

Costpoint Cloud Configuring Okta

Costpoint Cloud Configuring Okta

26 March 2026



While Deltek has attempted to verify that the information in this document is accurate and complete, some typographical or technical errors may exist. The recipient of this document is solely responsible for all decisions relating to or use of the information provided herein.

This publication contains proprietary information that is protected by copyright. All rights are reserved. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, or translated into another language, without the prior written consent of Deltek, Inc.

© Deltek, Inc.

Deltek's software is also protected by copyright law and constitutes valuable confidential and proprietary information of Deltek, Inc. and its licensors. The Deltek software, and all related documentation, is provided for use only in accordance with the terms of the license agreement. Unauthorized reproduction or distribution of the program or any portion thereof could result in severe civil or criminal penalties

All trademarks are the property of their respective owners.

Contents

Costpoint Cloud Configuring Okta 1

Costpoint Cloud Configuring Okta

Overview

There are four steps to setting up Okta for Deltek Costpoint Cloud.

Step	Procedure
1	Submit the SSO Setup Service Request
2	Configure Okta
3	Attach your Okta XML certificate to your SSO Setup Service Request ticket
4	Configure Costpoint user accounts to use Okta for authentication

Note: If you are already set up for SAML SSO authentication in Costpoint Cloud, you will need to set up a second configuration for the Costpoint Mobile T&E in the Cloud. Follow the instructions in this guide to set up your configuration. See the *Deltek Costpoint Mobile Time and Expense in the Cloud Administrator Guide* for more information on Costpoint Mobile T&E in the Cloud.

Submit the SSO Setup Service Request

1. When you submit the SSO Setup Service Request (for details, click [here](#)), Deltek will attach the following information to the service request ticket.
 - **Single sign on URL:** For example,
 - GCC <https://acme-cp.deltekenterprise/cpweb/LoginServlet.cps>
 - GCCM <https://cp-acme-prd.mydeltekgcc.com/cpweb/LoginServlet.cps>
 - **Recipient URL:** For example,
 - GCC <https://acme-cp.deltekenterprise/cpweb/LoginServlet.cps>
 - GCCM <https://cp-acme-prd.mydeltekgcc.com/cpweb/LoginServlet.cps>
 - **Destination URL:** For example,
 - GCC <https://acme-cp.deltekenterprise/cpweb/LoginServlet.cps>
 - GCCM <https://cp-acme-prd.mydeltekgcc.com/cpweb/LoginServlet.cps>
 - **Audience URI (SP Entity ID):** For example,
 - GCC <https://acme-cp.deltekenterprise/cpweb>
 - GCCM <https://cp-acme-prd.mydeltekgcc.com/cpweb>
 - **Default RelayState:** For example, system=ACME

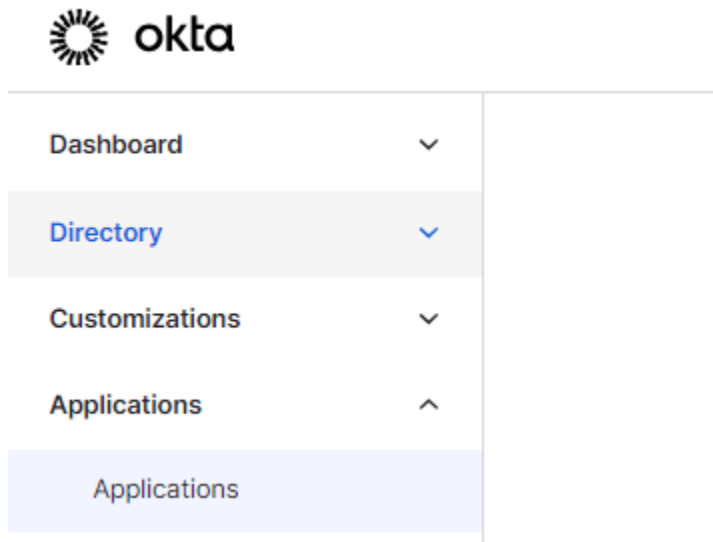
Note: If you are a Costpoint Essentials customer, Deltek will provide you with one set of URLs. If you are a Costpoint Enterprise customer, Deltek will provide you with three sets of URLs. The URLs for Costpoint GovCon Moderate Enterprise and Essentials will look different than this example, use the URLs that you are provided in the ticket.

