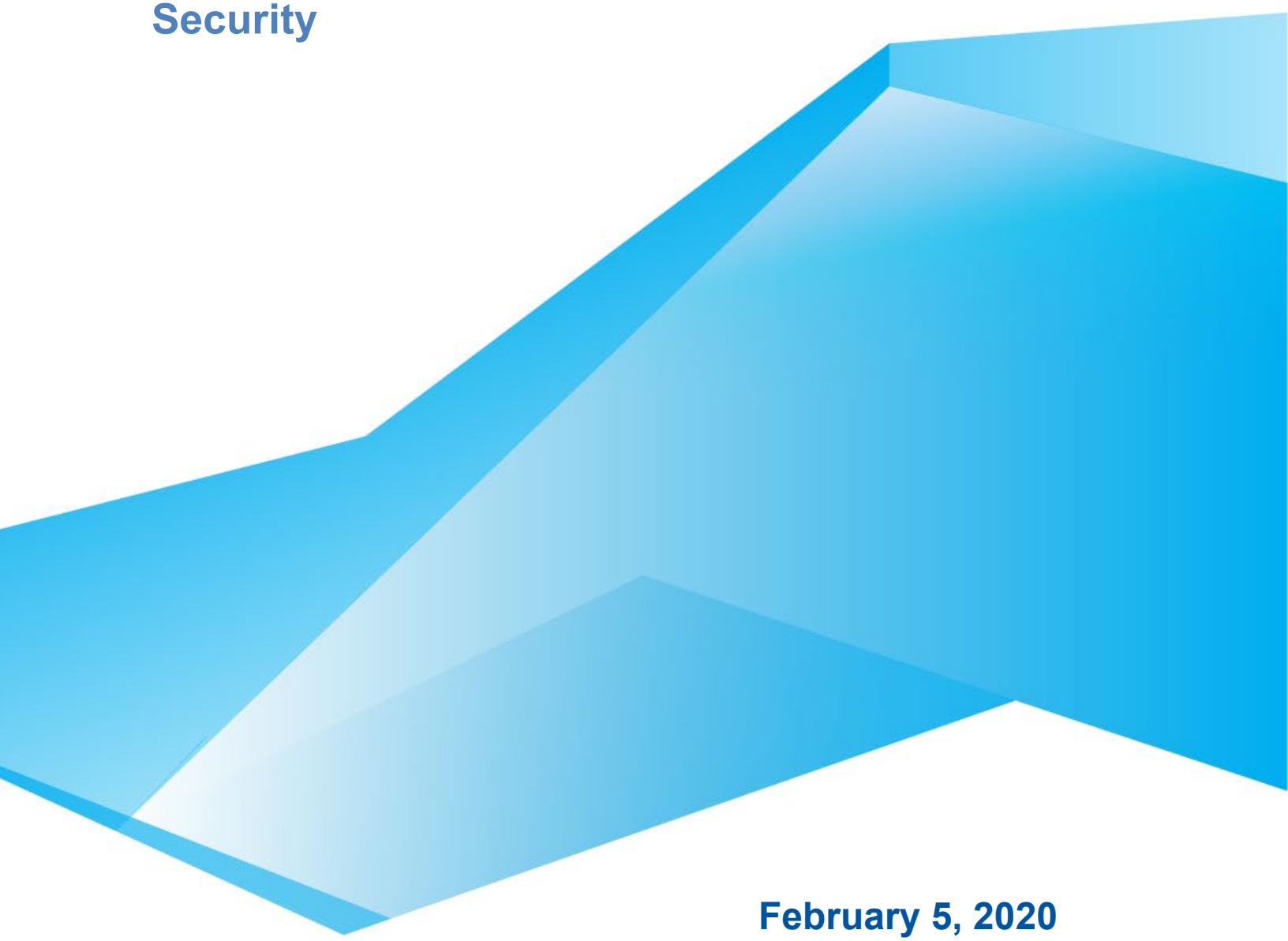
Deltek Know more. Do more.™

# Deltek Costpoint® 7.1.1

## Security



**February 5, 2020**

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.

The information contained in this publication is effective as of the publication date below and is subject to change without notice.



This edition published February 2020.

# Contents

# 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.

# Description of Authentication Methods

## Database

This authentication method supports all Costpoint users—it is the default authentication method. With this method, all passwords are checked against the Costpoint database.

Database verification requires no extra configuration efforts.

## Single Sign-on (Windows AD/Kerberos)

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.

## Single Sign-on (SAML)

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.

## 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.

## 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).

## 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)**: 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.

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

## 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.

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 (SSO)

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.

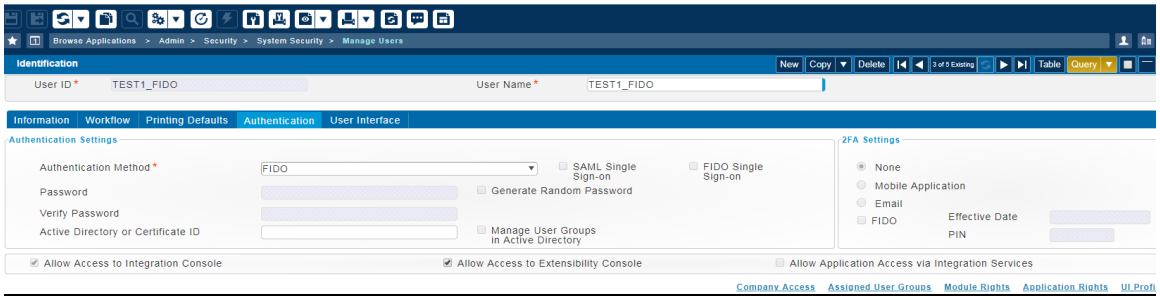
# Assign Authentication Methods to Users

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: Single Sign-on, Active Directory, Single Sign-on or Active Directory, Single Sign-on or Database, Windows Domain and Active Directory, and Certificate SSO.
- Using certain authentication methods (including Single Sign-on, Active Directory, Single Sign-on or Active Directory, 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**.



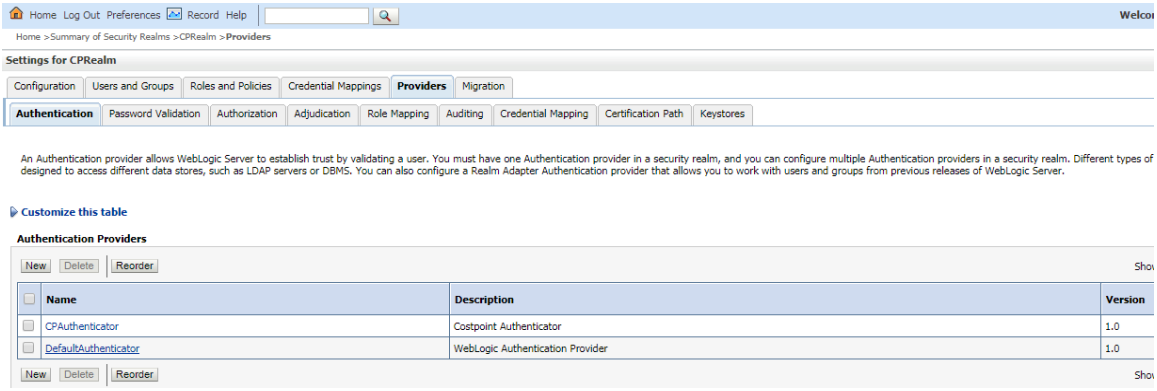

2. Select a user.
3. Click the Authentication tab.
4. Enter the following Authentication Settings:
   - **Authentication Method**: Select the user authentication method (for example, **Database** or **Single Sign-On**).
   - **Password**: Enter the user password (required for Database and Windows Domain 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 or SAML), Active Directory, Single Sign-on or Active Directory, Single Sign-on or Database, Windows Domain and Active Directory, Windows Domain and Database, and Certificate SSO 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 authentication for Costpoint users, including Active Directory, Database, 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

## 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.
- An integration client user identity must use the Database or Active Directory authentication methods. Additionally, the **Allow Application Access via Integration Service** check box must be selected.

The Costpoint system name must be sent concatenated with the user ID (for example, DELTEKPROD__SMITH).

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

# 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 user name/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 **FIDO Security Key** instead of having one-time passcodes. With Security Key, 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 then sends it to a user's email address. During login, the user enters the one-time passcode from the email along with their user name/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.
- **FIDO**: 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 FIDO 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.

  FIDO/biometric devices 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 passcodes to them instead of Costpoint. FIDO 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 the FIDO standard is supported by the latest Chrome, Edge, Safari, and Firefox browsers. FIDO is not supported on Internet Explorer 11.

## 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

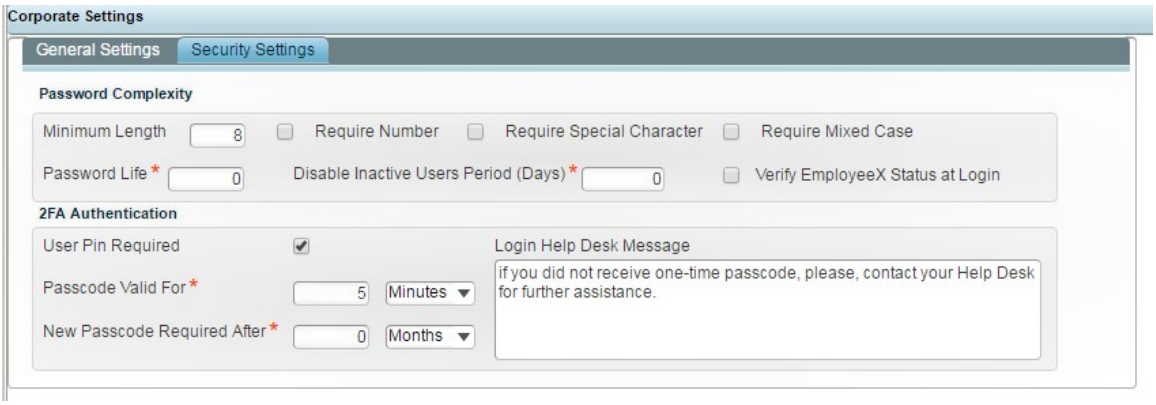
2FA can be enabled for a user with authentication method that requires entering user name/password combination on login page. Such methods are Database, Active Directory, Single Sign-on or Active Directory, Single Sign-on or Database, Windows Domain and Active Directory, Windows Domain and Database.

## 2FA System Settings

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

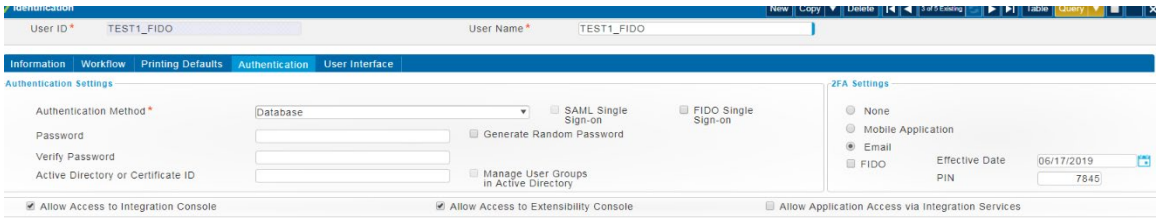
- **User PIN Required**: Selecting this check box indicates that the user's PIN is required during the login process.
- **Passcode Valid For**: This setting determines the time interval during which the passcode is valid.
- **New Passcode Required After**: This setting determines the time interval for 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.



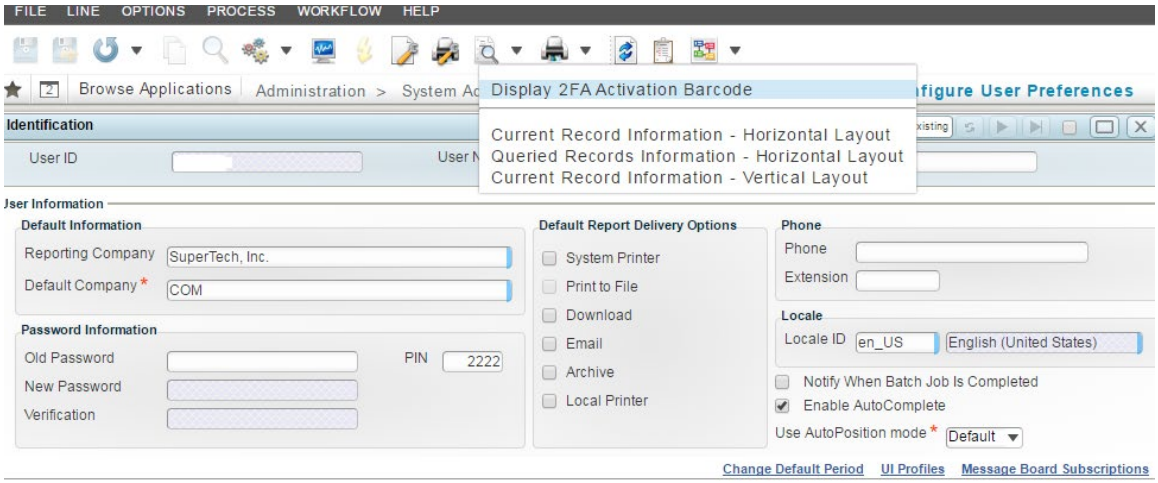

## 2FA User Setup

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 **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.



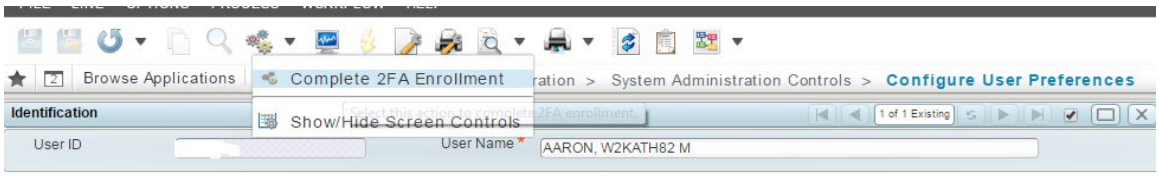

With the 2FA **Email** option, the 2FA login mode is effective immediately. Next time a user tries to log in to the system, a temporary passcode will be required.

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.

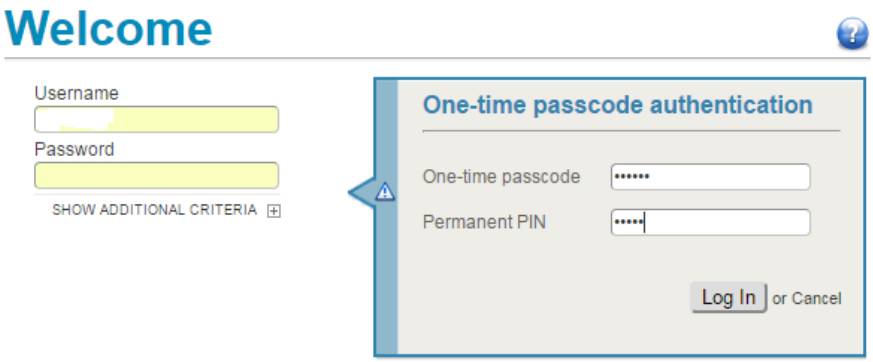




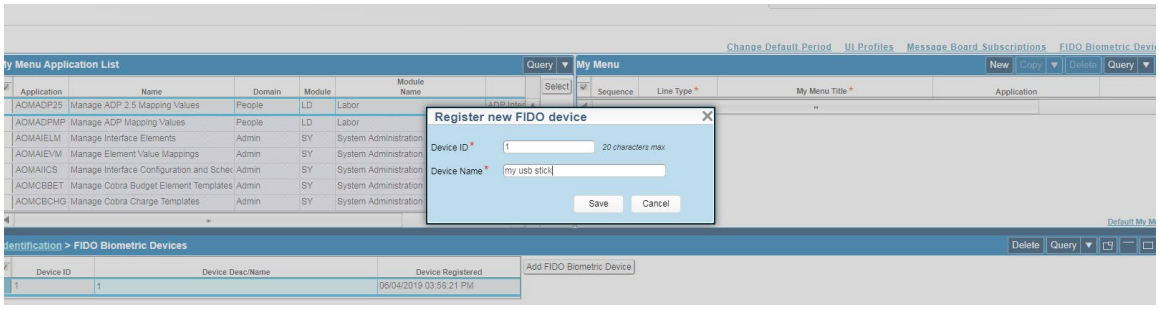
And finally, the user has to run the **Complete 2FA Enrollment** action, which will enable 2FA mode.



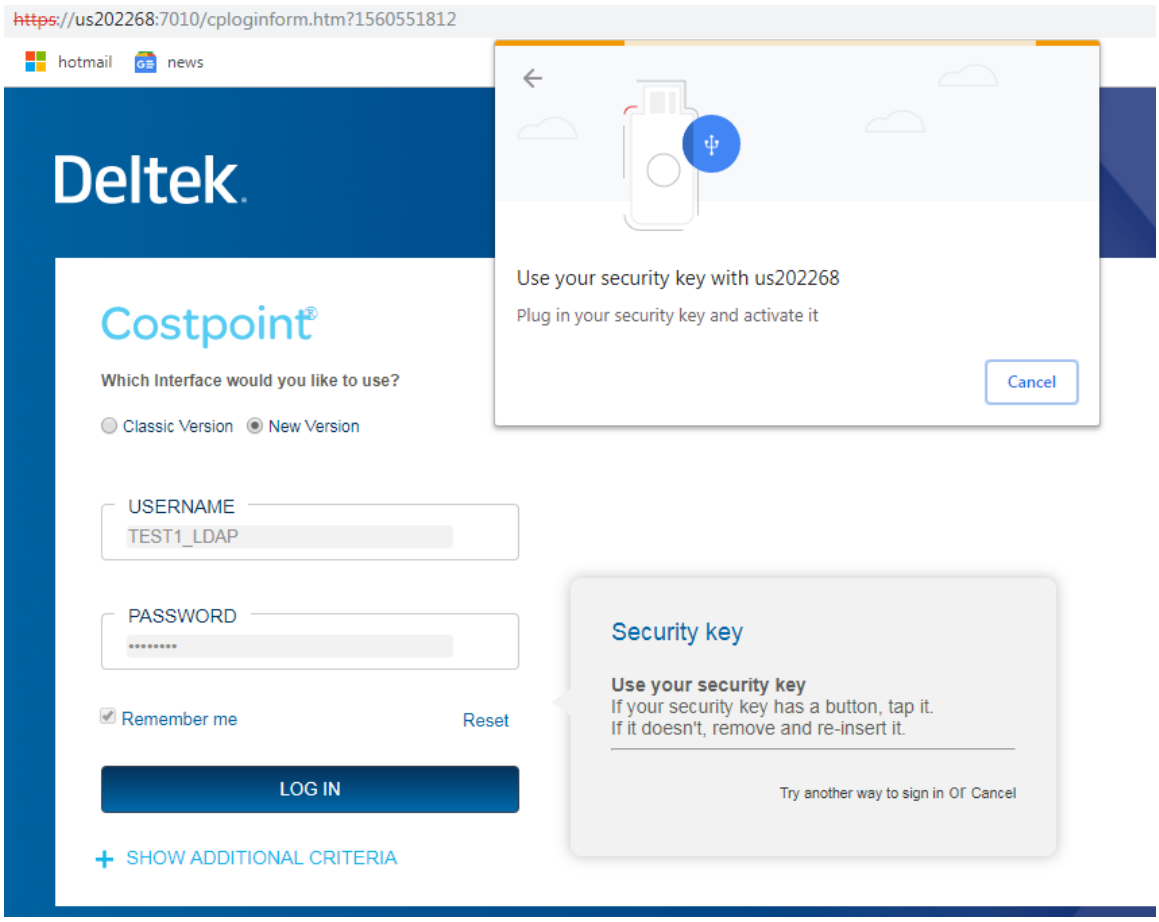
The next time the user tries to log in to the system, a temporary passcode will be required.




With the 2FA **FIDO** mode, additional steps are also required to complete the 2FA enrollment. First, **FIDO** 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 **FIDO**. 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 FIDO device in **User Preferences** by clicking the **Add FIDO Biometric Device** button on the **FIDO Biometric Devices** subtask and following the onscreen instructions.




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

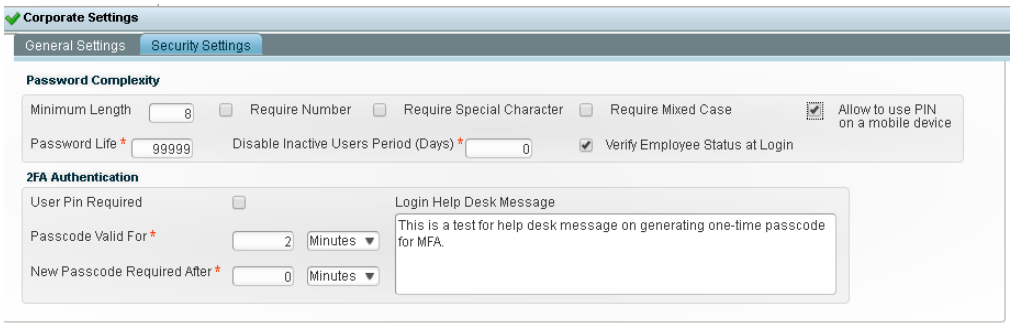

https://us202268:7010/cploginform.htm?1560551812
hotmail
news
Deltek
Costpoint®
Which Interface would you like to use?
Classic Version
New Version
USERNAME
TEST1_LDAP
PASSWORD
Remember me
Reset
LOG IN
SHOW ADDITIONAL CRITERIA
Use your security key with us202268
Plug in your security key and activate it
Cancel
Security key
Use your security key
If your security key has a button, tap it.
If it doesn't, remove and re-insert it.
Try another way to sign in
Cancel

# PIN Authentication on Mobile Device

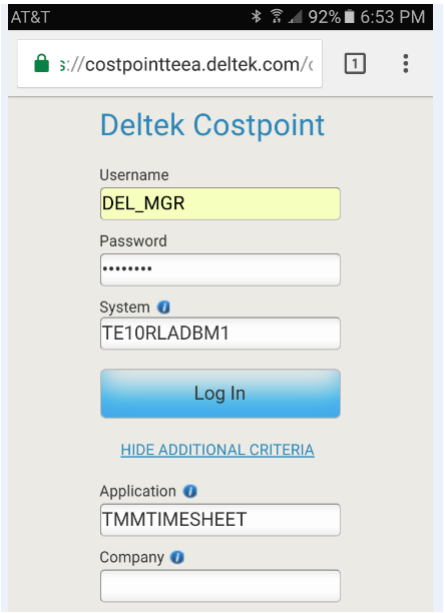
Users that run Costpoint on mobile devices may be able to log into the product by just providing a 4-digit PIN instead of a password. This feature must first be enabled/allowed by the System Administrator in the Configure System Settings application.

**To enable Login with PIN on a mobile device**:

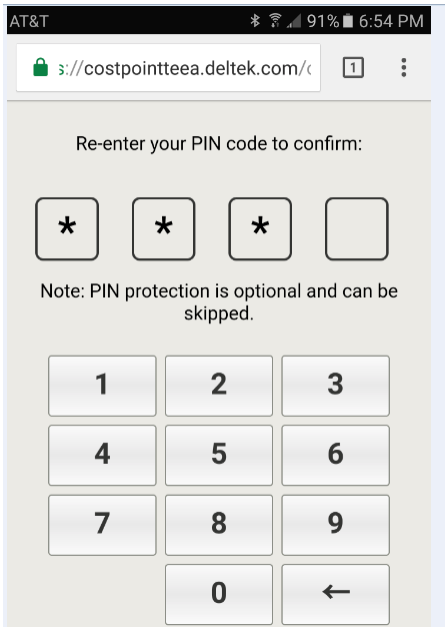
1. Click **Administration » Security » System Security » Configure System Settings**.
2. Go to the Corporate Settings subtask, and click the Security Settings tab.
3. Select the **Allow to use PIN on a mobile device** check box, and save changes.



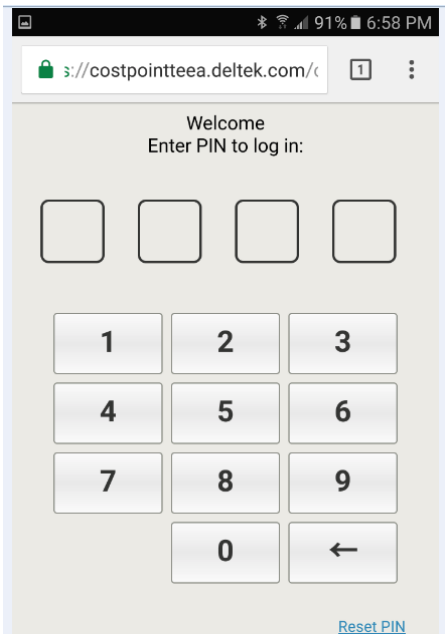

At the very first login only, a user on a mobile device will still be prompted to provide a password to verify their identity.

