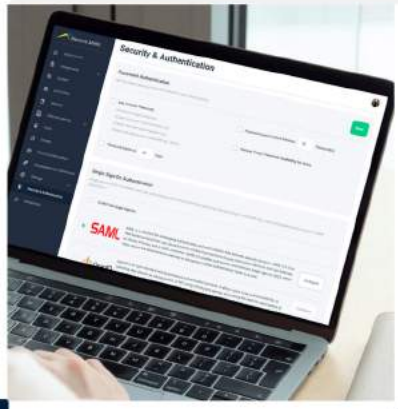
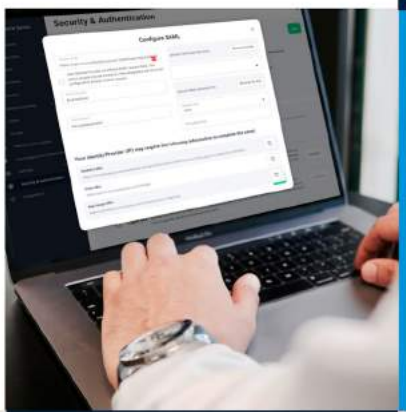
Security and Authentication Pinnacle Series Single Sign-On and Password Settings

Single sign-on is an authentication method that allows users to sign in using one set of credentials to multiple independent software systems.

With SSO, users can access all needed applications without being required to authenticate using different credentials.





Overview

This guide offers a comprehensive, step-by-step tutorial on setting up Single Sign-On (SSO) for seamless synchronization between your identity provider or SSO Service and Pinnacle Series. By following these instructions, you can establish a streamlined and secure user experience, enhancing the efficiency of your authentication process.

Microsoft renamed Azure Active Directory (Azure AD) to Microsoft Entra ID in January 2024. The names Azure Active Directory, Azure AD, and AAD are replaced with Microsoft Entra ID.

01 Benefits of Microsoft Entra ID Single Sign-On

02 Pre-Requisite Checks and Recommendations

03 Password Authentication Settings

04 Tactical Guidance

- SAML
- OpenID
- Exchange Web Services

Benefits of Microsoft Entra ID Single Sign-On:

Unlock streamlined access, heightened security, and efficient user management with Microsoft Entra's federated single sign-on. This method, compatible with SAML 2.0 applications, seamlessly authenticates users through their Microsoft Entra accounts, reducing password hassles.

- **Streamlined Access:**
  - Microsoft Entra ID SSO allows users to access multiple applications with a single set of credentials, reducing the need for multiple logins and simplifying the user experience.

- **Enhanced Security:**
  - By centralizing access controls, Microsoft Entra ID SSO helps organizations enforce consistent security policies, ensuring that users only have access to the resources they need. This contributes to a more robust security posture.

- **Efficient User Management:**
  - The configuration of Microsoft Entra ID SSO simplifies user provisioning and de-provisioning, enabling IT administrators to manage user accounts more efficiently. This is particularly beneficial in dynamic and rapidly changing organizational environments.

- **Password Efficiency:**
  - Microsoft Entra ID SSO streamlines user experience by requiring only a single set of credentials, reducing both IT support burden and potential password-related issues.

- **Enhanced Security:**
  - With multi-factor authentication support, Microsoft Entra ID SSO adds an extra layer of protection to sensitive data and applications, fortifying the authentication process.

Pre-Requisite Checks and Recommendations

Microsoft Entra Subscription and Permissions

- Microsoft Entra subscription
- One of the following roles:
  - Global Administrator
  - Cloud Application Administrator
  - Application Administrator
  - Owner of the service principal

- Ensure that you have Pinnacle Series administrator permissions

Network Connectivity:

- Check for stable internet connectivity as configuration processes may involve online authentication and data synchronization.

Before proceeding with the configuration, ensure that the pre-requisites are in place.

SAML vs OpenID vs Exchange Web Service

- We recommend SAML or OpenID for SSO configuration as they are designed with security best practices in mind, including token-based authentication and secure assertions.

- Exchange Web Service is not a dedicated SSO protocol, and using it for authentication purposes may introduce security risks. Additionally, it's important to note that Microsoft has announced the retirement of this service by the year 2026.

Key Considerations SAML vs Open ID

Maturity and Adoption:

- SAML has been around longer and is a widely accepted standard for SSO in enterprise environments. It has a proven track record and widespread adoption, especially in scenarios where SSO is critical.

Assertion-based vs. Token-based:

- SAML is assertion-based, while OpenID is token-based. Some organizations prefer assertions as they are XML-based and can be easily parsed and processed. This can be beneficial for certain integration scenarios.

Fine-Grained Access Control:

- SAML supports more granular access control through its Attribute Statements, allowing for the exchange of additional user attributes along with authentication. This can be useful in scenarios where detailed user information is required for authorization decisions.

Legacy Systems:

- If you have existing systems that already use SAML for SSO, it may be more straightforward to continue with SAML to maintain compatibility and avoid the need for additional infrastructure changes.

XML vs. JSON:

- SAML messages are typically XML-based, while OpenID messages use JSON. Depending on your existing infrastructure and preferences, you may find one data format more compatible or easier to work with than the other.

Security Features:

- SAML has been designed with security as a top priority and includes features like digital signatures for messages and assertions, which can enhance the overall security of the SSO process.

SECURITY AND AUTHENTICATION

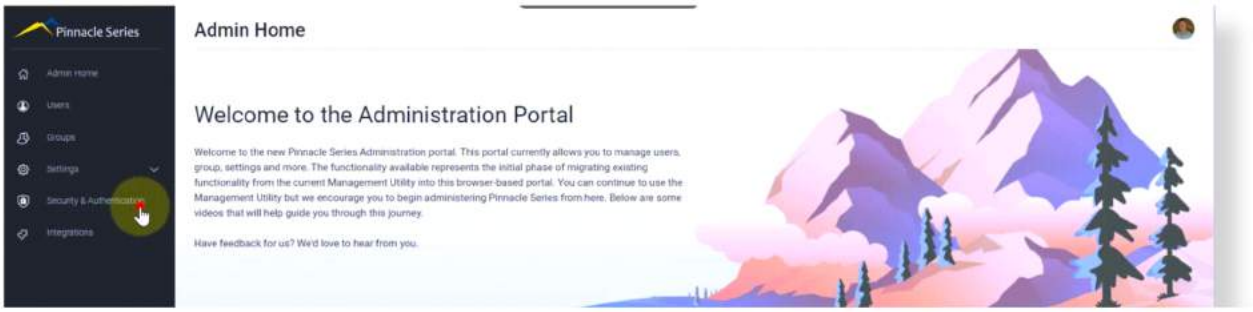
Password Authentication Settings

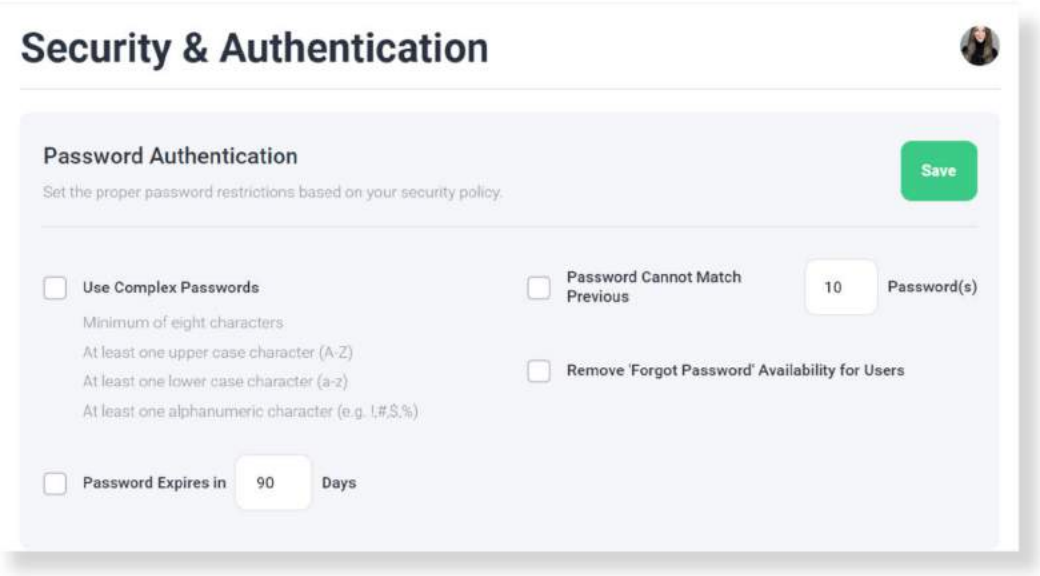
PINNACLE SERIES

by EAGLE POINT SOFTWARE

Password Authentication Settings

- Begin by logging into your Pinnacle Series web tenant and log into the Admin Portal.
- Navigate to the Security and Authentication menu, then review the Password Authentication section.





- Password Authentication settings provide administrators the ability to place requirements on Pinnacle Series login passwords such as:
    - **Complexity** - Complex passwords often include a combination of uppercase and lowercase letters, numbers, and special characters.
    - **Expiration intervals** - How frequently users are required to change their passwords
    - **Historical matching** - Historical matching involves preventing users from reusing old passwords when creating a new one.

