaning roller.

**Note:** Additional steps may be necessary to ready the printer for the cleaning card process. Refer to the specific printer's User's Guide for additional details.


3. Close the printer cover.
4. Insert a cleaning card into the printer.
5. From the *Cleaning Card* page, under Run Cleaning Card, select **Clean Printer** from the drop-down list.
6. Click **RUN** to begin the cleaning process. Note that, if a cleaning card has not been inserted, a dialog box also displays informing you that a card must be in place.

## Manage Supplies

The Supplies area shows the status of printer supplies and provides the option to order replacement supplies.


### View Supply Details

The Supply Details page shows the current status of the print ribbon, and other supplies. Use this page to determine if supplies need to be replaced.

1. From the Main Menu , select **Printers**. The Printers page opens.
2. Click on the printer name. The Printer Dashboard opens.
3. Click **Supply Details** to open the Supply Details page and displays the following information for print ribbons and other replaceable parts:
  - **Supply Type:** The name of the supply part.
  - **Supply Level:** The current percent of remaining use of the supply part.
  - **Part Number:** The part number of the supply part. Use this to reorder the supply part.
  - **Lot Code:** The code used to identify the supply part. Use this to reorder the supply part.

### Order Supplies

The Entrust Printer Dashboard includes the option to order supplies when the supplies in the printer are low.

1. From the Main Menu , select **Printers**. The Printers page opens.
2. Click on the printer name. The Printer Dashboard opens.
3. Click **Order Supplies**. A new tab or window opens to the web site of the service pro-



vider.

4. Follow the instructions on the web site to order new supplies.

## Printer Firmware Update

The Printer Dashboard includes the option to update printer firmware.

### Check for a Firmware Update

Instant ID as a Service automatically checks for new firmware updates once a day. After checking for an update, the color of the firmware status icon changes to indicate the current status of the firmware. All users can check for a firmware update. For more information, refer to "Firmware Status Icon Colors" below.

To check for a new firmware update, click **Check for Update**. Instant ID as a Service checks for new firmware then updates the firmware status icon with the current status.

### Update Printer Firmware

The Printer Dashboard includes the option to check for a new firmware version and update to that version. You can submit print jobs to the printer during the update process. Only the Super Administrator on the tenant can update the printer firmware. Follow these steps to update the printer firmware.

1. Click **Check for Update**. Instant ID as a Service checks for new firmware. If it finds a new firmware version, it enables the Update button.
2. Click **Update**. Instant ID as a Service updates the firmware on the printer. The printer restarts after updating the firmware.

### Firmware Status Icon Colors

The Printer Firmware area displays the status of the firmware using the following colors.

- **Green**: Indicates that the firmware is current.
- **Red**: Indicates that the firmware is out of date. The Firmware area also shows a note indicating that the firmware is out of date.

### Change the LED Color


The LED light strip on the front of Sigma printers can change color to suit branding needs or for aesthetic reasons. Follow these steps to change the color of the LED light strip.

1. From the Main Menu , select **Printers**. The Printers page opens.
2. Click on the printer name. The Printer Dashboard opens.

3. Click **LED Color** from the Summary area. The **LED Color** dialog box opens.
4. Slide the color selector along the color palate to select a color.
5. To change the shade, select a shade of that color.
6. Click **Save**. Instant ID as a Service changes the color of the LED light strip on the front of the printer.

### Enable Quiet Mode

Quiet mode reduces the noise produced by the printer. Follow these steps to enable quiet mode on a printer.

1. From the Main Menu , select **Printers**. The Printers page opens.
2. Click on the printer name. The Printer Dashboard opens.
3. In the Summary area, select **Quiet Mode**. The printer enables quiet mode and reduces the noise from printing a credential.

## Import Enrollment Records

Instant ID as a Service includes options to import multiple enrollment records by uploading an import ZIP file containing enrollment data. Instant ID as a Service parses the import file then creates enrollment records for each entry in the import file. Instant ID as a Service can also upload photographs and signature files for the applicants.



Follow this process to import enrollment records to Instant ID as a Service:

1. "Create an Enrollment Design" below
2. "Prepare the ZIP Import File" on the next page
3. "Import Enrollment Records" on page 139

**Note:** Refer to "Troubleshoot Import" on page 139 to resolve issues with the import process.

### Create an Enrollment Design

Before importing enrollment records, create an enrollment design that contains fields for the data in the imported enrollment records. Instant ID as a Service imports data from the enrollment records into the corresponding fields in the enrollment design. Create a credential design then, generate an enrollment design from the credential design. If the destination enrollment design does not have a matching field, Instant ID as a Service does not import the data for that field.

