Deltek
Speed. Clarity. Control.

# Costpoint Security

Costpoint Security

26 March 2026

Deltek

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.

Deltek

# Contents


Costpoint Security . . . . . 1

Authentication . . . . . 1

Description of Authentication Methods . . . . . 2

Assign Authentication Methods to Users . . . . . 5

Security Realm and Authentication Providers . . . . . 6

Authentication Process at Login . . . . . 7

Two-Factor Authentication . . . . . 10

PIN Authentication on Mobile Device . . . . . 15

Set-Up Steps Required for Each Authentication Method . . . . . 17

Windows Active Directory Setup . . . . . 18

SAML Single Sign-on Setup . . . . . 21

OIDC Single Sign-on Setup . . . . . 61

Manage User Groups in Active Directory/Identity Provider . . . . . 71

Single Sign-On (Windows Kerberos/AD) Setup . . . . . 75

Single Sign-On for Private or Public Cloud . . . . . 82

Single Sign-On on Mobile Device . . . . . 83

Client Certificate Setup . . . . . 86

Passkey (FIDO) . . . . . 90

Authentication Audit Logging . . . . . 100

User Access to Modules, Applications, Reports, Etc. . . . . 101

Deltek

# Costpoint Security

### Overview

Security is a critical part of any application. Applications must be secured against disclosure of confidential information, modification, or destruction of data, misappropriation of resources, and compromise of accountability. Implementing security measures, such as authentication, authorization, integrity, confidentiality, and non-repudiation, can secure applications.

This document details how the preceding principles are designed and implemented in Deltek Costpoint®. Costpoint uses both Oracle WebLogic® and Java™ Authentication and Authorization Service (JAAS) frameworks to authenticate and authorize clients who are interactive users, Web service clients, and application clients.

## Authentication

Authentication verifies the identity of an application user. Costpoint performs authentication using a login process during which the user supplies credentials, such as a username and password combination. When the user has been authenticated, Costpoint associates a set of identities (also known as *principals*) with that user. For example, the user's identities can include his or her username and group membership.

### Multiple Authentication Methods Available

Costpoint supports multiple authentication methods so that:

- Internet users and local area network users can access Costpoint simultaneously. Generally, the following categories of users access Costpoint:
  - **In-house users**: Users who are registered in the company network (Windows Active Directory) and who typically log into Costpoint only after passing through local network authentication
  - **In-house users who travel occasionally and *Consultants***: In-house users who occasionally log into Costpoint from remote sites without being authenticated in the company network
  - **Remote Office users**: Users who are not registered in the company network and who typically log into Costpoint via remote sites only
- Companies using Costpoint often have unique security requirements. For example, one company's rules may require users to be authenticated on their network before accessing Costpoint. Likewise, a company's rules may require Windows Active Directory to log users onto Costpoint.

Deltek

# Description of Authentication Methods

### Database

This authentication method supports all Costpoint users. With this method, user credentials are stored in the Costpoint database.

Database verification requires no extra configuration efforts.

### Kerberos Single Sign-on

This authentication method supports only In-house users who are currently logged into the company network (via Windows Active Directory). This method allows users to log into Costpoint without providing a user ID and password on the Costpoint Login screen.

Single Sign-On through Kerberos verification requires special WebLogic Server and Windows Active Directory configuration steps.

### SAML Single Sign-on

This authentication method supports only those users that are registered within the company SAML Identity Provider (AD FS, Azure, Okta, Ping, and so on). This method allows users to log into Costpoint without providing a user ID and password on the Costpoint Login screen.

Single Sign-On through SAML verification requires special configuration steps to be performed in Costpoint Configuration Utility and in SAML Identity Provider.

### Kerberos Single Sign-on or SAML Single Sign-on

This authentication method supports either in-house users who are currently logged into the company network (via Windows Active Directory) or those users that are registered within the company SAML Identity Provider (AD FS, Azure, Okta, Ping, and so on). This method allows users to log into Costpoint without providing a user ID and password on the Costpoint Login screen.

Single Sign-On through Kerberos or SAML verification requires special configuration steps to be performed in Costpoint Configuration Utility, WebLogic Server, Windows Active Directory, and in SAML Identity Provider.

### OIDC Single Sign-on

This authentication method supports only those users that are registered within the company OIDC (Open ID Connect) Identity Provider. This method allows users to log into Costpoint without providing a user ID and password on the Costpoint Login screen.

Single Sign-On through OIDC verification requires special configuration steps to be performed in the Costpoint Configuration Utility and in the OIDC Identity Provider.

### Kerberos Single Sign-on or OIDC Single Sign-on

This authentication method supports either in-house users who are currently logged into the company network (via Windows Active Directory) or those users that are registered within the company OIDC Identity Provider. This method allows users to log into Costpoint without providing a user ID and password on the Costpoint Login screen.

Single Sign-On through Kerberos or OIDC verification requires special configuration steps to be performed in the Costpoint Configuration Utility, WebLogic Server, Windows Active Directory, and in OIDC Identity Provider.

### Active Directory

This authentication method supports In-house users who are registered in the company network (via Windows Active Directory) but not necessarily logged into the company network. A user is required to provide a user ID and password on the Login screen to access Costpoint. This authentication method verifies passwords against the Windows Active Directory.

Active Directory verification requires special WebLogic Server and Windows Active Directory configuration steps.

### Passkey (FIDO)

This authentication method is based on using private-key/public-key cryptography and is completely passwordless. In order to log in, a user must possess a valid FIDO device, such as a FIDO USB key, or use a biometric method (typically a fingerprint, facial recognition, or personal PIN).

### Kerberos Single Sign-on or Active Directory

This authentication method supports In-house users and Consultants. It gives users two options for accessing Costpoint:

- **When a user is already logged into the company network (Single Sign-on Kerberos)**: The user can access Costpoint without providing a user ID and password on the Costpoint **Login** screen.
- **When a user is not logged into the company network (Active Directory)**: The user can access Costpoint by entering a user ID and password on the Costpoint Login screen. This method verifies passwords against the Windows Active Directory.

**Kerberos Single Sign-on or Active Directory** authentication requires special WebLogic Server and Windows Active Directory configuration steps.

### Kerberos Single Sign-on or Database

Similar to the above **Single Sign-on or Active Directory** method, this authentication method supports in-house users and consultants. It gives users two options for accessing Costpoint:

- **When a user is already logged into the company network (Single Sign-on)**: The user can access Costpoint without providing a user ID and password on the Costpoint **Login** screen.
- **When a user is not logged into the company network**: The user can access Costpoint by entering a user ID and password on the Costpoint Login screen. This method verifies passwords against the Costpoint database.

**Kerberos Single Sign-on or Database** authentication requires special WebLogic Server and Windows Active Directory configuration steps.

### Windows Domain and Active Directory

This authentication method supports In-house users who are currently logged into the company network (Windows Active Directory). A user is required to provide a user ID and password on the Costpoint Login screen. This method verifies passwords against Windows Active Directory.

Windows Domain and Active Directory authentication requires special WebLogic Server and Windows Active Directory configuration steps.

### Windows Domain and Database

This authentication method supports In-house users who are currently logged into the company network (Windows Active Directory). A user is required to enter a user ID and password on the Costpoint Login screen. This method verifies passwords against the Costpoint database.

This authentication method requires special configuration steps to be performed on WebLogic Server and Windows Active Directory.

### Certificate Single Sign-on

With this authentication method, the user identity is verified through the X.509 certificate installed on a user's machine. This is a special use of the Secure Sockets Layer (SSL), where both the WebLogic server and the user are identified by their own certificates. This is a very strong form of authentication which guarantees that a user can log into Costpoint only from a machine that has a valid certificate installed. All communication between server and client is encrypted. This method allows users to log into Costpoint without providing a user ID and password on the Costpoint Login screen.

This method is targeted to support all Costpoint users. It requires special configuration steps to be performed on WebLogic Server and on the client machine.

Deltek

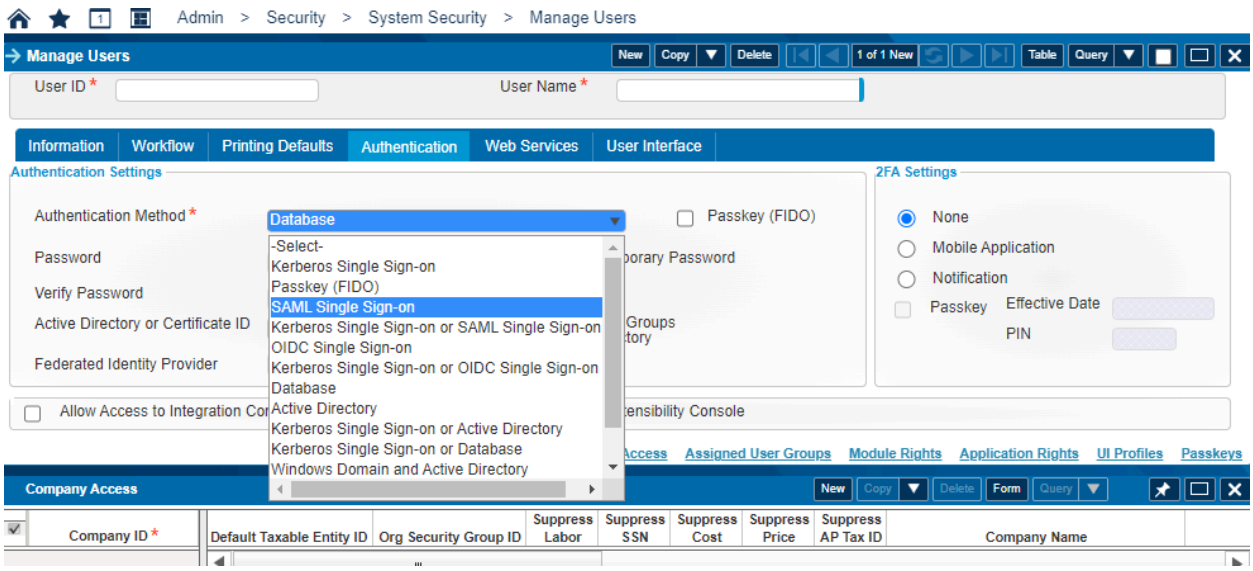
# Assign Authentication Methods to Users

Each Costpoint user has an assigned authentication method. You can assign authentication methods to users using the Authentication tab of the Manage Users screen (SYMUSR).

- An Active Directory ID must be entered for the following authentication methods:
  - SAML Single Sign-on
  - Kerberos Single Sign-on
  - Kerberos Single Sign-on or SAML Single Sign-on
  - OIDC Single Sign-on
  - Kerberos Single Sign-on or OIDC Single Sign-on
  - Active Directory
  - Kerberos Single Sign-on or Active Directory
  - Kerberos Single Sign-on or Database
  - Windows Domain and Active Directory
  - Certificate Single Sign-on
- Using certain authentication methods (including Kerberos Single Sign-on, Active Directory, Kerberos Single Sign-on or Active Directory, Kerberos Sign-on or Database, Windows Domain and Active Directory, Windows Domain and Database) requires special configuration steps to be performed by your company's IT team on the WebLogic Server and Windows Domain Controller machine.
- Using SAML Single Sign-on also requires special configuration steps to be performed by your company's IT in Costpoint Configuration Utility and in SAML Identity Provider.

**To assign an authentication method to a user:**

1. Click **Administration » Security » System Security » Manage Users**.




2. Select a user.

3. Click the Authentication tab.

4. Enter the following Authentication Settings:

   - **Authentication Method**: Select the user authentication method (for example, **Database** or SAML **Single Sign-On**).
   - **Password**: Enter the user password (required for Database and Windows Domain and Database authentication methods).
   - **Verify Password**: Re-enter the same password to verify its accuracy (required for Database authentication and Windows Domain and Database authentication methods).
   - **Active Directory or Certificate ID**: Select the user ID for login to the Windows Domain. This is required for Single Sign-on (Kerberos, SAML, or OIDC), Active Directory, Kerberos Single Sign-on or Active Directory, Kerberos Single Sign-on or Database, Windows Domain and Active Directory, Windows Domain and Database, and Certificate Single Sign-on authentication methods.
   - **Allow Application Access via Integration Service**: Select this check box to allow integration clients (Web service clients, application clients, and any other programs or services) to log into Costpoint with a Costpoint user ID (required).

# Security Realm and Authentication Providers

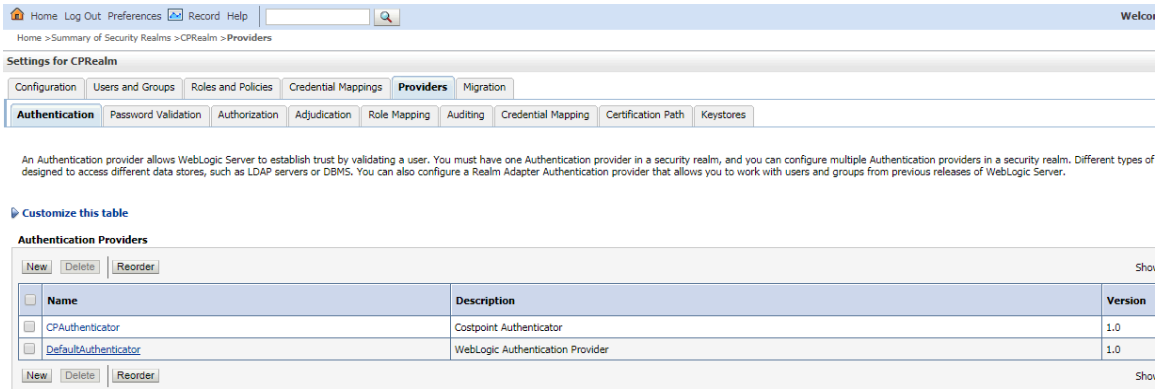
The WebLogic Server System Administrator configures the **CPRealm** security realm to support Costpoint

authentication. **CPRealm** is a chain of authentication providers in which each provider or set of providers is responsible for authenticating users of certain types, including Costpoint users and internal Weblogic users.

The following providers must be configured in the following order to support all Costpoint authentication methods:

1. **CPAuthenticator**: Performs all types of authentications for Costpoint users, including Active Directory, Database, Passkey (FIDO), Windows AD/Kerberos and SAML Single Sign-on.

2. **DefaultAuthenticator**: Performs authentication for built-in system WebLogic Server service accounts. This is required for use of WebLogic Administrator console.




# Authentication Process at Login

The Authentication process starts with client login requests. In Costpoint, we distinguish two types of clients: **real** (interactive) users and **integration** clients (Web service clients, rich application clients, and any other programs or services).

### Interactive User Login

There could be several distinguished authentication activities that occur in Interactive User Login mode:

- Database authentication
- Active Directory authentication
- Single Sign-On authentication through Client Certificate
- Single Sign-On authentication through Windows AD/Kerberos
- Single Sign-On authentication through SAML or OIDC
- Passkey (FIDO) authentication

## Integration Client Login

Integration clients, such as Web services and Java application clients, log into Costpoint through being invoked by a third-party tool or program.

- Integration clients must use a real Costpoint user ID to log in.
- Allow Application Access via Integration Service check box must be selected.
- An integration client user identity may use one of the following authentication methods:
  - Database
  - Active Directory
  - JWT
  - SAML

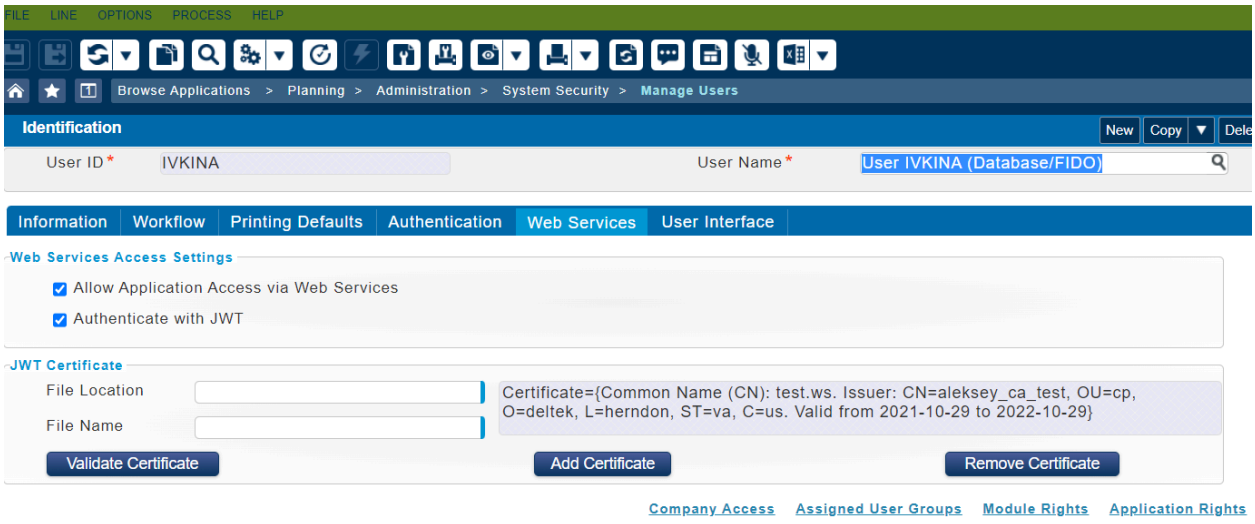
  Database, AD, and JWT authentication methods are based on Web Services UserName Token profile. SAML authentication is based on Web Services SAML Token Profile.

**Note:** In case of UserName Token profile, the Costpoint user ID must be sent concatenated with the system name (for example, SMITH __ DELTEKPROD).

Use two underscore characters "__" as the delimiter between the user ID and the system name.

For SAML, the default (first) system name will be used, or you can send it via a separate SAML attribute statement or claim with the predefined name "system."

JSON Web Token (JWT) authentication is based on the JSON Web Signature standard and private/public key/certificate or PKI infrastructure. You must generate a private key/public certificate pair first and then link public certificate to Costpoint user account that you want to use for web service authentication. The public certificate will be used to verify web service credentials presented in the form of signed JWT. You upload the public certificate using the Costpoint Manage Users function.



Once you have the verification certificate linked to user account you can generate a JWT and have it signed using a private key. In order to be successfully recognized and validated by Costpoint JWT must contain a few required claims such as “sub”, “iat”, “nbf”, “exp” and “alg”. Note that for security reasons minimum required length of RSA key must be at least 2048 and SHA256 hashing must be used.

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "typ": "JWT",
  "kid": "k1",
  "alg": "RS256"
}
```

PAYLOAD: DATA

```
{
  "exp": 1644004579,
  "jti": "Y7c70-zct2B5wS_rQXEXfg",
  "iat": 1644003679,
  "nbf": 1644003559,
  "sub": "CPSUPERUSER"
}
```

Use signed JWT as a password in web service username token profile call. For example:

Params Authorization Headers (9) Body Pre-request Script Tests Settings Cookies

none form-data x-www-form-urlencoded raw binary GraphQL XML Beautify

```
<soapenv:Envelope xmlns:cpw="http://www.deltek.com/enterprise/integration/ws/cpwwsgenericmodule" xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/
    ">

<soapenv:Header>

    <wsse:Security soapenv:mustUnderstand="1" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
        <wsse:UsernameToken wsu:Id="unt_MjgwNjA4OGMzZGMz" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
            <wsse:Username>CPSUPERUSER__CTB81DEO19</wsse:Username>
            <wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.
                0#PasswordText">eyJ0eXAiOiJKV1QiLCJraWQiOiJrMSIsImFsZyI6IlJTMjU2In0.
                eyJleHAiOjE2NDQwMDQ1NzksImp0aSI6Ilk3YzcwLXpjdDJCNXdTX3JRWEVYZmciLCJpYXQiOjE2NDQwMDM2NzksIm5iZiI6MTY0NDAwMzU1OSwic3ViIjoiQ1BTVVBFUlVTRVIifQ
                .
                f3LzNHj4_znOMOmK2gVAmbi58WcNJe-6u5zu6iwVYlb3P6JA1IjDNoJzxTxSitWY2ruRCxXxmbHA00yexetGxnxktL01oefcct9q2EmZJKjeD25-5UwIbjKCvqJc9jK1szvfj3vkS1
                5PiewN72beRm-c5igBaBQ1Ja9eUnk6ApLb_G-JYQJEKOF8knO5aTG2EHKOpDl2t3FGGbVWhvUWM2kAFAFputejh51MU9ymDJHR7D6Oe9YCQC0WsGeokDUHXmxopCszrqBATHHSlSS0
                fYPYo0wC56L9-oiCWZ7CO-GBtXFvwSmzxNcldcc8JwpDH0a45pK_3T56rza_ZxIxcQ</wsse:Password>

        </wsse:UsernameToken>
    </wsse:Security>
</soapenv:Header>

<soapenv:Body>
<cpw:cpwwsgenericimport>
<cpw:systemName>CTB81DEO19</cpw:systemName>
<cpw:companyId>1</cpw:companyId>
<cpw:document>
```

# Two-Factor Authentication

Two-factor authentication (2FA) is an extra layer of security that verifies the identification of users using a combination of two different components, such as the username/password component and the one-time passcode component. The one-time, 6-digit random number passcode is either generated by Costpoint and securely emailed to a user's email address or generated separately by a user on a mobile device through one of the available 2FA mobile applications such as Duo Security or Google Authenticator.

Users can also use a passkey instead of having one-time passcodes. With Passkey (FIDO) credentials, there's no looking at codes and re-typing. A user either inserts a personal Security Key into the computer's USB port when asked or proves his/her own identity through Windows or Android PIN or even biometrics (for example, face recognition, fingerprints, or a BLE (Bluetooth low energy) device).

### Supported 2FA Models

Costpoint supports the following models:

- Email: With this model, Costpoint generates a one-time passcode and sends it to a user's email address or mobile phone via SMS or produces a native notification on a user's registered device. During login, the user enters the received one-time passcode along with their username/password combination.
- Mobile Application: This model is a disconnected 2FA model where a one-time passcode is separately generated on the user's mobile device. During login, the user enters the generated one-time passcode along with their user name/password combination.
- Passkey: This model is a disconnected 2FA model where one-time passcodes are not generated or even required. Instead of having one-time passcodes, users insert a personal USB stick/device into the computer's USB port (Yubico, Feitian, or similar USB key) or BLE device or use a biometric method such as a fingerprint, facial recognition, or personal PIN when asked at login.
  Passkeys provide protection beyond what one-time passcodes already support. For example, sophisticated attackers could set up a lookalike site that asks a user to provide a one-time passcode to them instead of Costpoint. Passkeys offers better protection against this kind of attack because it uses cryptography instead of one-time passcodes and automatically works only with the website it is supposed to work with.
  Note that Passkeys are supported by the latest Chrome, Edge, Safari, and Firefox browsers.

### User PIN

In addition to a one-time passcode, a user may be asked to verify their identity through a personal four-digit personal identification number (PIN). This PIN is stored in User Preferences and may be required on the login page based on the Costpoint System Settings.

### Authentication Methods

2FA can be enabled for a user with authentication method that requires entering user name/password combination on login page. Such methods are Database, Active Directory, Kerberos Single Sign-on or Active Directory, Kerberos Single Sign-on or Database, Windows Domain and Active Directory, Windows Domain and

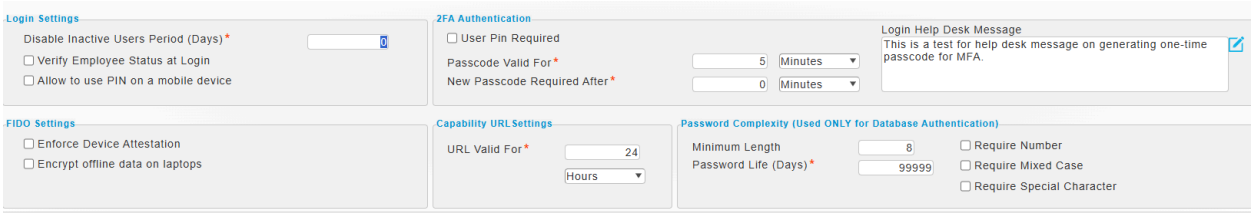
Database.

### 2FA System Settings

You can change the 2FA system settings on the Configure System Settings screen. System administrators control the following settings:

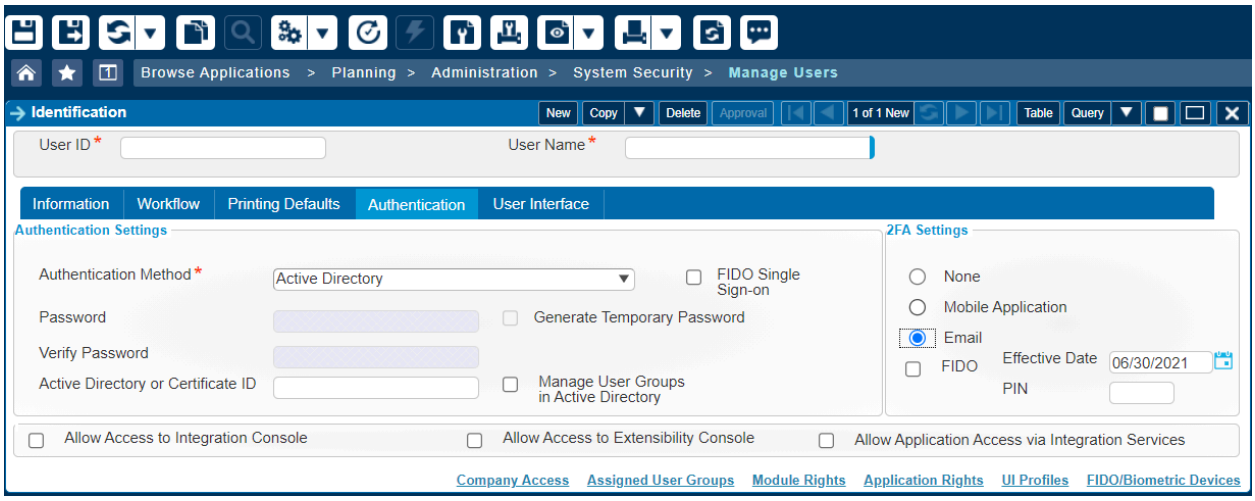
- **User PIN Required**: Selecting this check box indicates that the user's PIN is required during the login process.
- **Passcode Valid For**: This setting determines the time interval during which the passcode is valid.
- **New Passcode Required After**: This setting determines the time interval for which a new passcode won't be required at login.
- **Login Help Desk Message**: This field allows the system administrator to enter a message that displays at login when using 2FA mode.

These settings are effective for all users that have 2FA enabled on the Manage Users screen.



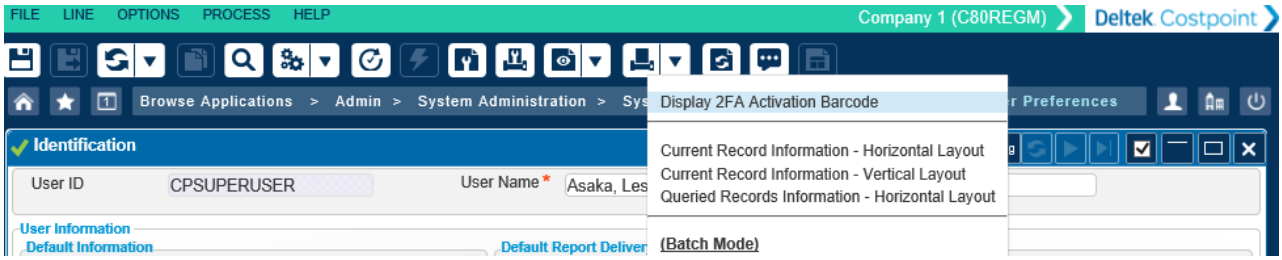

### 2FA User Setup

2FA user settings are configured on the Manage Users screen. System administrators can enable the 2FA mode for a user and select either the **Mobile Application**, **Email**, or **Passkey (FIDO)** 2FA model. The user's PIN can also be entered here as well as on the User Preferences screen. The **Effective Date** field controls the 2FA start date/time, thus allowing users to have some grace period to complete additional 2FA enrollment steps, such as setting up and configuring a 2FA account on a mobile phone.



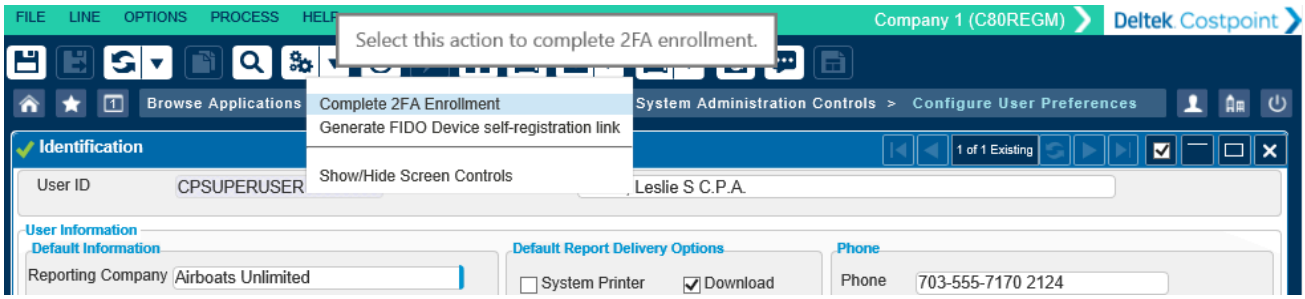

With the 2FA **Email** option, the 2FA login mode is effective immediately. Next time a user tries to log in to the system, a temporary passcode will be required.

With the 2FA **Mobile Application** mode, additional steps are required to complete the 2FA enrollment. First, the user has to install a 2FA mobile application such as Duo Security or Google Authenticator on their mobile device. Next, the user has to display the 2FA Activation Barcode report and scan the generated image by using the previously installed 2FA application.

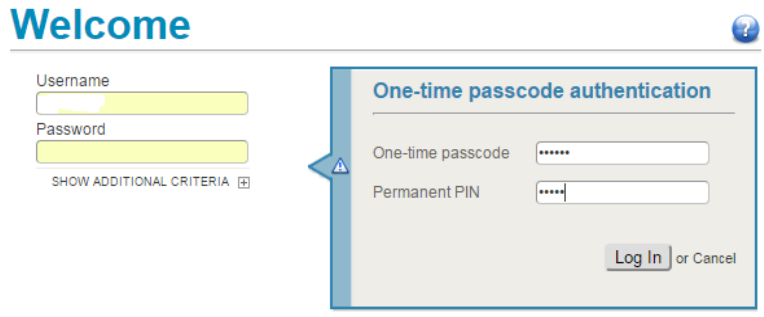



SuperTech, Inc.
2FA Activation Barcode
User:
Page 1 of 1
04/07/16
01:08 PM
Privacy Statement
This is confidential information

And finally, the user has to run the **Complete 2FA Enrollment** action, which will enable 2FA mode.

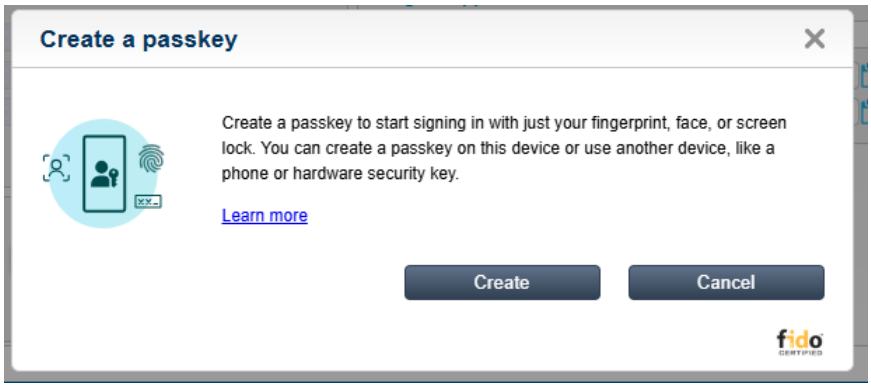



The next time the user tries to log in to the system, a temporary passcode will be required.

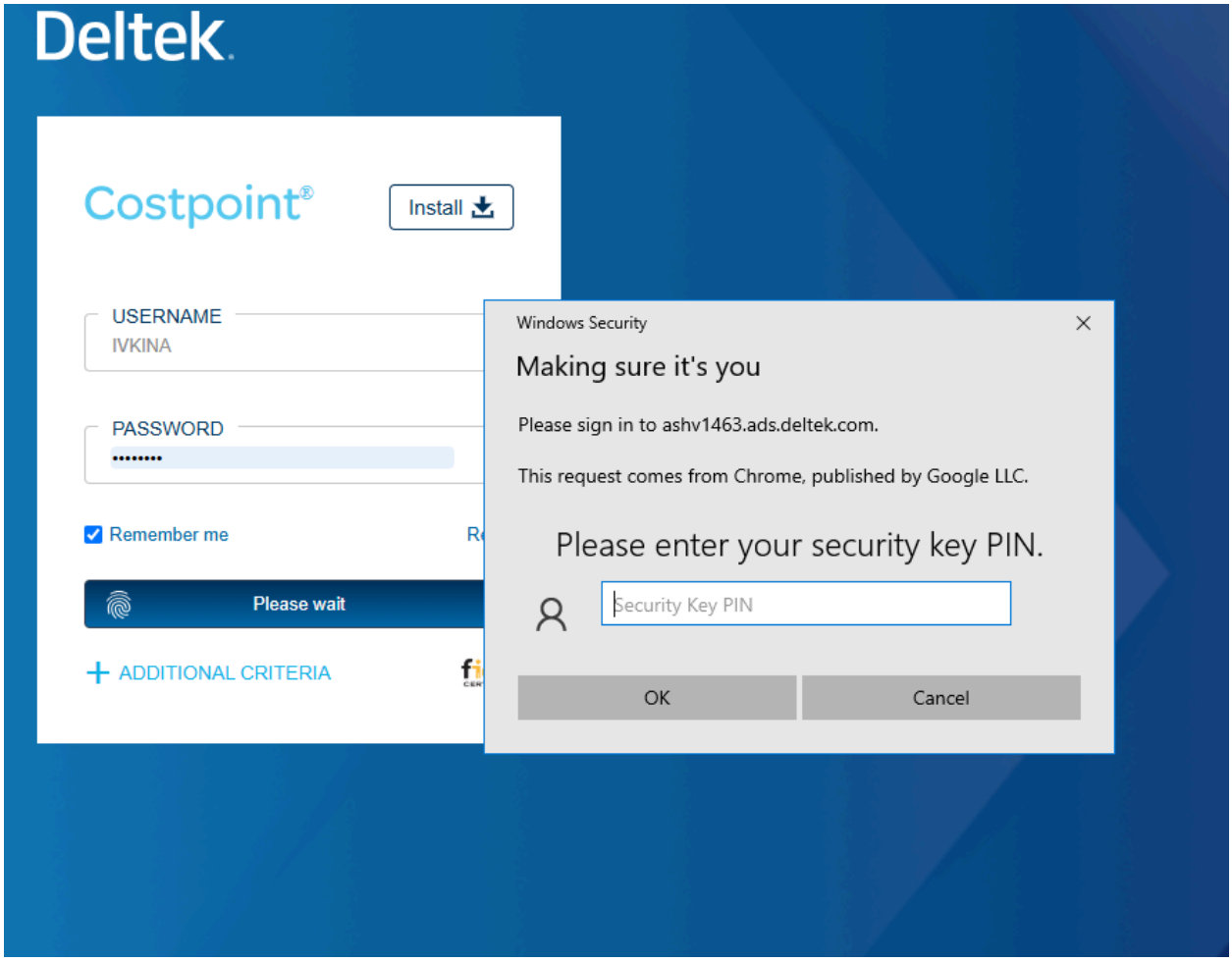



With the 2FA **Passkey** mode, additional steps are also required to complete the 2FA enrollment. First, **Passkey** mode requires the user to configure one of the 2FA base or backup modes: **Email** or **Mobile Application**. This is

necessary if the user's device does not support **Passkeys**. Then they can still log in to the system with a one-time passcode provided either through email or by the user's mobile phone. Second, the user has to register their Passkey in **User Preferences** by clicking the **Create Passkey** button and following the onscreen instructions.




The next time the user tries to log in to the system, the Passkey will be required.



# PIN Authentication on Mobile Device

Users that run Costpoint on mobile devices may be able to log into the product by just providing a 4-digit PIN instead of a password. This feature must first be enabled/allowed by the System Administrator in the Configure System Settings application.

To enable Login with PIN on a mobile device:

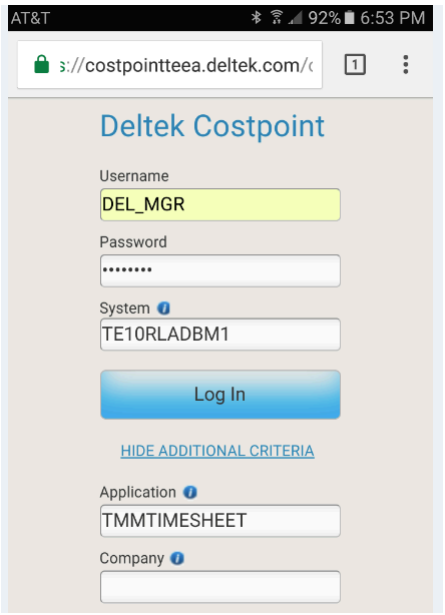
1. Click **Administration » Security » System Security » Configure System Settings**.

2. Go to the Corporate Settings subtask, and click the Security Settings tab.

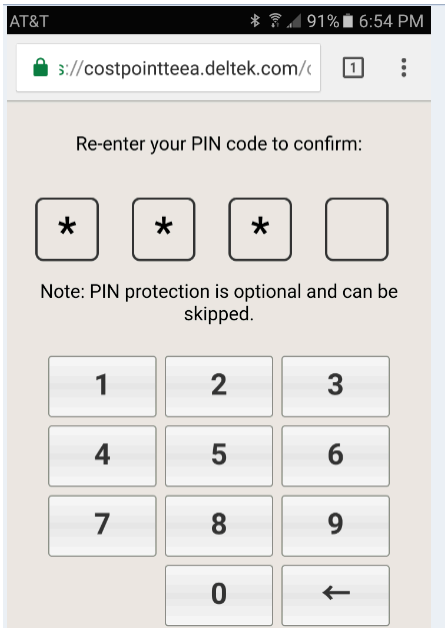
3. Select the **Allow to use PIN on a mobile device** checkbox and save changes.

