

Cloudpath Enrollment System SAML Authentication Server Configuration Guide, 5.9

Supporting Cloudpath Software Release 5.9

Copyright, Trademark and Proprietary Rights Information

© 2021 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Preface	5
Contacting RUCKUS Customer Services and Support.....	5
Document Feedback.....	6
RUCKUS Product Documentation Resources.....	6
Online Training Resources.....	6
Document Conventions.....	6
Command Syntax Conventions.....	7
Overview of Using SAML as an Authentication Server for Cloudpath	7
Required Parameters.....	7
Proceeding With One of the Tested SAML Configurations	8
Using SSOCircle as the SAML Identity Provider	8
Basic Tasks for Using SSOCircle.....	8
Adding a SAML Step To Your Workflow.....	8
Adding the SSOCircle SAML Authentication Server to the Workflow.....	9
Downloading the SAML Metadata for SSOCircle.....	13
Configuring Your Account on SSOCircle.....	15
Publishing the Workflow for SAML SSOCircle.....	20
Testing the User Experience for SAML SSOCircle.....	20
Using Shibboleth as the SAML Identity Provider	21
Basic Tasks for Using Shibboleth.....	21
Adding a SAML Step To Your Workflow.....	21
Adding the Shibboleth SAML Authentication Server to the Workflow.....	22
Downloading the Shibboleth SAML Metadata.....	26
Adding the Metadata to Your Shibboleth Identity Service Provider.....	26
Publishing the Workflow for SAML Shibboleth.....	27
Testing the User Experience for SAML Shibboleth.....	27
Using Gluu as the SAML Identity Provider	27
Basic Tasks for Using Gluu.....	28
Adding a SAML Step To Your Workflow.....	28
Adding the Gluu SAML Authentication Server to the Workflow.....	28
Downloading the SAML Metadata for Gluu.....	33
Connecting to the Gluu Identity Service Provider.....	34
Publishing the Workflow for SAML Gluu.....	39
Testing the User Experience for SAML Gluu.....	39
Using Google G Suite as the SAML Identity Provider	40
Basic Tasks for Using Google G Suite.....	40
Creating a Google Admin App.....	41
Adding a SAML Step To Your Workflow.....	46
Adding the Google G Suite SAML Authentication Server to the Workflow.....	47
Returning to Google G Suite Configuration.....	51
Publishing the Workflow for SAML Google G Suite.....	56
Testing the User Experience for SAML Google G Suite.....	56
Using Google Groups in the Workflow	57

Adding a Device Configuration to Your Workflow..... 57

Preface

Contacting RUCKUS Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their RUCKUS products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the RUCKUS Support Portal using <https://support.ruckuswireless.com>, or go to <https://www.ruckuswireless.com> and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at <https://support.ruckuswireless.com/contact-us> and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

Self-Service Resources

The RUCKUS Support Portal at <https://support.ruckuswireless.com> offers a number of tools to help you to research and resolve problems with your RUCKUS products, including:

- Technical Documentation—<https://support.ruckuswireless.com/documents>
- Community Forums—<https://forums.ruckuswireless.com/ruckuswireless/categories>
- Knowledge Base Articles—<https://support.ruckuswireless.com/answers>
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—<https://support.ruckuswireless.com/security>

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

Document Feedback

RUCKUS is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to RUCKUS at #Ruckus-Docs@commscope.com.

When contacting us, include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- RUCKUS SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

RUCKUS Product Documentation Resources

Visit the RUCKUS website to locate related documentation for your product and additional RUCKUS resources.

Release Notes and other user documentation are available at <https://support.ruckuswireless.com/documents>. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a RUCKUS Support Portal user account. Other technical documentation content is available without logging in to the RUCKUS Support Portal.

White papers, data sheets, and other product documentation are available at <https://www.ruckuswireless.com>.

Online Training Resources

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at <https://commscopeuniversity.myabsorb.com/>.

Document Conventions

The following table lists the text conventions that are used throughout this guide.

TABLE 1 Text Conventions

Convention	Description	Example
monospace	Identifies command syntax examples	<code>device(config)# interface ethernet 1/1/6</code>
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the Start menu, click All Programs .
<i>italics</i>	Publication titles	Refer to the <i>RUCKUS Small Cell Release Notes</i> for more information.

Notes, Cautions, and Safety Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE

A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION

An ATTENTION statement indicates some information that you must read before continuing with the current action or task.



CAUTION

A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.



DANGER

A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
<i>italic text</i>	Identifies a variable.
[]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{x y z}	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, <i>member[member...]</i> .
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Overview of Using SAML as an Authentication Server for Cloudpath

Security Assertion Markup Language (SAML) 2.0 is one of several authentication-server methods that Cloudpath supports.

SAML 2.0 is an XML-based protocol that uses security tokens containing assertions to pass information about an end user between a SAML Identity Provider (IdP) and a SAML Service Provider (SP).

To establish trust between Cloudpath and a SAML IdP, configuration is required on both Cloudpath and the IdP.

Required Parameters

The following are required parameters with any SAML authentication:

- IdP Metadata URL: URL of the SAML metadata file. IdPs typically publish SAML metadata at a publicly available URL. The Cloudpath system periodically fetches the metadata from this URL to obtain configuration details about the desired SAML communication options that the IdP requires.
- Entity IDs: An entity ID is a globally unique name for a SAML entity - either an IdP or an SP:
 - IdP Entity ID: The IdP *entityID* is the identity of the identity provider. Example: https://idp_name.example.edu/idp
 - SP Entity ID: The SP *entityID* is the identity of the service provider. Example: https://sp_name.example.edu/sp

Using SSOCircle as the SAML Identity Provider

Proceeding With One of the Tested SAML Configurations

NOTE

The SP Entity ID URI uniquely identifies the Cloudpath SAML authentication server as a Service Provider (SP) to the IdP. This becomes the *entityID* attribute of the *EntityDescriptor* element within the SP metadata XML that gets uploaded to the IdP. Changing this value after configuration has been completed requires the service provider metadata to be re-uploaded to the IdP.

Proceeding With One of the Tested SAML Configurations

This document presents four different, tested methods that you can use in which SAML is the authentication server:

- [Using SSOCircle as the SAML Identity Provider](#) on page 8
- [Using Shibboleth as the SAML Identity Provider](#) on page 21
- [Using Gluu as the SAML Identity Provider](#) on page 27
- [Using Google G Suite as the SAML Identity Provider](#) on page 40

Using SSOCircle as the SAML Identity Provider

You can use SSOCircle as the public SAML IdP with a tested Cloudpath configuration.

SSOCircle provides a ready-to-use Identity Provider that uses several strong 2-factor authentication methods.

Basic Tasks for Using SSOCircle

Configure SAML using SSOCircle as the IdP by performing the following tasks sequentially:

1. [Adding a SAML Step To Your Workflow](#) on page 8
2. [Adding the SSOCircle SAML Authentication Server to the Workflow](#) on page 9
3. [Downloading the SAML Metadata for SSOCircle](#) on page 13
4. [Configuring Your Account on SSOCircle](#) on page 15
5. [Publishing the Workflow for SAML SSOCircle](#) on page 20
6. [Testing the User Experience for SAML SSOCircle](#) on page 20

Adding a SAML Step To Your Workflow

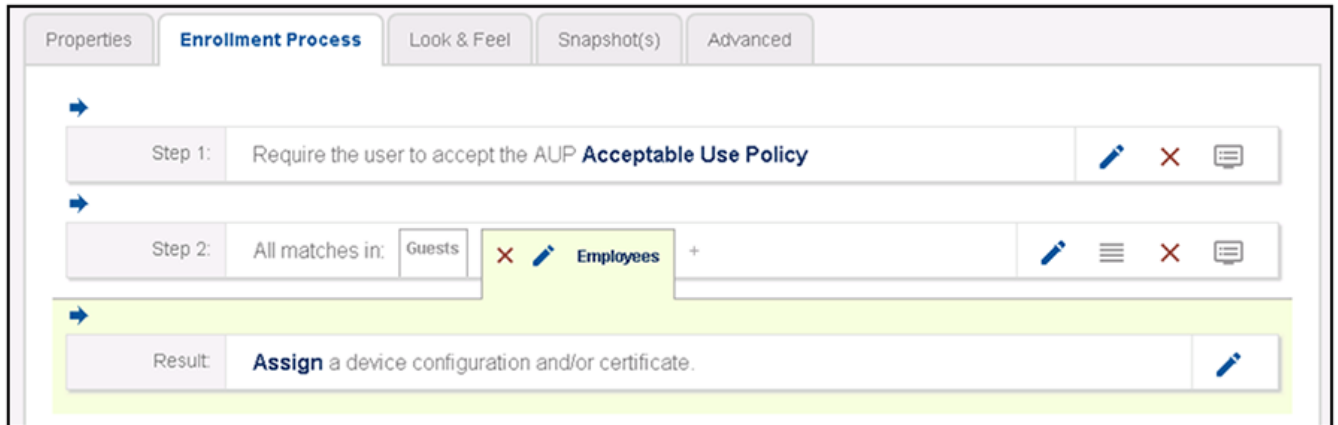
A SAML authentication server may be added to the workflow in place of a traditional Active Directory or LDAP server for authenticating users.

Determine in which branch and in which step to add a SAML authentication server plug-in to the workflow. For example, in the default workflow, you might create a split for Guests and Employees, and you could then use a SAML authentication server instead of the Active Directory authentication server, as shown below.

1. Log in to the Cloudpath user interface.
2. Go to **Configuration > Workflows**.
3. Click on a workflow (or create a new one) for which you want to configure SAML as the authentication server.

4. Highlight the tab in the workflow where you want to add the SAML authentication-server step. In this example below, it is the **Employees** tab.

FIGURE 1 Adding a SAML Step To Your Workflow

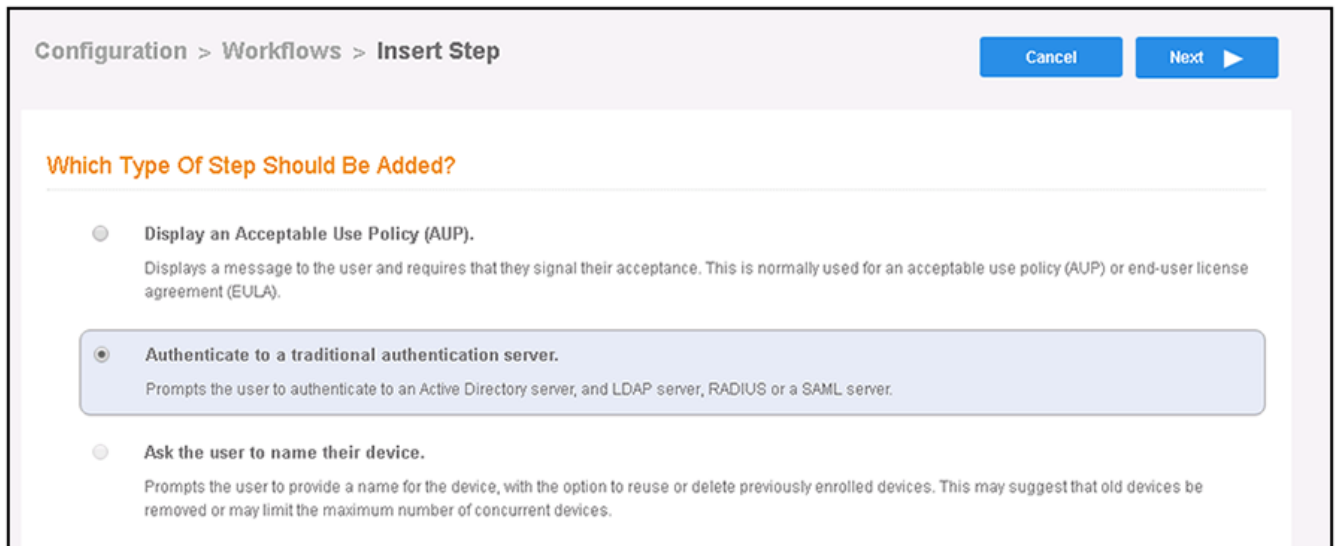


5. With the **Employees** branch of the workflow highlighted, click the blue arrow to insert a step below the Guests/Employees split.

Adding the SSOCircle SAML Authentication Server to the Workflow

1. Once you click the arrow to insert the SAML step, you receive the following prompt:
"Which Type Of Step Should Be Added?"
2. Select the button to authenticate to a traditional authentication server, as shown in the following screen:

FIGURE 2 Authenticate to a Traditional Authentication Server



3. Click **Next**.

Using SSO Circle as the SAML Identity Provider

Adding the SSO Circle SAML Authentication Server to the Workflow

4. If you have already defined an authentication server, you will get a prompt asking whether you want to reuse an existing authentication server or define a new authentication server. Choose the radio button to define a new authentication server, then click **Next**.
5. On the Authentication Server Configuration screen, select the **Connect to SAML** radio button:

FIGURE 3 Authentication Server Configuration Screen

The screenshot displays the 'Authentication Server Configuration' interface. At the top, the title 'Authentication Server Configuration' is shown in orange. Below it, there are five radio button options for selecting an authentication method:

- Connect to Active Directory**: Select this option to enable end-users to authenticate via Active Directory. This option is currently selected. It includes fields for: Default AD Domain (example: test.sample.local), AD Host (example: ldaps://192.168.4.2), AD DN (example: dc=test,dc=sample,dc=local), and AD Username Attribute (dropdown menu showing 'SAM Account Name').
- Connect to LDAP**: Select this option to enable end-users to authenticate via LDAP (or LDAPs).
- Connect to RADIUS**: Select this option to enable end-users to authenticate via RADIUS using PAP.
- Connect to SAML**: Select this option to enable end-users to authenticate via a SAML 2.0 IdP.
- Use Onboard Database**: Select this option to enable end-users to authenticate to accounts defined within this system.

Under the 'Connect to Active Directory' section, there are three sub-sections:

- Verify Account Status On Each Authentication**: Includes a checkbox for 'Perform Status Check' which is currently unchecked.
- Additional Logins**: Includes checkboxes for 'Use For Admin Logins' (unchecked) and 'Use For Sponsor Logins' (checked).
- Test Authentication**: Includes a checkbox for 'Run Authentication Test?' which is currently unchecked.

6. Complete the configuration as shown in the example below:

NOTE

You can click the "i" icons next to the field names to obtain the information required for each field.

FIGURE 4 SAML Configuration Fields for SSOCircle

The screenshot shows a configuration interface for SAML. It is titled "Connect to SAML" and includes a sub-header "Required SAML Information". Below this, there are four fields: "IdP Metadata Type" (a dropdown menu set to "URL"), "IdP Metadata URL" (text input: "https://idp.ssocircle.com"), "IdP EntityID" (text input: "https://idp.ssocircle.com"), and "SP EntityID" (text input: "urn:testsaml:cloudpath:Jeff").

Below the "Required SAML Information" section is the "SAML Attribute to Enrollment Mappings" section. It features a row of "Attribute Mapping Templates" with buttons for "eduPerson", "InCommon", "InetOrgPersonX.500", "Generic", and "Blank". The "eduPerson" template is selected. Below this, there are ten rows, each with an attribute name and a corresponding text input field:

- Username Attribute: EmailAddress
- Common Name Attribute: [ex. eduPersonPrincipalName]
- Affiliation/Group Attribute: [ex. eduPersonAffiliation]
- Email Attribute: EmailAddress
- First Name Attribute: FirstName
- Last Name Attribute: LastName
- City Attribute: (empty)
- State Attribute: (empty)
- Country Attribute: (empty)

- Required SAML Configuration section:
 - IdP Metadata Type: Use the **URL** option.
 - IdP Metadata URL: Enter the URL of: **https://idp.ssocircle.com**
 - IdP EntityID: Enter the URL of: **https://idp.ssocircle.com**
 - SP EntityID: Enter the string **urn:testsaml:cloudpath:**followed by your first name. For example: **urn:testsaml:cloudpath:Jeff**
- SAML Attribute to Enrollment Mappings - Required fields:
 - Username Attribute: Must be **EmailAddress**

Using SSO Circle as the SAML Identity Provider

Adding the SSO Circle SAML Authentication Server to the Workflow

- Email Attribute: Must be **EmailAddress**
- First Name Attribute: Must be **FirstName**
- Last Name Attribute: Must be **LastName**

NOTE

You can use defaults for the remaining fields.

- SAML Options (not shown in the screen shot above): Use all default settings.

7. Click **Next**.

The Server Certificate Information screen appears:

FIGURE 5 Pin or Upload the Current Server Certificate

Configuration > Workflows > Insert Step

Server Certificate Information

To authenticate via a SAML Identity Provider (IdP), the system needs to know which IdP HTTP SSL server certificate to accept.

Pin the Current Server Certificate.
Pin the current server certificate as a trusted certificate. This is the quickest and easiest but must be updated when the certificate is renewed.