1. From the Main Menu , select **Credential Designs**. The Credential Designs page opens.
2. Click Add . The Create a Credential Design page opens.
3. Select a credential design template. The Credential Designer opens.
4. Enter a name for the credential design in the **Card Name** field. For instructions, refer to "Configure Credential Settings" on page 50.
5. Add fields for each field in the imported enrollment records. For instructions on creating credential designs, refer to "Design a Credential" on page 25.
6. Name the fields to match the names of the fields in the enrollment records. Use the names of the fields in the credential design in the import file.
7. Click **Generate Enrollment** to generate an enrollment and save the credential design.

## Prepare the ZIP Import File

The ZIP import file contains all the data including photographs and signatures for an applicant. Follow the guidelines in this section to prepare the ZIP import file.

**Note:** Instant ID as a Service limits the size of each enrollment including signature and photograph files to 5 MB.

### Prepare Photographs

The photograph files must be prepared in the following ways to successfully upload photographs in an enrollment import.

- Photograph files must be located in a folder named **Photos**.
- The import CSV file must contain a column called **Photo** that contains the file names of the photographs in the Photos folder.
- Photographs must be in jpeg image format.

### Prepare Signatures

Follow these guidelines to upload images containing signatures from applicants.

- Signature image files must be located in a folder named **Signature**.
- The import CSV file must contain a column called **Signature** that contains the file names of the signature files in the Signature folder.
- Signature image files must be in jpeg image format.

## Prepare the Import File

The import file is a comma separated value (CSV) file that contains applicant data and references to photographs and signatures. Follow these guidelines when creating the import file.

Here is an example of a CSV import file:

Student ID	First Name	Last Name	Job Title	Prefix	Photo	Signature
1	Sarah	Sampleton	Staff	Ms.	photo1.jpg	signature1.jpg
2	Travis	Sampleson	Staff	Mr.	photo2.jpg	signature2.jpg
3	Mary	Exampleperson	Staff	Mrs.	photo3.jpg	signature3.jpg

Follow these steps to create an import CSV file:

1. Create a new spreadsheet using Microsoft Excel.
2. Add a column for each field in the credential design. The names of the columns must match the names of the fields in the credential design exactly.
3. Create a column called **Photo** to import photographs.
4. Create a column called **Signature** to import signatures.
5. Enter applicant data in the columns.
6. In the Photo column, enter the file name of the photograph in the Photos folder.
7. In the Signature column, enter the file name of the signature file in the Signature folder.
8. Save the spreadsheet as a CSV file.



## Prepare the ZIP File

Before uploading the ZIP file, ensure it meets the following requirements:

1. Add the CSV import file, Photos folder, and Signature folder to a ZIP file.
2. Ensure that the ZIP file contains the following files and folders in this structure:
  - [CSVFileName].csv
  - Photos
    - [PhotographFileName1].JPG
    - [PhotographFileName2].JPG
    - [PhotographFileName3].JPG
  - Signature
    - [SignatureFileName1].JPG
    - [SignatureFileName2].JPG
    - [SignatureFileName3].JPG

## Import Enrollment Records

Follow these step to upload an import ZIP file containing enrollment data. Instant ID as a Service imports the data and creates enrollment records for each row in the import file. Before importing enrollment records, prepare the import file. For instructions, refer to "Prepare the ZIP Import File" on page 137.



1. From the Main Menu , select **Bulk Operations**. The Bulk Operations page opens.
2. Click Add . The Add Bulk Operation wizard opens.
3. Select **Import** from the **Actions** list.
4. Select **Enrollments** from the **Operations** list.
5. Select an enrollment design from the **Enrollment Design** list.
6. Select the **File Delimiter** that the import file uses.
  - Select **Comma** if the import file uses commas to separate columns.
  - Select **Pipe** if the import file uses vertical bars to separate columns.
7. From the **Maximum Number of Retries** list select the number of times Instant ID as a Service is allowed to retry the import after an error.
8. Enter a name for the bulk operation in the **Name** field.
9. (Optional) Enter a description of the bulk operation in the **Description** field.
10. Click **Initiate**. The File to Upload page opens.
11. Click on the upload area. A file browser opens.
12. Select the import ZIP file and click **Open**. Instant ID as a Service adds the file to the wizard.
13. Click **Upload**. The Start/Stop page opens.
14. Review the details of the bulk operation then, click **Start**. Instant ID as a Service starts the import process.
15. Click **Finish**. The Bulk Operations page opens showing the status of the import process.