Note: If you are a Costpoint Mobile T&E customer, Deltek will provide you with two sets of URLs (one for Costpoint and one for Costpoint Mobile T&E).

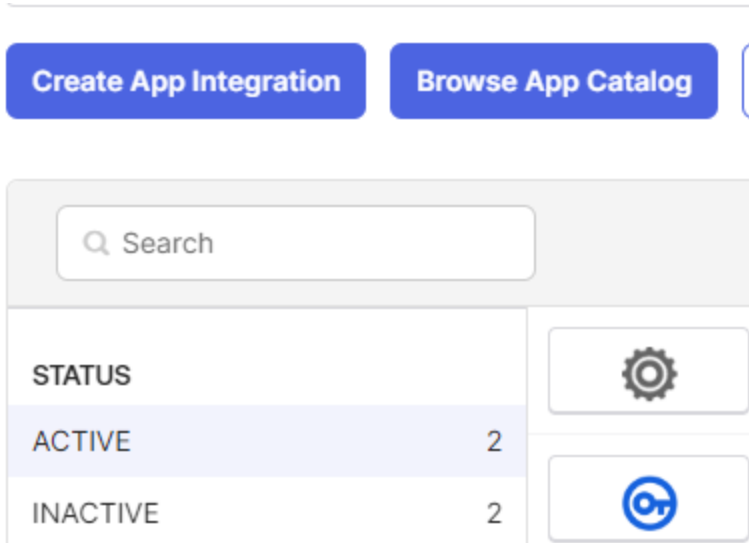
Configure Okta

To configure Okta:

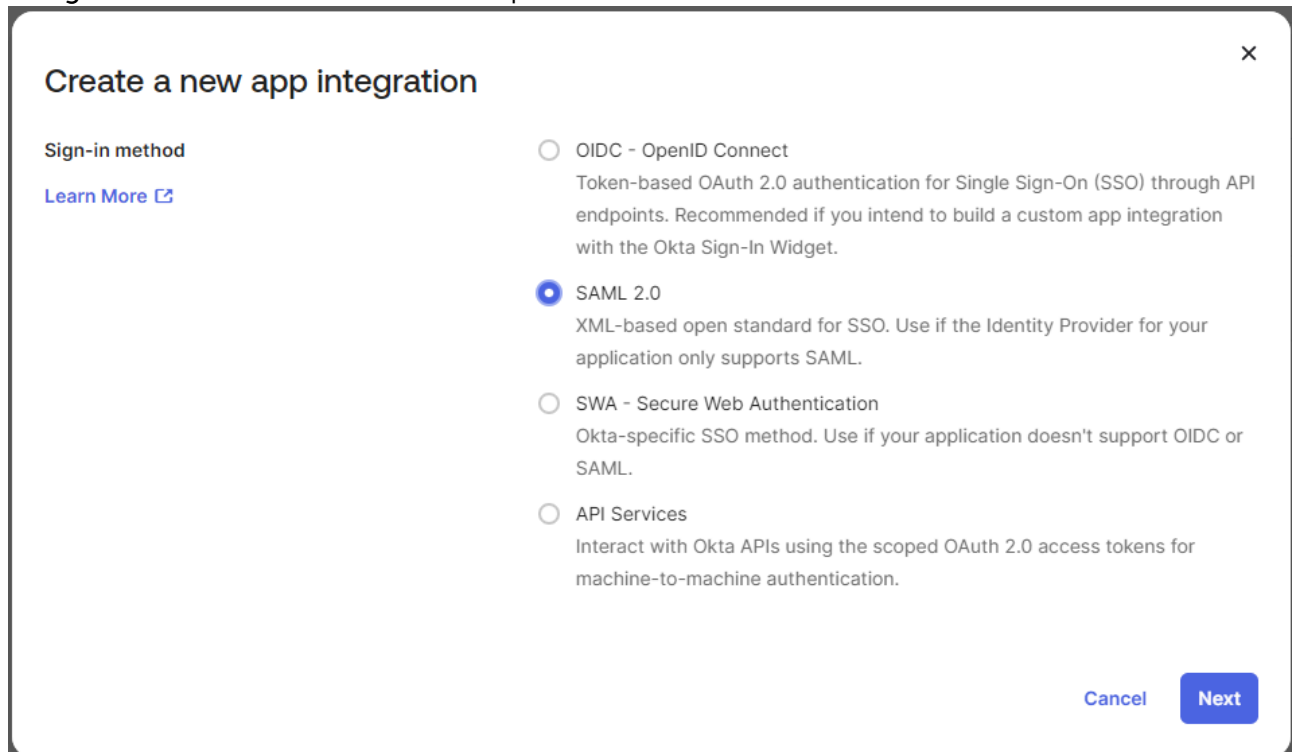
1. Log into the Okta portal and click **Applications**.



