appviewx

Platform Guides

Version: 2023.1.0 FP2

Copyright AppViewX, Inc.

Trademarks

External Reference Links

This product includes software developed by the CentOS Project (www.centos.org).

This product includes software developed by Red Hat, Inc. (www.redhat.com).

This product includes software developed by VMware, Inc. (www.vmware.com).

Contact Information

AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: info@appviewx.com

Web: www.appviewx.com

Contents

Preface

Revision History

Revision	Description	Date
1.2	Updated version of document for Release 2023.1.0 FP2	February 2024
1.1	Updated version of document for Release 2023.1.0 FP1	November 2023
1.0	Initial draft of document for release 2023.1.0 Platform.	September 2023

About the Documentation

This section includes the following guides that will give you an overview of Platform and Reporting module:

- Platform User Guide
- Platform API Guide
- Reporting User Guide

Audience

This guide is intended for CISO, PKI Security, and Application Teams.

Text Conventions

The following text conventions are used in this document:

Convention	Description
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in the text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`codeblock`	Indicates commands with a paragraph, URLs, codes in examples, text that appears on the screen, or text that you enter.
	Indicates a feature available only in the On-premise deployments of AppViewX.

Convention	Description
	Indicates a feature available only in the SaaS deployments of AppViewX.

Chapter 1: Platform User Guide

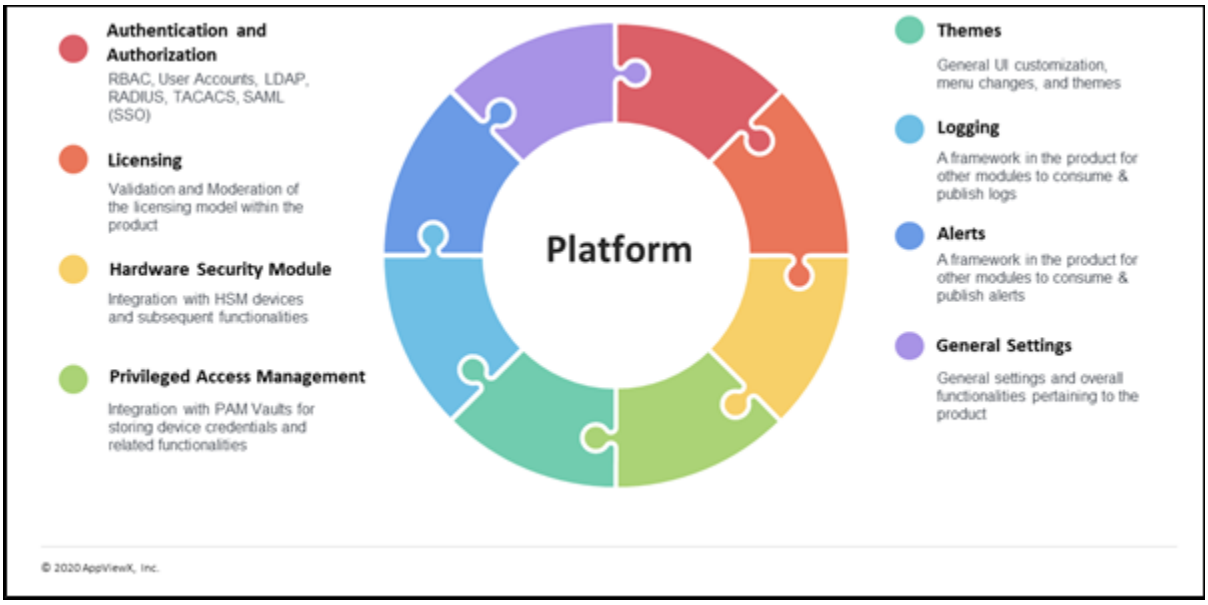
The AppViewX Platform is a module that lets you enable general configuration settings such as authentication, authorization, and integration of external services like log forwarding, HSM integration, SMTP configuration, and so on. These general configuration settings are applicable to all AppViewX subsystems such as ADC, CERT+, Security+, Visual Workflow, and so on.

Overview

The AppViewX Platform is a module that lets you enable general configuration settings such as authentication, authorization, and integration of external services like log forwarding, HSM integration, SMTP configuration, and so on. These general configuration settings are applicable to all AppViewX subsystems such as ADC, CERT+, Security+, Visual Workflow, and so on.

The Platform User Guide documents these general configuration settings.

Platform components common to all subsystems are shown in the image below:



Account Ownership

In AppViewX, the account used during signup becomes the designated Account Owner for that specific account. The ownership can be transferred to another user with Admin privileges at any time in the future. The Account Owner is possesses the following permissions, along with any other assigned permissions:

These permissions include:

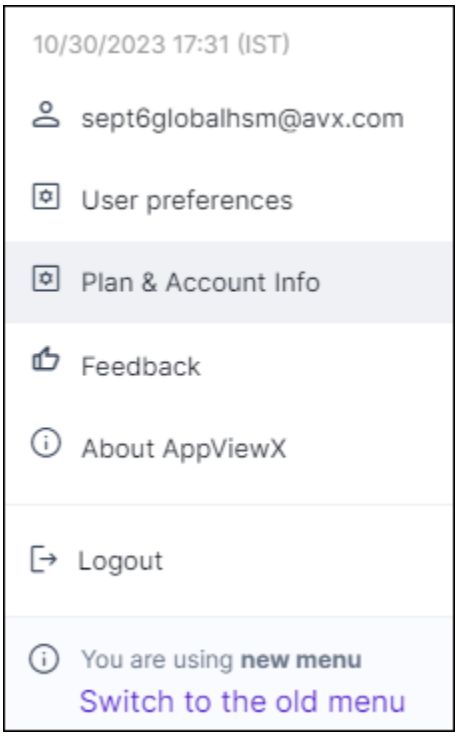
- MFA: Enabling/Disabling Multi-Factor Authentication for all users
- Enabling master key encryption
- Access to analytics and tracking
- Plan and account information.
- Transfer of Account Ownership

Transfer of Account Ownership

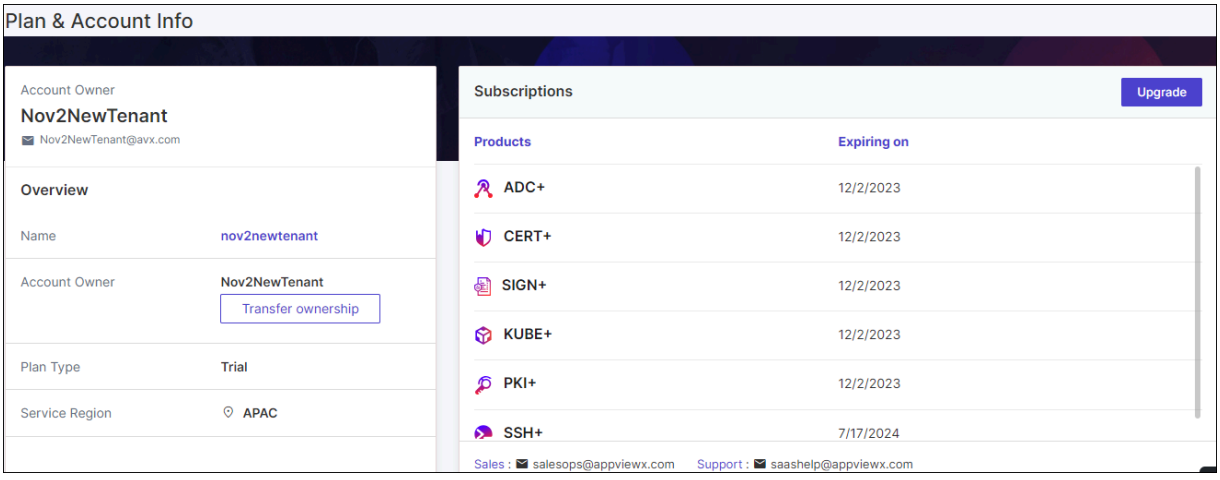
The ownership can be transferred to another user with admin privileges at any point in the future, but only by the current account owner. Upon transfer, all active sessions of the current account owner will be automatically logged out, and the new account owner will get account ownership permissions upon their next login. Both the existing and new account owners will receive email notifications regarding the ownership change. This action is exclusive to the account owner.

To initiate the transfer of ownership to another user, follow the steps below:

1. Login to AppViewX.
2. From the top right corner of your screen, click **(Profile)** icon.
   The drop down displays a list of menus.