```
<img src="./media/image17.png" style="width:6.5in;height:2.25in" />
<p> </p>
```

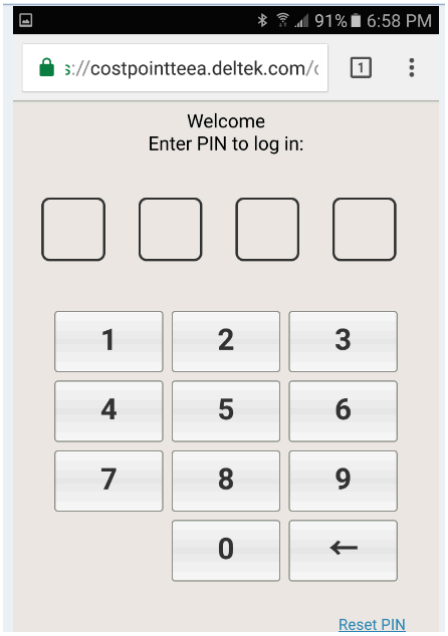
At the very first login only, a user on a mobile device will still be prompted to provide a password to verify their identity.

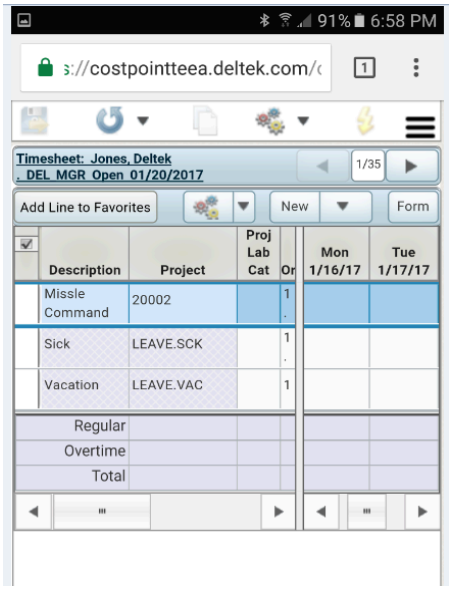



After the correct password is provided and verified, the user will be given the option to store PIN for next login.




After the PIN is confirmed, the same user on the same mobile device will be able to log into Costpoint by providing the PIN only. The password won't be required.






# Set-Up Steps Required for Each Authentication Method

If you want to use the Costpoint Database authentication method, you do not need to perform any extra configuration steps. However, all other authentication methods require some special configuration.

Each of the configuration steps is described later in this guide.

| Authentication Method | Configuration Steps Required |
|---|---|
| Database | None |
| Active Directory | Windows Active Directory Setup |
| Passkey (FIDO) | None |
| SAML Single Sign-On | SAML Setup |
| OIDC Single Sign-On | OIDC Setup |
| Kerberos Single Sign-On | Single Sign-On Setup (Windows AD/Kerberos) |
| Kerberos Single Sign-On or SAML Single Sign-On | Single Sign-On Setup (Windows AD/Kerberos) and SAML Setup |
| Kerberos Single Sign-on or Active Directory | Single Sign-On Setup (Windows AD/Kerberos) + Windows Active Directory Setup |
| Kerberos Single Sign-on or Database | Single Sign-On Setup (Windows AD/Kerberos) |
| Windows Domain and Active Directory | Single Sign-On Setup (Windows AD/Kerberos) + Windows Active |

| Authentication Method | Configuration Steps Required |
|---|---|
| | Directory Setup |
| Windows Domain and Costpoint Database | Single Sign-On Setup (Windows AD/Kerberos) |
| Certificate Single Sign-on | Certificate install on the client machine |

# Windows Active Directory Setup

To enable authentication of Costpoint users with Windows Active Directory:

1. Configure the Windows Domain Controller and Active Directory.

   The Active Directory service is the distributed directory service that is included with the Microsoft® Windows Server operating system. It enables centralized, secure management of an entire network. A domain controller is a server that is running a version of the Windows Server operating system and has Active Directory installed.

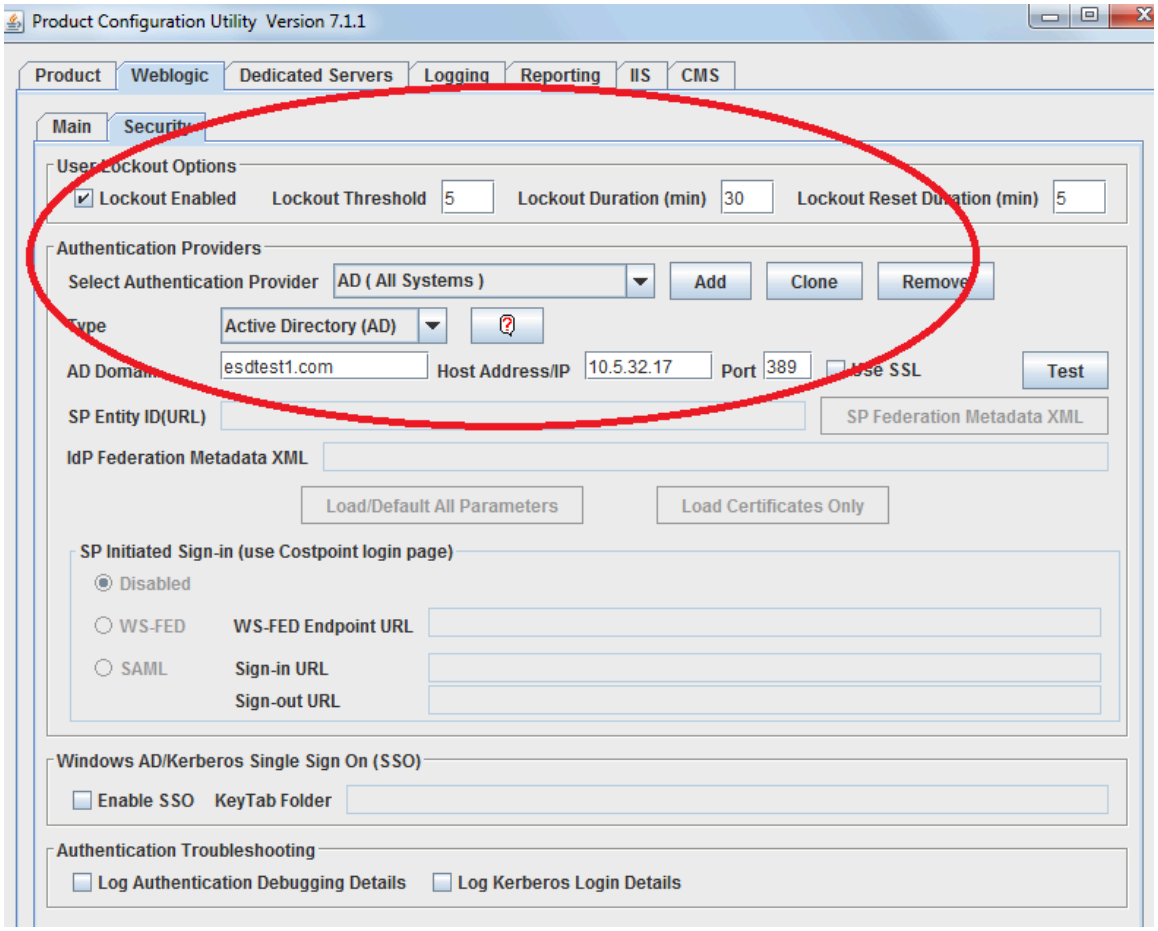
   **Attention:** For more information on how to set up the Domain Controller and Active Directory, refer to Microsoft documentation.

2. Update the Windows Active Directory settings using Configuration Utility:

   a. Click **Add** on the Weblogic » Security tab to enter a unique name for the LDAP server.

   b. Enter the domain name, the domain controller hostname, and the port.

   c. Click **Test** to verify the connectivity to LDAP server.




**Attention:** For detailed information about the Costpoint Configuration utility, see the *Deltek Costpoint 8.2 Configuration Utility Guide*.

**Note:** You can configure multiple LDAP servers/domains. A user will be authenticated against each server/domain until authentication succeeds.

## Update User Setup

The Costpoint Administrator must also assign the Active Directory authentication method to each user who will use it. Use the Manage Users (SYMUSR) application to make this assignment.

**To assign the Active Directory authentication method to a user:**

1. Click **Administration » Security » System Security » Manage Users**.

2. Select a user.

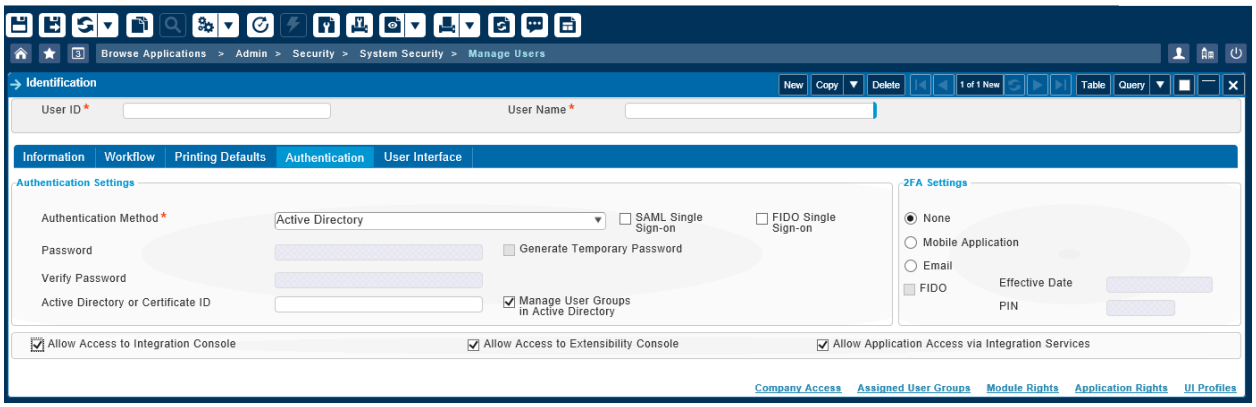
3. Click the Authentication tab.

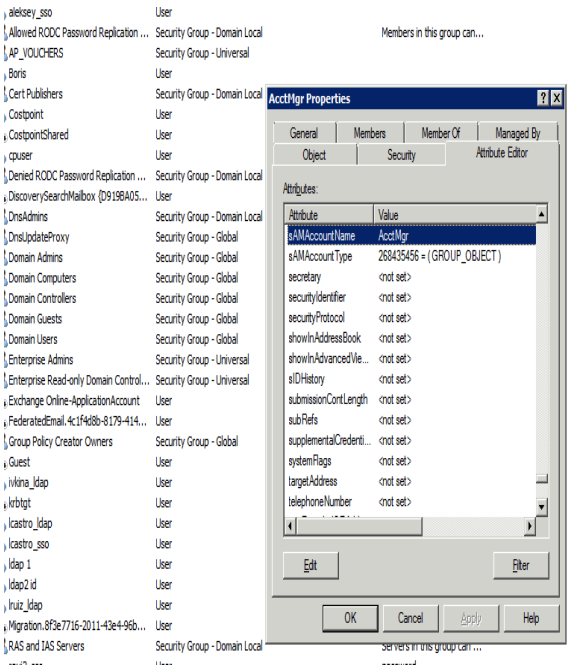
4. Enter the following Authentication Settings:

   - **Authentication Method**: Enter **Active Directory**.
   - **Active Directory or Certificate ID**: Enter the Active Directory user ID.

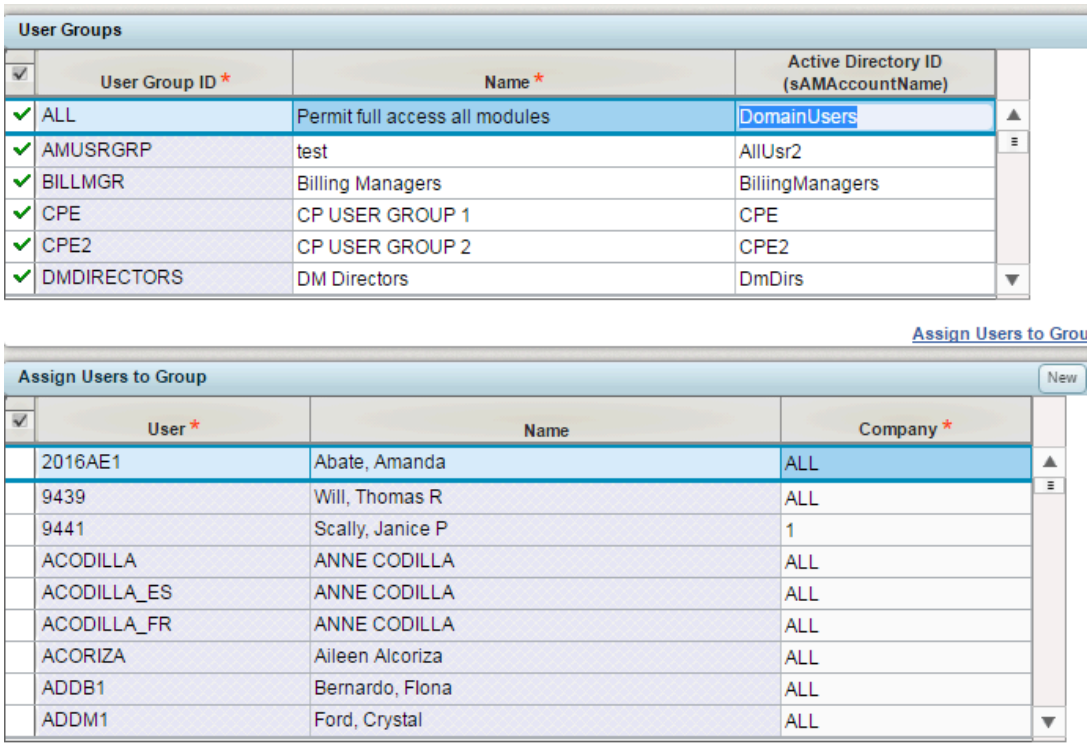
5. Save your changes.

6. Repeat these steps for any users who should have Active Directory authentication.



7. Repeat the above step for each Costpoint group that needs to be synced up with Active Directory group.



User Groups

| User Group ID * | Name * | Active Directory ID (sAMAccountName) |
|---|---|---|
| ALL | Permit full access all modules | DomainUsers |
| AMUSRGRP | test | AllUsr2 |
| BILLMGR | Billing Managers | BiliingManagers |
| CPE | CP USER GROUP 1 | CPE |
| CPE2 | CP USER GROUP 2 | CPE2 |
| DMDIRECTORS | DM Directors | DmDirs |

Assign Users to Grou

Assign Users to Group — New

| User * | Name | Company * |
|---|---|---|
| 2016AE1 | Abate, Amanda | ALL |
| 9439 | Will, Thomas R | ALL |
| 9441 | Scally, Janice P | 1 |
| ACODILLA | ANNE CODILLA | ALL |
| ACODILLA_ES | ANNE CODILLA | ALL |
| ACODILLA_FR | ANNE CODILLA | ALL |
| ACORIZA | Aileen Alcoriza | ALL |
| ADDB1 | Bernardo, Flona | ALL |
| ADDM1 | Ford, Crystal | ALL |

# SAML Single Sign-on Setup

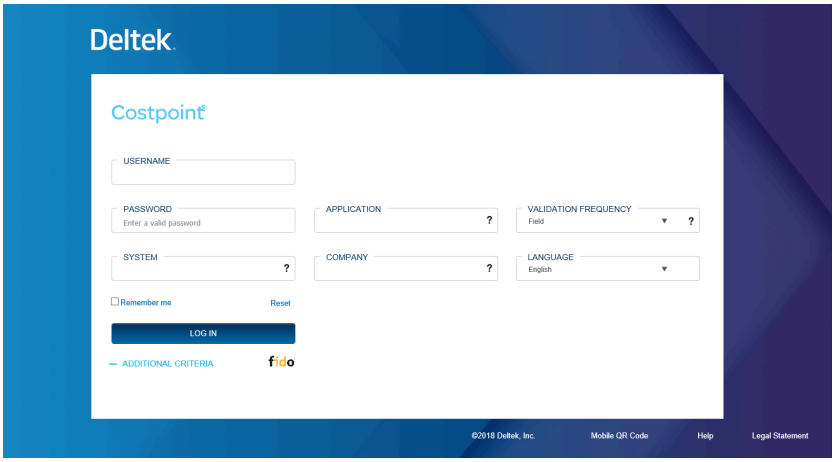
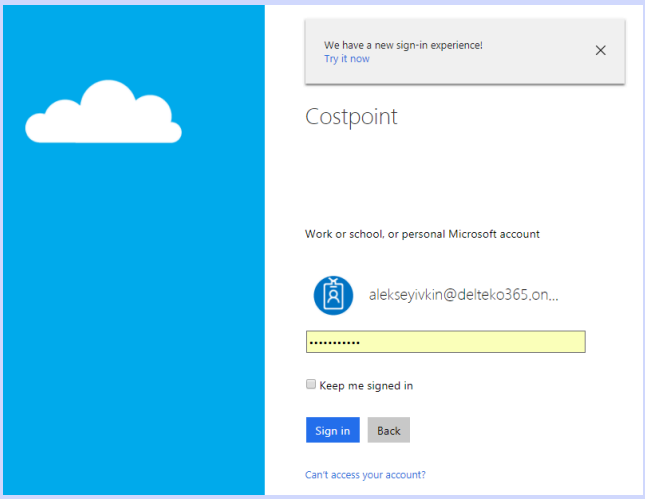
Costpoint can be configured to act as a SAML Service Provider to allow users to log into the system in SAML Single Sign-On (SAML SSO) mode. In this scenario, users do not provide credentials such as password or MFA on the Costpoint login page. Instead, AD FS or Azure Active Directory or any other SAML compliant server acts as a SAML Identity Provider responsible for verifying the user's identity.

There are two sign-in scenarios in case of SAML SSO:

- Costpoint initiated sign-in (SP-initiated sign in).
- SAML Identity Provider (AD FS, Azure, or other) initiated sign-in (IdP-initiated sign in).

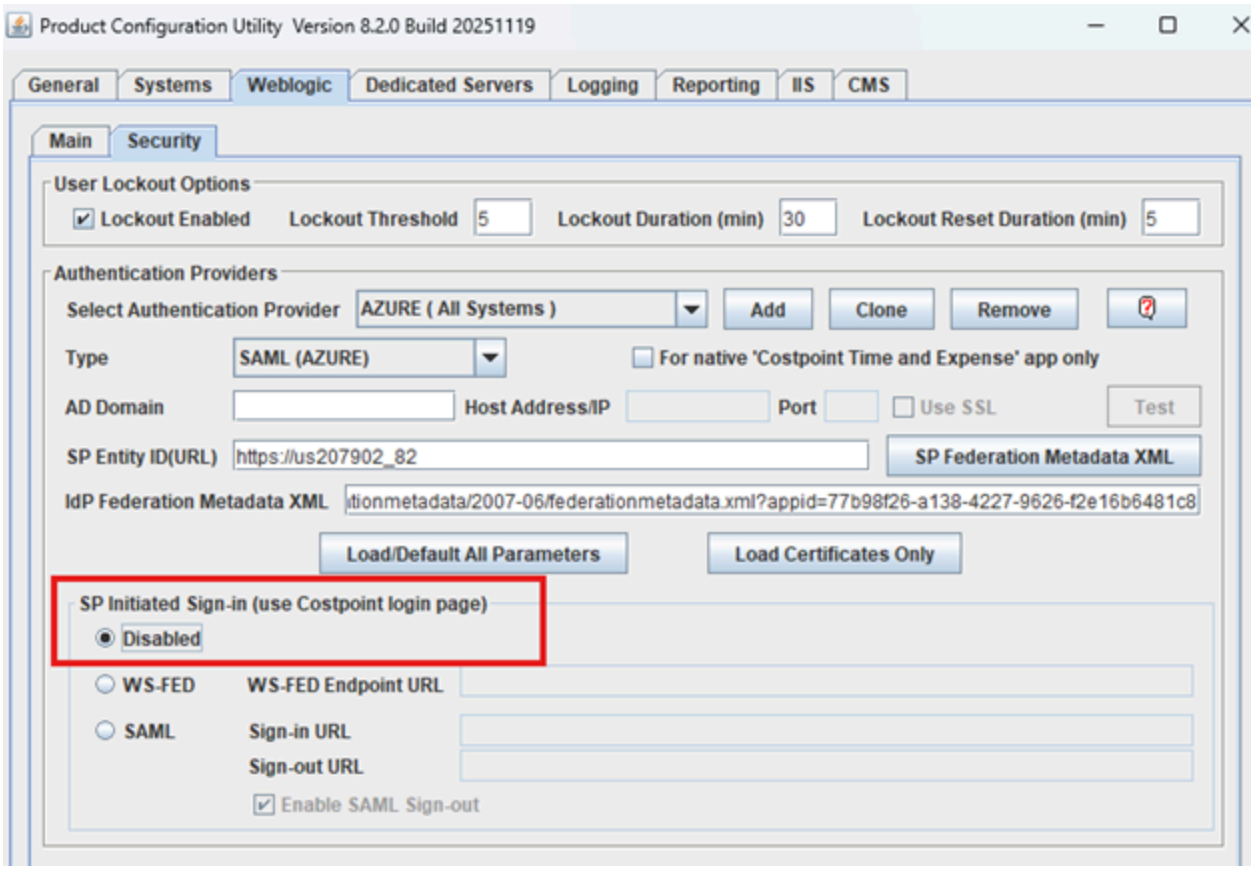
## Costpoint Initiated Sign-in

The following table outlines the steps for Costpoint initiated sign-in.

| Step | Description |
|---|---|
| 1 | The user goes to the Costpoint login page and provides a user name. The user does not type the password but instead tabs out of **Username** field or clicks the **Log In** button.<br>  |
| 2 | Costpoint redirects the user to the AD FS or Azure or other SAML server login page where the user provides credentials (user name, password, biometrics, certificates, MFA, and so on).<br>  |
| 3 | The user's identity is verified by SAML provider (AD FS, Azure, or other), and a SAML authentication token is issued. The user is redirected back to Costpoint, where Costpoint verifies the SAML authentication token. If token is valid, the user is allowed into Costpoint. |

SP initiated sign-in in Costpoint is done through SAML or WS-FED protocols. After initiating the sign-in process, the SAML Provider verifies user credentials. Upon successful verification, the SAML Provider issues SAML assertion to the Costpoint login module. The Costpoint login module verifies the SAML assertion and lets the user into the system upon successful verification.

The System Administrator can always disable Costpoint Initiated sign-in through **Costpoint Config Utility » Weblogic » Security » Authentication Provider** settings.



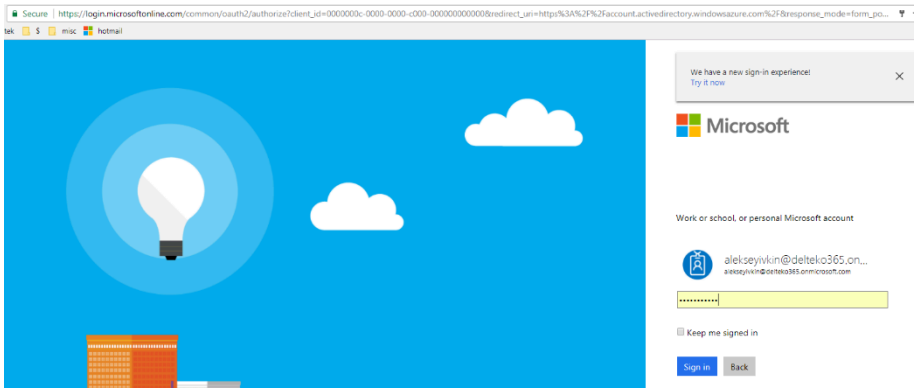
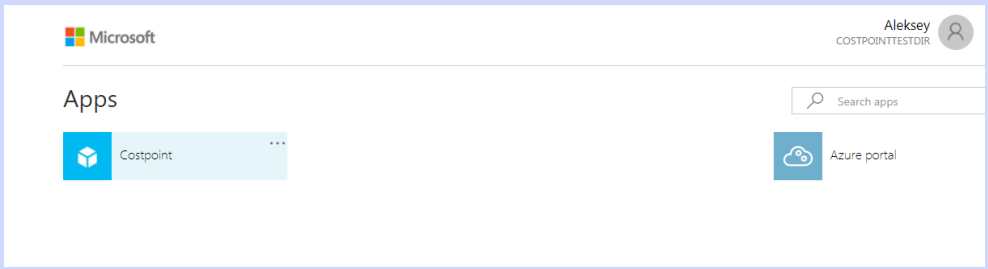

The System Administrator can also disable the redirect from the Costpoint login page to the SAML Provider login page due to company security restrictions. To do this, the System Administrator needs to modify the Costpoint **enterprise.properties** configuration file and run the **"Rebuild Global Settings>Reload All Settings"** function.

The IdP initiated sign-in flow described next is always enabled.

### Identity Provider Initiated Sign-in

The following table outlines the steps for Identity Provider initiated sign-in.

| Step | Description |
|---|---|
| 1 | The user logs into the SAML Provider (AD FS, Azure, or other) portal. |

| Step | Description |
|---|---|
| |  |
| 2 | The user clicks the Costpoint application icon configured in SAML provider portal.<br>  |
| 3 | SAML provider (AD FS, Azure, or other) issues a SAML authentication token and redirects the user to Costpoint, where Costpoint verifies the SAML authentication token. If the token is valid, the user is allowed into Costpoint. |

The Costpoint-side configuration process may vary depending on which SAML Identity Provider is selected to verify users' credentials. Generally, the overall process consists of three main parts:

1. Update the Costpoint Configuration Utility to add the SAML server to act as a SAML Identity Provider.

2. Select and configure SAML Server (AD FS, Azure, or other) to act as the SAML Identity Provider. You can select only one SAML Identity Provider for this configuration.

3. Activate SAML SSO mode for Costpoint user accounts.

### Configure SAML Single Sign-on between Costpoint and SAML IdP

Setting up SAML Single Sign-on between Costpoint and SAML Identity Provider requires changing configuration on both sides. Typically, you start configuring initial settings in Costpoint Configuration Utility. Then, having Costpoint (SP) SAML metadata, you complete IdP setup.

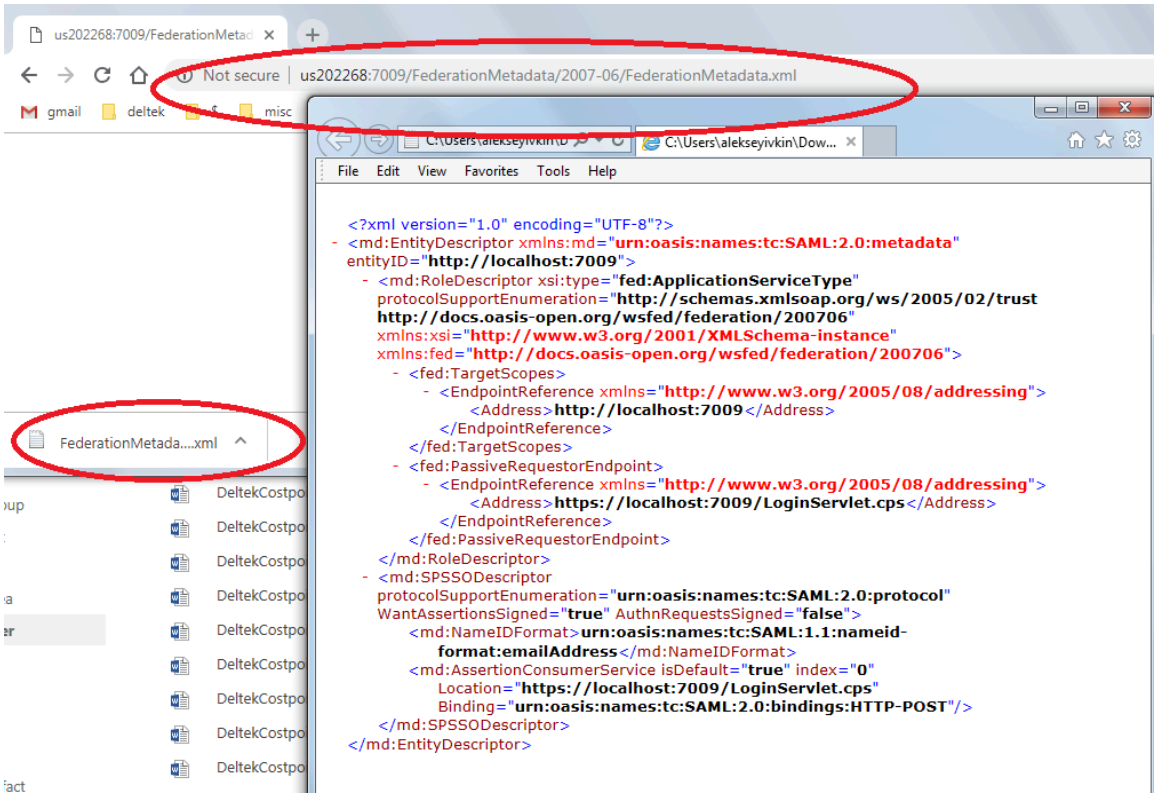
Finally, having IdP SAML metadata, you return to Costpoint Configuration Utility and complete Costpoint (SP) SAML configuration. Both parties, Costpoint and IdP, have their own SAML metadata. Usually, SAML metadata is defined through FederationMetadata.xml file. You generate Costpoint FederationMetadata.xml using one of the approaches:

1. Download Costpoint FederationMetadata.xml from your Costpoint Server public URL.

   Open browser and navigate to Costpoint FederationMetadata.xml URL. For example:

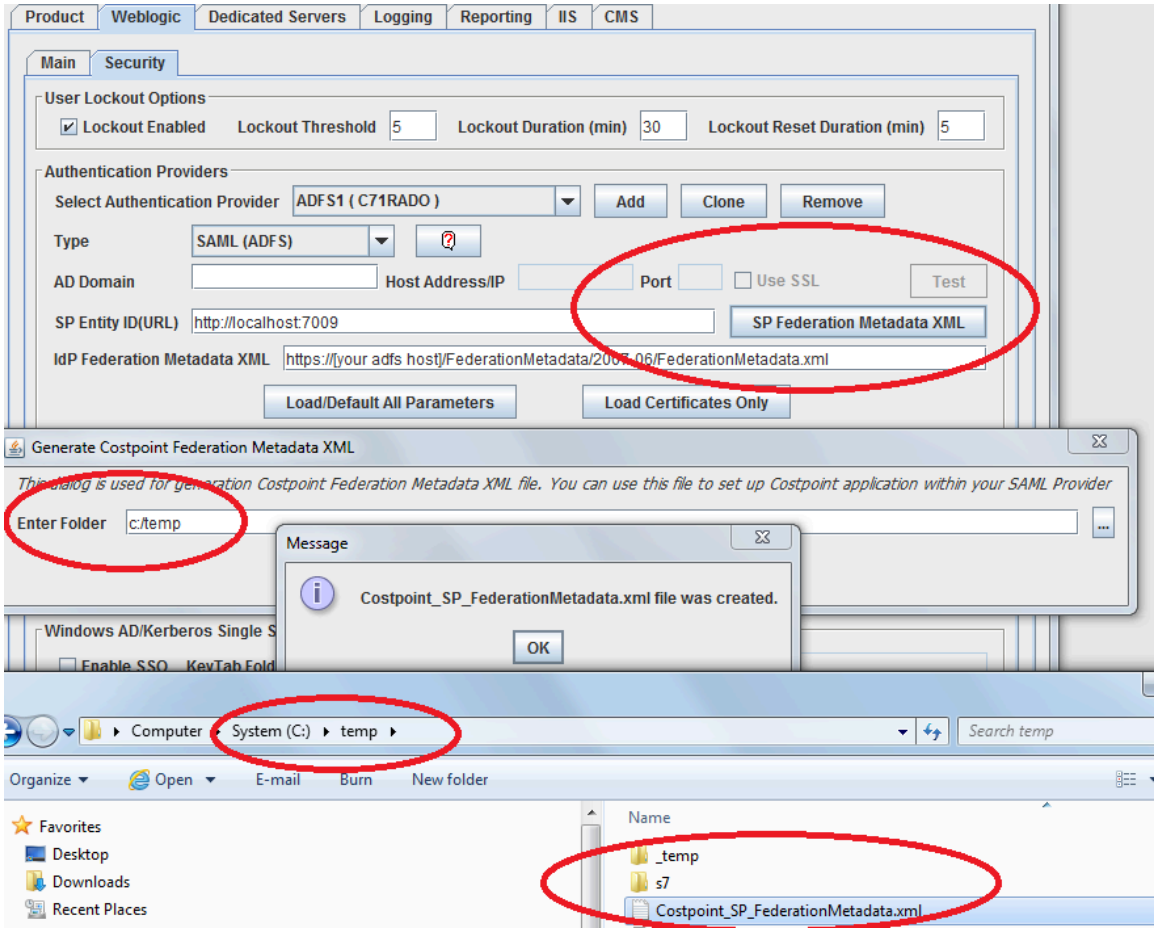
   - http://us202268:7009/FederationMetadata/2007-06/FederationMetadata.xml
   - http://myhost/CPWeb/FederationMetadata/2007-06/FederationMetadata.xml

   This URL is public. You don't have to be logged in into Costpoint to download FederationMetadata.xml.




2. Generate Costpoint FederationMetadata.xml using Costpoint Configuration Utility.

   Within Costpoint Configuration Utility, go to **Weblogic »Security » Add SAML Authentication Provider** and click **SP Federation Metadata XML**. Follow the instructions to generate the Costpoint FederationMetadata.xml file.




3. Log in to Costpoint and open System Integration Account (SYMINTGR) application.

   Follow the instructions on the screen and generate the Costpoint FederationMetadata.xml file on either one of the integration tabs available (for example, ADFS, Azure or SAML (Other) integrations).

Use **Costpoint (SP) Federation Metadata XML** to register Costpoint SAML application/connection within your SAML IdP. You can either upload the Costpoint FederationMetadata.xml file or update the settings manually using your SAML IdP console.

After you have set up Costpoint SAML application/connection within your SAML IdP, you can generate or download **IdP Federation Metadata XML**. Then, having the IdP Federation Metadata XML file, you return to Costpoint Configuration Utility and complete SAML setup.

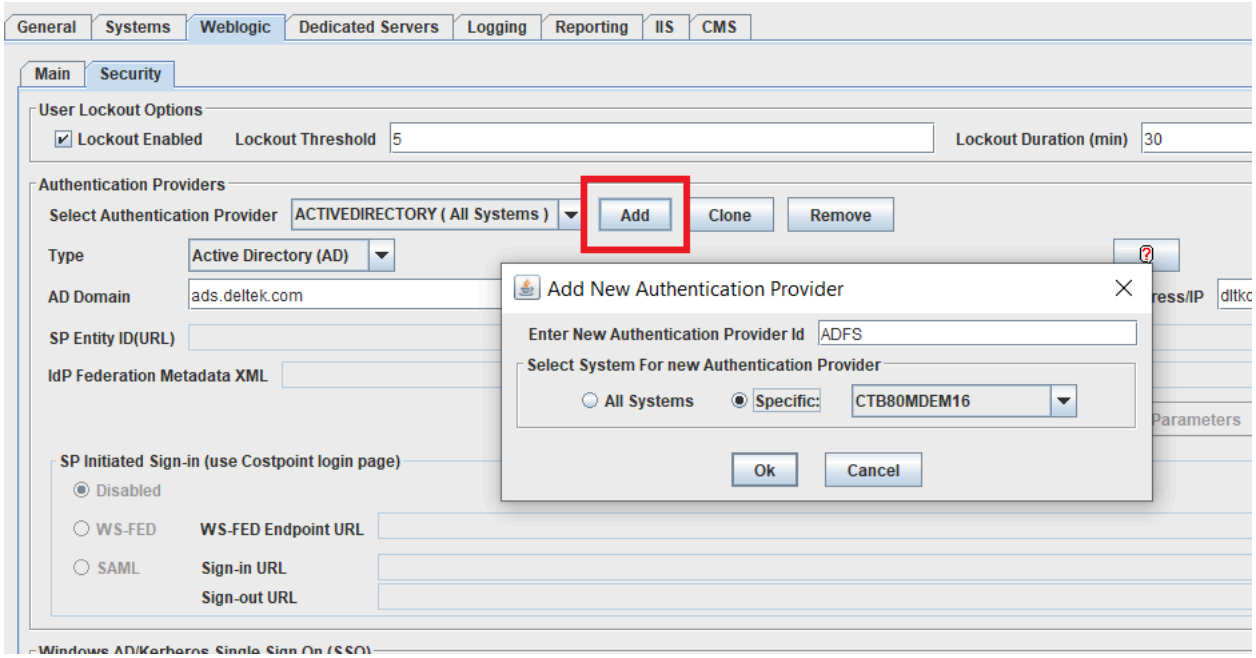
## Configure SAML Single Sign-on between Costpoint and Microsoft AD FS

1. Open Costpoint Configuration Utility and navigate to **Weblogic » Security**.

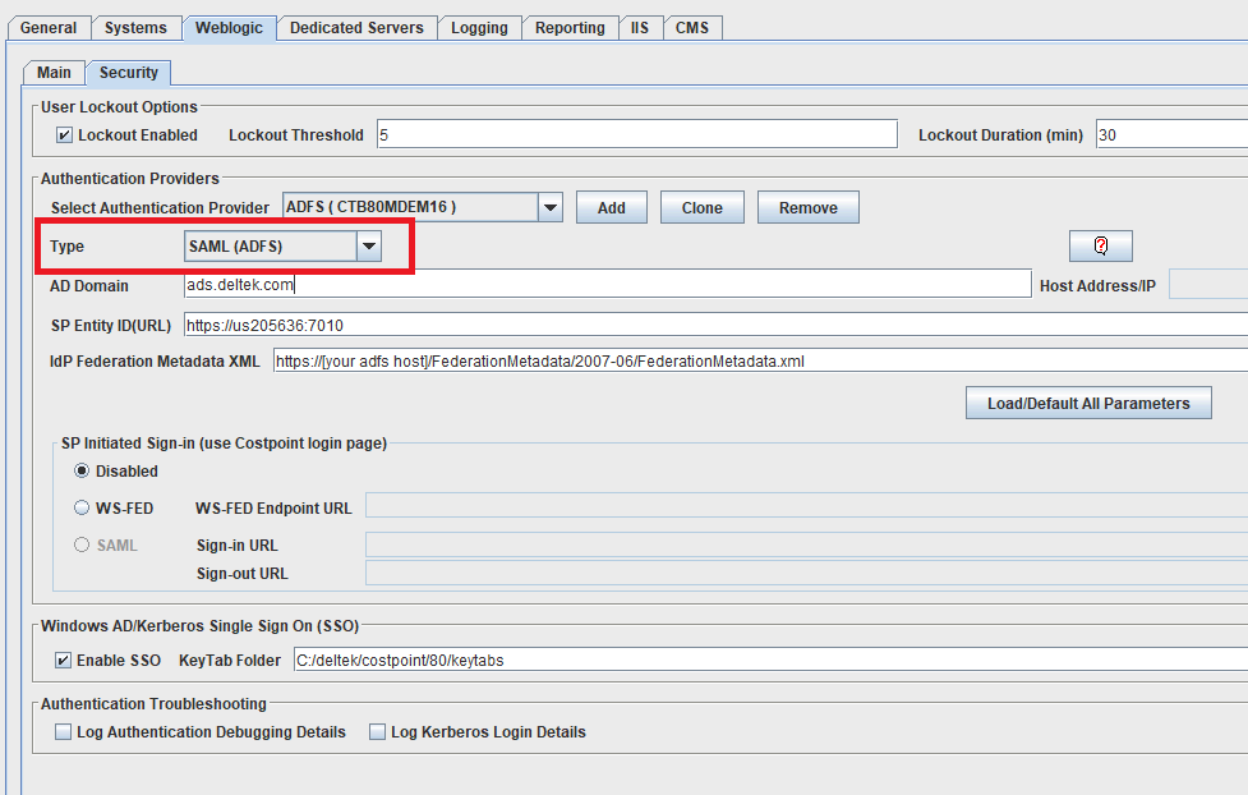
2. Click **Add** to add new (SAML) Authentication Provider.

   Provider can be added for a specific system or for all systems.

3. Enter a unique name for the Authentication Provider.




4. For the **Type**, select **SAML (ADFS)**.




5. Optional. Enter the **AD Domain** name.

   **Domain** is your company's SAML IdP (Windows AD) domain. It is used as a hint only to build the SAML user logon name during SAML IdP initiated sign-in. The system concatenates the **Domain** value with the **Active Directory ID** entered on the **Manage Users**. For example, if the **Active Directory ID** from the **Manage Users** configuration is **john.smith** and the **Domain** is **us.mycompany.com**, the system will use **john.smith@us.mycompany.com** as a default value for the SAML user account logon name on the SAML IdP login page.

   **Note:** A user can always modify the SAML user account logon name before signing in to SAML IdP.

   If the users authenticate from multiple SAML IdP domains, you can leave the **Domain** field blank and enter the fully qualified user logon name for **Active Directory ID** on the **Manage Users** screen for each user (for example, **john.smith@us.mycompany.com**, not just **john.smith**).

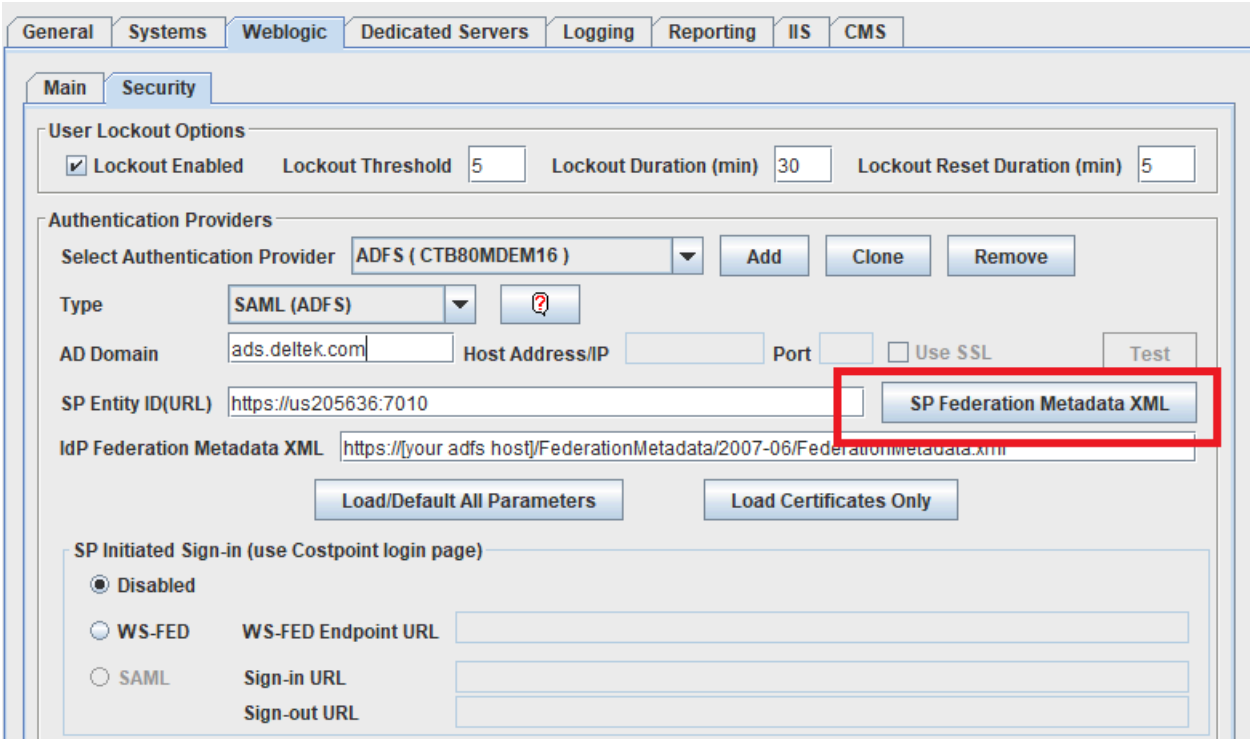
6. Enter the **SP Entity ID (URL)**.

   **SP Entity ID (URL)** is defaulted by **Enterprise App External URL**. You can change this value to use another identifier for the **SP Entity ID (URL)**. The value must conform to URL syntax and start with either http or https protocol. For example:

- https://my_adfs_test_system1
- https://costpoint_system_prod
- https://costpoint_system_dev

The value is case-sensitive. It must match exactly (including the case) to the **Relying party trust identifier** in AD FS.

7. Click **SP Federation Metadata XML** and follow the instructions on the screen to generate the **Costpoint_SP_FederationMetadata.xml** file.

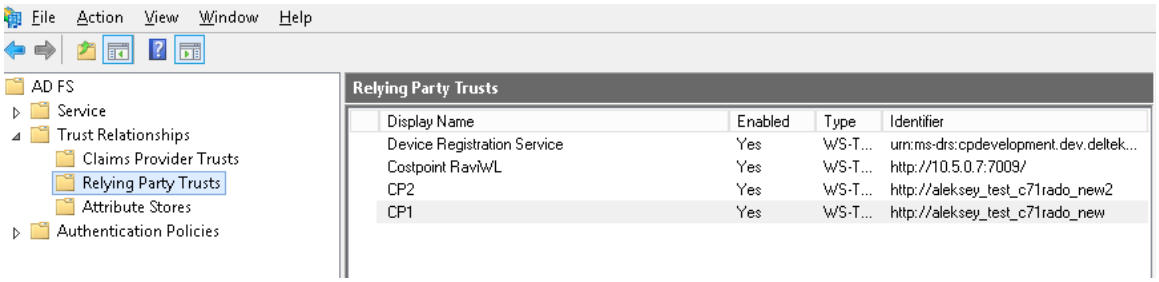



8. Click **Save** and stop making any further changes in Costpoint Configuration Utility for now.

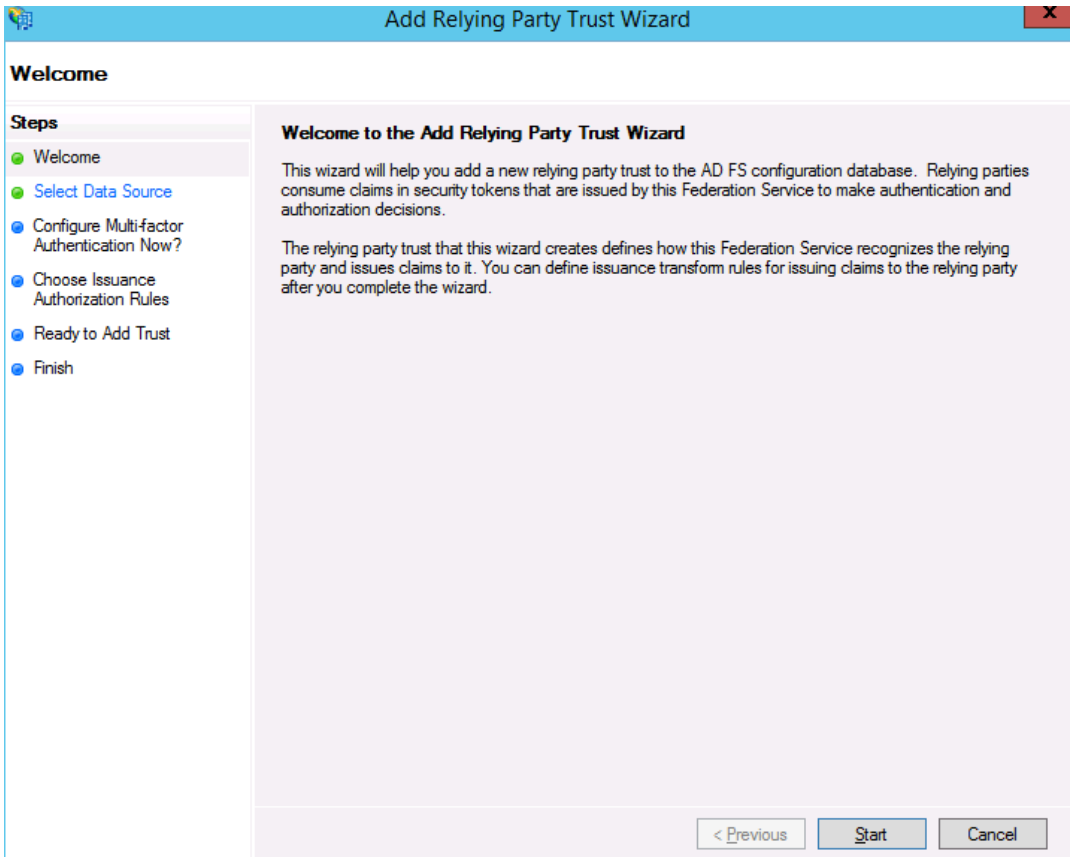
   Navigate to your AD FS host and complete the SAML configuration on the AD FS side. Then you will return to Costpoint Configuration Utility and finish the original setup.

9. On the AD FS host, open the AD FS Management tool.

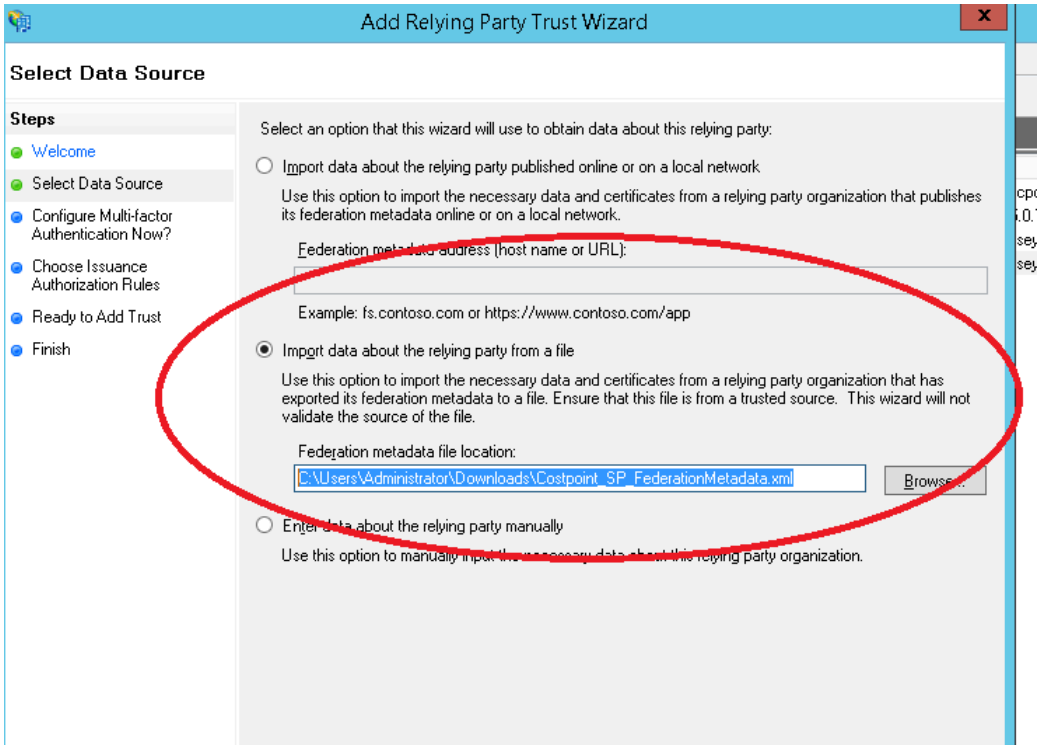
10. Select **Relying Party Trusts** and click **Add Relying Party Trust.**



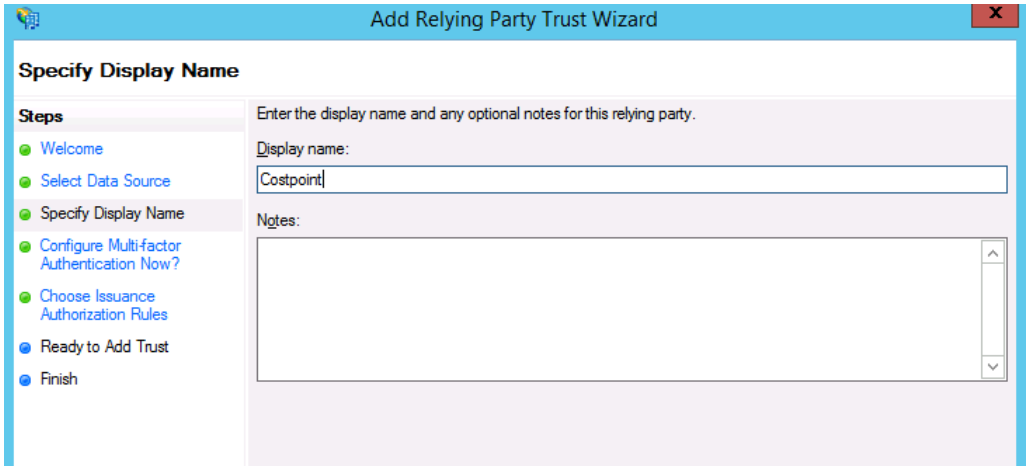

11. On the Welcome page of the Add Relying Party Trust Wizard, click **Start**.