## Troubleshoot Import

After importing enrollment records using the Bulk Operations page, issues might cause the import to fail. Use the information here to diagnose then fix issues with the import process.

### Download and Review the Logs File

The logs file contains information on the import process to assist in troubleshooting issues with the import process. To view more information on the import process and failures, download and review the logs file.

1. From the Main Menu , select **Bulk Operations**. The Bulk Operations page opens.
2. Click **Download Logs**  in the row for an import enrollments operation. The browser downloads the logs file.
3. Open the logs file using a text editor.
4. Review the logs file.
  - Each row in the logs file represents an error in the import process.
  - "ERROR" indicates that the row is an error message.
  - The number following "ERROR" is the line in the import file that caused the error. Use this to locate the issue in the import file.
  - The text in the row provides more information on the issue.

### **Solutions to Import Issues**

Refer to the recommendations on this page to resolve issues with importing enrollment records.

#### **The Credential Name Does Not Match**

The name of the first column in the import file must match the name of a credential design in Instant ID as a Service. Instant ID as a Service imports the enrollment records and attributes the imported enrollment records to that credential design.

**Solution:** Check the name of the credential design in Instant ID as a Service. Then change the name of the credential design in the import file to match the name of the credential design.

#### **The Import File Does Not Contain a Credential Column**

The import file must contain a column named **Credential** that includes the name of a credential design. This column indicates which credential design holds the enrollment records.

**Solution:** Add a column named **Credential** that contains the name of a credential design in Instant ID as a Service in each row.

#### **Columns in the Import File Do Not Match Fields on the Credential Design**

At least one column in the import file must match a field on the credential design. If the a column does not match the import fails. To import all of the data, ensure that each column in the import file matches a field on the credential design.

**Solution:** Ensure that the column names in the import file have a corresponding field on the credential design. Also ensure that the names match.

#### **The Credential Column Name is Incorrect**

The Credential column must be named **Credential**. If the column name is not Credential, the import will fail.

**Solution:** Change the name of the Credential column to **Credential**.

## **Configure and Enable Mobile Flash Pass**

Mobile Flash Passes are digital credentials that contain all information for an applicant. They also contain a barcode to identify the user or gaining access to an area. Mobile Flash Passes require the use of either Google Pay or Apple Wallet. Follow the instructions in this section to setup Apple or Google accounts for issuing Mobile Flash Passes then enable Mobile Flash Passes in Instant ID as a Service.

1. "Setup Accounts for Mobile Flash Pass" below
2. "Enable Mobile Flash Pass" on page 143

### **Setup Accounts for Mobile Flash Pass**

Mobile Flash Passes require an Apple Developer account or a Google Developer account. Follow the instructions on this page to configure developer accounts for issuing Mobile Flash Passes.

This page includes references to third-party instructions and links to third-party websites. These are provided for your convenience, but the third party may modify the content on the linked website. Because of this, ensure that you are following the most up-to-date instructions by reviewing these directly on the third-party website and in the third-party documentation. In the event of any conflict or discrepancy between the content of this page and that on the third-party website or related documentation, the latter shall prevail to the extent of the conflict or discrepancy.

#### **Apple Developer Account**

Consider these recommendations and notes when setting up an Apple Developer account for issuing Mobile Flash Passes from Instant ID as a Service.