Password Authentication Settings

- **Configure 'Use Complex Passwords':**
  - Toggle on the "Use Complex Passwords" option.
  - New passwords must meet the following criteria:
    - Minimum of eight characters
    - Note maximum character length for complex passwords is 20
    - At least one uppercase and lowercase character
    - Must contain at least one special character (e.g., exclamation point or dollar sign)

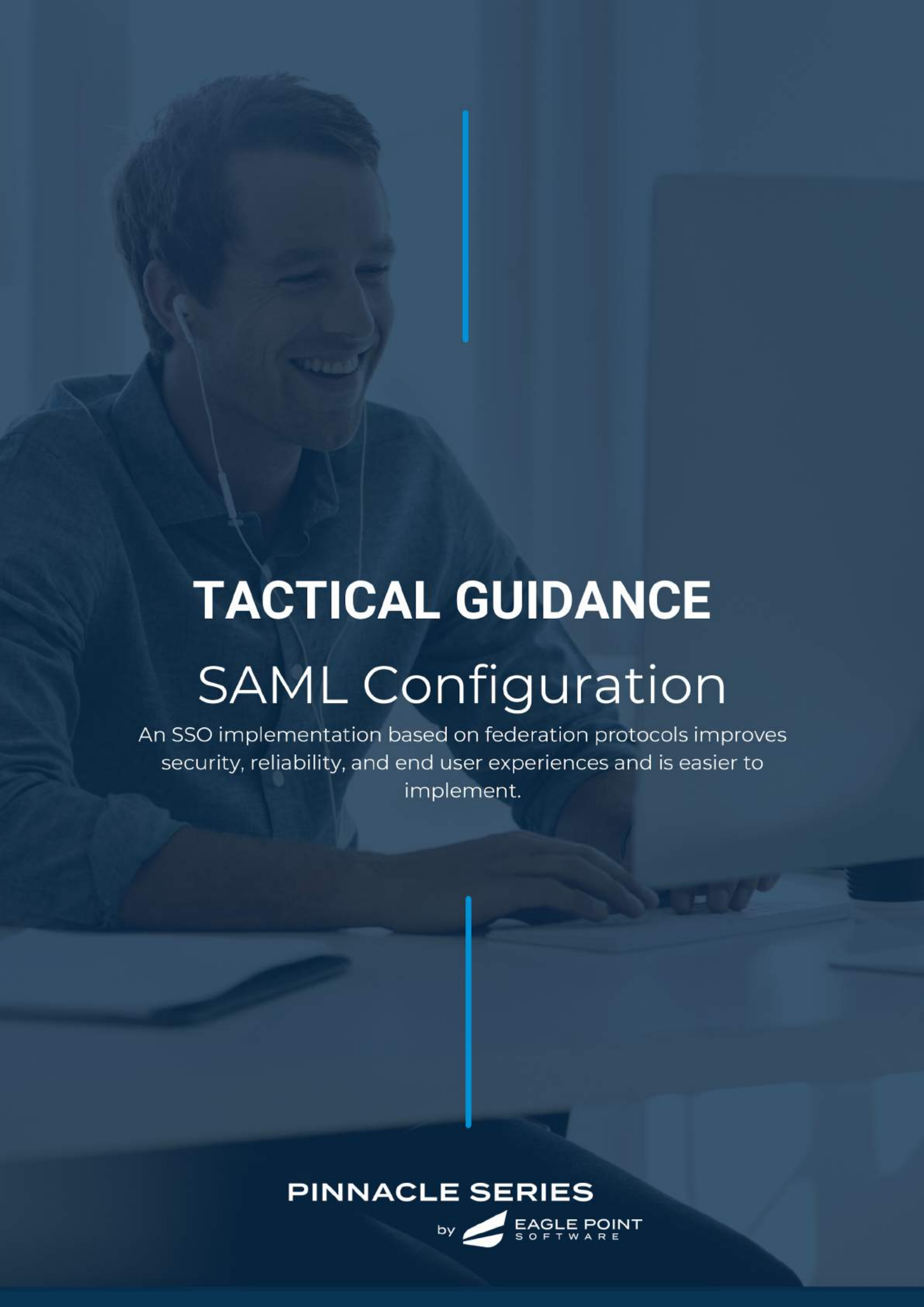
- **Configure Password Expiry:**
  - Toggle on the "Password Expires" option
  - Define the interval for password expiration within the "Days" field (e.g., set it to every 90 days)

- **Configure Historical Match Period:**
  - Toggle on and define the historical match period for passwords
  - This restricts the reuse of recent passwords, enhancing overall account security

- **Configure Remove Forgot Password:**
  - Toggle on the "Remove Forgot Password" option
  - This restricts standard end users from the self-service function of resetting their password
  - Organizational administrators must initiate the reset of any Pinnacle Series login credentials

Conclusion

These configurations contribute to a more secure environment by enforcing complex password requirements, managing password expiration, and limiting the ability to reuse historical passwords.



TACTICAL GUIDANCE

SAML Configuration

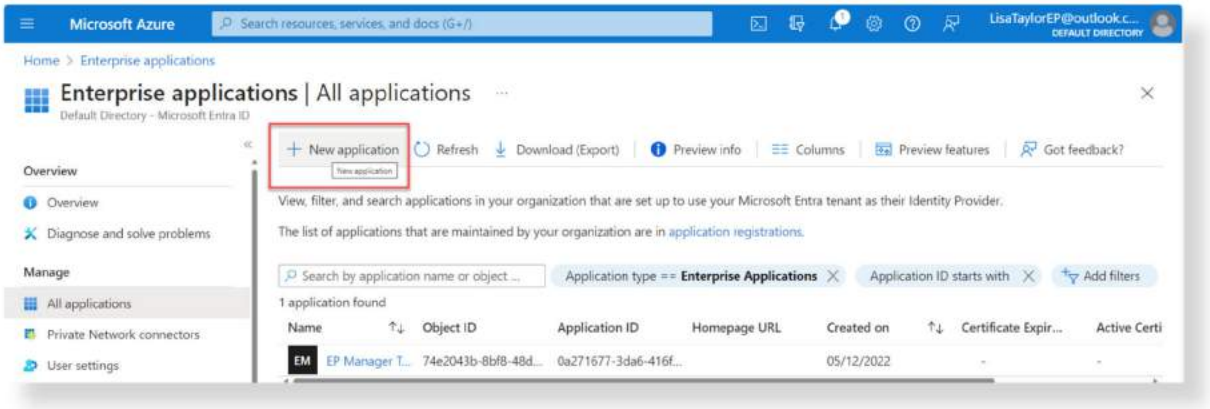
An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement.

PINNACLE SERIES

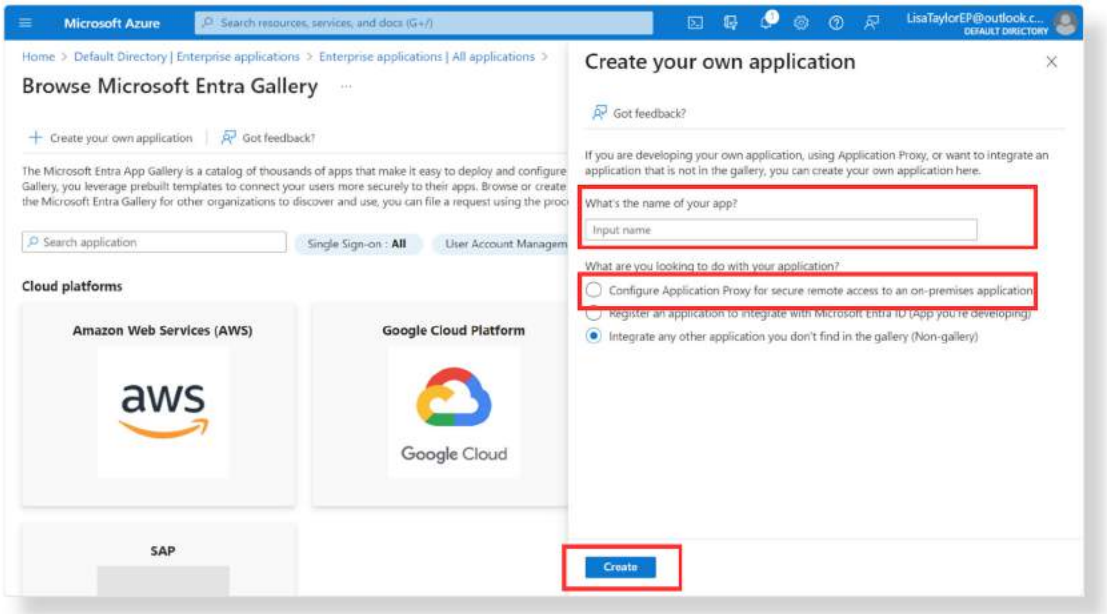
by EAGLE POINT SOFTWARE

Microsoft Entra ID SSO Configuration

- Within the Microsoft Entra ID Admin Portal, select the Microsoft Entra ID Service.
- Navigate to 'Enterprise Applications' on left-hand side of screen
  - Select 'New Application'.

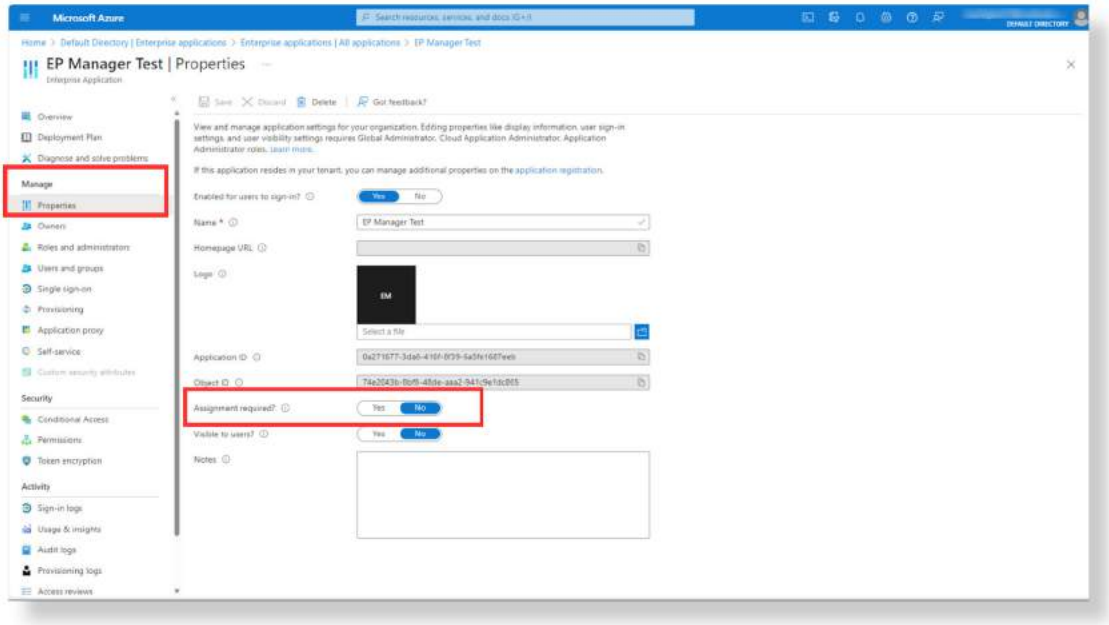


- Name application:
  - 'PinnacleSeriesSSO' *or*
  - 'ProductivityNowSSO' *or*
  - Something easily identifiable, with no spaces between letters.
- *If you've already created an app for Active Directory sync, we recommend using a similar naming convention).*
- Leave as 'Non-Gallery App' (see screenshot below) and click 'Create'

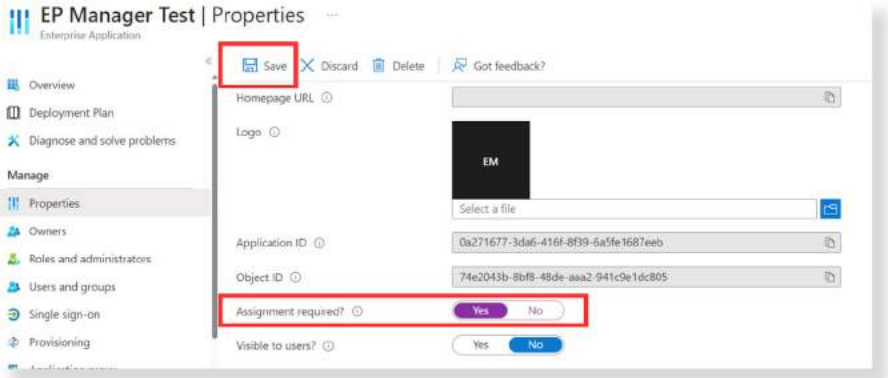


Microsoft Entra ID SSO User Assignment

- When configuring your SSO application in Azure, you have two options for specifying which of your users can utilize SSO in the Pinnacle Series platform. The options are based on the Yes/No value of the Assignment Required field, found under Manage > Properties.