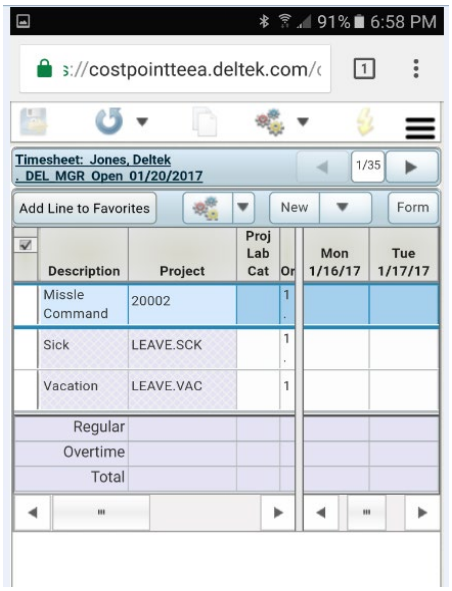


After the correct password is provided and verified, the user will be given the option to store PIN for next login.




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.




91% 6:58 PM
s://costpointteea.deltek.com/
Timesheet: Jones, Deltek
. DEL_MGR Open 01/20/2017
1/35
Add Line to Favorites
New
Form
Description
Project
Proj Lab Cat
Mon 1/16/17
Tue 1/17/17
Missle Command
20002
Sick
LEAVE.SCK
Vacation
LEAVE.VAC
Regular
Overtime
Total

# 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 |
| FIDO | None |
| Single Sign-On (SAML) | SAML Setup |
| Single Sign-On (Windows AD/Kerberos) | Single Sign-On Setup (Windows AD/Kerberos) |
| Single Sign-on or Active Directory | Single Sign-On Setup (Windows AD/Kerberos) + Windows Active Directory Setup |
| 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 Directory Setup |
| Windows Domain and Costpoint Database | Single Sign-On Setup (Windows AD/Kerberos) |
| Certificate SSO | Certificate install on the client machine |

# Windows Active Directory Setup

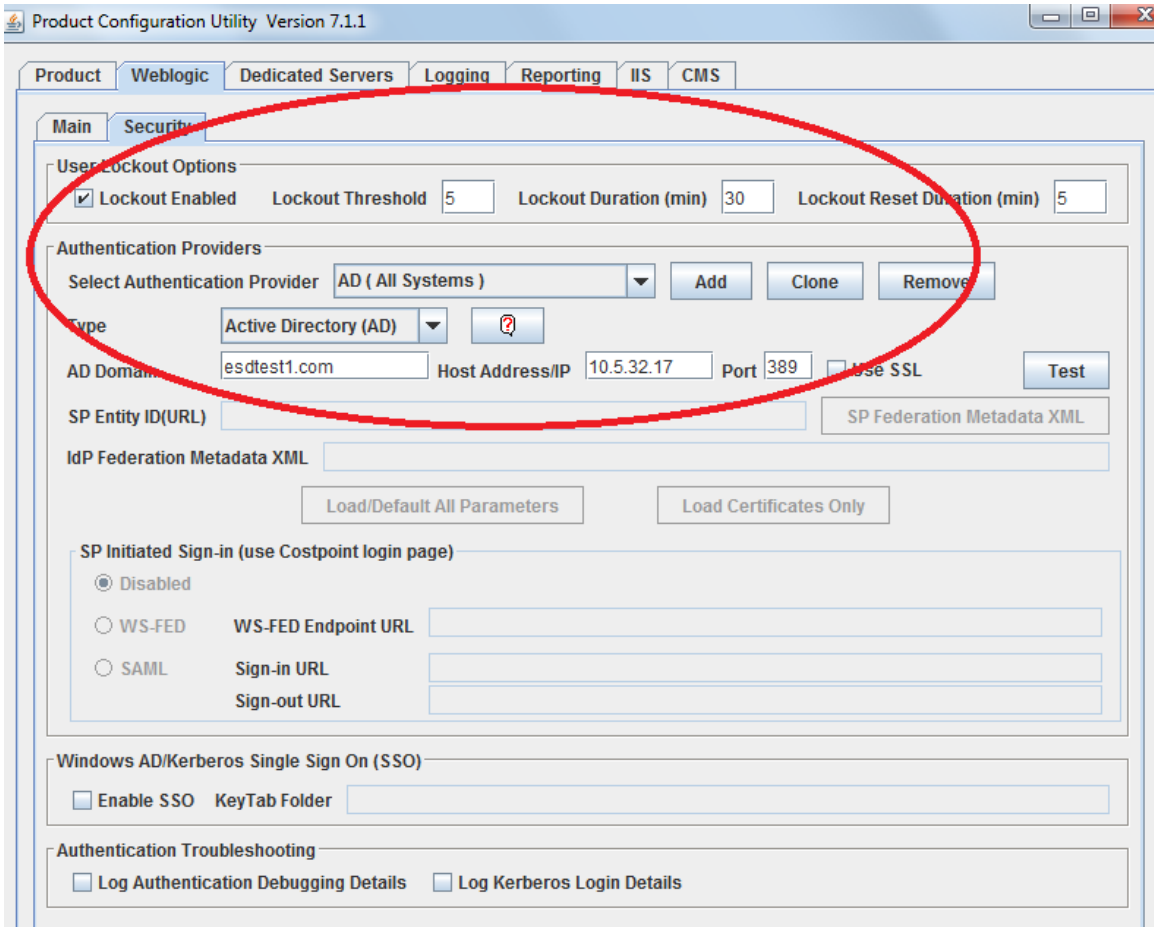
**To enable authentication of Costpoint users with Windows Active Directory**:

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.

   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.



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

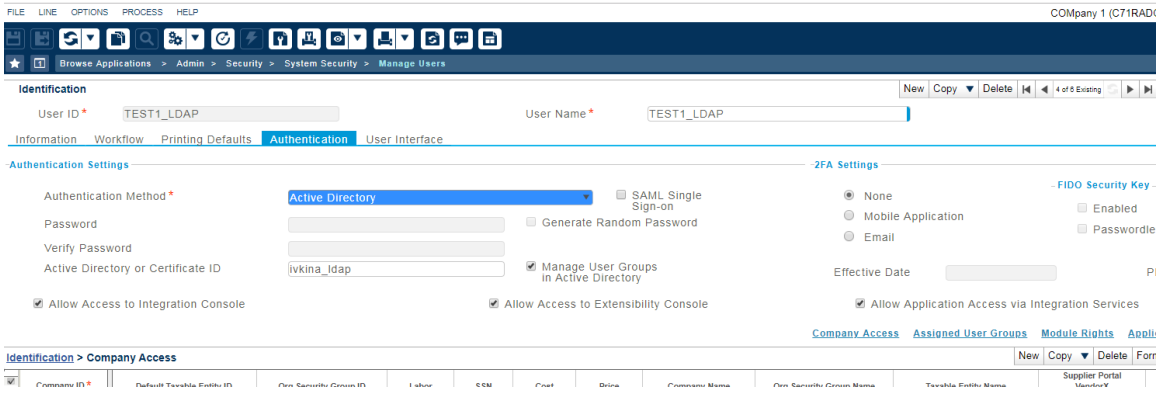
You can configure multiple LDAP servers/domains. A user will be authenticated against each server/domain until authentication succeeds.

## 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.



# Manage User Groups in Active Directory

As part of Active Directory (AD) setup, the Costpoint Administrator can also configure a user to synchronize AD groups with Costpoint groups. In this case, any changes in a user's group membership done in AD will be reflected in their group membership in Costpoint. The synchronization occurs each time users log into Costpoint. Costpoint supports this feature for most authentication methods except for Database and Certificate SSO. Those two methods are not related to user setup in AD.

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

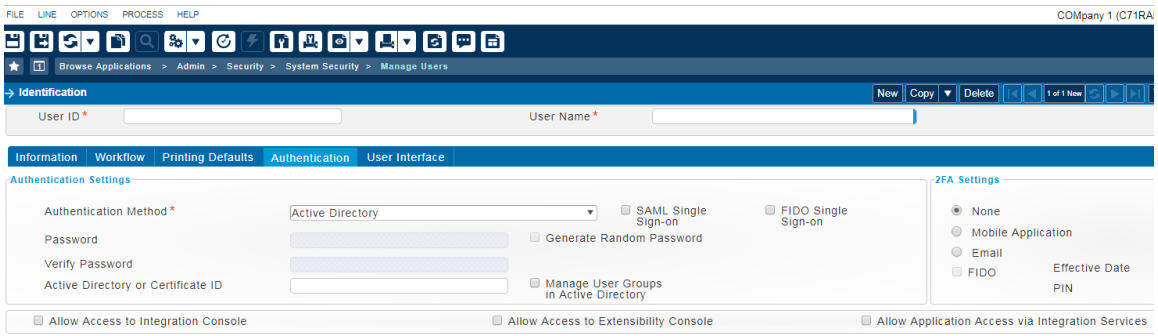
For all Single Sign-on authentication methods (such as Single Sign-on, Single Sign-on or Active Directory, Single Sign-on or Database, Windows Domain and Active Directory, Windows Domain and Database), the AD groups are also retrieved right at login but the retrieval process is slightly different. Kerberos 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 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.

**To manage User Groups in Active Directory**:

1. Click **Administration » Security » System Security » Manage Users**.
2. Select a user.

   One of the following authentication methods must be enabled:

   - Active Directory
   - Single Sign-on
   - Single Sign-on or Active Directory
   - Single Sign-on or Database
   - Windows Domain and Active Directory
   - Windows Domain and Database
3. Click the Authentication tab.
4. Select the **Manage User Groups in Active Directory** check box.



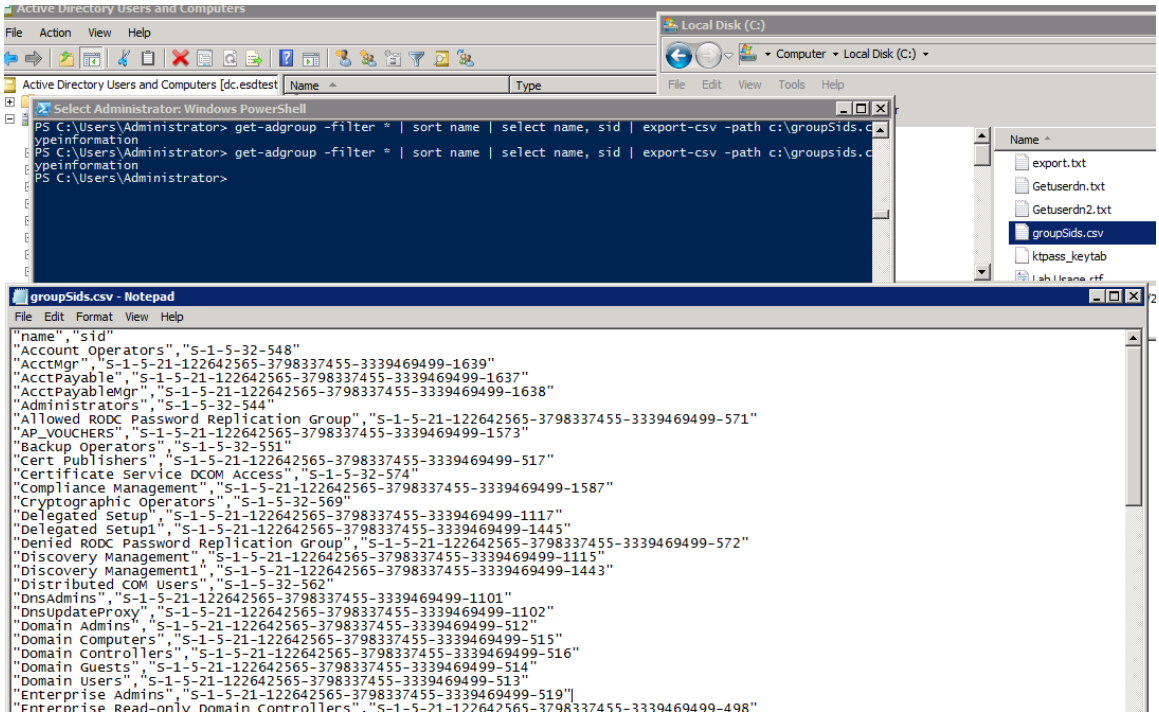

5. Repeat above steps for any users who should have Manage User Groups in Active Directory on.

6. Click **Administration » Security » System Security » Manage User Groups**.
7. If your users use Active Directory authentication method only and not a Single Sign-on (Windows Kerberos/AD) method, skip step 8 and proceed to step 9.
8. If your users use a Single Sign-on (Windows Kerberos/AD) 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:

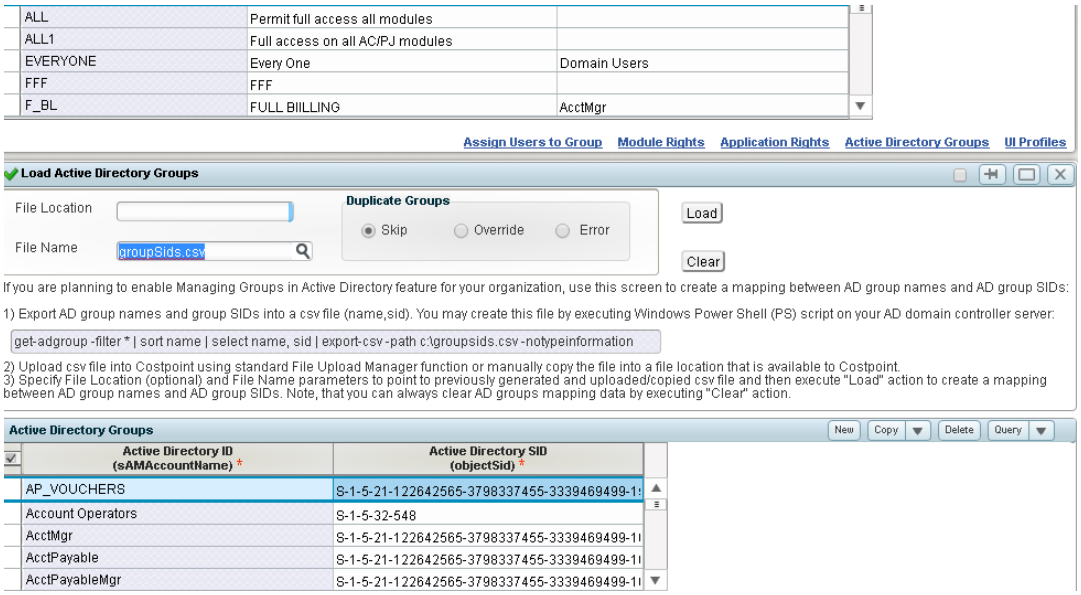
      ```
      get-adgroup -filter * | sort name | select name, sid | export-csv
      -path c:\groupsids.csv -notypeinformation
      ```

      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**.**



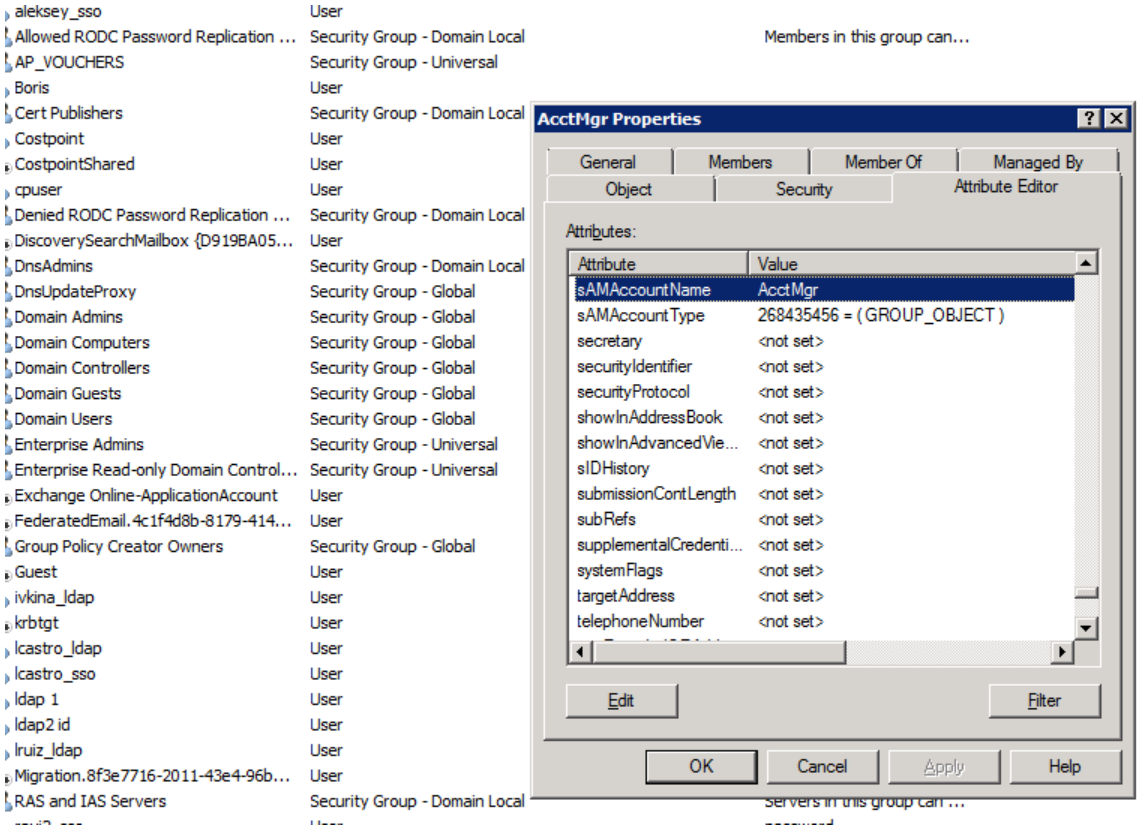

d. Specify the **File Location** (optional) and the **File Name** parameters to point to previously generated and uploaded/copied csv file

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

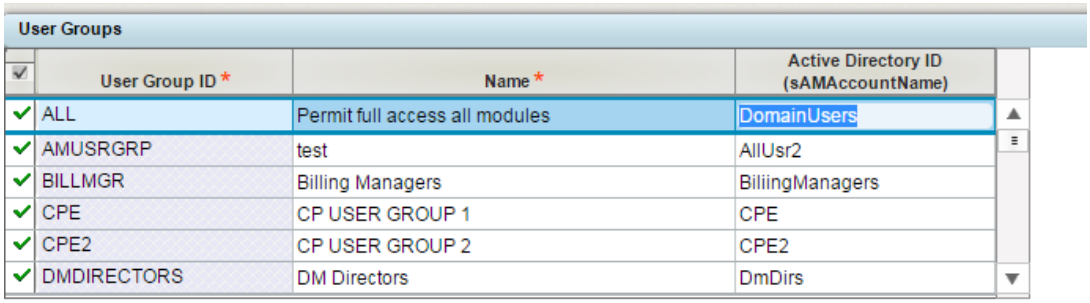
   Note that you can always clear the AD groups mapping data by clicking the **Clear** button.

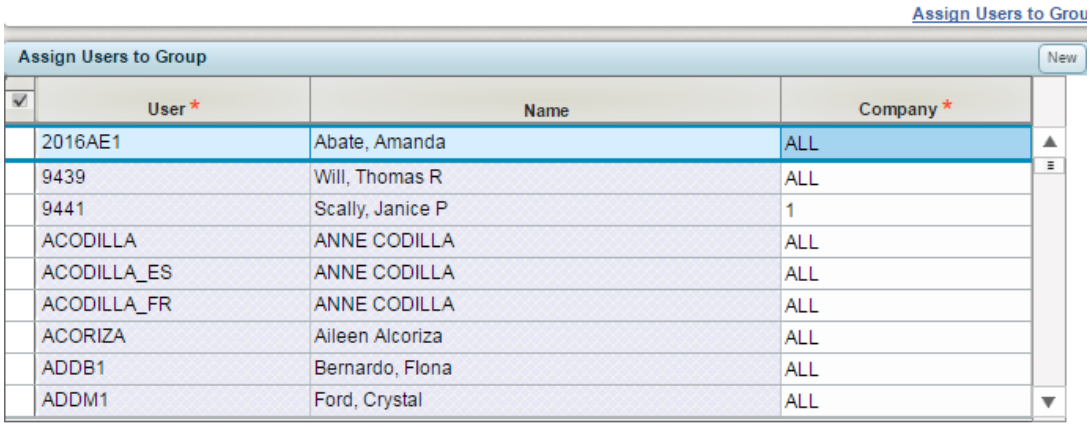
9. Update the mapping between Costpoint user group and Active Directory group by entering the Active Directory Group ID for the **Active Directory ID (sAMAccountName)** value.

   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.




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



# SAML Single Sign-on Setup

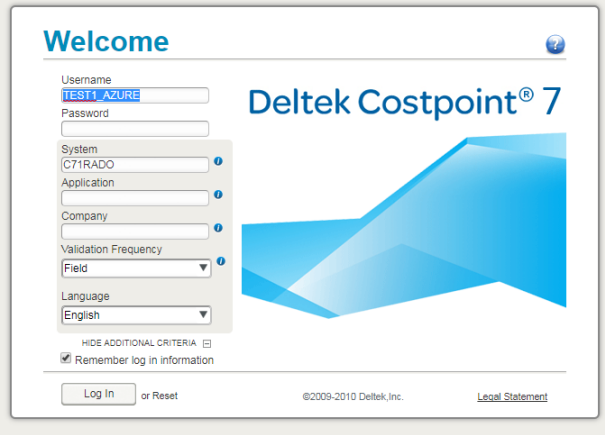
Costpoint can be configured to act as a SAML Service Provider to allow users to log into the system in SAML Single Sign-On (SAML SSO) mode. In this scenario, users do not provide credentials such as password or MFA on the Costpoint login page. Instead, AD FS or Azure Active Directory or any other SAML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

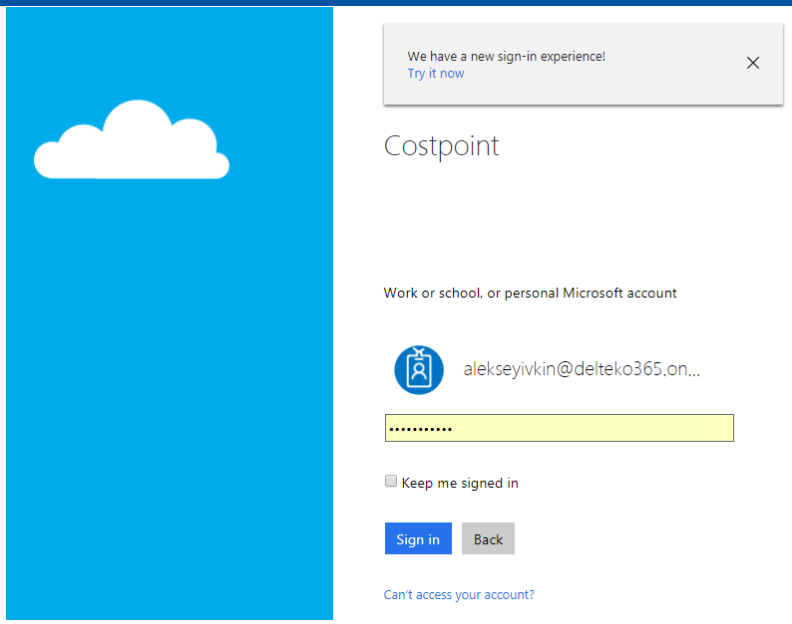
There are two sign-in scenarios in case of SAML SSO:

- 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

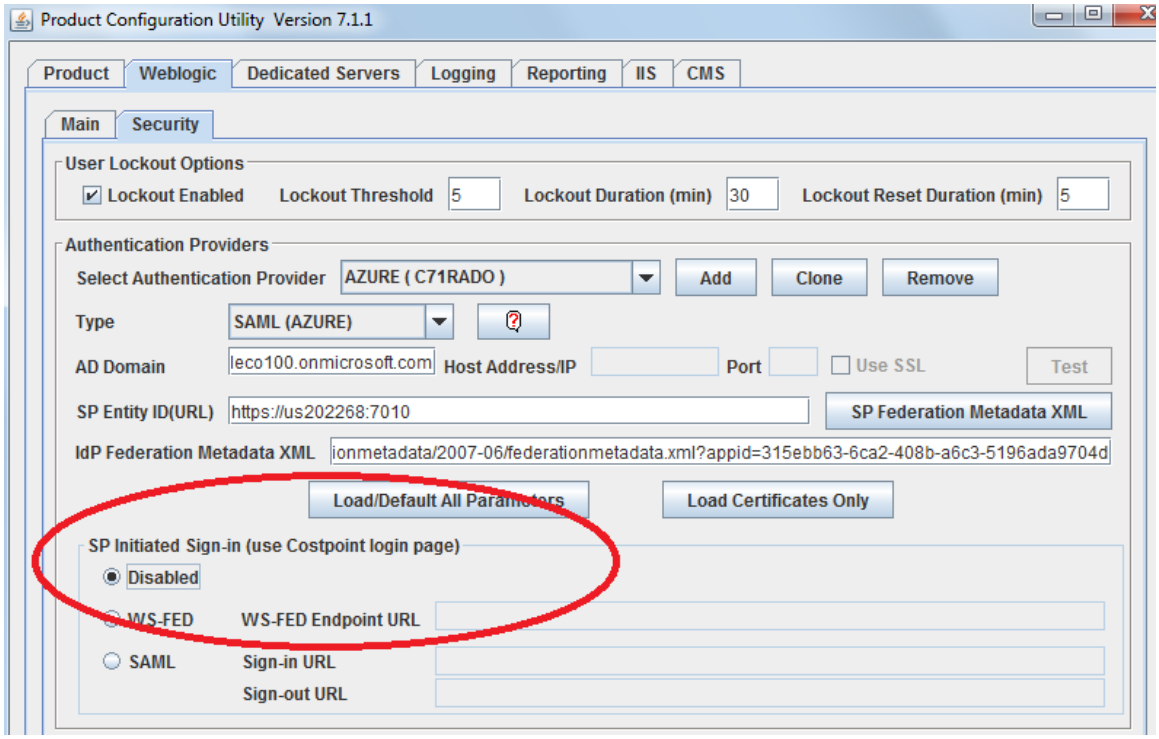
The following table outlines the steps for Costpoint initiated sign-in.

| 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). |

| Step | Description |
|---|---|
| |  |
| 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 WS-FED protocol. 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 by clearing the **Enable SP Initiated Sign-in via WS-FED Endpoint** check box in **Costpoint Config Utility » Weblogic » Security** 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.