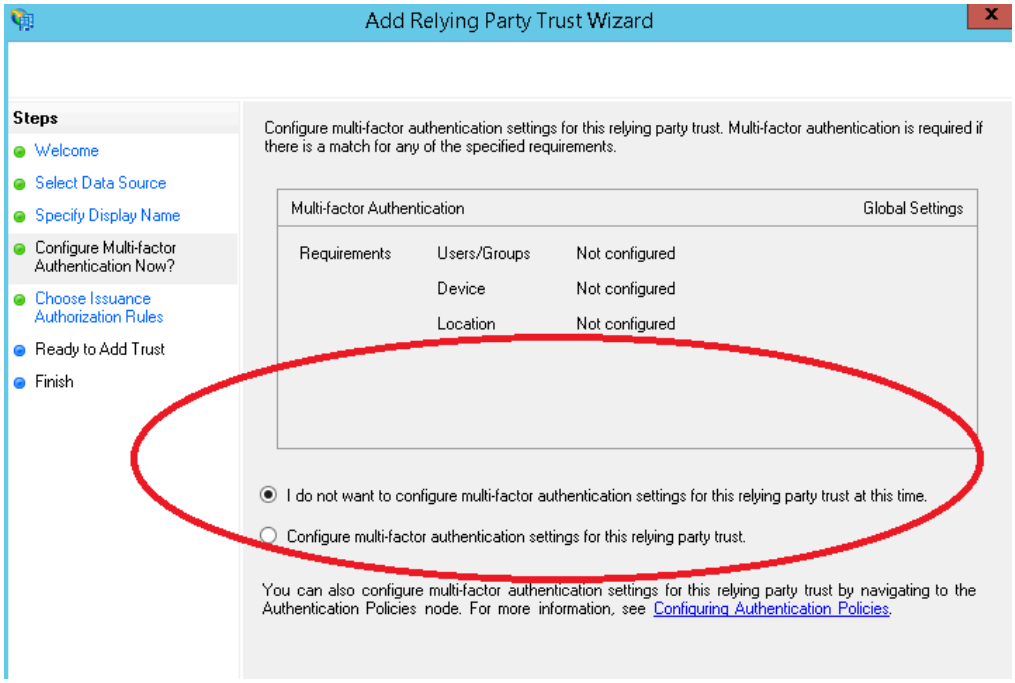

12. On the Select Data Source page, select **Import data about the relying party from a file**, point to the **Costpoint_SP_FederationMetadata.xml** file that you generated earlier using Costpoint Configuration Utility, and click **Next**.



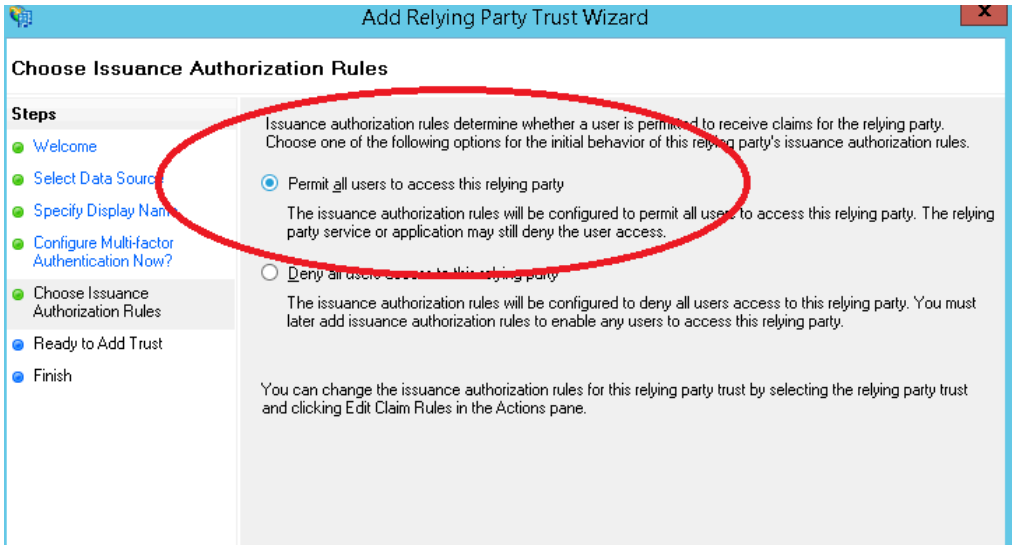

13. On the Specify Display Name page, enter **Costpoint** for the relying party **Display name**, and click **Next**.



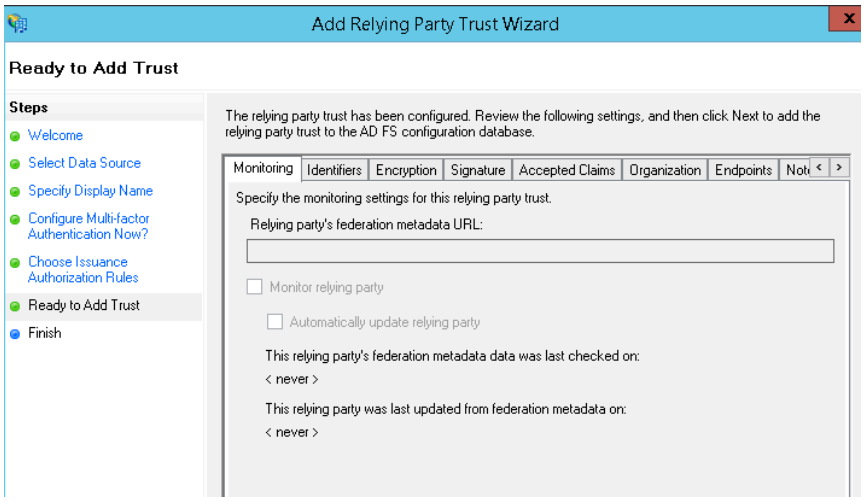

14. On the Configure Multi-factor Authentication Now page, accept the default selection for **Multifactor Authentication**, and click **Next**.



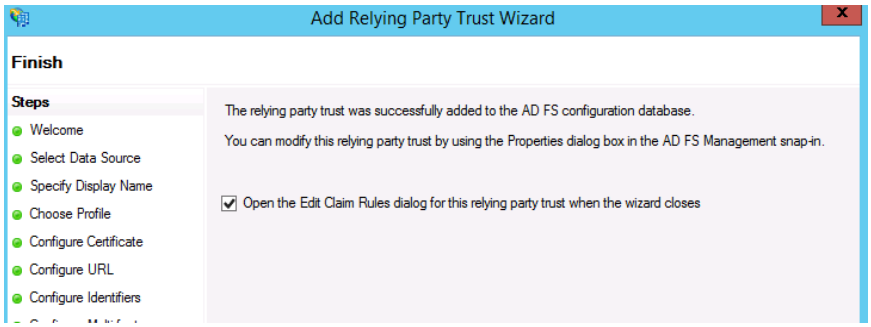

15. On the Choose Issuance Authorization Rules page, accept the default selection of **Permit all users to access this relying party**, and click **Next**.




16. On the Ready to Add Trust page, click **Next**.

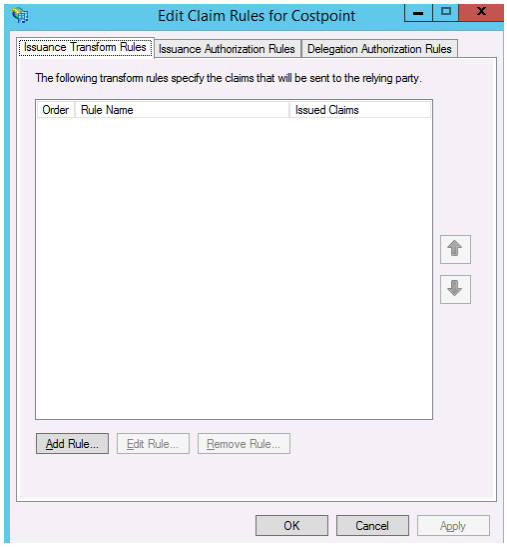



17. On the Finish page, ensure that the **Open the Edit Claim Rules for this relying party** check box is selected, and click **Close**.

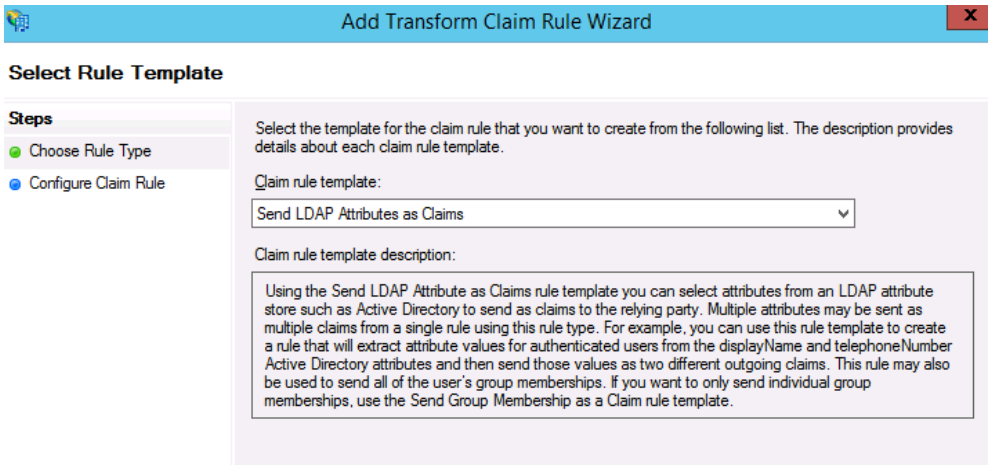



The next steps explain how to add an AD FS claim rule that will allow Costpoint to retrieve the group membership information from AD FS AD and synchronize this information with the Costpoint user groups data.

a. On the Edit Claim Rules for Costpoint dialog box, click **Add Rule**.

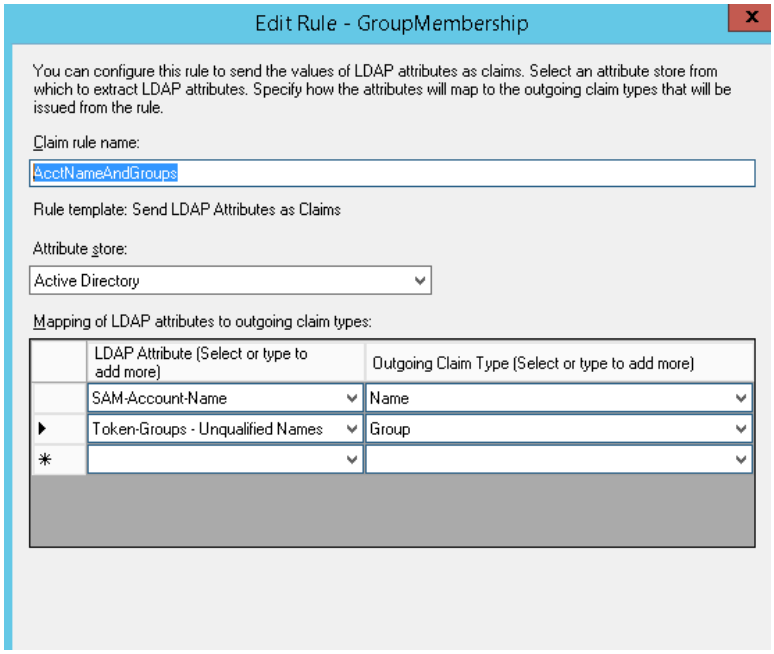



b. On the Select Rule Template page of the Add Transform Claim Rule Wizard, select **Send LDAP Attributes** in the **Claim rule template** drop-down list, and click **Next**.




c. On the Configure Rule page, perform the following:

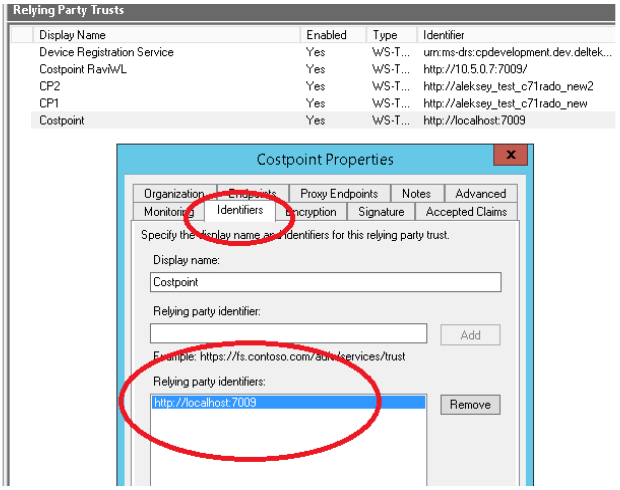
- **Claim rule name**: Enter **AcctNameAndGroups**.
- **Attribute store**: Select **Active Directory** from the drop-down list.
- Enter two lines for Mapping of LDAP attributes to outgoing claim types:
  - **LDAP Attribute**: Select **SAM-Account-Name** from the drop-down list.
  - **Outgoing Claim Type**: Select **Name** from the drop-down list.
  - **LDAP Attribute**: Select **Token-Groups – Unqualified Names** from the drop-down list.
  - **Outgoing Claim Type**: Select **Group** from the drop-down list.

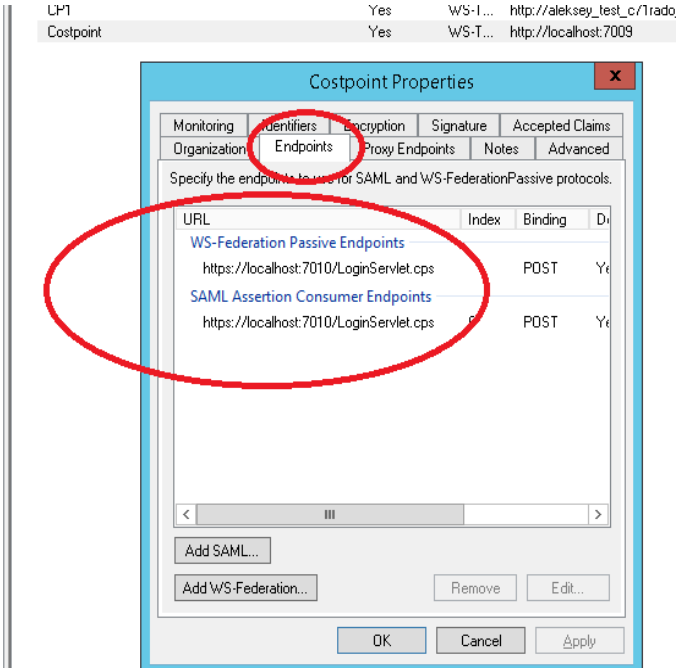



d. Click **Finish** and click **Ok**.

AD FS **Costpoint Relying Party Trust** is created and configured. Review **Relying Party Trust** settings such as Identifier and SAML Endpoint URLs for WS-Federation and SAML Assertion Consumer Service.

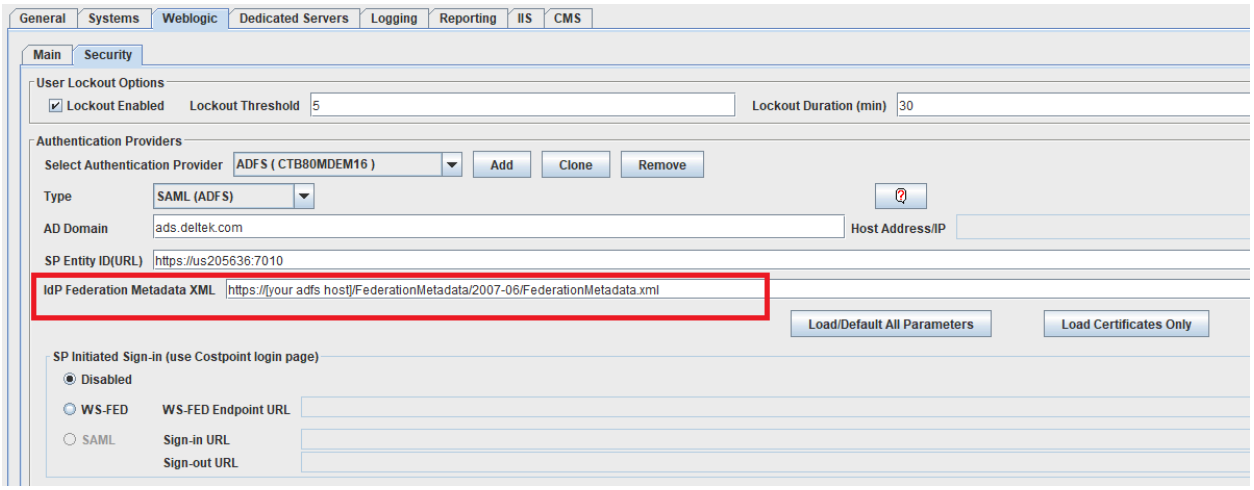
Note that you can always manually change any settings of the **Costpoint Relying Party Trust** in AD FS Management tool.





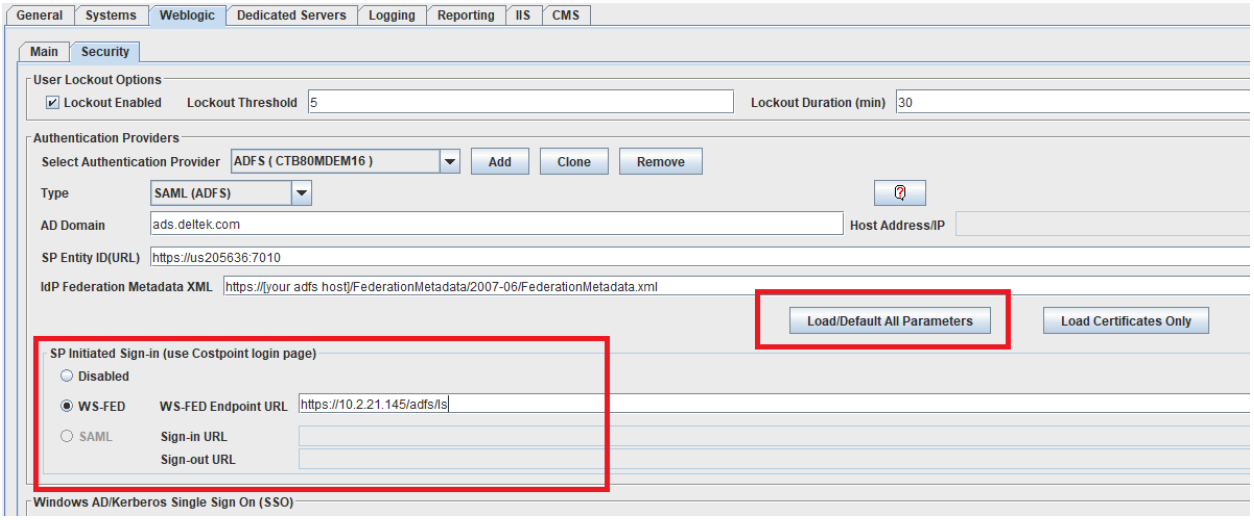

18. With AD FS **Costpoint Relying Party Trust** configured, return to Costpoint Configuration Utility and enter **IdP Federation Metadata XML**.

19. Enter the URL to your AD FS server FederationMetadata.xml.




20. Click **Load/Default All Parameters**.

This will update the **signing certificates** and **SP Initiated Sign-in** parameters. Note that you can always manually change these settings or even disable **SP Initiated Sign-in** (ability to log in via SAML Single Sign-on right from the Costpoint login page).




21. Click **Save**.

    Costpoint SAML Single Sign-on setup for Microsoft AD FS is complete. You can activate SAML SSO mode for Costpoint user accounts.

## Configure SAML Single Sign-on between Costpoint and Microsoft Azure

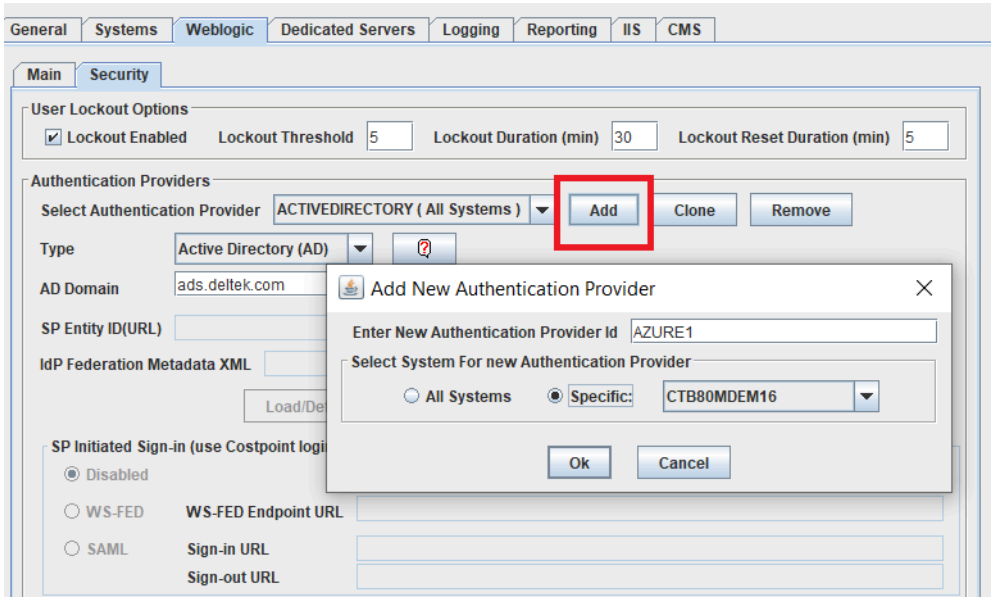
**To configure SAML Single Sign-on between Costpoint and MS Azure:**

1. Open Costpoint Configuration Utility and navigate to **WebLogic » Security.**

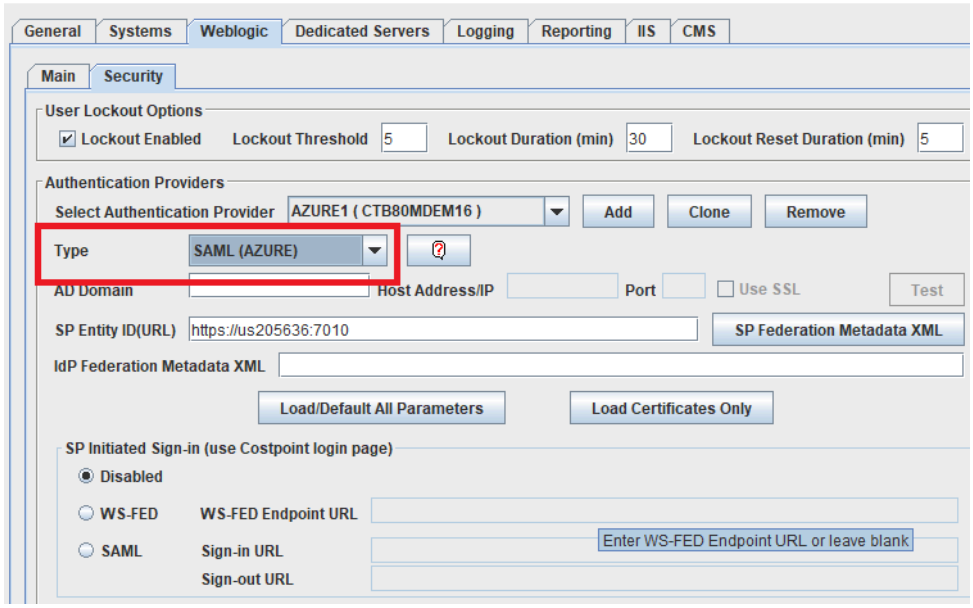
2. Click **Add** to add new (SAML) Authentication Provider.

   Provider can be added for a specific system or for all systems.

3. Enter a unique name for the Authentication Provider.




4. For the **Type**, select **SAML (AZURE)**.




5. Optional. Enter the **AD Domain** name.

   **Domain** is your company's SAML IdP (Windows AD) domain. It is used as a hint only to build the SAML user logon name during SAML IdP initiated sign-in. The system concatenates the **Domain** value with the **Active**

**Directory ID** entered on the **Manage Users**. For example, if the **Active Directory ID** from the **Manage Users** configuration is **john.smith** and the **Domain** is **us.mycompany.com**, the system will use **john.smith@us.mycompany.com** as a default value for the SAML user account logon name on the SAML IdP login page.

**Note:** A user can always modify the SAML user account logon name before signing in to SAML IdP.

If the users authenticate from multiple SAML IdP domains, you can leave the **Domain** field blank and enter the fully qualified user logon name for **Active Directory ID** on the **Manage Users** screen for each user (for example, **john.smith@us.mycompany.com**, not just **john.smith**).

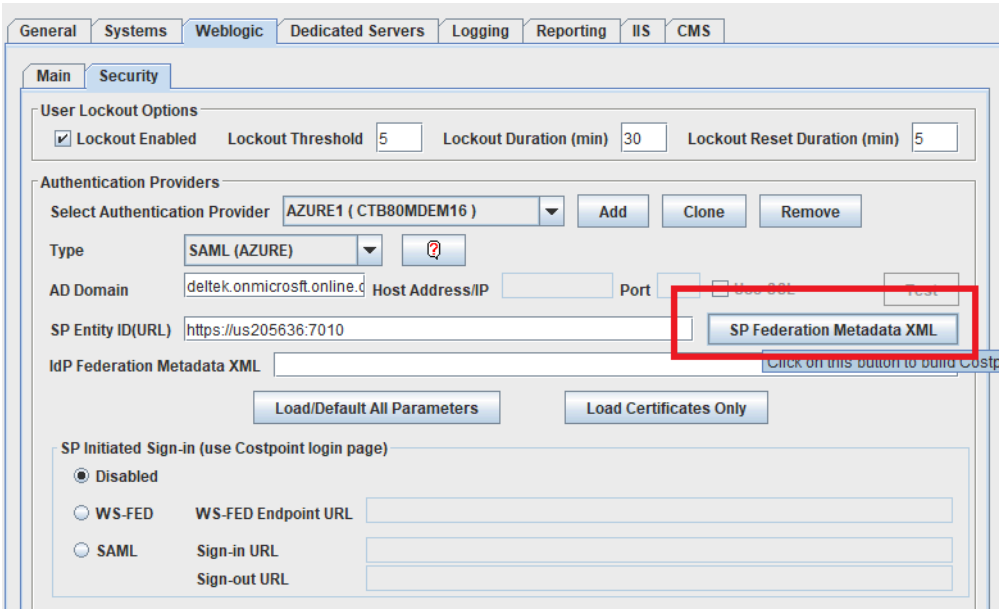
6. Enter **SP Entity ID (URL)**.

   **SP Entity ID (URL)** is defaulted by **Enterprise App External URL**. You can change this value to use another identifier for the **SP Entity ID (URL)**. The value must conform to URL syntax and start with either http or https protocol. For example:

   - https://mytestsystem1
   - https://costpoint_system_prod
   - https://costpoint_system_dev

   The value is case-sensitive. It must match exactly (including the case) to the **Identifier (Entity ID)** in Azure.

7. Click **SP Federation Metadata XML** and follow the instructions on the screen to generate the **Costpoint_SP_FederationMetadata.xml** file.

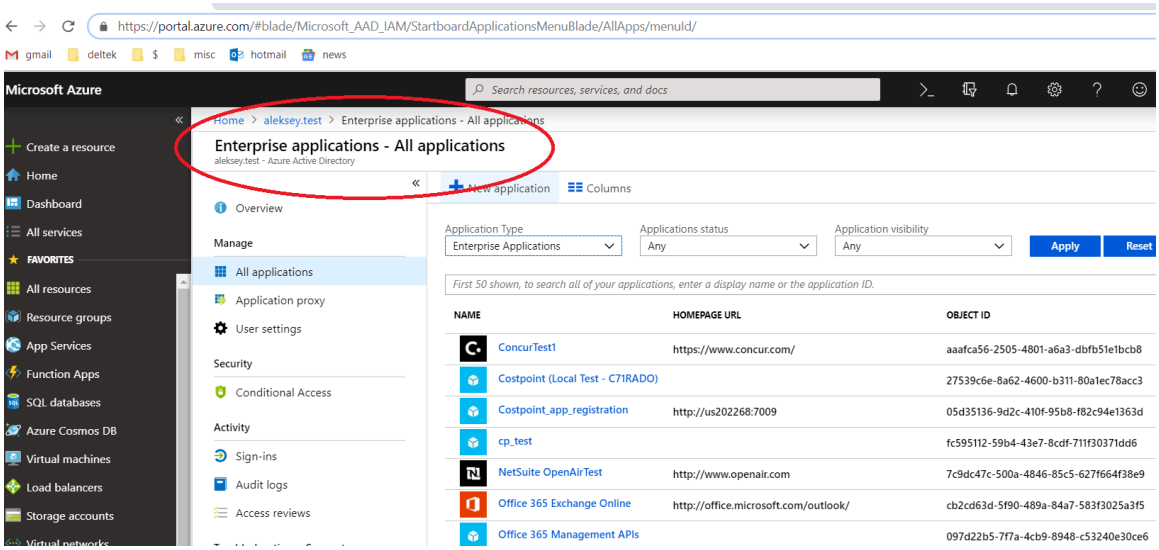


8. Click **Save** and stop making any further changes in Costpoint Configuration Utility for now.

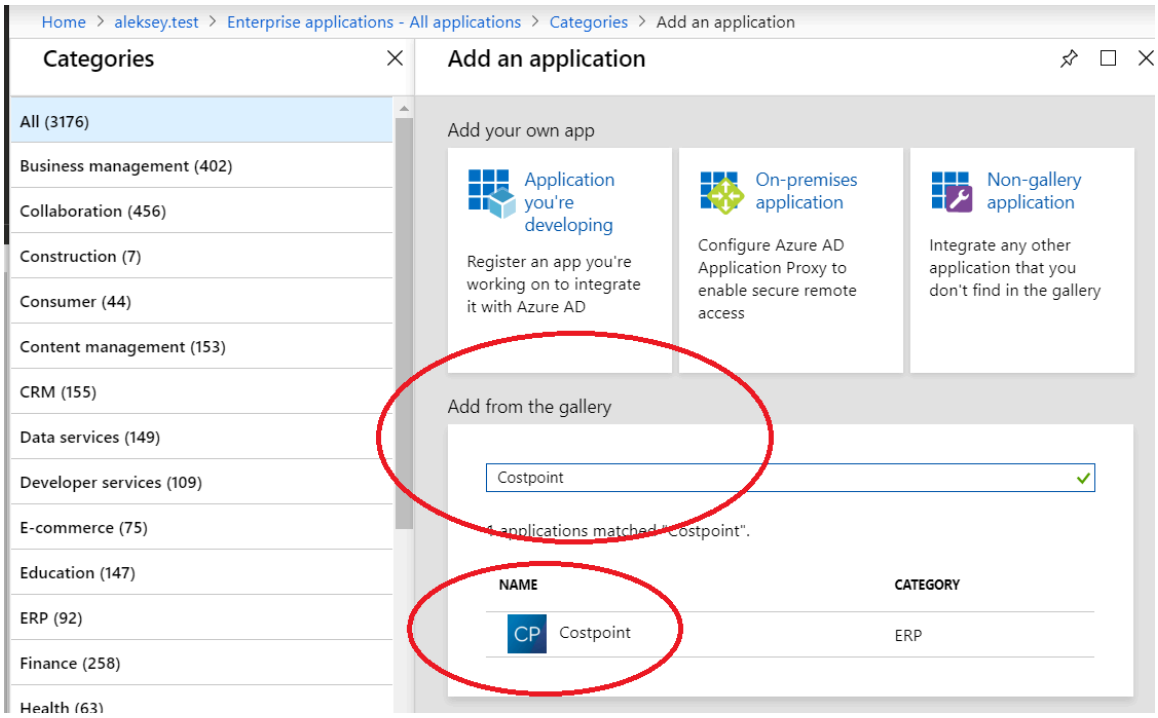
   You have to navigate to the Microsoft Azure Admin Console and complete the SAML configuration on the Azure side. Then you will return to Costpoint Configuration Utility and finish the original setup.

9. Open the Microsoft Azure Admin Console using <https://portal.azure.com>.

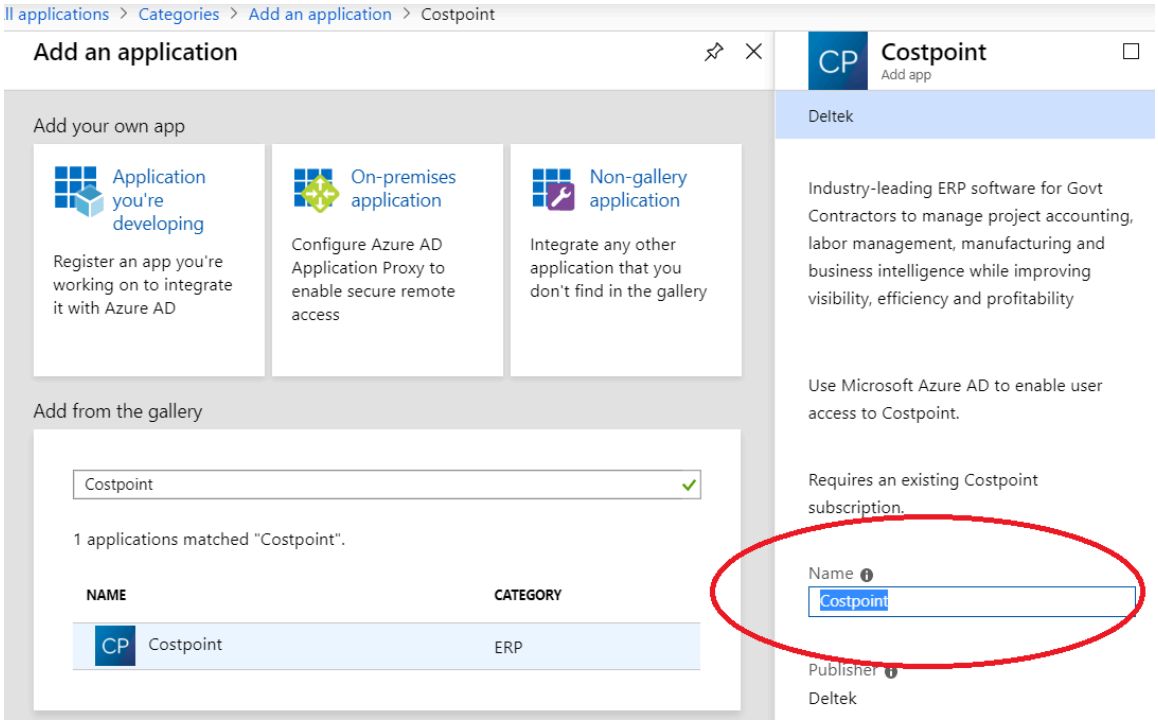
10. Navigate to **Azure Active Directory » Enterprise Applications » All Applications**.



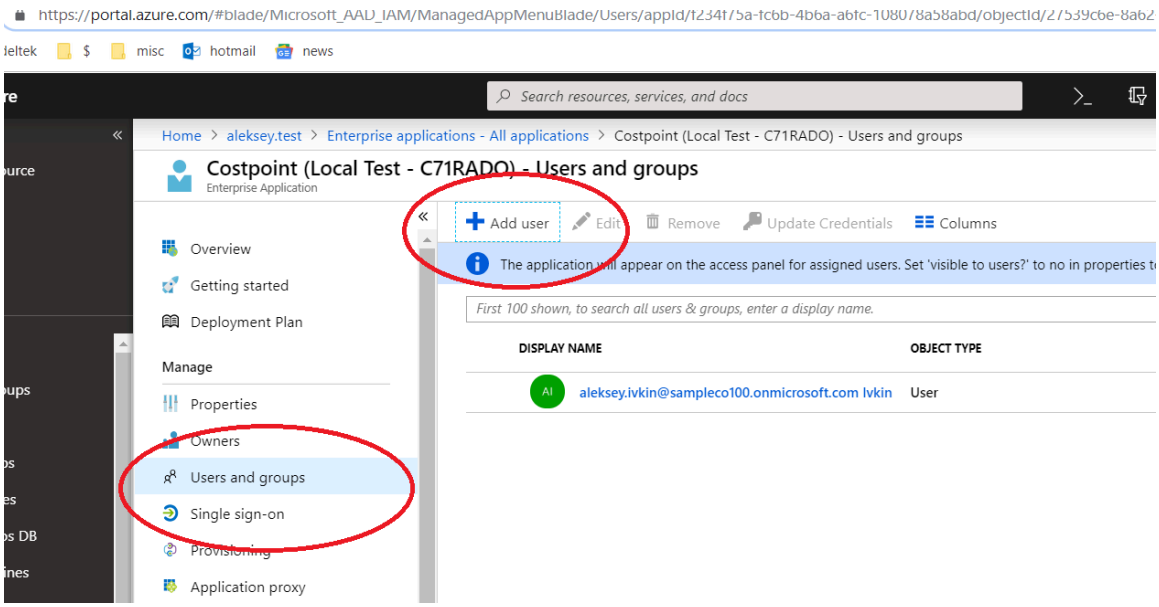

11. Click **+ New Application**, select the **Add from the gallery** option, and type **Costpoint**.



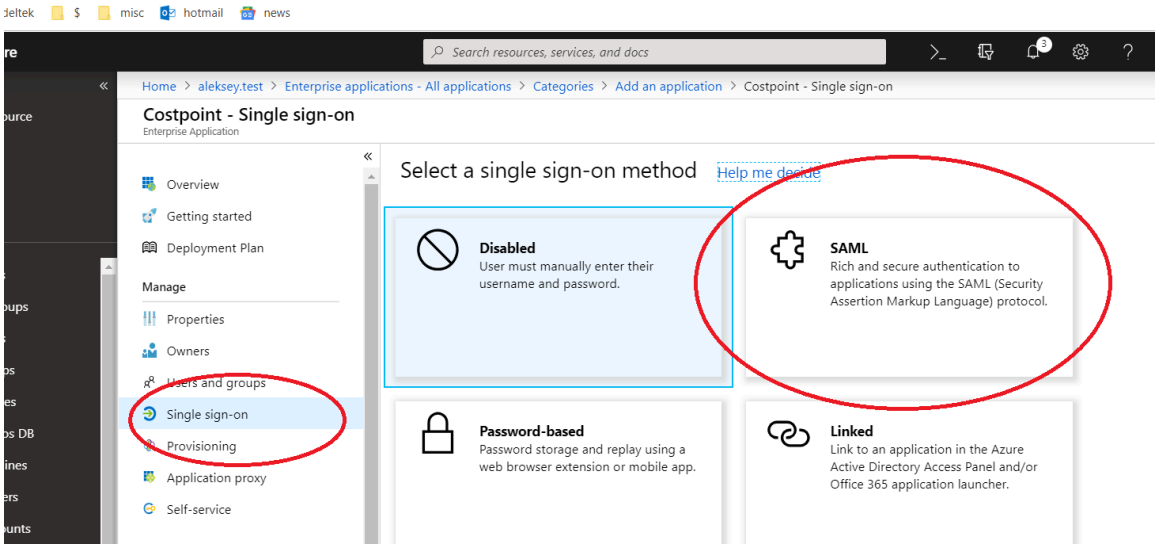

12. Click the **Costpoint** gallery template published by **Deltek**, accept default name **Costpoint** in the **Name** field, and click **Add**.



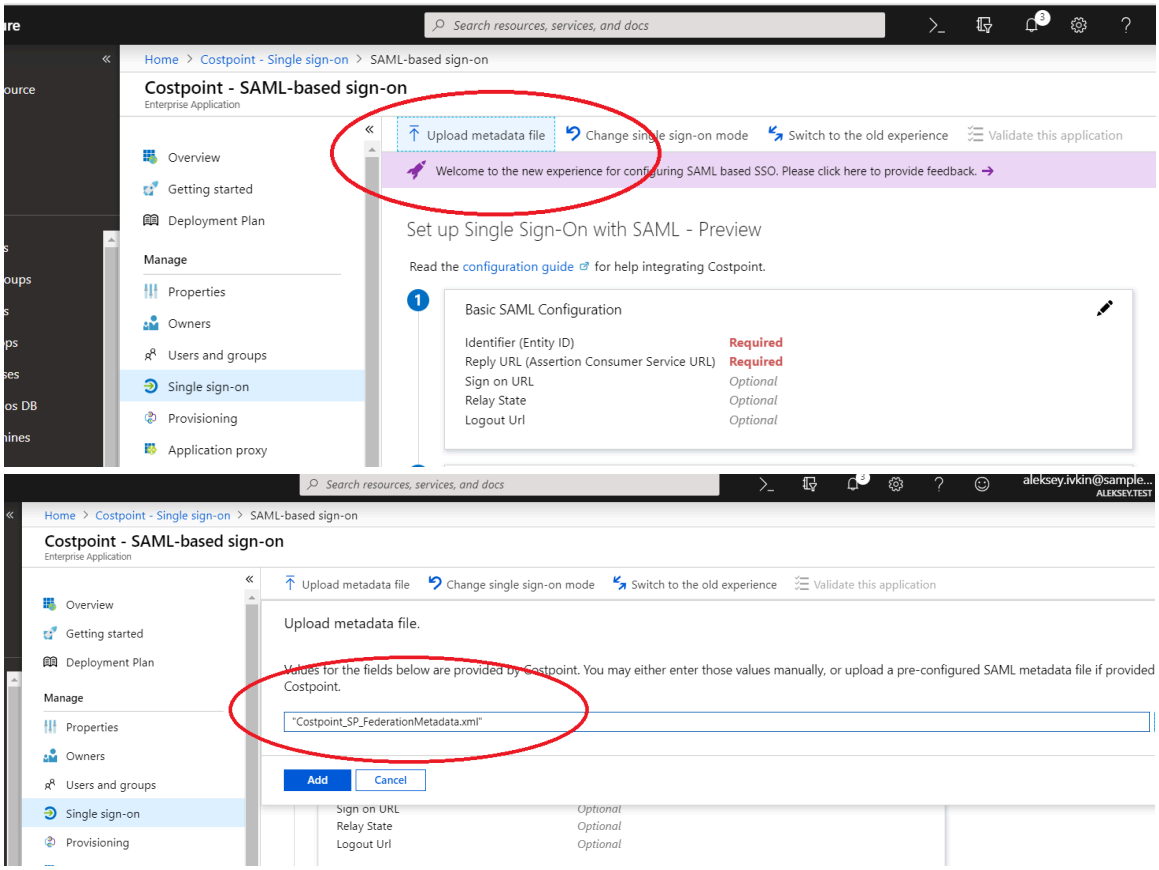
13. Click **Assign a user for testing**, or go to **Costpoint » Users and groups** on the left pane and click **Select** and **Assign** to select and assign users and/or user groups to have access to Costpoint.




14. Click **Configure single sign-on**, or go to **Costpoint » Single sign-on** on the left pane and click on **SAML** on the right.

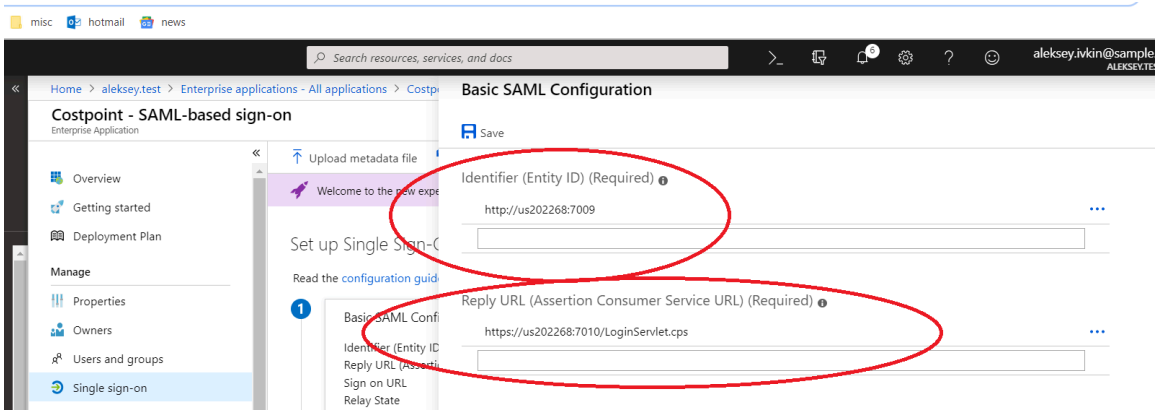


15. Click **Upload metadata file**, select the **Costpoint_SP_FederationMetadata.xml** file that you generated earlier using Costpoint Configuration Utility, and click **Add.**

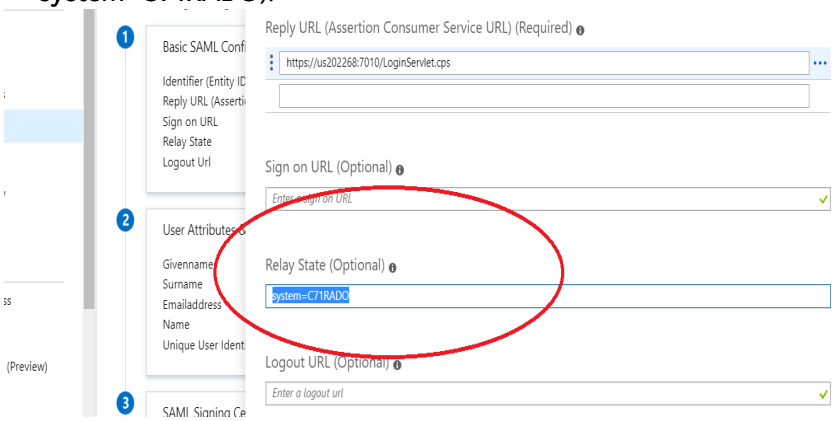



16. It will populate all The SAML required fields populate based on values from the **Costpoint_SP_FederationMetadata.xml** file.

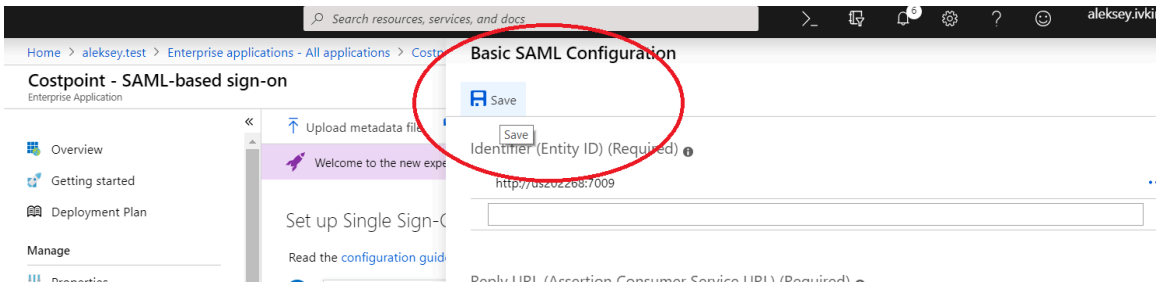
    You can always correct these values manually if needed.



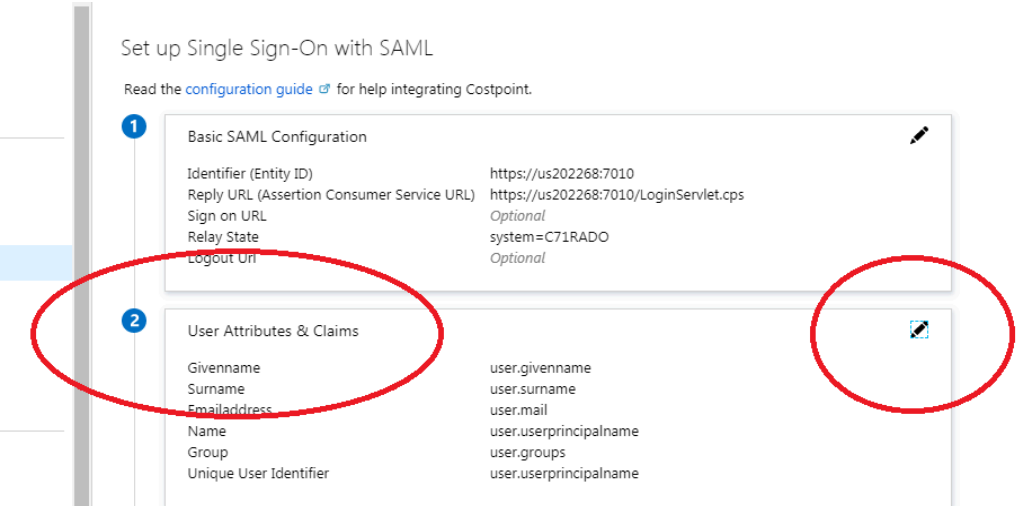

- **Identifier (Entity ID)**: The value must be unique across all applications registered within Azure. It is case-sensitive and must match exactly (including the case) to the **SP Entity ID (URL)** in Costpoint Configuration Utility.
- For **Reply URL**, enter the **HTTPS/SSL** Costpoint host/address URL ending with **/LoginServlet.cps**. This URL will be used by Azure to send the SAML token back to Costpoint.
- For **Relay State**, enter the Costpoint login system name as **system=<your system name>** (for example, **system=C71RADO**).



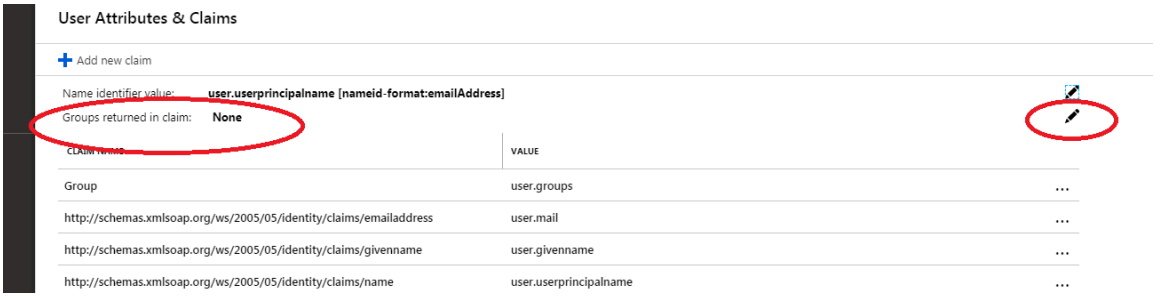

17. Leave everything else as-is on the screen, and click **Save** to save the **BasicSAML Configuration.**



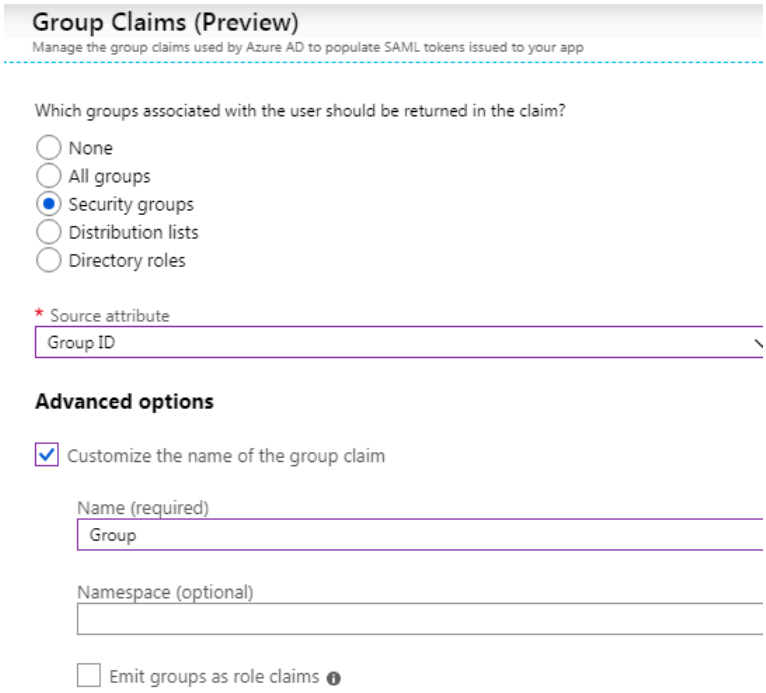
18. If you use **Manage User Groups in Active Directory** for your Costpoint users, scroll down to the **User Attributes & Claims** section and click **Edit**.




a. Click **Edit** for **Groups returned in claim**.

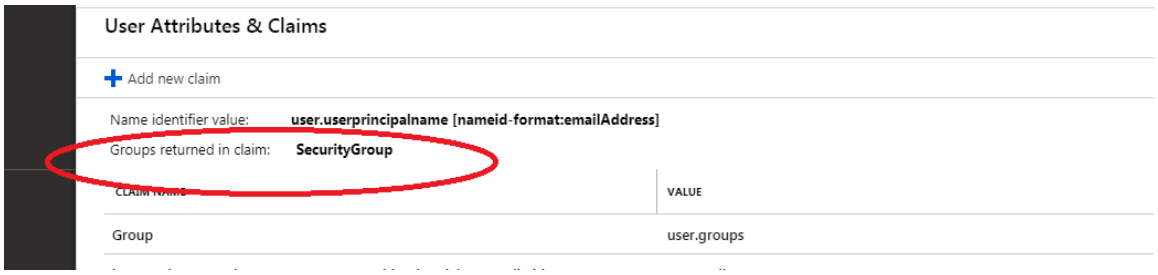



b. On the Group Claim dialog box, select **Security Groups** for **Which groups associated with the user should be returned in the claim**; choose **Group ID** or **sAMAccountName** (only if groups synchronized from an on-premises Active Directory using AAD Connect Sync 1.2.70.0 or above) as **Source Attribute**; and then select the **Customize the name of the group claim** check box under **Advanced Options** and enter **Group** in the **Name (required)** field.




c. Save your changes.

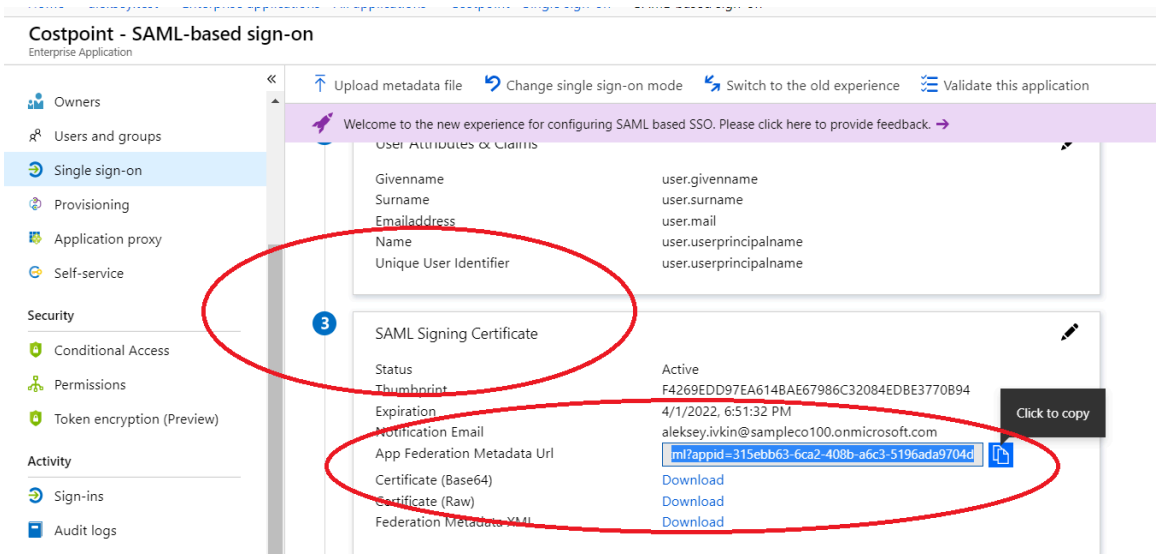
Security Groups will now be returned as part of SAML assertion.




**Attention:** For more details on how to configure group claims for applications with Azure Active Directory, refer to the following link:

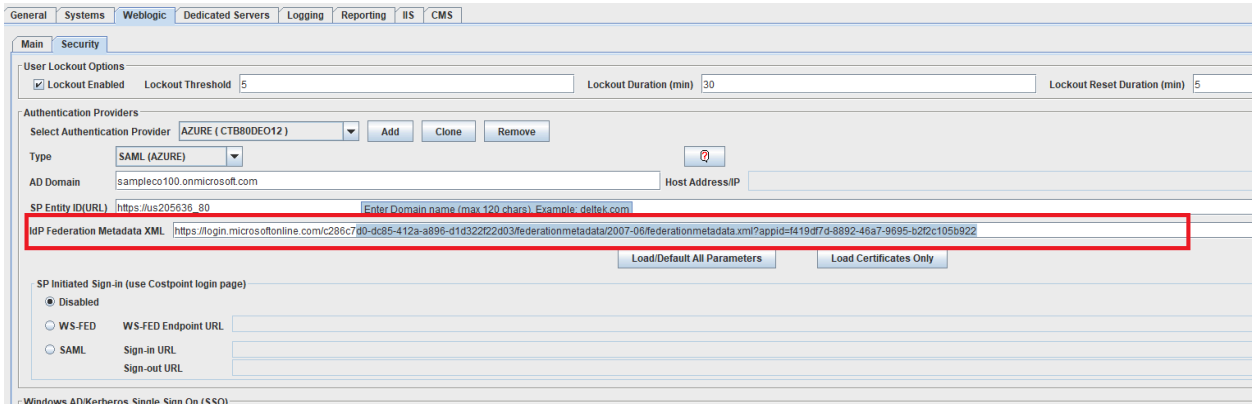
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-fed-group-claims

19. Scroll down to the **SAML Signing Certificate** section and copy the **App Federation Metadata Url**.



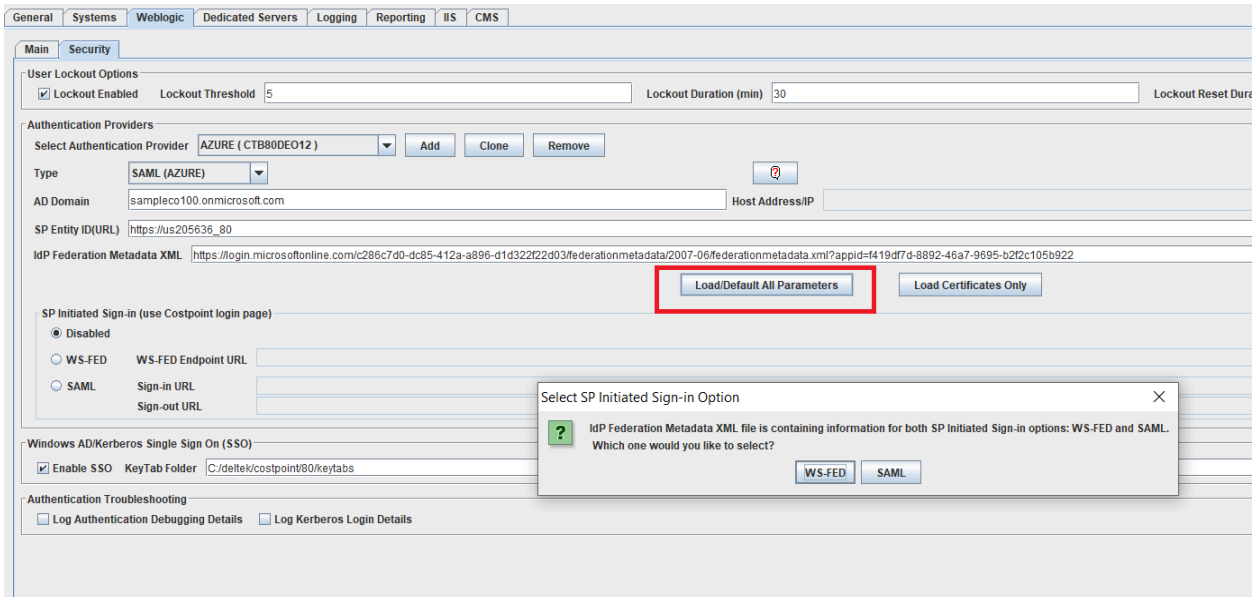

20. Return to Costpoint Configuration Utility and enter **IdP Federation Metadata XML**.

    Enter/paste the **App Federation Metadata Url** that you just copied in Azure.



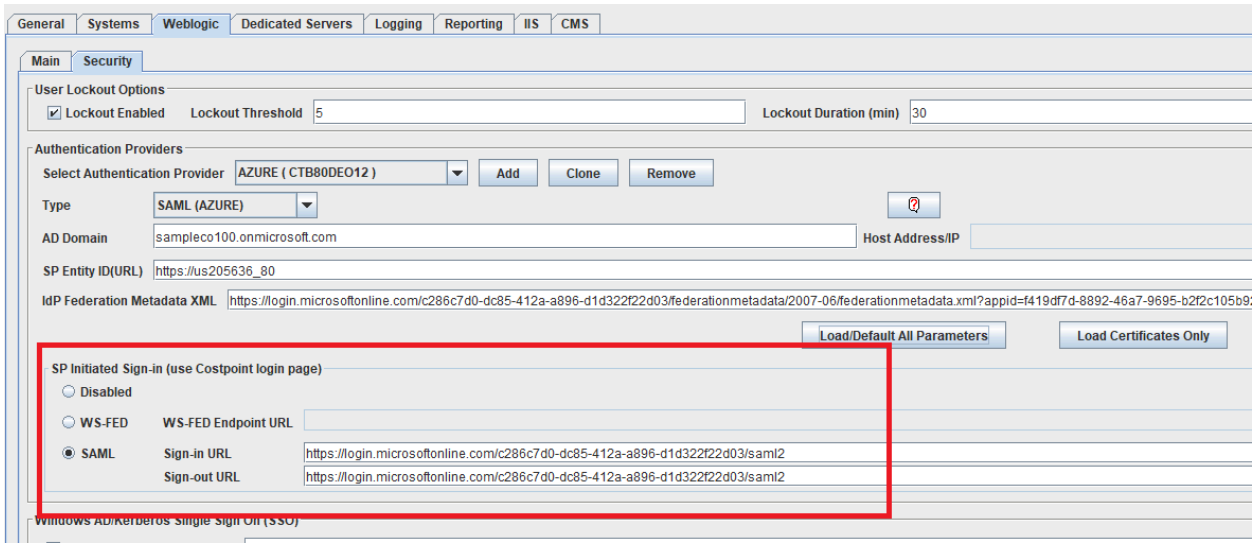

21. Click **Load/Default All Parameters**.

    This will update the **signing certificates** and **SP Initiated Sign-in** parameters. Note that you can always manually change these settings or even disable **SP Initiated Sign-in** (ability to log in via SAML Single Sign-on right from the Costpoint login page).




22. Select **SP Initiated Sign-in** method.

    You can disable it or choose between WS-FED or SAML protocols.




23. Click **Save**.

    Costpoint SAML Single Sign-on setup with Microsoft Azure is complete. You can activate SAML SSO mode for Costpoint user accounts.

## Configure SAML Single Sign-on between Costpoint and Other SAML Identity Providers

Besides using predefined SAML IdPs such as Microsoft AD FS and Microsoft Azure, SAML Single Sign-on can be configured for any other SAML IdP. For example, you can use PING-Federate, Okta, F5, and so on.

Same as with AD FS or Azure, you start with Costpoint Configuration Utility and generate the **Costpoint_SP_FederationMetadata.xml** file. Then you navigate to your SAML IdP Admin Console and register the Costpoint application/connection on the IdP's end. If your SAML IdP allows for SP metadata upload, the process becomes automatic in the same way it is with Microsoft AD FS or Azure. If SP metadata upload is not supported, you enter the Costpoint SP data manually based on the values from the **Costpoint_SP_FederationMetadata.xml** file.

Then you return to Costpoint Configuration Utility and finish the original setup.

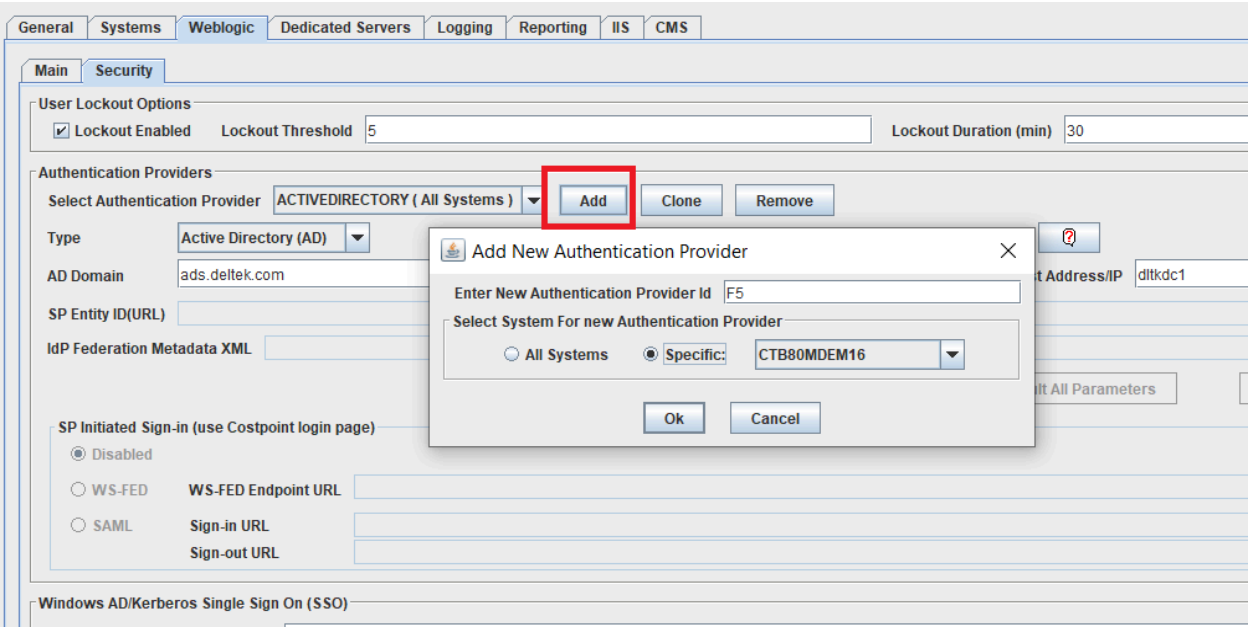
**To enable SAML Single Sign-on with SAML (Other) IdP:**

1. Open Costpoint Configuration Utility and navigate to **WebLogic » Security.**

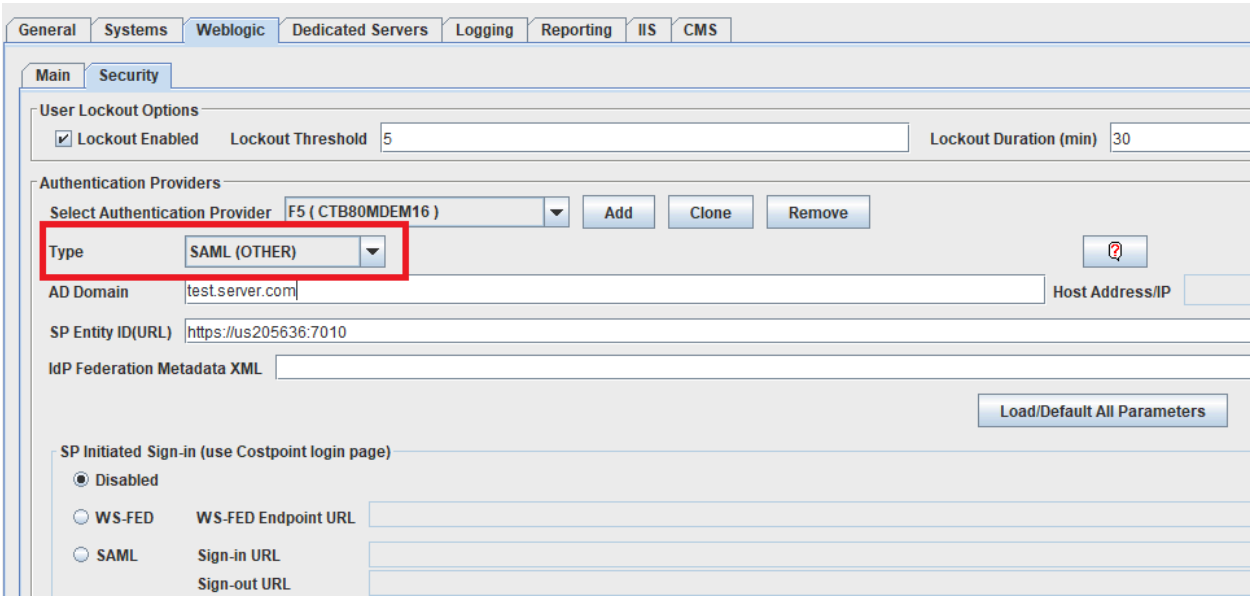
2. Click **Add** to add new (SAML) Authentication Provider.

   Provider can be added for a specific system or for all systems.

3. Enter a unique name for the Authentication Provider.



4. For the **Type**, select **SAML (OTHER)**.




5. Optional. Enter the **AD Domain** name.

   **Domain** is your company's SAML IdP (Windows AD) domain. It is used as a hint only to build the SAML user logon name during SAML IdP initiated sign-in. The system concatenates the **Domain** value with the **Active Directory ID** entered on the **Manage Users**. For example, if the **Active Directory ID** from the **Manage Users** configuration is **john.smith** and the **Domain** is **us.mycompany.com**, the system will use **john.smith@us.mycompany.com** as a default value for the SAML user account logon name on the SAML IdP login page.

   **Note:** A user can always modify the SAML user account logon name before signing in to SAML IdP.

   If the users authenticate from multiple SAML IdP domains, you can leave the **Domain** field blank and enter the fully qualified user logon name for **Active Directory ID** on the **Manage Users** screen for each user (for example, **john.smith@us.mycompany.com**, not just **john.smith**).

6. Enter **SP Entity ID (URL)**.

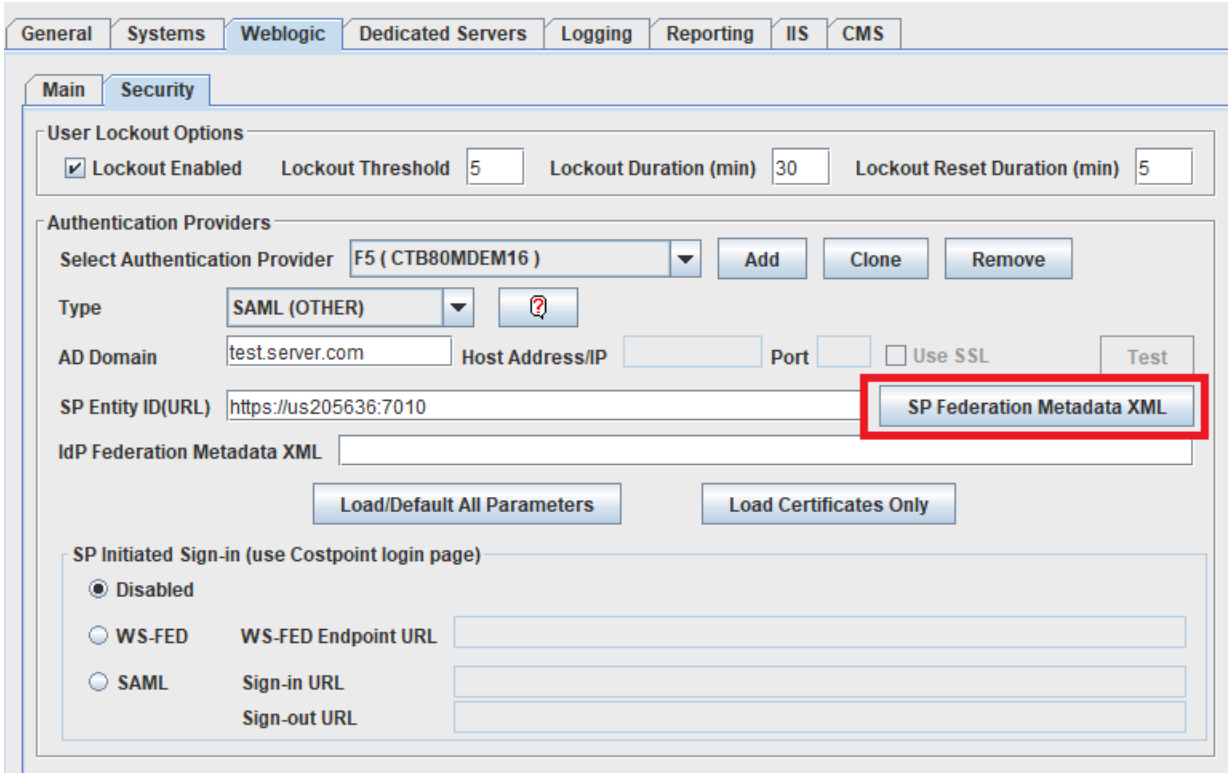
   **SP Entity ID (URL)** is defaulted by **Enterprise App External URL**. You can change this value to use another identifier for the **SP Entity ID (URL)**. The value must conform to URL syntax and start with either http or https protocol. For example:

   https://mytestsystem1, https://costpoint_system_prod, https://costpoint_system_dev.

   The value is case-sensitive. It must match exactly (including the case) to the **Identifier (SP Entity ID)** in your

SAML IdP.

7. Click **SP Federation Metadata XML**, and follow the instructions to generate the **Costpoint_SP_FederationMetadata.xml** file.




8. Click **Save** and stop making any further changes in Costpoint Configuration Utility for now.

   You have to navigate to your SAML IdP Admin Console and complete the SAML configuration on its side. Then you will return to Costpoint Configuration Utility and finish the original setup.

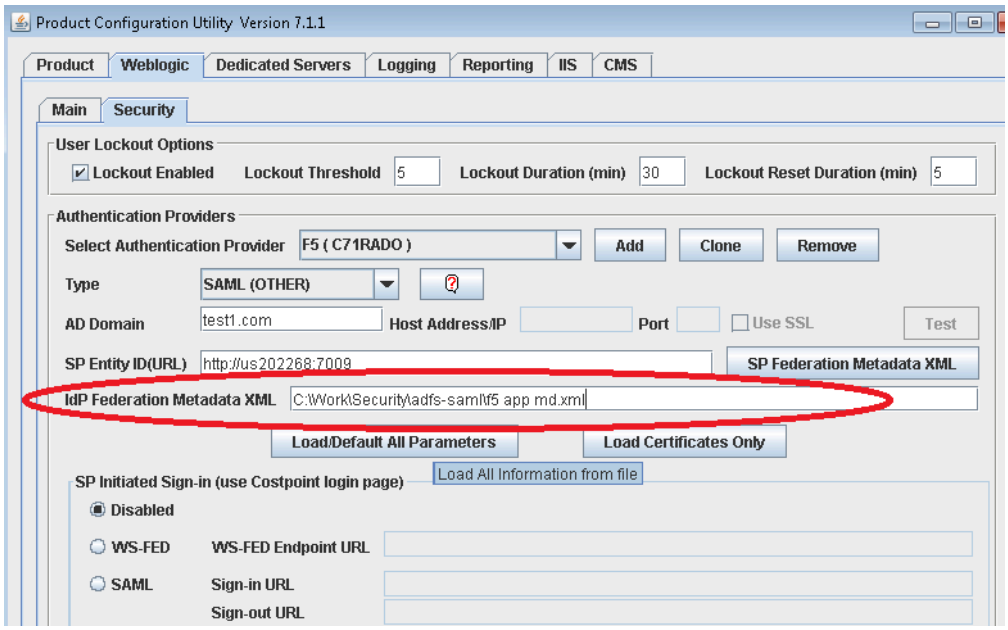
9. Keep in mind the following key things when configuring Costpoint application within your SAML IdP:

   - Costpoint application **Identifier (SP Entity ID)**: The value must be unique across all applications registered within your SAML IdP. It is case-sensitive and must match exactly (including the case) to the **SP Entity ID (URL)** in Costpoint Configuration Utility.
   - For **Reply URL (Assertion Consumer Service URL/ACS URL)**, enter the **HTTPS/SSL** Costpoint host/address URL ending with **/LoginServlet.cps**. This URL will be used by your SAML IdP to send the SAML token back to Costpoint.
   - For **Relay State**, enter the Costpoint login system name as **system=<your system name>** (for example,

system=C71RADO).

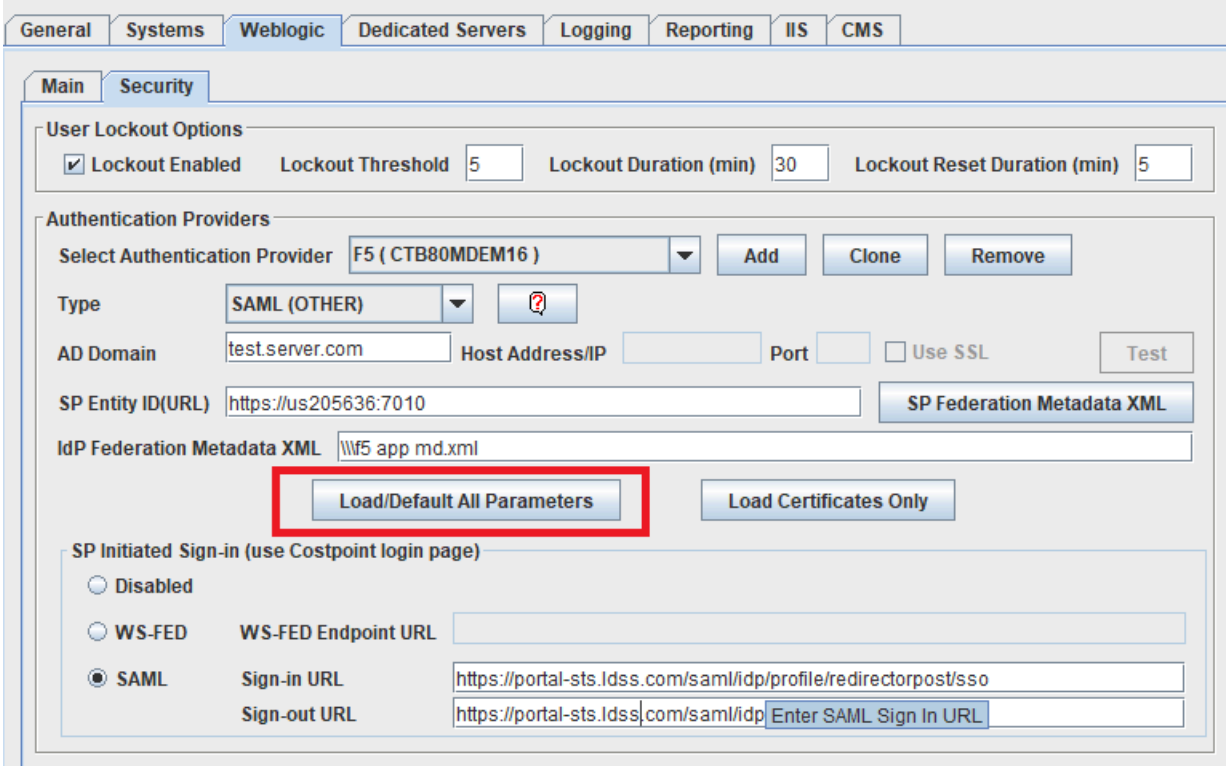
10. Return to Costpoint Configuration Utility, and enter **IdP Federation Metadata XML**.

    If your SAML IdP supports dynamic URL to IdP Federation Metadata, use this URL and enter it here. If dynamic URL is not supported, download the IdP Federation Metadata file to your local machine so that it is available and can be accessed by Costpoint Configuration Utility.



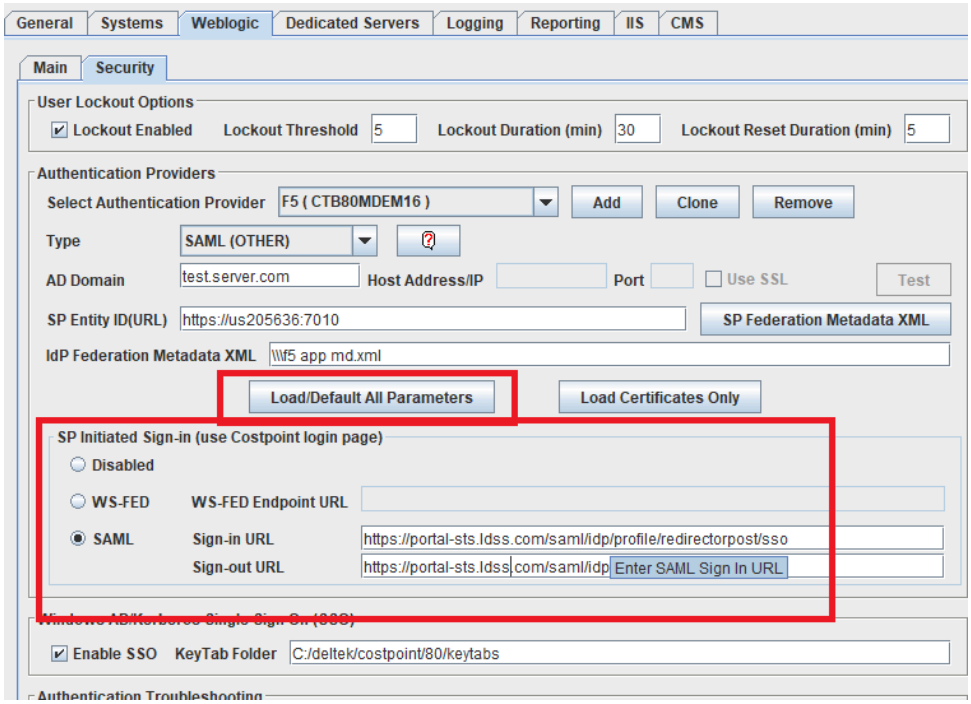

11. Click **Load/Default All Parameters**.

    This will update the **signing certificates** and **SP Initiated Sign-in** parameters. Note that you can always manually change these settings or even disable **SP Initiated Sign-in** (the ability to login via SAML Single Sign-on right from the Costpoint login page).




12. Select the **SP Initiated Sign-in** method.

    You can disable it or choose between **WS-FED** or **SAML** protocols.



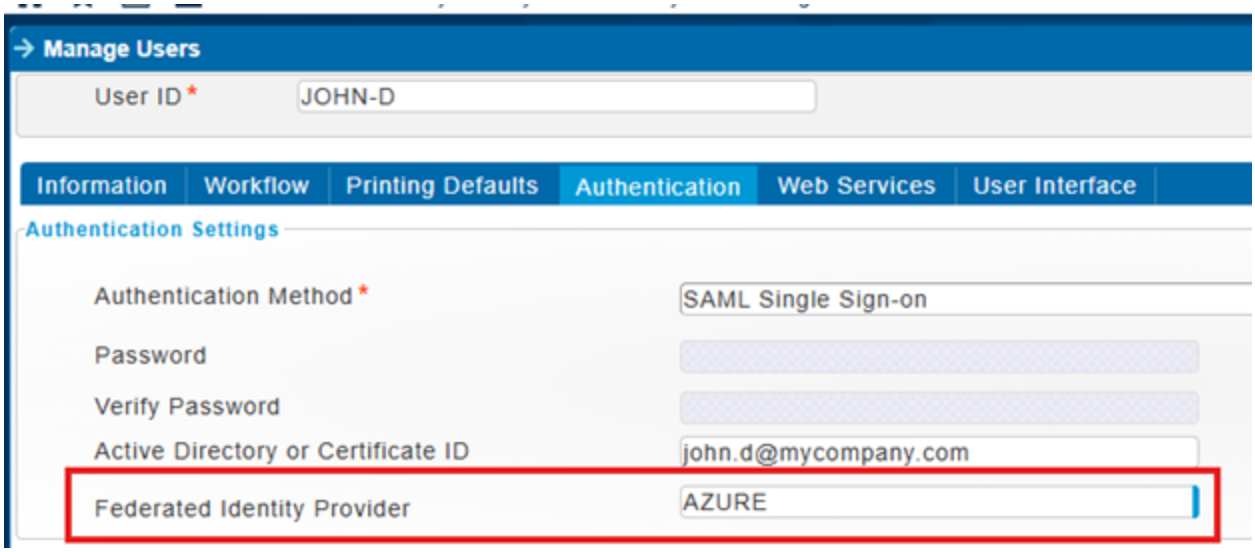

13. Click **Save**.

    Costpoint SAML Single Sign-on setup with SAML (Other) IdP is complete. You can activate SAML SSO mode for Costpoint user accounts.

## Multiple SAML Providers

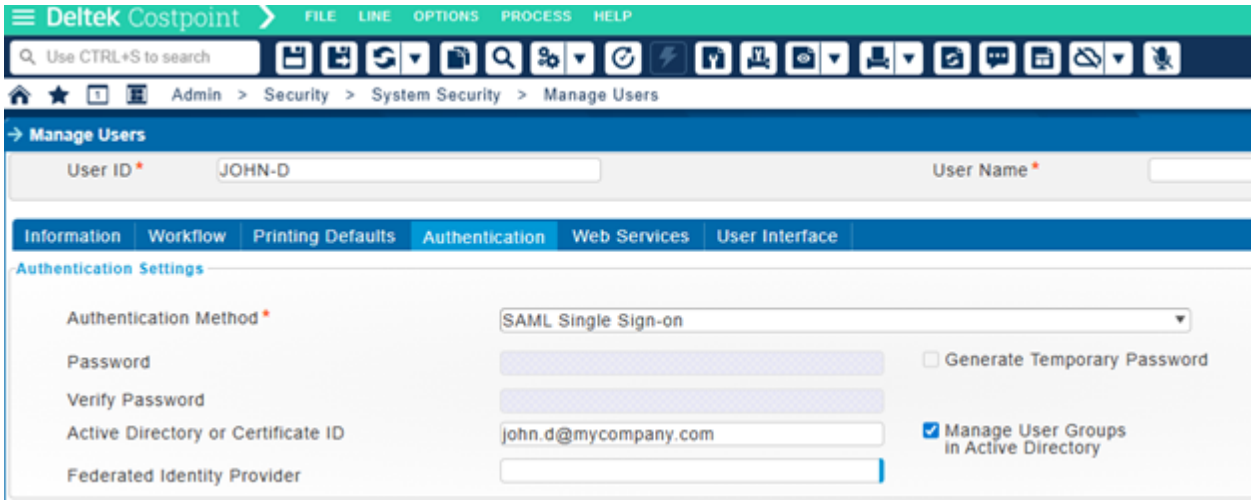
In most cases, having a single SAML provider is sufficient. However, there are situations where users from different identity providers need to authenticate to the system. Costpoint supports adding multiple SAML providers to address such requirements.

You can assign a specific SAML provider to each user account by updating the **Federated Identity Provider** field in **Administration » Security » System Security » Manage Users**. If the **Federated Identity Provider** field is left blank, the first (default) SAML provider will be used to authenticate the user.




## Activate SAML SSO Mode for Costpoint Accounts

1. Click **Administration » Security » System Security » Manage Users**.
2. Select a user.
3. Click the Authentication tab.
4. Select the **SAML Single Sign-On** authentication method to allow the user to log into Costpoint in SAML SSO mode.
5. For **Active Directory ID or Certificate ID**, enter the ID to reference the user account name within company IdP.




## SAML Assertion Validation and SAML Certificates

The SAML SSO authentication process involves these three parties:

- User
- SAML Identity Provider or IdP (Azure, AD FS, Okta, Ping)
- SAML Service provider or SP (Costpoint application)

A user makes a request to the Costpoint application. Costpoint then requests authentication from the IdP. The IdP sends a SAML assertion to Costpoint. Costpoint validates the SAML assertion. Then based on the validation results, it either grants or denies user access to Costpoint. If the user was not already logged in with the IdP, the IdP may prompt the user to authenticate before sending a SAML assertion to Costpoint.

A SAML assertion is the key element that tells Costpoint that a user is who it claims to be. SAML assertion contains all the information necessary for Costpoint to confirm user identity, including the source of the assertion, the time it was issued, and the conditions that make the assertion valid.

When Costpoint validates SAML assertion, it must perform the following steps:

1. Parse the XML document, which includes structure validation based on the supplied schema.

2. Validate the SAML assertion audience restriction, which confirms that the SAML assertion was issued specifically to Costpoint.

3. Validate the SAML assertion starting date/time and expiration time.

4. Validate the SAML assertion subject, which confirms that the user principal name from the subject matches the username from the **Active Directory ID** field on the Manage Users screen in Costpoint.

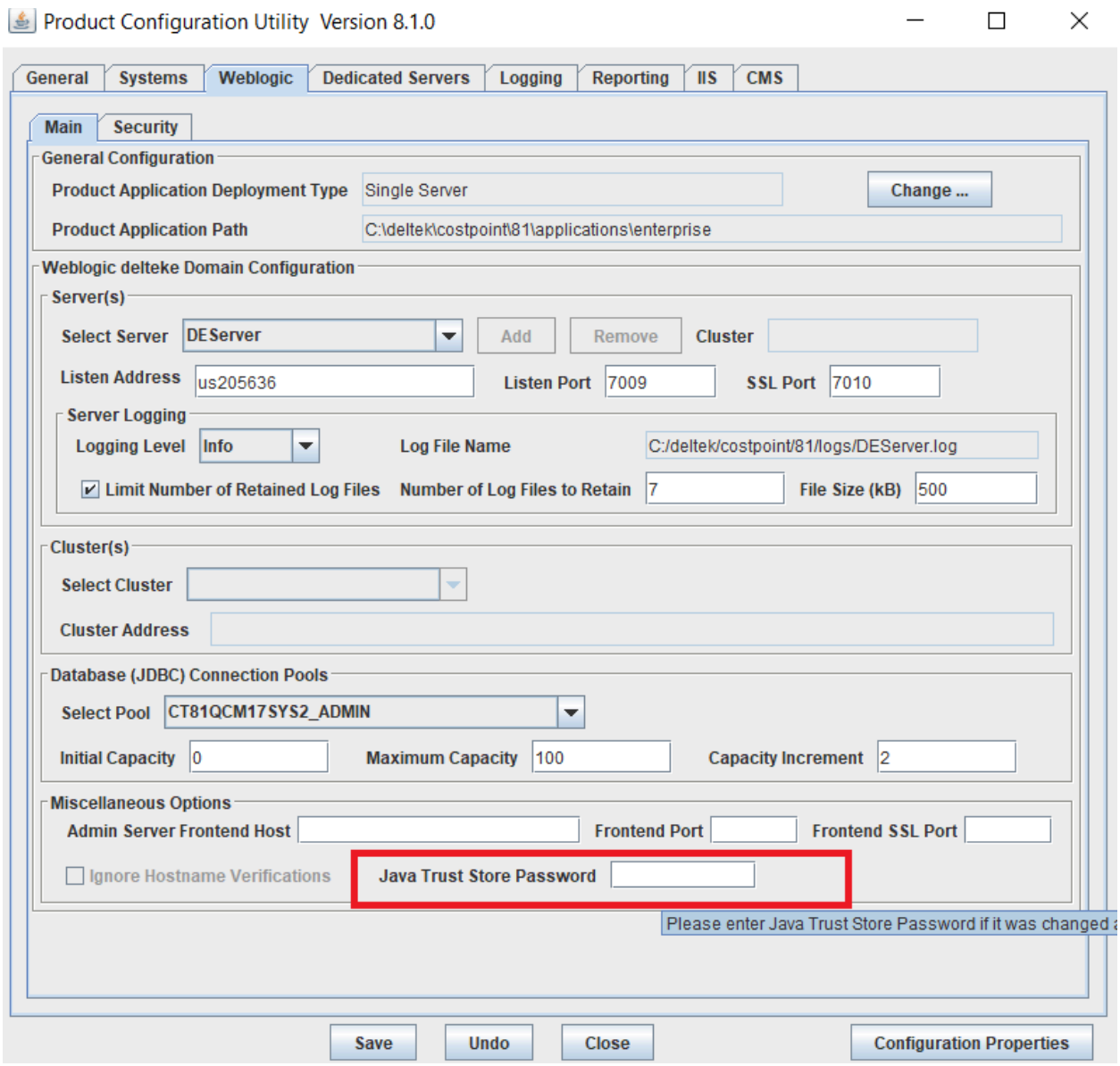
5. Validate the SAML assertion digital signature, which verifies the overall authenticity and integrity of the SAML assertion.

The successful validation of the message digital signature confirms that the message integrity, making sure that not a single bit of the message was tampered with or changed while in transit.

It also involves verifying the SAML certificate that proves the signature. Costpoint may only trust a SAML certificate that is trusted or confirmed either by the global Java certificate trust store or by the local Costpoint certificate trust store.

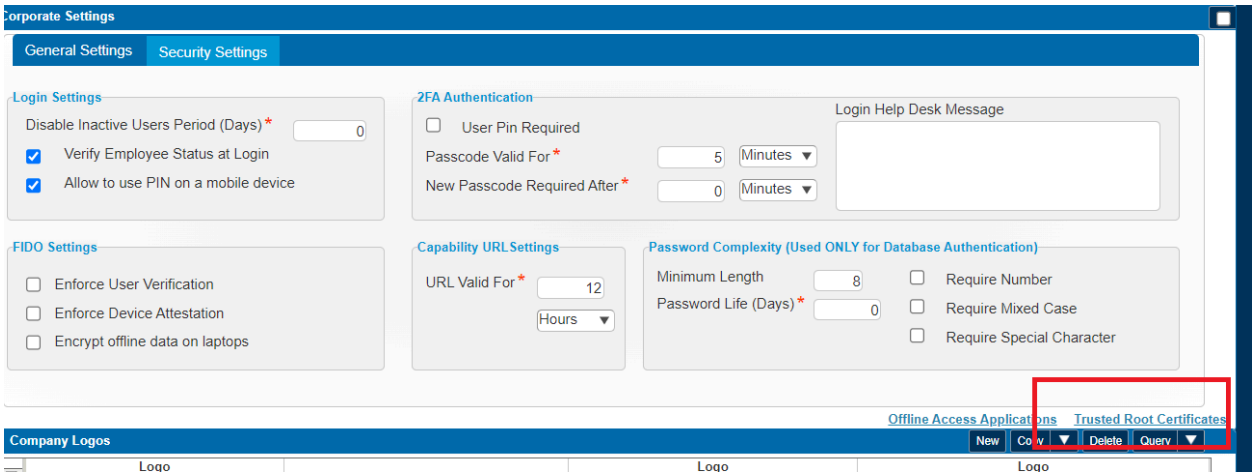
The global Java certificate trust store is part of the standard Java installation and typically contains all the well-known commercial root certificate authorities used for SAML. If for any reason you changed default password to the global Java certificate trust store (\jre\lib\security\cacerts), you must also reflect the change in Costpoint.

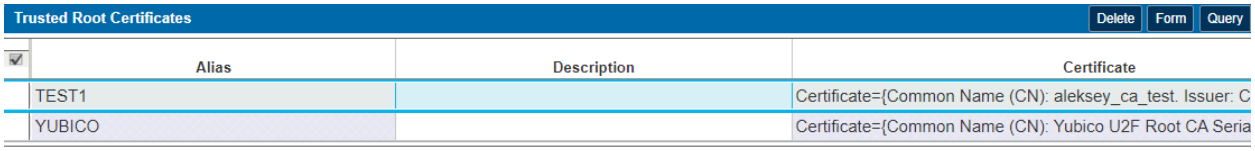
Run the Costpoint Configuration Utility and update the **Java Trust Store Password** on Weblogic » Main tab.

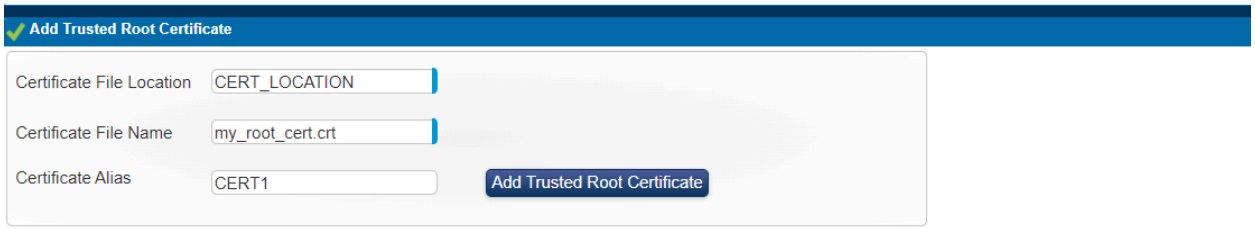



In case your IdP SAML certificate is not trusted by the global Java certificate trust store and you receive “a certificate cannot be trusted” error during SAML login, you can add your root certificate into the Costpoint local certificates trust store and, therefore, make your SAML certificate trusted.

You can update the Costpoint local certificates trust store and add your root certificate via **Costpoint » Configure System Settings » Corporate Settings » Trusted Root Certificates » Add Trusted Root Certificate**.




## Update SAML Provider Settings in Costpoint Cloud

Costpoint Configuration Utility allows you to configure Costpoint Single Sign-On authentication via SAML Identity Provider. Deltek highly recommends that Costpoint Administrators use this tool to make changes related to such configurations.

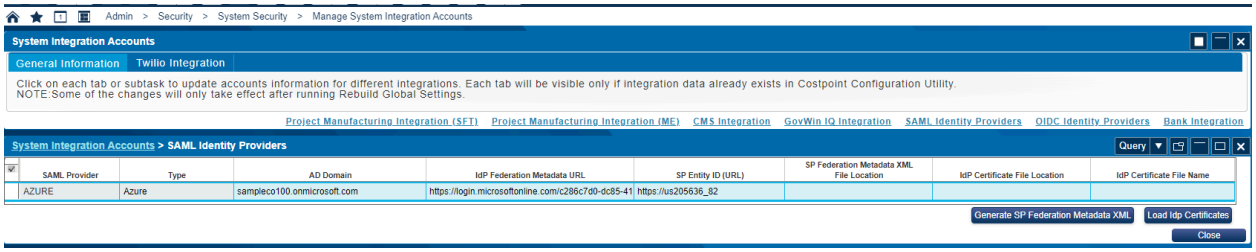
However, there may be use cases when Costpoint Administrators have limited access to the Costpoint/ Weblogic server environments and therefore, may not always run Costpoint Configuration Utility. Typically, this is the case when Costpoint is deployed in the Cloud.

As an alternative to Costpoint Configuration Utility, the Costpoint Administrator can use the Manage System Integration Accounts (SYMINTGR) application that provides some limited capabilities to update SAML Identity Provider settings.

To use Manage System Integration Accounts to update SAML Identity Provider settings:

1. Click **Administration » Security » System Security » Manage System Integration Accounts.**

2. Click **SAML Identity Providers** to open the subtask.

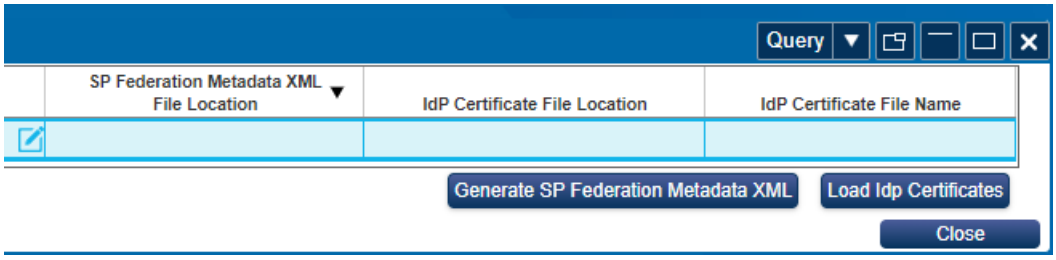



3. You can update the following **SAML Identity Provider** integration settings:

   - **AD Domain**: This setting is optional. The **AD Domain** is your company's SAML IdP (Windows AD) domain. It is used as a hint only to build the SAML IdP user logon name during sign-in. The system concatenates the **AD Domain** value with the **Active Directory ID** entered on the Manage Users screen. For example, if the **Active Directory ID** from the Manage Users screen is **john.smith** and the **AD Domain** is **us.mycompany.com**, the system will use **john.smith@us.mycompany.com** as a default value for the SAML user account logon name on the SAML IdP login page.
     If the users authenticate from multiple IdP domains, you can leave the **AD Domain** field blank and enter the fully qualified user logon name for **Active Directory ID** on the Manage Users screen for each user (for example, **john.smith@us.mycompany.com**, not just **john.smith**).
   - **IdP Federation Metadata URL**: This is the URL that points to the SAML IdP metadata. The value must conform to URL syntax and start with either http or https protocol.
   - **SP Entity ID (URL)**: This is the Costpoint application identifier within the IdP. The value is defaulted by **Enterprise App External URL** from the Costpoint configuration. You can change this value to use another identifier for the **SP Entity ID (URL)**. The value must conform to URL syntax and start with either http or https protocol (for example, **https://my_adfs_test_system1**, **https://costpoint_system_prod**).

4. Click **Generate SP Federation Metadata XML** to generate the SP Federation Metadata XML File and later use it as a starting point to load Costpoint application metadata into IdP.

5. Click **Load IdP Certificates** to load the IdP Certificates into the Costpoint configuration.




# OIDC Single Sign-on Setup

Costpoint can be configured to act as an OIDC Service Provider to allow users to log into the system in OIDC Single Sign-On (OIDC SSO) mode. In this scenario, users do not provide credentials, such as password or MFA, on the Costpoint login page. Instead, Azure Active Directory or any other OIDC-compliant server acts as an OIDC Identity Provider responsible for verifying the user's identity.

Open ID Connect (OIDC) is an authentication protocol based on the OAuth2 protocol (which is used for authorization). OIDC uses the standardized message flows from OAuth2 to provide identity services. The OIDC authentication flow is very similar to the SAML authentication flow with a different protocol in use. Same as with SAML, the authentication of the user must take place at an identity provider where the user's session or credentials will be checked. In addition to authentication, the user can be asked for consent. Consent is the user's explicit permission to allow an application to access protected resources. Consent is different from authentication because consent only needs to be provided once for a resource. Consent remains valid until the user or admin manually revokes the grant.

OIDC is a lightweight, easy to configure, and more modern authentication protocol in comparison to SAML. Most modern applications are now using OIDC instead of SAML for single sign-on authentication.

Same as with SAML, OIDC allows a user to log into an application using SP-initiated sign-in as well as IdP-initiated sign-in.

For SP-initiated sign-in, the user starts on the Costpoint login page, gets redirected to the company IdP, enters IdP credentials, obtains a valid OIDC token, and, finally, gets redirected back to Costpoint.

For IdP-initiated sign-in, a user starts on the company IdP portal. From there, the user clicks the Costpoint application icon/link and gets redirected to Costpoint.

### Configure OIDC SSO between Costpoint and OIDC IdP

Setting up OIDC Single Sign-on between Costpoint and OIDC Identity Provider requires changing the configuration on both sides. Typically, you start configuring the initial settings in IdP and then, having IdP metadata, you complete the setup on the Costpoint side.

## Configure OIDC SSO between Costpoint and Microsoft Azure

To configure OIDC SSO between Costpoint and Azure:

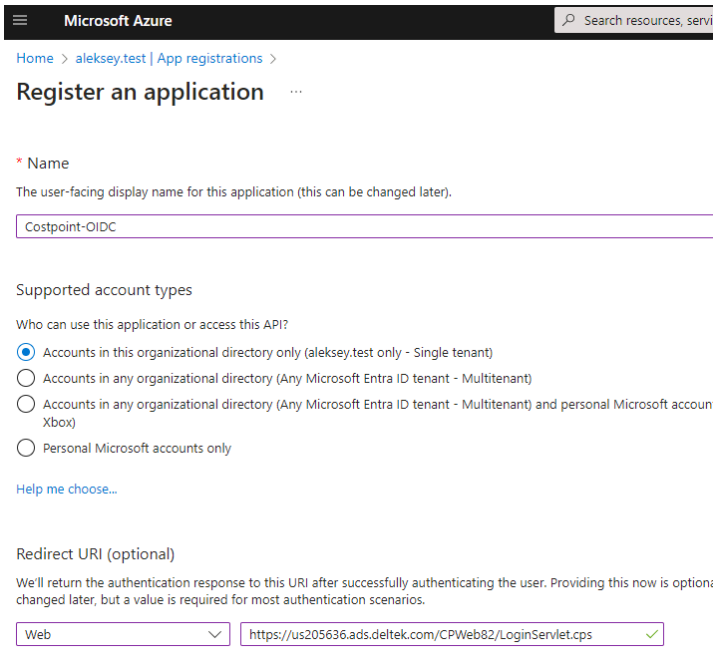
1. Navigate to **Azure Active Directory (Microsoft Entra ID) » App Registrations » All Applications**.

2. Click **New Registration**.

3. On the Register an application screen, take the following actions:

   - **Name**: Enter the name for the application (for example, **Costpoint-OIDC**).
   - **Supported account types**: Select the default value of **Accounts in this organization directory only**.
   - **Redirect URI**: Select **Web** as the platform and enter the Costpoint LoginServlet.cps URL (for example, **https://host/LoginServlet.cps**).

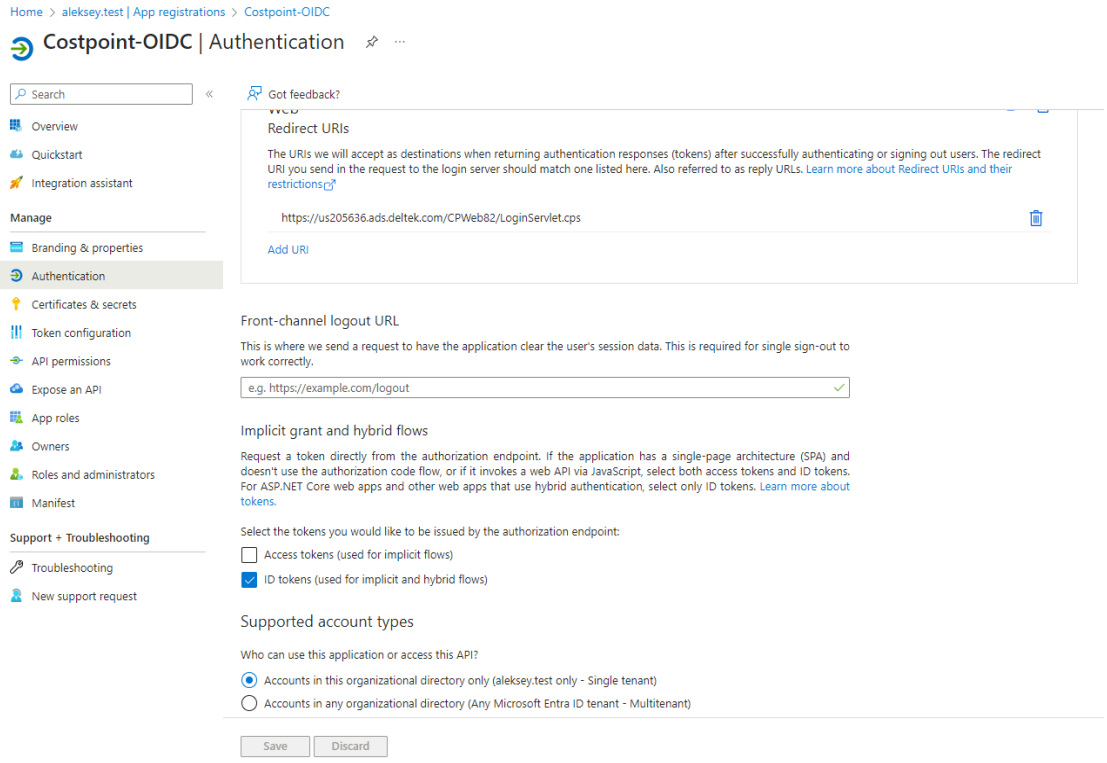
   Azure will send the OIDC authentication token to this URL.




4. Click **Register**.

5. On the newly created app registration screen, click **Authentication**.

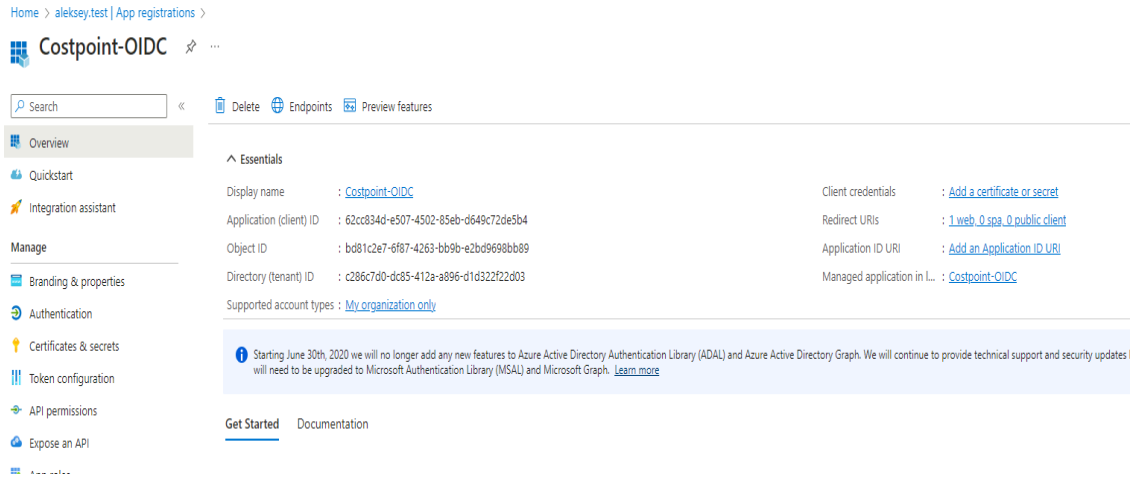
6. On the Authentication screen, select the **ID tokens (Used for implicit and hybrid flows)** checkbox, and click **Save**.




7. On the app registration page, click **Overview**.

8. In the **Essentials** section of the Overview screen, copy the **Application (client) ID** for later use.

   You will need this value to complete OIDC setup in Costpoint Config Utility.

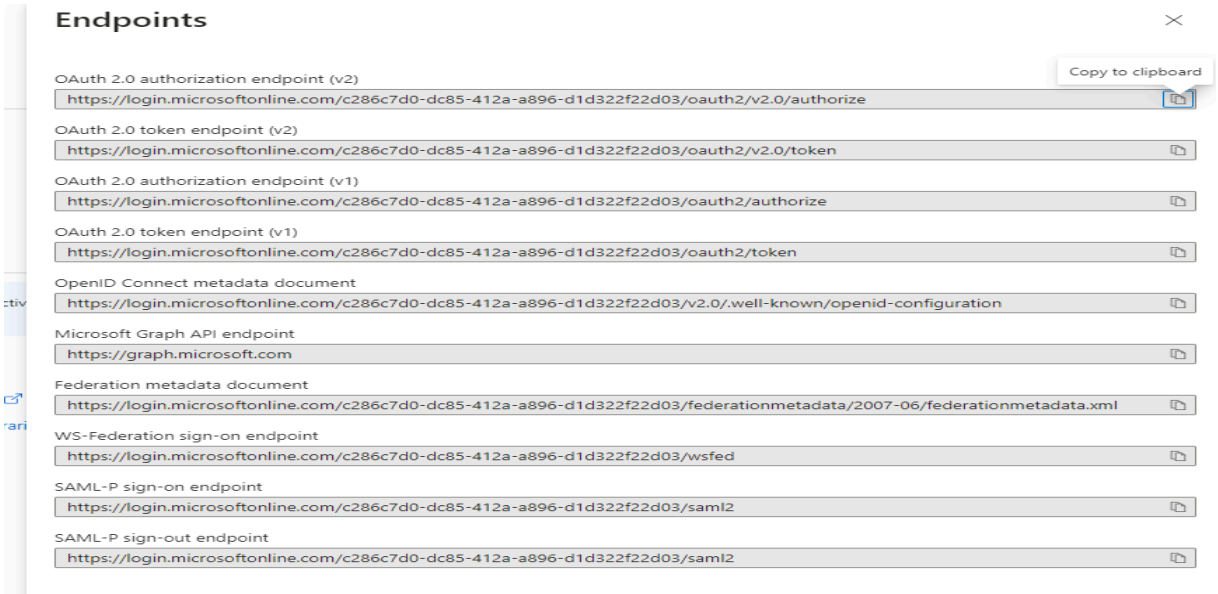



**Tip:** Select the application ID and click the **Copy to clipboard** icon that displays. Paste the ID into a temporary text file for quick reference when you complete OIDC setup in Costpoint Config Utility.

9. On the menu at the topic of the Overview screen, click **Endpoints**.

10. Copy the **OpenID Connect metadata document** URI for later use.

    You will need this value to complete OIDC setup in Costpoint Config Utility.




**Tip:** As with the application ID, use the **Copy to clipboard** icon to copy the URI and paste it into the

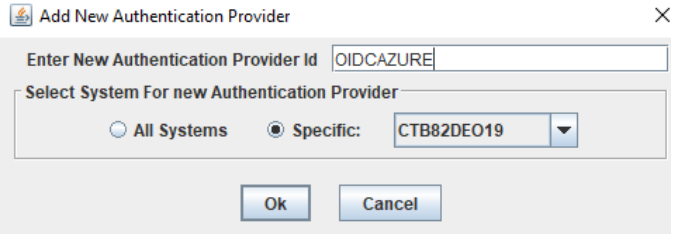
temporary text file for later use.

11. Open Costpoint Configuration Utility to register the new OIDC Authentication Provider.

12. Navigate to **WebLogic » Security**, and click **Add** to a add new (OIDC) Authentication Provider.

13. On the Add New Authentication Provider dialog box, take the following actions:

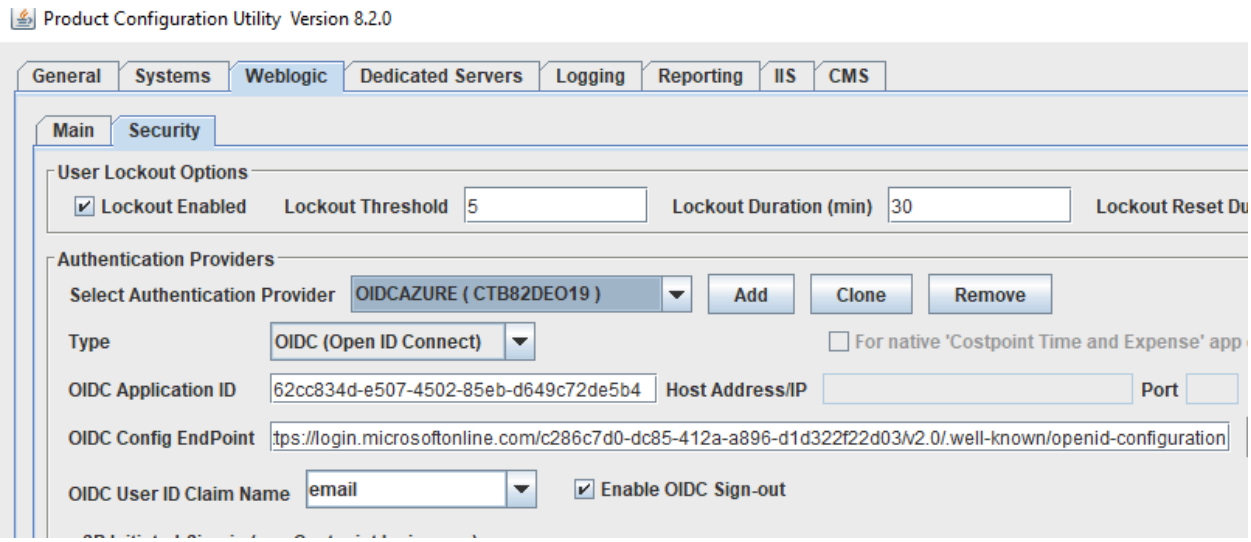
    - **Enter Authentication Provider Id**: Enter a name for the new authentication provider.