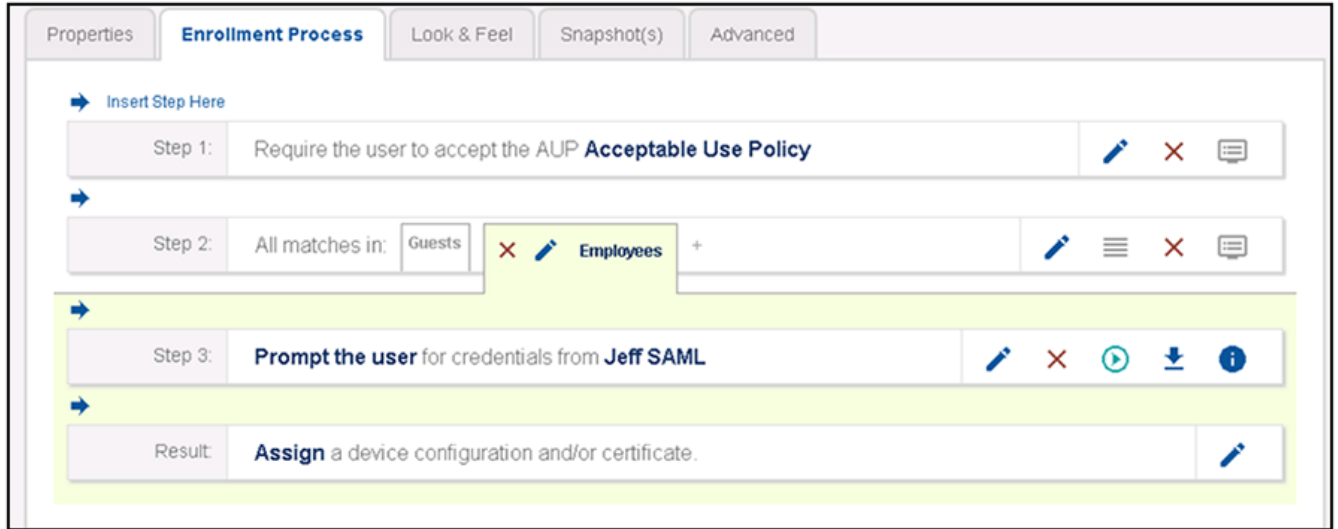
Common Name:	idp.ssocircle.com
Thumbprint:	A7EB9902CC73F903DCEAA09B48A8147998B4F7C5
Valid Period:	12/11/2017 - 03/11/2018
Issued By:	Let's Encrypt Authority X3

Upload the Chain for the Server Certificate.
Select this option to specify the common name of the LDAPS server certificate and to upload the issuing CA. This provides the most resilient form of server certificate validation and does not normally require updates when the certificate is renewed.

8. You can leave the **Pin the Current Server Certificate** radio button selected, or you can select the other radio button and upload the CA certificate for the SAML server (if you have that certificate). Whichever method you choose, click **Next** when you are done.

You are returned to the workflow screen, as shown in the example below:

FIGURE 6 Workflow After SAML Has Been Configured as Authentication Server



Downloading the SAML Metadata for SSOCircle

1. In the workflow, click the arrow (circled in red in the figure below) to download the SAML metadata:

FIGURE 7 Download Icon in Workflow for SAML Metadata



Using SSO Circle as the SAML Identity Provider
Downloading the SAML Metadata for SSO Circle

2. You will need to copy the contents to a clipboard in upcoming steps. For now, you can open the metadata file using Notepad to view the contents.

A snippet of what this metadata should look like is shown below:

FIGURE 8 SAML Metadata Snippet for SSO Circle

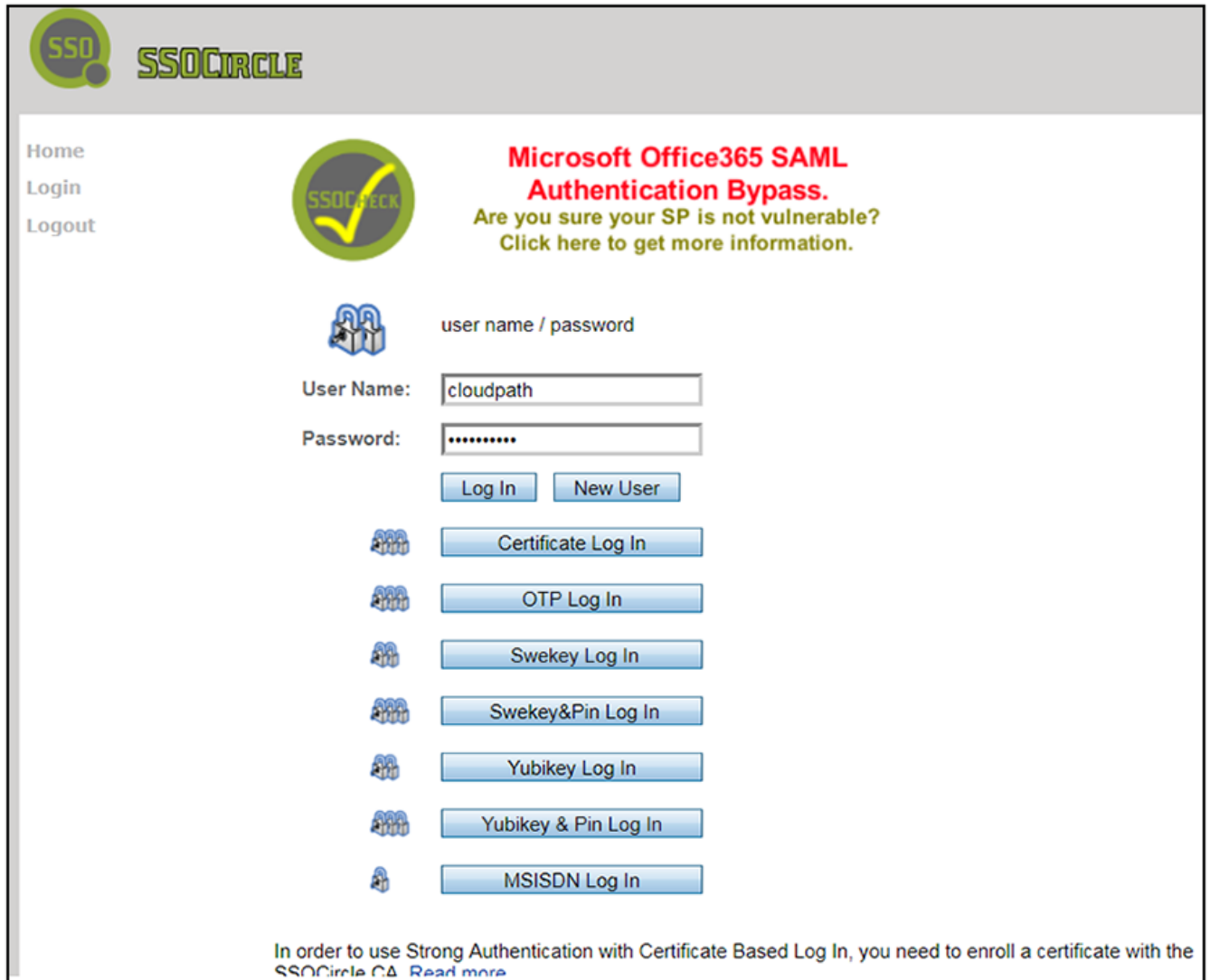
```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="urn:testsaml:cloudpath:Jeff" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
MA4GA1UECBMHQXJpem9uYTEtMBEgA1UEBxMKU2NvdHRzZGFsZTEaMBGGA1UEChMR29EYWRkeS5j
b20sIEluYy4xLTArBgNVBAsTJGh0dHA6Ly9jZKJ0cy5nb2RhZGR5LmNvbS9yZXBvc210b3J5LzEz
MDEGA1UEAxMqR28gRGFkZkZkZkU2VjdXJlIENlcnRpZmljYXR1IEF1dGhvcml0eSA0IENyMB4XDTE3
MTIwODAwMDkxMDEwODAwMDkxMDEwODAwMDkxMDEwODAwMDkxMDEwODAwMDkxMDEwODAwMDkxMDEw
aWRhdGVkMSIwIAYDVQQDDBkqLnd3aWUucnVja3Vzd2lyZWxlc3MuY29tMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAkqyJcvoQhHwT7ktxy9HjKo1Of1s5SHwvoULd7PrCTxJ14GB4dxY/
D8IrbzuwCtWdi1sMLU4JjSBpgN9/gFuazZmEpa7CAhEQj7vvrQow081HvTNeToso56dgnxJg16YE
9OsFfVVMb1QKwyn1XUiflp3Qjs3swMokbIJ2pyqNQYExdwq1RdcJe15+t8LndGUGkfgM/RwsFg9C
j03Apa++47S5LIsBR9Pr7/tgSqZJHUHtESbky6LO6oyY+uVowXsSFNEsJ0ExjbbC/h28oDqmA3
o6bW+t1JwMh6qQUGN1JEZruKw6spocHqbQAWx15OL0GONVzEoLPovdQQ16WsIwIDAQABo4IB0DCC
AcwDAYDVR0TAQH/BAIwADAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAWIwDgYDVR0PFAQH/
BAQDAgWgMDcGAlUdHwQwMC4wLKAQoCiGJmh0dHA6Ly9jcmwuZ29kYWRkeS5jb20vZ2RwZzJzMS03
OTQuY3JSMF0GA1UdIARWMFQwSAYLYIZIAYb9bQEHFwEwOTA3BggrBgEFBQcCARYraHR0cDovL2N1
enRzZm14YXVlbnV5LmNvbS9yZXBvc210b3J5LzEzMDUwODAwMDkxMDEwODAwMDkxMDEwODAwMDkxMDEw
```

Configuring Your Account on SSO Circle

1. In a browser, go to the following URL: <https://idp.ssocircle.com/sso/UI/Login>

The SSO login screen appears.

FIGURE 9 SSO Login Screen



Use your credentials to log in (or create a new account if you do not already have one):

2. Click **Log In**.

The User Profile screen appears, as shown in the following example screen:

FIGURE 10 User Profile Screen

The screenshot shows a user profile page with a left sidebar and a main content area. The sidebar contains several menu items: Logout, My Profile, My SAML Federations, My OpenID Trust, My Client Certificate, Manage Metadata, My Identity Graph, SSO Check, My Audit, My Debug, My Monitor, and My Subscriptions. The main content area is titled "User Profile" and contains a table with two columns: "Attribute" and "Value".

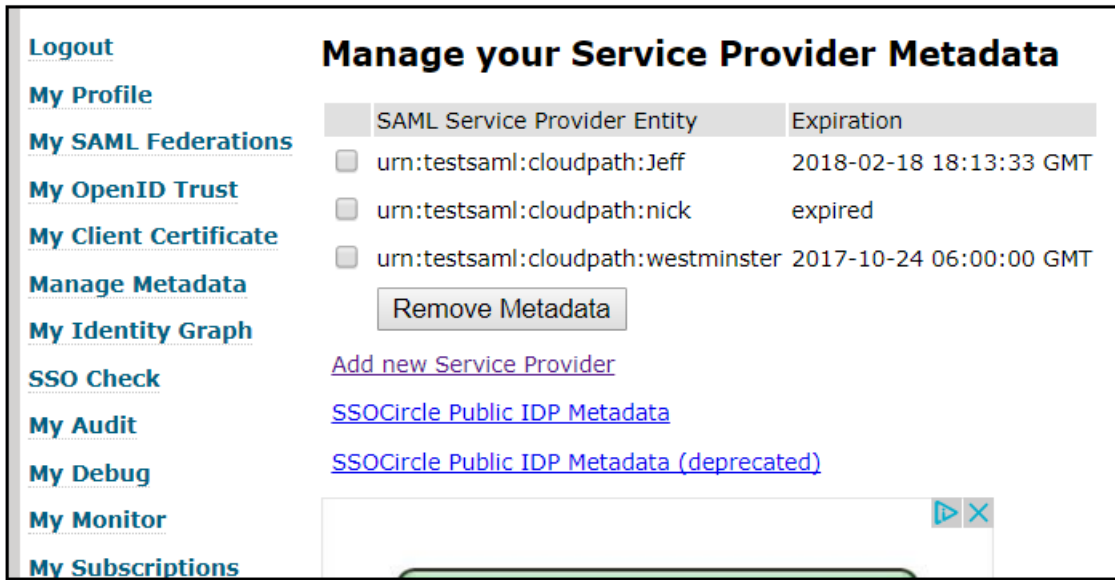
Attribute	Value
User ID	cloudpath
Google Apps Email.	No longer available
OpenID 1.0 Identifier	http://cloudpath.ssocircle.com
Client Certificate	Not Enrolled
Given name	<input type="text" value="Cloudpath"/>
Surname	<input type="text" value="SAMLTest"/>
Email	<input type="text" value="user@cloudpath.net"/>
ePass OTP token number	not assigned
Yubikey ID	<input type="text" value="not assigned"/>
Yubikey PIN	<input type="text" value="....."/>
Swekey ID detect	<input type="text" value="not assigned"/>
Swekey PIN	<input type="text" value="....."/>
MSISDN identification	<input type="text" value="not active"/>
Password (length > 8)	<input type="text"/>
Retype Password	<input type="text"/>

At the bottom of the table is a "Submit" button.

3. Click **Manage Metadata** on the left side of the screen.

The **Manage your Service Provider Metadata** screen appears:

FIGURE 11 Manage your Service Provider Metadata Screen



4. Click the **Add new Service Provider** link.

The **SAML Service Provider Metadata Import** screen appears:

FIGURE 12 SAML Service Provider Metadata Import Screen

SAML Service Provider Metadata Import

Logout Terminate your session

My Profile **User ID: cloudpath**

My SAML Federations

My OpenID Trust

My Client Certificate

Manage Metadata **Enter the FQDN of the Service Provider ex.: sp.cohos.de**

My Identity Graph

SSO Check

My Audit

My Debug

My Monitor

My Subscriptions

Attributes sent in assertion (optional)

FirstName

LastName

EmailAddress

UserID

Insert the SAML Metadata information of your SP
If your SP does not provide a XML formatted SAML Metadata document, you can build it [here](#)

5. On the **SAML Service Provider Metadata Import** screen, do the following:
 - a) For the FQDN, enter the SP Entity ID exactly as you entered it in your Cloudpath system: **urn:testsaml:cloudpath:<your first name>**. See [Figure 4](#) on page 11.
 - b) In the Attributes section, check **FirstName**, **LastName**, and **EmailAddress**.
 - c) In the **Insert the SAML Metadata information of your SP** section, copy and paste the entire contents of the metadata file that you downloaded earlier into the box provided. (Make sure there is no white space before the pasted contents.)

Once you have entered the necessary information, the **SAML Service Provider Metadata Import** screen should look similar to the following (not all of the metadata is shown below, however):

FIGURE 13 SAML Service Provider Metadata Import Screen After Information is Entered

SAML Service Provider Metadata Import

User ID: cloudpath
Submit

Enter the FQDN of the ServiceProvider ex.: sp.cohos.de
urn:testsaml:cloudpath:Jeff

Attributes sent in assertion (optional)

FirstName
 LastName
 EmailAddress
 UserID

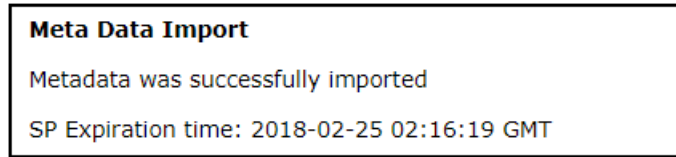
Insert the SAML Metadata information of your SP
If your SP does not provide a XML formatted SAML Metadata document, you can build it [here](#)

```
nRyb2wgVmFs
awRh�GVkMSIwIAYDVQODDBkqLnd3awUucnVja3Vzd2lyZlwxlc3MuY29tMIIIBIjANB
gkqhkIG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAKqyJcvoQhHwT7ktxy9HjKo1Of1s5SHwvoULd7PrCT
xJ14GB4dxY/
D8IrbzuwCtWd1sMLU4JjSBpgN9/gFuaZZmEpa7CAhEQj7vvrQow081HvTNeToso5
6dgnxJg16YE
9OsFfVVMb1QKwyn1XUiflp3QjS3swM0kbIJ2pyqNQYExdwq1RdcJe15+t8LndGUGk
fqM/RwsFg9C
j03ApA++47S5LI5BR9Pr7/tgSqZJHUHTESbky6L06oyY+uVowXsSFNEsJJoExjhb
C/h28oDqmA3
o6bw+t1JwMh6QUGN1JEZruKw6spocHqbQAwx15OL0GONVzEoLPovdQQ16WsIwIDA
QABo4IB0DCC
AcwwDAYDVR0TAQH/BAIwADAdBgNVHSUEFjAUBgggrBgEFBQcDAQYIKwYBBQUHAwIwD
gYDVR0PAAQH/
BAQDAgWgMDCGA1UdHwQwMC4wLKAqoCiGJmh0dHA6Ly9jcmwuz29kYWRkeS5jb20vZ
2RpZzJzMS03
OTQuY3JsMF0GA1UdIARlMFQwSAYLYIZIAYb9bQEHFwEwOTA3BgggrBgEFBQcCARYra
HR0cDovL2N1
cnRpZm1jYXR1cy5nb2RhZGR5LmNvbS9yZXBvc210b3J5LzAIBGZngQwBAgEwdgYIK
wYBBQUHAQEE
ajBoMCQGCCsGAQUFBzABhhodHRwOi8vb2NzcC5nb2RhZGR5LmNvbS8wYAYIKwYBB
QUHMAKGNhG0
dHA6Ly9jZXJ0awZpY2F0ZXMuZ29kYWRkeS5jb20vcmlvbnNpdG9yeS9nZGl1e31j
nQwHwYDVR0j
RRwFgALVOMQ7147MNTAw5dDYJ2v8LQcM4wDQYDVR0BBPDAALIT7K45Zd311Le31Y
```

6. Click **Submit**.

If the import is successful, you will receive a message such as the following:

FIGURE 14 Metadata-Import -Successful Message



7. Click **Logout**.

Publishing the Workflow for SAML SSO Circle

1. Return to the workflow on your Cloudpath system by navigating to the **Configuration > Workflows** screen.
2. Complete the workflow by adding a device configuration. Refer to [Adding a Device Configuration to Your Workflow](#) on page 57.
3. Publish the workflow by clicking the Publish icon to the left of the workflow name.