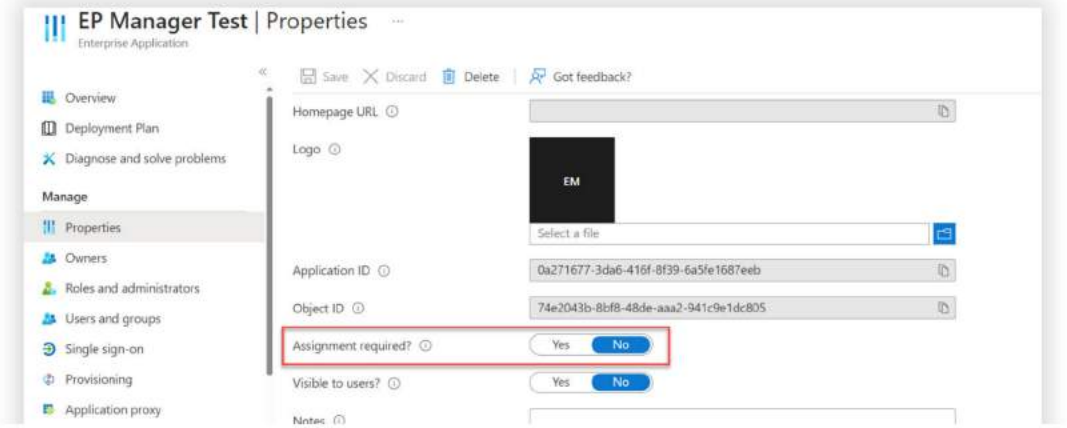


- Restrict access to specific Users and Groups (Assignment Required = “Yes”)
  - If you only want to grant SSO access to certain users, or groups of users, you would set the Assignment Required option to “Yes”, then hit Save near the top left.



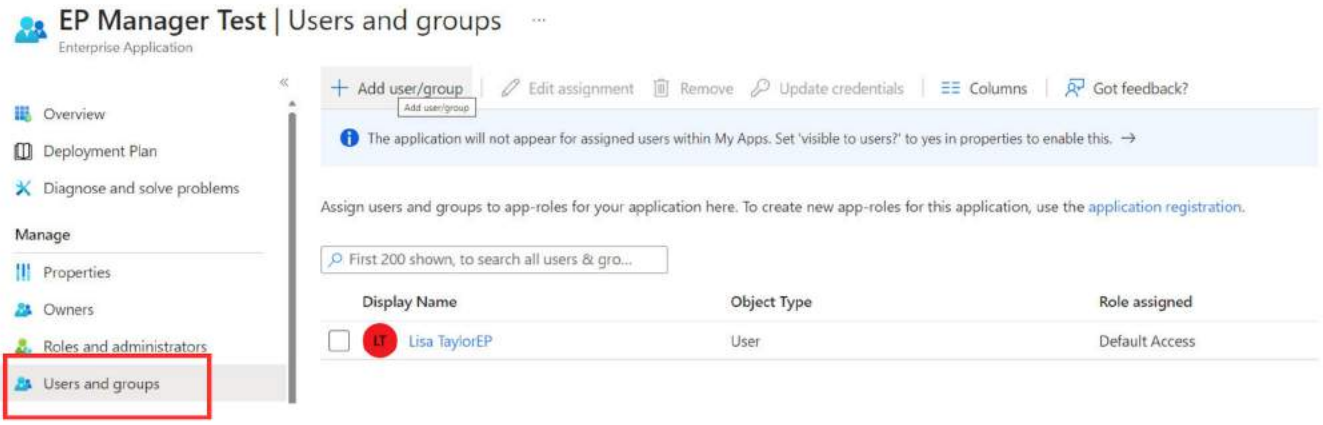
Microsoft Entra ID SSO User Assignment

- Allow SSO access to all users with a Pinnacle Series account (Assignment Required = “No”)
  - If you would like **anyone** at your organization with a Pinnacle Series account to utilize SSO, you would set the Assignment Required option to “No”, then hit Save near the top left.

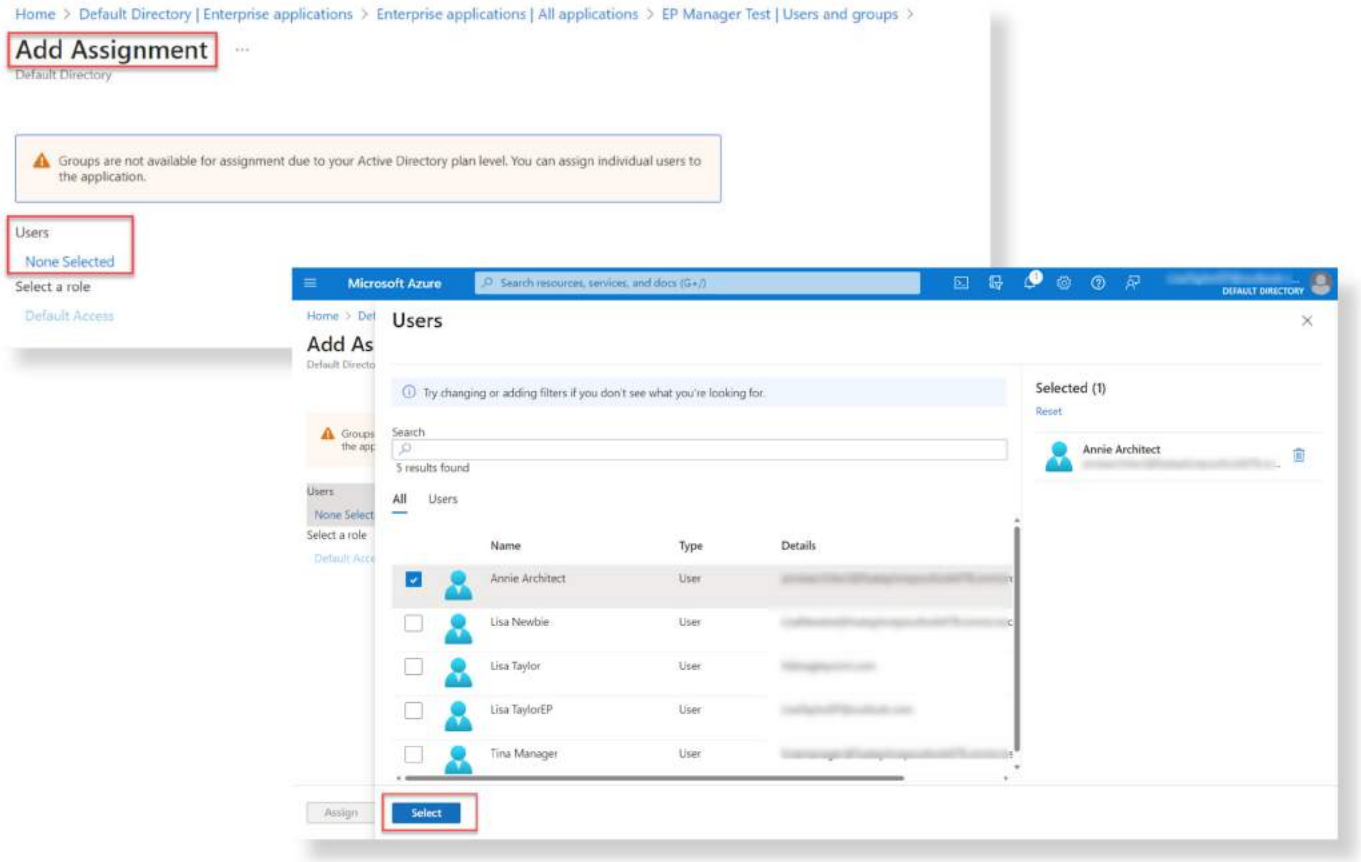


Microsoft Entra ID SSO User Assignment

- Once saved, if you set 'Assignment Required' to 'Yes', then navigate to "Users and groups" under the Manage section
- Choose Add user/group

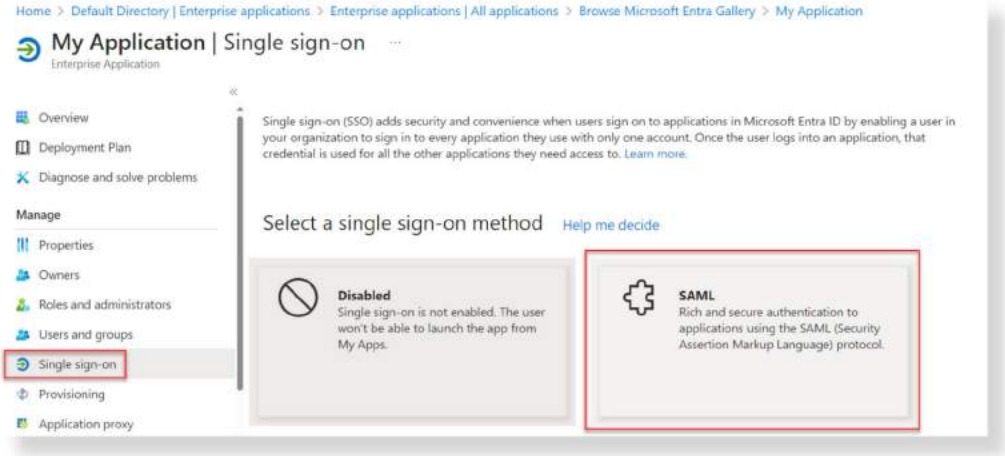


- Click "None Selected" under the appropriate headings to search for the users/groups.
- Once a user is found in the search, click their name, hit Select, then click Assign at the bottom left of the 'Add Assignment' screen.