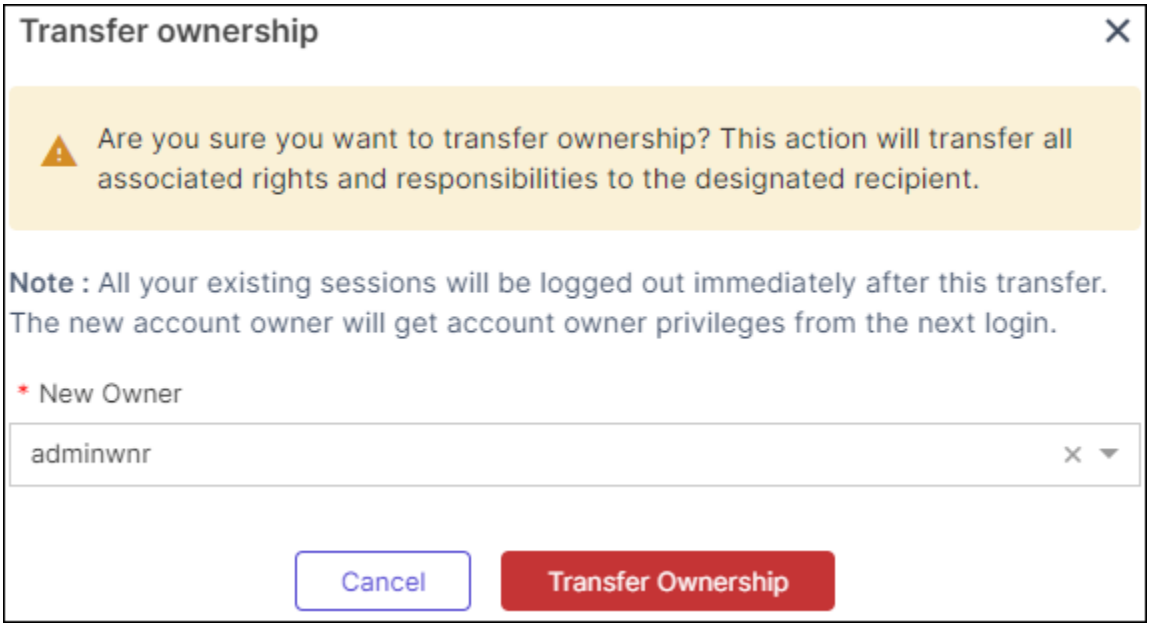


3. Click **Plan & Account Info**.
   The **Plan & Account Info** page is displayed, featuring account details and a list of subscribed products.



4. In the **Account Owner** section, click **Transfer ownership**.

The **Transfer ownership** dialog box appears.



CAUTION: Are you sure you want to transfer ownership? This action will transfer all associated rights and responsibilities to the designated recipient.

Note: All your existing sessions will be logged out immediately after this transfer. The new account owner will get account owner privileges from the next login.

5. Select the **New Owner** from the dropdown list, then proceed to click **Transfer Ownership** to confirm the change of ownership.
   AppViewX assigns the owner role to the selected new owner.

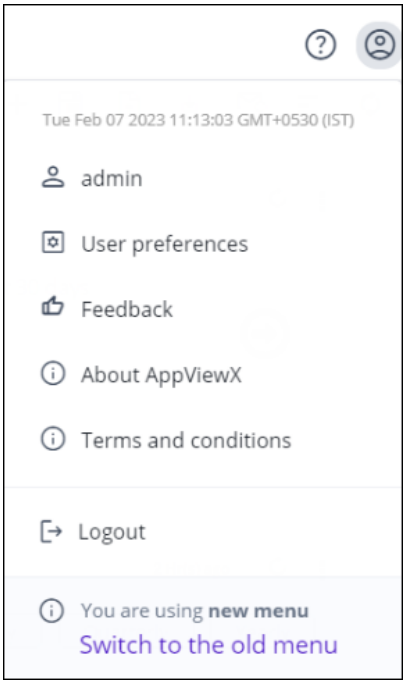
Note: The account owner will be logged out of all sessions of the previous account owner immediately, ensuring the prompt application of permission changes.

Note: AppViewX will send email notifications to both the previous and new account owners to confirm the successful transfer of account ownership.

Switching between Menus

To check which menu you are using:

1. From the top right corner of your screen, click **(Profile)** icon.
   The dropdown displays which menu is in use.



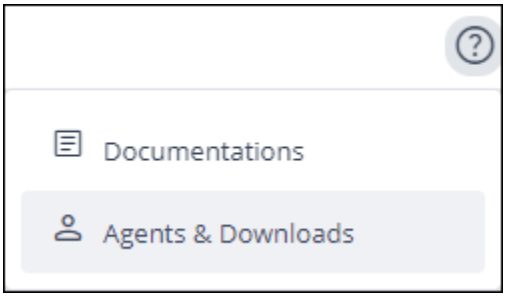
2. Click **Switch to the old menu**.

• Platform Agents & Download Service

Platform Agents & Download Service

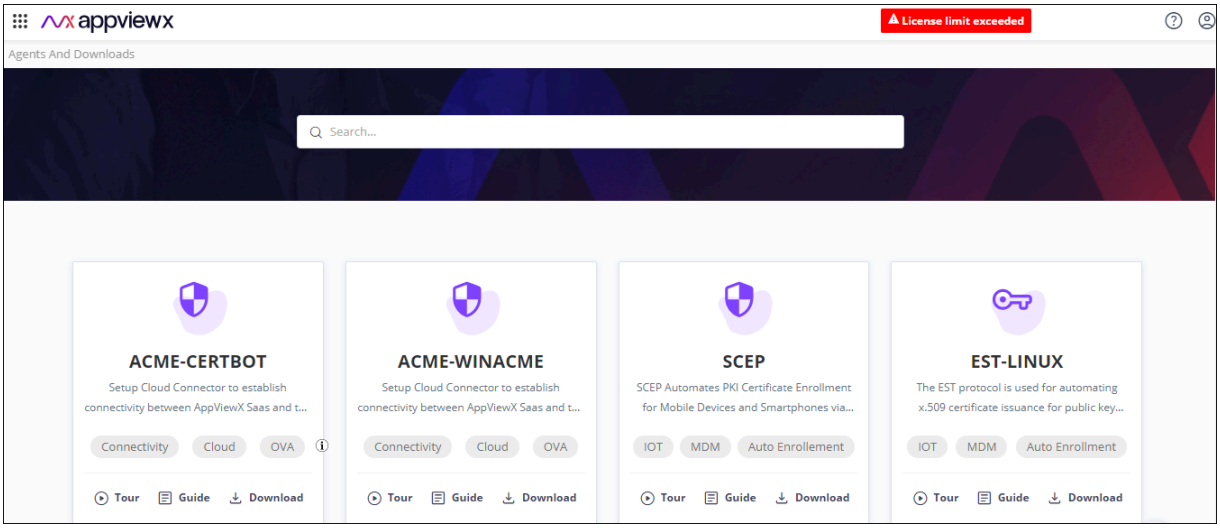
1. From the top right corner of your screen, click **(Profile)** icon.

   The dropdown displays **Documentation** and **Agents & Downloads**.



2. Click **Documentation** to view the helpcenter of AppViewX.
3. Click **Agents & Downloads** for the service to download agents.

The **Agents & Downloads** page is displayed.



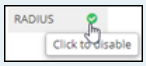
4. Click **(Download)** icon on the corresponding agents to download.

Configuring Authentication Settings

In addition to configuring authentication settings, AppViewX also lets you enable birthright provisioning for new users, configure the order in which user credentials are authenticated, enable/disable an authentication check, and other user and node settings.

To configure the authentication settings:

1. On the **Settings :: Authentication** page, under the **Authentication settings** tab, to enable **Birthright provisioning** for new users who log into the system with a predefined set of permissions (associated with the user group), turn on the **Enable Birthright** toggle.
   To do this, the admin should select the user group (Assigned with the defined permissions), which will act as a default user group for all the users logging in to AppViewX. For more details, refer to the content on creating a role and associating it with a user group.
2. To define the order in which the authentication settings will be checked, in the **Order** section, drag and drop the authentication labels to the required corresponding levels.
   If the level 1 check is set to Local and the level 2 check is set to LDAP, user credentials will be authenticated locally first and then on the LDAP server.

Note: You can also disable, and then enable a level of authentication. To do this, click the green tick 

next to the server name.

3. In the **User settings** section, enter the required field information.

Field descriptions for User settings

Field	Description
Create User an unique E-mail ID	To ensure that every AppViewX user has a unique email ID, turn on this toggle.
Create User on Authorization Failure	To create a user even if authorization fails (but the user is authenticated successfully), turn on this toggle.
Session Timeout	AppViewX lets you set a session timeout limit between 2 and 480 minutes. To set a web session timeout limit, enter the value in minutes.

4. If the AppViewX node password is updated, in the **Node Settings** section, enter the updated Node Password.

Note: The value entered in the Node Password field should be the same as the node password. To apply the changes, restart the avx-config-server pod in every datacenter.

5. Click **Save**.

- LDAP Authentication
- TACAS Authentication
- RADIUS Configuration
- Single Sign On Configuration
- IP Restriction Configuration
- Authentication Settings Configuration
- OAuth Settings
- MFA Settings Configuration
- SCIM Configuration

LDAP Authentication

LDAP Authentication is a method used by systems to authenticate user identities against a centralized LDAP (Lightweight Directory Access Protocol) directory service. It validates user credentials, such as username and password, stored in the LDAP server to grant access to various applications and services within an organization's network.

Accessing LDAP Authentication Settings

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **ACCESS MANAGEMENT**, select **LDAP**. The **Settings :: Authentication** page is displayed with the **LDAP** tab open by default.	1. From the main navigation menu, click **Settings**. 2. On the **Settings** page, from the left menu, select **General** > **Authentication**. The **Settings :: Authentication** page is displayed with the **LDAP** tab open by default.
Note: For more information on how to switch between menus, click here.	