2. Click **Create App Integration**.



3. On the Create a New Application Integration screen, select or specify the following details and click **Create**:
 - **Sign on method**: Select the **SAML 2.0** option.



4. On the General Settings screen, select or specify the following details and click **Next**:
 - **App name**: Enter any name.
 - **App logo (optional)**: If so desired, upload a logo for the application
 - **App visibility**: Select either check box. You can choose not to display the application icon to users or not



to display the application icon in the Okta Mobile application.

Create SAML Integration

1 General Settings	2 Configure SAML	3 Feedback
--------------------	------------------	------------

1 General Settings

App name

App logo (optional)  

App visibility Do not display application icon to users
 Do not display application icon in the Okta Mobile app

[Cancel](#) [Next](#)

5. On the SAML Settings A screen, complete the following:

Note: `/LoginServlet.cps` is required where specified below.

- **Single sign on URL:** This URL is provided by Deltek in the service request.
 - GCC <https://acme-cp.deltekenterprise/cpweb/LoginServlet.cps>
 - GCCM <https://cp-acme-prd.mydeltekgcc.com/cpweb/LoginServlet.cps>
- **Audience URI (SP Entity ID):** This URL is provided by Deltek in the service request.
 - GCC <https://acme-cp.deltekenterprise/cpweb>
 - GCCM <https://cp-acme-prd.mydeltekgcc.com/cpweb>
- **Default RelayState:** This setting is provided by Deltek in the service request.
For example: `system=ACME`
- **Response:** Unsigned

A SAML Settings

General

Single sign-on URL ?
 Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID) ?

Default RelayState ?
If no value is set, a blank RelayState is sent

Name ID format ?

Application username ?

Update application username on

[Show Advanced Settings](#)

6. Click Next.

☰ Edit SAML Integration

1 General Settings	2 Configure SAML	3 Feedback
--------------------	------------------	------------

3 Help Okta Support understand how you configured this application

Are you a customer or partner?

I'm an Okta customer adding an internal app

I'm a software vendor. I'd like to integrate my app with Okta

1 The optional questions below assist Okta Support in understanding your app integration.

App type **1**

This is an internal app that we have created

[Previous](#) [Finish](#)

Why are you asking me this?

This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.

7. Click Finish.

8. Sample Settings

● SAML 2.0

Default Relay State	system=ACME
---------------------	-------------

Metadata details

Metadata URL	https://dev-153391.oktapreview.com/app/exk1w8mtf7kyJCT2m0h8/sso/saml/metadata Copy
--------------	---

▼ Hide details

Sign on URL	https://dev-153391.oktapreview.com/app/dev-153391_deltekcostpoint_3/exk1w8mtf7kyJCT2m0h8/sso/saml Copy
Sign out URL	https://dev-153391.oktapreview.com Copy
Issuer	http://www.okta.com/exk1w8mtf7kyJCT2m0h8 Copy
Signing Certificate	Download Copy

➤ Certificate fingerprint

9. After the application is created, export the IDP metadata as an .XML file or Copy the metadata URL.
Costpoint does not support file with .cert extension.

Note: For Costpoint Enterprise users, you must repeat step 3 for each Cloud Environment (Production, Implementation/Test/Preview, Dev) that you would like to set up the Okta for.

Note: For Costpoint Mobile T&E users, you must repeat step 3 for each Costpoint Mobile T&E environment that you would like to set up Okta for.

Attach Your Okta XML Certificate to Your SSO Setup Service Request Ticket

Attach the Okta XML certificate you created in Step 3 (Configure Okta) to the SSO Setup Service Request ticket you created in Step 2 (Submit the SSO Setup Service Request).