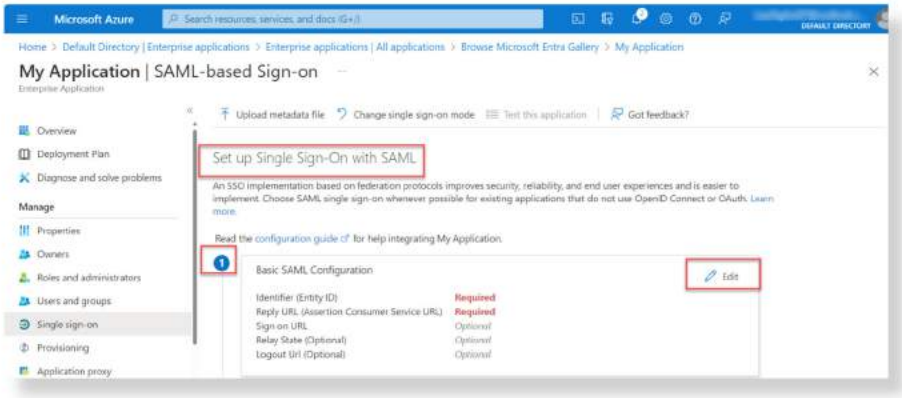


Microsoft Entra ID SSO Configuration - SAML

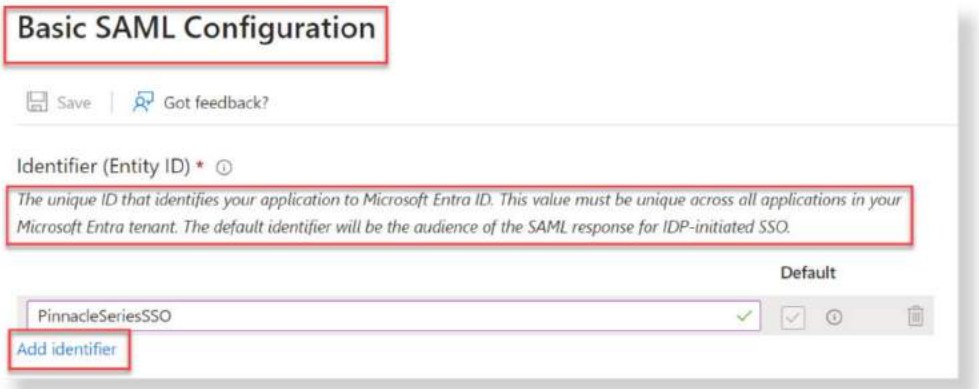
- Select 'Single sign-on'.
  - Choose SAML.



- Select 'Edit' in Section 1. (Basic SAML Configuration)

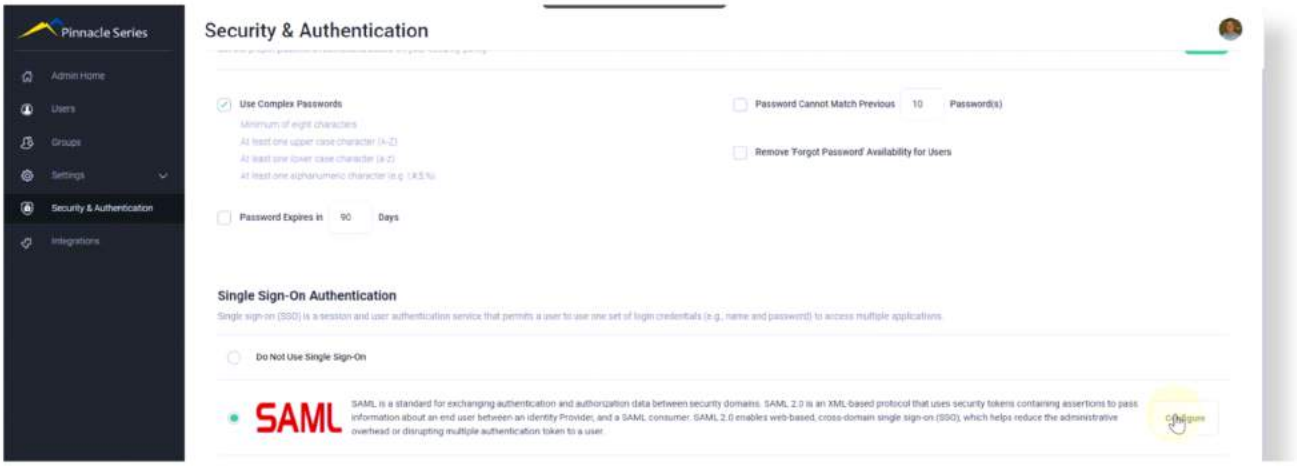


- Click "Add Identifier"
- Under Identifier (Entity ID), enter the app name (e.g. PinnacleSeriesSSO or ProductivityNowSSO).
- Make sure the box for 'Default' is checked.

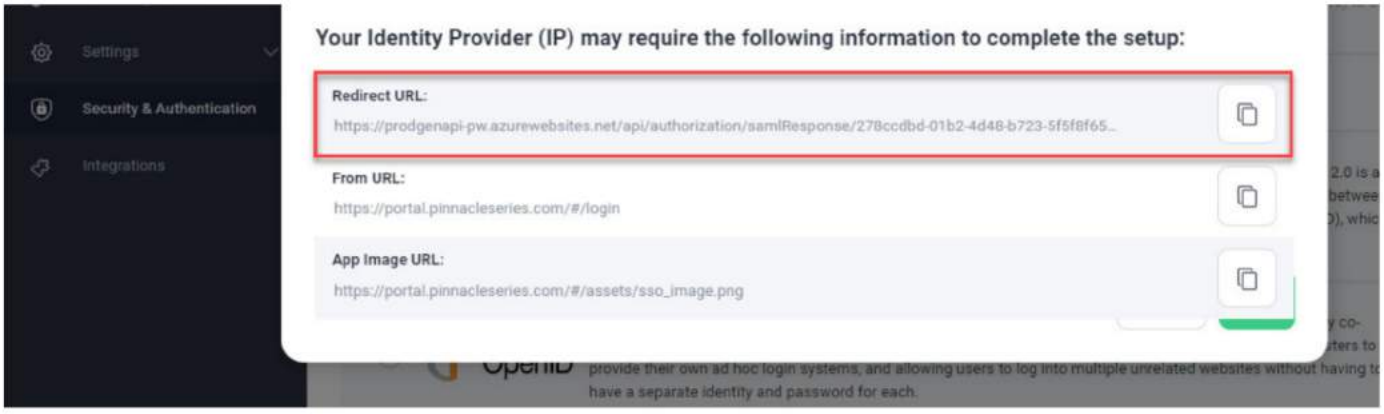


Admin Browser Configuration - SAML

- Next, with Azure still open on the edit screen from, open a browser window, log into the Pinnacle Series portal, and launch the Administration Portal.
- Once launched, select Security & Authentication, then choose SAML >Configure which will open up the configuration window.

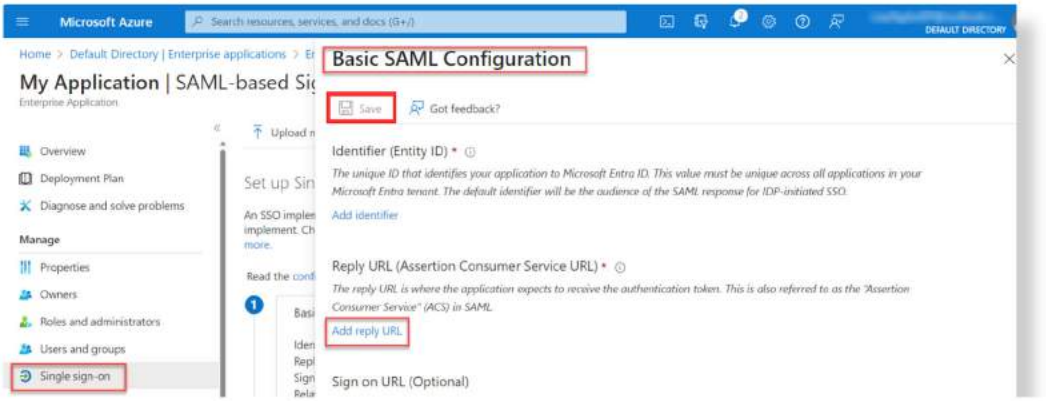


- The bottom section of the Configure SAML window contains URLs that are needed for your identity provider setup.
- You will need the 'Redirect URL' for the Microsoft Entra ID configuration that follows.
- From within the Configure SAML window, copy the **Redirect URL**

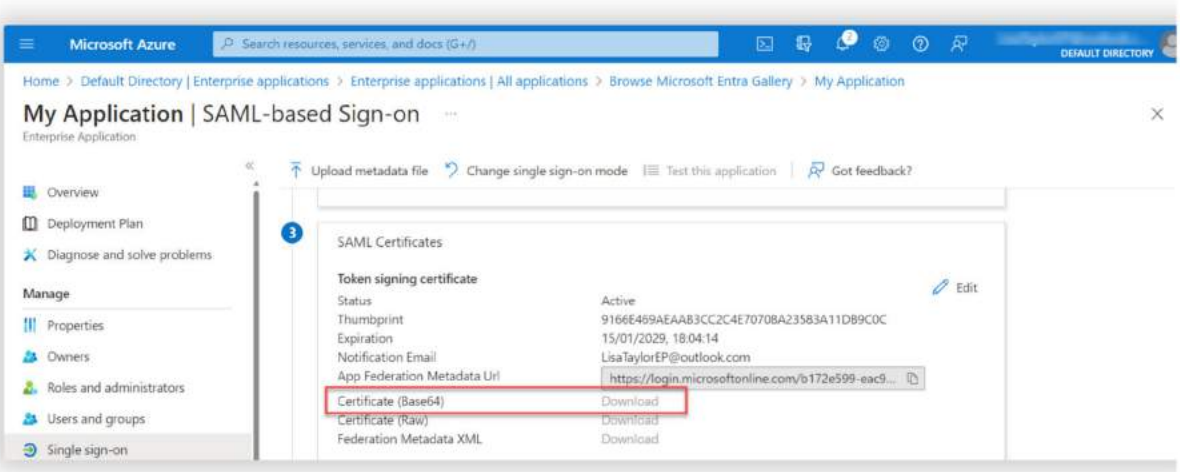


Admin Browser Configuration - SAML *(Continues)*

- Paste the Redirect URL into the Reply URL section in Azure (see screenshot below), then hit Save at the top. (you will need to click "Add Reply URL" to display the text field). If the settings won't stick, or the Save button does not become active, then 'Refresh' Azure.