- Open enterprise.properties in a Text Editor, and add the following line:

  **<system name>.checkUserIdModeOnLogin=false**

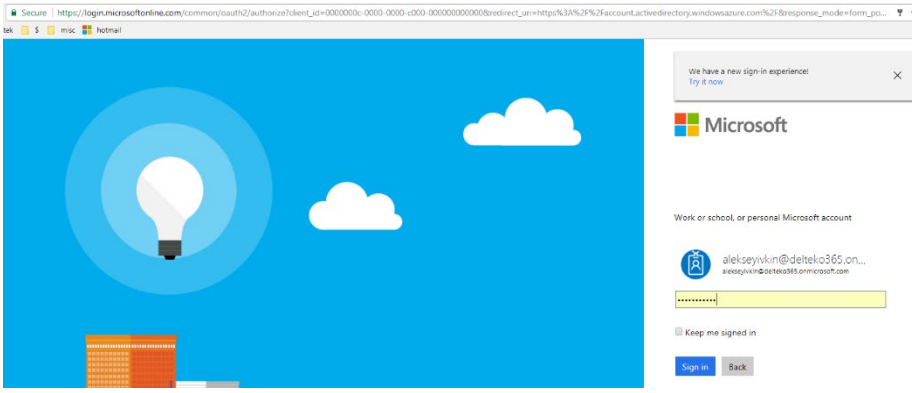
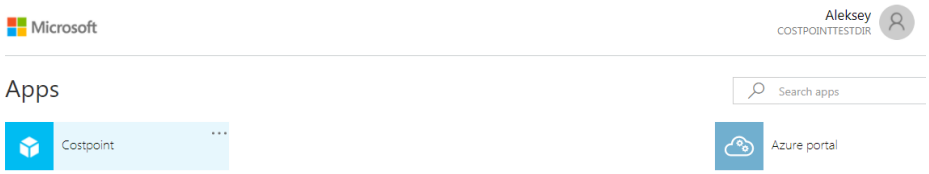
```
C71RADO.sslOnly=false
C71RADO.rsCacheSize=500
C71RADO.dbFetchSize=100
C71RADO.rptFetchSize=2000
C71RADO.Cms.cmsEndpoints=SHPNT01,SHPNT02,DCMT01,ASCO01,SHPCMIS
C71RADO.enableExtensions=true
C71RADO.enableExtensions=true
C71RADO.checkUserIdModeOnLogin=false
```

- Log into Costpoint and run the **"Rebuild Global Settings>Reload All Settings"** function.

The IdP initiated sign-in described next is always available whether or not SP initiated sign-in is on or off.

## 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.<br>  |
| 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:

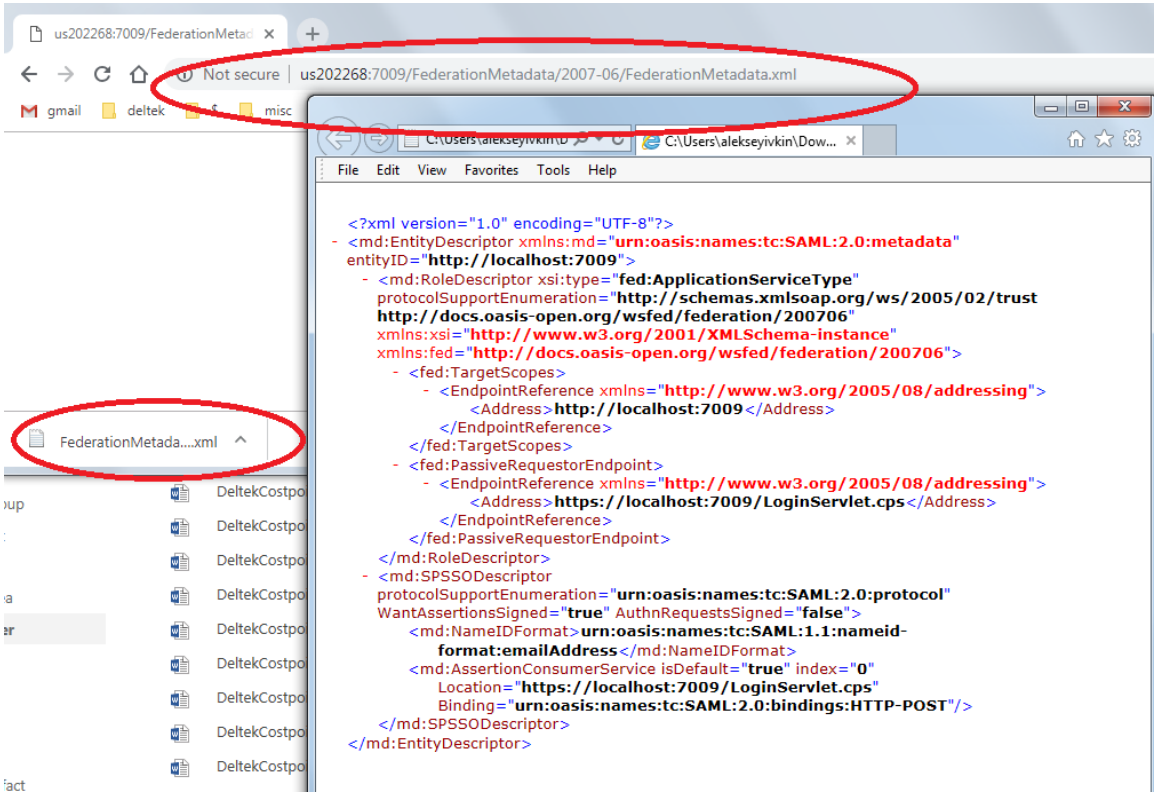
1. Download Costpoint FederationMetadata.xml from your Costpoint Server public URL.

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

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

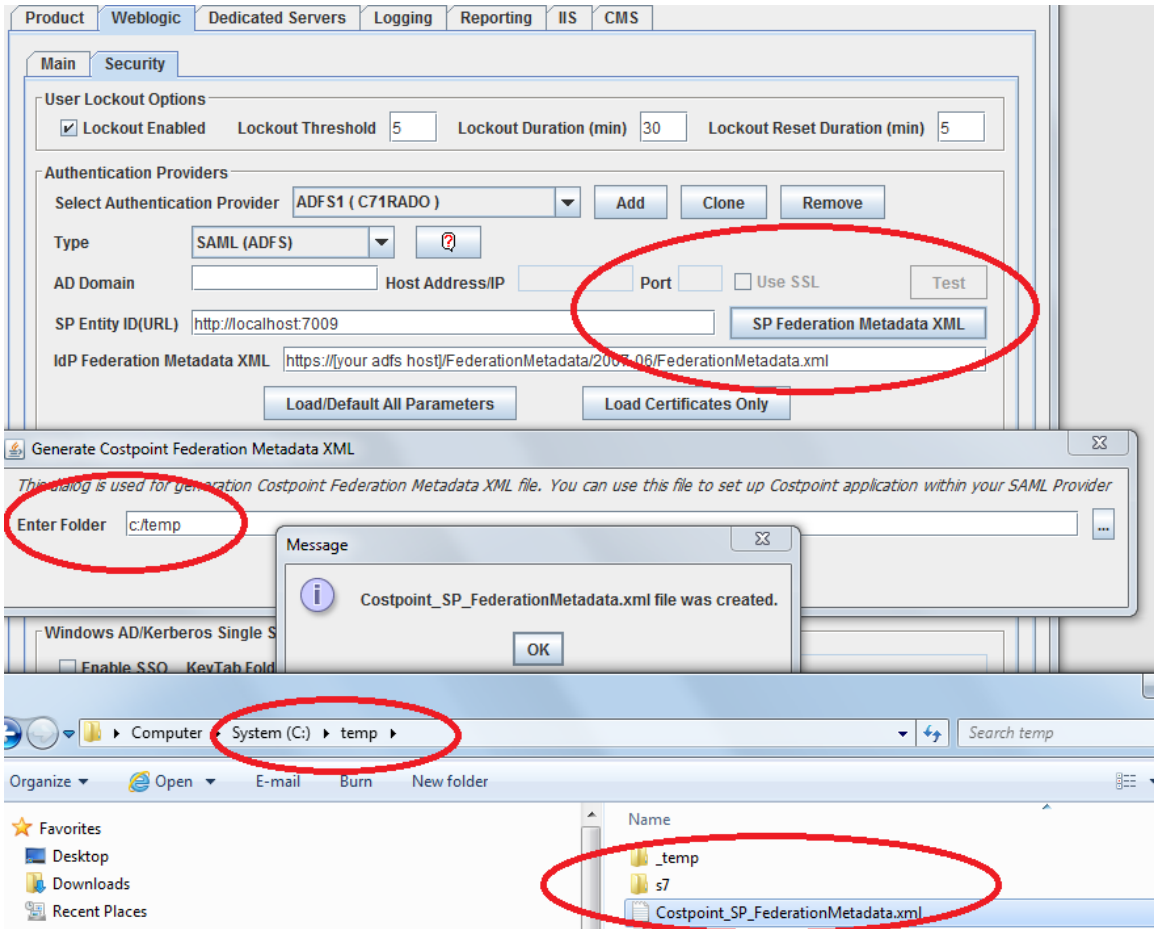
   http://myhost/CPWeb/FederationMetadata/2007-06/FederationMetadata.xml

   This is 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).

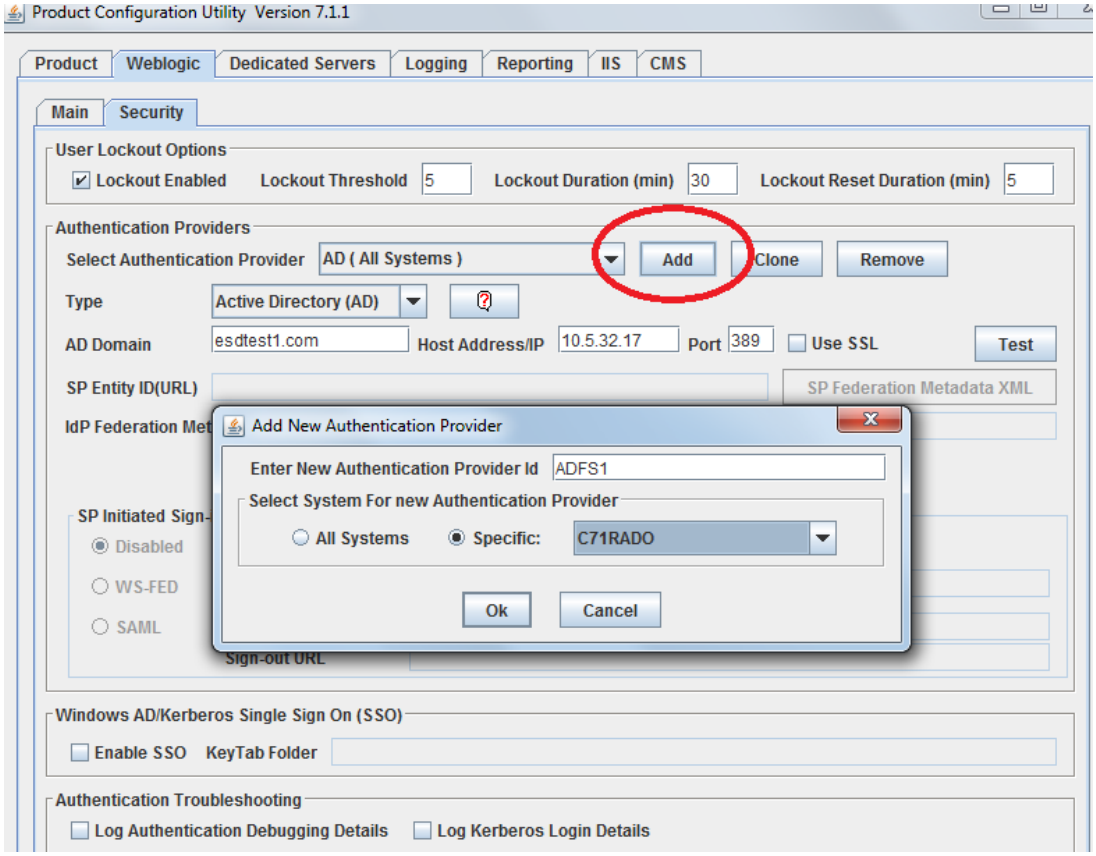
Use **Costpoint (SP) Federation Metadata XML** to register Costpoint SAML application/connection within your SAML IdP. You can either upload the Costpoint FederationMetadata.xml file or update the settings manually using your SAML IdP console.

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.

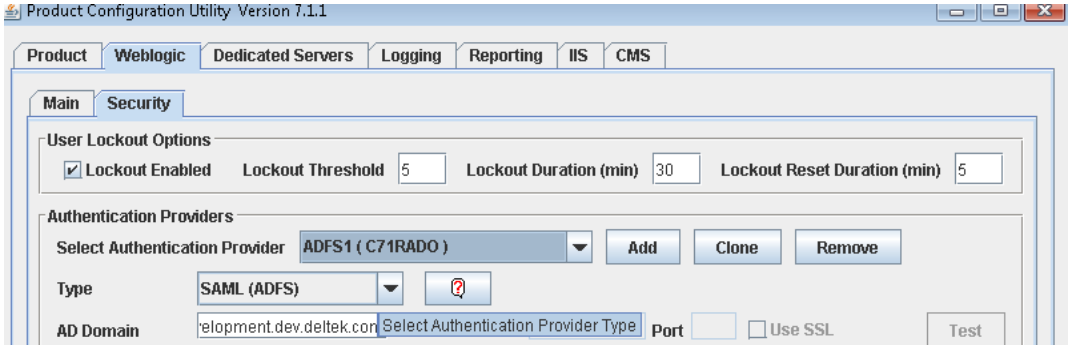
# Configure SAML Single Sign-on between Costpoint and Microsoft AD FS

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. Enter the **AD Domain** name.

   Domain is your company's Windows AD domain. During SAML assertion verification, the system concatenates the **Domain** value with the **Active Directory ID** entered on the Manage Users screen.

   For example, if **Active Directory ID** from Manage Users configuration is **john.smith** and AD **Domain** is **us.mycompany.com**, the system will use **john.smith@us.mycompany.com** and will try to match it to the user principal name found in the Security Subject of SAML assertion. If it matches exactly (case-insensitive) and the SAML assertion signature is valid, the user is let into the system. Otherwise, the authentication request will be rejected.

   Though it is not recommended, you may leave the **AD Domain** field blank, but you will have to enter fully qualified name for **Active Directory ID** on the Manage Users screen (for example, **john.smith@us.mycompany.com,** not just **john.smith.**

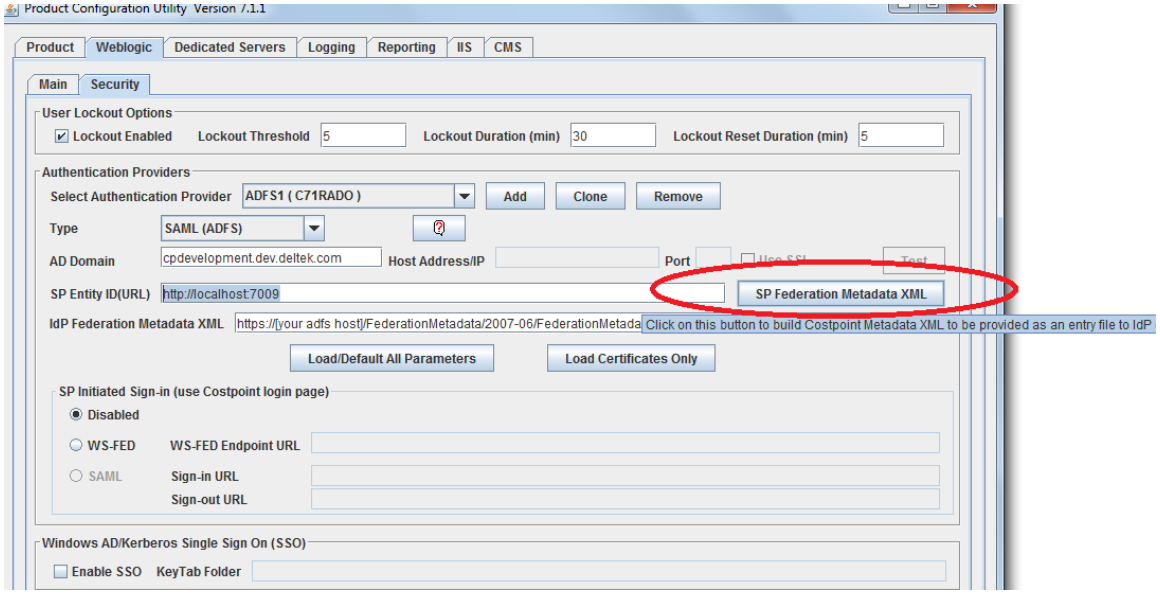
6. Enter the **SP Entity ID (URL)**.

   **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.

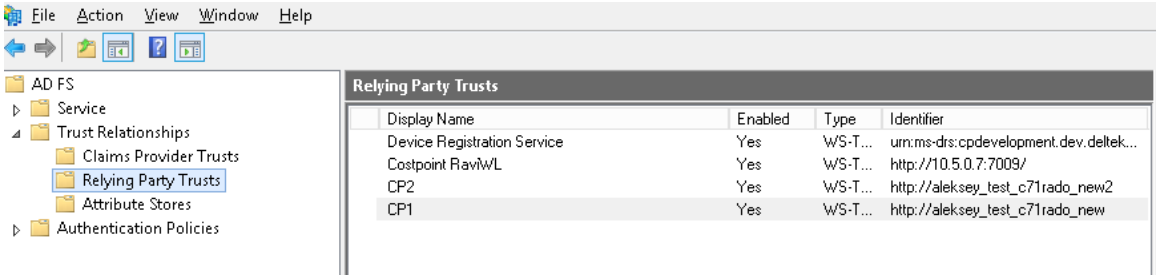
7. Click **SP Federation Metadata XML** and follow the instructions to generate the **Costpoint_SP_FederationMetadata.xml** file.



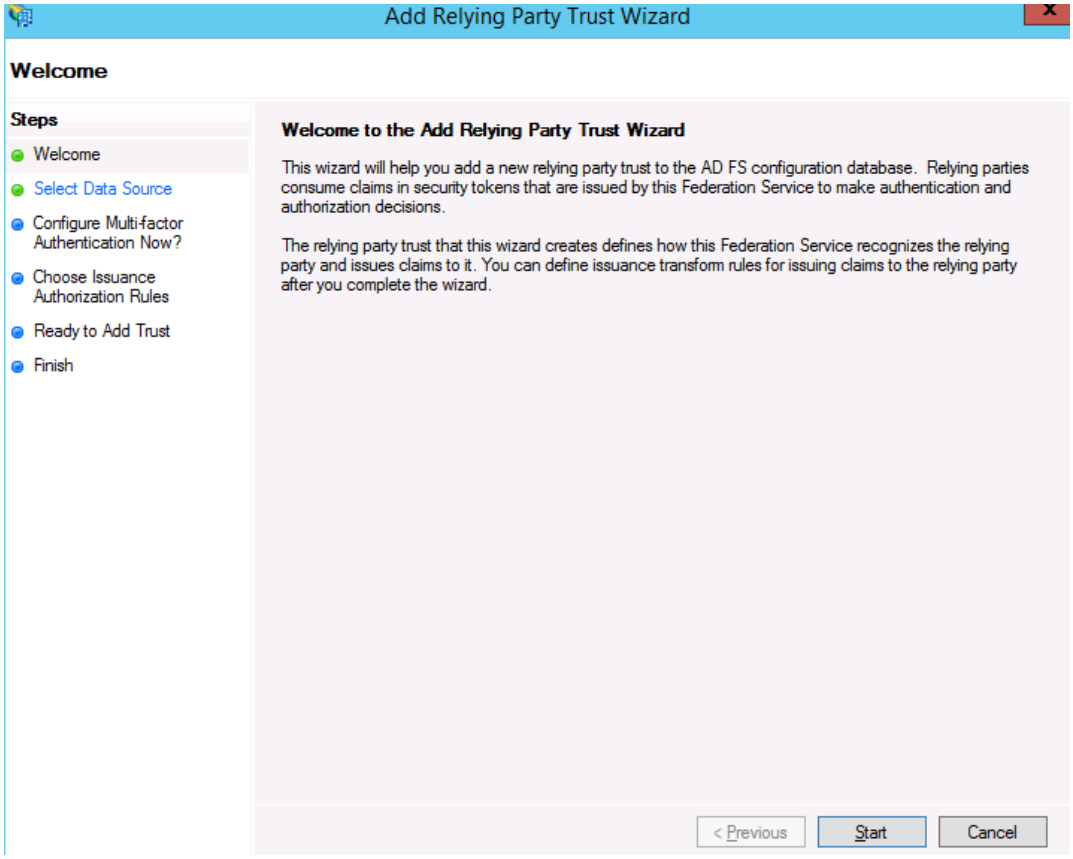

8. Click **Save** and stop making any further changes in Costpoint Configuration Utility for now.

   You have to navigate to your 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.