    - **Select System For new Authentication Provider**: You can add the provider to **All Systems** or a **Specific** system. If you add the provider to a specific system, select that system using the drop-down field.




14. Click **Ok**.

15. On the Weblogic » Security screen, take the following actions:

    - **Type**: From drop-down list, select **OIDC (Open ID Connect)**.
    - **OIDC Application ID**: Enter the application ID from step 8 above.
    - **OIDC Config EndPoint**: Enter the endpoint URI from step 10 above.
      **Tip:** If you copied the application ID and endpoint URI to a temporary text file, you can quicky copy and paste the information into the corresponding fields.
    - **OIDC User ID Claim Name**: Leave the default value of **email** for this field.
    - **Enable OIDC Sign-out**: Select this checkbox so that when users log out of Costpoint, they also log out of Open ID Connect.




16. Click **Save** to register the new OIDC authentication provider in Costpoint Configuration Utility.

### Limit User Access to Costpoint

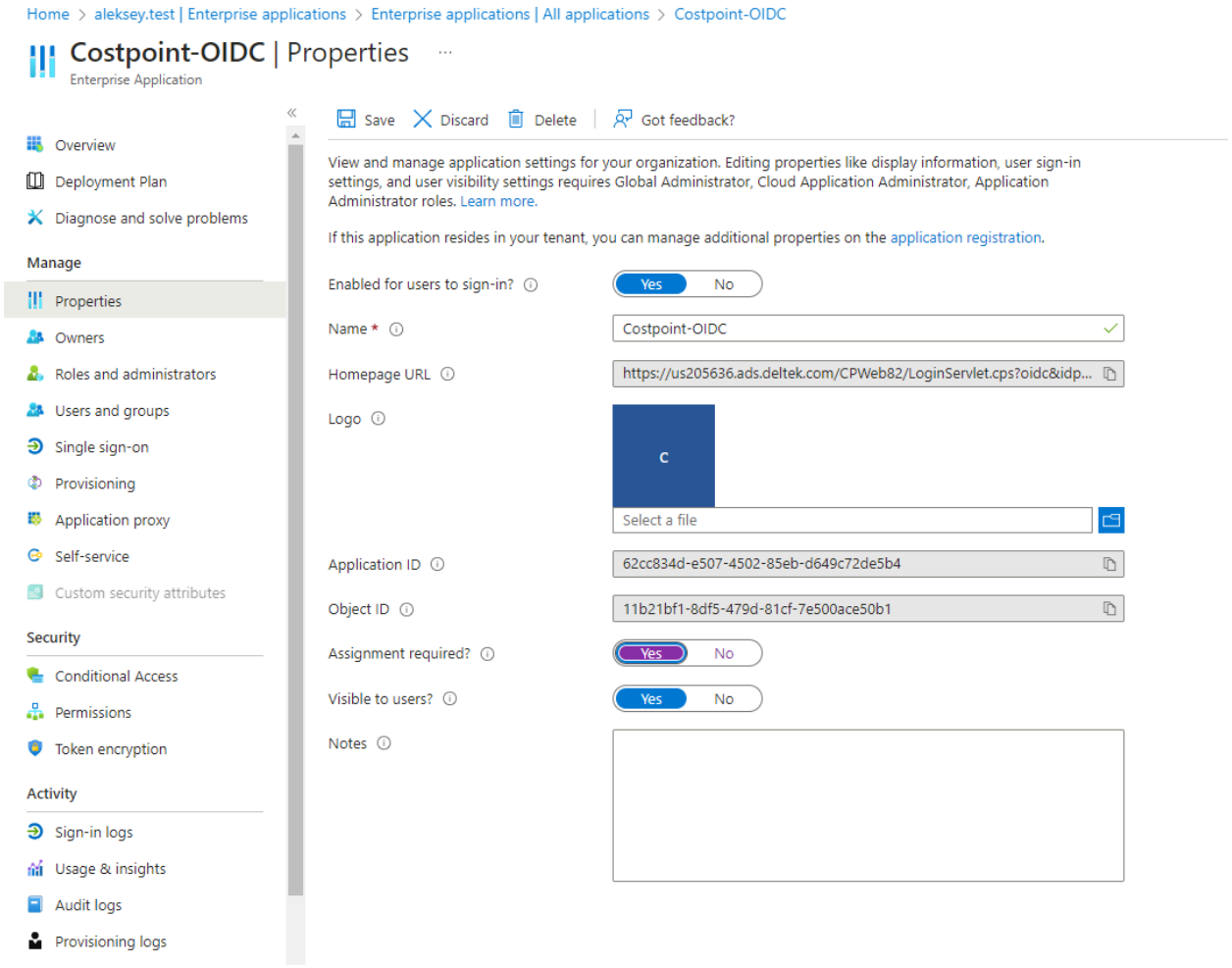
By default, all users in your organization directory will have rights to access Costpoint, but you can limit access rights to Costpoint for specific users or groups.

**To limit access rights to Costpoint:**

1. Return to the Azure Active Directory (Microsoft Entra ID) portal.

2. For the authentication provider, navigate to **Enterprise Applications » Properties**.

3. Change the **Assignment Required** setting to **Yes**.




4. Go to **Enterprise Applications » Users and groups** to allow specific users and groups access to the Costpoint application.

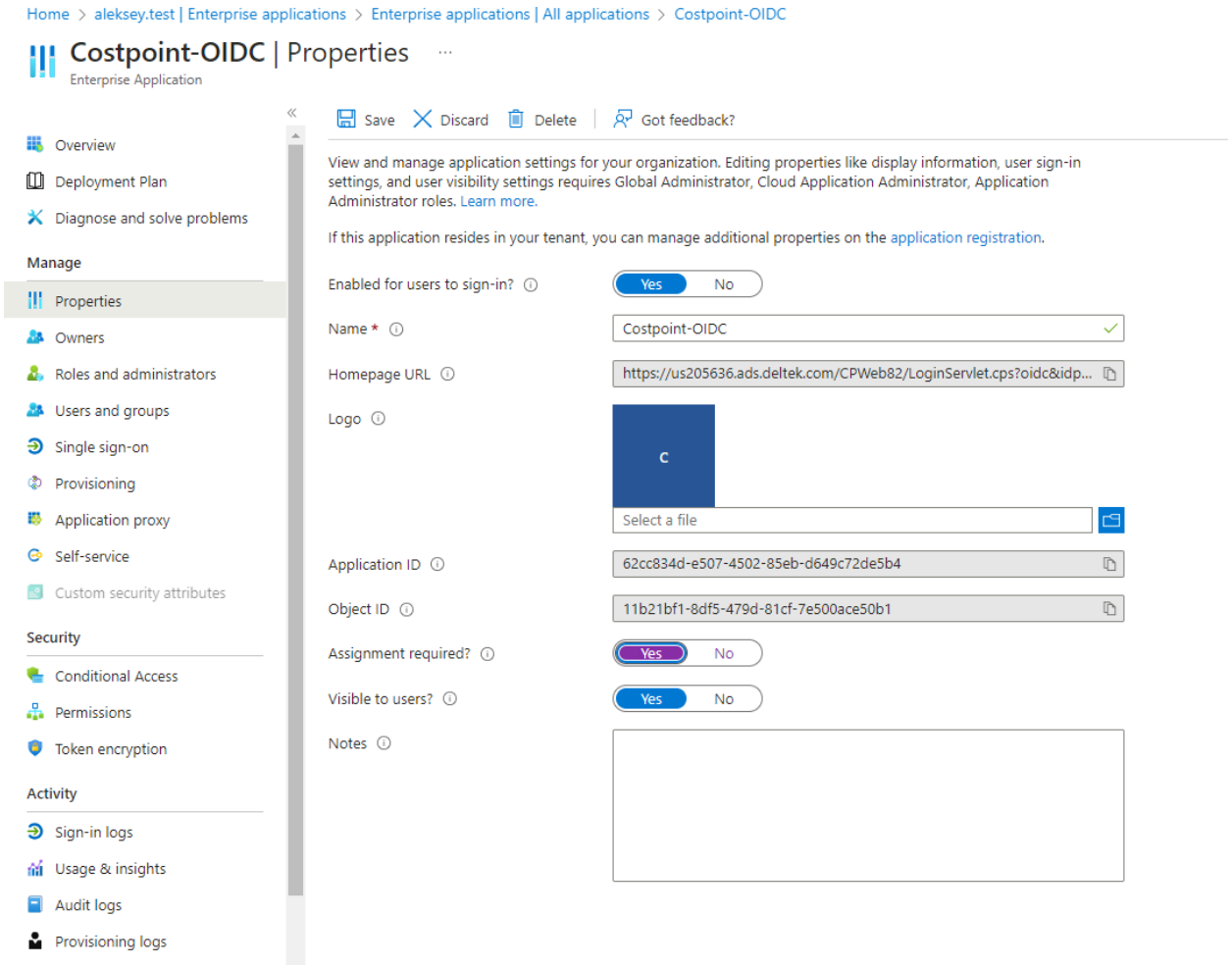
## Configuring IdP-initiated SSO

**To configure IdP-initiated sign-in:**

1. Return to the Azure Active Directory (Microsoft Entra ID) portal.

2. For the authentication provider, navigate to **Enterprise Applications » Properties**.

3. Change the **Visible to users** setting to **Yes**.

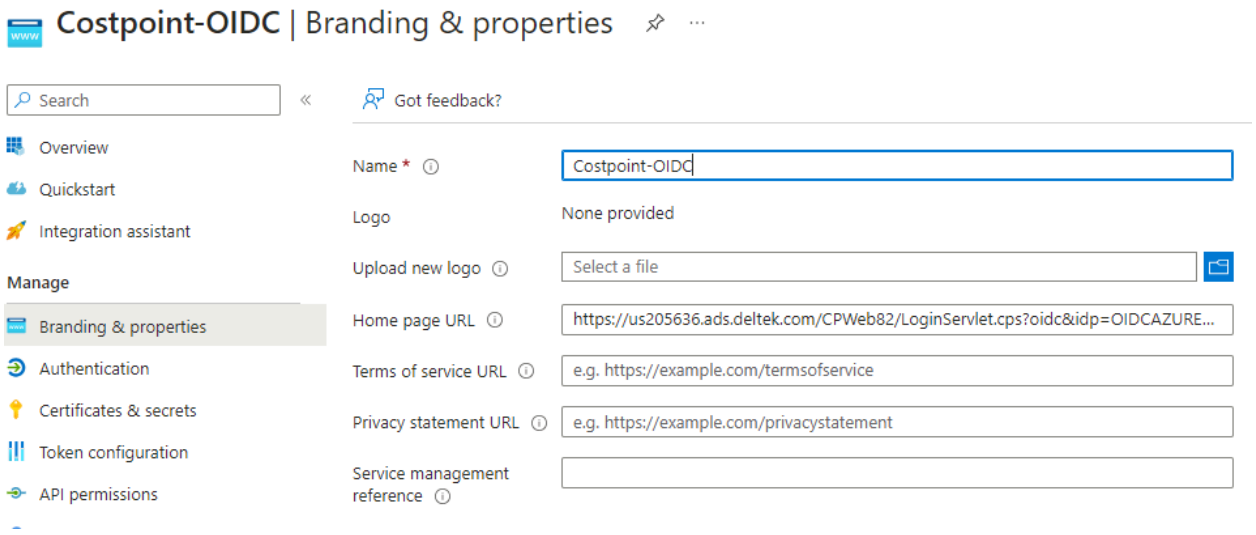



4. Navigate to **App Registration » Branding & properties**.

5. In the **Home page URL** field, enter the URL that points to your Costpoint LoginServlet.cps.

   Add URL query parameters **idp** and **system** to specify your Costpoint OIDC Authentication Provider name and Costpoint System. For example:

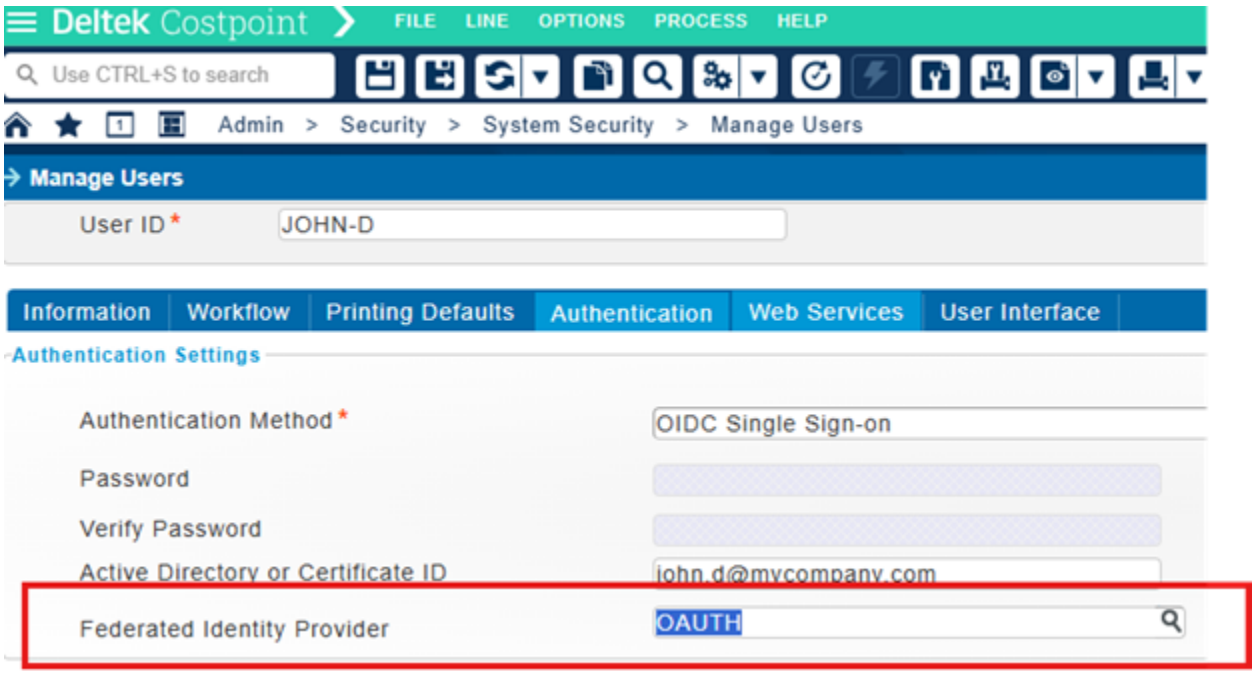
   https://myserver.com/CPWeb82/LoginServlet.cps?oidc&idp=OIDCAZURE&system=CTB82DEO19




## Multiple OIDC Providers

In most cases, having a single OIDC provider is sufficient. However, there are situations where users from different identity providers need to authenticate to the system. Costpoint supports adding multiple OIDC providers to address such requirements.

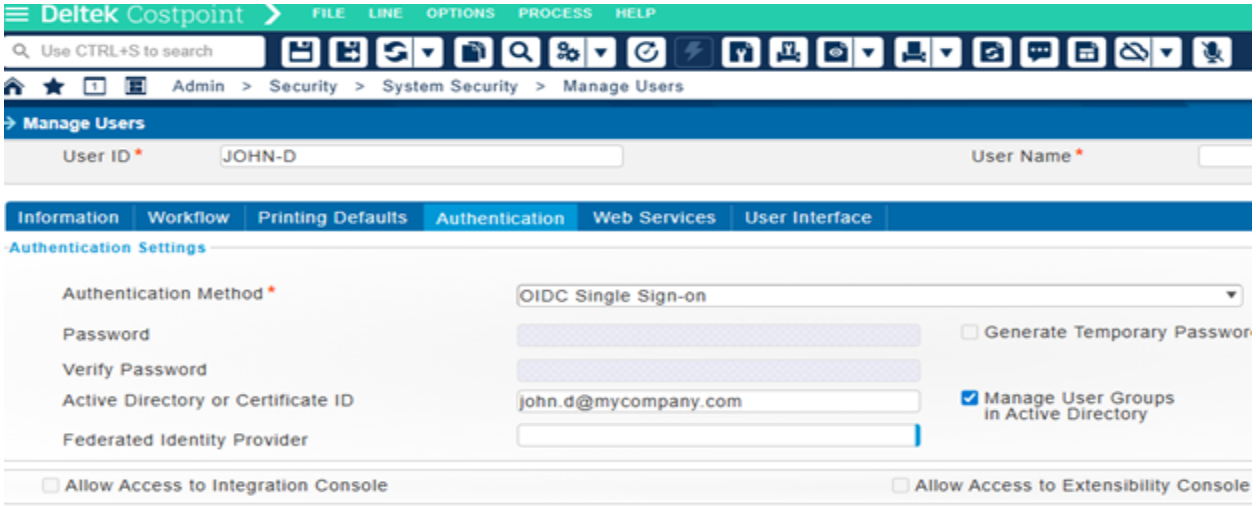
You can assign a specific OIDC provider to each user account by updating the **Federated Identity Provider** field in **Administration » Security » System Security » Manage Users**. If the **Federated Identity Provider** field is left blank, the first (default) OIDC provider will be used to authenticate the user.



## Activate OIDC SSO Mode for Costpoint Accounts

To activate OIDC SSO mode:

1. Click **Administration » Security » System Security » Manage Users**.
2. Select a user.
3. Click the Authentication tab.
4. For **Authentication Method**, select **OIDC Single Sign-On** to allow the user to log into Costpoint in OIDC SSO mode.
5. For **Active Directory ID or Certificate**, enter the ID to reference the user account name within company IdP.




## Update OIDC Provider settings in Costpoint Cloud

Costpoint Configuration Utility allows to configure Costpoint Single Sign-On authentication via OIDC Identity Provider. Deltek highly recommends that Costpoint Administrators use this tool to make changes related to such configurations.

However, there may be use cases when Costpoint Administrators have limited access to the Costpoint/ Weblogic server environments and therefore, may not always run Costpoint Configuration Utility. Typically, this

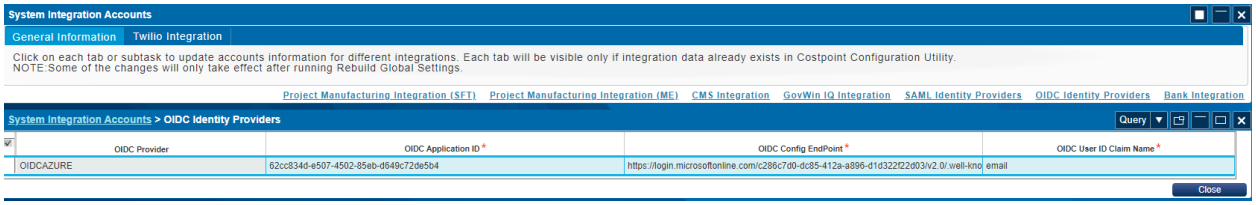
is the case when Costpoint is deployed in the Cloud.

As an alternative to Costpoint Configuration Utility, Costpoint Administrator can use the Manage System Integration Accounts (SYMINTGR) application that provides some limited capabilities to update OIDC Identity Provider settings.

To use Manage System Integration Accounts to update OIDC Identity Provider settings:

1. Click **Administration » Security » System Security » Manage System Integration Accounts**.

2. Open OIDC Identity Provider subtask




3. Update the following OIDC Provider integration settings:

   - **OIDC Application ID**: This is the Costpoint application (client) ID configured on the IdP side.
   - **OIDC Config EndPoint**: This is the URL that points to the IdP OIDC metadata. The value must conform to URL syntax and start with either http or https protocol.
   - **OIDC User ID Claim Name**: This is the IdP authentication token claim name that carries the user account name. The default value is **email**.

## Manage User Groups in Active Directory/Identity Provider

Costpoint Administrator can also configure a user to synchronize Active Directory/Identity Provider groups with Costpoint groups. In this case, any changes in a user's group membership done in AD/IdP will be reflected in their group membership in Costpoint. The synchronization occurs each time users log into Costpoint. Costpoint supports this feature for those authentication methods that use AD/IdP as a centralized place for managing user accounts.

- Active Directory
- Kerberos Single Sign-on
- SAML Single Sign-on
- Kerberos Single Sign-on or SAML Single Sign-on
- OIDC Single Sign-on

- Kerberos Single Sign-on or OIDC Single Sign-on
- Kerberos Single Sign-on or Active Directory
- Kerberos Single Sign-on or Database
- Windows Domain and Active Directory
- Windows Domain and Database

For Active Directory authentication method, the user's assigned AD groups (group names) are retrieved from the AD server and synchronized at login.

For all Kerberos Single Sign-on authentication methods (such as Kerberos Single Sign-on, Kerberos Single Sign-on or Active Directory, Kerberos Single Sign-on or Database, Windows Domain and Active Directory, Windows Domain and Database), the AD groups are also retrieved right at login but the retrieval process is slightly different. Kerberos ticket, which is used to authenticate a user in a Single Sign-on mode, doesn't have user assigned group names. Instead, the ticket contains group SIDs. Therefore, the Costpoint administrator has to create a mapping between Active Directory group names and group SIDs. This is achieved by first exporting the Active Directory group names and SIDs information into a csv file, and then uploading the csv file into Costpoint. Note that for all Kerberos Single Sign-on authentication methods, Costpoint is not required to have direct access to the company AD server. A typical use case of that would be when Costpoint is deployed in the Cloud.

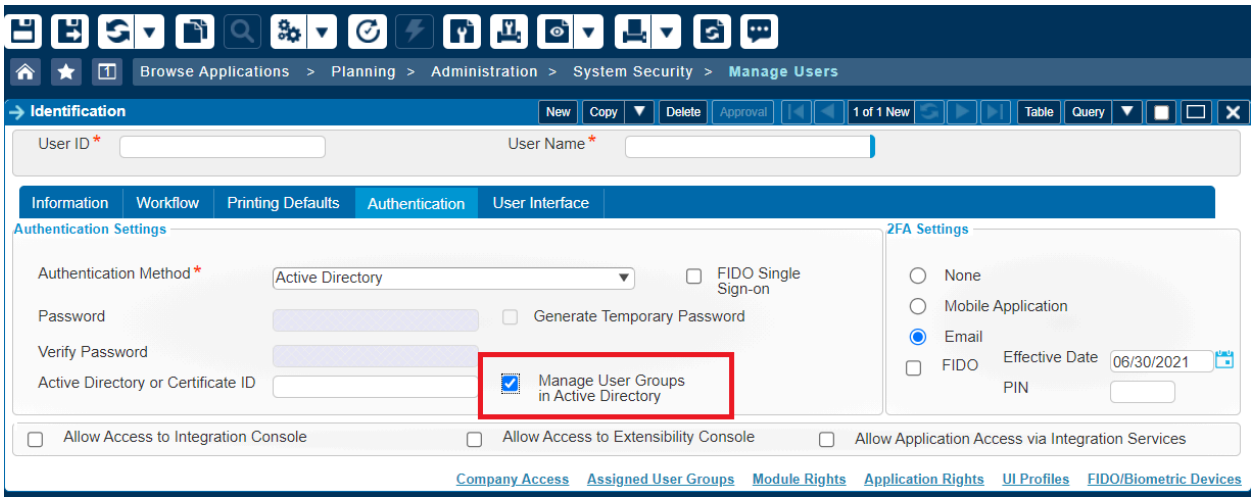
For SAML and OIDC authentication methods, the IdP groups are retrieved right at login as well under condition that SAML or OIDC authentication tokens contain "Group" claim that lists current groups a user is assigned to.

The IdP Administrator must explicitly add the **Group** claim to be passed to Costpoint via a SAML/OIDC token. Costpoint recognizes either of the following names for the **Group** claim:

- "Group"
- "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name"

**To manage User Groups in Active Directory/Identity Provider:**

1. Click **Administration » Security » System Security » Manage Users**.
2. Select a user.
3. Click the Authentication tab.
4. Select the **Manage User Groups in Active Directory** check box.




5. Repeat above steps for any users who should have **Manage User Groups in Active Directory** on.

6. Click **Administration » Security » System Security » Manage User Groups**.

7. If your users use Active Directory or SAML authentication methods only and not a Kerberos Single Sign-on method, skip step 8 and proceed to step 9.

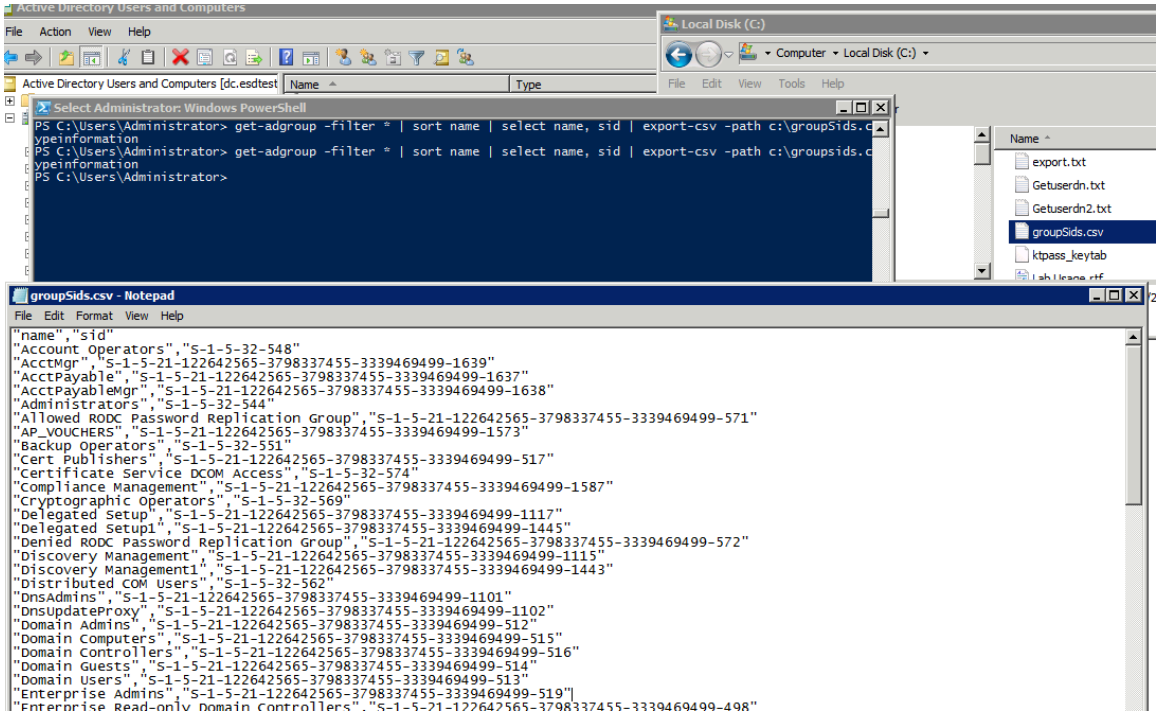
8. If your users use a Kerberos Single Sign-on authentication method, you have to create a mapping between the Active Directory group names and group SIDs.

   a. Execute the following Windows Power Shell (PS) script on your AD domain controller server:

   ```
   get-adgroup -filter * | sort name | select name, sid | export-csv -path c:\gr
   oupsids.csv -notypeinformation
   ```

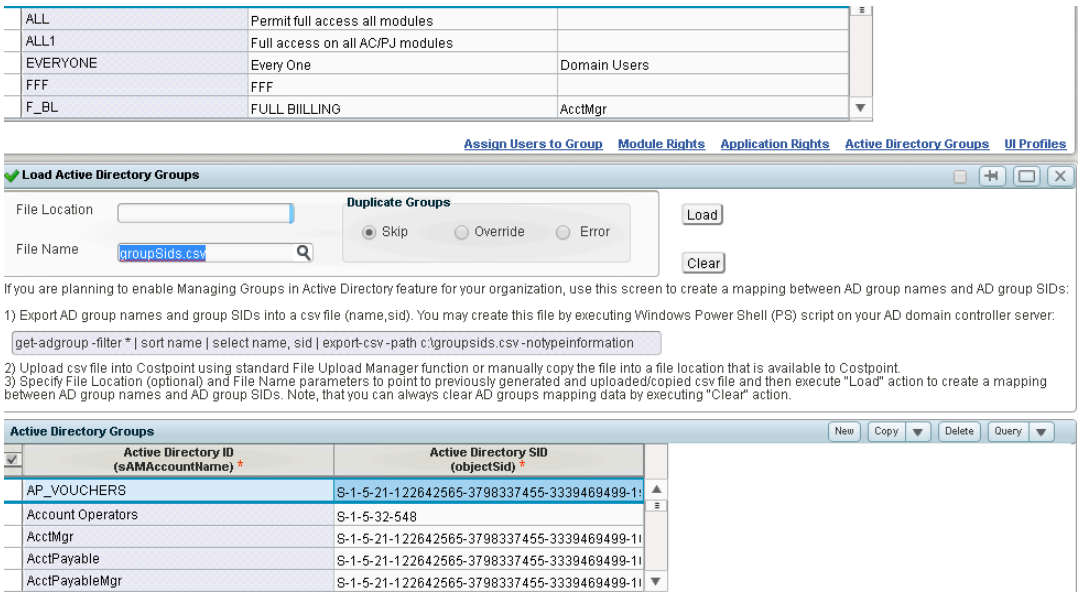
   This creates a csv file with the following simple structure:

   ```
   "name","sid"
   ```




b. Upload the csv file into Costpoint using the File Upload Manager function or manually copy the file into a file location that is available to Costpoint.

c. Open the **Manage Users Groups » Active Directory Groups** subtask.




d. Specify the **File Location** (optional) and the **File Name** parameters to point to previously generated and

uploaded/copied csv file.

e. Click the **Load** button to create a mapping between the AD group names and the AD group SIDs.

**Note:** You can always clear the AD groups mapping data by clicking the **Clear** button.

9. Update the mapping between Costpoint user group and Active Directory group by entering the Active Directory Group ID for the **Active Directory ID (sAMAccountName)** value.

   Use either Lookup in case you processed a csv file with the group names and SIDs information (see step 8) or enter the value manually. This value must be identical to the **sAMAccountName** attribute in group setup in Active Directory.

# Single Sign-On (Windows Kerberos/AD) Setup

Setting up Kerberos Single Sign-On is a four-step process:

- Step One: Create a Kerberos Service Principal and keytab file
- Step Two: Configure the Costpoint WebLogic Server
- Step Three: Update User Setup in Costpoint to Use Single Sign-On

## Step One: Create a Kerberos Service Principal and keytab File

The configuration discussed in this section is the generic Microsoft Windows Kerberos setup using Windows Active Directory and its Kerberos tools.

**Note:** Deltek recommends that you consult the Microsoft documentation on Kerberos services if you have additional questions on these steps.

This step needs to be performed on the Active directory server of the domain in which the end users are registered. In case the end users span across multiple Active Directory reals, separate Kerberos principals are created for Costpoint Server in each of those participating Windows Domains resulting in one multiple keytab files one per domain irrespective of the location of Costpoint servers.

### Create a New User Account in Active Directory

**To create a new user account in Active Directory:**

1. Start the Active Directory Users and Computers program on the Active Directory server.

2. Click **New User**.

3. Name the new user account in lower case (for example, **sso_weblogic**).

4. Under **Account Options**, select the **This account supports Kerberos AES 128 bit encryption** option.

   **Warning:** Enabling AES encryption can corrupt the user's password. Reset the password after this step.

   Deltek recommends that you use all lowercase letters in User account. Subsequent steps in this process may result in errors if the case doesn't match.

5. Under **Account Options**, clear the **Do not require Kerberos preauthentication** check box.

### Use ktpass to Create the SPN and keytab

Use the **ktpass** utility to configure the service principal name for the Costpoint application servers and then generate the keytab file that contains the shared secret key of the service. The keytab file will later be used on the application server for further configuration.

**Attention:** For more information about ktpass.exe, refer to TechNet:

https://technet.microsoft.com/en-us/library/cc753771(v=ws.11).aspx

1. Open a command window and run the following command

   ```
   ktpass -princ HTTP/appserver.domainx.com@DOMAINY.COM** -mapuser sso_weblogi
   c@DOMAINY.COM -pass password -crypto ALL -ptype KRB5_NT_PRINCIPAL -out C:\ss
   o_weblogic_keytab
   ```

   Where **princ** is the SPN value and **mapuser** is the active directory account created in previous steps.

   - **appserver.domainx.com**: This is the fully qualified host name of the Costpoint service in lower case. In most cases, it is the hostname of the IIS server which is used as a proxy or load balancer to a WebLogic cluster. Kerberos negotiation will happen by mapping the URL to the SPN account created in this step, so it is important to create the SPN based on the URL used by end users. Unless it is absolutely necessary to access the application server(s) directly, there is no need to create additional SPNs to the host names of the application server or cluster nodes. This value must be based on a DNS A record in order for a Kerberos ticket to be properly constructed.
   - **DOMAINY.COM**: This is the domain to which the active directory server belongs. This value needs to be written in uppercase letters.
   - **sso_weblogic@DOMAINY.COM**: This is the user account created in the previous steps. The user ID should match the case of the account created in the previous steps, and the domain should be written in uppercase letters.
   - **password**: This is the password for the account created in the previous steps.

- **sso_weblogic_keytab**: This is the filename of the generated keytab file. It needs to be copied to the WebLogic server for further configuration.

2. Use the following command to verify the SPNs associated with user account:

```
setspn -L sso_weblogic
```

The following output displays:

Registered ServicePrincipalNames for CN=sso_weblogic,CN=Users,DC=domainy,DC=com

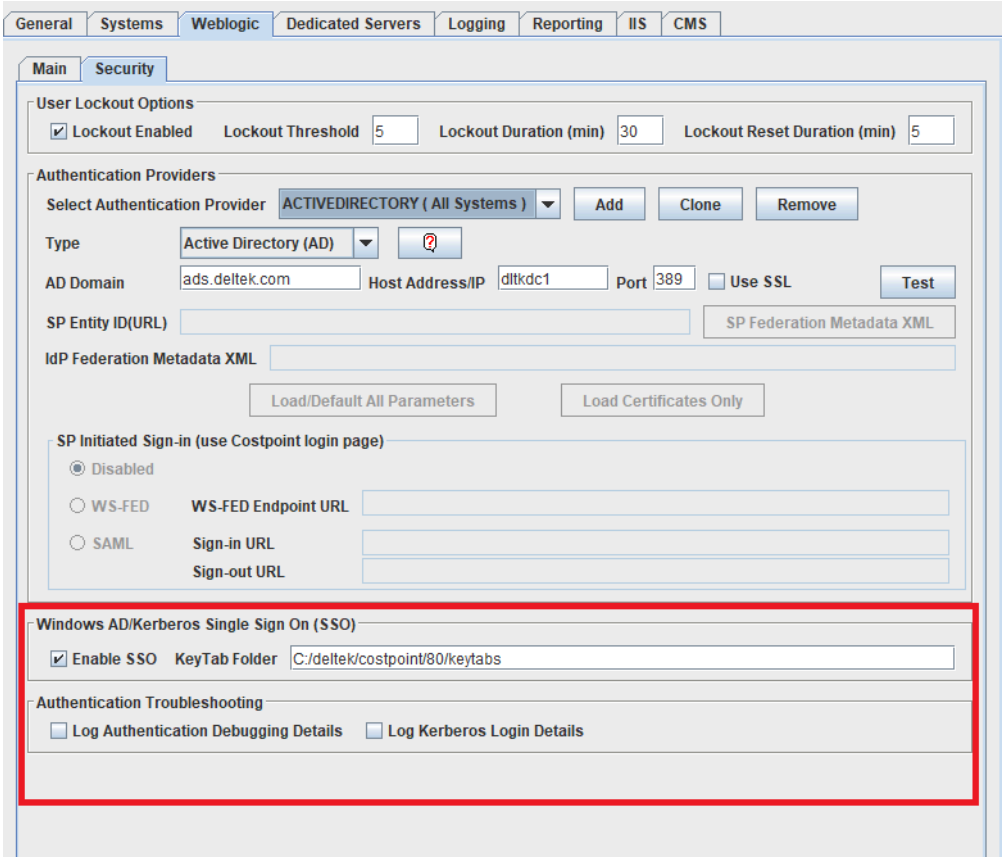
HTTP/appserver.domainx.com@DOMAINY.COM

**Warning:** This step is critical. If the same service is linked to a different account in the Active Directory server, the client does not send a Kerberos ticket to the server.

### Step Two: Configure the Costpoint WebLogic Server

The WebLogic server needs to be configured to enable Kerberos Negotiation. The keytab file created in the previous steps needs to be copied to a location that is accessible to the WebLogic servers. The configuration discussed in this section is performed on the WebLogic Admin server using the Costpoint Configuration utility.

Launch the Configuration Utility, and navigate to Weblogic tab » Security tab to the enable SSO.




- **Enable SSO**: Select this check box for WebLogic to support Kerberos authentication.
- **KeyTab Folder**: This is the folder that contains the keytab files. The WebLogic server reads the keytab files under this folder at runtime to negotiate the identity of the end user. In case of a cluster configuration, all nodes should have access to the keytab files. For this reason, Deltek recommends that you create a separate folder and place all the keytab files in single location under the Costpoint installation directory.
- **Log Authentication Debug Details**: Select this check box to debug the Kerberos Authentication process. Enabling/Disabling this feature requires restarting the WebLogic server(s).

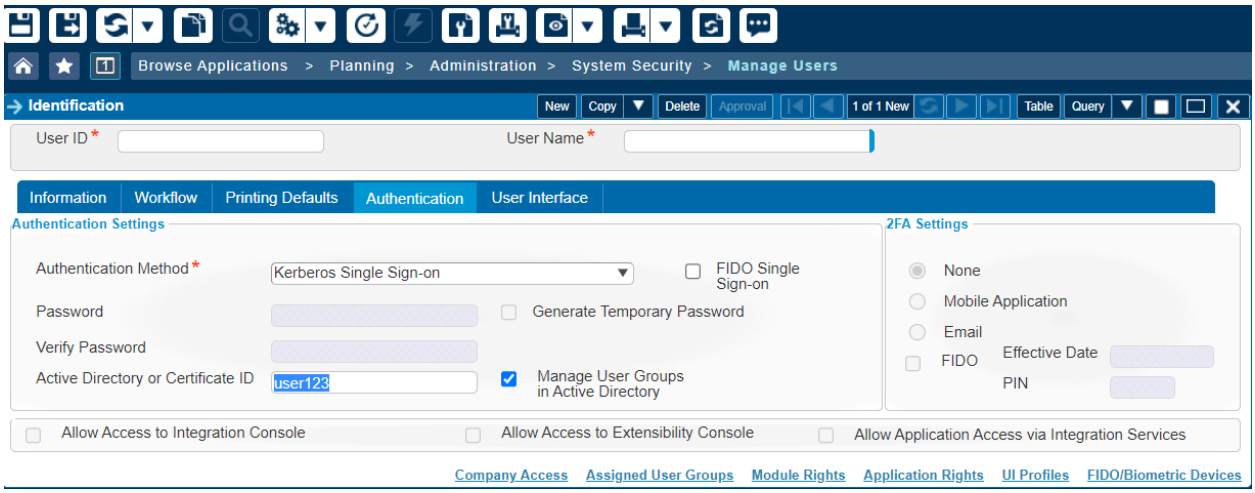
**Attention:** For detailed information about the Costpoint Configuration utility, see the *Deltek Costpoint 8.2 Configuration Utility Guide*.

The WebLogic servers need to be restarted when enabling SSO for the first time. For a cluster configuration, all nodes and the admin server have to be restarted. Further changes to the keytab folder (such as adding a new keytab, editing, or removing a file) will not require restarting the servers. Such changes can be applied at runtime by running the Rebuild Global Settings application.

### Step Three: Update User Setup in Costpoint to Use Kerberos Single Sign-On

**To update the user setup in Costpoint using Manage Users application to use Kerberos Single Sign-On:**

1. Log into Costpoint as the system administrator (CPSUPERUSER).
2. Click **Administration » Security » System Security » Manage Users**.
3. Select a user who should be assigned the Kerberos Single Sign-On authentication method.
4. Click the Authentication tab.
5. In the **Authentication Method** field, select Kerberos **Single Sign-On**.
6. In the **Active Directory or Certificate ID** field, enter the Active Directory user ID.
7. Save your changes.



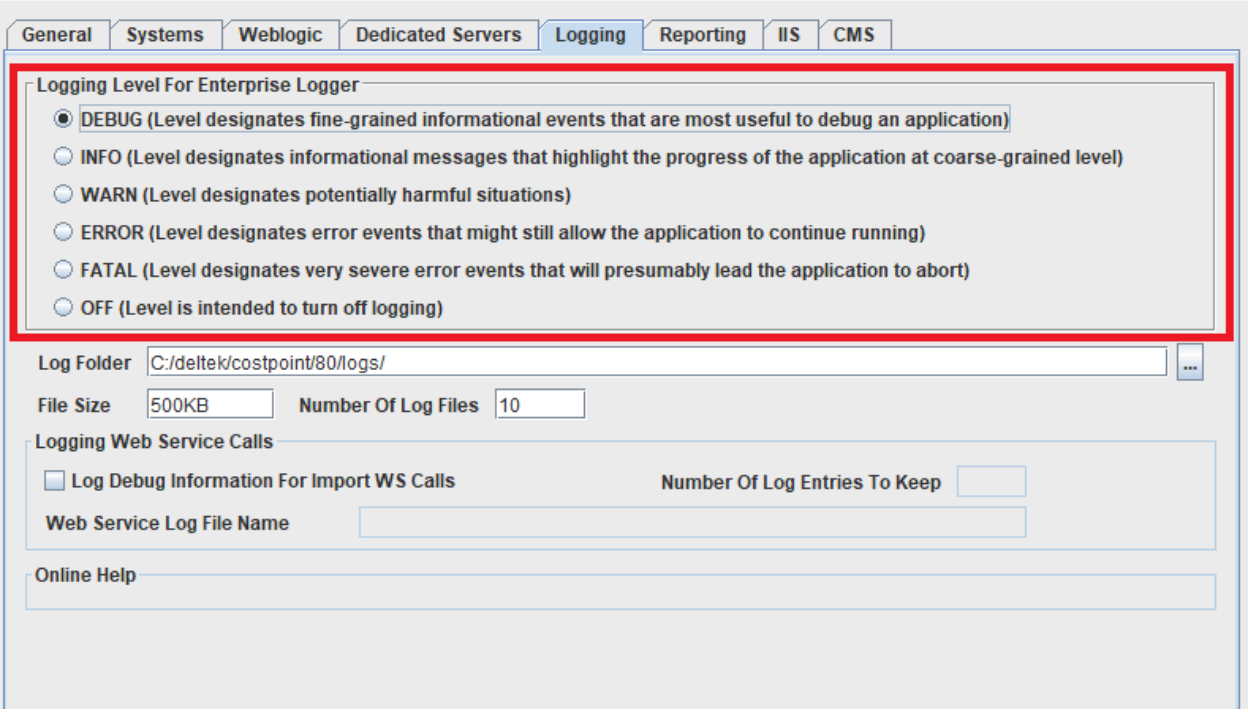

8. Repeat these steps for other users who should be assigned the Kerberos Single Sign-On authentication method.

## Single Sign-On Troubleshooting

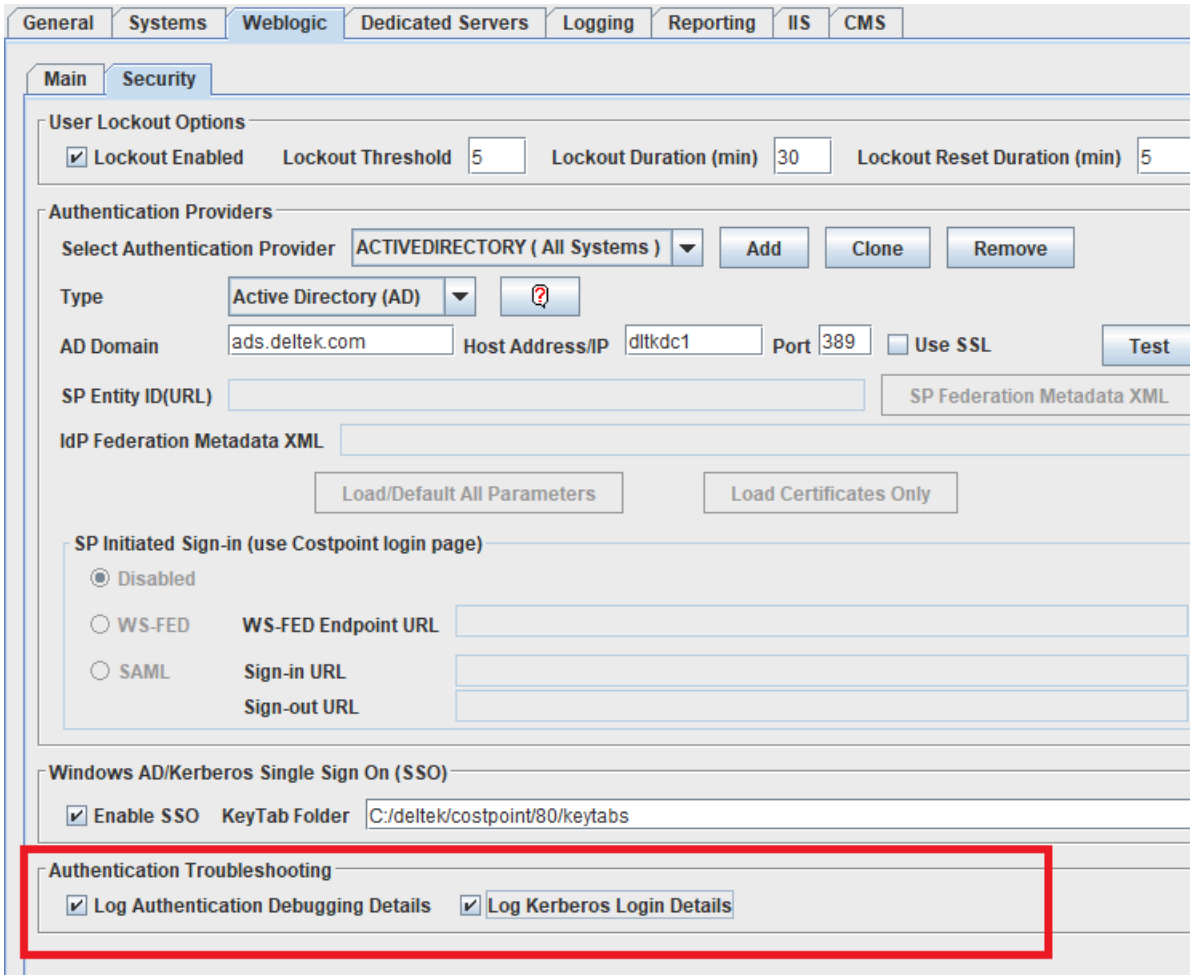
Troubleshooting Single Sign-On related problems cannot be performed during production hours while end users are actively accessing the applications. It needs to be scheduled during downtime without any user activity.

**To debug SSO-related problem, use Configuration Utility to do the following:**

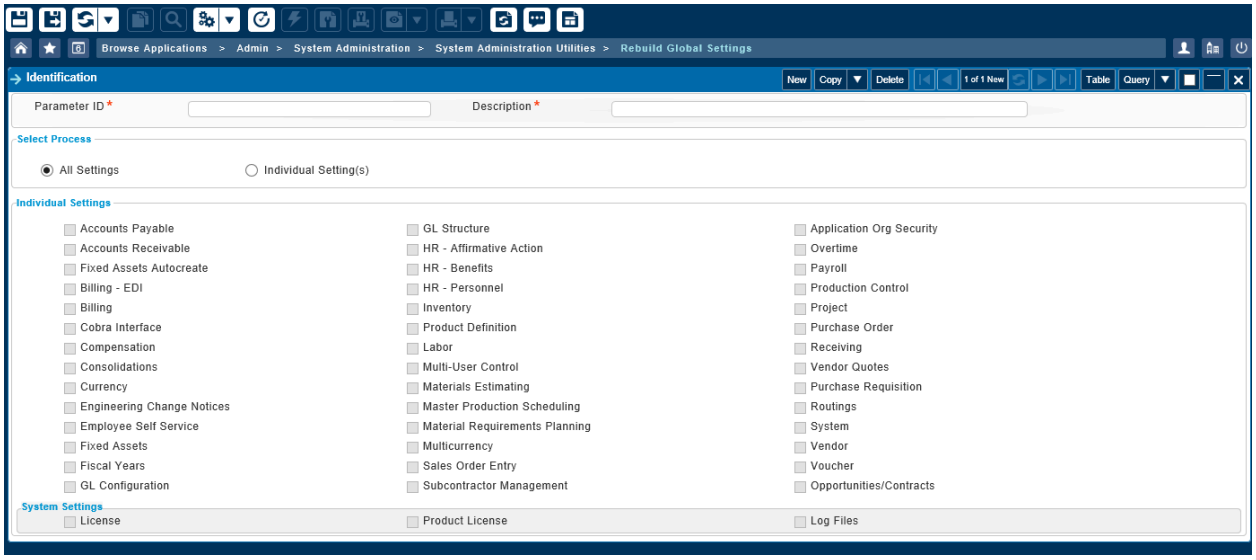
1. On the Logging tab, change the **Logging Level for Enterprise Logger** to **DEBUG**.




2. On the **Weblogic » Security tab**, select the **Log Authentication Debug Details and Log Kerberos Login Details** checkbox.




3. Login to Costpoint as CPSUPERUSER, and execute **Rebuild Global Settings » Reload Settings**.




# Single Sign-On for Private or Public Cloud

If you are deploying Costpoint in a Private or Public cloud, you can configure SSO between Costpoint in the cloud and local to end-user Active Directory. In other words, a user who is logged in into domain “ABC” (local LAN which a user belongs to his company) can seamlessly log in to Costpoint deployed in a private or public cloud outside of domain “ABC.” Costpoint deployment in the cloud will have no visibility/connectivity to Active Directory in domain “ABC”.

If all access to the hosted Costpoint deployment comes from a single local Active Directory forest, the steps for SSO setup will be the same as described in the “Single Sign-On Setup: Java 8 and Above section. That is, the same setup/steps work regardless of whether Costpoint is installed within the same local domain as used by end-users or Costpoint is deployed outside of user domain in the private or public cloud.

Typically, though, a cloud deployment of Costpoint will also use a multi-tenancy model with multiple systems being deployed within a single Costpoint cluster. Each system can represent a company/division in a private cloud or truly independent companies in case of a public cloud. Each division or company in the above scenario may have its own local Active directory domain/realm without any trust between them. In this case, to configure SSO for multiple tenants, you need to create a SPN and keytab in each of those Active Directories and copy all those keytabs to a single location accessible to the Costpoint servers.

For example, if Costpoint is deployed at **http://costpoint.hostdomain.com**, and two companies (ABC.COM and XYZ.COM) access the service, this would require creating two keytabs. Company ABC should create a SPN for **HTTP/costpoint.hostdomain.com@ABC.COM**, and company XYZ should create a SPN for **HTTP/costpoint.hostdomain.com@XYZ.COM**. The resulting two keytabs should be copied to a location on the Costpoint servers. At runtime, for the incoming request, WebLogic will pick the appropriate keytab based on matching the SPN value and perform the negotiation.

# Single Sign-On on Mobile Device

Users on iOS and Android mobile devices (for example, iPhone, iPad, Pixel, or Galaxy) can log in to Costpoint in SSO mode.

### Enable Kerberos SSO on iOS Devices

An iOS device has to be logged into the corporate LAN and be able to connect to your corporate AD. In other words, the device should be using either the corporate Wi-Fi (logged in into corporate LAN) or VPN. Typical usage would be to configure VPN, which is considered to be a "best practice" for accessing corporate resources from mobile devices, regardless of SSO usage. The configuration of the VPN is outside the scope of this document. Instructions should come from your corporate IT department.

To complete SSO enrollment, you need to deploy the SSO profile on your iOS device. This is typically done by IT pushing it to user devices through a corporate MDM server. It can also be done by each user sending a text file with ".mobileconfig" extension to themselves as an attachment and opening it on iOS device.

Note:

1. You put your own GUIDs (in yellow) into the file by generating new ones (for example, through this link: https://guidgenerator.com/online-guid-generator.aspx).

2. Replace "Realm" (my.company.com) with the user's corporate AD server.

3. Replace the URL pattern with sites where you want SSO to be used.

Additional information about various parameters used in the profile configuration can be accessed on Apple website:

https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html

The following is sample contents of such text file with a SSO profile:

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">

<plist version="1.0">
```

```
<dict>

<key>PayloadVersion</key>

<integer>1</integer>

<key>PayloadUUID</key>

<string>9adfb330-9783-472a-b2ea-f1365569ecd3</string>

<key>PayloadType</key>

<string>Configuration</string>

<key>PayloadIdentifier</key>

<string>com.deltek.ssoconfig</string>

<key>PayloadContent</key>

<array>

<dict>

<key>PayloadType</key>

<string>com.apple.sso</string>

<key>PayloadVersion</key>

<integer>1</integer>

<key>PayloadIdentifier</key>

<string>com.deltek.sso.test.kerberos</string>

<key>PayloadUUID</key>

<string>66c2568c-91d5-4946-bbf8-464323326a7b</string>

<key>PayloadDisplayName</key>
```

```
<string>SSO profile for my enterprise</string>

<key>Name</key>

<string>AccountName</string>

<key>Kerberos</key>

<dict>

<key>Realm</key>

<string>my.company.com</string>

<key>URLPrefixMatches</key>

<array>

<string>http://*.my.company.com:7009/</string>

</array>

</dict>

</dict>

</array>

</dict>

</plist>
```