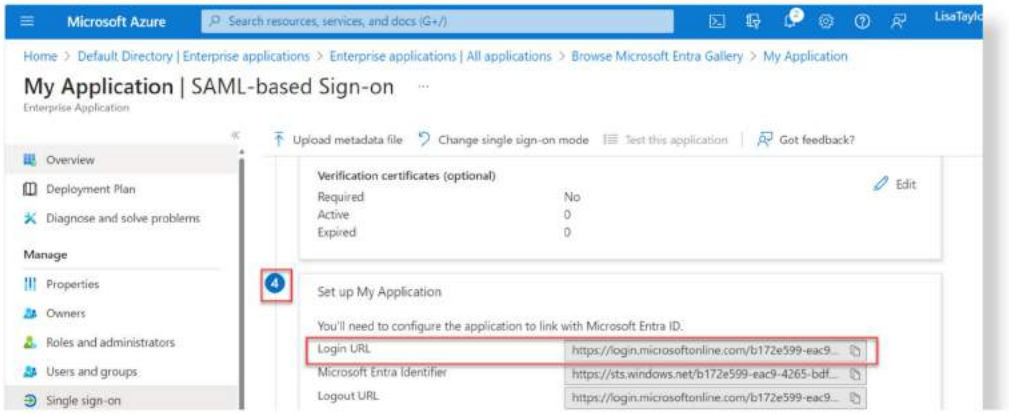


- Once the Identifier and Reply URL are saved in Microsoft Entra ID
  - Go to Section 3
  - Click 'Download' next to 'Certificate (Base64)'
  - Note where it gets saved on your machine

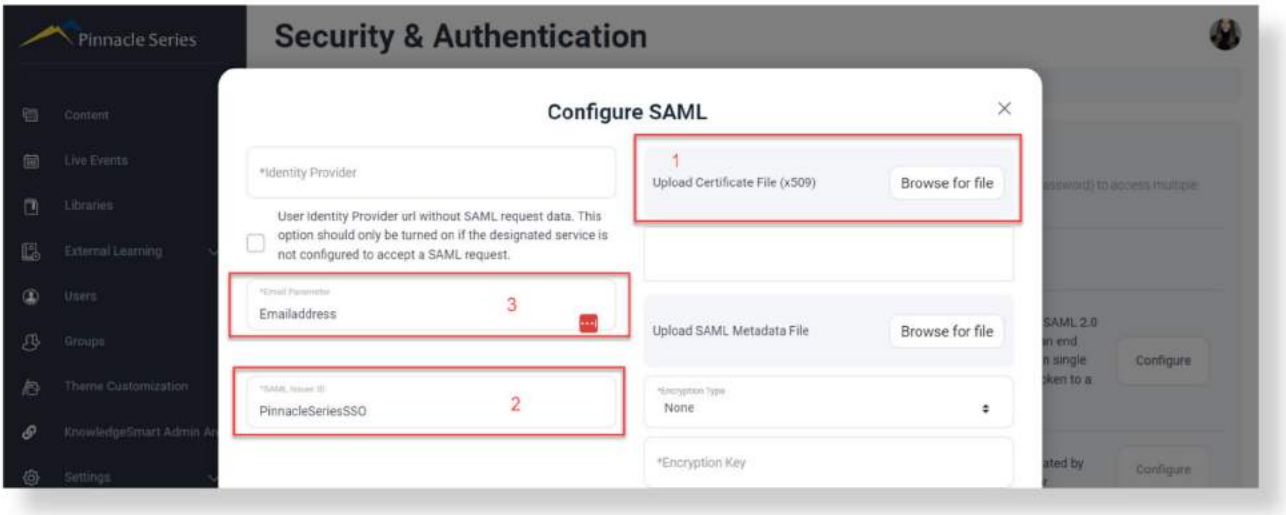


Admin Browser Configuration - SAML *(Continues)*

- Next, go down to Section 4 and copy out the Login URL



- Go back to the Configure SAML screen in the Administration Portal
  - Select 'Browse' by certificate. Upload certificate file to Administration Portal *(1 below)*
  - Enter your Azure SSO application name exactly how it shows in Azure (e.g. PinnacleSeriesSSO) for 'SAML Issuer ID' *(2 below)*
  - In Email Parameter Field, type "Emailaddress" *(3 below)*, which indicates that SSO will look at your user's email address for authentication



- Once finished, hit Save, and it will prompt you to test the SSO configuration using your email address. If the test passes, SSO is now successfully configured and running for your organization!

TACTICAL GUIDANCE

SAML Configuration - OKTA

Let's explore the nuances of Okta SAML configuration for enhanced identity and access management.

PINNACLE SERIES

by EAGLE POINT SOFTWARE

Okta SSO Configuration - SAML

To configure your SAML application in Okta you'll need the Pinnacle Series URLs found within the Admin Browser > Security and Authentication > SAML > Configure.

- Configure your SAML application in Okta for your Pinnacle Series tenant.
  - Copy and paste the Redirect URL from Pinnacle Series into the Single Sign-On URL field in the SAML Settings *(Ref 1)*

(1) Redirect URL
(2) From URL

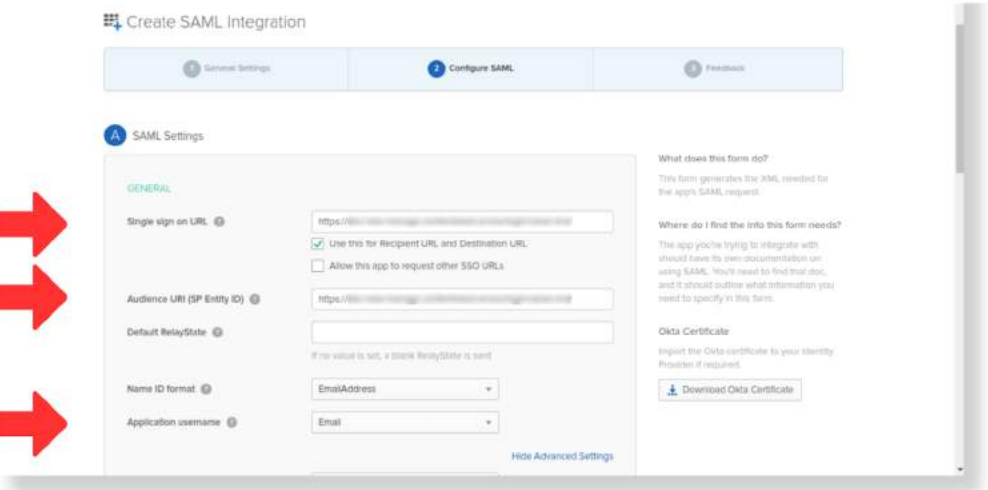
Redirect URL
The Redirect URL is required for OKTA to forward on the authorization packet to Pinnacle Series for user sign-in. This URL is unique to your organization and includes within the URL string the Pinnacle Series ApplicationID along with your organization's TenantID for the platform.

  - Copy and paste the From URL: from Pinnacle Series into the Audience URI (SP Entity ID) field in the SAML Settings. *(Ref 2)*

From URL
The From URL is the landing page for the Pinnacle Series Browser sign-in. For Eagle Point Customers this will be: (https://portal.pinnacleseries.com/#/login)

  - In your SAML Settings, in the Application username droplist select Email. *(Ref 3)*

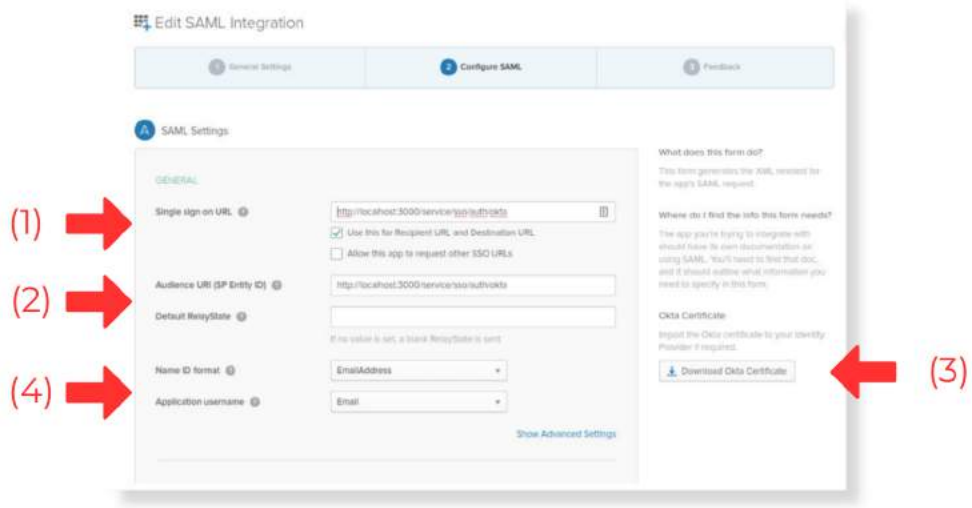
(1) Redirect URL
(2) From URL
(3) Select Email

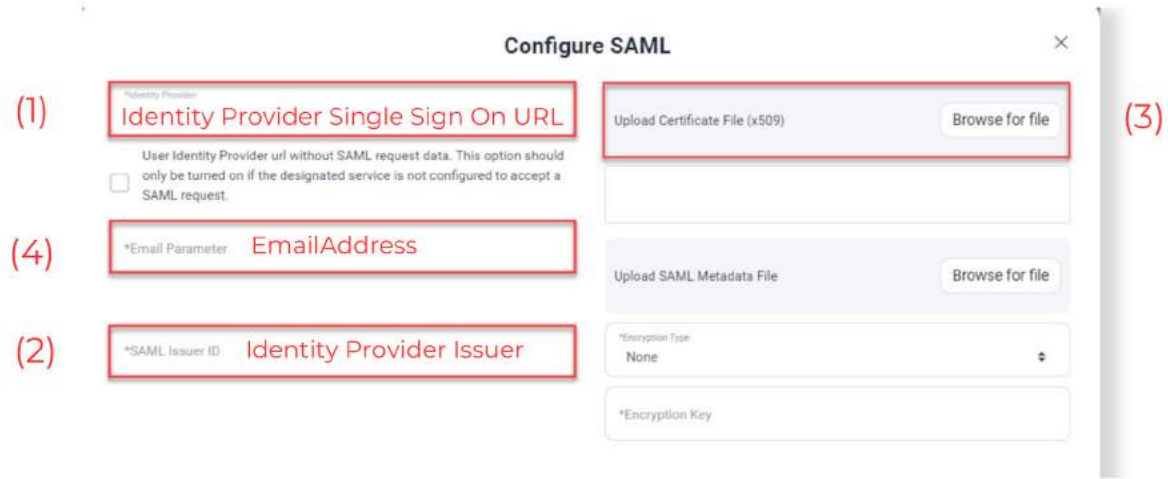


Okta SSO Configuration - SAML

Configure Pinnacle Series Admin Browser for your SAML application in Okta.

- Copy and paste the Identity Provider Single Sign-On URL from your SAML application into the Identity Provided URL field in Pinnacle Series *(Ref 1)*
- Copy and paste the Identity Provider Issuer URL from your SAML application into the SAML Issuer ID field in Pinnacle Series. *(Ref 2)*
- Copy and paste the X.509 Certificate: from your SAML application into the Certificate File (x509): field in Pinnacle Series. *(Ref 3)*
- In the Email Field: in Pinnacle Series enter the email attribute that will be returned from your SAML application. The default attribute (EmailAddress – case sensitive) can be used or a custom attribute that returns the user's email. *(Ref 4)*





Okta SSO Configuration - SAML *(Continues)*

Identity Provider URL:
The Identify Provider is required to redirect the user from the Pinnacle Series sign-in to the Identity Provider sign-in page.