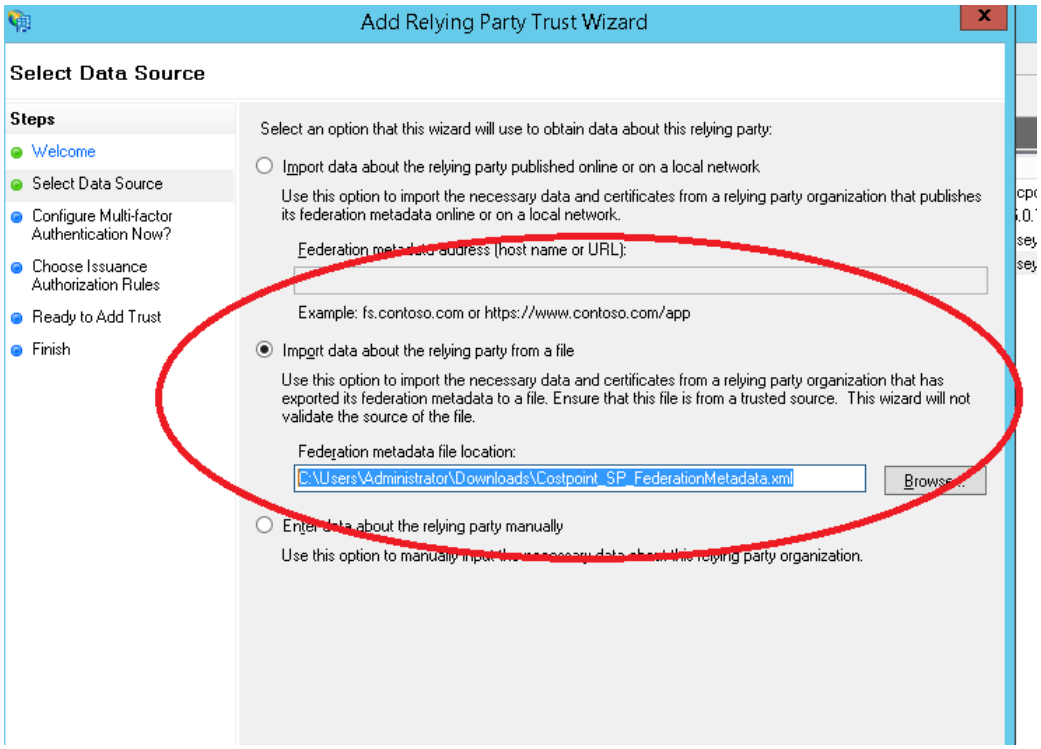
9. On the AD FS host, open the AD FS Management tool.
10. Select **Relying Party Trusts**, and click **Add Relying Party Trust.**



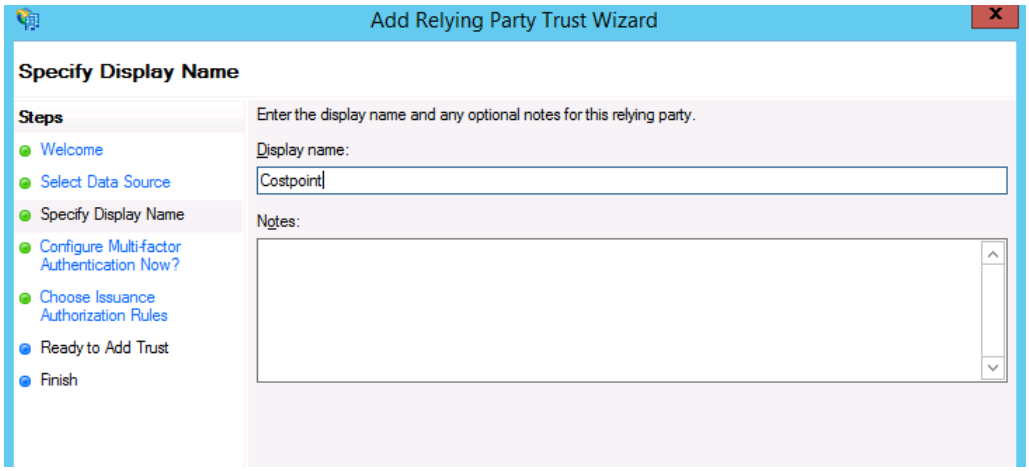

11. On the Welcome page of the Add Relying Party Trust Wizard, click **Start**.



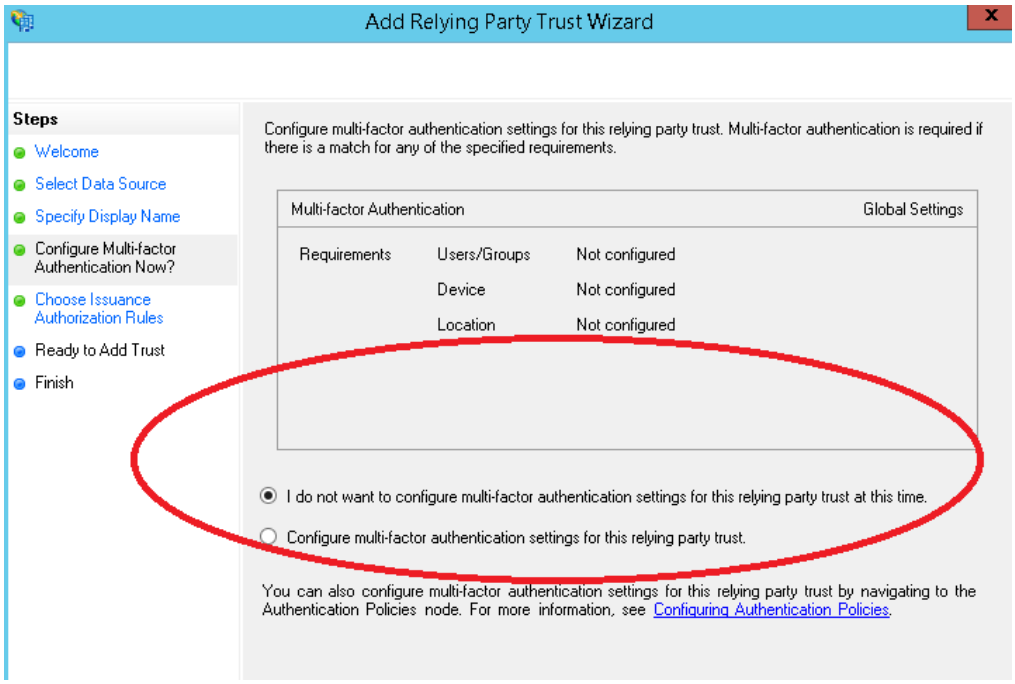
12. On the Select Data Source page, select **Import data about the relying party from a file**, point to the **Costpoint_SP_FederationMetadata.xml** file that you generated earlier using Costpoint Configuration Utility, and click **Next.**



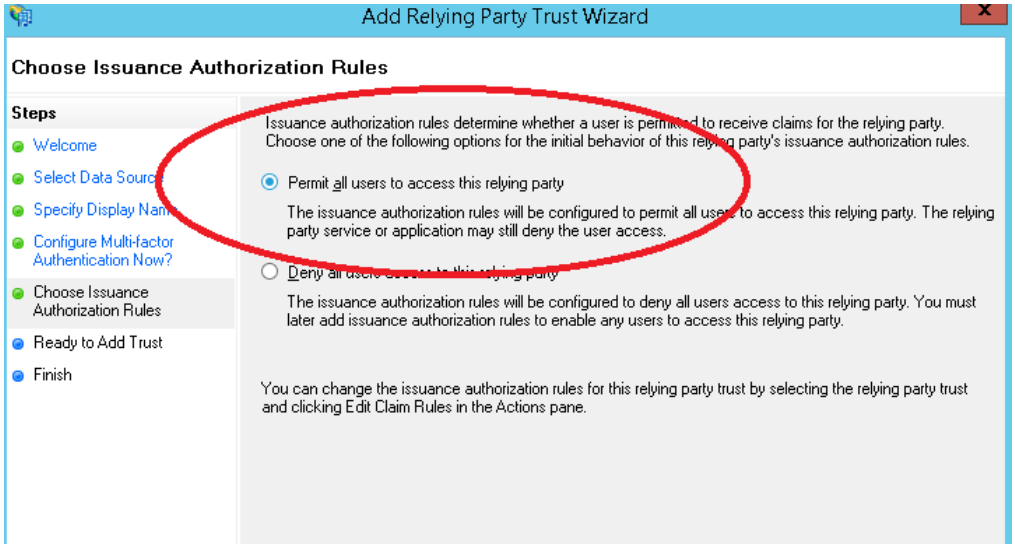

13. On the Specify Display Name page, enter **Costpoint** for the relying party **Display name**, and click **Next**.



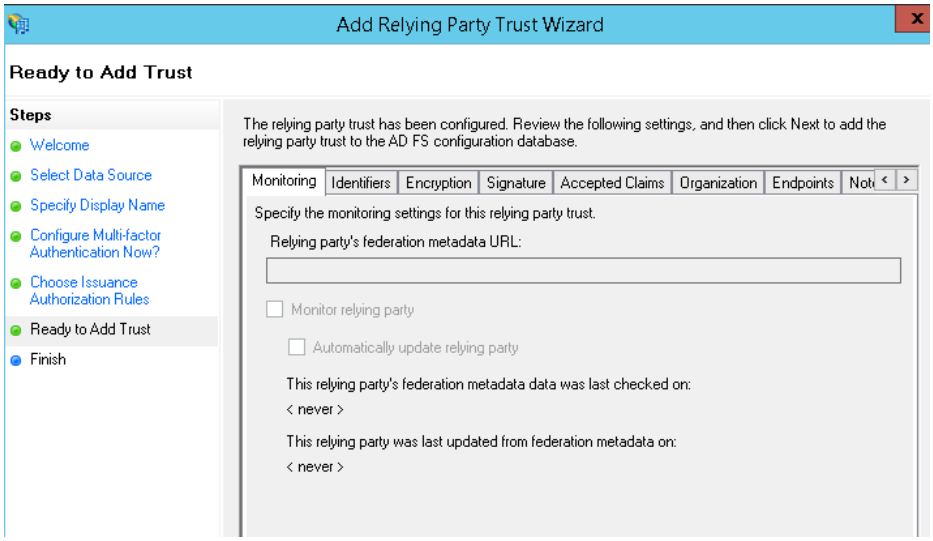
14. On the Configure Multi-factor Authentication Now page, accept the default selection for **Multifactor Authentication**, and click **Next**.



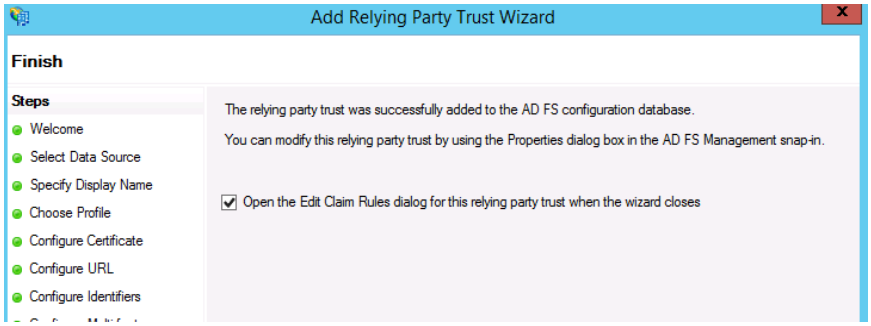

15. On the Choose Issuance Authorization Rules page, accept the default selection of **Permit all users to access this relying party**, and click **Next**.



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

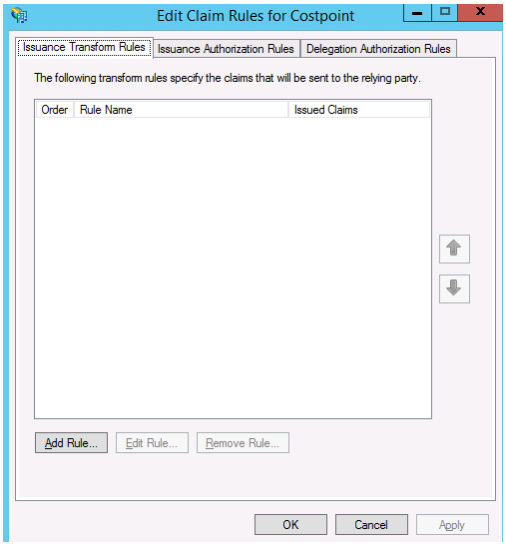



17. On the Finish page, ensure that the **Open the Edit Claim Rules for this relying party** check box is selected, and click **Close**.

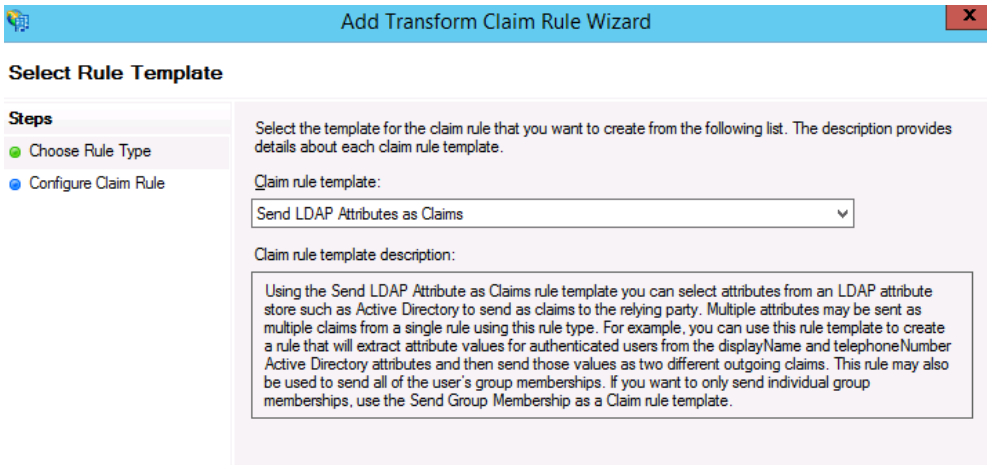



The next steps explain how to add an AD FS claim rule that will allow Costpoint to retrieve the group membership information from AD FS AD and synchronize this information with the Costpoint user groups data.

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

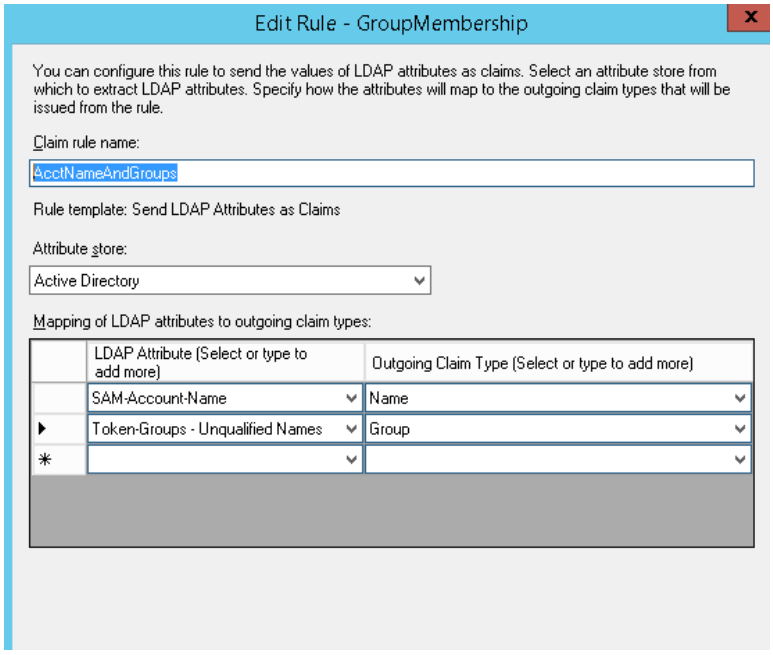


b) On the Select Rule Template page of the Add Transform Claim Rule Wizard, select **Send LDAP Attributes** in the **Claim rule template** drop-down list, and click **Next**.




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

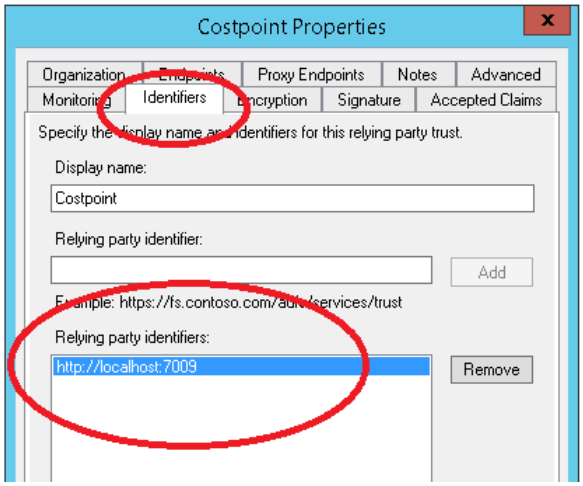
- **Claim rule name**: Enter **AcctNameAndGroups**.
- **Attribute store**: Select **Active Directory** from the drop-down list.
- Enter two lines for Mapping of LDAP attributes to outgoing claim types:
  - **LDAP Attribute**: Select **SAM-Account-Name** from the drop-down list.
  - **Outgoing Claim Type**: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

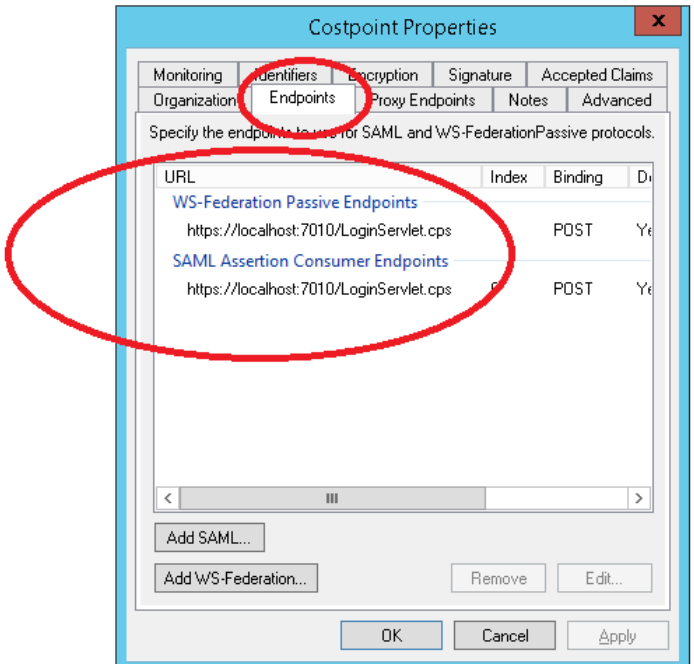


d) Click **Finish**, and click **Ok**.

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.

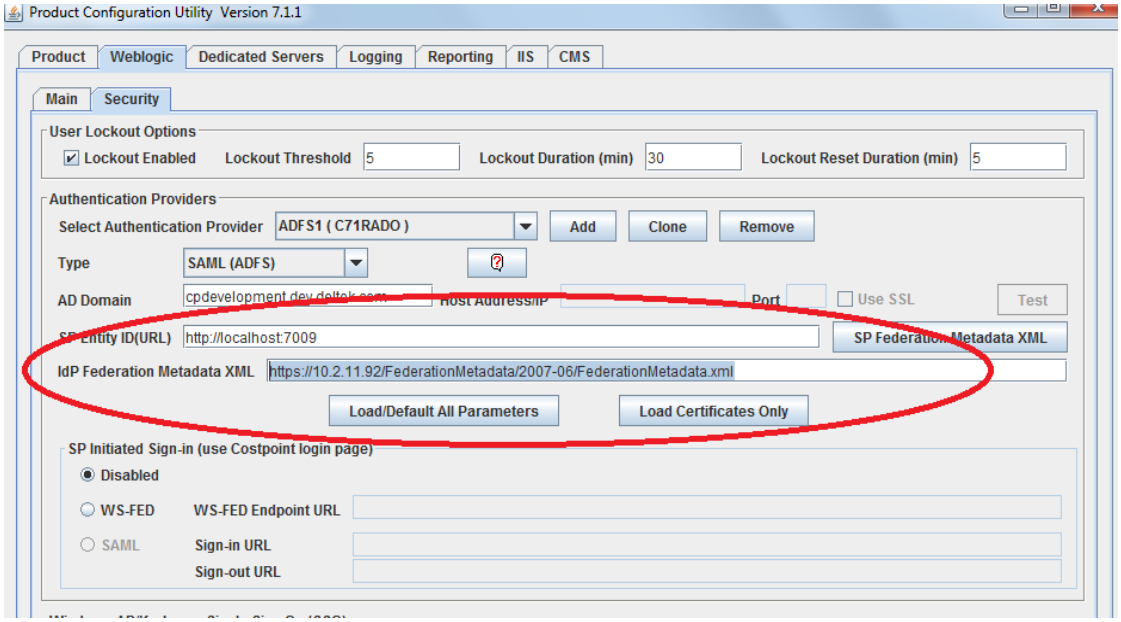
Note that you can always manually change any settings of the **Costpoint Relying Party Trust** in AD FS Management tool.



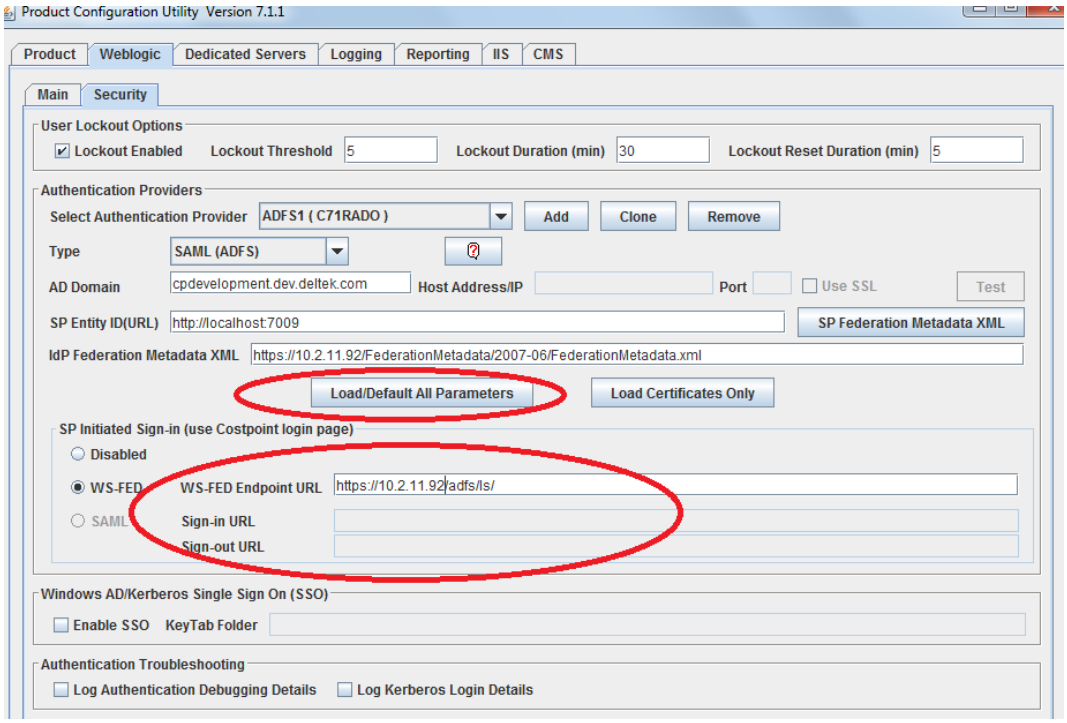

18. With AD FS **Costpoint Relying Party Trust** configured, return to Costpoint Configuration Utility and enter **IdP Federation Metadata XML**.

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**.