1. Create an Apple Developer account at [developer.apple.com](https://developer.apple.com).
2. Enroll the Apple Developer account in the Apple Developer Program. For more information, refer to ["What You Need To Enroll" on developer.apple.com](https://developer.apple.com/what-you-need-to-enroll).
3. Create a Pass Type ID for the Apple Developer account. For specific instructions, refer to ["Register a pass type identifier" on help.apple.com](https://help.apple.com/register-a-pass-type-identifier).
4. Create a Pass Type ID Certificate. For detailed instructions on creating a Pass Type ID Certificate, refer to ["Create a Pass Type ID certificate" on help.apple.com](https://help.apple.com/create-a-pass-type-id-certificate)
5. Add the Certificate file to Keychain Access application on a Mac. For detailed instructions on adding a certificate to Keychain Access, refer to ["Add certificates to a keychain using Keychain Access on Mac" on support.apple.com](https://support.apple.com/add-certificates-to-a-keychain-using-keychain-access-on-mac)
6. Export the private key from the certificate using Keychain Access. When exporting the private key, Keychain Access will request a password for the private key file. For more information on exporting a private key file from Keychain Access, refer to ["Export keychain items" on support.apple.com](https://support.apple.com/export-keychain-items).
  - a. Right-click on the private key file for the certificate.
  - b. Select **Export**.
  - c. Select a name and location for the private key file then click **Save**.
  - d. Enter a password for the private key file then click **OK**.
  - e. Enter a password for the administrator user on the Mac then click **OK**. Keychain Access saves a .p12 or .pfx private key file.
7. Save the Pass Type ID, Key File, and Key File Password for configuring and enabling Mobile Flash Pass in Instant ID as a Service.

## Google Developer Account

Consider these recommendations and notes when setting up a Google Developer account for issuing Mobile Flash Passes from Instant ID as a Service.

1. Create a Google account using a company email address at <https://developer-s.google.com/pay/passes>.
  - Ensure that the purpose for the account is **To manage my business**.
  - The account requires Google approval. This might take a few days.
2. Complete and submit the Google Pay API for Passes application form. Google reviews then approves the application. Ensure that the following options are selected in the application form.
  - Under **Integration Type with Google Pay**, select **Loyalty Cards**.
  - Under **Integration Platform Type**, select **Android**, **Web**, and **Email/SMS**.
  - Under **Redemption Method**, select **On-screen barcode redemption**.
  - Under **Do your barcode readers support scanning from a phone screen?**, select **Yes**.



- Enter a description and purpose of your Mobile Flash Pass in the text box labeled **Please describe the nature of the content you wish to make available to your customers through Google Pay.**

Google reviews the application and approves based on the information in the application.

3. Register your Mobile Flash Pass as an application with Google Pay API to obtain a certification .json file. For instructions on registering the Mobile Flash Pass, refer to ["Register your application" on developers.google.com.](#)
4. Connect your Google account with the Google Pay API to obtain the Issuer ID. For instructions on connecting your Google account with the Google Pay API, refer to ["Tie your service account to your Google Pay API for Passes account" on developers.google.com.](#)
5. Save the Issuer ID and the credentials .json file for configuring and enabling Mobile Flash Passes in Instant ID as a Service.



Next Steps: "Configure and Enable Mobile Flash Pass" on page 141

## Enable Mobile Flash Pass

Flash Passes require the use of either Google Pay or Apple Wallet. Follow these steps to enable and configure Mobile Flash Passes in Instant ID as a Service.

### Enable Mobile Flash Pass for Apple Wallet



Follow these steps to enable and configure Mobile Flash Pass to use with Apple Wallet.

1. From the Main Menu , select **Administration > Settings > Mobile Flash Pass**. The Mobile Flash Pass page opens.
2. Select **Enabled** in the Apple Wallet Settings area.
3. In the **Apple Wallet Pass Type ID** field, type the Pass Type ID for the Apple Developer account that will issue Mobile Flash Passes. For more information on locating the Pass Type ID, refer to "Setup Accounts for Mobile Flash Pass" on page 141.
4. Upload an Apple Wallet key file. For more information on setting up an Apple Wallet private key file, refer to "Setup Accounts for Mobile Flash Pass" on page 141.
  - a. Under **Apple Wallet Key File**, click Upload .
  - b. Locate and open the Apple Wallet .p12 or .pfx private key file.
5. Enter the password for the Apple Wallet key file in the **Apple Wallet Password** field.

6. In the **Download Lifetime** field, enter the amount of time after which the Mobile Flash Pass links expire. Download Lifetime applies to the Apple Wallet and Google Pay Mobile Flash Passes.
7. Click **Save**.

### Enable Mobile Flash Pass for Google Pay

Follow these steps to enable and configure Mobile Flash Pass to use with Google Pay.

1. From the Main Menu , select **Administration > Settings > Mobile Flash Pass**. The Mobile Flash Pass page opens.
2. Select **Enabled** in the Google Pay Settings area.
3. In the **Google Pay Issuer ID** field, enter the Issuer ID for your Google account. For instructions on obtaining the Issuer ID, refer to "Setup Accounts for Mobile Flash Pass" on page 141
4. Upload the Google Pay credentials .json file.
  - a. Under **Google Pay Credentials File**, click Upload .
  - b. Locate and open the Google Pay credential .json file.