Testing the User Experience for SAML SSO Circle

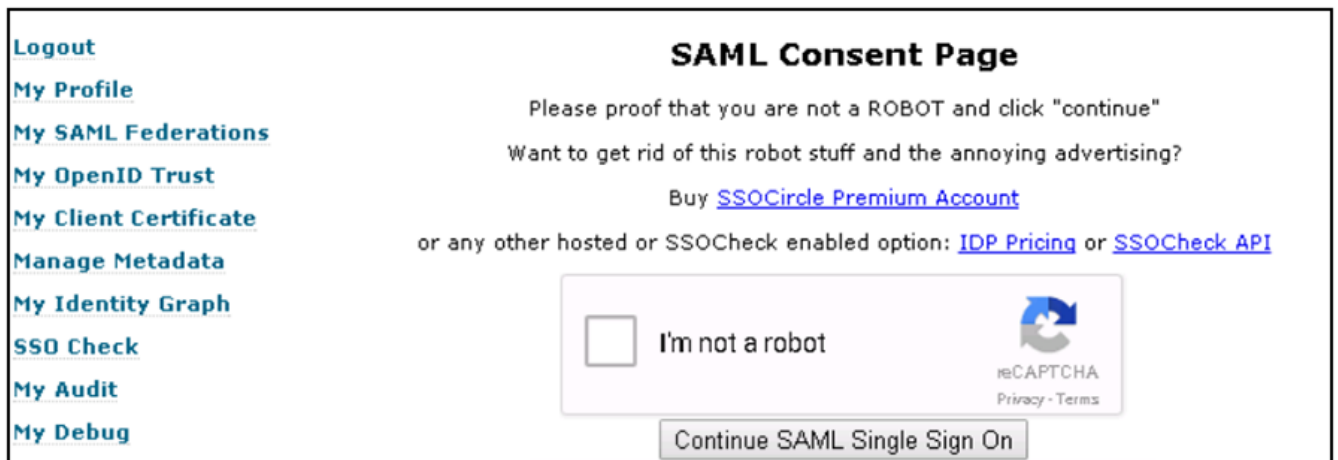
1. Test the enrollment process by clicking on the enrollment portal URL for the workflow at the top of the **Configuration > Workflows** screen.
2. When you are presented with the Welcome screen, click **Start**.
3. When you are presented with various branches of your workflow, navigate down a branch that uses the SAML authentication server you just configured.

You are directed to the SSO Circle login page.

4. Log in with your credentials.

The SAML consent page appears:

FIGURE 15 SAML Consent Page



5. Check the "I'm not a robot" box, and follow the on-screen instructions.
6. When a green check mark appears next to the "I'm not a robot" box, click **Continue SAML Single Sign On**.
7. If the SAML authentication is successful, you are returned to the Cloudpath system, where you can continue with the enrollment.

Using Shibboleth as the SAML Identity Provider

You can use Shibboleth as the public SAML IdP with a tested Cloudpath configuration.

Shibboleth allows users to securely send trusted information about themselves to remote resources. This information can be used for authentication, authorization, content personalization, and enabling single sign-on from many different providers.

Basic Tasks for Using Shibboleth

Configure SAML using Shibboleth as the IdP by performing the following tasks sequentially:

1. [Adding a SAML Step To Your Workflow](#) on page 21
2. [Adding the Shibboleth SAML Authentication Server to the Workflow](#) on page 22
3. [Downloading the Shibboleth SAML Metadata](#) on page 26
4. [Adding the Metadata to Your Shibboleth Identity Service Provider](#) on page 26
5. [Publishing the Workflow for SAML Shibboleth](#) on page 27
6. [Testing the User Experience for SAML Shibboleth](#) on page 27

Adding a SAML Step To Your Workflow

A SAML authentication server may be added to the workflow in place of a traditional Active Directory or LDAP server for authenticating users.

Determine in which branch and in which step to add a SAML authentication server plug-in to the workflow. For example, in the default workflow, you might create a split for Guests and Employees, and you could then use a SAML authentication server instead of the Active Directory authentication server, as shown below.

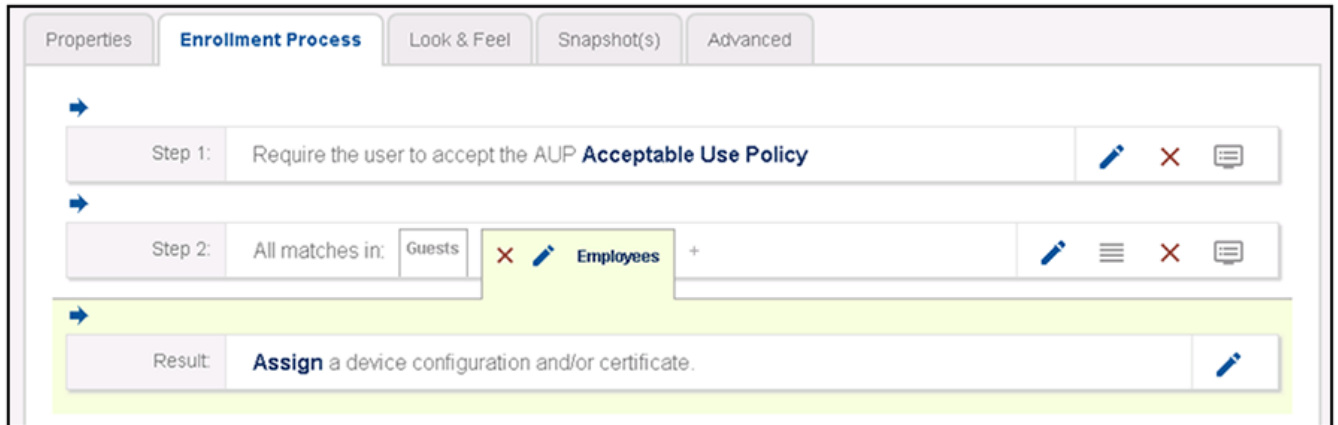
1. Log in to the Cloudpath user interface.
2. Go to **Configuration > Workflows**.
3. Click on a workflow (or create a new one) for which you want to configure SAML as the authentication server.

Using Shibboleth as the SAML Identity Provider

Adding the Shibboleth SAML Authentication Server to the Workflow

4. Highlight the tab in the workflow where you want to add the SAML authentication-server step. In this example below, it is the **Employees** tab.

FIGURE 16 Adding a SAML Step To Your Workflow

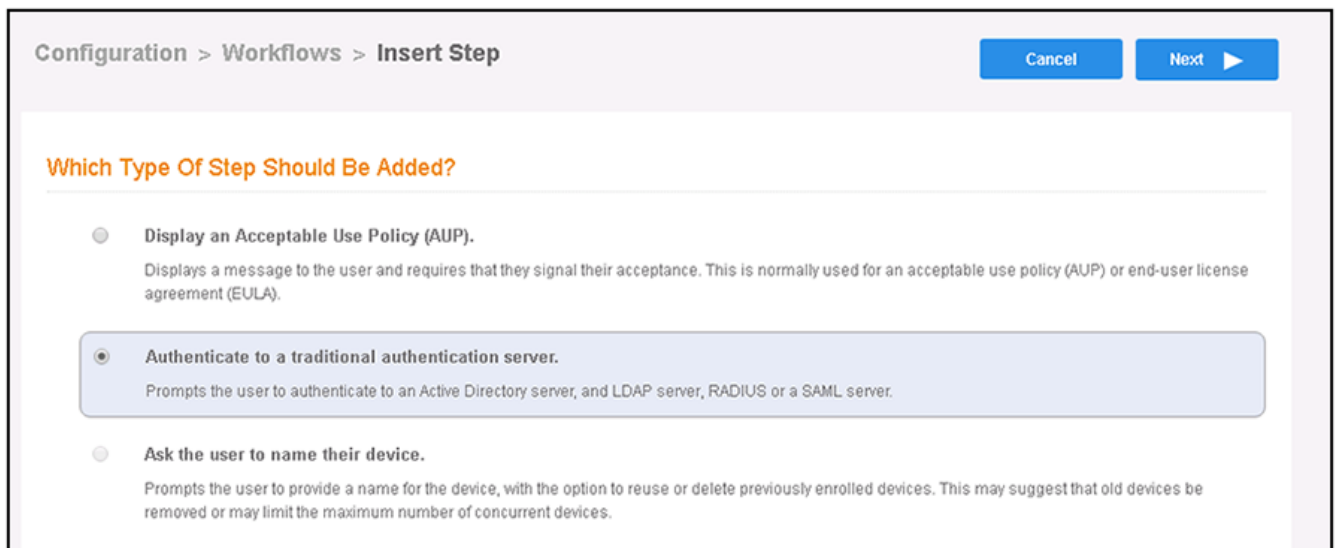


5. With the **Employees** branch of the workflow highlighted, click the blue arrow to insert a step below the Guests/Employees split.

Adding the Shibboleth SAML Authentication Server to the Workflow

1. Once you click the arrow to insert the SAML step, you receive the following prompt:
"Which Type Of Step Should Be Added?"
2. Select the button to authenticate to a traditional authentication server, as shown in the following screen:

FIGURE 17 Authenticate to a Traditional Authentication Server



3. Click **Next**.

4. If you have already defined an authentication server, you will get a prompt asking whether you want to reuse an existing authentication server or define a new authentication server. Choose the radio button to define a new authentication server, then click **Next**.
5. On the Authentication Server Configuration screen, select the **Connect to SAML** radio button:

FIGURE 18 Authentication Sever Configuration Screen

The screenshot displays the 'Authentication Server Configuration' interface. At the top, the title 'Authentication Server Configuration' is shown in orange. Below the title, there are five main configuration options, each with a radio button and a descriptive sub-header:

- Connect to Active Directory**: Select this option to enable end-users to authenticate via Active Directory. It includes fields for 'Default AD Domain' (example: test.sample.local), 'AD Host' (example: ldaps://192.168.4.2), 'AD DN' (example: dc=test,dc=sample,dc=local), and 'AD Username Attribute' (dropdown menu showing 'SAM Account Name').
- Verify Account Status On Each Authentication**: A section with a checkbox for 'Perform Status Check'.
- Additional Logins**: A section with checkboxes for 'Use For Admin Logins' and 'Use For Sponsor Logins' (which is checked).
- Test Authentication**: A section with a checkbox for 'Run Authentication Test?'.
- Connect to LDAP**: Select this option to enable end-users to authenticate via LDAP (or LDAPs).
- Connect to RADIUS**: Select this option to enable end-users to authenticate via RADIUS using PAP.
- Connect to SAML**: This option is selected with a filled radio button. The description is 'Select this option to enable end-users to authenticate via a SAML 2.0 IdP.'
- Use Onboard Database**: Select this option to enable end-users to authenticate to accounts defined within this system.

Using Shibboleth as the SAML Identity Provider

Adding the Shibboleth SAML Authentication Server to the Workflow

- Complete the configuration. An example configuration screen is shown below, and descriptions of the fields follow the screen.

NOTE

You can click the "i" icons next to the field names to obtain the information required for each field.

FIGURE 19 SAML Configuration Fields for Shibboleth

The screenshot shows a configuration interface for connecting to a SAML Identity Provider (IdP). The main heading is "Connect to SAML" with a sub-instruction: "Select this option to enable end-users to authenticate via a SAML 2.0 IdP." Below this, there are two main sections:

- Required SAML Information:** This section contains four fields, each with an information icon (i) to its left:
 - IdP Metadata Type:** A dropdown menu set to "URL".
 - IdP Metadata URL:** A text input field containing "https://testshib.org/metadata/testshib-providers.xml".
 - IdP EntityID:** A text input field containing "https://idp.testshib.org/idp/shibboleth".
 - SP EntityID:** A text input field containing "urn:testsaml:cloudpath:Jeff".
- SAML Attribute to Enrollment Mappings:** This section starts with "Attribute Mapping Templates:" and has five buttons: "eduPerson", "InCommon", "InetOrgPersonX.500", "Generic", and "Blank". Below this are 15 rows of attribute mappings, each with an information icon (i) and a text input field:
 - Username Attribute:** uid
 - Common Name Attribute:** eduPersonPrincipalName
 - Affiliation/Group Attribute:** eduPersonAffiliation
 - Email Attribute:** eduPersonPrincipalName
 - First Name Attribute:** givenName
 - Last Name Attribute:** sn
 - City Attribute:** (empty)
 - State Attribute:** (empty)
 - Country Attribute:** (empty)
 - OU Attribute:** (empty)
 - Distinguished Name Attribute:** cn
 - Company Attribute:** (empty)
 - Department Attribute:** (empty)
 - Office Name Attribute:** (empty)

- Required SAML Configuration section:
 - IdP Metadata Type: Use the **URL** option.
 - IdP Metadata URL and IdP EntityID: These URLs should be in a format similar to: **idp.<customer_ shibboleth_ server>.org**
 - SP EntityID: Enter the string **urn:testsaml:cloudpath:** followed by your first name. For example: **urn:testsaml:cloudpath:Jeff**
- SAML Attribute to Enrollment Mappings - Required fields:
 - Username Attribute: Must be **uid**
 - Common Name Attribute: Must be **eduPersonPrincipal_Name**

- Affiliation/Group Attribute: Must be **eduPersonAffiliation**
- Email Attribute: Must be **eduPersonPrincipal_Name**
- First Name Attribute: Must be **givenName**
- Last Name Attribute: Must be **sn**
- Distinguished Name Attribute: Must be **cn**

NOTE

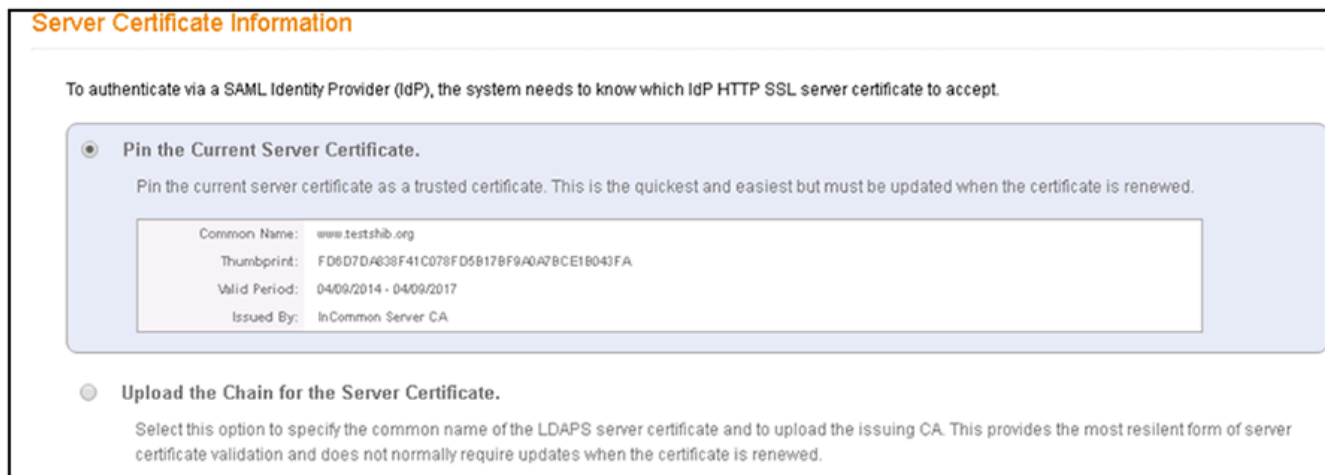
You can use defaults for the remaining fields.

- SAML Options (not shown in the screen shot above): Use all default settings.

7. Click **Next**.

The Server Certificate Information screen appears:

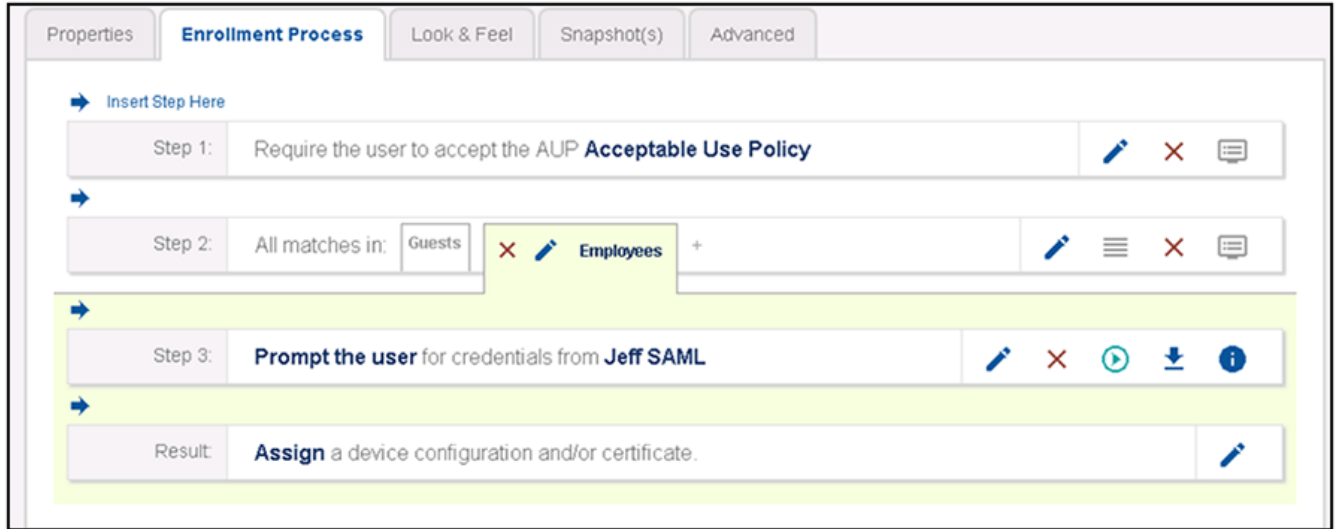
FIGURE 20 Pin or Upload the Current Server Certificate



8. You can leave the **Pin the Current Server Certificate** radio button selected, or you can select the other radio button and upload the CA certificate for the SAML server (if you have that certificate). Whichever method you choose, click **Next** when you are done.