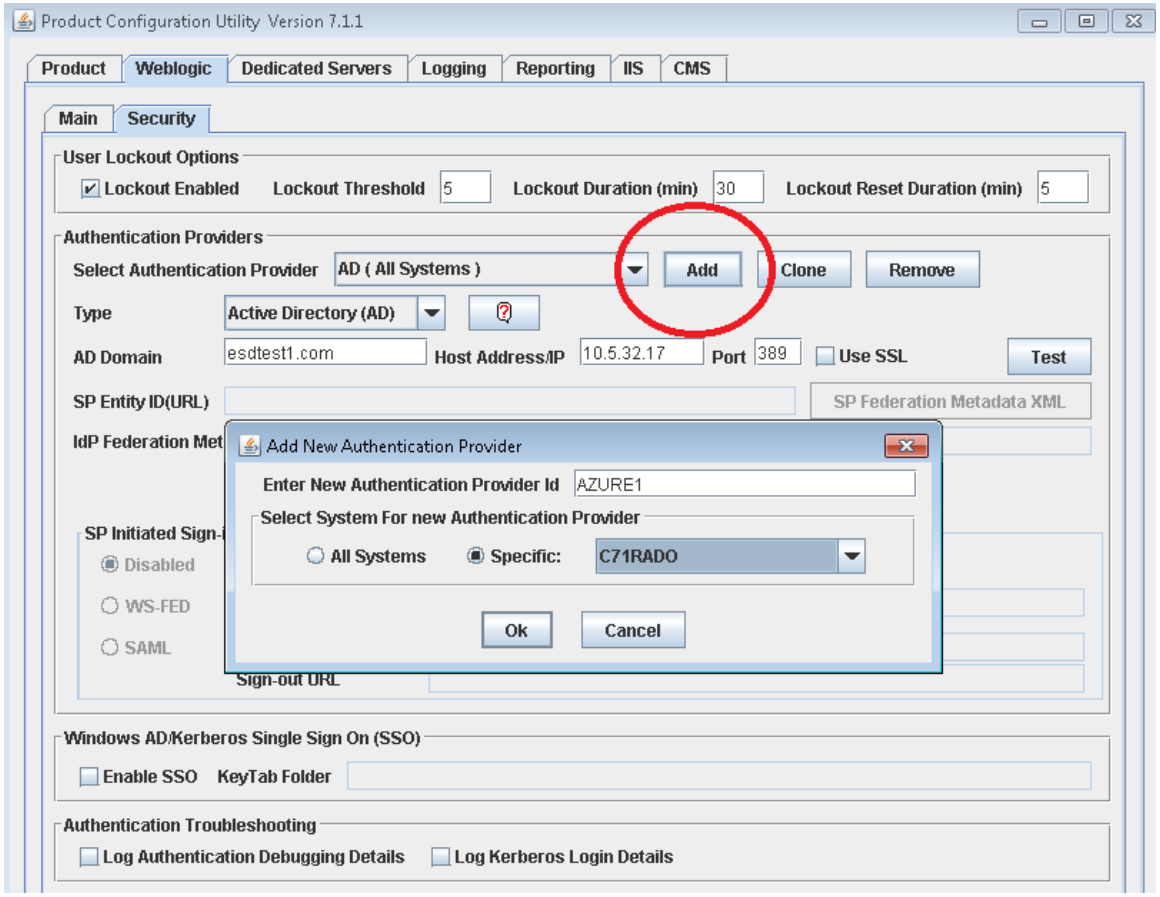
    Costpoint SAML Single Sign-on setup for Microsoft AD FS is complete. You can activate SAML SSO mode for Costpoint user accounts.

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

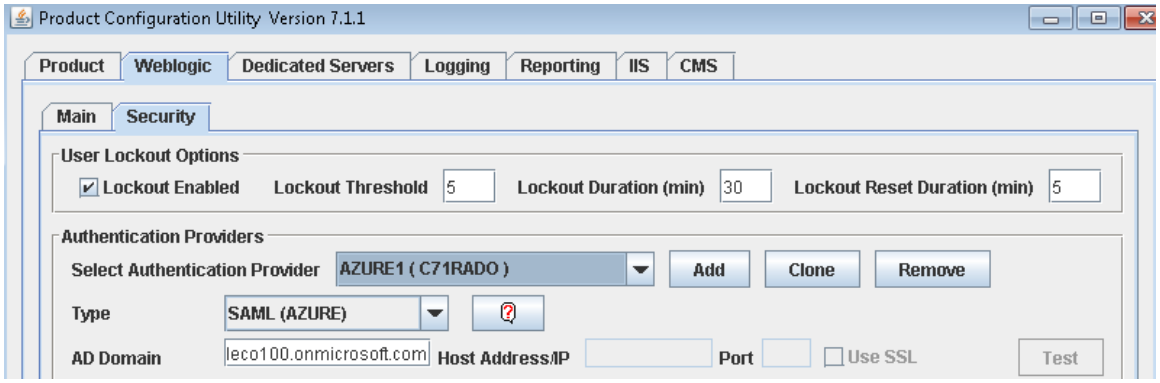
**To configure SAML Single Sign-on between Costpoint and MS Azure:**

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. Enter the **AD Domain** name.

   Domain is your company's Windows AD domain. During SAML assertion verification, the system concatenates the **Domain** value with the **Active Directory ID** entered on the Manage Users screen.

   For example, if the **Active Directory ID** from Manage Users configuration is **john.smith** and the **AD Domain** is **us.mycompany.com**, the system will use **john.smith@us.mycompany.com** and will try to match it to the user principal name found in the Security Subject of SAML assertion. If it matches exactly (case-insensitive) and the SAML assertion signature is valid, the user is let into the system. Otherwise, the authentication request will be rejected.

   Though it is not recommended, you can leave the **AD Domain** field blank, but you will have to enter fully qualified name for the **Active Directory ID** on the Manage Users screen (for example, **john.smith@us.mycompany.com**, not just **john.smith.**

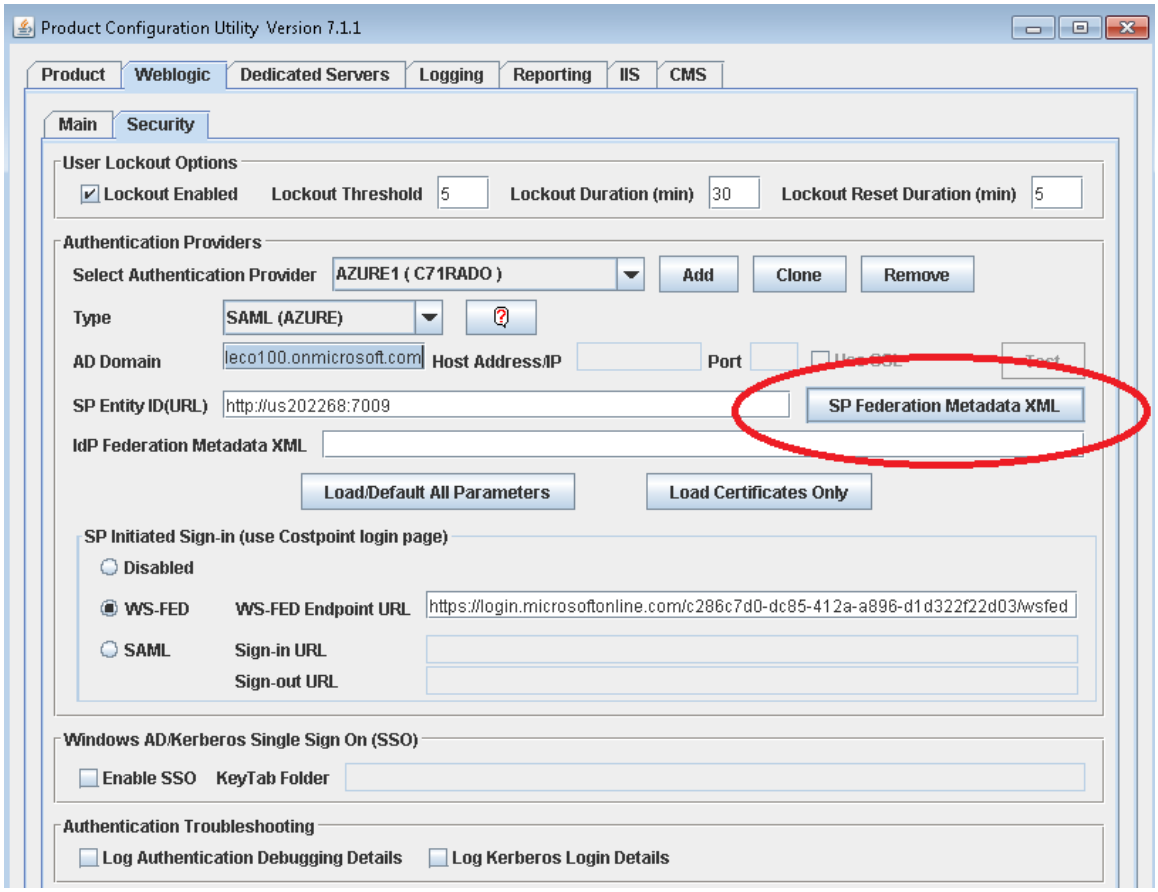
6. Enter **SP Entity ID (URL)**.

   **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 to generate the **Costpoint_SP_FederationMetadata.xml** file.

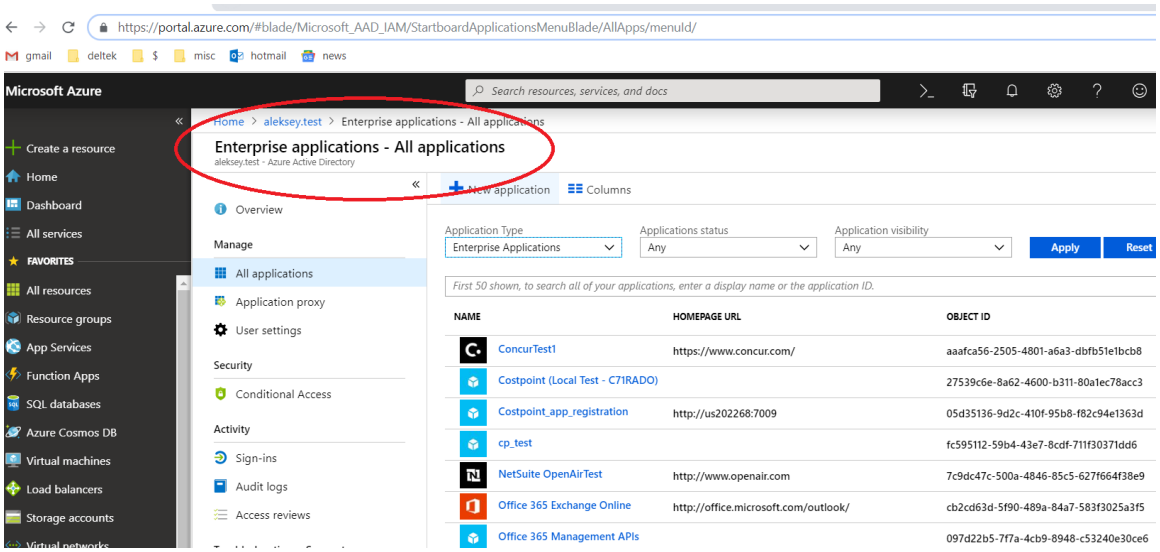



8. Click **Save** and stop making any further changes in Costpoint Configuration Utility for now.

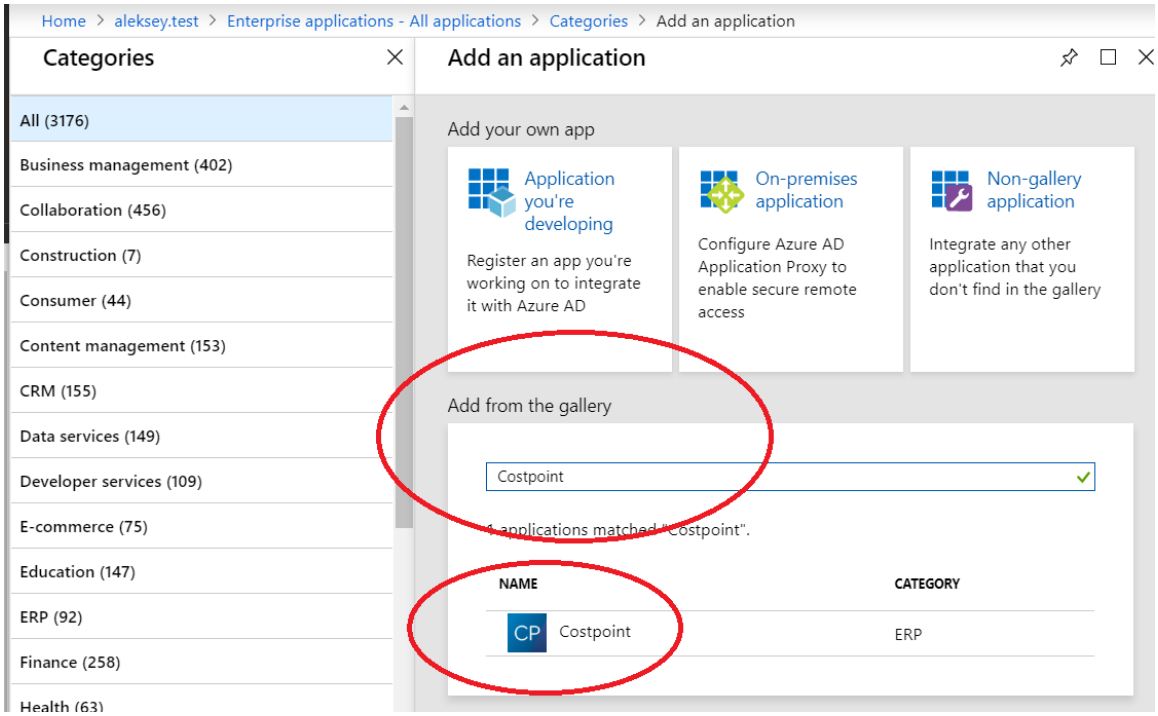
   You have to navigate to the Microsoft Azure Admin Console and complete the SAML configuration on the Azure side. Then you will return to Costpoint Configuration Utility and finish the original setup.

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

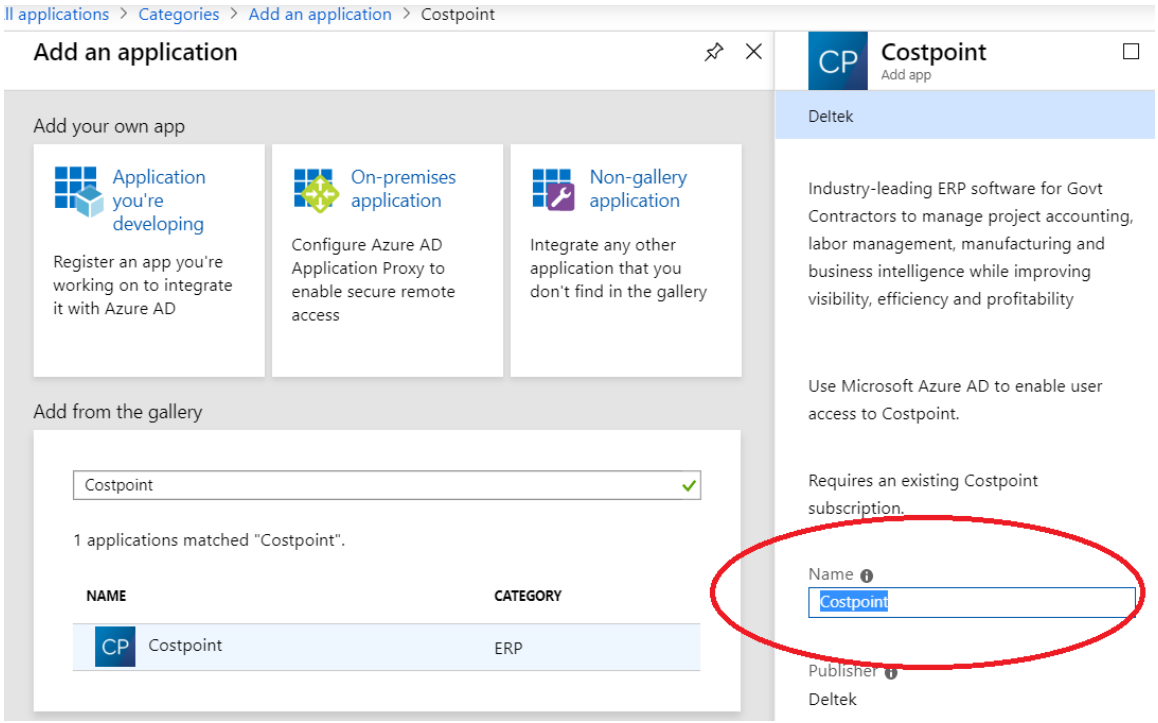
10. Navigate to **Azure Active Directory » Enterprise Applications » All Applications**.



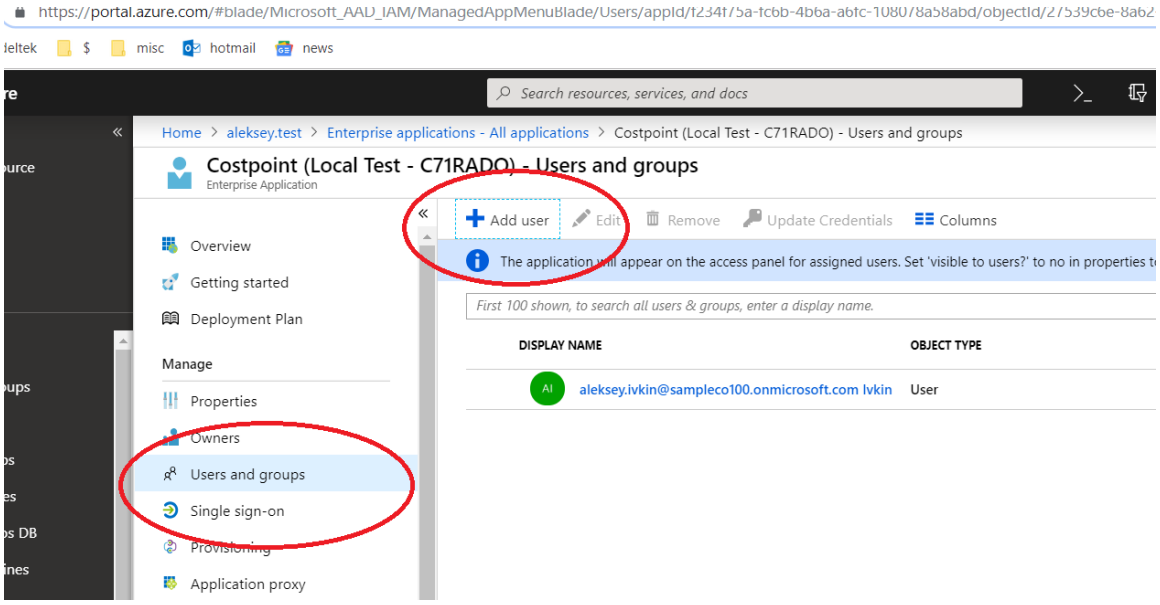

11. Click **+ New Application**, select the **Add from the gallery** option, and type **Costpoint**.



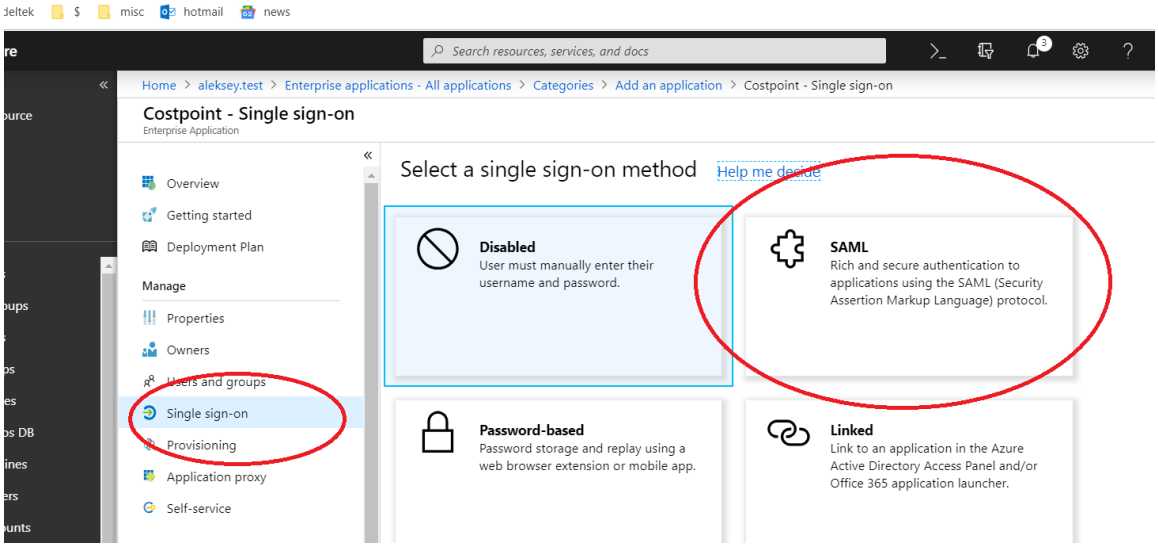

12. Click the **Costpoint** gallery template published by **Deltek**, accept default name **Costpoint** in the **Name** field, and click **Add**.



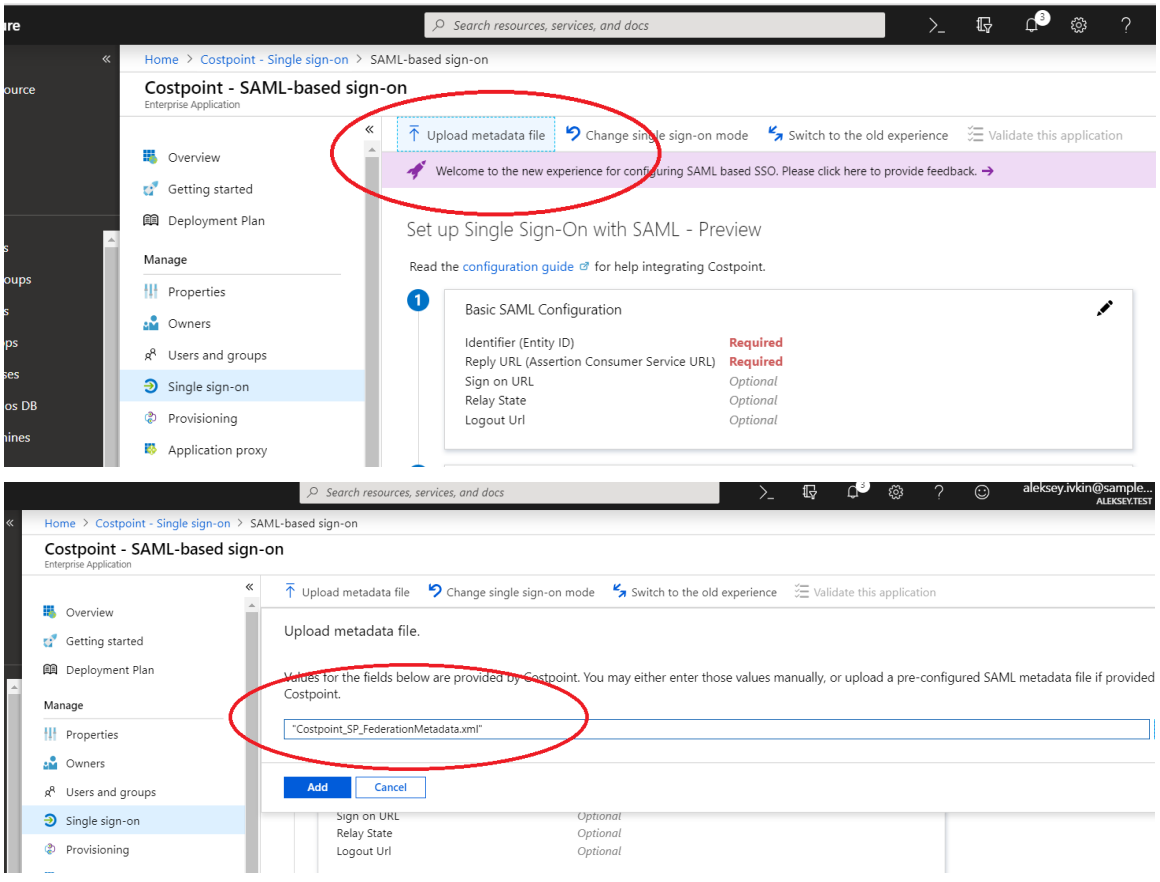

13. Click **Assign a user for testing**, or go to **Costpoint** » **Users and groups** on the left pane and click **Select** and **Assign** to select and assign users and/or user groups to have access to Costpoint.