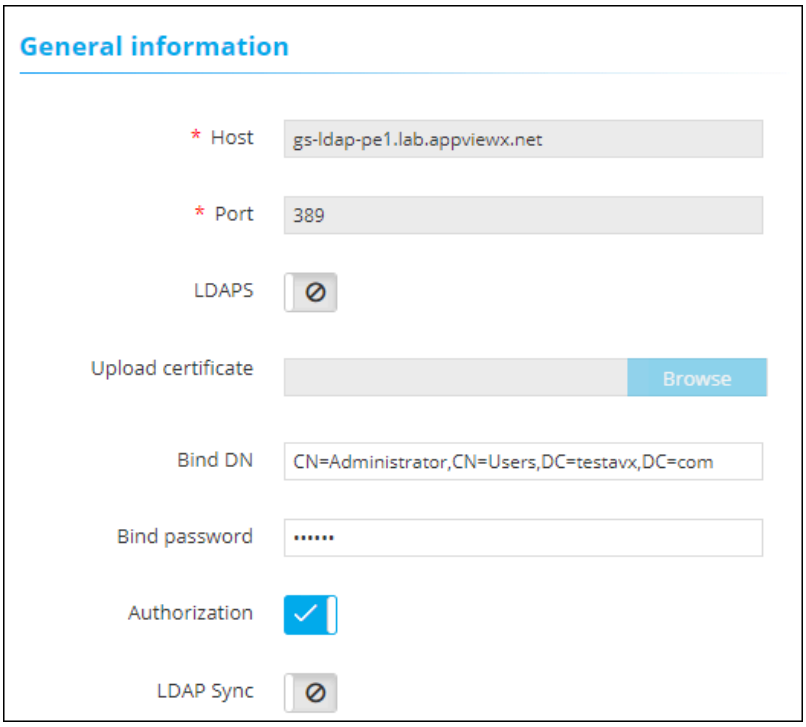
Configuring the LDAP Authentication

The Lightweight Directory Access Protocol (LDAP) is an authentication protocol to validate a user's credentials entered in an application, against the credentials stored in the Active Directory database.

AppViewX integrates with the Active Directory and Open LDAP for authentication of external users. It also enables configuring multiple servers in the event that users belong to multiple domains.

To configure the LDAP authentication:

1. On the **Settings :: Authentication** page, under the **LDAP** tab, in the **General Information** section, enter the following details (sample values are shown in the image):



Field descriptions for General Information

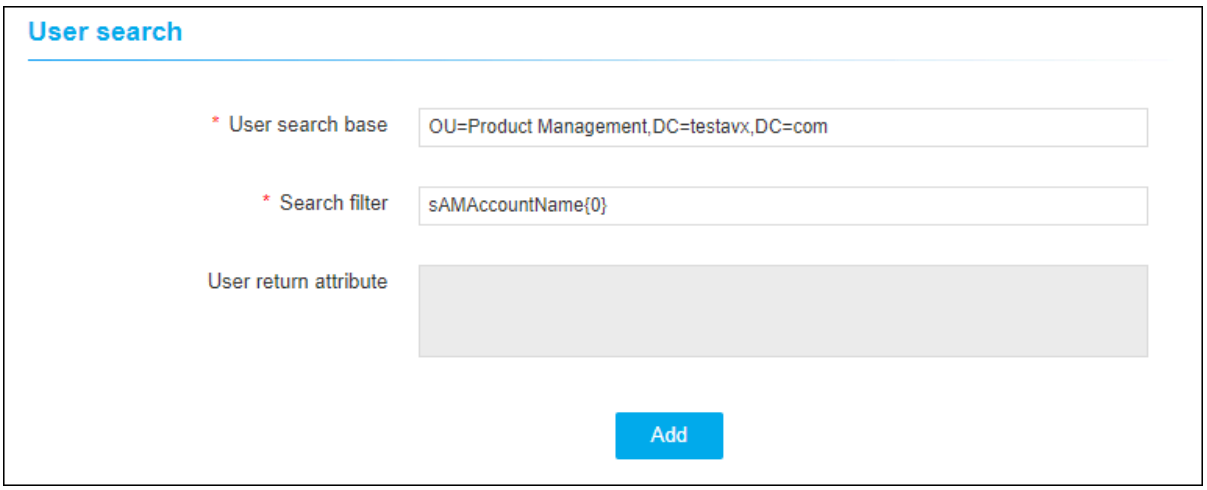
Field	Description
***Host**	Host name (domain name) of the LDAP server.
***Port**	Port number of the LDAP server. **Note:** This value is entered based on the port number used in your deployment. By default, port number **389** is used for a LDAP configuration and port number 636 is used for a LDAPS configuration.
LDAPS	The LDAPS protocol is used for secure communication between AppViewX and Active Directory/Open LDAP. To enable use of the LDAPS protocol, enable this toggle.
Upload Certificate	**Note:** This field is enabled only when the **LDAPS** is enabled.

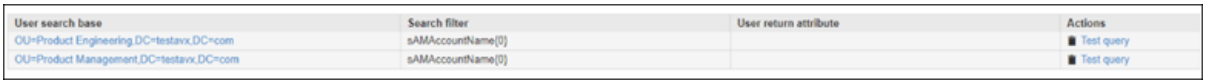
Field	Description
	To upload a LDAP server certificate: a. Click **Browse Certificate**. b. Navigate to the location of the **.pem** certificate file. **Note:** If the LDAP servers are load balanced with VIP, upload the root certificate of the LDAP server instead of the server certificate. c. Select the certificate to be uploaded and click **Open**. The selected certificate is uploaded. **Note:** Only a single certificate can be uploaded for each server.
Bind DN	Username of the base authentication endpoint that will be used to connect to LDAP.
Bind password	Password of the base authentication endpoint that will be used to connect to LDAP.
Authentication	In addition to authentication, AppViewX also lets you perform user authorization against the LDAP server. To enable authorization along with authentication, turn on the toggle. **Note:** If **Authorization** is not enabled, AppViewX will only carry out LDAP authentication for the given user.
LDAP Sync	To enable the use of the SSH module in AppViewX for SSH key discovery use case, turn on the toggle.
Note: The asterisk (*) symbol indicates mandatory fields.	

2. After entering the above connection details, to test if the host is reachable and the port is valid for establishing a LDAP/LDAPS connection, click **Test Connection**.

Note: You can test the connection of LDAPS only when you save all of the configuration details. Bind DN and Bind password details cannot be validated through a test connection.

3. The **User Search** section collects information to validate a user's presence in the Active Directory. In the **User Search** section, enter the following details (sample values are shown in the image):





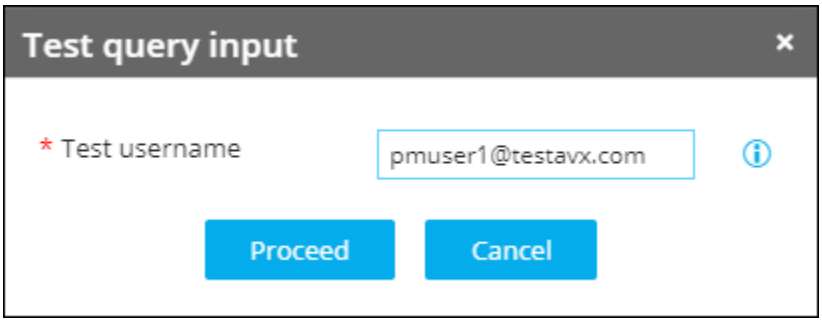
Note: You can now add multiple OUs in User search so that it checks multiple OUs to validate a user's presence in the Active Directory.

Field descriptions for User Search

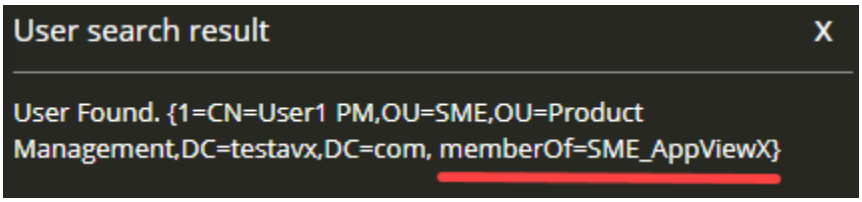
Field	Description
***User search base**	Base directory where the user is present.
***Search filter**	Criteria for searching for the user from the search base.
User return attribute	User information to be retrieved from the search base. **Note:** This field is enabled only when the **Authorization** toggle (in the **General Information** section) is turned on. **Note:** You can specify only **User return attribute**.

Field	Description
	Note: The asterisk (*) symbol indicates mandatory fields.

4. For the given configuration, to check the user's presence, click **Test query**.
5. In the **Test query input** dialog box, enter the **Test username**.



The output is displayed as shown in the image below:



6. To test which user group the user belongs to, in the **Group search** section, enter the following details:

Note: This section is enabled only when the **Authorization** toggle (in the **General Information** section) is turned on.

Field descriptions for Group search

Field	Description
***Group search base**	Base directory where the user group is present.
***Search filter**	Criteria to search the user group from the search base.
Group return attribute	User group information to be retrieved from the search base.
	Note: The asterisk (*) symbol indicates mandatory fields.

> **Note:** You are allowed to check the query response for User search and Group search only when the connection is valid.

> **Note:** Group search can be performed only if the customer's LDAP is of type Open LDAP. Microsoft Active Directory does not need group search configuration. For Open LDAP, group search needs to be configured mandatorily. The User return attribute in the User search section does not return the group membership details.

7. After entering the above details, to test if the group search query thus configured works, click **Test Query**. For Open LDAP, when the user runs the test query for group search, the user search base details are passed to the group search test query and the group membership details for that user are returned.
8. To save the LDAP settings, click **Save**.
   The LDAP authentication settings thus configured are saved and displayed in the table shown at the end of this screen:

> **Note:** In the case of multiple LDAP servers, to define/update the order in which the servers will be authenticated, drag and drop the entries in this table.