You are returned to the workflow screen, as shown in the example below:

FIGURE 21 Workflow After SAML Has Been Configured as Authentication Server



Downloading the Shibboleth SAML Metadata

1. In the workflow, click the arrow (circled in red in the figure below) to download the SAML metadata:

FIGURE 22 Download Icon in Workflow for SAML Metadata



2. Save the XML metadata to a local file in the following format: `testsaml_cloudpath_<your_first_name>.xml`. Example: `testsaml_cloudpath_jeff.xml`

Adding the Metadata to Your Shibboleth Identity Service Provider

1. In a browser, go to the URL of your Shibboleth server.
2. On the Shibboleth site, click the **Choose File** button at the bottom of the screen.
3. Browse to select the metadata file that you previously downloaded, then click the **Upload File** button.

You should receive a message on the next screen that indicates that your metadata was uploaded successfully.

Publishing the Workflow for SAML Shibboleth

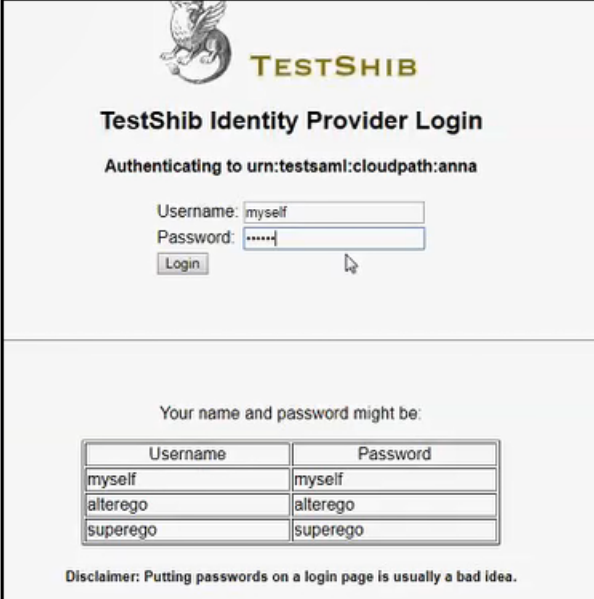
1. Return to the workflow on your Cloudpath system by navigating to the **Configuration > Workflows** screen.
2. Complete the workflow by adding a device configuration. Refer to [Adding a Device Configuration to Your Workflow](#) on page 57.
3. Publish the workflow by clicking the Publish icon to the left of the workflow name.

Testing the User Experience for SAML Shibboleth

1. Test the enrollment process by clicking on the enrollment portal URL for the workflow at the top of the **Configuration > Workflows** screen.
2. When you are presented with the Welcome screen, click **Start**.
3. When you are presented with various branches of your workflow, navigate down a branch that uses the SAML authentication server you just configured.

You are directed to the Shibboleth login page, such as the one shown in the following example:

FIGURE 23 Shibboleth Login During Enrollment



TESTSHIB

TestShib Identity Provider Login

Authenticating to urn:testsaml:cloudpath:anna

Username: myself

Password: ****

Login

Your name and password might be:

Username	Password
myself	myself
alterego	alterego
superego	superego

Disclaimer: Putting passwords on a login page is usually a bad idea.

4. Enter your credentials for your Shibboleth server, then click **Login**.
5. If the SAML authentication is successful, you are returned to the Cloudpath system, where you can continue with the enrollment.

Using Gluu as the SAML Identity Provider

You can use a Gluu server with Shibboleth Version 3 as the IdP with the Cloudpath server.

A Gluu server is a fully certified OpenID Provider that supports a number of OpenID Connect specifications.

Basic Tasks for Using Gluu

Configure SAML using Gluu as the IdP by performing the following tasks sequentially:

1. [Adding a SAML Step To Your Workflow](#) on page 28
2. [Adding the Gluu SAML Authentication Server to the Workflow](#) on page 28
3. [Downloading the SAML Metadata for Gluu](#) on page 33
4. [Connecting to the Gluu Identity Service Provider](#) on page 34
5. [Publishing the Workflow for SAML Gluu](#) on page 39
6. [Testing the User Experience for SAML Gluu](#) on page 39

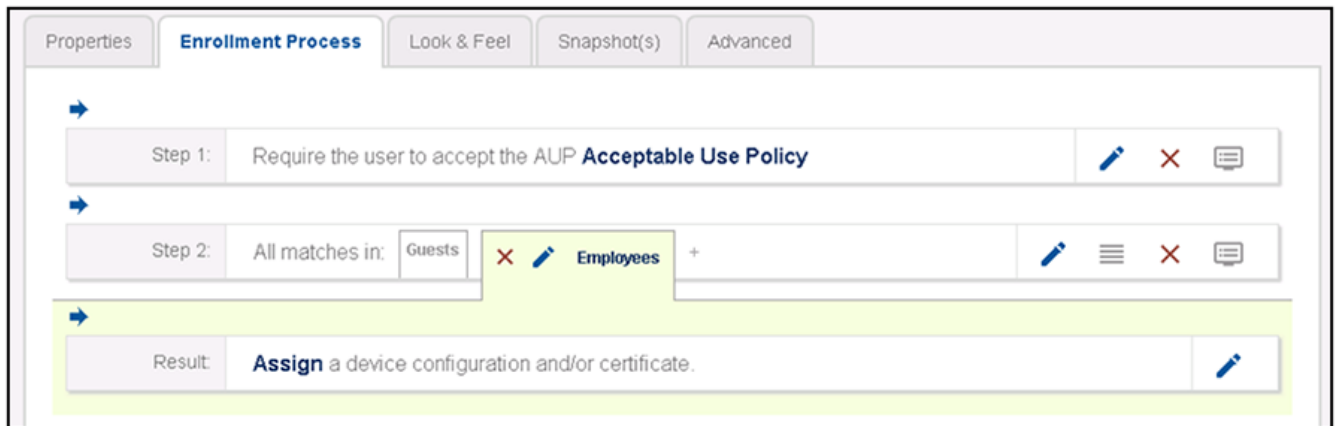
Adding a SAML Step To Your Workflow

A SAML authentication server may be added to the workflow in place of a traditional Active Directory or LDAP server for authenticating users.

Determine in which branch and in which step to add a SAML authentication server plug-in to the workflow. For example, in the default workflow, you might create a split for Guests and Employees, and you could then use a SAML authentication server instead of the Active Directory authentication server, as shown below.

1. Log in to the Cloudpath user interface.
2. Go to **Configuration > Workflows**.
3. Click on a workflow (or create a new one) for which you want to configure SAML as the authentication server.
4. Highlight the tab in the workflow where you want to add the SAML authentication-server step. In this example below, it is the **Employees** tab.

FIGURE 24 Adding a SAML Step To Your Workflow



5. With the **Employees** branch of the workflow highlighted, click the blue arrow to insert a step below the Guests/Employees split.

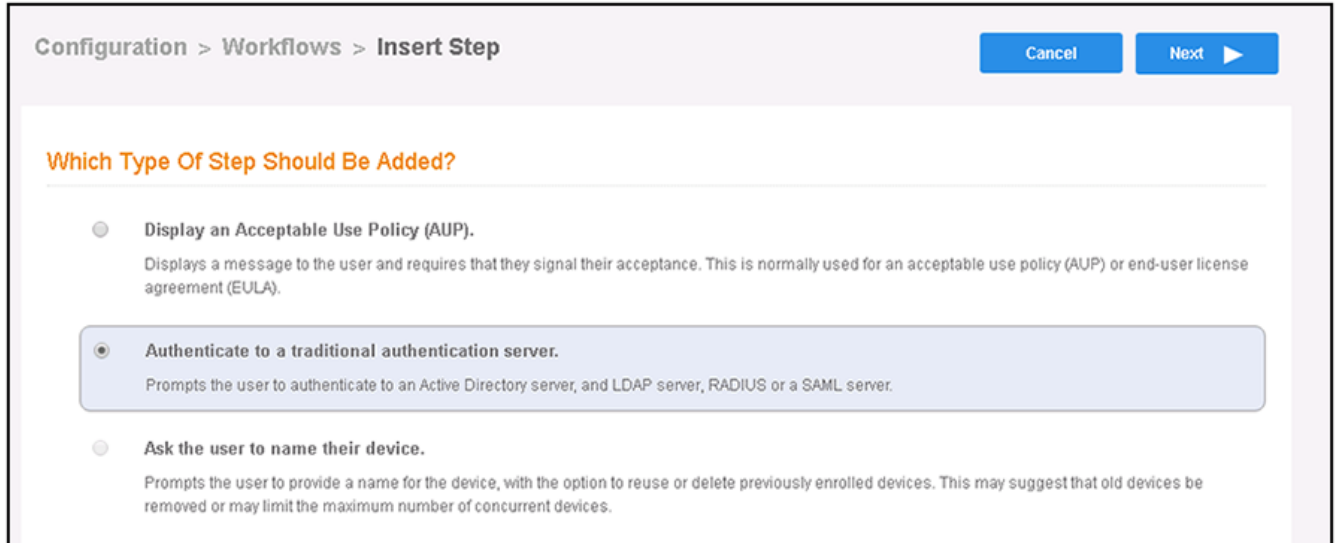
Adding the Gluu SAML Authentication Server to the Workflow

1. Once you click the arrow to insert the SAML step, you receive the following prompt:

"Which Type Of Step Should Be Added?"

2. Select the button to authenticate to a traditional authentication server, as shown in the following screen:

FIGURE 25 Authenticate to a Traditional Authentication Server



3. Click **Next**.
4. If you have already defined an authentication server, you will get a prompt asking whether you want to reuse an existing authentication server or define a new authentication server. Choose the radio button to define a new authentication server, then click **Next**.

Using Gluu as the SAML Identity Provider

Adding the Gluu SAML Authentication Server to the Workflow

5. On the Authentication Server Configuration screen, select the **Connect to SAML** radio button:

FIGURE 26 Authentication Sever Configuration Screen

The screenshot displays the 'Authentication Server Configuration' interface. At the top, the title 'Authentication Server Configuration' is shown in orange. Below the title, there are five radio button options for connecting to different authentication services. The 'Connect to SAML' option is selected, indicated by a filled radio button. The other options are 'Connect to Active Directory', 'Connect to LDAP', 'Connect to RADIUS', and 'Use Onboard Database'. The 'Connect to Active Directory' section is expanded, showing several configuration fields: 'Default AD Domain' (text input with placeholder '[ex. test.sample.local]'), 'AD Host' (text input with placeholder '[ex. ldaps://192.168.4.2]'), 'AD DN' (text input with placeholder '[ex. dc=test,dc=sample,dc=local]'), and 'AD Username Attribute' (dropdown menu with 'SAM Account Name' selected). Below these fields are three sections: 'Verify Account Status On Each Authentication' with a 'Perform Status Check' checkbox (unchecked), 'Additional Logins' with 'Use For Admin Logins' (unchecked) and 'Use For Sponsor Logins' (checked) checkboxes, and 'Test Authentication' with a 'Run Authentication Test?' checkbox (unchecked).

- Complete the configuration. An example configuration is shown in the screen below, followed by field descriptions.

NOTE

You can click the "i" icons next to the field names to obtain the information required for each field.

FIGURE 27 SAML Configuration Fields for GLUU

Connect to SAML
Select this option to enable end-users to authenticate via a SAML 2.0 IdP.

Required SAML Information

- IdP Metadata Type: URL
- IdP Metadata URL: https://test117.cloudpath.net/idp/shibboleth
- IdP EntityID: https://test117.cloudpath.net/idp/shibboleth
- SP EntityID: urn:testsaml:cloudpath:Jeff

SAML Attribute to Enrollment Mappings

Attribute Mapping Templates: eduPerson InCommon inetOrgPerson/X.500 Generic Blank

- Username Attribute: uid
- Common Name Attribute: cn
- Affiliation/Group Attribute: memberOf
- Email Attribute: mail
- First Name Attribute: gn
- Last Name Attribute: sn
- City Attribute: l
- State Attribute: st
- Country Attribute: c
- OU Attribute: ou
- Distinguished Name Attribute: cn
- Company Attribute: company
- Department Attribute: department
- Office Name Attribute: physicalDeliveryOfficeName

- Required SAML Configuration section:
 - IdP Metadata Type: Use the **URL** option.
 - IdP Metadata URL: Enter the URL, using your hostname. Example URL: **https://test117.cloudpath.net/idp/shibboleth**
 - IdP EntityID: Enter the URL, using your hostname. Example URL: **https://test117.cloudpath.net/idp/shibboleth**
 - SP EntityID: Enter the string **urn:testsaml:cloudpath:** followed by your first name. For example: **urn:testsaml:cloudpath:Jeff**
- SAML Attribute to Enrollment Mappings: Click the **inetOrgPerson/X.500** tab to automatically have the fields filled in.
- SAML Options (not shown in the screen shot above): Use all default settings.

Using Gluu as the SAML Identity Provider

Adding the Gluu SAML Authentication Server to the Workflow

7. Click **Next**.

The Server Certificate Information screen appears:

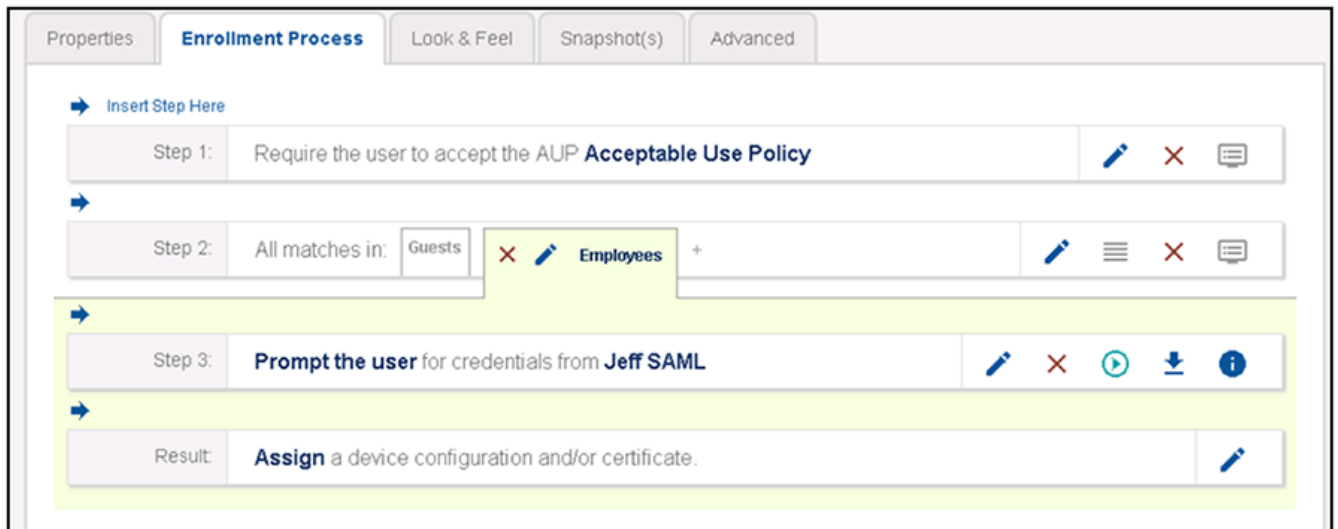
FIGURE 28 Pin or Upload the Current Server Certificate



8. You can leave the **Pin the Current Server Certificate** radio button selected, or you can select the other radio button and upload the CA certificate for the SAML server (if you have that certificate). Whichever method you choose, click **Next** when you are done.

You are returned to the workflow screen, as shown in the example below:

FIGURE 29 Workflow After SAML Has Been Configured as Authentication Server



Downloading the SAML Metadata for Gluu

1. In the workflow, click the arrow (circled in red in the figure below) to download the SAML metadata, and save it to a local file:

FIGURE 30 Download Icon in Workflow for SAML Metadata



2. You will need to copy the contents to a clipboard in upcoming steps. For now, you can open the metadata file using Notepad to view the contents.