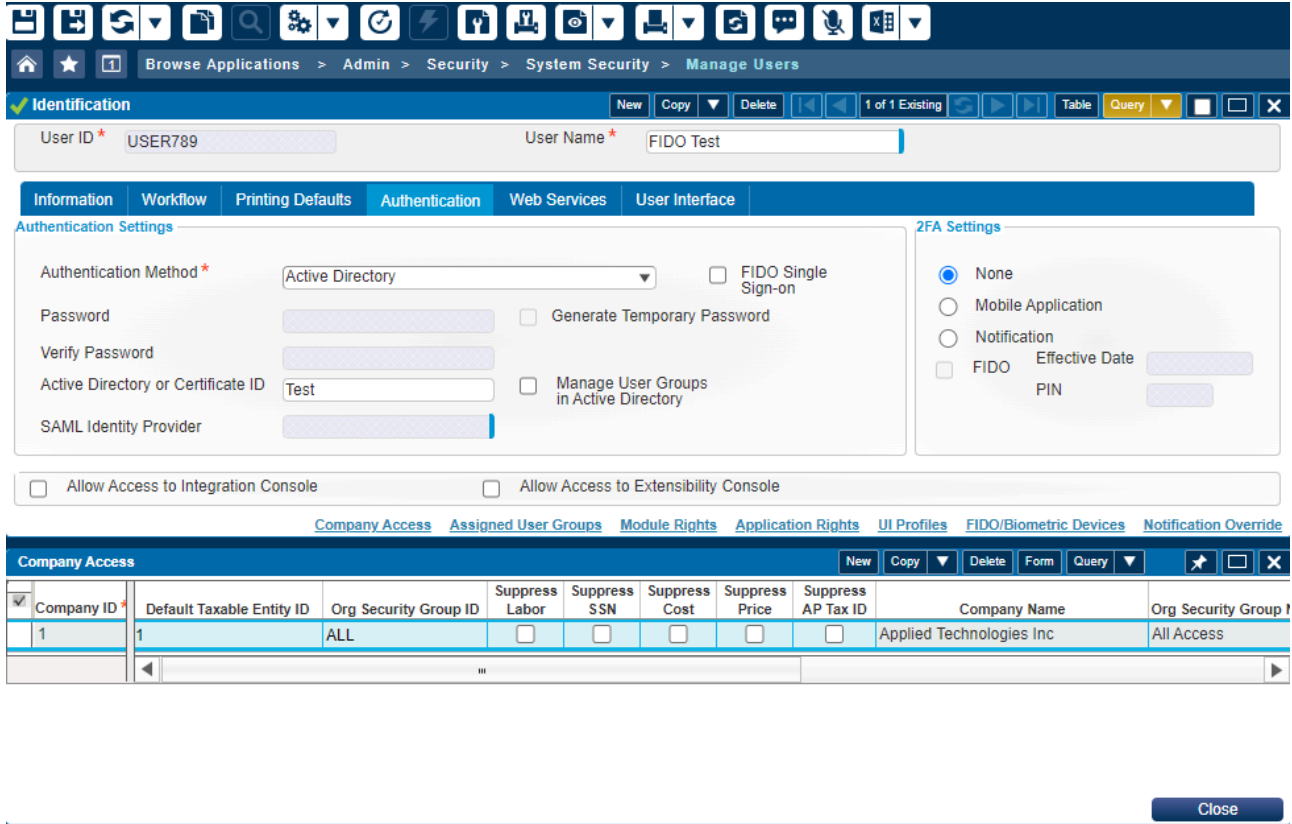
You also need to let the cloud team if your SAML ID Attribute is an email account or a unique identifier like an employee number. Your users will all need to use the same type of attribute.

Configure Costpoint User Accounts to Use Okta for Authentication

In order to log into Costpoint with your Okta credentials, you must first modify the authentication properties of your Costpoint user account.

To modify the authentication properties:

1. Primary SaaS Admin will need to login and adjust the authentication properties of your users.
 - **GCCM Customers:** Log into your Costpoint systems using the Primary SaaS Admins SAML Attribute (i.e., the email address(upn) or a unique identifier).
 - i. When logging into Costpoint, use the SAML Attribute as the Costpoint Username.
 - ii. Developers will need 2 Costpoint accounts in the DEV system, their end user account for testing that uses SAML and a second account that uses Active Directory as the authentication method. The attribute will be clientid.developerfirstname.developerlast name, for example 50053.Mickey.Mouse. You can find more information on setting up the Cloud Active Directory for your developers [here](#)).
 - **GCC Customers:** Log into your Costpoint systems using a Cloud Active Directory (User Manager) account that has access to the Manage Users application within Costpoint.
2. Navigate to **Admin » Security » System Security » Manage Users** and locate the account to modify.
3. Click the Authentication tab.