9. To reconfigure the settings, click **Reset**.

TACAS Authentication

TACACS (Terminal Access Controller Access-Control System) is a remote authentication protocol commonly used to manage access to network devices. It ensures secure user authentication, authorization, and accounting (AAA) services in network security by validating users attempting to gain access to a network.

- Accessing TACAS Authentication Settings
- Configuring the TACACS Authentication

Accessing TACAS Authentication Settings

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **ACCESS MANAGEMENT**, select **TACAS**. The **Settings :: Authentication** page is displayed with the **TACAS** tab open by default.	1. From the main navigation menu, click **Settings**. 2. On the **Settings** page, from the left menu, select **General** > **Authentication**. The **Settings :: Authentication** page is displayed with the **LDAP** tab open by default. 3. Click the **TACAS** tab.

Note: For more information on how to switch between menus, click here.

Configuring the TACACS Authentication

The Terminal Access Controller Access Control System (TACACS) authentication is used to validate users requesting remote access. AppViewX integrates with TACACS for authentication of external users.

To configure the TACACS authentication:

1. On the **Settings :: Authentication** page, under the **TACAS** tab, enter the following details:

Field descriptions for TACAS Test connection

Field	Description
***Server name**	Name of the TACACS server.
***IP address**	IP address of the TACACS server.
***Port**	Port number of the TACACS server.

Note: The asterisk (*) symbol indicates mandatory fields.

2. To test the connectivity between AppViewX and the IP address mentioned above, click **Test connection**.

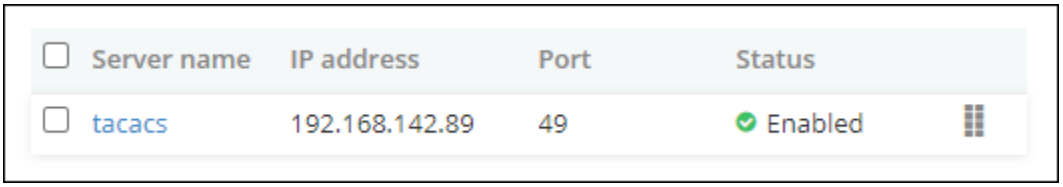
3. Enter the following details (sample values are shown in the image):

Field descriptions for TACAS

Field	Description
***Secret key**	A unique key for authentication between the AppViewX server and the TACACS server.
***Service**	Name of the service used by the user requested to be authorized. Specifying the service name is mandatory because it enables the TACACS+ server to behave according to the type of each authorization request. Commonly, the Point-to-Point Protocol (PPP) is used for authorization checks.
***Protocol**	The protocol associated with the value specified in Service Name, which is a subset of the associated service being used for client authorization or system accounting Commonly, the Internet Protocol (IP) is used as the modifier with PPP to indicate the protocol layer for authorization check.
***Authorization Attribute Name**	Attribute that will be returned from the TACACS server to authenticate and authorize the connection between the AppViewX server and the TACACS server.

Note: The asterisk (*) symbol indicates mandatory fields.

4. To save the TACACS authentication settings, click **Add**.
   The TACACS authentication settings thus configured are saved and displayed in the table shown in the left half of the screen:



> **Note:** In the case of multiple TACACS servers, to define/update the order in which the servers will be authenticated, drag and drop the entries in this table.

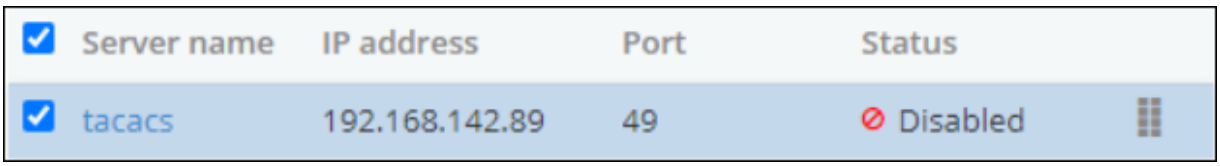
5. To reconfigure the settings, click **Reset**.

• Enabling a TACACS Server for Authentication
• Disabling a TACACS Server for Authentication
• Deleting a TACACS Server

Enabling a TACACS Server for Authentication

To enable a TACAS server for authentication:

1. On the **Settings :: Authentication** page, under the TACAS tab, from the table displayed in the left half of the page, for the server you want to enable, select the check box corresponding to the server name.

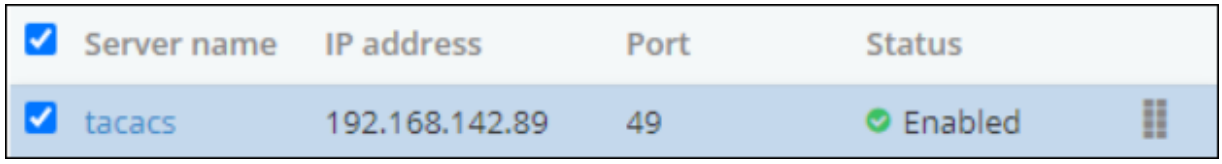


2. From the top-right corner of the page, click **(Enable)** icon.
3. In the **Confirmation message** dialog box, click **Proceed**.

Disabling a TACACS Server for Authentication

To disable a TACAS server for authentication:

1. On the **Settings :: Authentication** page, under the TACAS tab, from the table displayed in the left half of the page, for the server you want to disable, select the check box corresponding to the server name.

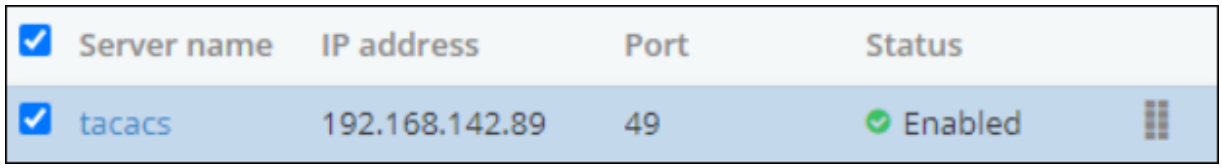


2. From the top-right corner of the page, click **(Disable)** icon.
3. In the **Confirmation message** dialog box, click **Proceed**.

Deleting a TACACS Server

To delete a TACAS server :

1. On the **Settings :: Authentication** page, under the TACAS tab, from the table displayed in the left half of the page, for the server you want to delete, select the check box corresponding to the server name.



2. From the top-right corner of the page, click **(Delete)** icon.
3. In the **Confirmation message** dialog box, click **Proceed**.

RADIUS Configuration

RADIUS (Remote Authentication Dial-In User Service) Configuration involves setting up a networking protocol that provides centralized authentication, authorization, and accounting management for users connecting to a network. It establishes a secure method for users to access resources via a client-server protocol.

- Accessing the RADIUS Configuration Settings
- Configuring the RADIUS Configuration

Accessing the RADIUS Configuration Settings

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **ACCESS MANAGEMENT**, select **RADIUS**. The **Settings :: Authentication** page is displayed with the **RADIUS** tab open by default.	1. From the main navigation menu, click **Settings**. 2. On the **Settings** page, from the left menu, select **General** > **Authentication**. The **Settings :: Authentication** page is displayed with the **LDAP** tab open by default. 3. Click the **RADIUS** tab.
Note: For more information on how to switch between menus, click here.	