A snippet of what the metadata should look like is shown below:

FIGURE 31 SAML Metadata Snippet for GLUU

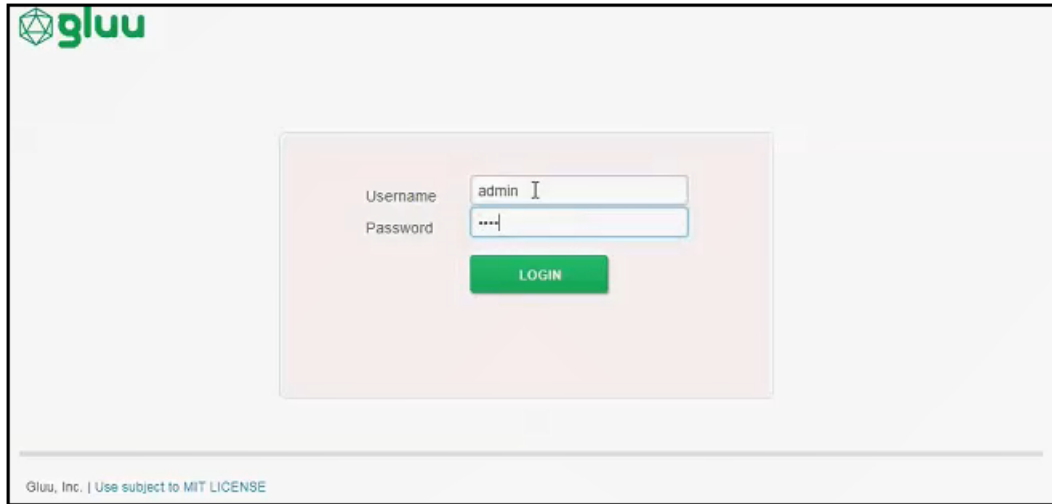
```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<!-- Copyright 2006-2018 Ruckus Wireless Inc. All rights reserved. -->
<!-- Use of this software is subject to, and signifies acceptance of, the Terms and Conditions. -->
<html>
<head>
  <META HTTP-EQUIV='X-UA-Compatible' content='IE=EDGE; IE=10; IE=9; IE=8; IE=7;' />
  <META HTTP-EQUIV='Content-Type' content='text/html; charset=utf-8' />
  <META name='cpnPageName' content='cp-general-error' />
  <title>Cloudpath ES</title>
  <script type='text/javascript' src='/admin/resources/js/jquery-1.6.2.min.js'></script>
  <script type='text/javascript' src='/admin/resources/js/jquery-ui-1.8.16.custom.min.js'></script>
  <script type='text/javascript' src='/admin/resources/js/jquery.jmesa.js'></script>
  <script type='text/javascript' src='/admin/resources/js/jmesa.js'></script>
  <script type='text/javascript' src='/admin/resources/js/jscolor.js'></script>
  <script type='text/javascript' src='/admin/resources/js/cloudpath.js'></script>
  <script type='text/javascript' src='/admin/resources/js/jquery.ptTimeSelect.js'></script>
  <script type='text/javascript' src='/admin/resources/js/svg.js'></script>
  <script type='text/javascript' src='/admin/resources/js/jquery.sparkline.js'></script>
  <script type='text/javascript' src='/admin/resources/js/d3.v3.min.js'></script>
  <script type='text/javascript'>jscolor.dir='/admin/resources/images/jscolor/'</script>
  <link type='text/css' href='/admin/resources/css/custom-theme/jquery-ui-1.8.16.custom.css' rel='stylesheet' />
  <link type='text/css' href='/admin/resources/css/cloudpath-base.css' rel='stylesheet' />
  <link type='text/css' href='/admin/resources/css/cloudpath-accordion-menu.css' rel='stylesheet' />
  <link type='text/css' href='/admin/resources/css/cloudpath-accordion-standard.css' rel='stylesheet' />
  <link type='text/css' href='/admin/resources/css/cloudpath-list.css' rel='stylesheet' />
```

Connecting to the Gluu Identity Service Provider

1. In a browser, go to the URL of your Gluu server.

The Gluu login screen appears.

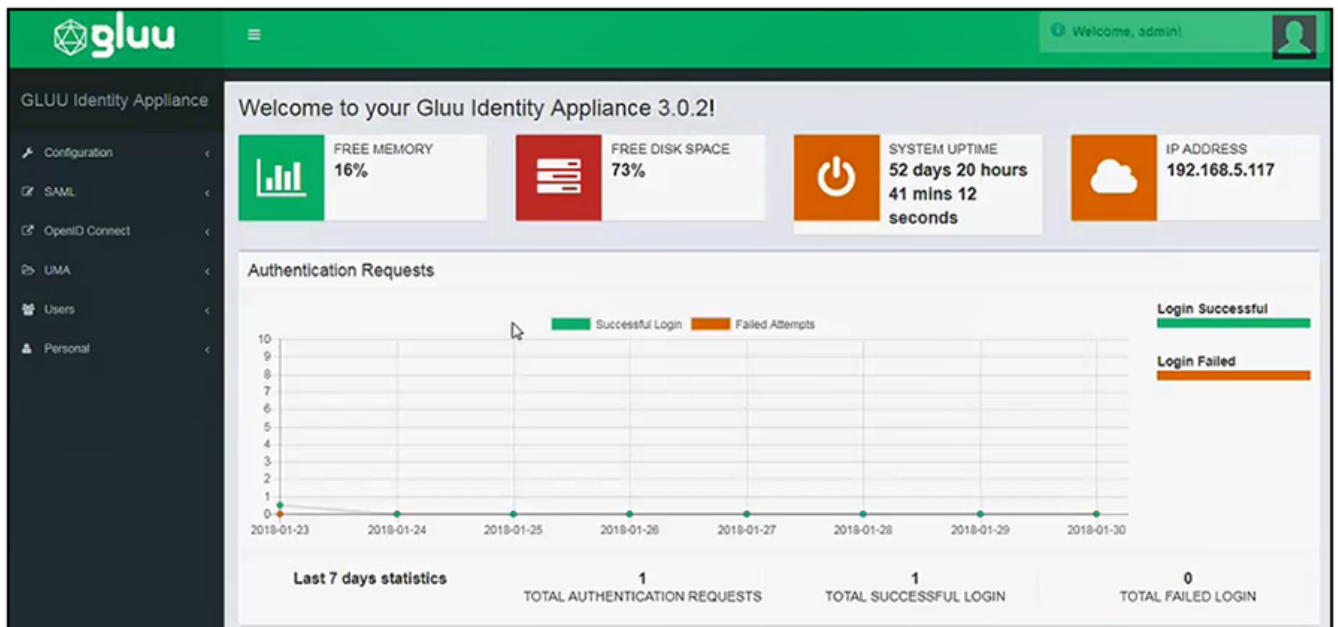
FIGURE 32 Gluu Login Screen



2. Enter your credentials, then click **LOGIN**.

The Gluu Welcome screen appears:

FIGURE 33 Gluu Welcome Screen



3. On the left-side menu, click **SAML > Add Trust Relationships**.

The following screen appears:

FIGURE 34 Add Trust Relationships - Initial Screen

The screenshot displays the 'SAML > Add Trust Relationship' configuration page. On the left, a list of attributes is shown under the heading 'Release additional attributes'. The 'gluuPerson' attribute is selected. The right side of the page features two tabs: 'Trust Agreement' and 'Associated contacts'. The 'Trust Agreement' tab is active, showing the following fields:

- Display Name***: A text input field.
- Description***: A text area input field.
- Entity Type***: A dropdown menu with 'Entity type' selected.
- Metadata Location***: A dropdown menu with 'Metadata type' selected.

At the bottom of the page, there are two buttons: 'Add' and 'Cancel'.

Using Gluu as the SAML Identity Provider

Connecting to the Gluu Identity Service Provider

4. Configure the following fields:
 - Display Name: The hostname of your Cloudpath system.
 - Description: Any description you want to enter. This field is required, however.
 - Entity Type: Select "Single SP" from the drop-down list.
 - Metadata Location: Select "File" from the drop-down list, then click **Choose File**, and upload the metadata file that you downloaded earlier.

The screen has now expanded and will appear like the figure shown below:

FIGURE 35 Add Trust Relationships - Expanded Screen

The screenshot shows the 'SAML Add Trust Relationship' configuration interface. On the left, a 'Release additional attributes' panel lists various attributes, with 'gluuPerson' selected. The main configuration area is divided into two tabs: 'Trust Agreement' and 'Associated contacts'. The 'Trust Agreement' tab contains the following fields:

- Display Name***: Text input field containing 'anna45.cloudpath.net'.
- Description***: Text input field containing 'description here'.
- Entity Type***: Drop-down menu with 'Single SP' selected.
- Metadata Location***: Drop-down menu with 'File' selected.
- Sp Metadata File ***: 'Choose File' button followed by the filename 'samlMetadata (1).xml'.
- SP Logout URL (optional)**: Empty text input field.
- Configure Relying Party**: A checked checkbox with a green link 'Configure RelyingParty' next to it.
- Released**: A blue button labeled 'New Trust Relationship'.

At the bottom of the screen are 'Add' and 'Cancel' buttons. The top right corner shows the breadcrumb 'Trust Relationships > Add Trust Relationships'.

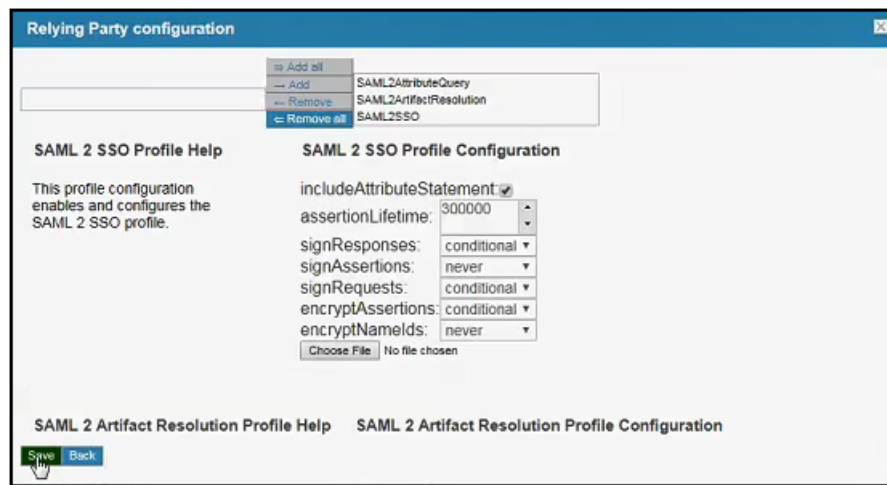
5. Continue by doing the following:
 - a. SP Logout URL (optional): You can leave this blank if you wish.
 - b. Configure Relying Party: Check the box, after which a green link of the same name appears.
 1. Click the green link. The following screen appears:

FIGURE 36 Relying Party Configuration Screen - Selecting Add All



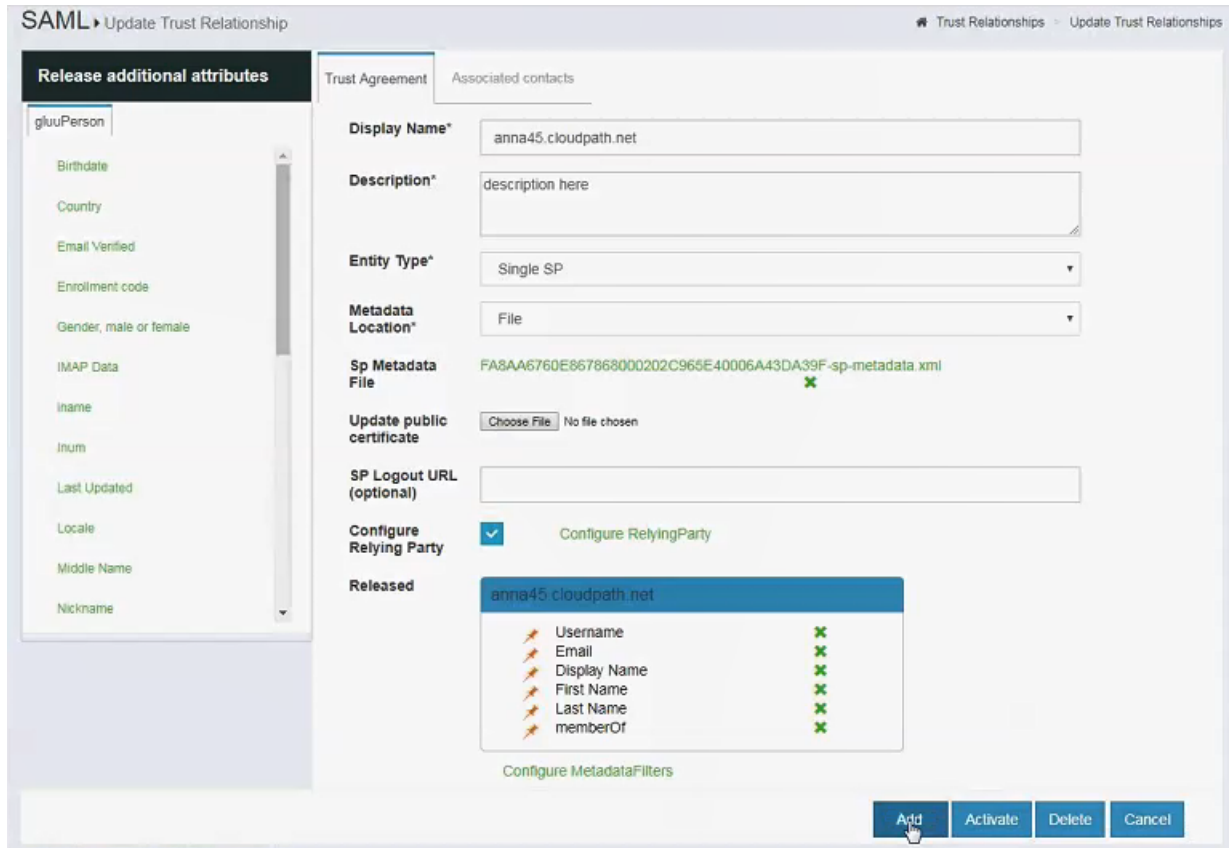
2. Select **Add All**. The following expanded screen appears:

FIGURE 37 Relying Party Configuration Screen - Expanded Screen



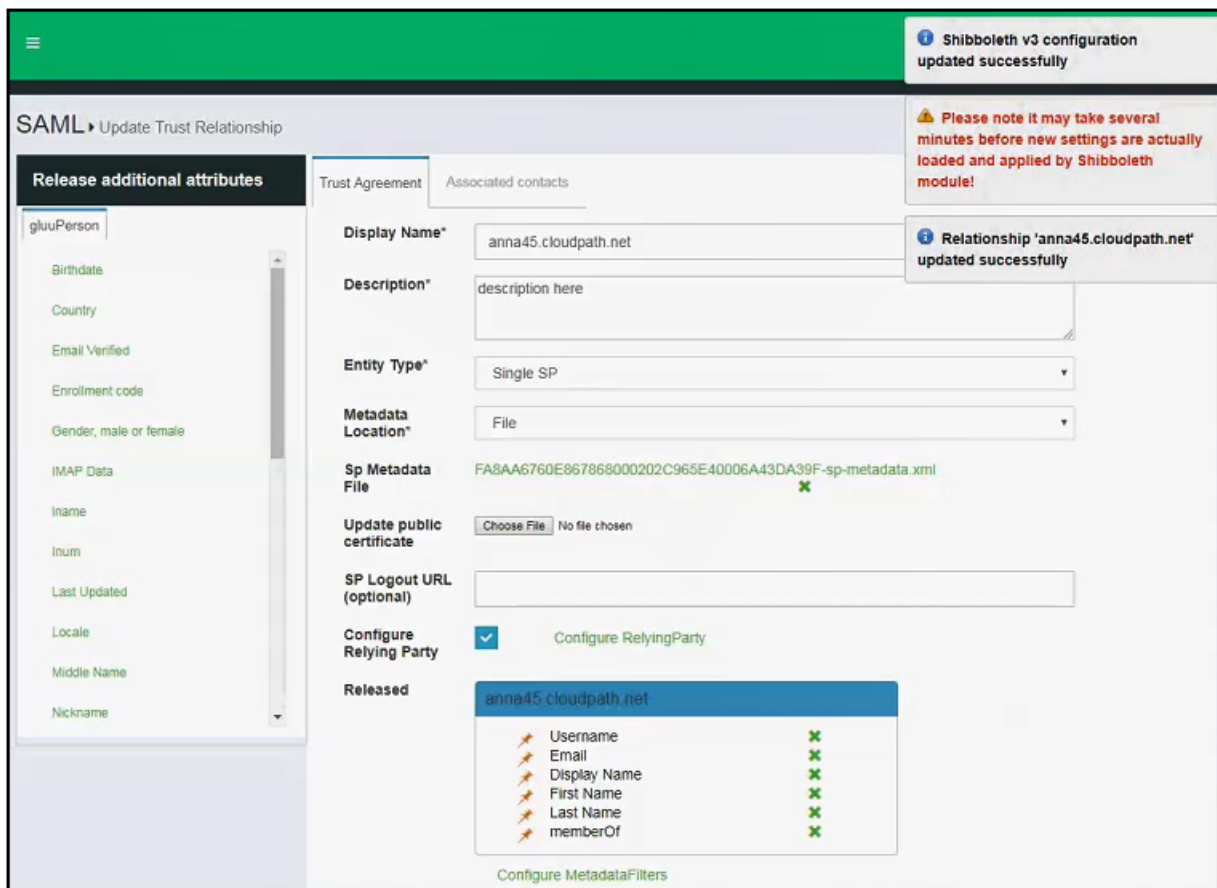
3. Keep all the default selections, and click **Save**.
 - c. Released: Highlight **New Trust Relationships**, then click on any attributes on the left side of the screen that you wish to add for user information. It is recommended to at least add the following: Username, Email, Display Name, First Name, Last Name, and memberOf. After making your selections, click **Add**. The following screen example shows the attributes that have been selected before clicking the **Add** button:

FIGURE 38 Selecting Additional Attributes



- d. Click **Activate**. If successful, you should see a screen such as the following:

FIGURE 39 Addition of Attributes is Successful



- e. Log out of the Gluu interface.

Publishing the Workflow for SAML Gluu

1. Return to the workflow on your Cloudpath system by navigating to the **Configuration > Workflows** screen.
2. Complete the workflow by adding a device configuration. Refer to [Adding a Device Configuration to Your Workflow](#) on page 57.
3. Publish the workflow by clicking the Publish icon to the left of the workflow name.