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

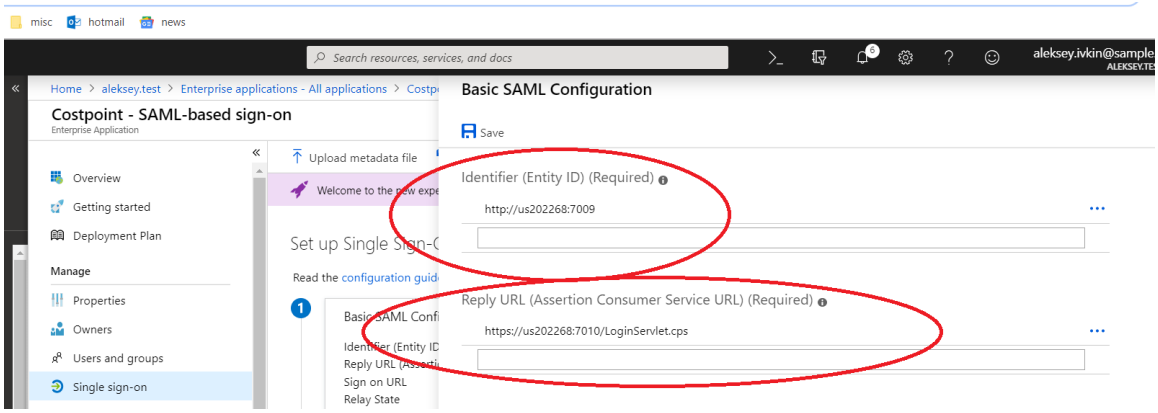



15. Click **Upload metadata file**, select the **Costpoint_SP_FederationMetadata.xml** file that you generated earlier using Costpoint Configuration Utility, and click **Add.**

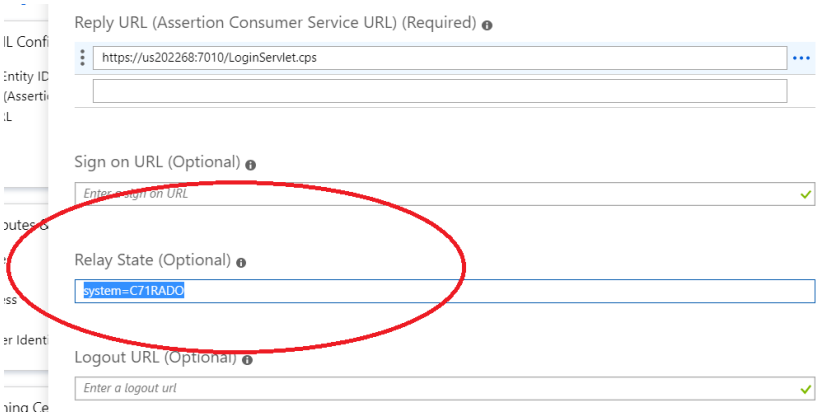



16. It will populate all The SAML required fields populate based on values from the **Costpoint_SP_FederationMetadata.xml** file.

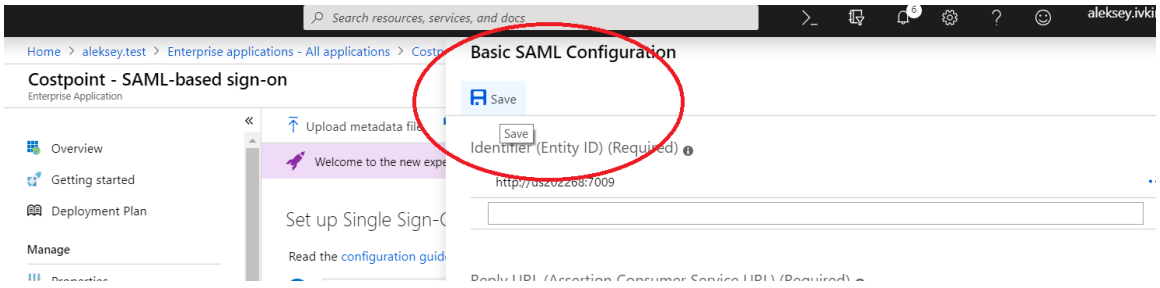
    You can always correct these values manually if needed.



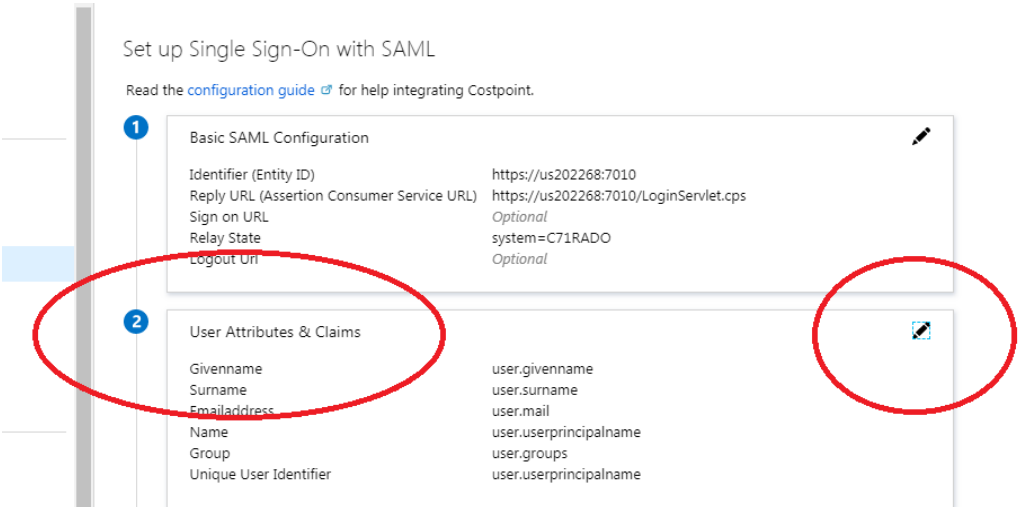

- **Identifier (Entity ID)**: The value must be unique across all applications registered within Azure. It is case-sensitive and must match exactly (including the case) to the **SP Entity ID (URL)** in Costpoint Configuration Utility.
- For **Reply URL**, enter the **HTTPS/SSL** Costpoint host/address 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**).



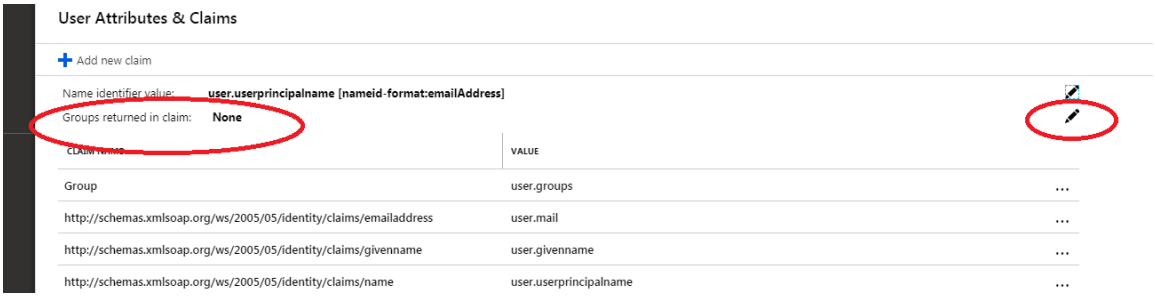

17. Leave everything else as-is on the screen, and click **Save** to save the **BasicSAML Configuration.**



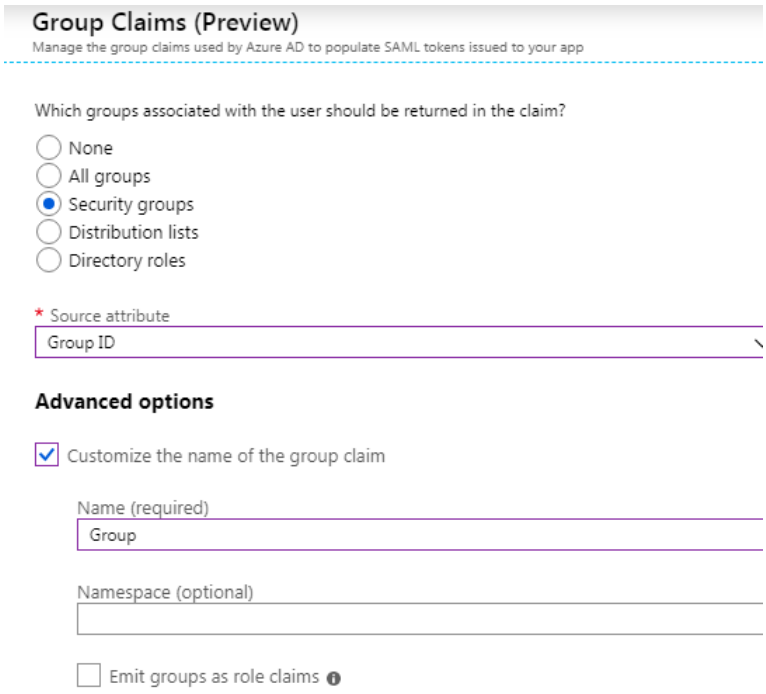
18. If you use **Manage User Groups in Active Directory** for your Costpoint users, scroll down to the **User Attributes & Claims** section and click **Edit**.




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

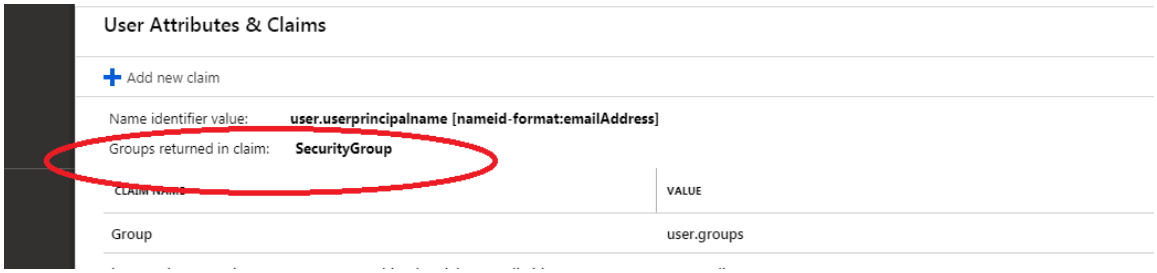



b) On the Group Claim dialog box, select **Security Groups** for **Which groups associated with the user should be returned in the claim**; choose **Group ID** or **sAMAccountName** (only if groups synchronized from an on-premises Active Directory using AAD Connect Sync 1.2.70.0 or above) as **Source 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.

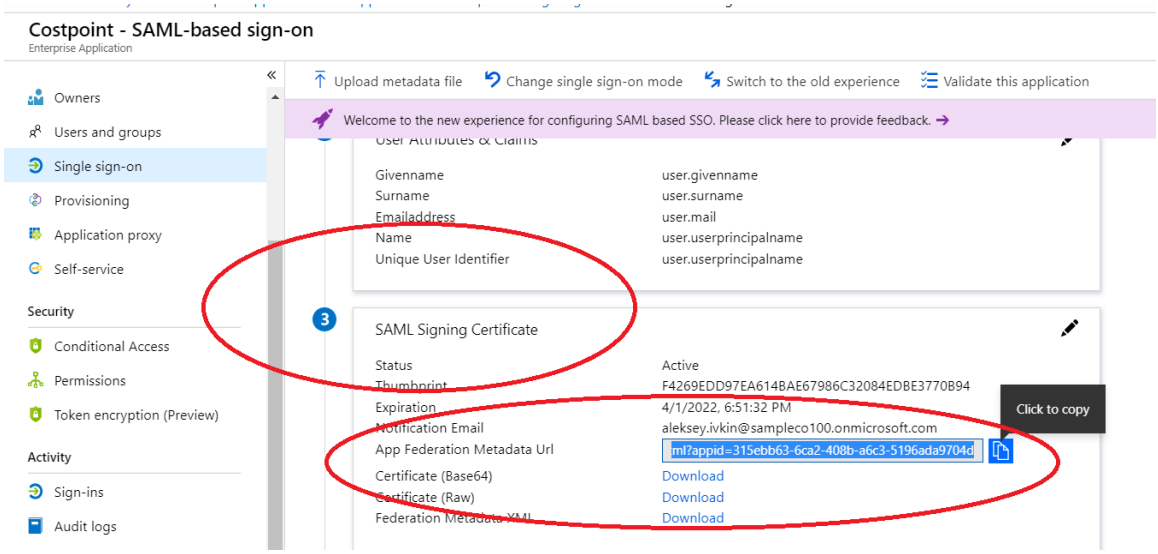
Security Groups will now be returned as part of SAML assertion.




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

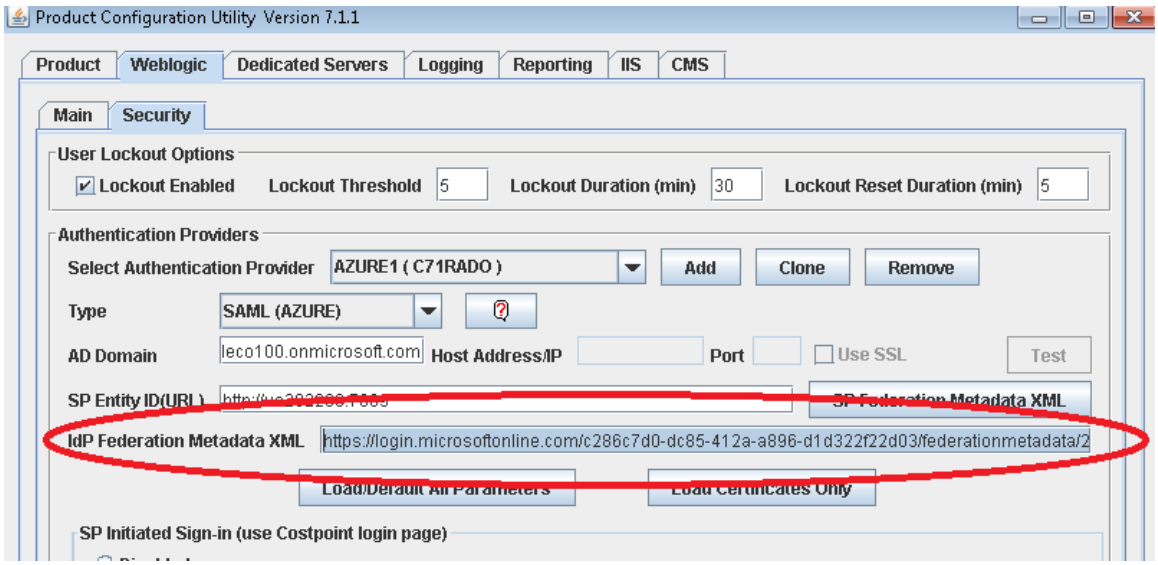
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-fed-group-claims.

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



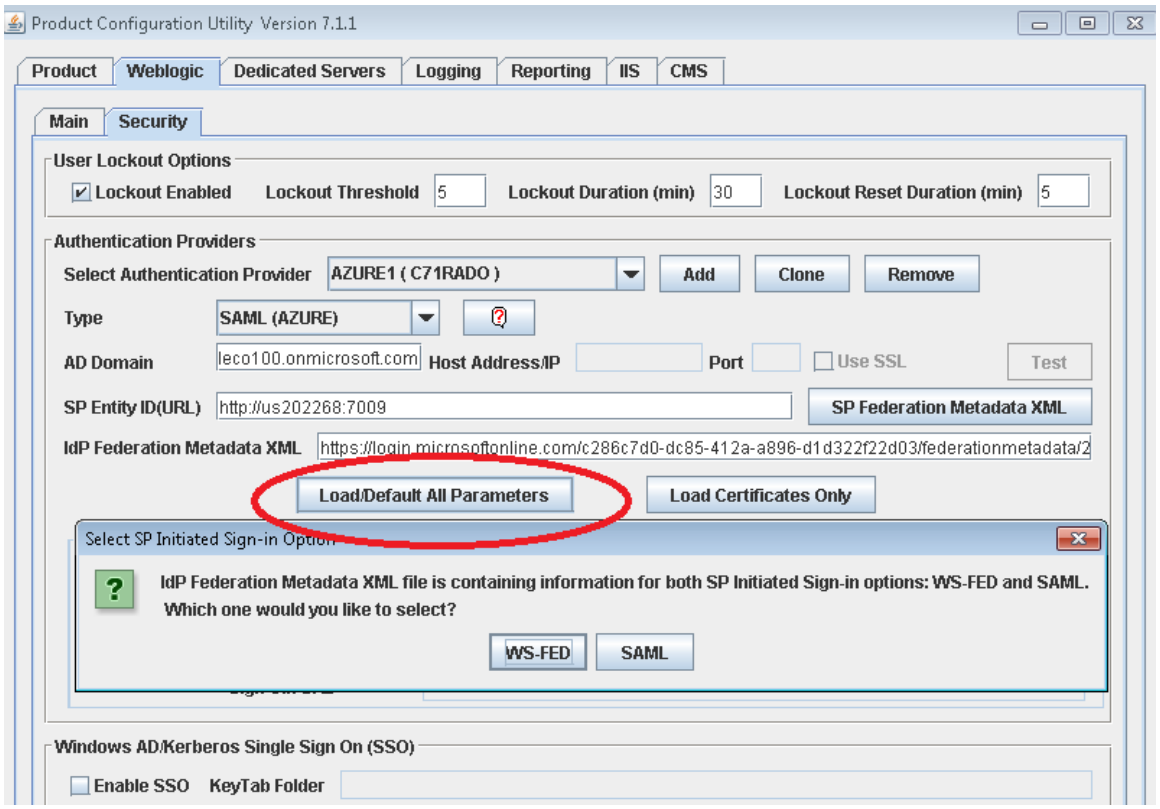

20. Return to Costpoint Configuration Utility and enter **IdP Federation Metadata XML**.

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



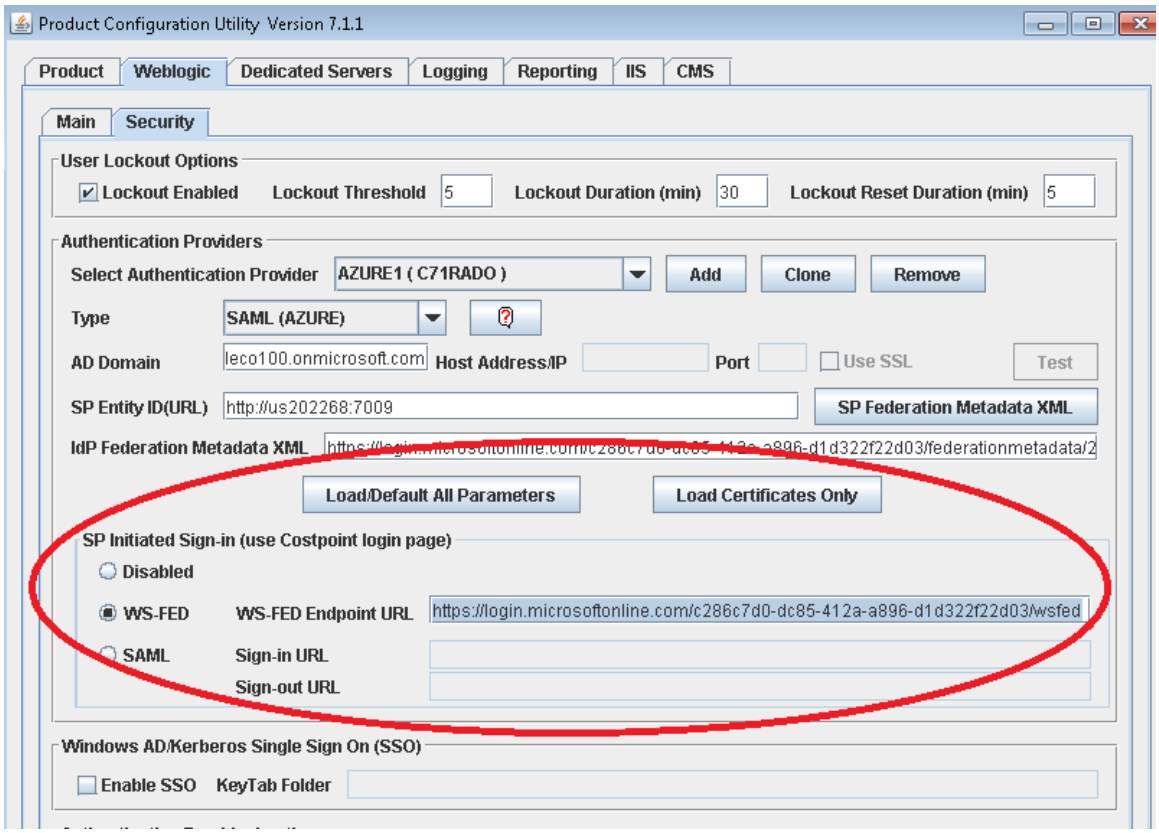

20. Click **Load/Default All Parameters**.

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

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




22. 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.

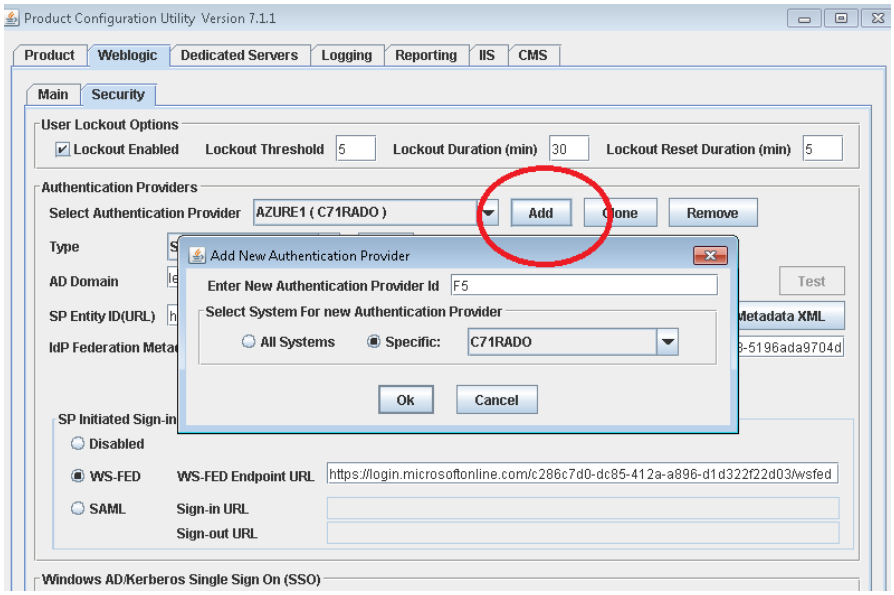
Same as with AD FS or Azure, you start with Costpoint Configuration Utility and generate the **Costpoint_SP_FederationMetadata.xml** file. Then you navigate to your SAML IdP Admin Console and register the Costpoint application/connection on the IdP's end. If your SAML IdP allows for SP metadata upload, 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.

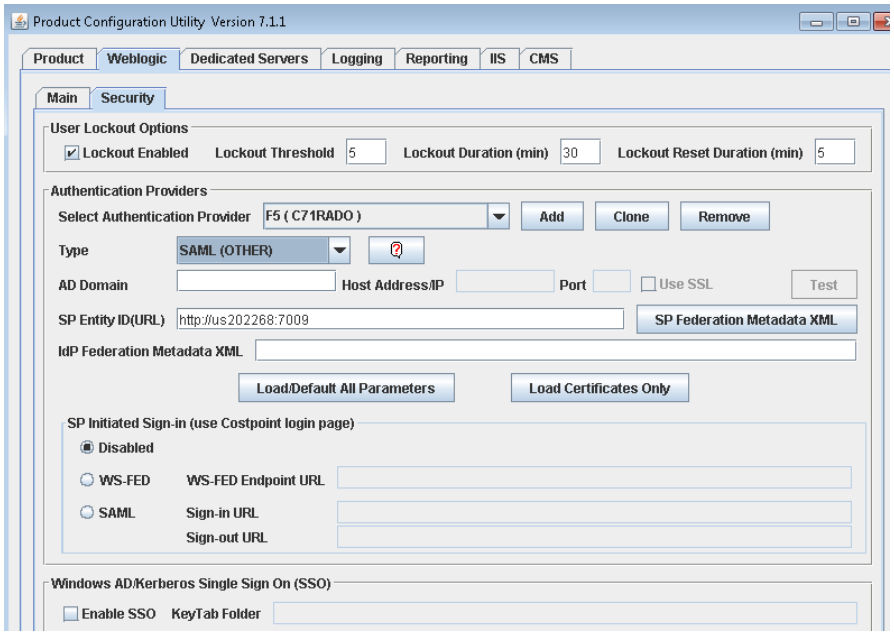
**To enable SAML Single Sign-on with SAML (Other) IdP:**

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. Enter the **AD Domain** name.

   Domain is your company's Windows AD domain. During SAML assertion verification, the system concatenates the **Domain** value with the **Active Directory ID** entered on the Manage Users screen.

   For example, if the **Active Directory ID** from Manage Users configuration is **john.smith** and the **AD Domain** is **us.mycompany.com**, the system will use **john.smith@us.mycompany.com** and will try to match it to the user principal name found in the Security Subject of SAML assertion. If it matches exactly (case-insensitive) and the SAML assertion signature is valid, the user is let into the system. Otherwise, the authentication request will be rejected.

Though it is not recommended, you can leave **AD Domain** field blank, but you will have to enter fully qualified name for the **Active Directory ID** on the Manage Users screen (for example, **john.smith@us.mycompany.com**, not just **john.smith**).