After connecting to the VPN, the profile is installed and your user account in Costpoint (or TE10 or BP7) is configured for SSO. You can open the Costpoint application via an icon on the iOS device, and click the **Login** button without entering your credentials (you only need the system name).

The device may ask you for your AD password the first time you log in. After that, your Kerberos ticket will be cached and you will not need to do anything on the login screen; it will automatically log you in. When the Kerberos ticket expires, you will be prompted for your password again. IT can deploy a certificate as part of the SSO profile on the iOS device that will allow the iOS to auto-renew the Kerberos ticket without asking the user to re-enter the password.

### Enable Kerberos SSO on Android Devices

To enable Kerberos SSO on Android devices, use third-party Kerberos authenticator tools. For more information, refer to the following links:

- https://bayton.org/docs/enterprise-mobility/mobileiron/setup-kerberos-authentication-on-mobileiron-core-for-android-enterprise/
- https://hypergate.com

## Client Certificate Setup

Client Certificate authentication or Mutual TLS (mTLS) is an extension of Transport Layer Security (TLS) where both the client and server authenticate each other using digital certificates. Unlike regular TLS, where only the server presents a certificate to prove its identity, mTLS requires both parties to exchange and validate certificates before establishing a secure connection.

Typically, you have the following configuration with mTLS:

Browser (Client) » IIS/IIS Cluster (Web Server) » WebLogic Server/Weblogic Cluster (Application Server)

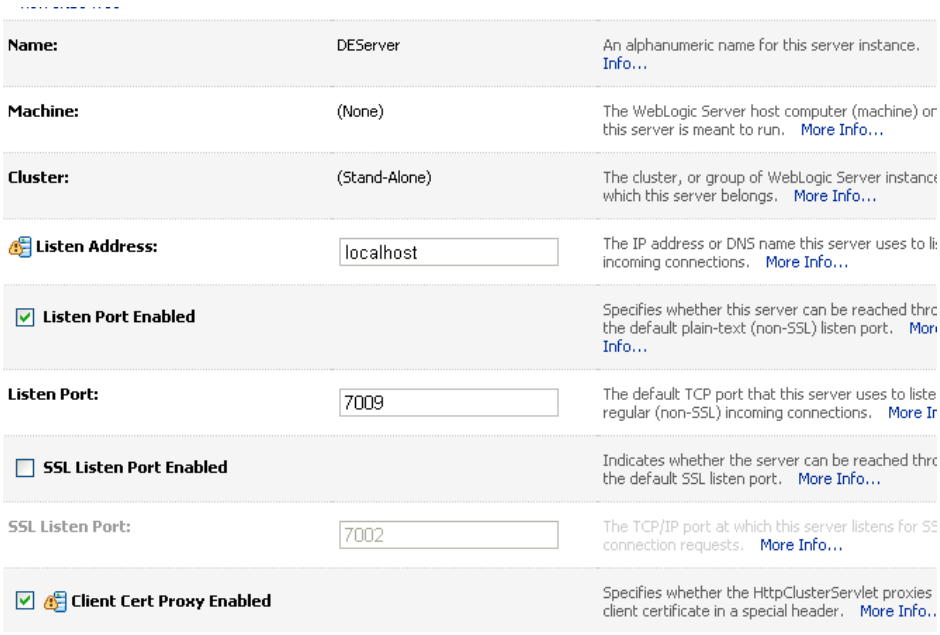
Follow the steps below to enable mTLS authentication.

### WebLogic Server

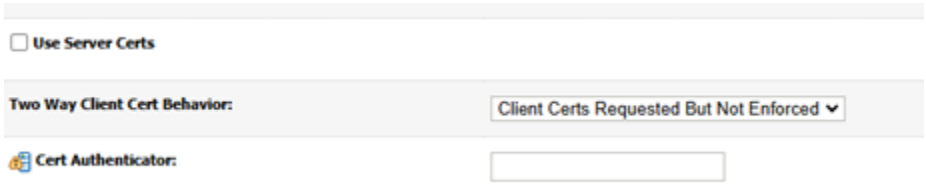
1. Log into the WebLogic Server console and navigate to **Environment » Server**.

   If you are using a WebLogic Server Cluster, make the change for each server node.

2. Navigate to **General** and select the **Client Cert Proxy Enabled** checkbox.

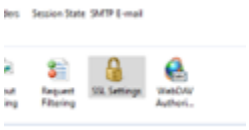



3. Navigate to **SSL » Advanced** and select **Client Certs Requested But Not Enforced** from the **Two Way Client Cert Behavior** drop-down field.

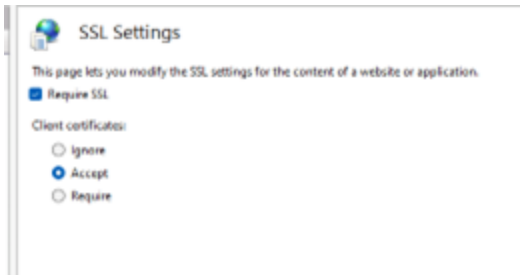



## IIS Server

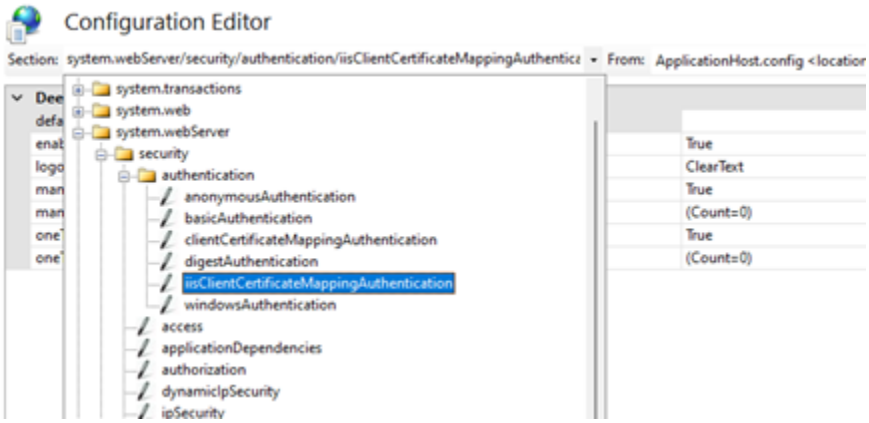
1. Open IIS Manager, navigate to your website or application, and click **SSL Settings** in **Features View**.

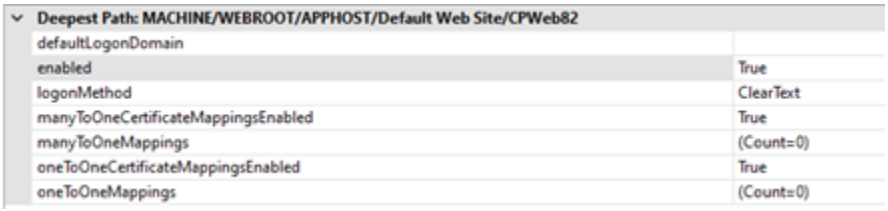


2. Select the **Require SSL** checkbox and click **Accept** for **Client certificates**.




3. Click **Configuration Editor** and navigate to **system.webServer » authentication » iisClientCertificateMappingAuthentication**, and select **enabled = True**.




4. Enable **SSL Binding » Client Cert Negotiation** by running **Windows PowerShell** and executing the “netsh http update sslcert” script.

   - Execute **netsh http show sslcert** and copy the **Certificate Hash** and **Application ID** parameter values. You will need these parameters for the **netsh http update** in the next step.

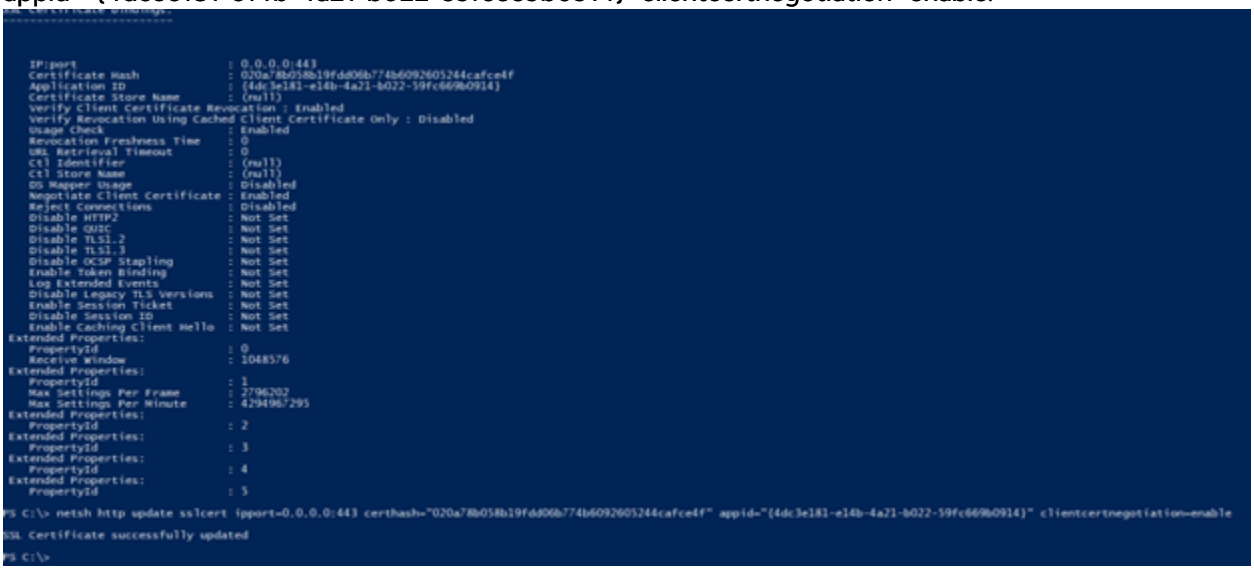
```
PS C:\> netsh http show sslcert

SSL Certificate bindings:
-------------------------



    IP:port                      : 0.0.0.0:443
    Certificate Hash             : 020a78b058b19fdd06b774b6092605244cafce4f
    Application ID               : {4dc3e181-e14b-4a21-b022-59fc669b0914}
    Certificate Store Name       : (null)
    Verify Client Certificate Revocation : Enabled
    Verify Revocation Using Cached Client Certificate Only : Disabled
    Usage Check                  : Enabled
    Revocation Freshness Time    : 0
    URL Retrieval Timeout        : 0
    Ctl Identifier               : (null)
    Ctl Store Name               : (null)
    DS Mapper Usage              : Disabled
    Negotiate Client Certificate : Enabled
    Reject Connections           : Disabled
    Disable HTTP2                : Not Set
    Disable QUIC                 : Not Set
    Disable TLS1.2               : Not Set
    Disable TLS1.3               : Not Set
    Disable OCSP Stapling        : Not Set
    Enable Token Binding         : Not Set
    Log Extended Events          : Not Set
    Disable Legacy TLS Versions  : Not Set
    Enable Session Ticket        : Not Set
    Disable Session ID           : Not Set
    Enable Caching Client Hello  : Not Set
Extended Properties:
    PropertyId                   : 0
    Receive Window               : 1048576
Extended Properties:
    PropertyId                   : 1
    Max Settings Per Frame       : 2796202
    Max Settings Per Minute      : 4294967295
Extended Properties:
    PropertyId                   : 2
Extended Properties:
    PropertyId                   : 3
Extended Properties:
    PropertyId                   : 4
Extended Properties:
```

- Execute netsh http update sslcert ipport=0.0.0.0:443 certhash="020a78b058b19fdd06b774b6092605244cafce4f" appid="{4dc3e181-e14b-4a21-b022-59fc669b0914}" clientcertnegotiation=enable.



5. Obtain a valid client certificate in **PFX** format and install it in the **Personal Certificates Store** of a client browser.

   This could be done manually on the client machine or via IT/Group Policy push to the client machine. The certificate must be trusted by IIS and WebLogic server, meaning the certificate must be signed by a **Trusted Certificate Authority**.

Now, test mTLS configuration by logging in into Costpoint without providing a User ID and password on the Costpoint Login page.

# Passkey (FIDO)

FIDO is a standard for verifying user's digital credentials on the web. It stands for **F**ast **ID**entity **O**nline, and it works on any web browser and on all your devices, including smartphones, desktop or laptop computers, tablets, and smartwatches. FIDO makes logging in to your online accounts much easier while keeping your information safe from hackers and trackers.

FIDO is built on Passkeys. A Passkey is a digital credential that allows users to sign in to a website or app without entering a password or username. Passkeys are a more secure and convenient alternative to passwords. In Costpoint, Passkeys are used for authentication and digital document signing.

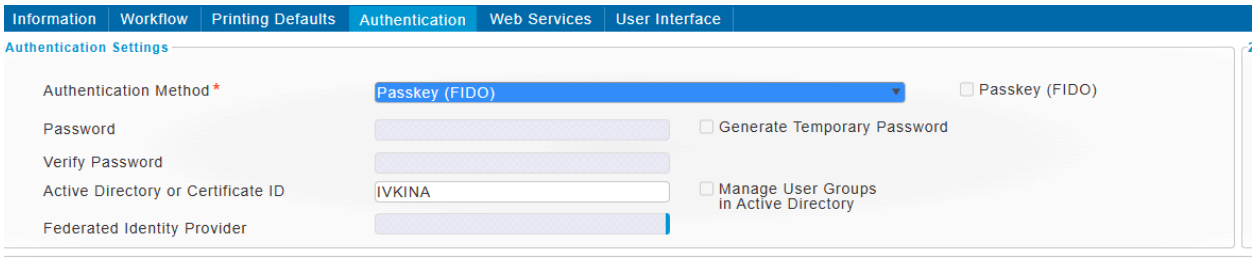
**Attention:** For more information about FIDO and Passkeys, go to https://fidoalliance.org/passkeys/.

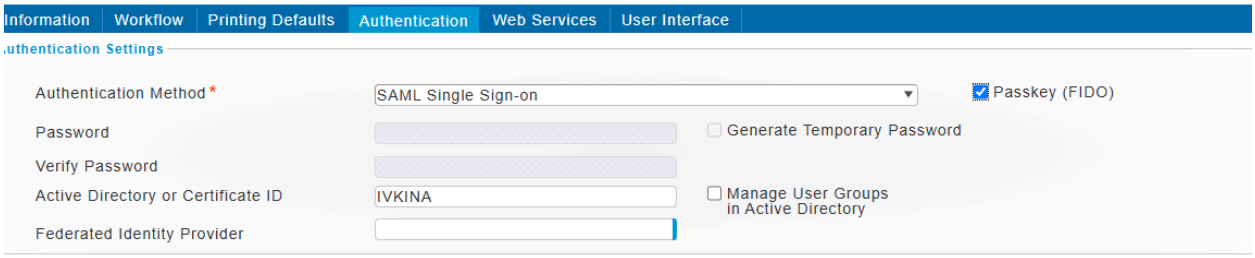
## Authentication

Any Passkey device—such as a simple or biometric USB stick, smartphone, laptop computer with Windows Hello service, smartwatch, and so on—can be used to log in to Costpoint. Passkeys provide a unique experience for a user to be able to authenticate via biometric verification (for example, a fingerprint scan, face or voice recognition, pin). Passkeys either eliminate passwords providing a passwordless login, or it works as a strong second factor for password-based authentication.

### Passkey Authentication Method

To authenticate with Passkey, a user must have the authentication method set to Passkey (**FIDO**) or have the **Passkey** checkbox enabled with other authentication methods. This is done by a System Administrator during user setup in **Manage Users**.




**Attention:** Refer to Manage Users application online help for more details on configuring Passkey authentication for user accounts.

### Passkey Registration

The next step is to register the Passkey on the user's account. Any Passkey compliant device can be used, for example:

- An external USB security key
- A user's personal mobile phone
- A tablet PC
- A laptop with Windows Hello biometric authentication enabled.

The registration step is important as it provides a secure link between the user account and the Passkey. If the Passkey is not registered on the account, a user won't be able to log into the application.

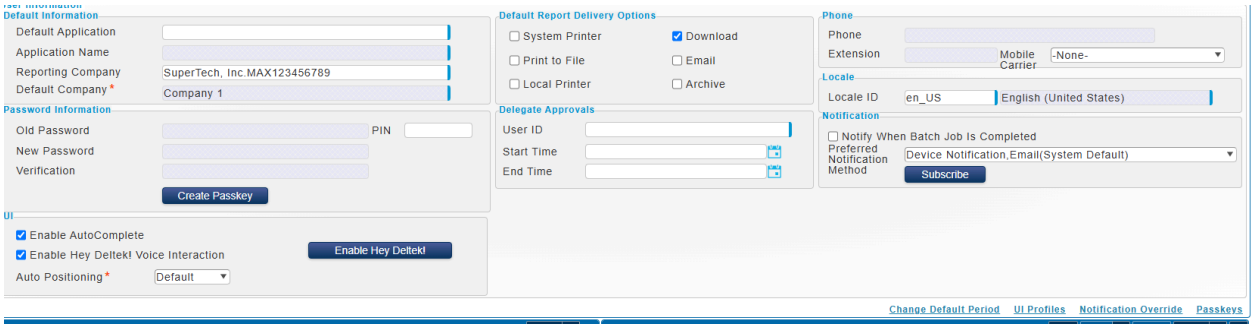
#### Creating a Passkey Via User Preferences

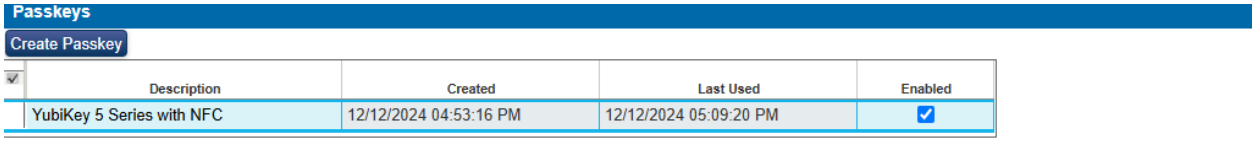
If a user is set up for multiple authentication methods and can log in to Costpoint, the user can create a new Passkey in **User Preferences**.

**To create a Passkey via User Preferences:**

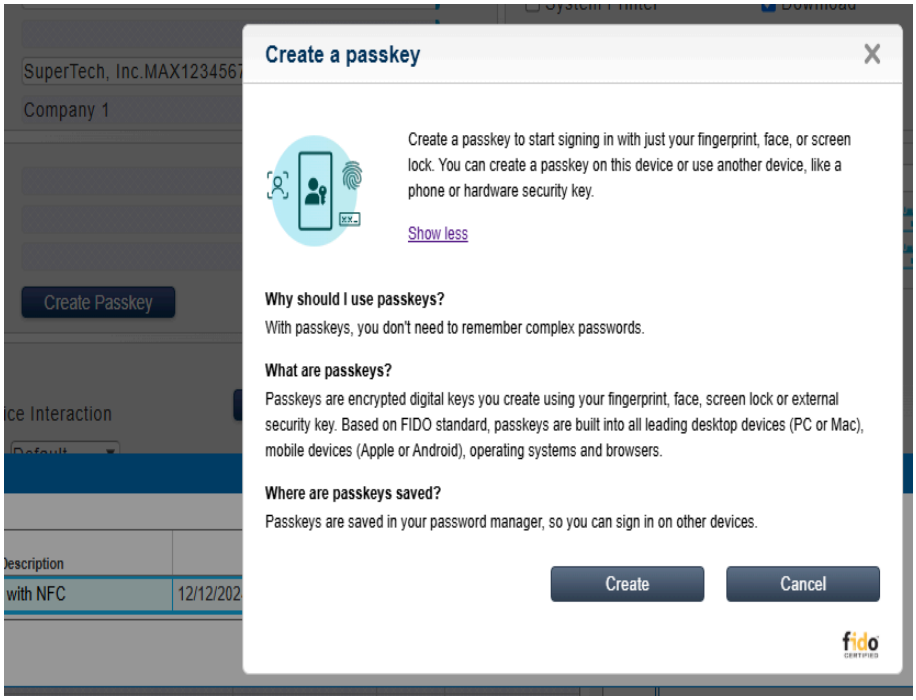
1. Log into Costpoint.

2. Open **User Preferences**.

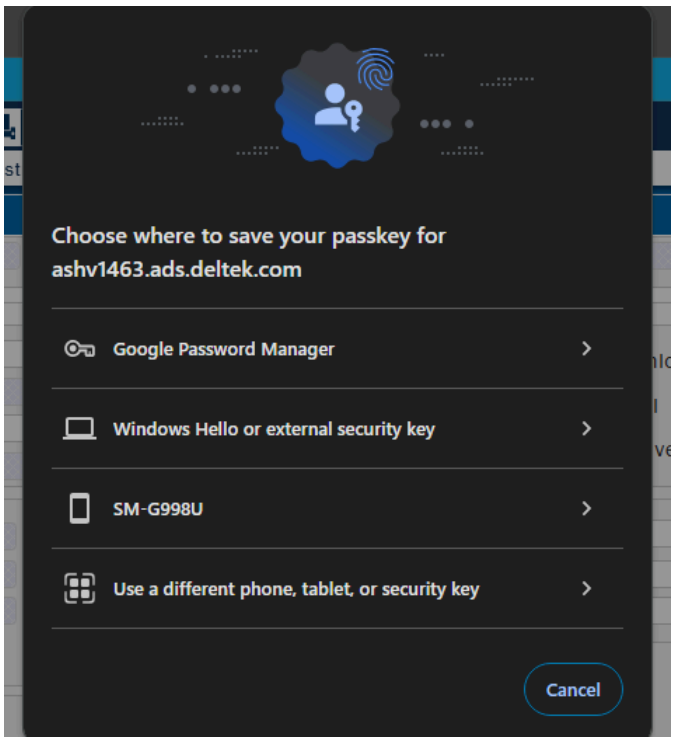


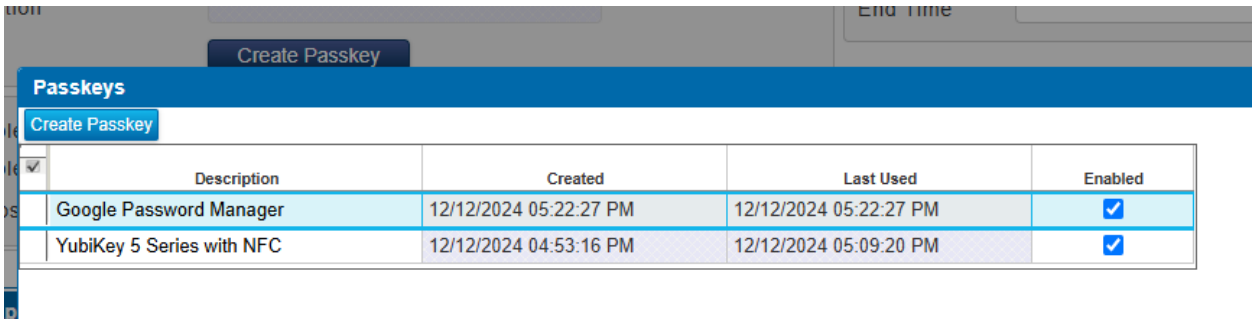

3. Click **Create Passkey** and follow browser instructions.



From that point, the Passkey registration is controlled by the user's web browser and operating system. The user may see other system dialog boxes specific to their web browser and operating system that will help them finish the registration process. For example, a user may be asked to select how to create and save a Passkey.




4. After the registration is completed, you should see a new record saved in **Passkeys** subtask.




### Creating a Passkey Via Email Invite

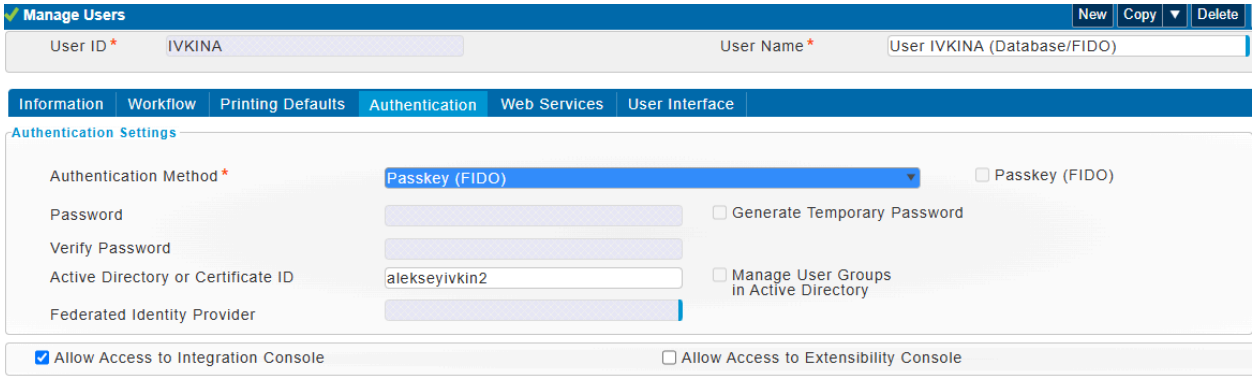
If a user is set up for Passkey authentication only and cannot log into Costpoint using another authentication

method, a System Administrator can send a Passkey registration invite email to the user. The email will contain a link to create new Passkey.