Testing the User Experience for SAML Gluu

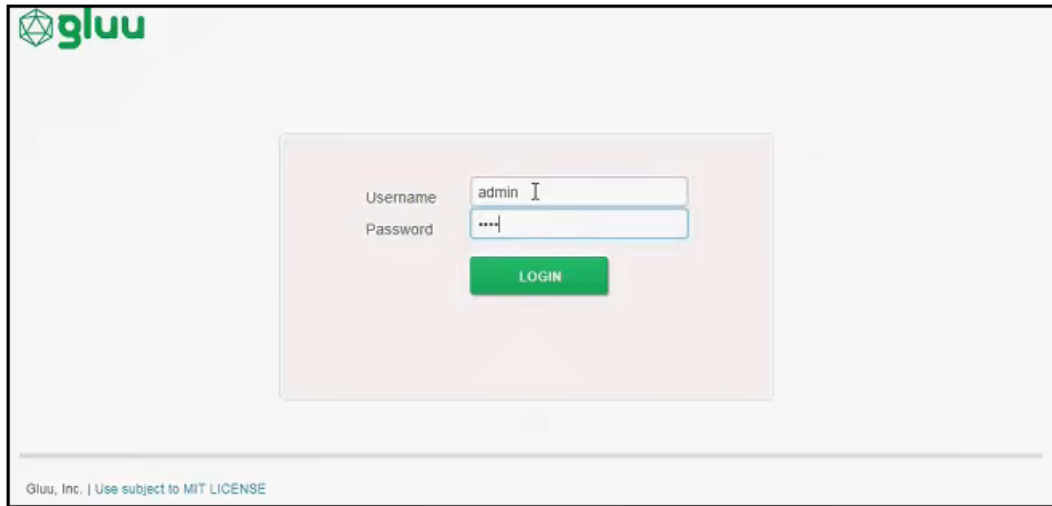
1. Test the enrollment process by clicking on the enrollment portal URL for the workflow at the top of the **Configuration > Workflows** screen.
2. When you are presented with the Welcome screen, click **Start**.

Using Google G Suite as the SAML Identity Provider

3. When you are presented with various branches of your workflow, navigate down a branch that uses the SAML authentication server you just configured.

You are directed to the Gluu login page:

FIGURE 40 Gluu Login Page



4. Log in with your credentials.
5. If the SAML authentication is successful, you are returned to the Cloudpath system, where you can continue with the enrollment.

Using Google G Suite as the SAML Identity Provider

You can use Google G Suite as the public SAML IdP with a tested Cloudpath configuration.

Users can sign in with their managed Google account credentials to enterprise cloud applications via Single Sign-On (SSO).

Basic Tasks for Using Google G Suite

Configure SAML using Google G Suite as the IdP by performing the following tasks sequentially:

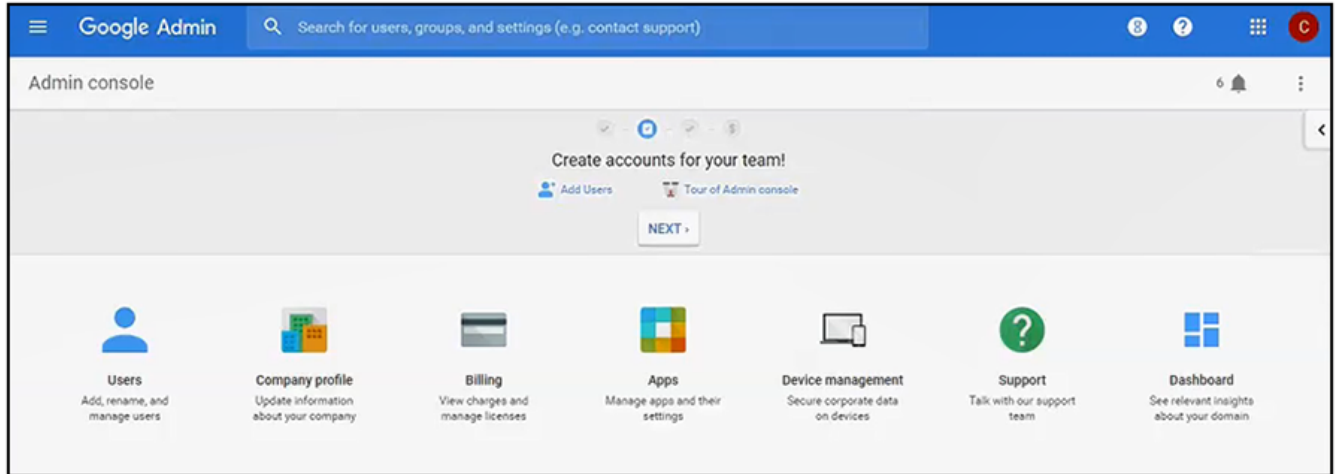
1. [Creating a Google Admin App](#) on page 41
2. [Adding a SAML Step To Your Workflow](#) on page 46
3. [Adding the Google G Suite SAML Authentication Server to the Workflow](#) on page 47
4. [Returning to Google G Suite Configuration](#) on page 51
5. [Publishing the Workflow for SAML Google G Suite](#) on page 56
6. [Testing the User Experience for SAML Google G Suite](#) on page 56

Creating a Google Admin App

1. Log in to (or create) a Google administration account at admin.google.com.

The Google administration console appears:

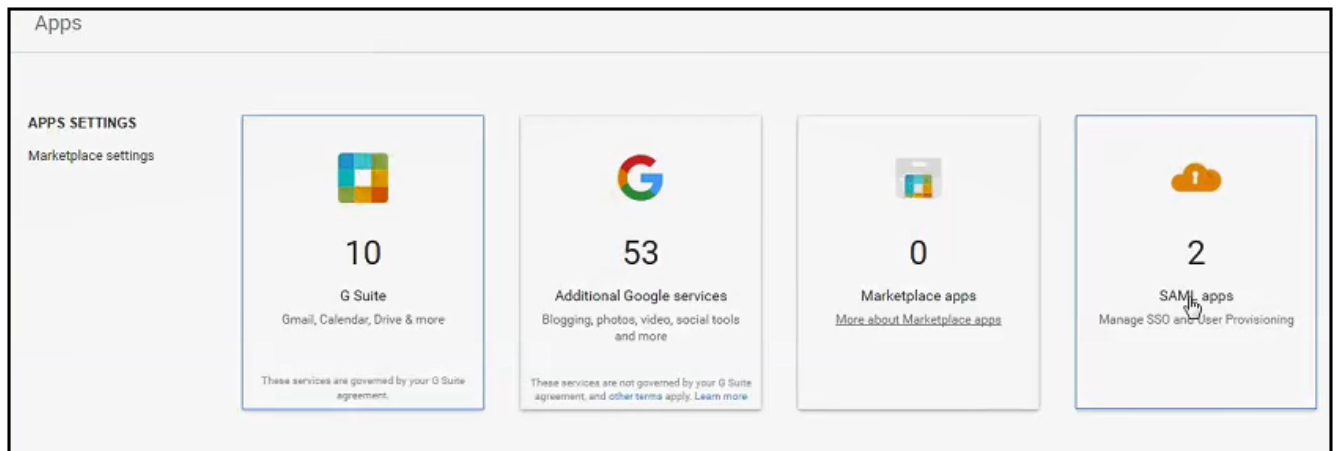
FIGURE 41 Google Admin Console Main Screen



2. Click **Apps**.

The Apps Settings screen appears:

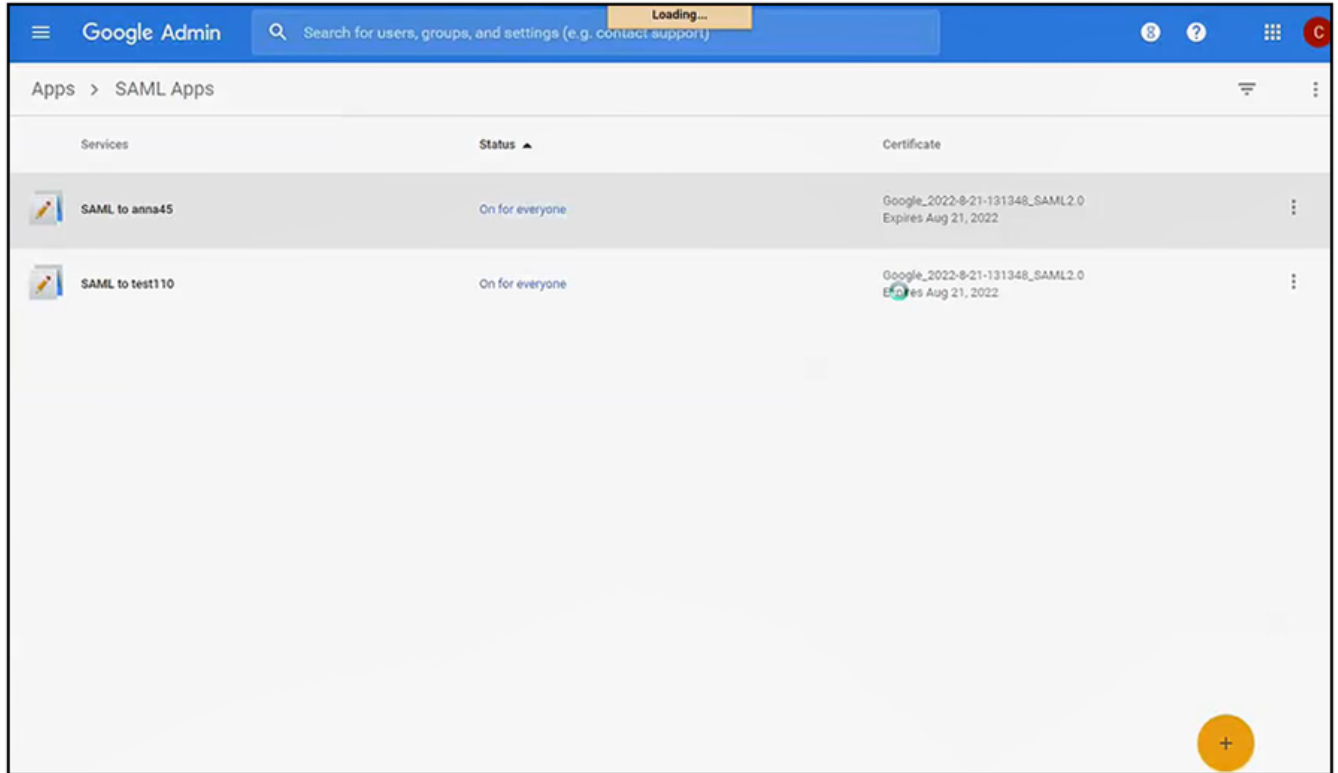
FIGURE 42 Google Apps Settings Screen



Using Google G Suite as the SAML Identity Provider
Creating a Google Admin App

- 3. Click **SAML apps**. The SAML Apps screen appears:

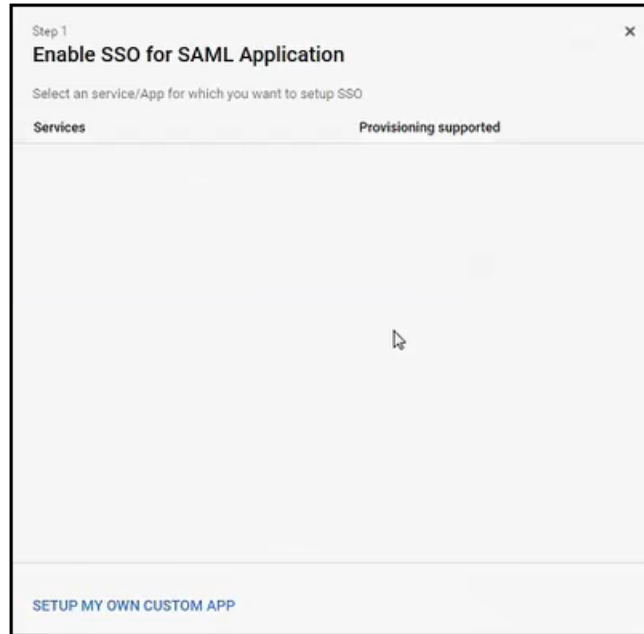
FIGURE 43 SAML Apps Screen



4. Click the + sign at the bottom of the screen to add a new SAML app (or, you can edit an existing one).

The **Enable SSO for SAML Application** screen appears:

FIGURE 44 Enable SSO for SAML Application Screen



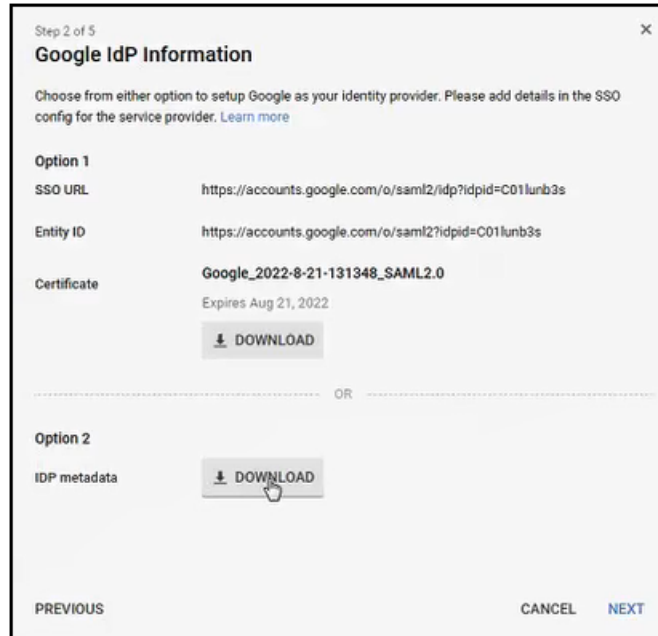
Using Google G Suite as the SAML Identity Provider

Creating a Google Admin App

5. Click **SETUP MY OWN CUSTOM APP**.

The Google IdP Information screen appears:

FIGURE 45 Google IdP Information Screen



- In the Option 2 portion of the screen, click **DOWNLOAD** to download the IdP metadata. Later on, you will need to copy and paste this metadata into a field on a configuration screen in your Cloudpath workflow.

The following figure is an example of what this metadata looks like, after being opened in Notepad:

FIGURE 46 Google Metadata After Being Opened in Notepad

```

1  <?xml version="1.0" encoding="UTF-8" standalone="no" ?>
2  <md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://accounts.google.com/o/saml2?idpid=C01lumb3g" validUntil=
3  <md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
4  <md:KeyDescriptor use="signing">
5  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
6  <ds:X509Data>
7  <ds:X509Certificate>MIIDdCCAlYgAwIBAgIGAV4LYXC7MA0GCSqGSIb3DQEBCwUAMHxwFDASBgNVBAoTC0dvb2dsZSB7
8  bmMhMRwYFAyDVOQHew1nb3VudGpbiBwWV3MQ8wDQYDVQQDEwZhb29nbGUxGDAwBgNVBAUwTD0dv
9  b2dsZSB7b3IgdV9yazEIMakGA1UEBHMCMVVMkEzARBgNVBAgTCk9hbGlnb3JuaWEwHhcNMTcwODIy
10  MTkxMzQ4WhcNMjIwODIyMTkxMzQ4WjB7MRQWEgIDVQKKEwThb29nbGUxGSw5jLjEwMBQGA1UEBGMx
11  TW91bnRhaW4gVmlldzEPMA0GA1UEAxMGR29vZ2x1MRgwFgYDVQQLLEw9b29nbGUxGSw5jLjEwMBQGA1
12  UeBGMQGA1UEBGMxMzQ4WjB7MRQWEgIDVQKKEwThb29nbGUxGSw5jLjEwMBQGA1UEBGMxMzQ4WjB7
13  MIIBCgKCAQEA4wRlH0JacEMDxhuwoqHa8fi62ztKJXOkj5RGI1BhDXgQ419AyxLLWslYy2eEtCQ
14  DoMqVccMYTavd4u0FUD+Ge3BUW4lyBIO+BlknqTnYteyjcRqRHORINqTlG9Ju3F+KQC3Bv/98ve
15  Ndqg/aJ0neGbZjZomEoWUgPp7C+RqOSP/b516jBPs4WkaesAJFizi0ejS4qu1jwsq2q/9CKe6k1q
16  5jtsf7+Rq8IBR7M+C/tEe48gUq6PbV3V1ptuDH4L7wGpPe3qa3Frr0R+UfJR3sVd46c0BnhS18D
17  5SWLPdLk4TzXKOCipt5L9wD8YKfcdN/4nboi9sfw5fva/Z2vCwIDAQAEMA0GCSqGSIb3DQEBCwUA
18  A4IBAQCld96ukfLna3auYlKAt7g2028FazFfz/1YNjNvTAAJ8syUvEv6L9LEdu+h6Q8QmMra4T
19  xh2a0+RH89RG6NSK72213hj07ZTf0hNwenIXnpJ3IFsZ9mct9YGDeySn5OZid2Ptyh0ZKL2y269/
20  VHgY+8qwTrEQTunpCSU8v1Tr9417SqlGqLYovBGeCvNbjWLMpZtHfzP6d5hV7in7xZapJfC7OPJ2
21  QDUEj1R/n5zaq8tRqT4mBCWJRzRVTOlKgAQdFVYQskNzm5eH7RQQ7bbDXiH0JEC7uyk6VdNN1+T9
22  c/j1HD7LhrICgbPk4qs7vUNIeo5ZY5EY3jQQgQTyteyY</ds:X509Certificate>
23  </ds:X509Data>
24  </ds:KeyInfo>
25  </md:KeyDescriptor>
26  <md:NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
27  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://accounts.google.com/o/saml2/idp?idp
28  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://accounts.google.com/o/saml2/idp?idpid=C
29  </md:IDPSSODescriptor>
30 </md:EntityDescriptor>
  
```

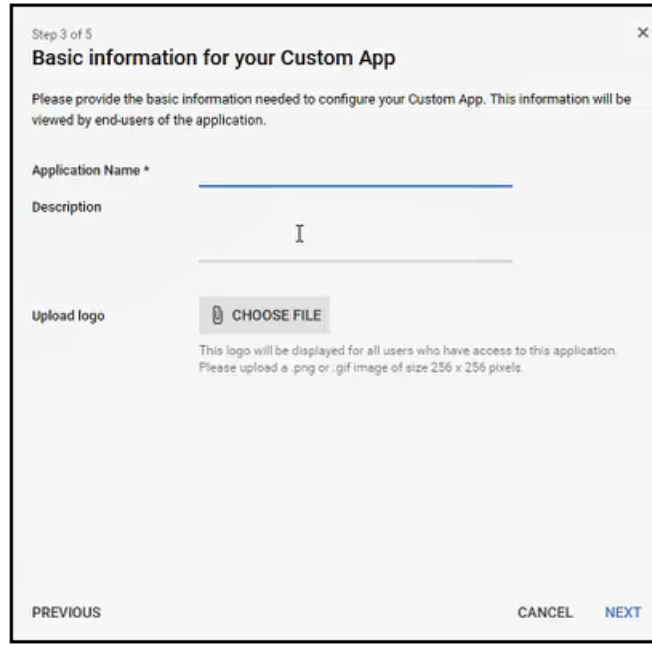
Using Google G Suite as the SAML Identity Provider

Adding a SAML Step To Your Workflow

7. Click **Next**.

The Basic Information for your Custom App screen appears:

FIGURE 47 Basic Information for your Custom App Screen



Step 3 of 5

Basic information for your Custom App

Please provide the basic information needed to configure your Custom App. This information will be viewed by end-users of the application.