Email field name returned from IP:
The user email attribute must be returned to Pinnacle Series to access the user account in Pinnacle Series. The default attribute defined in most identity provider protocols is NameID (case sensitive). If configured differently in your identity provider application use the appropriate attribute name to return the user's email.

Certificate File (x509):
The certificate file is required for authentication and authorization. This can be copied/pasted from the identity provider application or imported from a file.

SAML Issuer ID:
The Issuer ID can be copied and pasted from the identity provider application configuration.

Authenticate the SSO configuration.

- Click OK on the Configure SAML dialog box and Pinnacle Series will authenticate your configuration.
  - Use your SSO credentials to validate the authentication with your SAML application.
  - If your authentication fails check that all the parameters are matched up correctly and try again. If the authentication continues please log a support ticket referencing the error message you receive upon validation.

TACTICAL GUIDANCE

OpenID Configuration

OpenID allows individuals to use a single set of credentials, typically in the form of an OpenID identifier, to access multiple platforms, eliminating the need for separate usernames and passwords.

PINNACLE SERIES

by EAGLE POINT SOFTWARE

Open ID - How does it work?

OpenID is an open standard and decentralized authentication protocol. It allows users to be authenticated by co-operating sites (known as relying parties, or RP) using a third-party service, eliminating the need for webmasters to provide their own ad hoc login systems, and allowing users to log into multiple unrelated websites without having to have a separate identity and password for each. The primary goal of OpenID is to eliminate the need for separate usernames and passwords for each site, making the user experience more seamless.

Here's a basic overview of how OpenID works:

- **User Registration:**
  - Users register with an OpenID identity provider (IdP). This could be a dedicated OpenID provider or a service that supports OpenID.

- **Authentication Request:**
  - When a user tries to access a website or application that supports OpenID authentication, the site sends an authentication request to the user's chosen OpenID provider.

- **User Authentication:**
  - The OpenID provider authenticates the user using their credentials (username and password or other authentication methods).

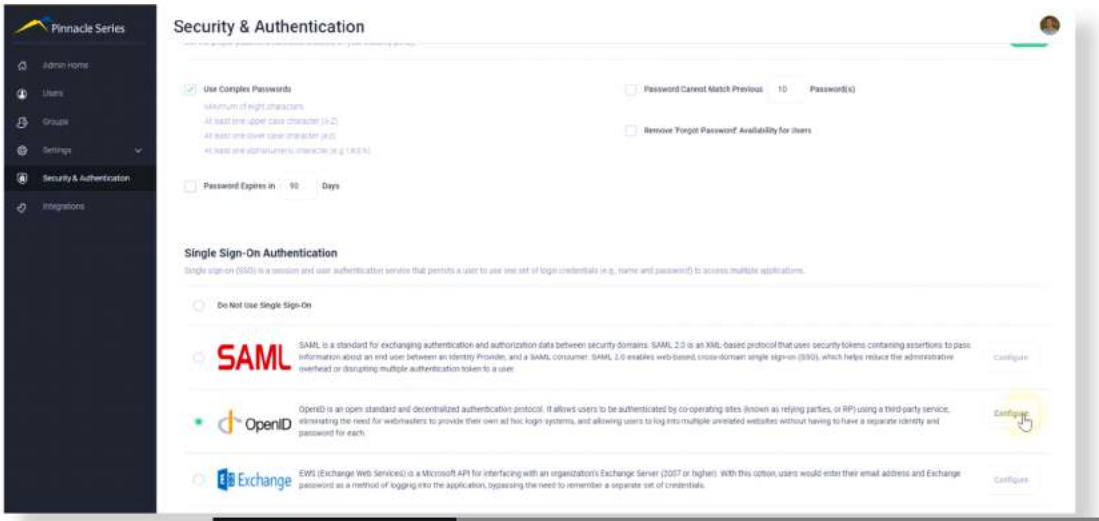
- **Authorization:**
  - After successful authentication, the user is asked to authorize the release of certain information to the relying party (the website or application requesting authentication).

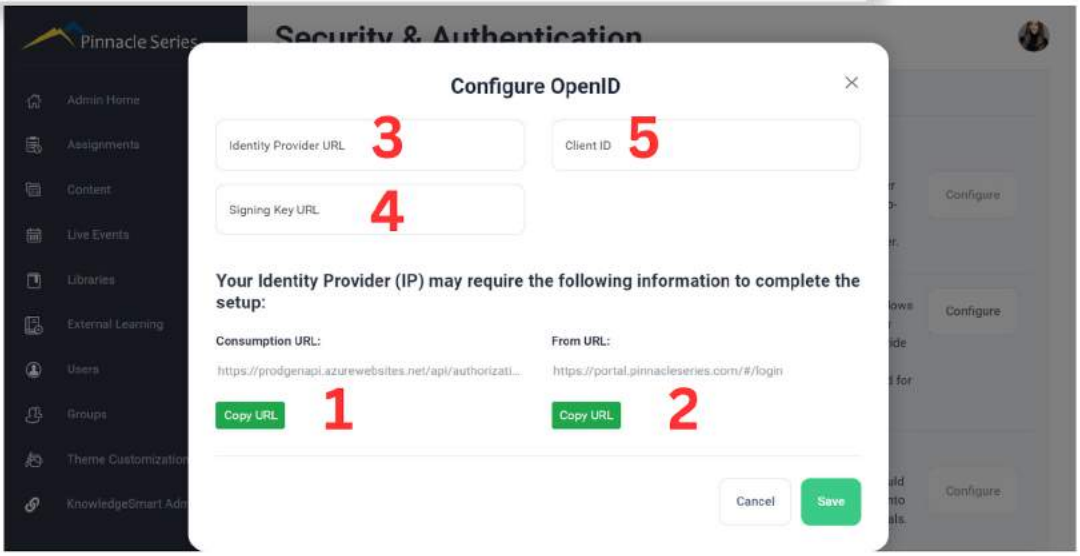
- **Assertion:**
  - The OpenID provider sends an assertion (a digitally signed statement) to the relying party, confirming the user's identity.

- **Access Granted:**
  - The relying party uses the assertion to log the user in, and the user gains access without the need to create a new account or remember a separate set of credentials.

Admin Browser Configuration - OpenID

- From the Security & Authentication Menu within the Pinnacle Series Admin Portal mark the indicator field next to OpenID, then select 'Configure'





- Copy and paste the Consumption URL *(ref 1)* and the From URL *(ref 2)* into your identity provider's application.
- In the upper section of the Configure OpenId window, you will need to enter information from your identity provider's application.
  - In the Identity Provider URL (*ref 3*), append the default application server path.
  - In the Signing Key URL(ref 4), append the default application server path to include the extended path.
- The Client ID field (ref 5) requires the application title from within your identity provider's application.
- Select Save to apply your configuration.

TACTICAL GUIDANCE

OpenID Configuration - OKTA

Let's explore the nuances of OKTA OpenID configuration for enhanced identity and access management.

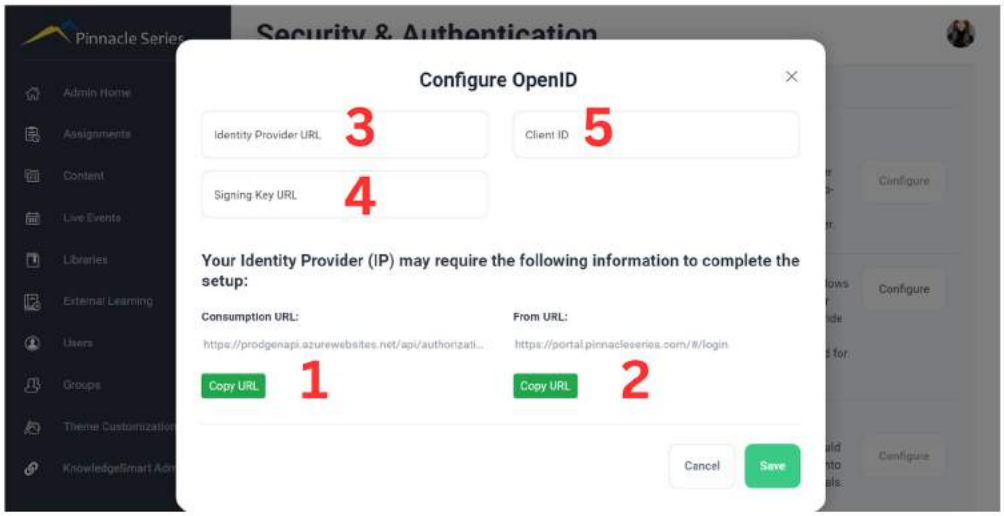
PINNACLE SERIES

by EAGLE POINT SOFTWARE

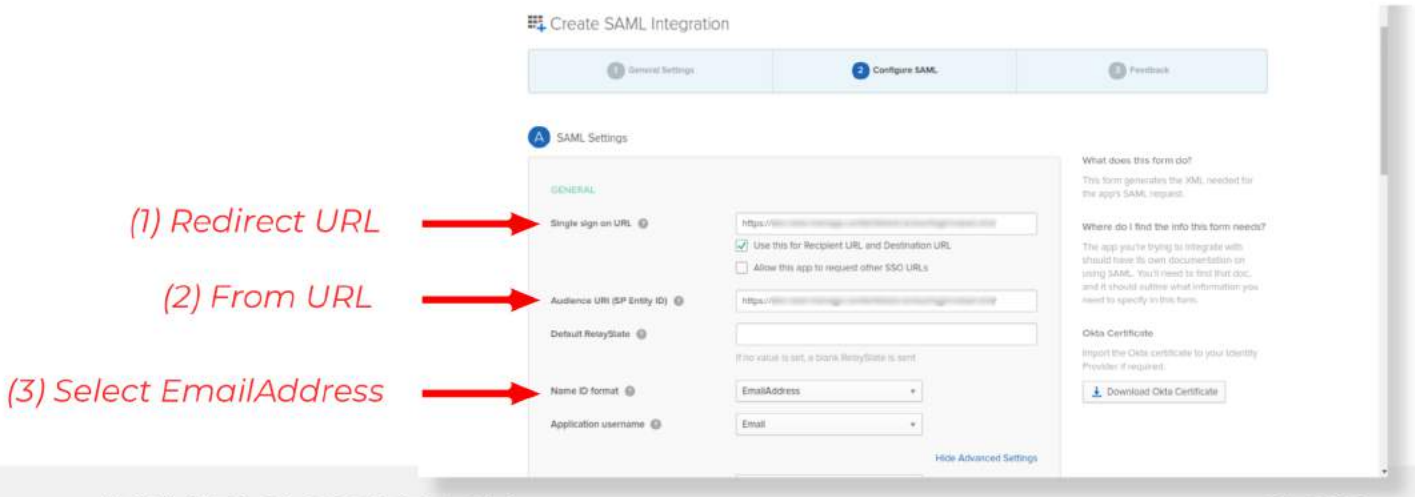
SSO Configuration - OpenID (Okta)

To configure an OpenID application in Okta you'll need the Pinnacle Series URLs found within the Admin Browser > Security and Authentication > SAML > Configure. These URLs are unique to your organization and to your Pinnacle Series service provider.