For instructions on obtaining the Google Pay credential .json file, refer to "Setup Accounts for Mobile Flash Pass" on page 141.

5. In the **Download Lifetime** field, enter the amount of time after which the Mobile Flash Pass links expire. Download Lifetime applies to the Apple Wallet and Google Pay Mobile Flash Passes.
6. Click **Save**.

# Supervisor




Issuance Supervisors view the status of printers, reviews credential designs, and monitors enrollments. Refer to the following tasks:

- "View the Issuance Dashboard" below
- "Monitor Printing" below
- "View Credential Designs" on the next page
- "View Enrollment Records" on the next page

## View the Issuance Dashboard

The Instant ID as a Service dashboard contains issuance information for monitoring credential designs and the issuance process. The dashboard also contains links to other pages in Instant ID as a Service for monitoring printers, credential designs, and enrollments.


Refer to the following instructions for more information on the Instant ID as a Service dashboard functions:

- Click **Printers**  to view the status of printers managed by Instant ID as a Service. For instructions, refer to "Monitor Printing" below.
- Click **Designs**  to view credential designs. For instructions, refer to "View Credential Designs" on the next page.
- Click **Credentials**  to view the credentials and enrollments. For instructions, refer to "View Enrollment Records" on the next page.

## Monitor Printing


The Printers page displays the status of all printers managed by Instant ID as a Service. The Print Queue page displays the status of print jobs submitted to the printers. Follow these steps to monitor the printers and print jobs.

1. View printers.
  - a. Select Main Menu  > **Printers**. The Printers page opens.
  - b. To filter the list of printers, enter text in the **Quick filter** field.

2. View print jobs.
  - a. Select Main Menu  > **Print Queue**. The Print Queue page opens.
  - b. To filter the list of printers, enter text in the **Quick filter** field.

## View Credential Designs




Follow these steps to view the credential designs in Instant ID as a Service.

1. Select Main Menu  > **Credential Designs**. The Credential Designs page opens.
2. To view a credential design, click on a credential design row. The credential design opens in the Credential Designer.
3. To filter the list of credential designs, enter text in the **Type text to filter** field.

## View Enrollment Records

The Credentials page displays the enrollment records sorted by the credential design.

View the enrollments to monitor the credentials issued for each credential design.

1. Select Main Menu  > **Credentials**. The Credentials page opens displaying the credential designs.
2. Click **Search**  in the area for a credential. The Search Enrollment page opens and lists all of the enrollments for the credential.
3. Click **Filter Search** . The Search Panel dialog box opens. The Search Panel dialog box contains fields for each text field on the credential.
4. Enter text in a field to search the enrollments for text in the matching field on the credential.  
For example, enter a name in the **Name** field to search the enrollments for that name.
5. Click **Search**. Instant ID as a Service searches for enrollments that match the search criteria.

## Manage the Print Queue

The Print Queue displays print jobs for all printers visible to the current user.




## Printer Statuses

After submitting a print job, the Print Queue page displays the print job and its status. The status of the print job indicates the current state of the print job. Below is a list of the possible print job statuses.

- **Queued:** Instant ID as a Service sent the print job to the printer.
- **In Progress:** The printer is preparing and printing the credential.
- **Failed:** The printer encountered an error causing the print job to fail.
- **Waiting for Smartcard:** The printer is waiting on information provided by the smart car reader.

## View Print Jobs

The Print Queue displays print jobs for all printers visible to the current user. Follow these steps to view the Print Queue page to monitor print jobs.

1. From the Main Menu , click **Print Queue**. The Print Queue page opens.
2. Click on a column title to sort the column in descending or ascending order.
3. To filter print jobs:
  - a. Click **Filter** . The Filter print jobs dialog box opens.
  - b. In the **Printer name** field, enter the name of a printer name to filter the print job list based on the printer.
  - c. In the **Print job name** field, enter text to filter the print job list based on the print job name.
  - d. Click **Search**. Instant ID as a Service filters the print job list based on the criteria.
4. Click **Reset**  to reset the filters applied the list of print jobs to the default filters.

## Delete Print Jobs

Delete a print job to clear it from the list of print jobs. Instant ID as a Service allows only print jobs with Waiting or Stopped statuses to be deleted.

To delete a print job, click **Delete** .