Application Name *

Description

Upload logo

CHOOSE FILE

This logo will be displayed for all users who have access to this application. Please upload a .png or .gif image of size 256 x 256 pixels.

PREVIOUS CANCEL NEXT

8. In the Basic Information for your Custom App screen, do the following:

- In the Application Name field, provide a meaningful name.
- Optionally, you can add a Description and/or use the Upload logo function.
- At this point, you need to proceed to the "Adding a SAML Step To Your Workflow" below before you can proceed with the screen above. However, keep the window open that contains the screen above, because you will be directed to return to this screen.

Adding a SAML Step To Your Workflow

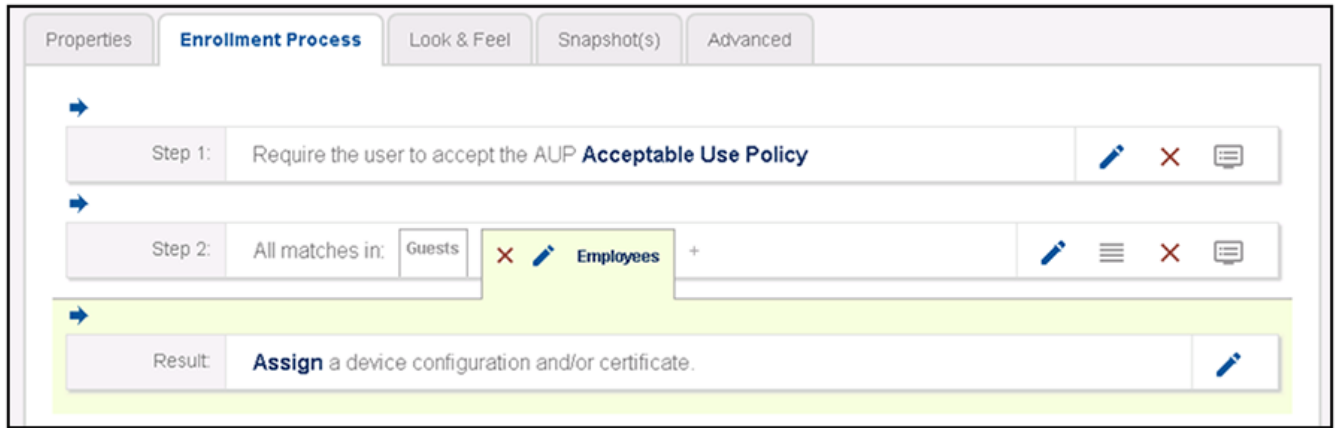
A SAML authentication server may be added to the workflow in place of a traditional Active Directory or LDAP server for authenticating users.

Determine in which branch and in which step to add a SAML authentication server plug-in to the workflow. For example, in the default workflow, you might create a split for Guests and Employees, and you could then use a SAML authentication server instead of the Active Directory authentication server, as shown below.

- Log in to the Cloudpath user interface.
- Go to **Configuration > Workflows**.
- Click on a workflow (or create a new one) for which you want to configure SAML as the authentication server.

4. Highlight the tab in the workflow where you want to add the SAML authentication-server step. In this example below, it is the **Employees** tab.

FIGURE 48 Adding a SAML Step To Your Workflow

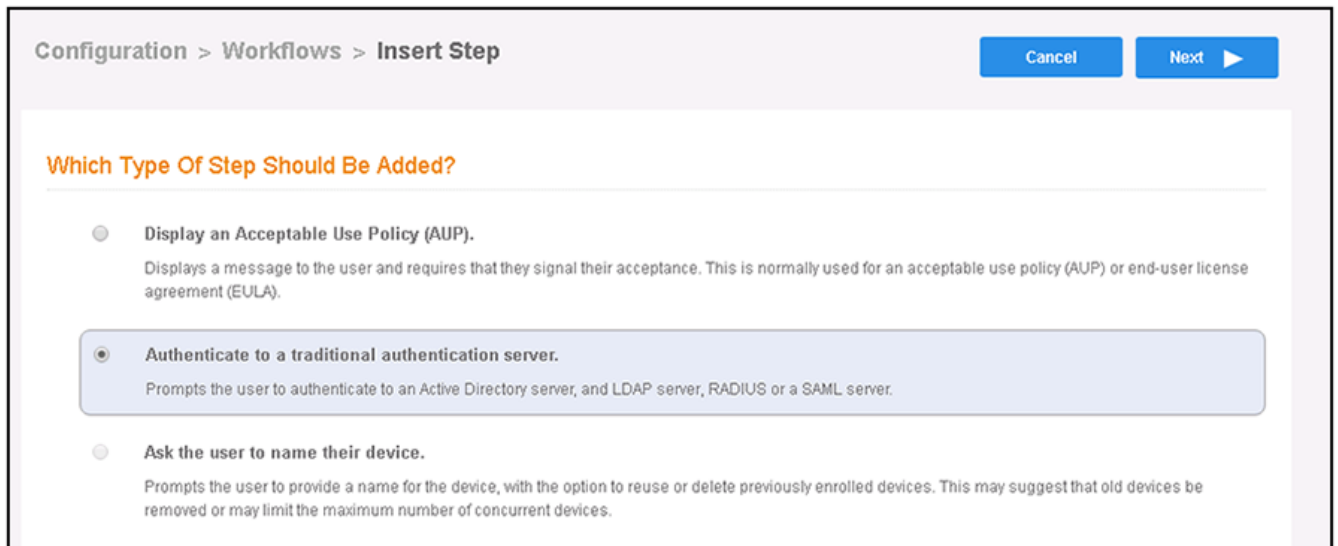


5. With the **Employees** branch of the workflow highlighted, click the blue arrow to insert a step below the Guests/Employees split.

Adding the Google G Suite SAML Authentication Server to the Workflow

1. Once you click the arrow to insert the SAML step, you receive the following prompt:
"Which Type Of Step Should Be Added?"
2. Select the button to authenticate to a traditional authentication server, as shown in the following screen:

FIGURE 49 Authenticate to a Traditional Authentication Server



3. Click **Next**.

Using Google G Suite as the SAML Identity Provider

Adding the Google G Suite SAML Authentication Server to the Workflow

4. If you have already defined an authentication server, you will get a prompt asking whether you want to reuse an existing authentication server or define a new authentication server. Choose the radio button to define a new authentication server, then click **Next**.
5. On the Authentication Server Configuration screen, select the **Connect to SAML** radio button:

FIGURE 50 Authentication Server Configuration Screen

The screenshot displays the 'Authentication Server Configuration' interface. At the top, the title 'Authentication Server Configuration' is shown in orange. Below it, there are five radio button options for selecting an authentication method:

- Connect to Active Directory**: Select this option to enable end-users to authenticate via Active Directory. This option is currently selected. It includes input fields for:
 - Default AD Domain: [ex. test.sample.local]
 - AD Host: [ex. ldaps://192.168.4.2]
 - AD DN: [ex. dc=test,dc=sample,dc=local]
 - AD Username Attribute: SAM Account Name (dropdown menu)
- Connect to LDAP**: Select this option to enable end-users to authenticate via LDAP (or LDAPs).
- Connect to RADIUS**: Select this option to enable end-users to authenticate via RADIUS using PAP.
- Connect to SAML**: Select this option to enable end-users to authenticate via a SAML 2.0 IdP.
- Use Onboard Database**: Select this option to enable end-users to authenticate to accounts defined within this system.

Under the 'Connect to Active Directory' section, there are three sub-sections:

- Verify Account Status On Each Authentication**: Includes a checkbox for 'Perform Status Check' which is currently unchecked.
- Additional Logins**: Includes checkboxes for 'Use For Admin Logins' (unchecked) and 'Use For Sponsor Logins' (checked).
- Test Authentication**: Includes a checkbox for 'Run Authentication Test?' which is currently unchecked.

- Complete the configuration as shown in the example below (refer to the field descriptions after the screen):

NOTE

You can click the "i" icons next to the field names to obtain the information required for each field.

FIGURE 51 SAML Configuration Fields for Google G Suite

The screenshot shows a configuration page for SAML. The 'Required SAML Information' section contains the following fields:

- IdP Metadata Type:** Static XML
- IdP Metadata XML:** <?xml version="1.0" encoding="UTF-8" standalone="no"?><md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
- IdP EntityID:** https://accounts.google.com/o/saml2?idpid=C011unb3s
- SP EntityID:** urn:testsaml:cloudpath:jeff

The 'SAML Attribute to Enrollment Mappings' section shows a list of attribute mapping templates (eduPerson, InCommon, inetOrgPerson/X.500, Generic, Blank) and a list of attributes with their corresponding values:

Attribute	Value
Username Attribute	username
Common Name Attribute	cn
Affiliation/Group Attribute	group
Email Attribute	email
First Name Attribute	first_name
Last Name Attribute	last_name
City Attribute	city
State Attribute	state
Country Attribute	country
OU Attribute	ou
Distinguished Name Attribute	dn
Company Attribute	company
Department Attribute	department

- Required SAML Configuration section:
 - IdP Metadata Type: Use the **Static XML** option.
 - IdP Metadata XML: Copy and paste the google metadata that you downloaded in [Figure 46](#) on page 45 into this field. Be sure you copy the entire contents of the metadata file, but do not have any extra spaces.
 - IdP EntityID: Obtain this value from your downloaded metadata file. Look for the string "entityID" near the top of the file. That string is followed by an = sign and a URL in quotation marks. It is the value within these quotation marks that you need to paste into this field. For example, in [Figure 46](#) on page 45, the Entity ID = https://accounts.google.com/o/saml2?idpid=c011unb3s
 - SP EntityID: Enter the string **urn:testsaml:cloudpath:** followed by your first name. For example: **urn:testsaml:cloudpath:jeff**
- SAML Attribute to Enrollment Mappings: Click the **Generic** tab to automatically have the fields filled in.
- SAML Options (not shown in the screen shot above): Use all default settings.

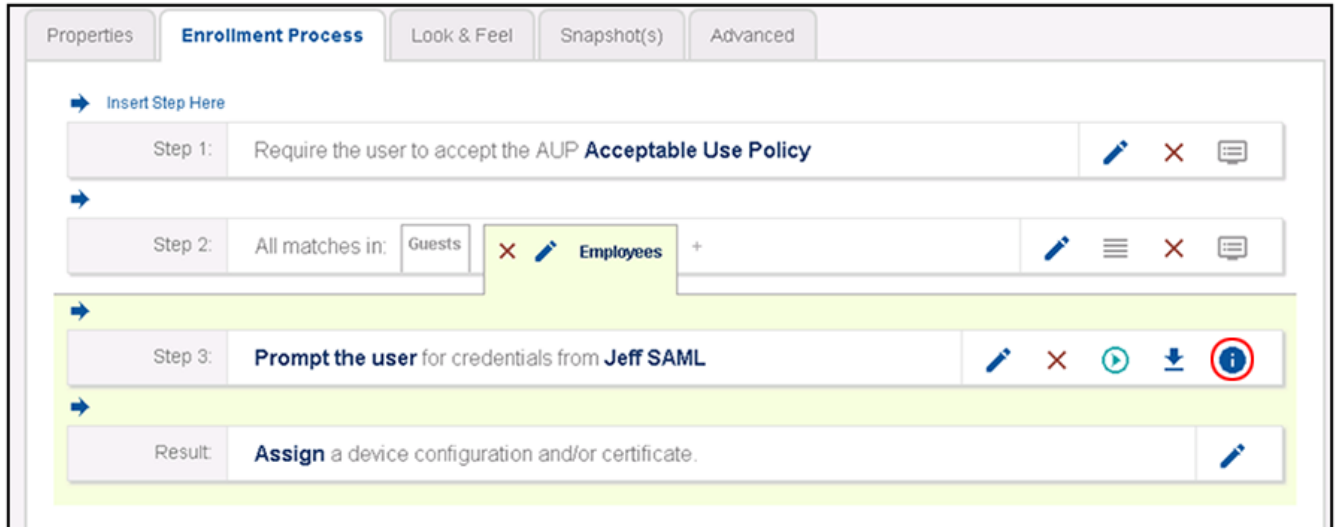
Using Google G Suite as the SAML Identity Provider

Adding the Google G Suite SAML Authentication Server to the Workflow

7. Click **Next**.

You are returned to the workflow screen, as shown in the example below:

FIGURE 52 Workflow After SAML Has Been Configured as Authentication Server



8. In the SAML authentication server step (Step 3), click the "i" icon on the far right (shown in the previous screen, with red circle around the "i").

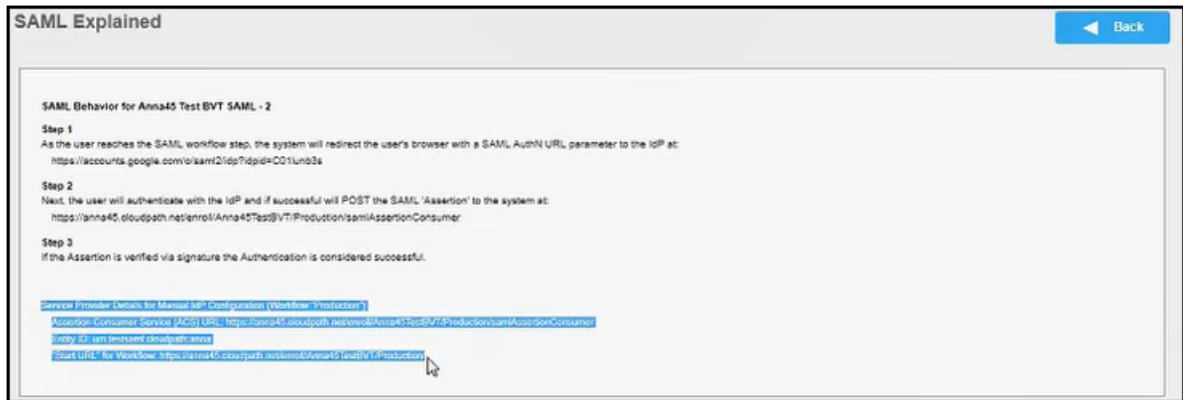
The SAML Explained screen appears:

FIGURE 53 SAML Explained



- Copy the bottom portion of this screen (highlighted below) and, optionally, paste it into a text file. You will need this information later in the configuration process:

FIGURE 54 SAML Explained - Text You Will Need to Copy



- Proceed to the "Returning to Google G Suite Configuration" section.

Returning to Google G Suite Configuration

- Back on your Google configuration, you left off at Figure 47 on page 46. Once you have entered an Application Name, click **Next**. The Service Provider Details screen appears:

FIGURE 55 Service Provider Details

A screenshot of a "Service Provider Details" configuration screen, labeled "Step 4 of 5". The screen contains the following fields and options: "ACS URL *" (text input), "Entity ID *" (text input), "Start URL" (text input), "Signed Response" (checkbox), "Name ID" (dropdown menu with "Basic Information" selected), "Primary Email" (dropdown menu), and "Name ID Format" (dropdown menu with "UNSPECIFIED" selected). At the bottom, there are three buttons: "PREVIOUS", "CANCEL", and "NEXT".

Using Google G Suite as the SAML Identity Provider

Returning to Google G Suite Configuration

2. Use the information from the SAML Explained screen to complete the Service Provider Details configuration, as shown and described below:

FIGURE 56 Service Provider Details - Example Configuration

Step 4 of 5 X

Service Provider Details

Please provide service provider details to configure SSO for your Custom App. The ACS url and Entity ID are mandatory.