- Copy and paste the Consumption URL (*ref 1*) and the From URL (*ref 2*) into your identity provider's application.



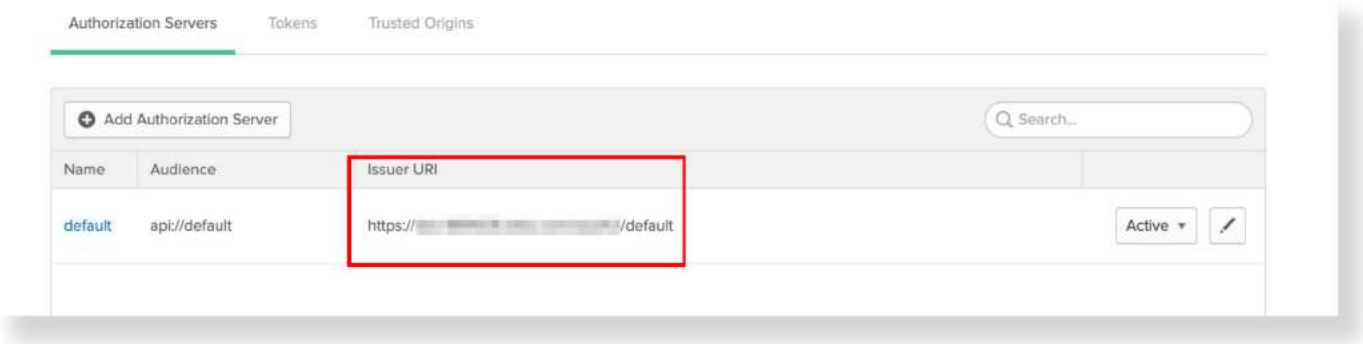
- In the upper section of the Configure OpenId window, you will need to enter information from your identity provider's application.
  - In the Identity Provider URL(*ref 3*), append the default application server path.
  - In the Signing Key URL (*ref 4*), append the default application server path to include the extended path.
- The Client ID (*ref 5*) field requires the application title from within your identity provider's application.
- Select Save to apply your configuration.



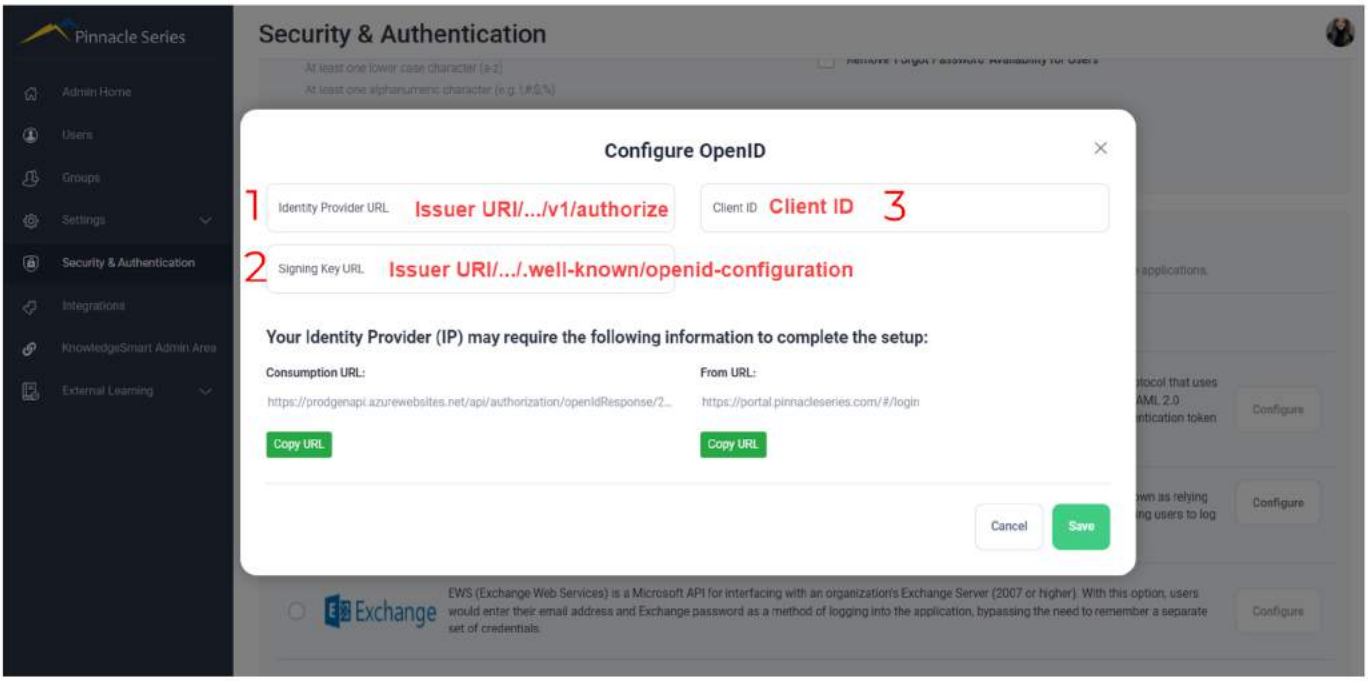
SSO Configuration - OpenID (Okta) *(Continues)*

Configure Pinnacle Series for your OpenID application in Okta.

- Copy and paste the Issuer URI: from the *API Application Servers* in your OpenID application into the Identity Provider URL: field in Pinnacle Series.
- To get the Issuer URI you must go to Okta and then, go to Security > API. You will find a list of Authorization Servers, copy the Issuer URI from the server you want to use.



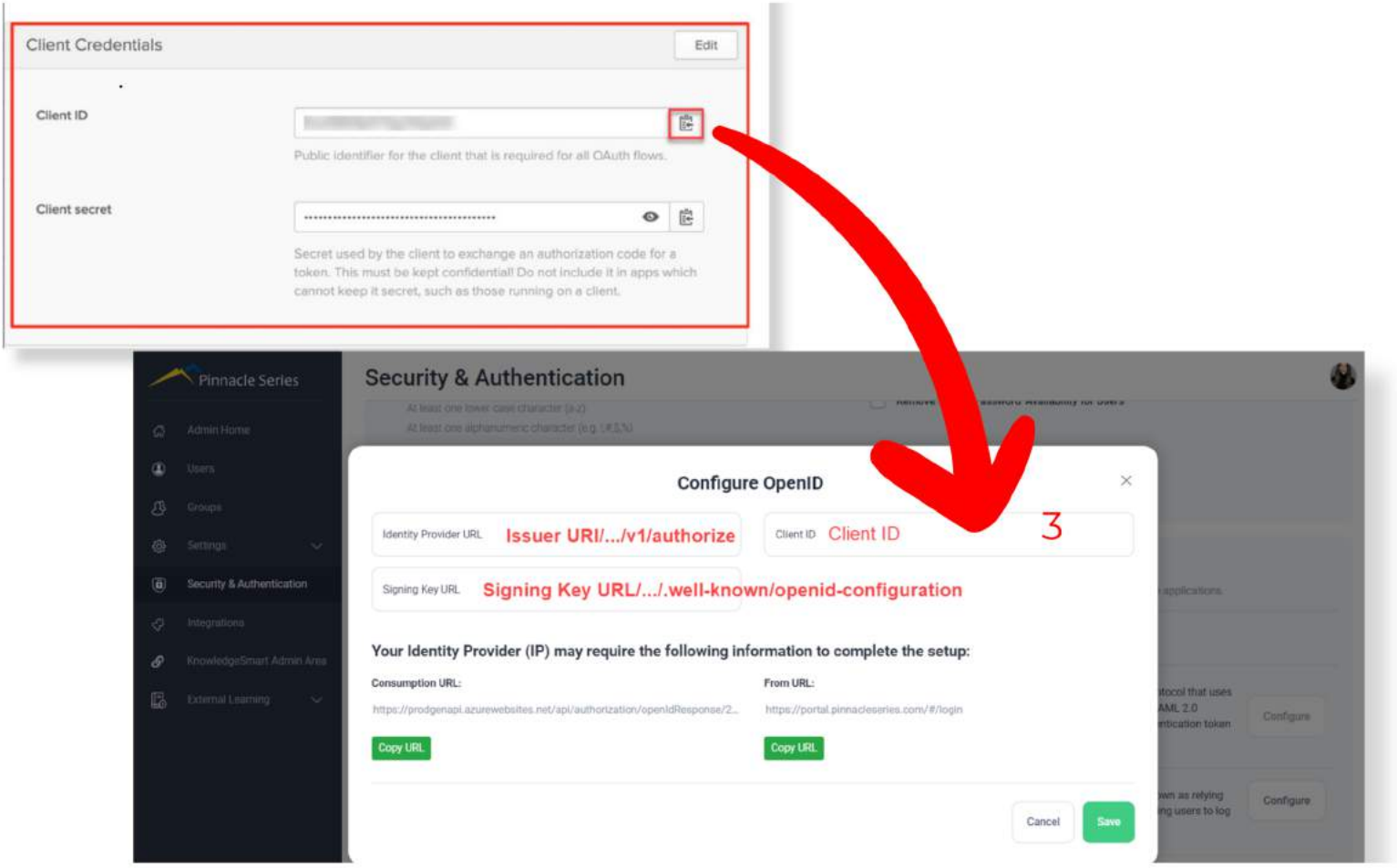
- Append the Issuer URI path in the Identity Provider URL: to include /v1/authorize. (ref 1)



- Append the Issuer URI path in the Signing Key URL: to include /.well-known/openid-configuration (ref 2)

SSO Configuration - OpenID (Okta) *(Continues)*

- Next you will need to copy the Client ID.
  - Navigate to Applications tab, you should see your app. Then click on the app, click General tab on the app, and scroll down to see Client Credentials section. You'll be able to see the Client ID and Client Secret there.
  - Paste the Client ID: field into the Pinnacle Series admin browser, OpenID configuration pop-up as per (*ref 3*) below.