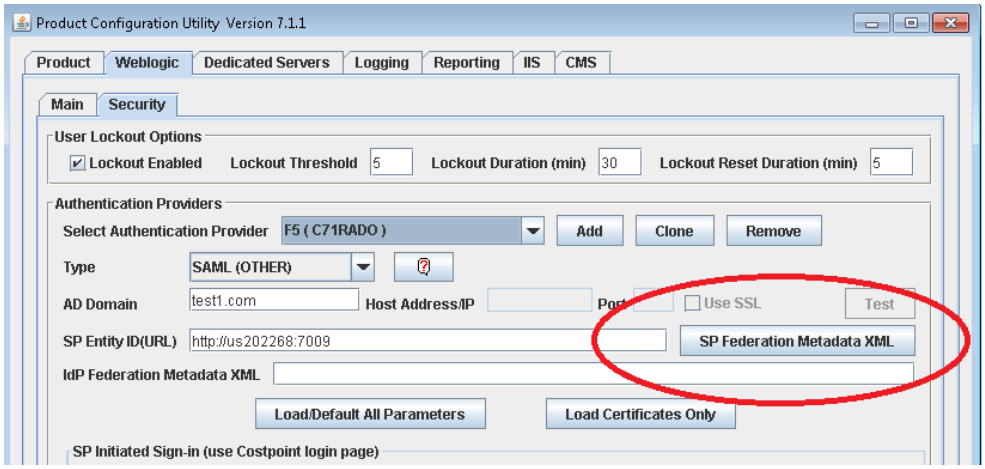
6. Enter **SP Entity ID (URL)**.

   **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.

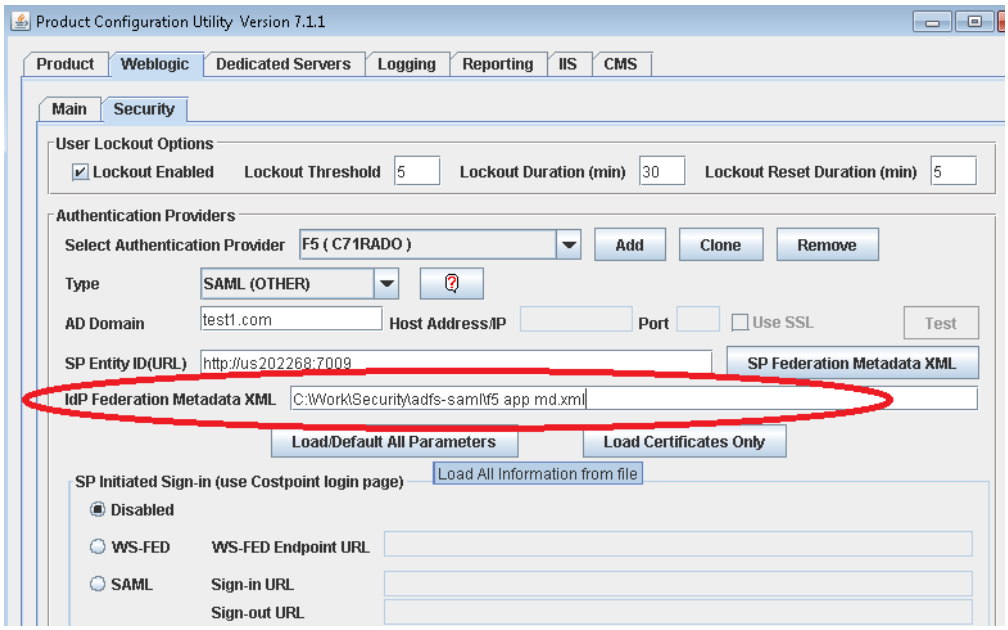
   You have to navigate to your SAML IdP Admin Console and complete the SAML configuration on its side. Then you will return to Costpoint Configuration Utility and finish the original setup.

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**).

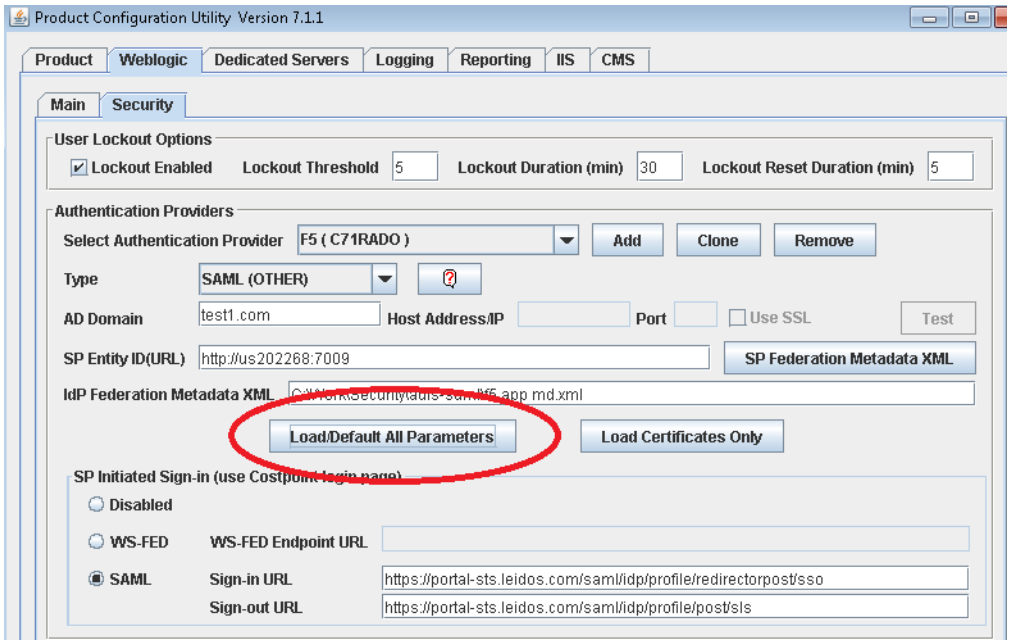
10. Return to Costpoint Configuration Utility, and enter **IdP Federation Metadata XML**.

    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.



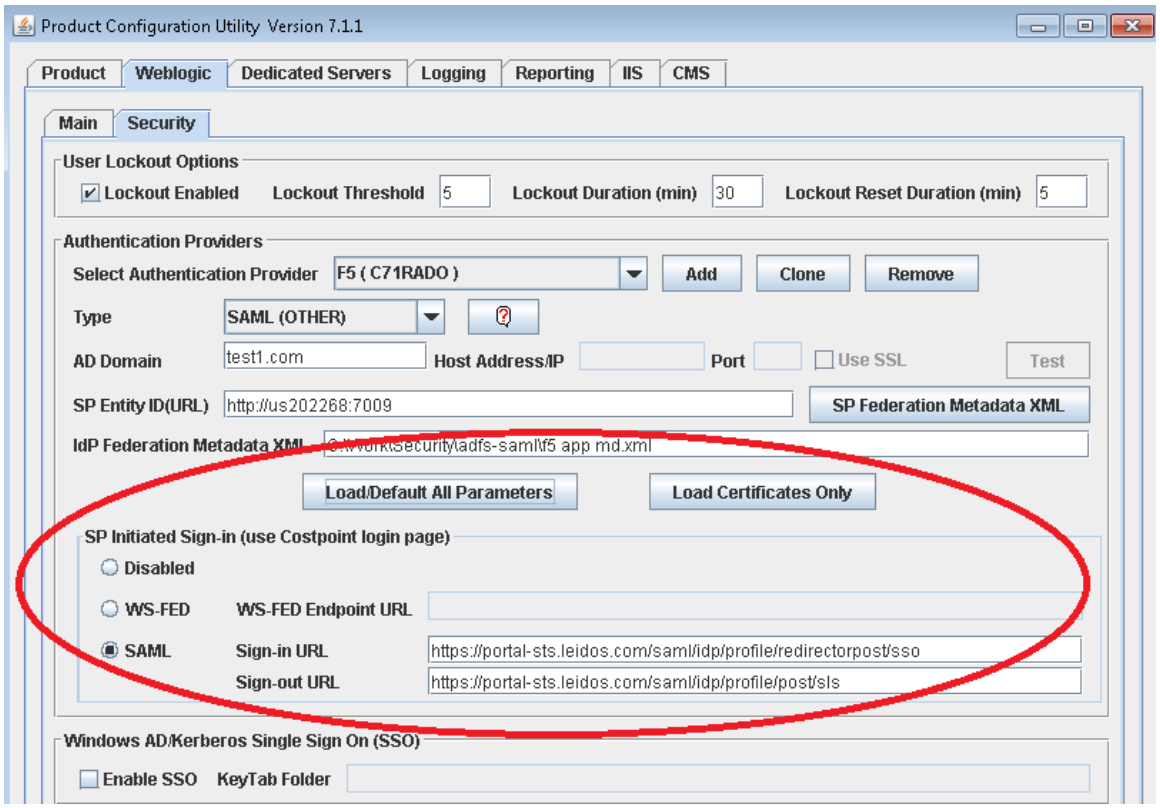

11. Click **Load/Default All Parameters**.

    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.

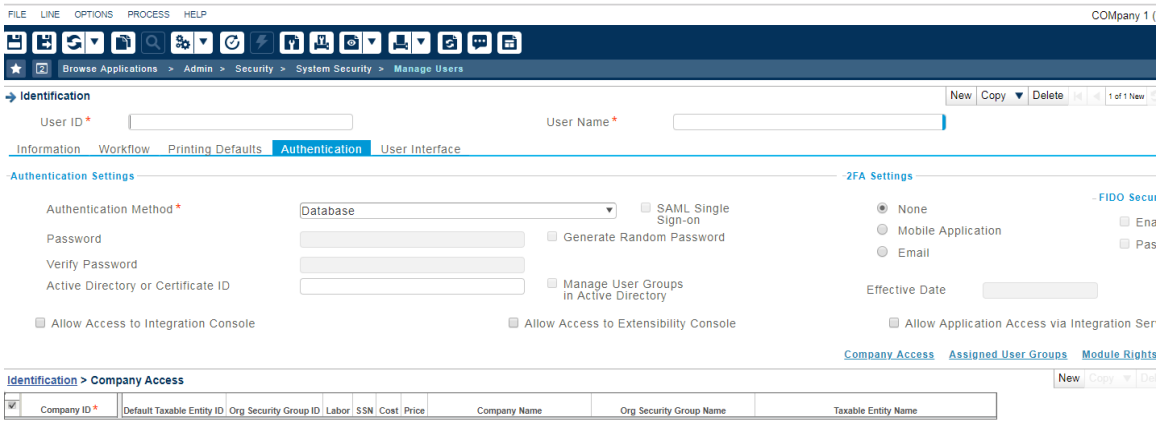



13. Click **Save**.

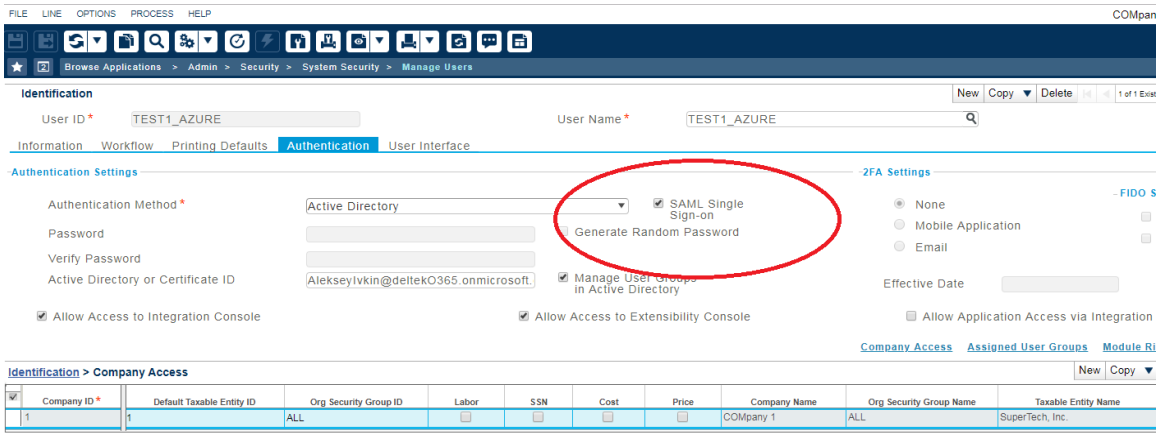
    Costpoint SAML Single Sign-on setup with SAML (Other) IdP is complete. You can activate SAML SSO mode for Costpoint user accounts.:

## 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** check box to allow the user to log into Costpoint in SAML SSO mode.




## Update SAML Provider settings in Costpoint Cloud

Costpoint Configuration Utility provides every capability to configure Costpoint authentication with SAML Provider. Deltek highly recommends that Costpoint Administrators use this tool to make changes related to such configurations.

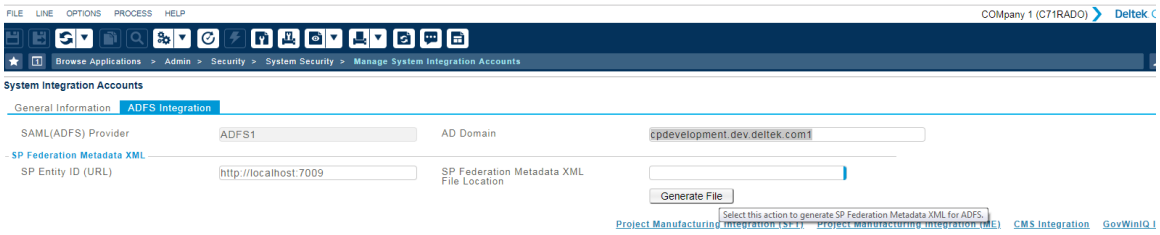
However, there may be use cases when Costpoint Administrators have limited access to the Costpoint/Weblogic server environments and therefore, may not always run Costpoint Configuration Utility. Typically, this is the case when Costpoint is deployed in the Cloud.

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

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

1. Click **Administration » Security » System Security » Manage System Integration Accounts**.
2. If AD FS was initially configured as the SAML Identity Provider for the current system, click the **ADFS Integration** tab.

If using Azure or SAML (Other), skip to step 4 and 5.




You use this tab to generate the **Costpoint_SP_FederationMetadata.xml** file. This file allows you to create and configure **Costpoint Relying Party Trust** automatically within the AD FS. This step is explained in the **Configure SAML Single Sign-on between Costpoint and Microsoft AD FS** section.

Enter the following:

- **SP Entity ID (URL)**: The value 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

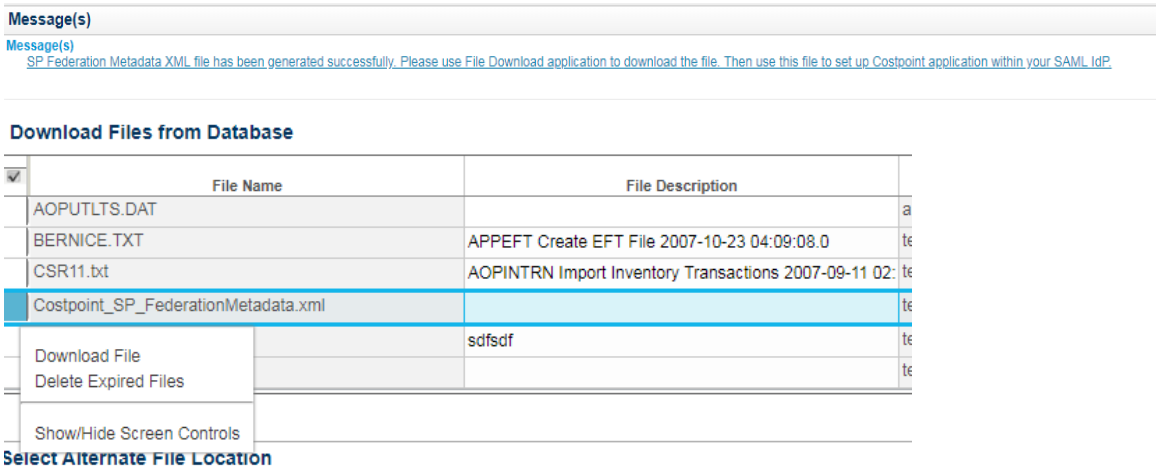
  The value is case-sensitive. It must match exactly (including the case) to the **Relying party trust identifier** in AD FS.
- **AD Domain**: Domain is your company's Windows AD domain. During SAML assertion verification, the system concatenates the **Domain** value with the **Active Directory ID** entered on the Manage Users screen.

  For example, if the **Active Directory ID** from Manage Users configuration is **john.smith** and the **AD Domain** is **us.mycompany.com**, the system will use **john.smith@us.mycompany.com** and will try to match it to the user principal name found in the Security Subject of SAML assertion. If it matches exactly (case-insensitive) and the SAML assertion signature is valid, the user is let into the system. Otherwise, the authentication request will be rejected.

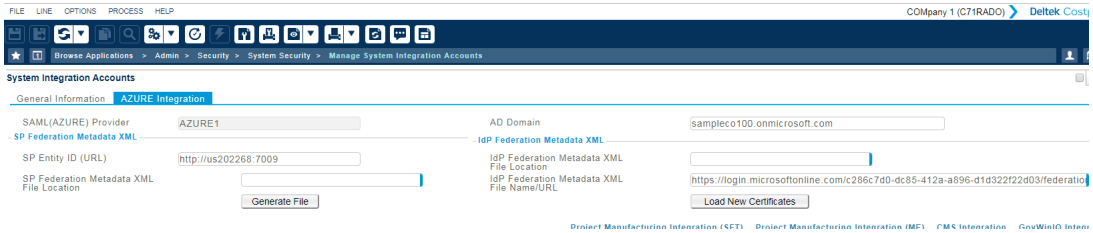
  Though it is not recommended, you can leave the **AD Domain** field blank, but you will have to enter a fully qualified name for the **Active Directory ID** on the Manage Users screen (for example, **john.smith@us.mycompany.com**, not just **john.smith**).
- **SP Federation Metadata XML File Location**: Enter the optional **Costpoint Alternate File Location** where you want to generate the **Costpoint_SP_FederationMetadata.xml** file. If you leave this blank, the **Costpoint_SP_FederationMetadata.xml** file will be generated in the database.

3. Click **Generate File**.

   After the file is generated, download the file using the standard **File Download/Download File from Database/Alternate File Location** function. Use downloaded file to automatically create and configure **Costpoint Relying Party Trust** within the AD FS.




4. If Azure was initially configured as SAML Identity Provider for the current system, click the **AZURE Integration** tab.




You use this tab to generate the **Costpoint_SP_FederationMetadata.xml** file. This file allows you to register the Costpoint application automatically within Azure. This step is explained in the “Configure SAML Single Sign-on between Costpoint and Microsoft Azure” section.

You can also use this tab to update the URL to Azure Federation Metadata XML file or to register new Azure certificates from the Azure Federation Metadata XML file, which is explained in the “Configure SAML Single Sign-on between Costpoint and Microsoft Azure” section. The preferred way is to use the URL to the Azure Federation Metadata XML file so that all of the Azure SAML settings, including certificates, will be loaded dynamically at run-time. If specifying the URL to the Azure Federation Metadata XML file is not possible, you can manually update the Azure certificates from the Azure file:

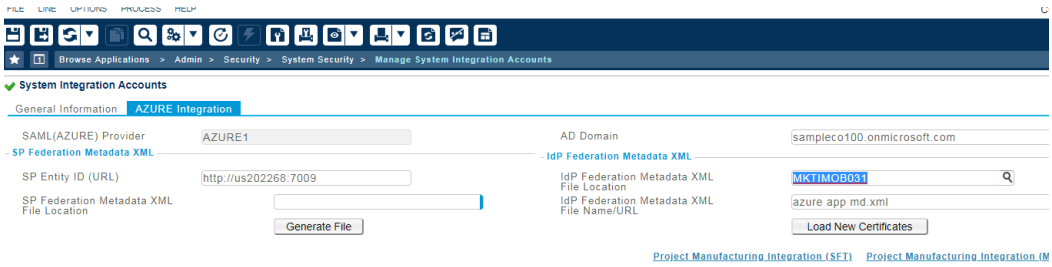
a. Upload Azure Federation Metadata XML file into Costpoint, using either the **File Upload** function or by copying the file into the **Costpoint Alternate File Location.**

b. In the **IdP Federation Metadata XML File Location** field, enter the optional **Costpoint Alternate File Location** from which you want to read the Azure Federation Metadata XML file.

   If you leave this blank, Costpoint reads the Azure Federation Metadata XML file from the database.

c. In the **IdP Federation Metadata XML File Name/URL** fields, enter the file name or use a lookup to select the file name.

d. Click **Load New Certificates** to register new Azure certificates from Azure Metadata XML file.




You can also update the **SP Entity ID (URL)** property. The value is defaulted by **Enterprise App External URL**. You can change this value and use other Identifier as **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

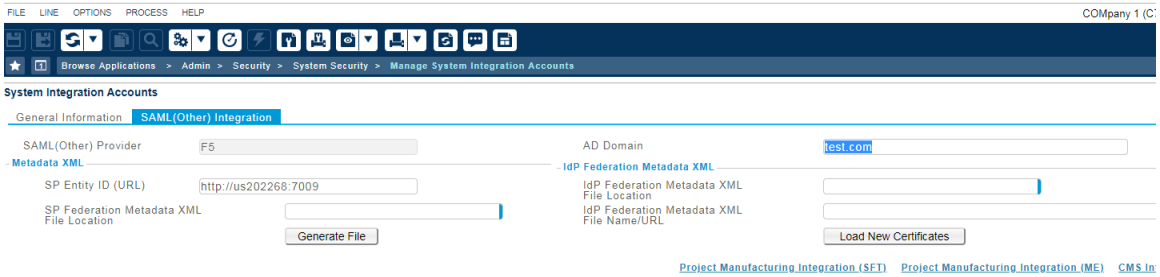
The value is case-sensitive. It must match exactly (including the case) to the **Identifier (Entity ID)** in Azure.

You can also update the **AD Domain** property. Domain is your company's Windows AD domain. During SAML assertion verification, the system concatenates the **Domain** value with the **Active Directory ID** entered on the Manage Users screen.

For example, if the **Active Directory ID** from Manage Users configuration is **john.smith** and the **AD Domain** is **us.mycompany.com**, the system will use **john.smith@us.mycompany.com** and will try to match it to the user principal name found in the Security Subject of SAML assertion. If it matches exactly (case-insensitive) and the SAML assertion signature is valid, the user is let into the system. Otherwise, the authentication request will be rejected.

5. If SAML (Other) Provider (for example, Okta, Ping-Federate, or F5) was initially configured as the SAML Identity Provider for the current system, click the SAML (Other) integration tab.

   Same as with Azure, use this tab to generate the **Costpoint_SP_FederationMetadata.xml** file. This file allows you to register the Costpoint application automatically within your other SAML IdP. This step is explained in the "Configure SAML Single Sign-on between Costpoint and other SAML Identity Providers" section.




   You can also update the **SP Entity ID (URL)** property. **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.

   You can also update the **AD Domain** property. Domain is your company's Windows AD domain. During SAML assertion verification, the system concatenates the **Domain** value with the **Active Directory ID** entered on the Manage Users screen.

   For example, if the **Active Directory ID** from the Manage Users configuration is **john.smith** and the **AD Domain** is **us.mycompany.com**, the system will use **john.smith@us.mycompany.com** and will try to match it to the user principal name found in the Security Subject of SAML assertion. If it matches exactly (case-insensitive) and the SAML assertion signature is valid, the user is let into the system. Otherwise, the authentication request will be rejected.

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

Setting up 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 Four: Configure Internet Explorer to work with this configuration.

## 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.

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.

   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.