4. In **Authentication Method**, select **SAML Single Sign-on**.
5. In the **Active Directory or Certificate ID** field, enter the user's Active Directory user name in your domain.
This can be the username or the username in UPN format (for example, `user@mydomain.local`).
6. Save the record.
7. Repeat steps 3 through 6 for each user in each Costpoint system who want to use the Okta authentication.

Logging into the Costpoint User Interface Environments

Here are examples of the client URLs - the ABC needs to be replaced by your client system name.

Development Environment

This environment is used to build your extensions or web services as needed. Be default, Enterprise customers have a Development environment. Essentials customers can request a WebService Integration Console to build webservices.

URL for front end access:

GCC Customers: <https://ABC-cpd.deltekenterprise.com/cpweb>

GCCM Customers: <https://cp-ABC01-dev.npr.mydeltekgcc.com/cpweb>

System Names: ABCDEV

Non-Production Environment

This environment is used to test your data as it goes into the cloud and for future use to test new functionality or features of future Costpoint releases.

URL for front end access:

GCC Enterprise Customers: <https://ABC-cpt.deltekenterprise.com/cpweb>

GCCM Customers: <https://cp-ABC-tst.npr.mydeltekgcc.com/cpweb>

System Names: ABCTEST, ABCCONFIG, ABCSBOX

Production Environment

This environment is used to test your data as it goes into the cloud and for future use to test new functionality or features of future Costpoint releases.

URL for front end access:

GCC Customers: <https://ABC-cp.deltekenterprise.com/cpweb>

GCCM Customers: <https://cp-ABC-prd.mydeltekgcc.com/cpweb>

System Names: ABCPROD

Configure Costpoint GCCM Developer Accounts for Citrix Access

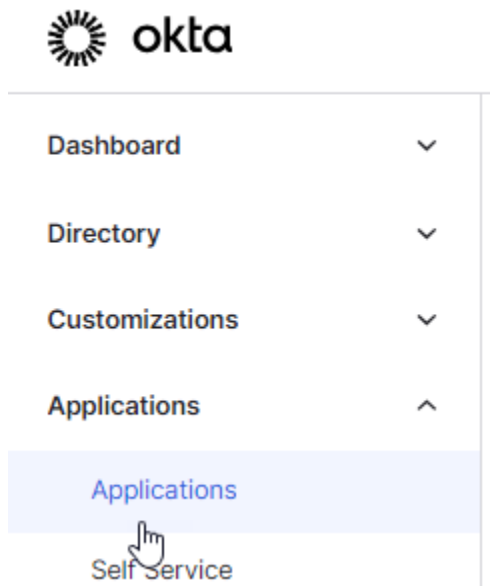
Your developers will access Citrix to get to your Dev machine and build extensions or web services. In order for them to authenticate using Okta idP, you must enable the Citrix application in OKTA and assign your developers to the Citrix account.

Note: You will need to submit the Service Request for Citrix Access to establish the SAML SSO connectivity with our Citrix, in addition to creating the Citrix Access within Okta.

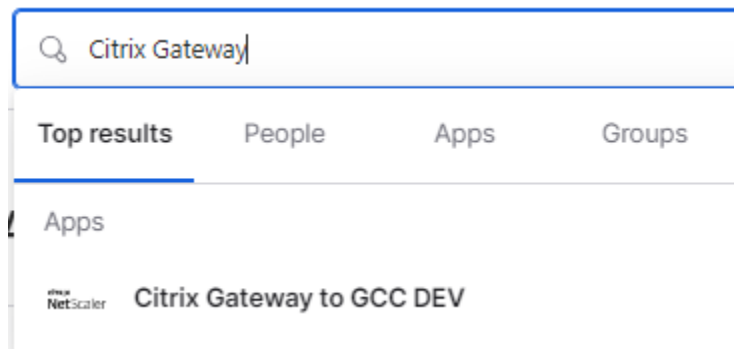
The Okta idP SAML integration for Costpoint GCCM only supports SP-initiated SSO so the customer must point

their browser to the Deltek Citrix Gateway URL - <https://cp-ctx01.pss.mydeltekgcc.com/> and enter their username and hit enter. This will query Citrix policies and then Active Directory to find a match and redirect to their company OKTA website. Therefore, idP-initiated SSO is not allowed (user going OKTA site first to login).