- Get the Client ID and the Client Secret in Applications > Applications. Copy and paste the Client ID: from the *Client credentials*, in the *General Setting* of your OpenID application into the Client ID: field in Pinnacle Series**.**

SSO Configuration - OpenID (Okta) *(Continues)*

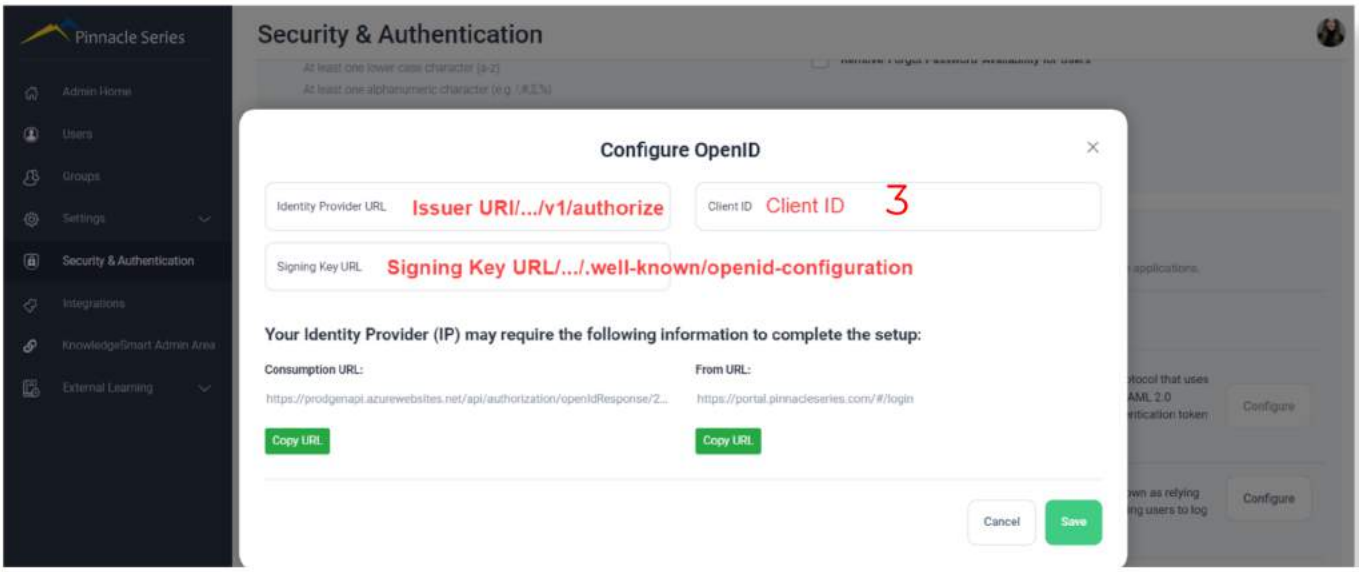
- **Identity Provider URL:**
  - The Identify Provider is required to redirect the user from the Pinnacle Series sign-in to the Identity Provider sign-in page.

- **Client ID:**
  - This field is populated with the Client ID from the Identity Provider application.

- **Signing Key URL**: (Required)
  - This URL points to the dynamic certificate used in the OpenID configuration.

Authenticate the SSO configuration.

- Click OK on the **Configure OpenID** dialog box and Pinnacle Series will authenticate your configuration.
- Use your SSO credentials to validate the authentication with your OpenID application. If your authentication fails, check that all the parameters are matched up correctly and try again.



TACTICAL GUIDANCE

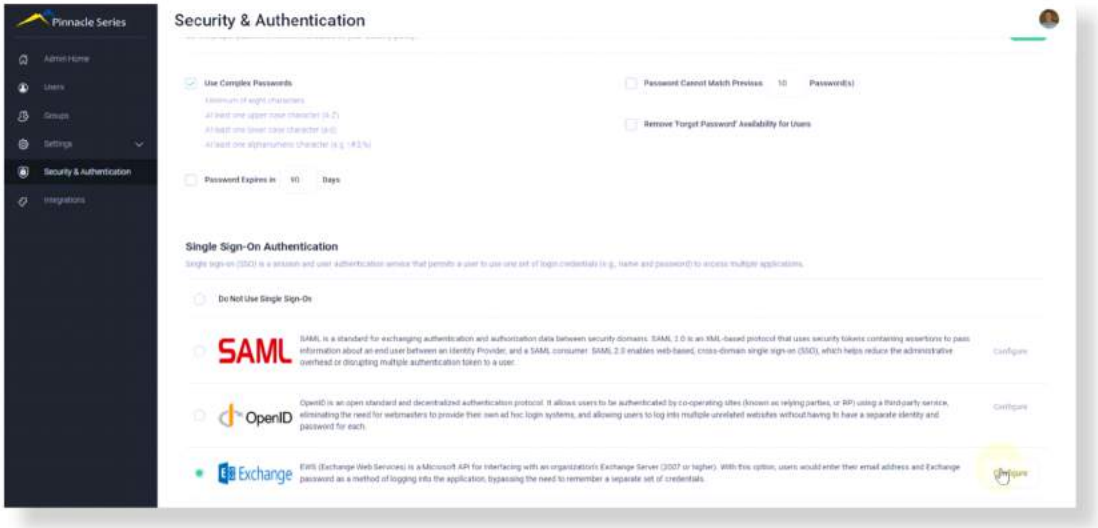
Exchange Web Services Configuration

PINNACLE SERIES

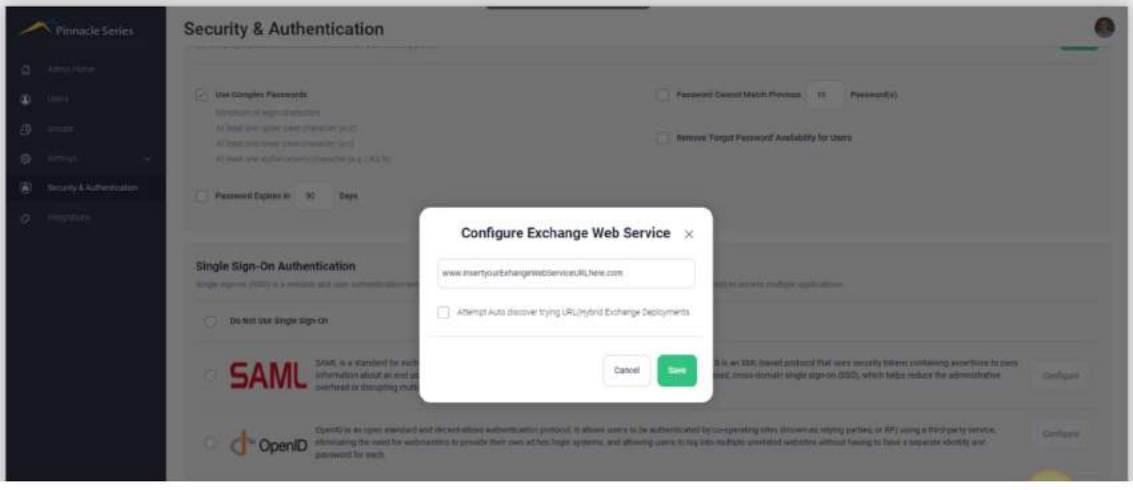
by EAGLE POINT SOFTWARE

Admin Browser Configuration - Exchange Web Services

- From within the Security & Authentication menu within the Pinnacle Series Admin Browser mark the indicator next to Exchange Web Services, then select 'Configure'.



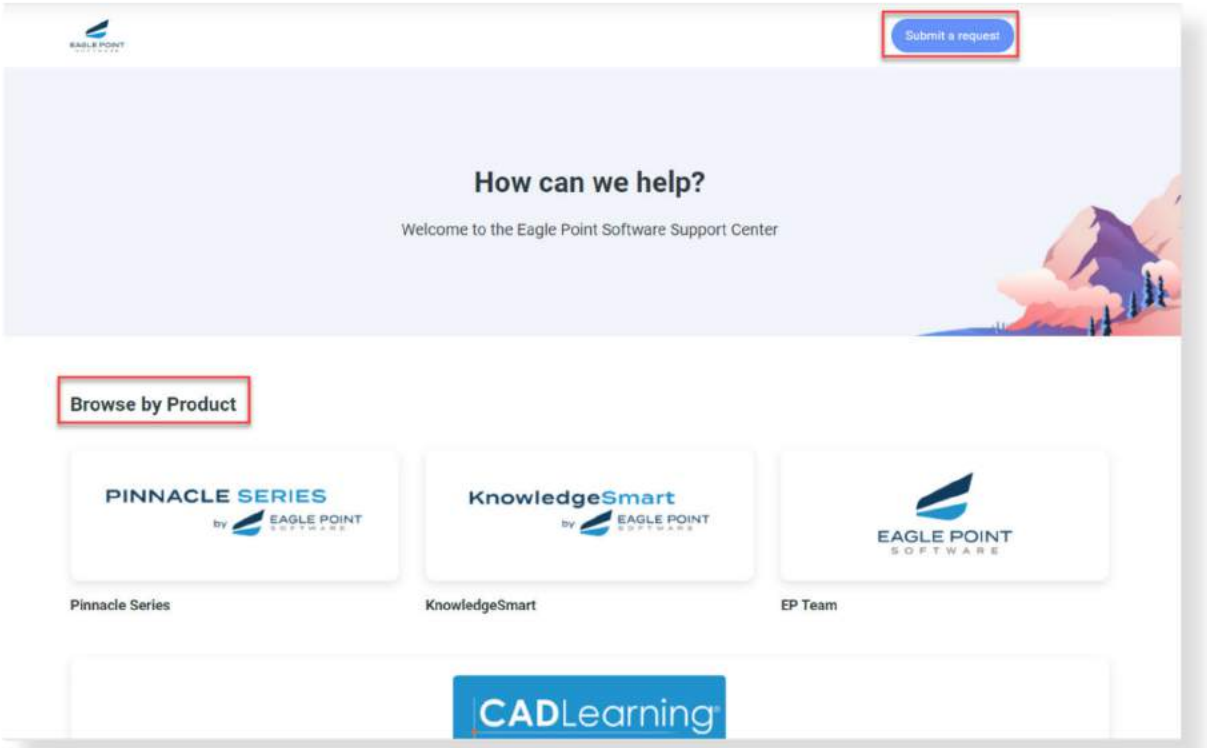
- EWS or Exchange Web Services can be used if you have an on-premise Microsoft Exchange Server or Office 365.
  - This option does not support multifactor authentication, and MFA must be disabled on the exchange service to work with Pinnacle Series SSO.
- Specify your Exchange URL on-premise or Office 365 server and paste it within the Exchange URL field in Pinnacle Series.
- Select Save to apply your configuration.



Need Support?

- Raise a support ticket
- Browse Knowledgebase Articles by Product

Author: Eagle Point Software Support Team
Publish date: 23. 01. 2024



EAGLE POINT SOFTWARE