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_weblogic@DOMAINY.COM -pass password -crypto ALL -ptype
   KRB5_NT_PRINCIPAL -out C:\sso_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
   ```

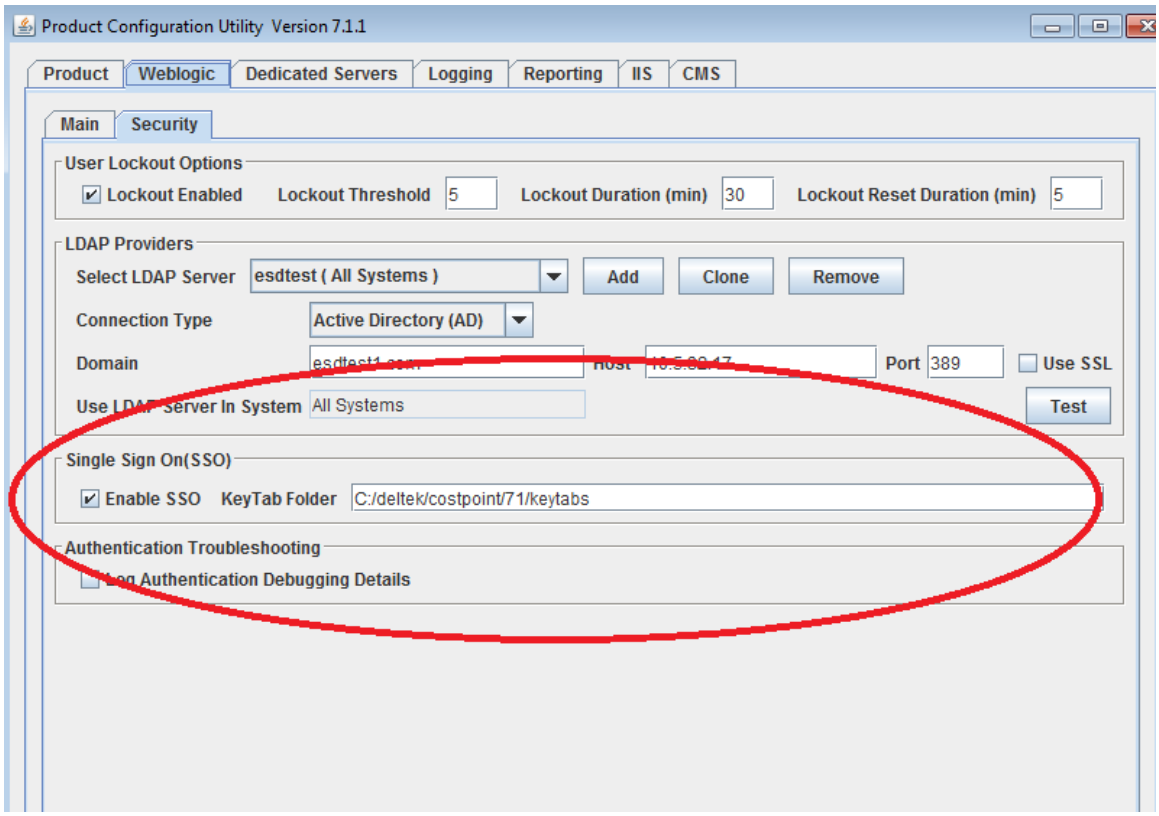
   

   This step is critical. If the same service is linked to a different account in the Active Directory server, the client does not send a Kerberos ticket to the server.

## 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).

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

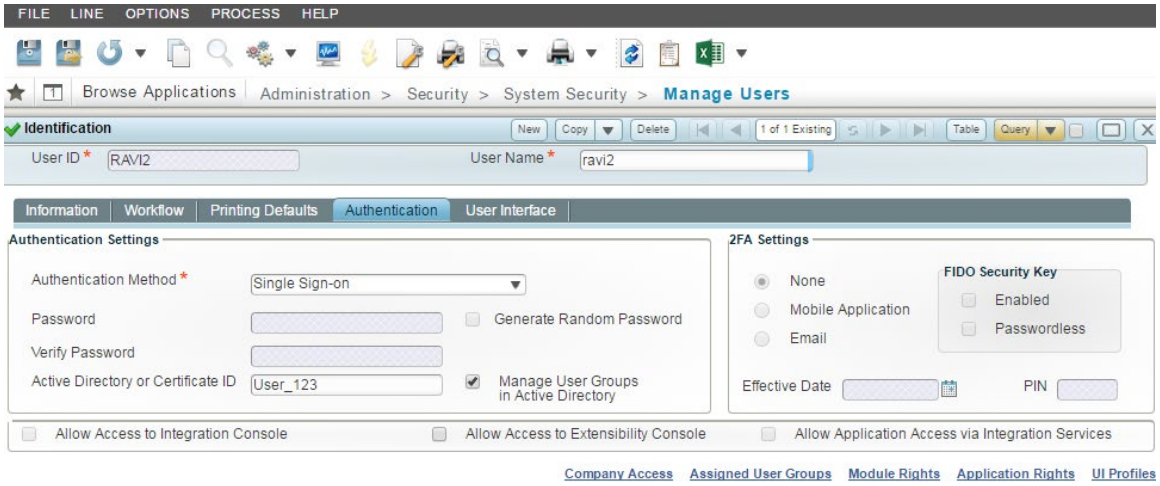
The WebLogic servers need to be restarted when enabling SSO for the first time. For a cluster configuration, all nodes and the admin server have to be restarted. Further changes to the keytab folder (such as adding a new keytab, editing, or removing a file) will not require restarting the

servers. Such changes can be applied at runtime by running the Rebuild Global Settings application.

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

**To update the user setup in Costpoint using Manage Users application to use 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 Single Sign-On authentication method.
4. Click the Authentication tab.
5. In the **Authentication Method** field, select **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 Single Sign-On authentication method.

## Step Four: Configure Internet Explorer to Work with Single-Sign On

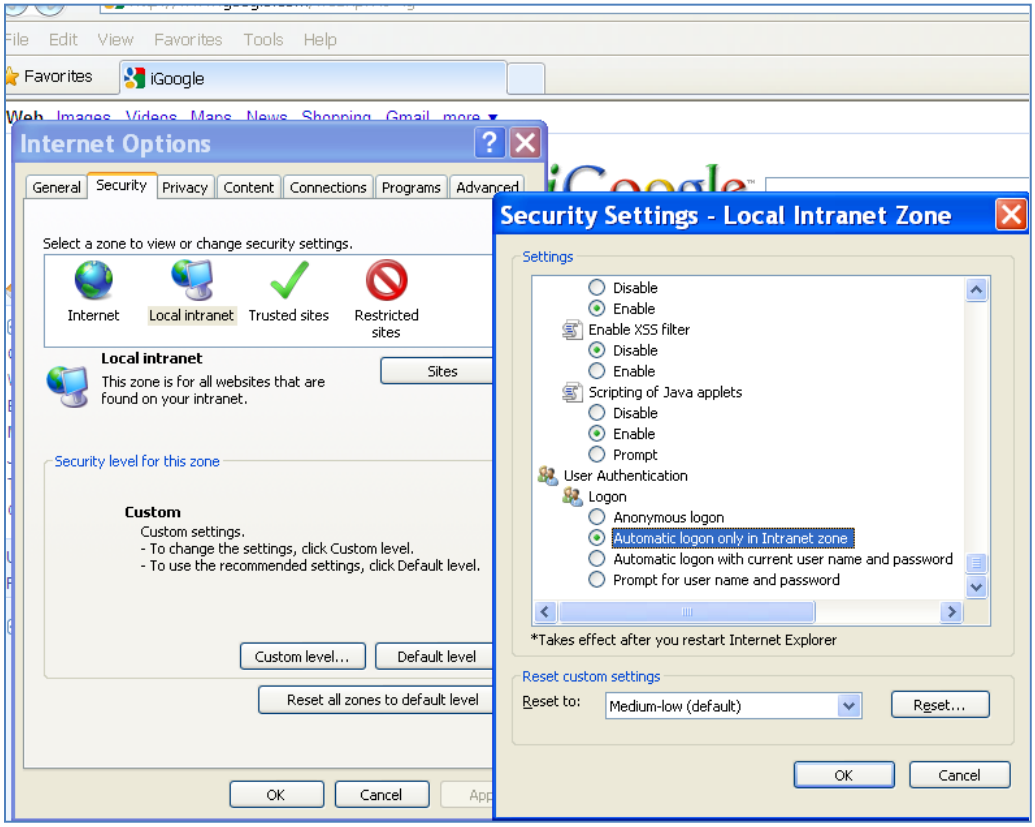
**To enable clients to use Single Sign-On with Internet Explorer browsers**:

1. Add the Costpoint URL to your Local Intranet zone sites:
   a. From Internet Explorer, click **Tools » Security » Local intranet » Sites » Advanced**.
   b. Add the Costpoint URL to the list of local intranet sites.

   Use only the fully qualified WebLogic machine name in the Costpoint URL.

This should be the name that was configured on the Active Directory machine using **ktpass** (for example, **http://appserver.domainx.com**).

2. On the Security tab, click the **Custom Level** button.
3. Under **User Authentication/Logon**, verify that the **Automatic Logon Only in Intranet zone** option is selected.



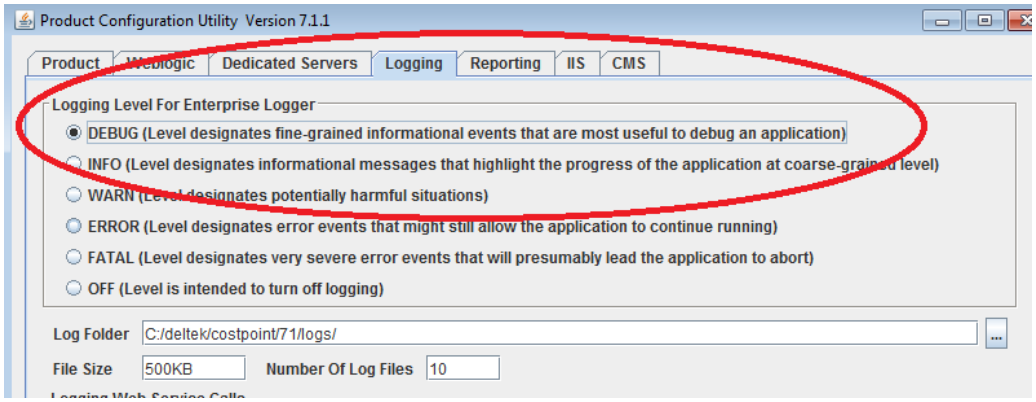

3. Click **Tools » Internet Options » Advanced**, and ensure that the **Enable Integrated Windows Authentication** option is selected.

# Single Sign-On Troubleshooting

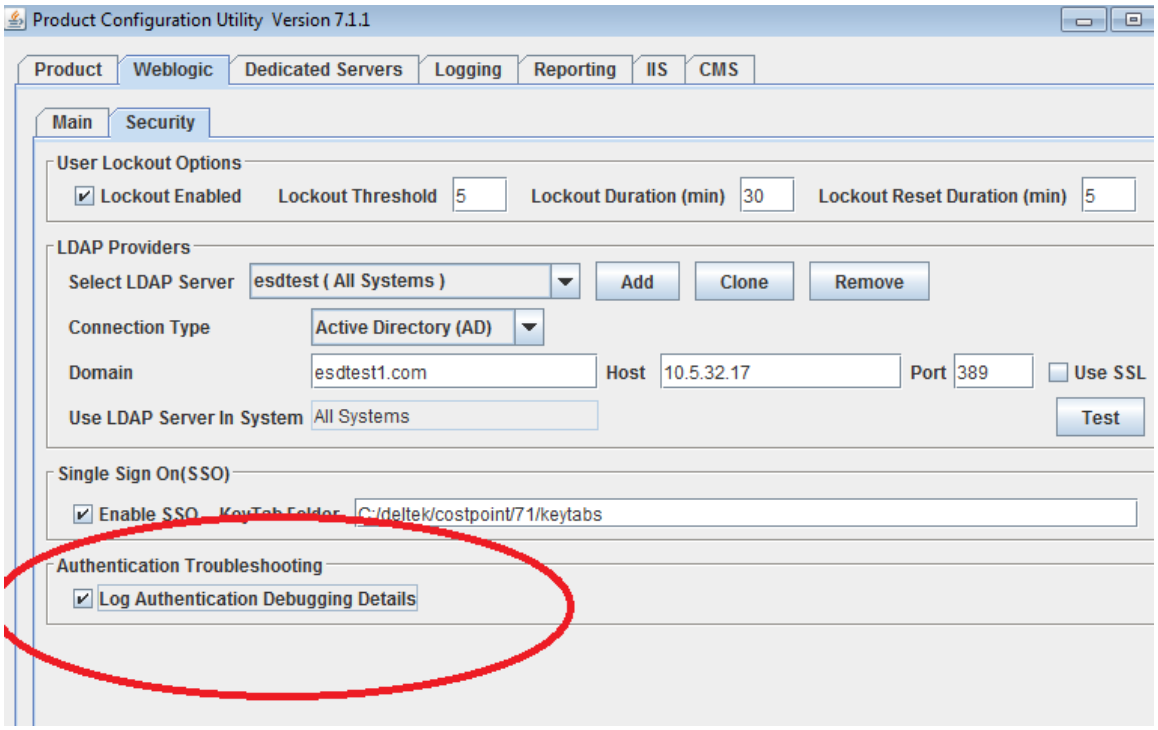
Troubleshooting Single Sign-On related problems cannot be performed during production hours while end users are actively accessing the applications. It needs to be scheduled during downtime without any user activity.

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

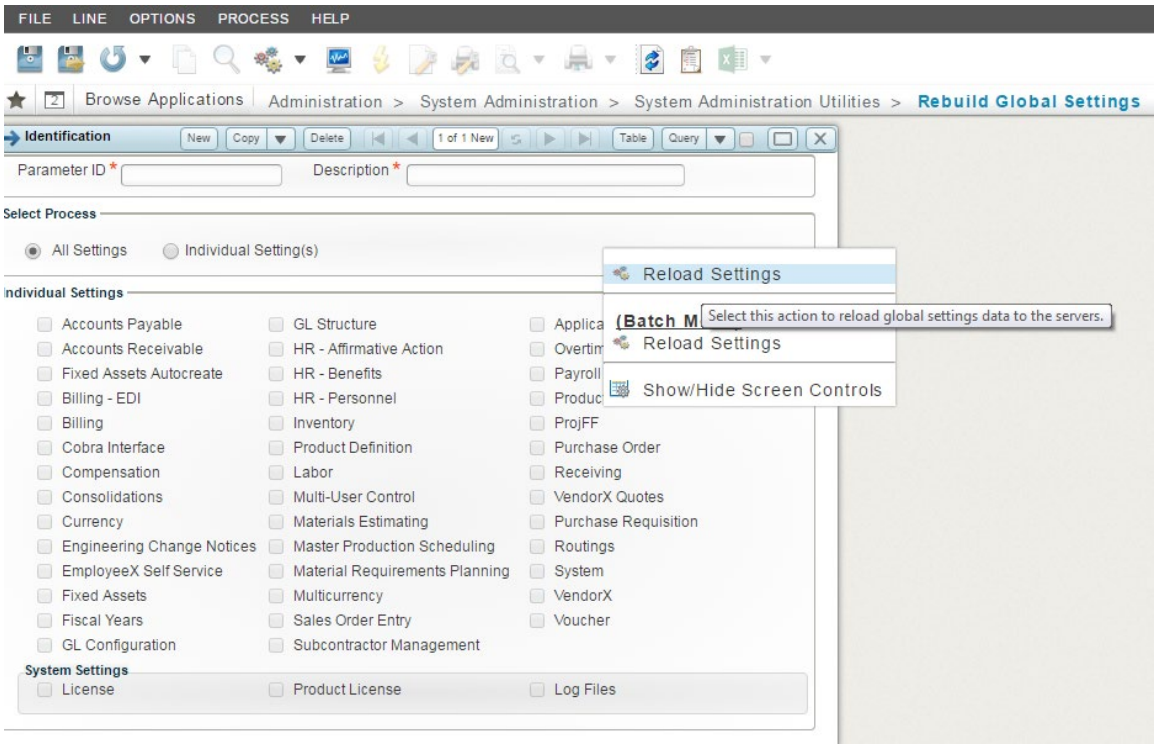
1. On the Logging tab, change the **Logging Level for Enterprise Logger** to **DEBUG**.




2. On the **Weblogic » Security tab**, select the **Log Authentication Debug Details** check box.



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 ht**tp**:**//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 WiFi (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.

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

In order 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

Follow the steps below to enable Client Certificate authorization.

## Two Setup Methods

You can use either of these approaches to Client Certificate authorization.

- **Browser » WebLogic Server**

  With this authentication method, all the communication between the browser and the WebLogic Server is over https protocol. Therefore, WebLogic Server must be configured to support two-way SSL.

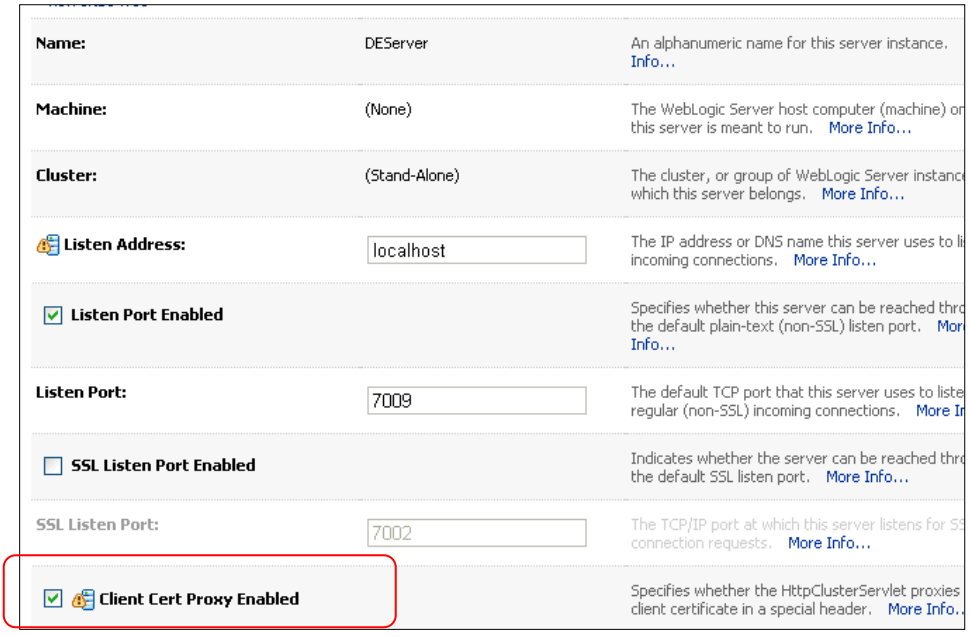
- **Browser » IIS » WebLogic Server (Cluster of WebLogic Servers)**

  With this configuration, all communication between the browser and IIS occurs over https protocol. The communication between IIS and the WebLogic Server can be implemented over https or just http. If the WebLogic Server (or WebLogic Server Cluster) and IIS sit inside the same local area network, Deltek recommends that you use http (not https) between IIS and WebLogic Server, because the SSL encryption and decryption routine creates unnecessary overhead between two (or more that two, if you use a WebLogic Server Cluster) trusted peers.

  In addition, you have to configure the IIS proxy to forward client certificates to the WebLogic Server (or the WebLogic Server Cluster).

  **To configure the IIS proxy to forward client certificates**:

  1. Log into the WebLogic Server console, and navigate to **Environment » Server » General**.
  2. Select the **Client Cert Proxy Enabled** check box. If you are using a WebLogic Server Cluster, make the change for each server node.



## Requirement for Valid Certificate

Both approaches to Client Certificate authentication require that the client (browser) has a valid certificate that can be trusted by WebLogic Server or IIS. The certificate must be installed on each user's machine. The next steps assume that the client has a valid certificate. This certificate must be imported into the browser.

**To import a certificate into the browser (for example, Internet Explorer)**:

1. Obtain a signed personal certificate from your organization's IT department, VeriSign, or another trusted certificate authority.
2. In Internet Explorer, click **Tools » Internet Options » Content tab » Certificates » Personal**.
3. Click **Import**, and use the Certificate Import wizard to import the certificate. When prompted, enter the password associated with the certificate.
4. Open the Costpoint Login page.

   For example:

   - https://costpoint_server:7002 (**Browser » WebLogic Server**)
   - https://costpoint_server/CPWeb (**Browser » IIS » WebLogic Server**)

   You should be able to log in to Costpoint without providing a User ID and password on the Costpoint Login page.

# 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.

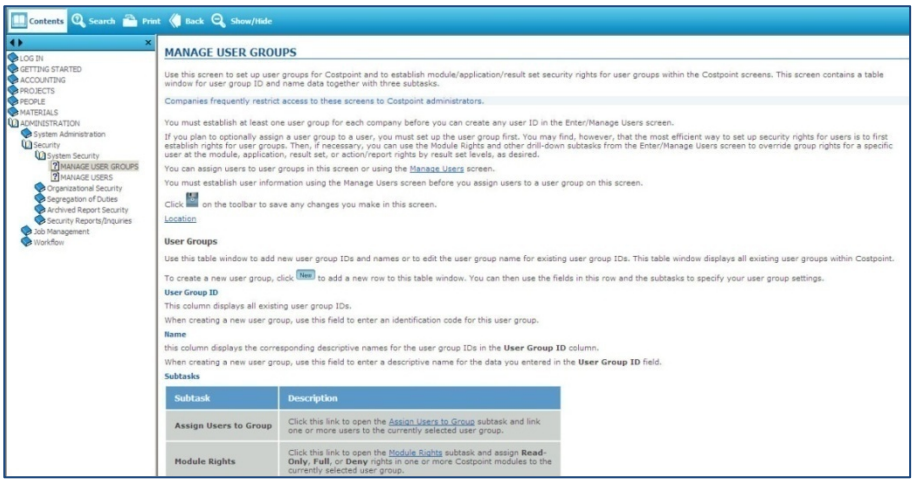
Also for new installations and for upgrades from previous versions of Costpoint for which the **Apply Default User Groups and Permissions** option was selected, the installation will add an out-of-the-box, predefined set of user groups and permissions. The idea is to help clients by giving them a template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

The Costpoint 7 online help provides detailed instructions for assigning rights to users. Look under **Administration » Security**.




Follow these guidelines:

In Costpoint 7, 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 7, unlike previous versions of Costpoint, 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.

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.

### Hierarchy of Security Settings for Users

**Maintain Users (SYMUSR) [W_USER_UGRP_LIST, filter on TYPE = U]**

- User Company Access [W_USER_COMPANY]
- Assign Groups to User [W_USER_GRP_USERS]
- Web Module Rights [W_MODULE_RIGHTS]
  - Web Application Rights by Module [W_APP_RIGHTS]
    - Result Set Rights by Application [W_RS_RIGHTS]
      - Action Rights by Result Set [W_ACTION_RIGHTS]
      - Report Rights by Result Set [W_RPT_RIGHTS]

### Hierarchy of Security Settings for Users

**Maintain User Groups (SYMGRP) [W_USER_UGRP_LIST, filter on TYPE = G]**

- Assign Users to Group [W_USER_GRP_USERS]
- Web Module Rights [W_MODULE_RIGHTS]
  - Web Application Rights by Module [W_APP_RIGHTS]
  - Result Set Rights by Application [W_RS_RIGHTS]
    - Action Rights by Result Set [W_ACTION_RIGHTS]
    - Report Rights by Result Set [W_RPT_RIGHTS]

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

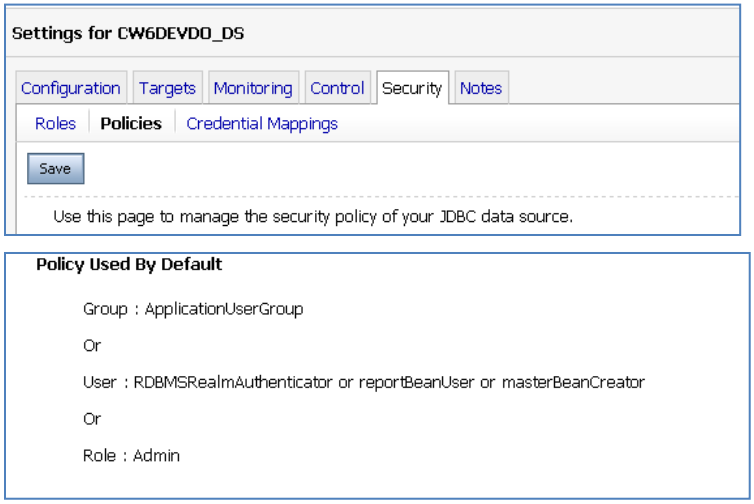
Each of these components and services must be protected; there are security polices implemented for each component. Implementation of these polices is vendor-specific.

## 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:



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.

Deltek is the leading global provider of enterprise software and information solutions for government contractors, professional services firms and other project- and people-based businesses. For decades, we have delivered actionable insight that empowers our customers to unlock their business potential. 20,000 organizations and millions of users in over 80 countries around the world rely on Deltek to research and identify opportunities, win new business, recruit and develop talent, optimize resources, streamline operations and deliver more profitable projects. Deltek – Know more. Do more.®

deltek.com