1. OKTA already has created the Citrix Gateway application and is currently available in the OKTA portal to configure and assign to users.
2. Customer must have an OKTA Admin login to the portal and select applications.



3. Search for Citrix Gateway and select Citrix Gateway to GCC DEV button.



4. Select Inactive and select Activate to activate the application.

← Back to Applications

The screenshot shows the configuration page for 'Citrix Gateway to GCC DEV'. On the left is the 'CITRIX NetScaler' logo. The main title is 'Citrix Gateway to GCC DEV'. Below the title, there is a status dropdown menu currently set to 'Inactive'. A mouse cursor is hovering over the 'Activate' option in the dropdown menu. Other options in the dropdown are 'Delete'. To the right of the status dropdown are icons for a lock and a green checkmark, followed by links for 'View Logs' and 'Monitor Imports'. Below the main content area, there are tabs for 'General', 'Sign On', and 'Assignments', with 'Assignments' being the active tab.

← Back to Applications

This screenshot shows the same configuration page for 'Citrix Gateway to GCC DEV', but the status dropdown menu is now set to 'Active'. The 'Activate' option is no longer visible in the dropdown. The rest of the interface, including the logo, title, icons, links, and tabs, remains the same.

5. Customer must configure their Citrix Gateway application URL to Deltek's Citrix Gateway - <https://cp-ctx01.pss.mydeltekgcc.com> by going to General>App Settings>Login URL as shown below section.



Citrix Gateway to GCC DEV

Active ▾



[View Logs](#) [Monitor Imports](#)

- General
- Sign On
- Mobile
- Import
- Assignments

App Settings Edit

Application label	Citrix Gateway to GCC DEV
Login URL	https://cp-ctx01.pss.mydeltekgcc.com
Application visibility	<input type="checkbox"/> Do not display application icon to users <input type="checkbox"/> Do not display application icon in the Okta Mobile app
Browser plugin auto-submit	<input checked="" type="checkbox"/> Automatically log in when user lands on login page
Provisioning	<input type="checkbox"/> Enable on-premises provisioning
Auto-launch	<input type="checkbox"/> Auto-launch the app when user signs into Okta.
Application notes for end users	
Application notes for admins	

- Next the customer will need to provide the Sign On method configuration for SAML by going to the Sign On>Settings>Sign on methods>SAML 2.0>Credentials details>Application username format>default. This can be changed to other attributes, but this is the default format.

Credentials Details

Application username format

Okta username

Update application username on

Create and update

Password reveal

Allow users to securely see their password
(Recommended)

● Password reveal is disabled, since this app is using SAML with no password.

Save

● SAML 2.0

Default Relay State

Disable Force
Authentication




Metadata details

Metadata URL

https://dev-
153391.oktapreview.com/app/exk1w8nqurtap7bm70h
8/sso/saml/metadata

 Copy

 More details

● SAML 2.0

Default Relay State

Disable Force Authentication

Metadata details

Metadata URL `https://dev-153391.oktapreview.com/app/exk1w8nqurtap7bm70h8/sso/saml/metadata`
[Copy](#)

● Hide details

Sign on URL `https://dev-153391.oktapreview.com/app/citrixnetscalergateway_saml/exk1w8nqurtap7bm70h8/sso/saml`
[Copy](#)

Sign out URL `https://dev-153391.oktapreview.com`
[Copy](#)

Issuer `http://www.okta.com/exk1w8nqurtap7bm70h8`
[Copy](#)

Signing Certificate [Download](#) [Copy](#)

● Certificate fingerprint

Credentials Details

Application username format

Okta username

Update application username on

Custom

Email

Email prefix

Okta username

Okta username prefix

(None)

Password reveal

7. Add your developers into this SAML Application to enable their ability to login to Citrix.
8. The SaaS Admin will need to login to Cloud AD Manager and create an AD account and grant access to DEV Groups.