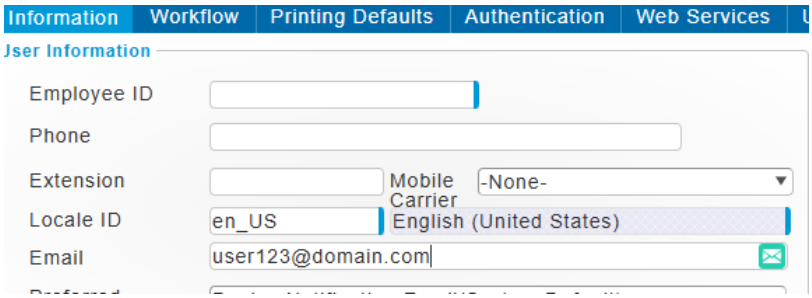
To create a Passkey via email invite:

1. Log into Costpoint as System Administrator.

2. Open **Manage Users** and query single or multiple user accounts set up for Passkey (FIDO) authentication.

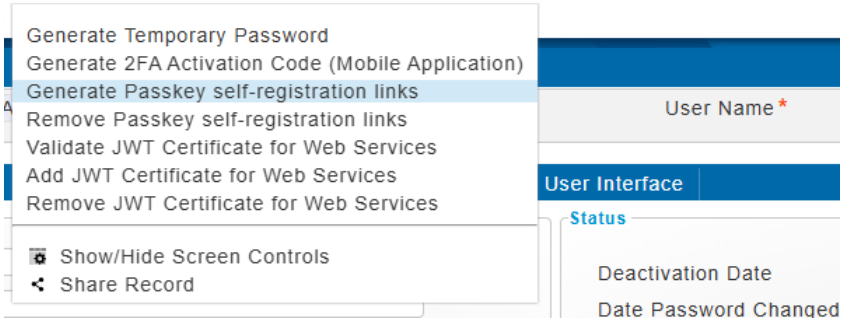



3. Verify that a user has a valid email address entered.



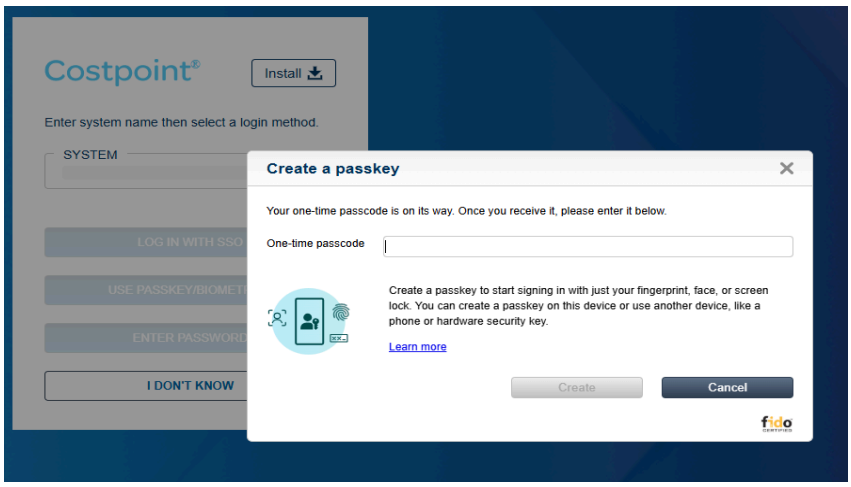

4. Execute the **Generate Passkey self-registration links** action.

   The system will send an email to each affected user. Each email will contain a unique link for that user to create a new Passkey.




5. A user receives a Passkey registration email from Costpoint and clicks the link to create their new Passkey.


6. The web browser opens the **Create a passkey** dialog box.

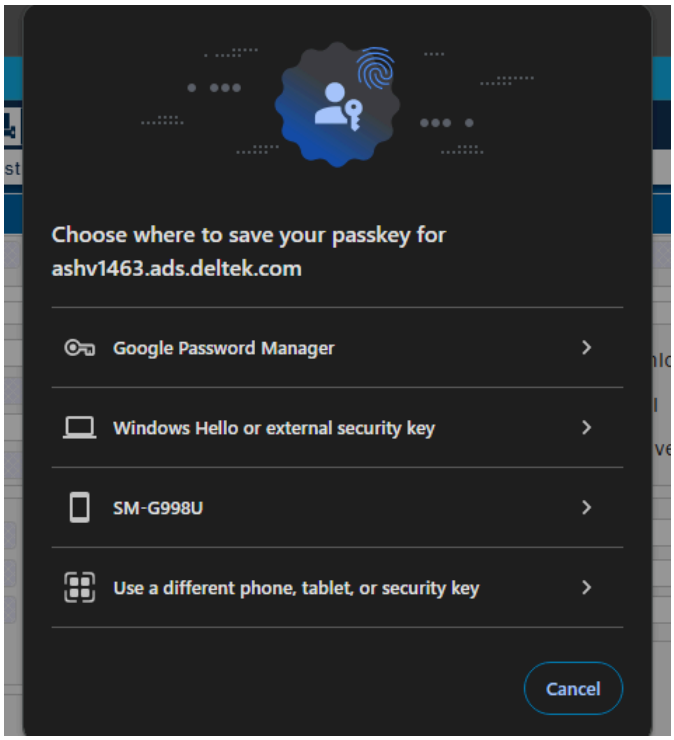



7. The user waits for another email with a one-time security passcode sent for verification purposes.

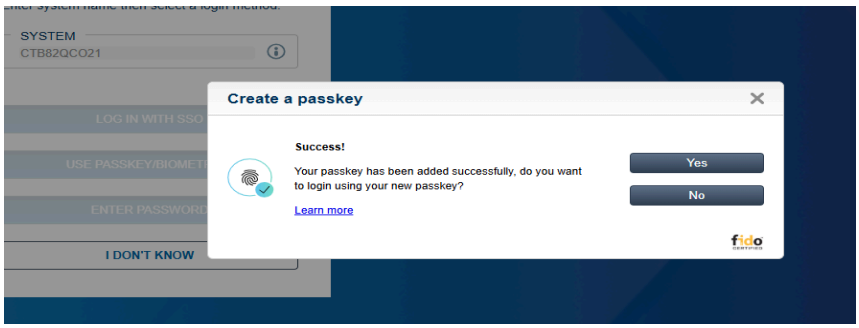
8. Enter the one-time security passcode **Create a passkey** dialog box and click **Create.**

   From that point, the Passkey is controlled by user's web browser and operating system. The user may see other system dialog boxes specific their browser and operating system that will help them finish the

registration process.




9. The user should see the “Your passkey has been added successfully” message and an invitation to log into Costpoint.



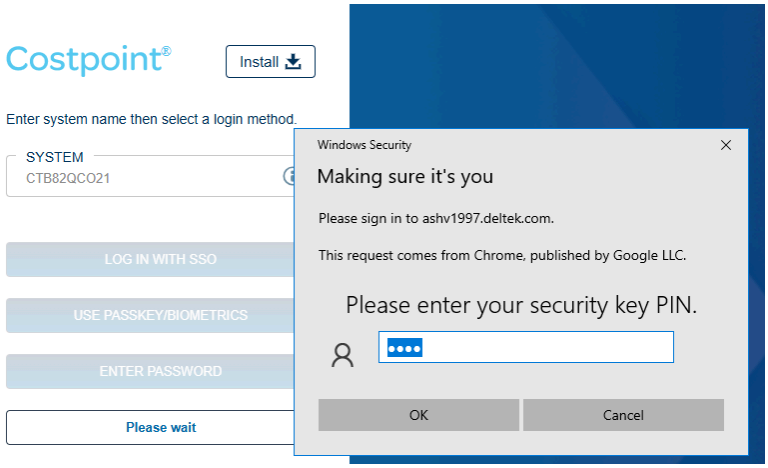

### Login with Passkey

A user can now log into Costpoint with just a simple USB key touch or biometric verification on their phone or laptop.

To log in to Costpoint with a Passkey:

1. Open the Costpoint login page, enter your **USERNAME** and **SYSTEM**, and click **Log In**.

2. You may be asked to touch your security key or provide biometric verification on your phone or laptop depending on what type of Passkey device you are using to log in.




3. After Passkey verification is completed, you will be successfully logged into Costpoint.

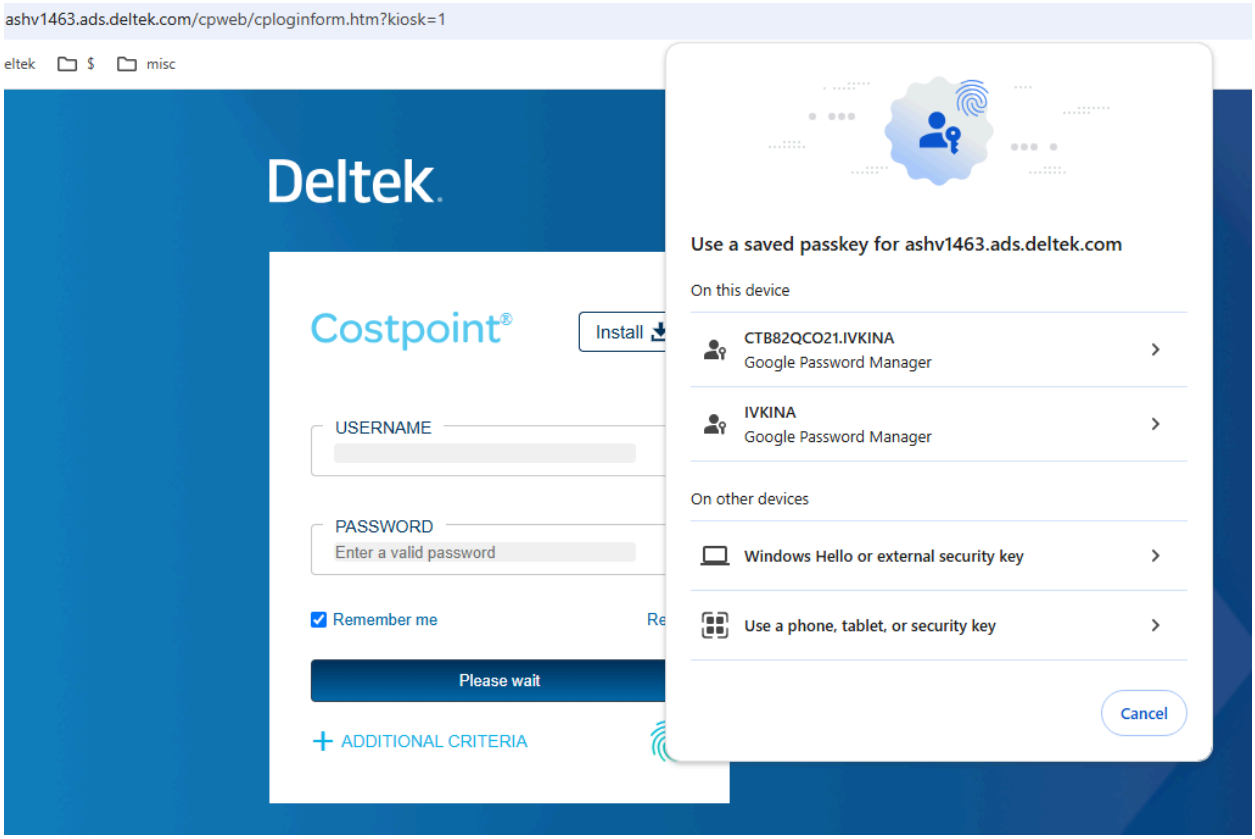
## Username-less Autentication with Passkey (Kiosk Mode)

FIDO standards allow users to experience not just a password-less login but also a login when users do not provide a username on the login page (that is, password-less and username-less authentication). In order to use this feature in Costpoint, the following condition must be met:

- **Users must enter a special "kiosk mode" URL to log into Costpoint.**

Kiosk mode authentication assumes having a single, shared device (for example, a laptop, a tablet pc, or any other mobile device that can run a web browser and is connected to the network). Typically, various users who have their own Passkey devices check into that single, shared by everyone kiosk device to log into Costpoint. The Kiosk Mode URL expects having a special URL parameter **kiosk=1** (for example, https://machineA.subdomain.mycompany.com/CPWeb?**kiosk=1**).

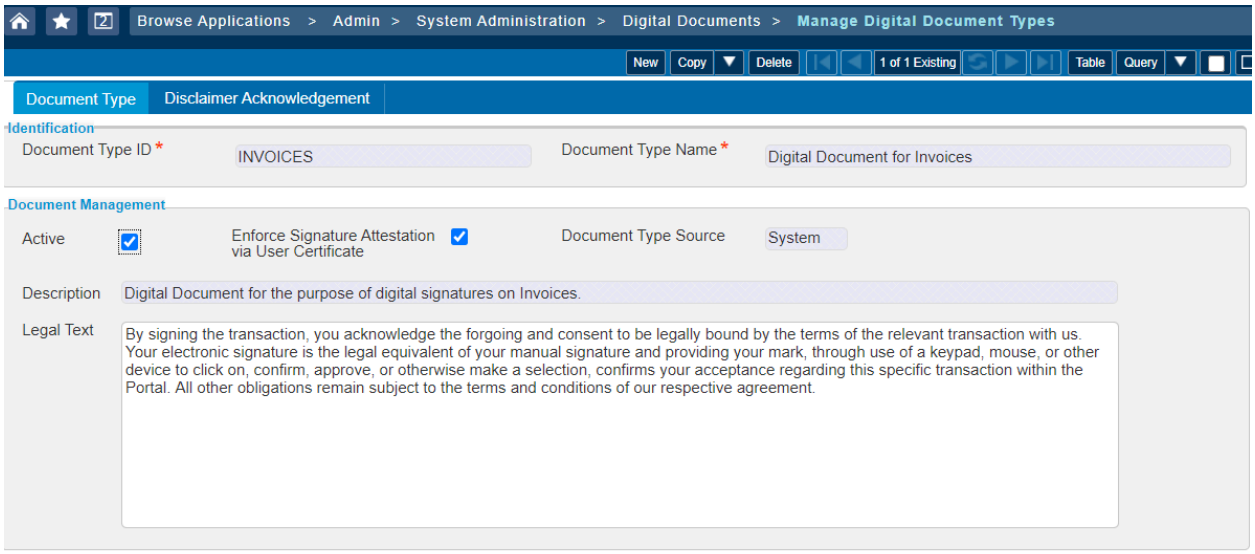
A user clicks the **Login** button on the Costpoint login page without typing a username and password. The system prompts for a user's Passkey credential that could be provided via USB stick or biometrics on the mobile device (for example, face or voice recognition, fingerprint, pin, and so on). Once the Passkey credential is presented and verified, a user is allowed to log into Costpoint.

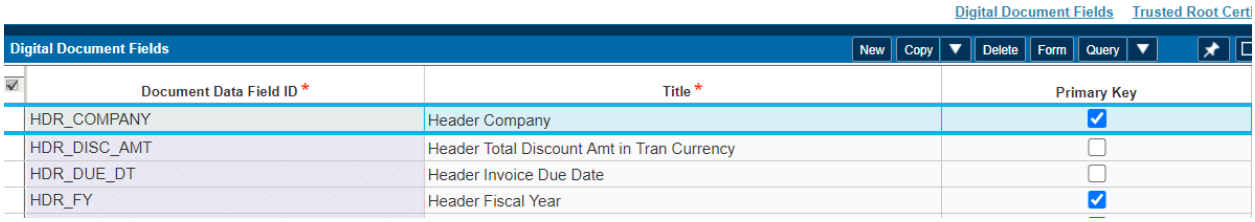


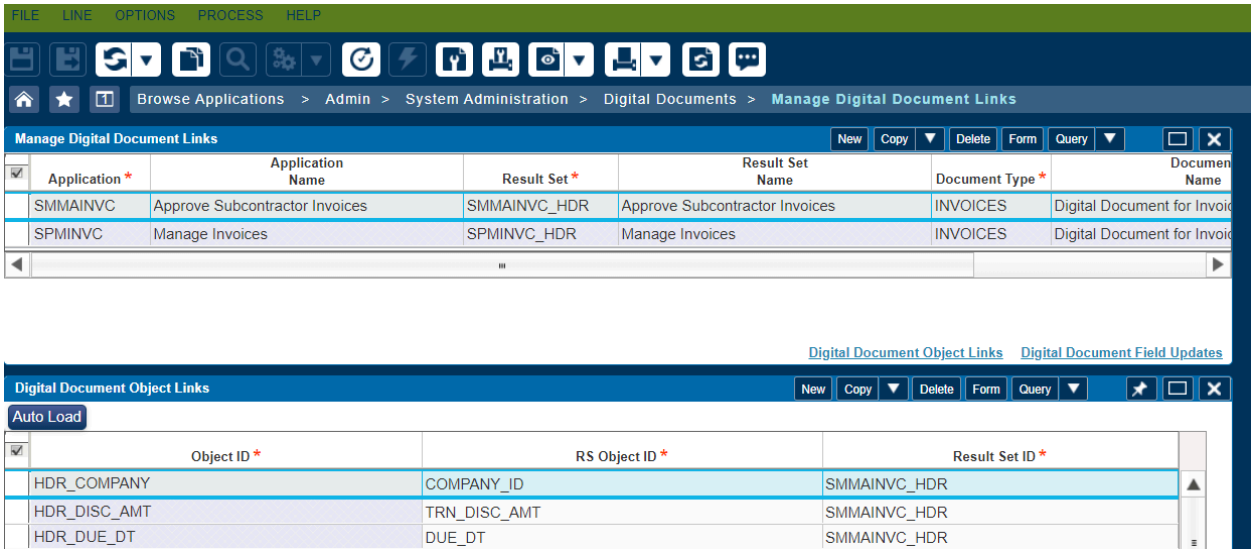

## Digital Signing

Costpoint provides a flexible, self-configurable digital document solution where users can define their own digital document types and choose data that goes into such documents by providing mapping between the document type fields and any existing application (screen) fields. After configuring a digital document, users can digitally sign the document as well as verify the signed data integrity and the validity of an existing signature right on a Costpoint screen using a Passkey.

**Attention:** For more details on digital document setup, refer to the Costpoint Online Help for Manage Digital Document Types and Manage Digital Document Links applications.




**Attention:** For more details on how to register your own Passkey for digital document signing, refer to the Costpoint Online Help for the User Preferences application.

# Authentication Audit Logging

Successful or unsuccessful login attempts can be logged by the system for audit trace purposes. The audit logging is activated by default for the ITAR Cloud environment. For all other environments (DCO or on-premises deployments), the audit logging can be turned on by adding the logging level property **logSigninsLevel** and setting value of this property to **info** in the **enterprise.properties** file.

For example:

- **logSigninsLevel=info**: Logging is activated.
- **logSigninsLevel=off**: Logging is deactivated.

In addition, system administrators can override logging settings by editing **CPLog4j.properties** to enable audit logging only for a specific system.

For example:

**com.deltek.enterprise.Cluster.system.security.signins.CTB81DEV19=info**

If authentication audit logging is activated, the system will create a new log file called **CP_Signins_ServerName.log** and will start recording all successful and unsuccessful login attempts. Logout requests will also be recorded.

The following data will be recorded in the audit log file:

- Login/Log-out Date/Time
- Login URL
- Server Session ID
- System name
- User ID
- Active Directory/Certificate User ID
- Authentication Method
- Authentication Source (Interactive/Web services/API/Mobile)
- Authentication Status (Success or Failure)
- Authentication Failure Reason
- Client Origin IP address

(Sep 03 2021 10:35:20:[[ACTIVE] ExecuteThread: '1' for queue: 'weblogic.kernel.Default (self-tuning)']: INFO eltek.enterprise.DEServer.system.security.signins.CTB81DEO19 ) AuthUtils.java - <|>2021-09-03 10:35:20.186<|>https://us205636.ads.deltek.com:443/LoginServlet.cps<|>rH2sFadedU6sGQLHumqJgSUxRI1uJ6fysL009OnkpdFt8eVfaPFz!118267436?!1630679705454<|>CTB81UI<|>Succeeded<|><|>192.168.35.44<|>

(Sep 03 2021 11:09:10:[[ACTIVE] ExecuteThread: '1' for queue: 'weblogic.kernel.Default (self-tuning)']: INFO eltek.enterprise.DEServer.system.security.signins.CTB81DEO19 ) AuthUtils.java - <|>2021-09-03 11:09:10.417<|>https://us205636.ads.deltek.com:443/LoginServlet.cps<|>rH2sFadedU6sGQLHumqJgSUxRI1uJ6fysL009OnkpdFt8eVfaPFz!1182674367!1630679705454<|>CTB81UI<|>Log-out<|><|>192.168.35.44<|>

# User Access to Modules, Applications, Reports, Etc.

Authorization controls access to resources by answering the following question: “Does a user have rights to access a protected resource?”

In Costpoint, we identify two types of resources that require protection:

- Application business objects
- J2EE server components/services

A security policy must be implemented for each component in the previous lists. A security policy answers the question: “Who has access to a resource?”

| Resource Type | Components | Security Policies Defined By: |
|---|---|---|
| Application business objects | Modules, applications, result sets, actions, and reports | Costpoint security applications such as the following: Manage Users, Module Rights, Application Rights, Report Rights, Report Archive Rights, Action Rights, and Result Set Rights |
| J2EE server components/ services | Web applications, EJBs, JDBC connection pools, JMS servers, Java connectors, and mail sessions | Server administration tools (for example, the WebLogic Server console) |

When Costpoint is installed, only one user account called **CPSUPERUSER** is created. This is s predefined administrative user in Costpoint that has full rights to all modules and applications. We expect clients to login to product under this account and setup additional user groups and users with appropriate privileges in Manage Users and Manage User Groups applications. Keep in mind that those are regular Costpoint applications, and you will need to provide rights for those applications to your Costpoint administrative users, who will be able to change other users’ privileges in Costpoint, create new Costpoint users and groups, and/ or remove unneeded user accounts.

Also, for new installations and for upgrades from previous versions of Costpoint for which the **Apply Default User Groups and Permissions** option was selected, the installation will add an out-of-the-box, predefined set of user groups and permissions. The idea is to help clients by giving them a template of what user groups they

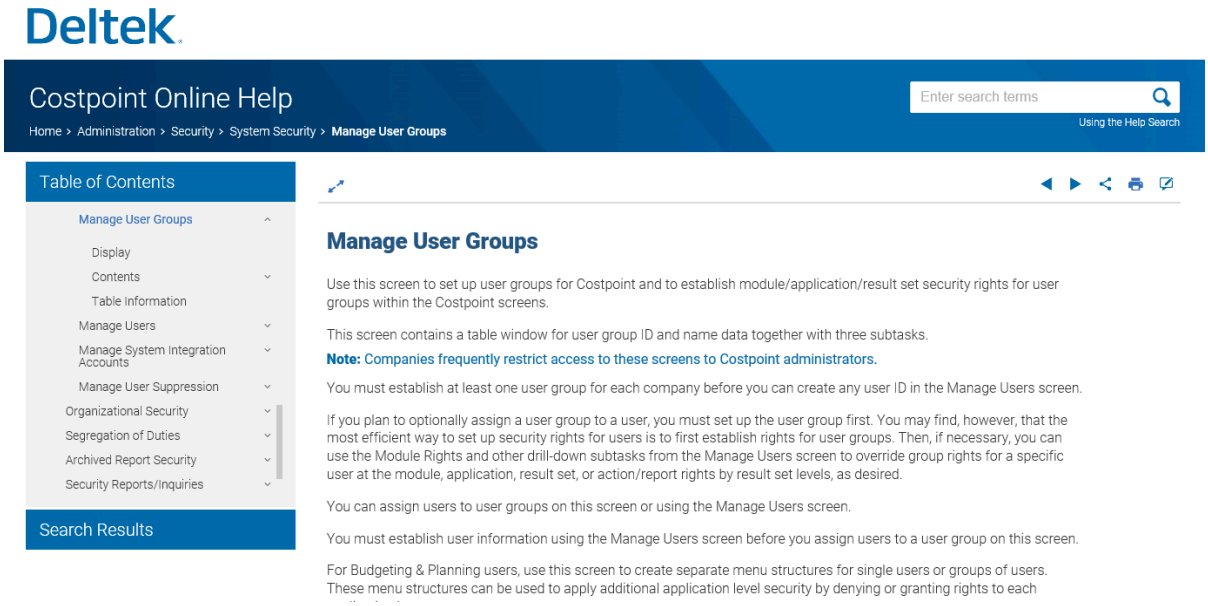
might want to have in the organization and what rights these user groups should typically have. For example, the "AP clerk" user group will be created, which will have all the permissions that one would expect AP clerks should have.

In total, the installation creates 47 user groups that all start with a **STD_** prefix (for example, STD_AP_MGR" - "Accounts Payable Manager," "STD_CM_CLRK" -"Cash Management Clerk," and so on).

### Assign Rights to Application Business Objects

You can control a user's access to application business objects using Costpoint screens and tables for entering and storing security information.

**Note:** The Costpoint Online Help provides detailed instructions for assigning rights to users. Look under **Administration » Security**.




Follow these guidelines:

**Note:** In Costpoint 8, Organization security works the same way as it did in previous client/server versions of Costpoint, using the same screens and database tables.

- A user can be assigned to one or more user groups or to no user groups. In Costpoint 8, security rights defined at the user ID level do not override user group security rights.
- A user or user group can be given module-level security rights that control whether the user or group has **Full**, **Read-Only**, or **Deny** rights to a module in the Costpoint menu. If application security is not specified, module-level security also determines what, if any, access users have to applications within a module.
- A user or user group can be given application-level security rights that control whether the user or group has

**Full**, **Read-Only**, or **Deny** rights to an application in the Costpoint menu. If a user has **Read-Only** rights for a maintenance application, he or she can only view result sets called from that application, regardless of what their result set rights may be. If a user's rights or any of their user group rights are set to **Deny**, the user will not be able to see that application in the Costpoint menu or access it directly.

- An application may be used in multiple modules. If application-level security is not specified for an application for a user and his or her user groups, the access rights of all the modules that contain that application are used to determine if that application can be accessed. If one or more of those module rights is set to **Deny**, the user does not have access to the application.
- Result set security is used to determine the specific activities a user can perform within a given result set. **No, Read, Update**, **Insert**, or **Delete** rights can be given for a maintenance result set. If a result set is used in more than one application, the result set security applies to all applications that call that result set. Result set security will not override application security rights (or module rights if the application security rights are not defined).
- Action security specifies whether or not the user can execute actions for the result set. Rights for actions are either granted or denied. In general, unless **Action** rights are explicitly denied, the user may run actions associated with the result set.
  **Note:** If the result set by design is not Read-Only (in other words, one or more of **Insert**, **Update**, and **Delete** are available for that result set in the Design Tool), and the user has **Read-Only** rights for the result set in the W_RS_RIGHTS table, that user will not be able to execute any actions for that result set, unless they have been explicitly granted rights to those actions. Conversely, if the result set is set to **Read-Only** in the Design Tool, the default behavior is that the user can run actions for that result let unless action rights are explicitly denied.
- Report security specifies whether or not the user can run reports for the result set. Rights for reports are either granted or denied. By default, the user can run any report associated with the result set unless rights are explicitly denied.
- Report archive security specifies whether or not the user can view archived reports. Rights are set at different levels, based on a group of reports, a specific report, or a particular instance of a report. Rights can be set within one company or for all companies. Access to archived reports can be either granted or denied. You can also specify different levels of access, such as view reports, modify archive policy, and delete archived reports. In addition, organization security can be either ignored or taken into account when viewing archived reports. In the latter case, users with different organization security profiles can access the same archived reports.
- Security rights do not need to be explicitly specified in the database at each of the levels in order to fully view/access applications and result sets. If no application security is set up for a user and his or her user groups, module security can be used. If result set security is not defined for a user and his or her groups, application security determines what the user can do in that screen. If action and report rights are not specified, Costpoint allows the user to execute the actions or reports.
- Initially, Lookup result sets (result sets called from another result set using the **Lookup** button) are excluded from result set security because the Lookups do not allow users to modify data.

### User and User Group Assignments

Because users can be assigned to multiple user groups and can have security rights of their own, the logic for determining what a user can access or modify is complex. To determine if a user has rights to access a module, application, or result set, data must be read from the user's own rights as well as the rights of all of the user

groups to which the user belongs.

### Module Security

The following rules are used to determine a user's module security rights:

- If there are no rows for a given module within the W_MODULE_RIGHTS table for a user or the user's assigned user groups, the user cannot view/access that module.
- If in one or more W_MODULE_RIGHTS rows for that user or his assigned user groups, the user is denied access to that module (ACCESS_FL = 9), the user cannot view/access that module.
- If one or more W_MODULE_RIGHTS rows exist for that module and none have the Deny setting (ACCESS_FL = 9) the user can view/access the module.

### Application Security

The following rules are used to determine a user's application security rights:

- If there are no rows for that application within the W_APP_RIGHTS tables for the user or the user's assigned user groups, the application must determine security by checking the module rights for ALL modules that contain that application.
- If there are no rows for modules that contain the application, the user cannot access the application.
- If there are one or more module rows where access is denied (W_MODULE_RIGHTS. ACCESS_FL = 9) for the user or the groups the user belongs to, then the user cannot access the application.
- If there are one or more module rows selected for the user and the user's assigned user groups where access is denied (W_MODULE_RIGHTS. ACCESS_FL = 9).
- If one or more module rows selected for the user and the user's assigned user groups have **Full** access (W_MODULE_RIGHTS. ACCESS_FL = 5), the user can view and change data in the application.
- If one or more module rows exist, but all of the rows' access codes are set to **Read-Only** (W_MODULE_RIGHTS. ACCESS_FL = 1), the user can view the data in the application but cannot change it.
- If one or more W_APP_RIGHTS rows exist for the application and the user and the user's assigned user groups, use the following logic to determine the application rights:
  - If, in one or more W_APP_RIGHTS rows for the user and the user's assigned user groups, the user is denied access to the application (ACCESS_FL = 9), the user cannot view/access that application.
  - If, in one or more W_APP_RIGHTS rows for the user or the user's assigned user groups, the user is given **Full** rights to the application (ACCESS_FL= 5), for process applications, the user will be allowed to run processes that update the database.
  - If one or more W_APP_RIGHTS rows exist and they all have an access code of **Read-Only** (ACCESS_FL =1), the user can access and view the application, but not change data (even if the result set security would normally allow it). For process applications, the user can generate reports, but cannot perform processes that update the Costpoint database.

### Result Set Security

The following rules are used to determine a user's result set security rights:

- If a user has **Full** access to an application, result set security is used to determine which result sets the user can view, add, change, or delete. If the user has **Read-Only** access to an application, result set security is used only to determine which result sets the user can view.
- If there are no rows for the result set within the W_RS_RIGHTS tables for the user or the user's assigned user groups, the application/module security determines the user's rights to result sets within a given application.
- If the user has **Full** rights to an application (or module if no application rights are defined), the user can select, insert, update, and delete rows within all result sets for that application.
- If, in one or more W_RS_RIGHTS rows for the user or the user's assigned user groups, the user is denied access to a result set (DENY_FL = Y), the user cannot view or update data in that result set.
- The user can view rows in the result set if one or more selected rows in the W_RS_RIGHTS table has the SELECT_FL = Y. The user can insert, update, and delete rows in that result set if one or more of the selected rows' INSERT_FL, UPDATE_FL, and DELETE_FL are set to **Y**, respectively (if they also have **Full** rights to that application).

### Action Security

The following rules are used to determine a user's result set security rights:

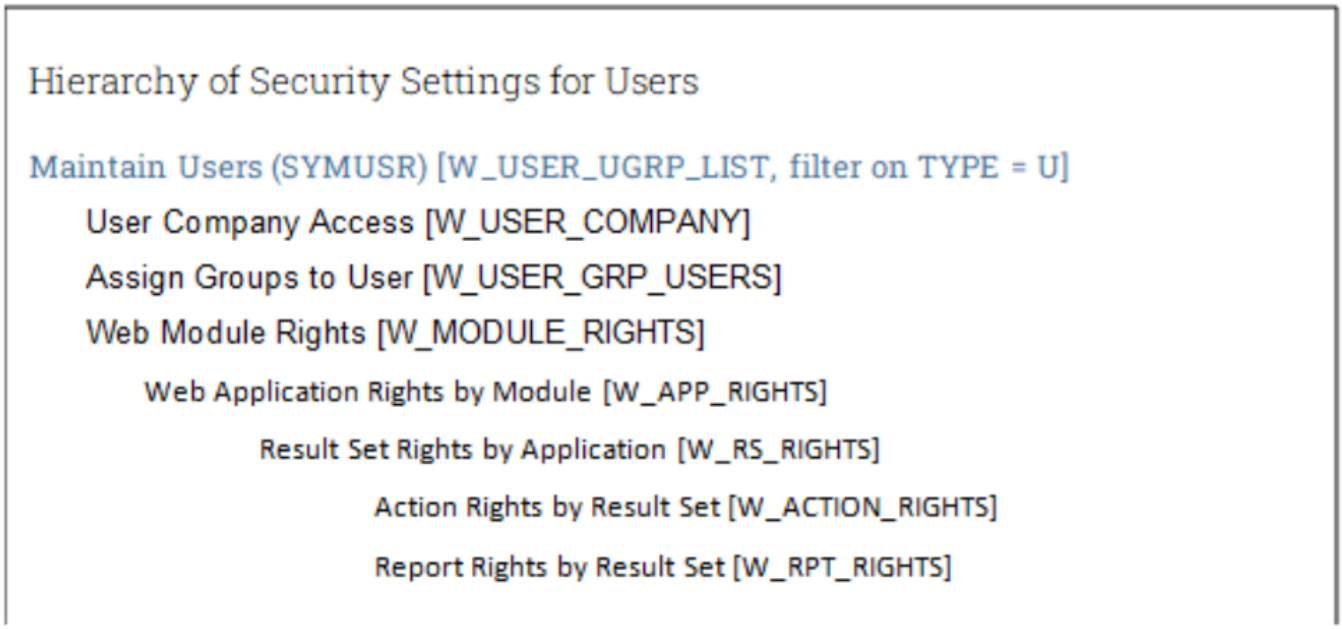
- If a user has full access to a result set, result security is used to determine which actions the user can execute.
- If the result set is **Read-Only** by design (INSERT_FL, DELETE_FL, and UPDATE_FL are all **N** in S_RS_LIST), then, by default, the user can execute any action, regardless of data in the W_RS_RIGHTS table.
- If the result set is not **Read-Only** by design (one or more of INSERT_FL, DELETE_FL, UPDATE_FL are set to **Y** in S_RS_LIST) and the user has **Read-Only** access in W_RS_RIGHTS, the user will not be allowed to execute any actions on that result set unless rights are explicitly granted to him or her in W_ACTION_RIGHTS.
- In all other cases in which the user has rights to the result set, if the EXEC_FL is **N** in W_ACTION_RIGHTS for the action, the user cannot execute the action; if the EXEC_FL is **Y** in W_ACTION_RIGHTS or there are no rows in W_ACTION_RIGHTS for that result set, the user may execute the action.

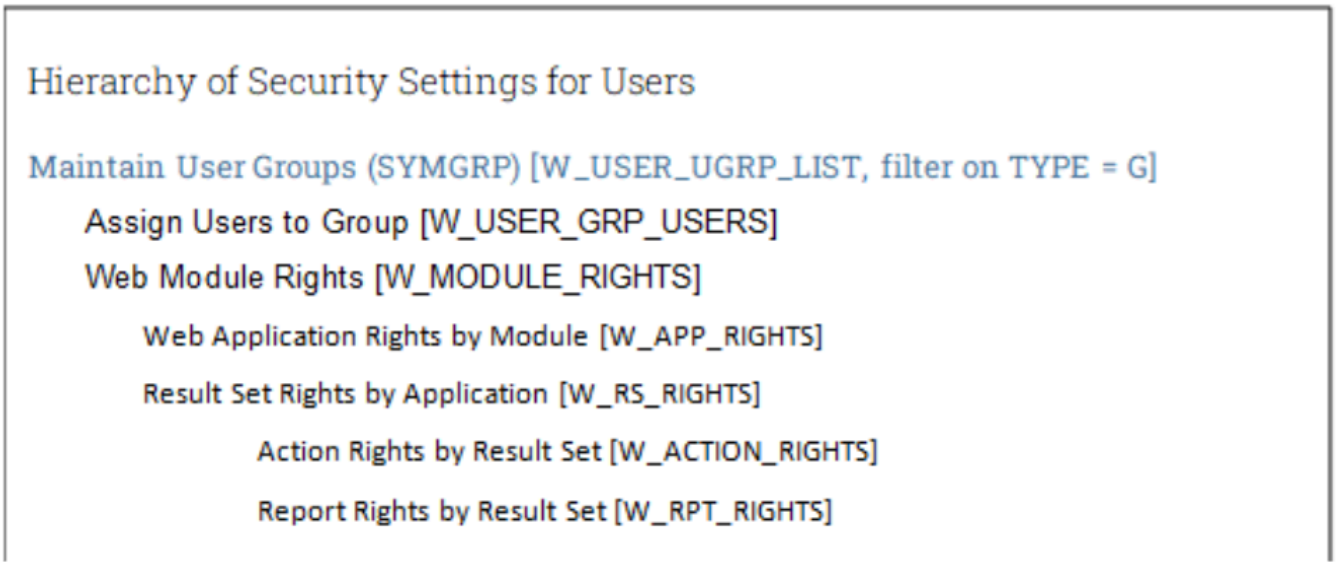
### Report Security

If the user has any access at all to the result set, he or she may run any report associated with that result set unless there is a row in W_REPORT_RIGHTS with EXEC_FL = 'N' for that report.

### Hierarchy Diagrams

The diagrams below show the hierarchy of security settings for individual users and user groups.




**Note:** There are a few restrictions in the Application Security override of result set security:

- If a user has no access to an application, he or she cannot view any result sets from within that application, no matter what result set security access he or she has.
- If a user has **Read-Only** access to an application, he or she cannot modify data in any result set from within that application, even if the user has **Full** rights to the result set. However, the user may be able to view those result sets from other applications.

### Implementing Security for J2EE Server Components and Services

The Costpoint application runs on a J2EE server (for example, a WebLogic Server) and uses the following J2EE

components and services:

- Web application
- EJB
- Java connector
- JDBC service
- JMS service
- Mail service

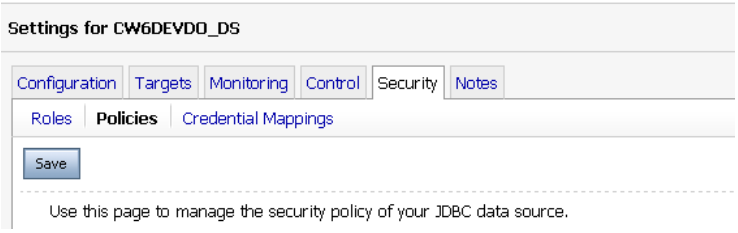
Each of these components and services must be protected; there are security polices implemented for each component. Implementation of these polices is vendor-specific.

### WebLogic Server Implementation

Security policies for the WebLogic server are defined at the user level. Costpoint ships with some built-in users that support these security policies:

- **reportDataUser**: This user accesses the report bean during report generation.
- **reportBeanUser**: This user is used to run the report bean through the run-as property in the bean's Deployment Descriptor.
- **masterBeanCreator**: This user is used to create the master bean through the login bean.
- **asyncProcessUser**: This user is used for running processes and reports asynchronously or through the process server.
- **RDBMSRealmAuthenticator**: This user is used to access JDBC pools during the login process.

Security policies for these components and services are defined through the WebLogic console. For more details, log into the WebLogic console, select the targeted component or service, and go to the **Security/Policies** tab. For example, this is the security policy for a JDBC connection pool:



**Policy Used By Default**

Group : ApplicationUserGroup

Or

User : RDBMSRealmAuthenticator or reportBeanUser or masterBeanCreator

Or

Role : Admin

**Warning:** To achieve maximum security, Costpoint ships with WebLogic security policies pre-configured for built-in Costpoint users and user groups. Do not modify security policies to decrease the rights given to built-in users or user groups.