ACS URL *	https://anna45.cloudpath.net/enroll/Anna45TestBV*	
Entity ID *	urn:testsaml:cloudpath:anna	
Start URL	https://anna45.cloudpath.net/enroll/Anna45TestBV*	
Signed Response	<input type="checkbox"/>	
Name ID	Basic Information	Primary Email
Name ID Format	EMAIL	

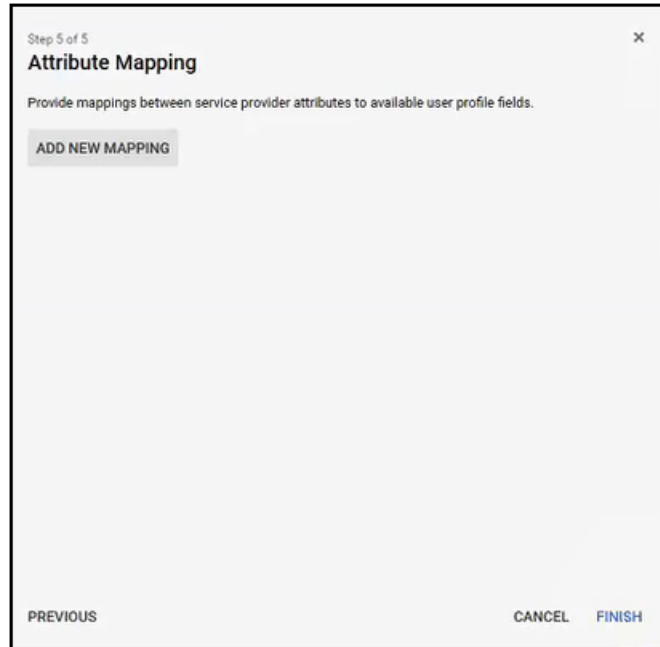
PREVIOUS CANCEL **NEXT**

- ACS URL, Entity ID, and Start URL: You obtain all three of these values from [Figure 54](#) on page 51. Copy and paste each value into the screen.
- Signed Response: Leave this box unchecked.
- Name ID: Be sure to use the "Basic Information" and "Primary Email" settings from the drop-down lists.
- Name ID Format: From the drop-down list, select EMAIL.

Click **Next**.

The Attribute Mapping screen appears:

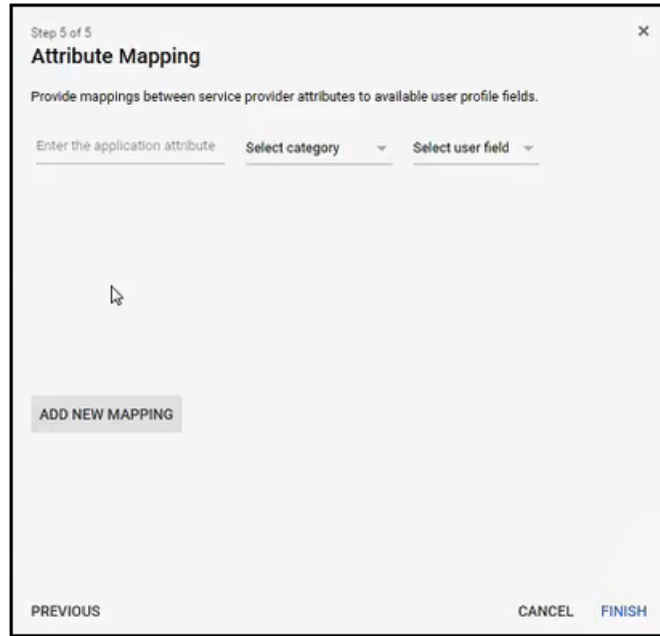
FIGURE 57 Attribute Mapping Screen



3. Click **ADD NEW MAPPING**

- The Attribute Mapping screen gets modified to allow you to enter information:

FIGURE 58 Adding Attributes in the Attribute Mapping Screen



The following table lists the attributes and their corresponding settings that you need to add.

TABLE 2 Required Attributes

Name of Application Attribute	Select Category drop-down list	Select User Field drop-down list
username	Basic information	Primary Email
first_name	Basic information	First Name
last_name	Basic information	Last Name
dn	Basic information	Primary Email
department	Employee Details	Department

- In the left-most column of the Attribute Mapping screen, enter the name of the first attribute, which is **username**, then select the following from the two drop-down lists:
 - From the Select category drop-down, select **Basic Information**.
 - From the Select user field drop-down, select **Primary Email**.

- Once you have completed your first entry, click **ADD NEW MAPPING** again, and repeat the process until you have added all the mappings that are shown in the previous table as well as in the following screen:

FIGURE 59 Attribute Mapping Screen Completed

The screenshot shows a window titled "Attribute Mapping" with a close button (X) in the top right corner. Below the title, it says "Step 5 of 5" and "Provide mappings between service provider attributes to available user profile fields." The screen displays five rows of mappings, each with a text input field for the service provider attribute, a dropdown menu for the category, and another dropdown menu for the user profile field. The mappings are:

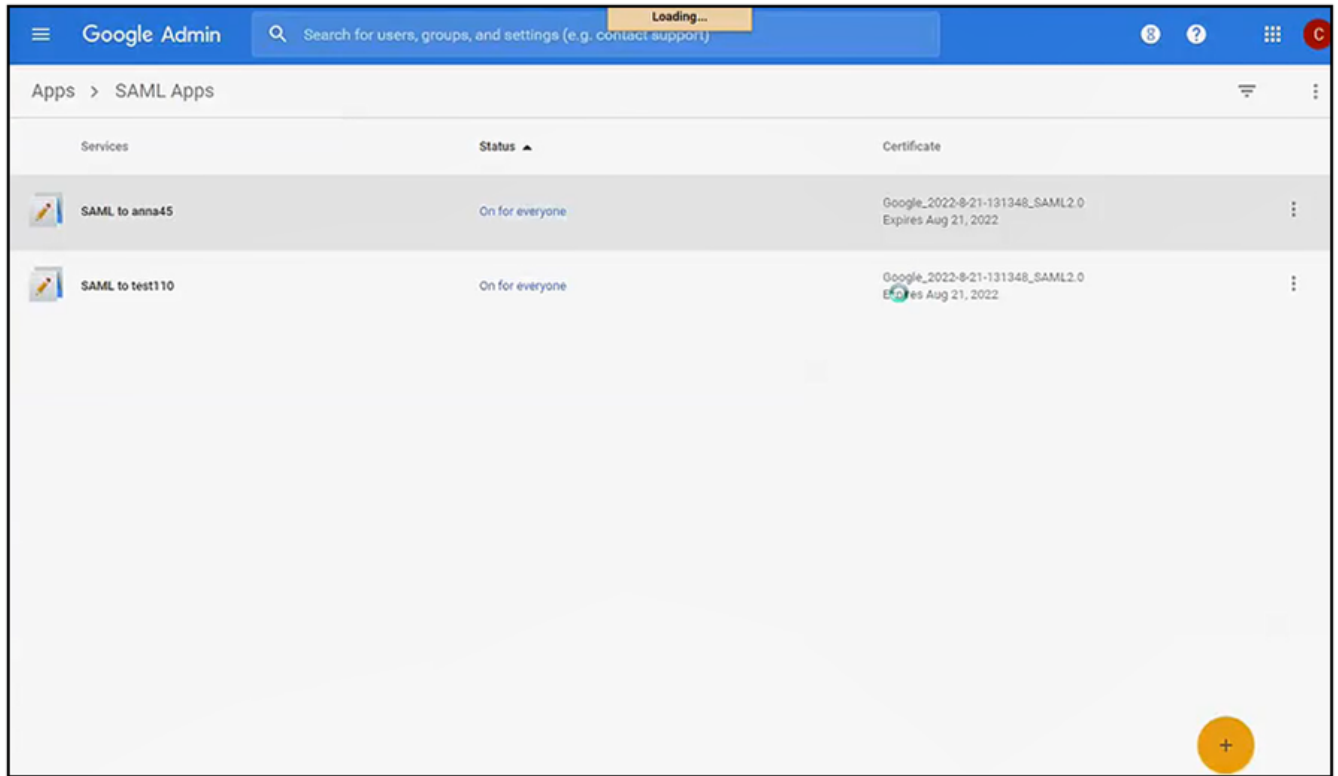
Service Provider Attribute	Category	User Profile Field
username	Basic Information	Primary Email
first_name	Basic Information	First Name
last_name	Basic Information	Last Name
dn	Basic Information	Primary Email
department	Employee Details	Department

Below the mappings is a button labeled "ADD NEW MAPPING". At the bottom of the window, there are three buttons: "PREVIOUS", "CANCEL", and "FINISH". A mouse cursor is pointing at the "FINISH" button.

- When you have added these attributes as shown above, click **FINISH**.

8. Make sure that the SAML App you have created is "On for everyone," as shown in the Status column on the following example screen. You can use the three vertical buttons on the right side of the screen to toggle this setting.

FIGURE 60 SAML App On for Everyone



9. Log out of the Google interface.

Publishing the Workflow for SAML Google G Suite

1. Return to the workflow on your Cloudpath system by navigating to the **Configuration > Workflows** screen.
2. Complete the workflow by adding a device configuration. Refer to [Adding a Device Configuration to Your Workflow](#) on page 57.
3. Publish the workflow by clicking the Publish icon to the left of the workflow name.

Testing the User Experience for SAML Google G Suite

1. Test the enrollment process by clicking on the enrollment portal URL for the workflow at the top of the **Configuration > Workflows** screen.
2. When you are presented with the Welcome screen, click **Start**.
3. When you are presented with various branches of your workflow, navigate down a branch that uses the SAML authentication server you just configured.

You are directed to the Google login page.

4. Log in with your Google administrative credentials.
5. If the SAML authentication is successful, you are returned to the Cloudpath system, where you can continue with the enrollment.

Using Google Groups in the Workflow

You can create Google groups to synchronize with your SAML workflow.

If you wish to use Google groups as part of the SAML workflow, one fairly quick method of setting up groups and adding users is by using the Google Configuration Manager. Refer to Google administration documentation for details.

Once you have a Google group configured, and you want it to be part of your SAML workflow in Cloudpath, be sure that the Google group name you configured is the same name that you enter in the Affiliation/Group Attribute field of [Figure 51](#) on page 49.

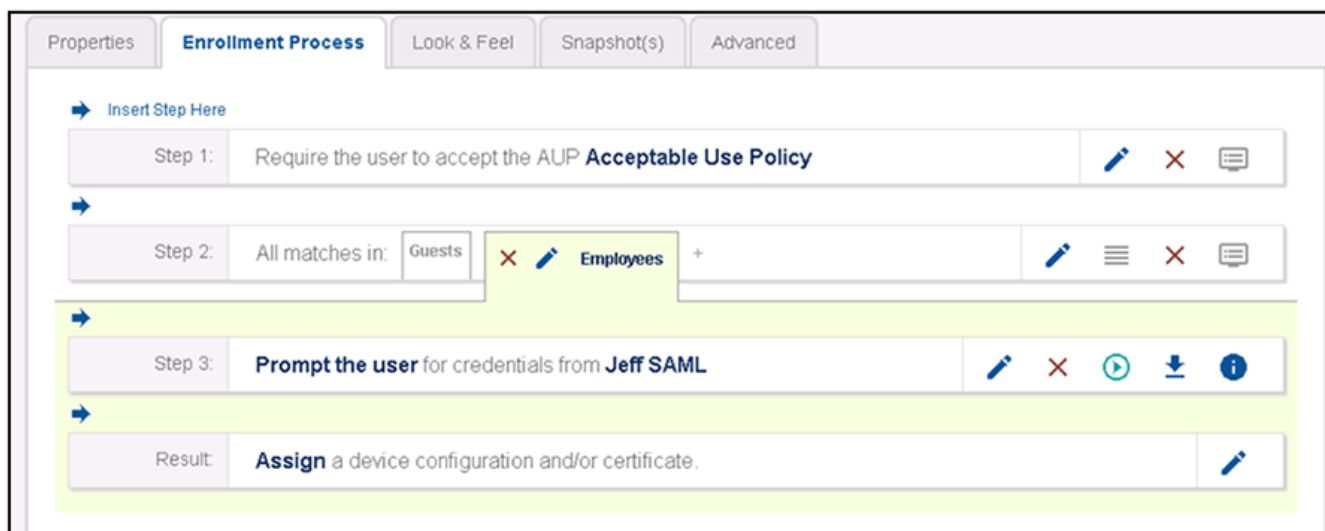
For details of the entire process, you can still follow the procedures described in the [Using Google G Suite as the SAML Identity Provider](#) on page 40 section. Also, if you want to filter on various attributes within the Google group you have created, you can refer to the "Create a Filter in the Device Type Split" section of the *Cloudpath Enrollment System Administration Guide*.

Adding a Device Configuration to Your Workflow

Be sure you have added a device configuration step before publishing the workflow.

1. In the workflow, click **Assign** in the **Result** step:

FIGURE 61 Assigning a Device Configuration to Your Workflow



Adding a Device Configuration to Your Workflow

- Next, you can either select an existing device configuration from the drop-down or you can add a new device configuration. In the example below, an existing device configuration is selected to move the user to an already configured secure network during the enrollment process.

FIGURE 62 Using an Existing Device Configuration for Your SAML Workflow

The screenshot shows a configuration screen titled "Configuration > Workflows > Result". At the top right, there are "Cancel" and "Next" buttons. The main heading is "Which device configuration should be used?". There are three radio button options:

- An existing device configuration.**
Configure the user using an existing configuration.
Device Configuration:
- A new device configuration.**
Configure the user using a new configuration.
- None.**
Do not configure the user.

Click **Next**.

- Select the radio button to create a new certificate template, as shown below, then click **Next**.

FIGURE 63 Creating a New Certificate Template for Your Workflow

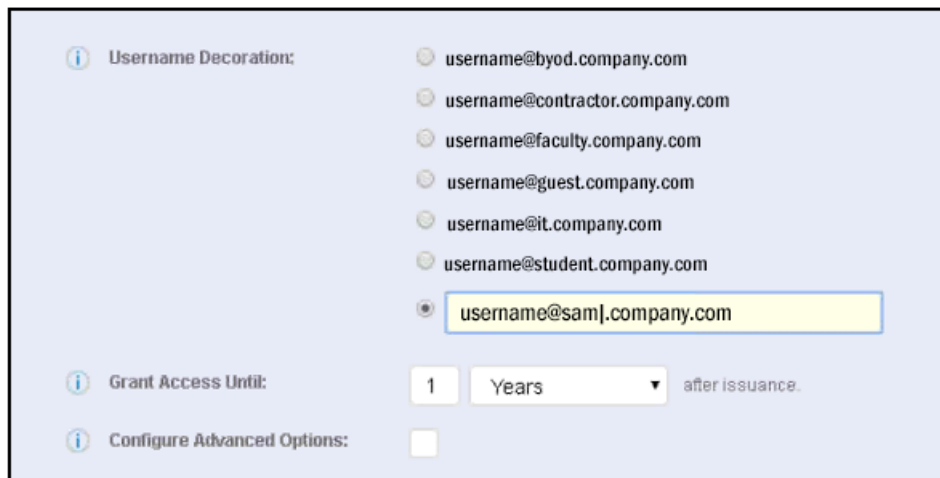
The screenshot shows a configuration screen titled "Configuration > Workflows > Result". At the top right, there are "Cancel", "Back", and "Next" buttons. The main heading is "What certificate template should issue the certificate?". There are three radio button options:

- An existing certificate template.**
Issue the certificate using an existing certificate template.
- A new certificate template.**
Create a new certificate template, which specifies the attributes of the certificate issued to the user.
- Do not issue a certificate to the user.**

- On the next screen, called "Which CA should sign the certificates?", click **Next**.

- In the **Manage Templates > Create** screen, in the "Username Decoration" section, select the bottom radio button, then edit it accordingly to denote that it will be used for your SAML authentication. See the figure below for an example:

FIGURE 64 Editing Username for a SAML Certificate Template

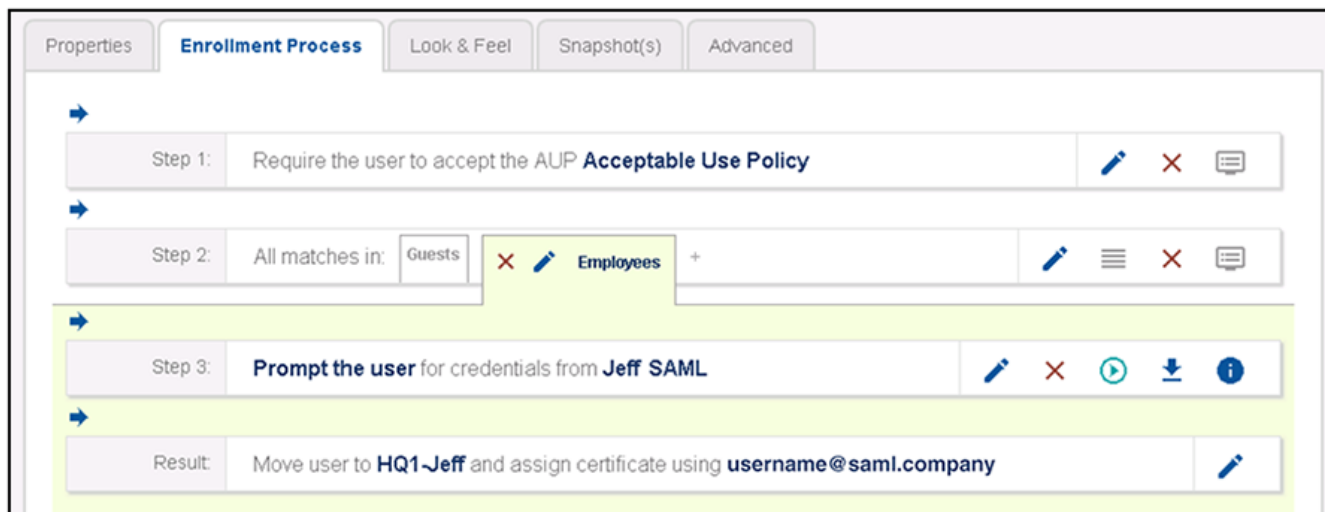


Click **Next**.

- When you are returned to your workflow, make sure that your device and certificate template configurations appear as part of the result step.

The screen below shows an example, based on the selections shown in the previous steps:

FIGURE 65 Workflow Example After Completing Device Configuration



Return to the SAML section that referred you to this device configuration section. You will be instructed to publish your workflow.