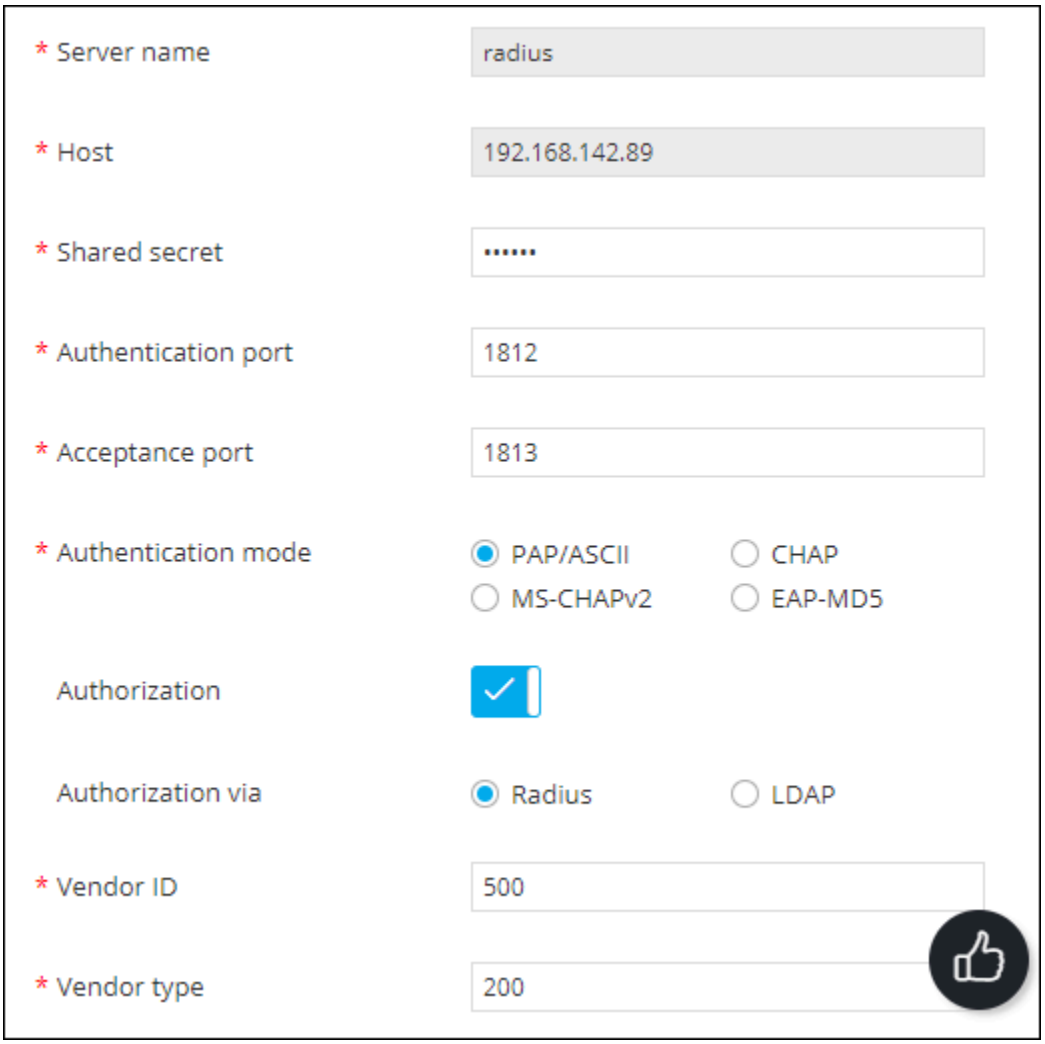
Configuring the RADIUS Configuration

The Remote Authentication Dial-In User Service (RADIUS) protocol is a networking protocol that provides centralized authentication, authorization, and accounting management.

AppViewX integrates with RADIUS for authentication of external users.

To configure the RADIUS authentication:

1. On the **Settings :: Authentication** page, under the **RADIUS** tab, enter the following details (sample values are shown in the image):



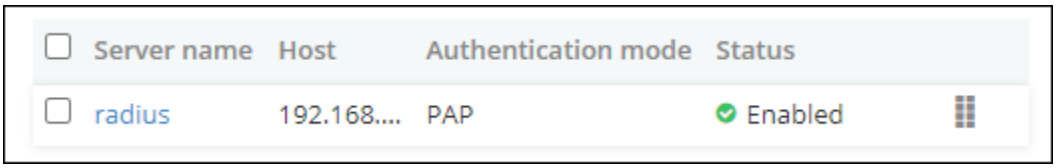
Field descriptions for RADIUS

Field	Description
***Server name**	Name of the RADIUS server.
***Host**	The IP address of the RADIUS server.
***Shared secret**	A unique key for authentication between the AppViewX server and the RADIUS server.
***Authentication port**	Port number that AppViewX will use for authentication.

Field	Description
	Note: The default authentication port number is 1812. Please check with your system admin if your organization uses a different port number.
***Acceptance port**	Port number that AppViewX will use to accept a response from the RADIUS server. **Note:** The default acceptance port number is 1813. Please check with your system admin if your organization uses a different port number.
***Authentication mode**	Select one of the following authentication modes: • PAP/ASCII • CHAP • MS-CHAPv2 • EAP-MD5 **Note:** Ensure that the selected authentication mode is also confirmed in the RADIUS server settings.
***Authorization**	In addition to authentication, AppViewX also lets you perform user authorization against the RADIUS server. To enable authorization along with authentication, turn on the toggle. **Note:** If Authorization is not enabled, AppViewX will only carry out RADIUS authentication for the given user.
***Authorization via**	Select from one of the following authorization modes: • RADIUS: To perform both, authentication and authorization, via the RADIUS server • LDAP: To perform authentication via the RADIUS server and authorization via the LDAP server

Field	Description
	Note: This field is enabled only when the **Authentication** toggle is turned on.
***Vendor ID**	Enter the vendor ID. **Note:** AppViewX does not have a unique vendor ID. We use a free vendor ID: **500**. Ensure that this is configured as part of the RADIUS server settings. **Note:** This field is enabled only when the **Authentication** toggle is turned on and authorization is done via the RADIUS server.
***Vendor type**	Enter the vendor type. **Note:** AppViewX does not have a unique vendor type. We use a free vendor ID: **200**. Ensure that this is configured as part of the RADIUS server settings. **Note:** This field is enabled only when the **Authentication** toggle is turned on and authorization is done via the RADIUS server.
***LDAP**	From the drop-down menu, select the LDAP server to be used for the authorization. **Note:** This field is enabled only when the **Authentication** toggle is turned on and authorization is done via the LDAP server.
Note: The asterisk (*) symbol indicates mandatory fields.	

2. To save the RADIUS authentication settings entered above, click **Add**.
   The RADIUS authentication settings thus configured are saved and displayed in the table shown in the left half of the screen:



Note: In the case of multiple RADIUS servers, to define/update the order in which the servers will be authenticated, drag and drop the entries in this table.

3. To reconfigure the settings, click **Reset**.

• Enabling a RADIUS Server for Authentication
• Disabling a RADIUS Server for Authentication
• Deleting a RADIUS Server

Enabling a RADIUS Server for Authentication

To enable a RADIUS server for authentication:

1. On the **Settings :: Authentication** page, under the **RADIUS** tab, from the table displayed in the left half of the page, for the server you want to enable, select the check box corresponding to the server name.

2. From the top-right corner of the page, click **(Enable)** icon.
3. In the **Confirmation message** dialog box, click **Proceed**.

Disabling a RADIUS Server for Authentication

To disable a RADIUS server for authentication:

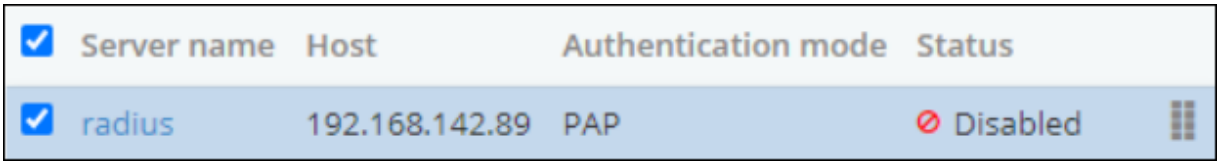
1. On the **Settings :: Authentication** page, under the **RADIUS** tab, from the table displayed in the left half of the page, for the server you want to disable, select the check box corresponding to the server name.

2. From the top-right corner of the page, click **(Disable)** icon.
3. In the **Confirmation message** dialog box, click **Proceed**.

Deleting a RADIUS Server

To delete a RADIUS server:

1. On the **Settings :: Authentication** page, under the **RADIUS** tab, from the table displayed in the left half of the page, for the server you want to delete, select the check box corresponding to the server name.



2. From the top-right corner of the page, click **(Delete)** icon.
3. In the **Confirmation message** dialog box, click **Proceed**.

Single Sign On Configuration

Single Sign-On Configuration involves setting up systems to enable users to access multiple applications with a single set of credentials, simplifying authentication processes and enhancing user experience across different platforms or services.

- Accessing the SSO Configuration Settings
- Configuring Single Sign On Settings with AppViewX

Accessing the SSO Configuration Settings

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **ACCESS MANAGEMENT**, select **SSO**. The **Settings :: Authentication** page is displayed with the **SSO** tab open by default.	1. From the main navigation menu, click **Settings**. 2. On the **Settings** page, from the left menu, select **General** > **Authentication**. The **Settings :: Authentication** page is displayed with the **LDAP** tab open by default. 3. Click the **SSO** tab.

Note: For more information on how to switch between menus, click here.

Configuring Single Sign On Settings with AppViewX

Single sign-on (SSO) is an authentication method that enables users to securely authenticate with multiple applications and websites by using just one set of credentials.

To configure single sign on settings with AppViewX:

On the **Settings :: Authentication** page, under the **SSO** tab, turn on the **Enable SSO** toggle.

The **Authentication protocol** field is displayed with the following options:

- **SAML** (selected by default)
- **OIDC**

Security Assertion Markup Language

SAML Overview

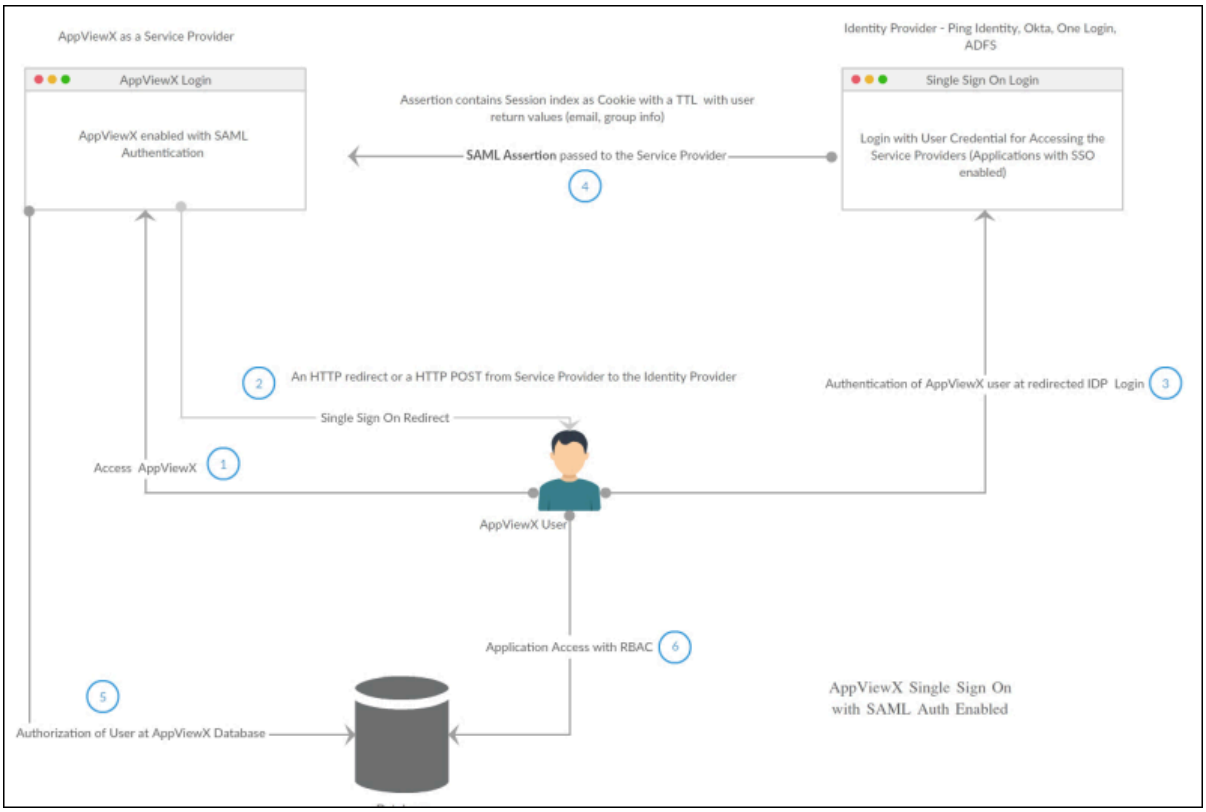
Security Assertion Markup Language (SAML) is a mechanism used for communicating identities between two web applications. It enables a web-based Single sign-on (SSO) and hence, it eliminates the need for maintaining credentials for various applications and reduces identity theft.

SAML integration requires the following parameters:

- IDP – Identity Provider (Okta, OneLogin, PingIdentity, and OpenSSO)
- SP – Service Provider (any application which supports SAML 2.0), AppViewX in this case
- User – Access the application.

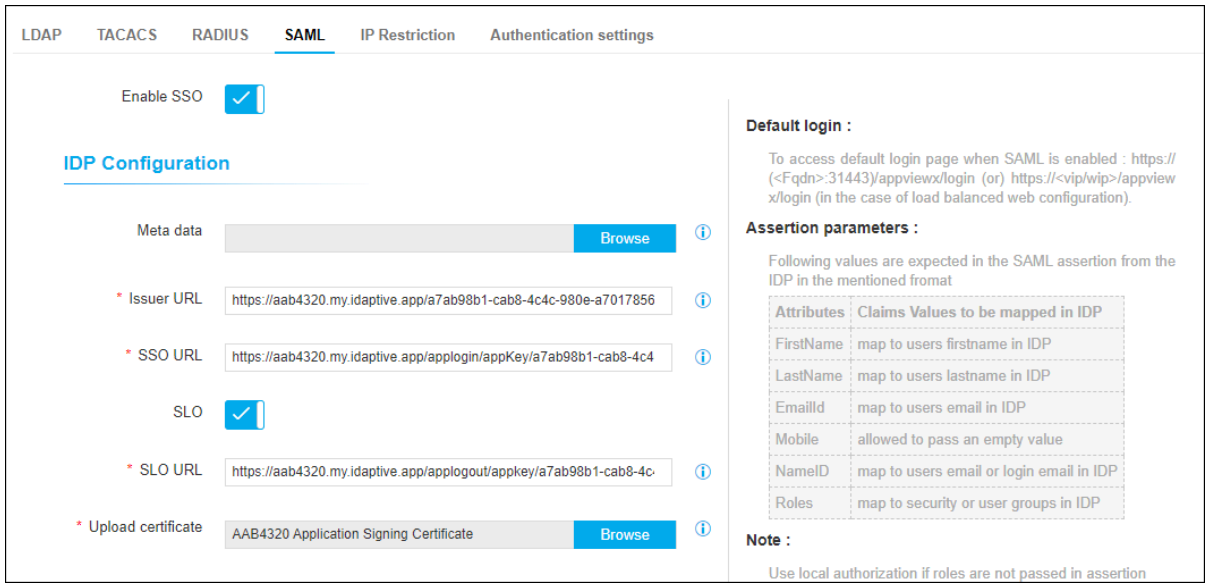
Basic SAML Flow

A user requests a SAML SSO to access a resource protected by a service provider. The service provider requests the identity provider to authenticate and authorize the user. The identity provider checks the existence of the user and sends back an assertion to the service provider that may or may not include the user information. The communication passes through the HTTP/HTTPS.



Configuration of SAML Parameters in AppViewX (Service Provider)

1. On the **Settings :: Authentication** page, under the **SSO** tab, turn on the **Enable SSO** toggle.
2. In the **Authentication Protocol** field, select the **SAML** option.
3. Enable the **Enable SSO** toggle. This action will populate the service provider contents for the integration.
4. Under the **IDP Configuration** section, enter the required field information.



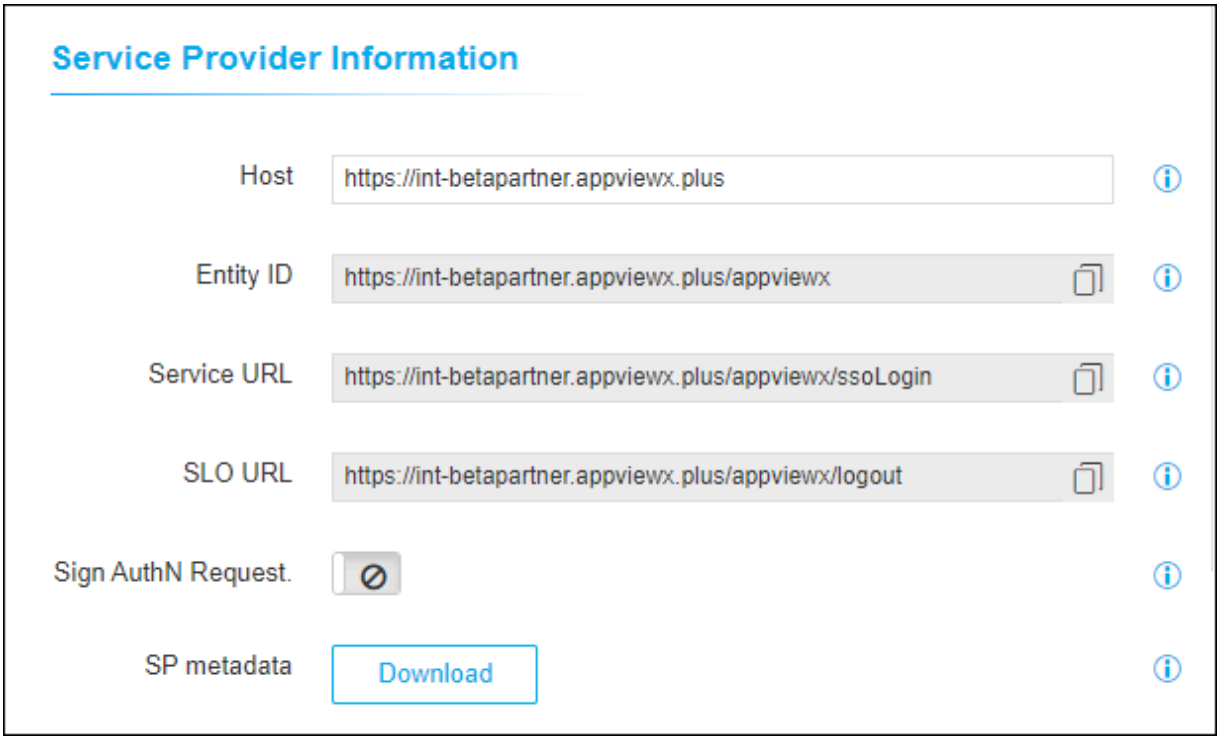
Field descriptions for IDP Configuration

Field	Description
Meta data	Upload the Metadata, which is downloaded from your Identity Provider. **Note:** Upload of metadata automatically parses the fields SSO, SLO, and so on.
***Issuer URL**	**Note:** This field is auto-populated upon uploading of the **Meta data**. In case the **Meta data** is unavailable, enter the ID of the Identity Provider.
***SSO URL**	**Note:** This field is auto-populated upon uploading of the **Meta data**. In case the **Meta data** is unavailable, enter the SSO URL, which is a single sign-on URL for the service provider to authenticate the users.
SLO	Enable/Disable SLO as per requirement.
***SLO URL**	**Note:** This field is auto-populated upon uploading of the **Meta data**.

Field	Description
	In case the **Meta data** is unavailable, enter the SLO URL, which is the SAML logout URL to send logout responses.
***Upload certificate**	Upload the IdP certificate in **.pem** format if it is not available as a part of your IdP metadata.

Note: The asterisk (*) symbol indicates mandatory fields.

5. Under the **Service Provider Information** section, enter the required field information.

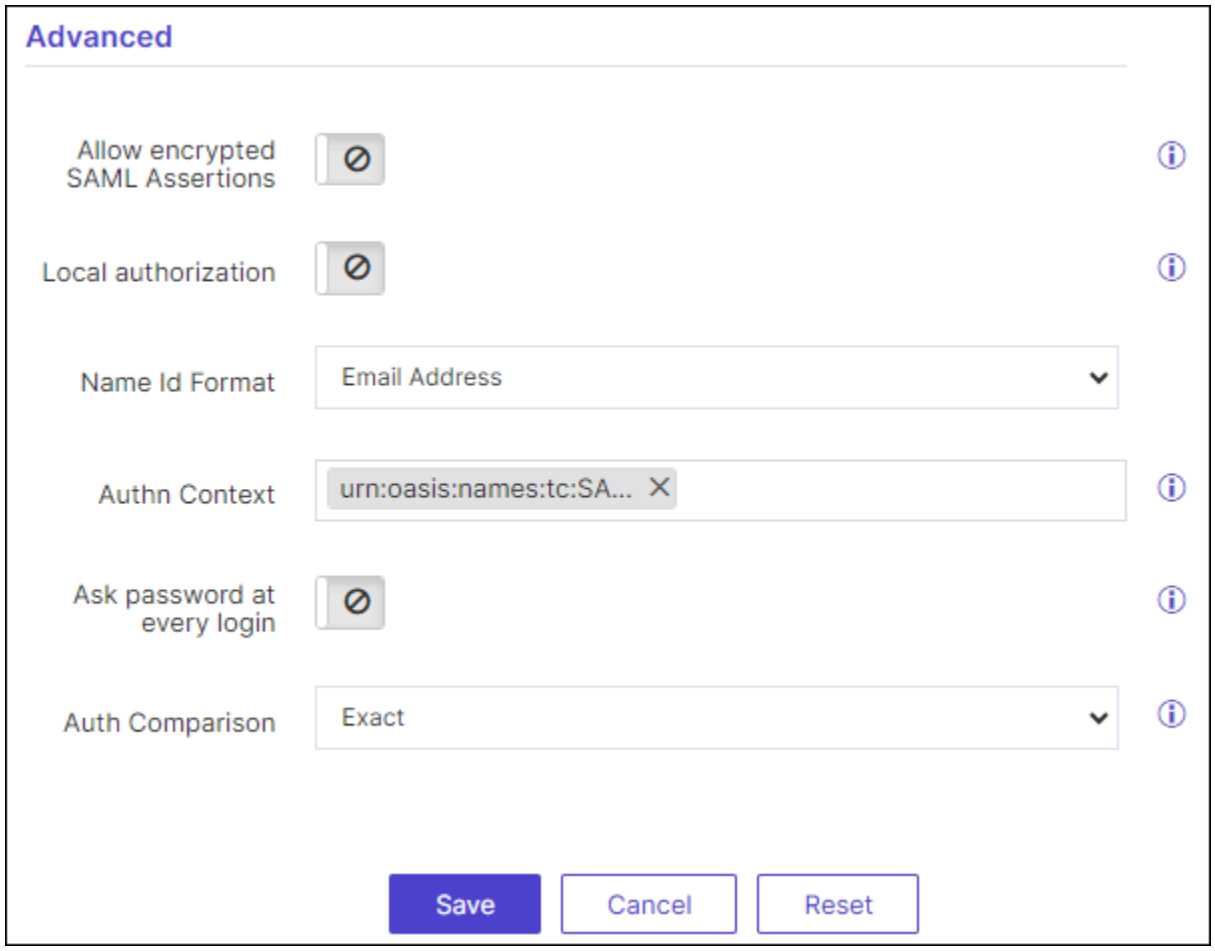


Field descriptions for Service Provider Information

Field	Description
Host	Enter the host information for AppViewX in the Host field. The host information can be the Hostname/URL used to access the application. **Note:** The **Entity ID**, **SSO URL** and the **SLO URL** fields will be auto-populated based on the Host information provided.

Field	Description
Entity ID	**Note:** This field is auto-populated based on the **Host** information provided.
Service URL	**Note:** This field is auto-populated based on the **Host** information provided.
SLO URL	**Note:** This field is auto-populated based on the **Host** information provided.
Sign AuthN Request	Enable/Disable the Sign AuthN Request toggle to send signed AuthN requests from AppViewX to your Identity Provider. **Note:** This is to be enabled only when your IdP requires a sign authN request from service provider. Once the Sign AuthN Request is enabled, Upload a Service Provider certificate and private key in a p12 format and provide the p12 Password. Choose the Signing Algorithm (Recommended Algorithm: SHA-256) from the drop-down list. The Service provider certificate should be shared with the IDP to validate the Service Provider SAML assertion signature.
SP metadata	Download the Service Provider information (Entity Id, SSO/Service URL, SLO URL) to be consumed at IdP.

6. Under the **Advanced** section, enter the required field information.



Field descriptions for Advanced

Field	Description
Allow encrypted SAML Assertions	Enable/Disable the Allow encrypted SAML Assertions to encrypt SAML assertion using decryption certificate and decryption certificate password. If SAML Assertions are encrypted in the IDP, enable this field to decrypt the SAML assertions before using them in AppViewX. Once Allow Encrypted SAML Assertions is enabled, upload the Assertions decryption certificate and private key in a p12 format, and the password of the Assertions decryption certificate provide the p12 password to decrypt the private key in the certificate. The service provider certificate should be shared with the IDP to validate the service provider SAML assertion.
Upload Assertions	Upload the Assertions decryption certificate. Private key in this certificate will be used to decrypt the SAML assertions.

Field	Description
decryption certificate	**Note:** This field is visible only when 'Allow encrypted SAML Assertions' is enabled.
Password of Assertions decryption certificate	Enter the password to decrypt the private key in the certificate. **Note:** This field is visible only when 'Allow encrypted SAML Assertions' is enabled.
Local authorization	Enable/Disable the Local authorization to authenticate in IdP and authorize in AppViewX. If the IDP is unable to pass the roles/usergroup as a part of the SAML assertion and requires AppViewX to perform the Authorization then the above feature can be used. **Note:** This feature is available from 20.1 version of AppViewX.
Name Id Format	Choose the Name id Format from the drop-down list.
Authn Context	Enter the Authn Context in the text field. Use any one of the below values for a customized type of authn request needed by your IDP. Other RFC SAML2.0 standard authn request can also be used. (Copy and paste the below values or add values in the same format from RFC to the AuthN context field). • urn:oasis:names:tc:SAML:2.0:ac:classes:X509. • urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient. • urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport • urn:oasis:names:tc:SAML:2.0:ac:classes:Password • urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos • urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol
Ask password at every login	If this option is enabled, the user will be required to enter their password during each login, even if a single sign-on (SSO) session is currently active.
Auth Comparison	Choose the Auth Comparison from the drop-down field. This indicates how the authentication context URI in the Authn Request message compares to the context defined at the asserting party. It is preferred to be exact.

7. Click **Save**.
8. If the configuration provided needs to be removed, click **Reset**.

Mapping User Groups for Local Authorization

Administrators can map user groups manually for external users login through SSO by using either Manual mapping or Birthright.

Manual Mapping

Once the user logins to AppViewX using SSO if no proper Roles are passed in the Assertion the user will end on a No Usergroup found page. Now the administrator can log in with the default login URL **https://ip:port/appviewx/login** and navigate to Account > Users. The user who has not logged in will have the user-created tag and will be in an inactive state. Administrators can modify the user and map the user to a user group that is available and this will enable the user to login successfully on the next attempt.

Birthright Role

The administrator can enable a birthright role and map a user group by default for all the sso users to log in initially when they do not have a role/user group passed in the SAML assertion. This would enable the user to login successfully and access the application with the access given in the specific user group. If required now the administrator can create different sets of user groups and assign manually to the respective users who do not need the birthright user group which will be reflected in the subsequent login.

Troubleshooting

Enable the SAML extension in the browser. While performing the login, enable the DEV tools and open the SAML tab. During the operation, the SAML assertions are passed in the HTTP headers. Similar to the external authentication configuration, if the role name passed in the SAML assertion matches the role name in the AppViewX database, the login will be successful.

Sample Configuration of SAML Assertion

Number of SAML Assertions in HTTP Headers

Sample SAML Assertion

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:Response Destination="https://192.168.x.x:31443/appviewx/ssoLogin"
   ID="id246345791662193091218321378" InResponseTo="ONELOGIN_23e56e9e-99e6-449f-ace2-67002e6fcc91"
   IssueInstant="2019-02-06T13:46:48.185Z" Version="2.0"
   xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:xs="http://www.w3.org/2001/XMLSchema">
   <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
      xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">http://www.okta.com/exk9y6yf2Td4qxk5M356</saml2:Issuer>
   <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo><ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/><ds:SignatureMethod
 Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
         <ds:Reference URI="#id246345791662193091218321378">
            <ds:Transforms><ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
               <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ec:InclusiveNamespaces PrefixList="xs"
 xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/></ds:Transform>
            </ds:Transforms><ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
            <ds:DigestValue>V4ngGSIWBR81C4VzBI2K8nM4QTxrexhuJAVDZ1f4cYQ=</ds:DigestValue>
         </ds:Reference>
      </ds:SignedInfo>

 <ds:SignatureValue>ZBrsl0pRRB8gaqYHnoyjISEsA8s1cUAn5Fy5rJ/MyNRxtLlKDPrBBKgT0s0LkKodMEQavwgr2uN6pc0LdXVvRge8Taea1apeiThGWLjt17hRU
NBUTJFbLllgpfjf6dBf6E4FpqAO6p0/SbGRkeFKU1dUVUHwlizsNxjeS+QoTJG9OwivLxgxvzfNuLicPgrPJMesZcgyEOiFXB09OK5RwcSktOWE7C7iGCP6OMbUpP
KasJTJ89iJrW4/ATaHBZJ3faV/gqbYcQerdKxyXsMQMM/MzIRAfd9CfXyPsL+T/26BOnLN5F/Gq/36cYGrEuUJ0MdzHBrRualKe/bRiqQR2Q==</ds:SignatureVal
ue>
      <ds:KeyInfo>
         <ds:X509Data>
            <ds:X509Certificate>MIIDqDCCApCgAwIBAgIGAWiodnVYMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYDVQQGEwJVUzETMBEG
```

```
            A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
            MBIGA1UECwwLU1NPUHJvdmlkZXIxFTATBgNVBAMMDGFwcHZpZXd4LXNzbzEcMBoGCSqGSIb3DQEJ
            ARYNaW5mb0Bva3RhLmNvbTAeFw0xOTAyMDEwOTQ4MjJaFw0yOTAyMDEwOTQ5MjJaMIGUMQswCQYD
            VQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsG
            A1UECgwET2t0YTEUMBIGA1UECwwLU1NPUHJvdmlkZXIxFTATBgNVBAMMDGFwcHZpZXd4LXNzbzEc
            MBoGCSqGSIb3DQEJARYNaW5mb0Bva3RhLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
            ggEBAIc22r1CR7gbMVcyYnRjkDLGRwHJ1zhQkWTVoEZdbk/KTHwVMXHpNinkOhUcxbzfHePBf6wx
            9jEThiNvvHZVIg6ZktYotG9DF/FF0fMxhzfweqR5yt27ihiuVTeGT8GjNcXwOoyzJdrDuZg27ybI
            jriqGPKrLiwrrot54R1LP2VclM0FdIOWdOoU1N5IEnFAd+2UECZZLQ0gJrDpFcbDisuhmp5bTKUS
            1RpIxarNeacH2klRY4efeqQdVgaghgs+zMN44iz+YGs8uELElKErOabEtoYiTJmsVnqEcs8fUvKx
            LLdZevPhh89v0MJiZI9gTjjt/f9N+NEUzyJsHfxqmnUCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEA
            RZo42X1gDE3d9xnftXr2LoUItdTQeVoFdkIJIqJla21kDRCwHis2OvuFwOW+QdUeh5uUIjGxbhaA
            cQIeJUvuD1aEK/ynUDKGA0jvdLR7IbwTK69i7c19F7pti6b5sq8yjl5fOavit1N3INIzZdkrPlP1
            hJnKcjOSVyMPv8a7rDXOtXxDoZgi+pWj0qlp4E9tKOrWJgKdjS8j03ulWwtOx4Jak4yYueaY8nH1
            +amyE6w96Qm6ScEGLcxXzboczS7BMjZ0M4Mr6zXOTS8pU+AX6NBmdNkdwO9JSeXm3U6lRWv59jet
            qMeKqf4aKRg+oqbw9hkH3X6qT69AeEiPz6YPmQ==</ds:X509Certificate>
        </ds:X509Data>
    </ds:KeyInfo>
  </ds:Signature>
  <saml2p:Status xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"><saml2p:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></saml2p:Status>
  <saml2:Assertion ID="id246345791662997898329801l6" IssueInstant="2019-02-06T13:46:48.185Z"
    Version="2.0" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:xs="http://www.w3.org/2001/XMLSchema">
    <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
      xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">http://www.okta.com/exk9y6yf2Td4qxk5M356</saml2:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo><ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/><ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
        <ds:Reference URI="#id246345791662997898329801l6">
          <ds:Transforms><ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ec:InclusiveNamespaces PrefixList="xs"
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/></ds:Transform>
          </ds:Transforms><ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
          <ds:DigestValue>hnTKZKSyxKC6WGZTK7iD+iQv4+nj/91eX8vhrkyi+1k=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
```

<ds:SignatureValue>OtgpFXWkIIO0hSZiHpAdTDBg6v11+/unBzyPOFSBl+0+b2i22s3lHtzCqsEVp4Xn9J1XoL12tCr/uhg7b4kxcTslMsAYFVQipUZLKanEIaEOSv2
tnjQuAoE3fBMTm2d/3+nlXofyGiOMEY5OrFaGGjC9ZAMk2qJDAEzjZHhjOyooLQItzDocfVFvXeFSl/bAaDNSRPYT0B9dXsGpjpUlA6CMpmJXSxgAPwogaM20d48
o7iKi3THjTgm1L2z9nntQajfaRERkoTfAV0sGE6iKlUAhWmtMkUDOUXbMeBXo61cpQ5A/WsfxpbZKhJkDes/9lzcDoPkI7w+TshJnQMQA3A==</ds:SignatureVal
ue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>MIIDqDCCApCgAwIBAgIGAWiodnVYMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxFTATBgNVBAMMDGFwcHZpZXd4LXNzbzEcMBoGCSqGSIb3DQEJ
ARYNaW5mb0Bva3RhLmNvbTAeFw0xOTAyMDEwOTQ4MjJaFw0yOTAyMDEwOTQ5MjJaMIGUMQswCQYD
VQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsG
A1UECgwET2t0YTEUMBIGA1UECwwLU1NPUHJvdmlkZXIxFTATBgNVBAMMDGFwcHZpZXd4LXNzbzEc
MBoGCSqGSIb3DQEJARYNaW5mb0Bva3RhLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBAIc22r1CR7gbMVcyYnRjkDLGRwHJ1zhQkWTVoEZdbk/KTHwVMXHpNinkOhUcxbzfHePBf6wx
9jEThiNvvHZVIg6ZktYotG9DF/FF0fMxhzfweqR5yt27ihiuVTeGT8GjNcXwOoyzJdrDuZg27ybI
jriqGPKrLiwrrot54R1LP2VcIM0FdIOWdOoU1N5IEnFAd+2UECZZLQ0gJrDpFcbDisuhmp5bTKUS
1RpIxarNeacH2klRY4efeqQdVgaghgs+zMN44iz+YGs8uELElKErOabEtoYiTJmsVnqEcs8fUvKx
LLdZevPhh89v0MJiZI9gTjjt/f9N+NEUzyJsHfxqmnUCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEA
RZo42X1gDE3d9xnftXr2LoUItdTQeVoFdkIJIqJla21kDRCwHis2OvuFwOW+QdUeh5uUIjGxbhaA
cQIeJUvuD1aEK/ynUDKGA0jvdLR7IbwTK69i7c19F7pti6b5sq8yjl5fOavit1N3INIzZdkrPIP1
hJnKcjOSVyMPv8a7rDXOtXxDoZgi+pWj0qlp4E9tKOrWJgKdjS8j03ulWwtOx4Jak4yYueaY8nH1
+amyE6w96Qm6ScEGLcxXzboczS7BMjZ0M4Mr6zXOTS8pU+AX6NBmdNkdwO9JSeXm3U6lRWv59jet
qMeKqf4aKRg+oqbw9hkH3X6qT69AeEiPz6YPmQ==</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
<saml2:Subject xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
<saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">saml@appviewx.com</saml2:NameID>
<saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><saml2:SubjectConfirmationData
InResponseTo="ONELOGIN_23e56e9e-99e6-449f-ace2-67002e6fcc91"
NotOnOrAfter="2019-02-06T13:51:48.185Z" Recipient="https://192.168.x.x:31443/appviewx/ssoLogin"/></saml2:SubjectConfirmation>
</saml2:Subject>
<saml2:Conditions NotBefore="2019-02-06T13:41:48.185Z" NotOnOrAfter="2019-02-06T13:51:48.185Z"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
<saml2:AudienceRestriction>
<saml2:Audience>https://192.168.x.x:31443/appviewx/</saml2:Audience>


```
        </saml2:AudienceRestriction>
    </saml2:Conditions>
    <saml2:AuthnStatement AuthnInstant="2019-02-06T13:46:46.836Z"
        SessionIndex="ONELOGIN_23e56e9e-99e6-449f-ace2-67002e6fcc91"
        xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
        <saml2:AuthnContext>
            <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClassRef>
        </saml2:AuthnContext>
    </saml2:AuthnStatement>
    <saml2:AttributeStatement xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
        <saml2:Attribute Name="EmailId" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">saml@appviewx.com</saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute Name="FirstName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">saml</saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute Name="LastName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">appviewx</saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute Name="NameID" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">saml@appviewx.com</saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute Name="Mobile" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">0</saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute Name="Roles" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">oktarole</saml2:AttributeValue>
        </saml2:Attribute>
    </saml2:AttributeStatement>
  </saml2:Assertion>
</saml2p:Response>
```

The data in bold contains the attributes passed to AppViewX for a successful login. If this data is not passed in assertion, the assertion must be revisited.

Vendors Certified with AppViewX

AppViewX has been certified with the below SAML 2.0 enabled SSO vendors:

- Okta
- OneLogin
- ADFS
- Forgerock
- Idaptive
- Azure
- ADFS
- PingIdentity

Types of SAML Vendors

- ADFS Integration
- Okta Integration
- ForgeRock Integration
- OneLogin Integration
- Idaptive Integration

ADFS Integration

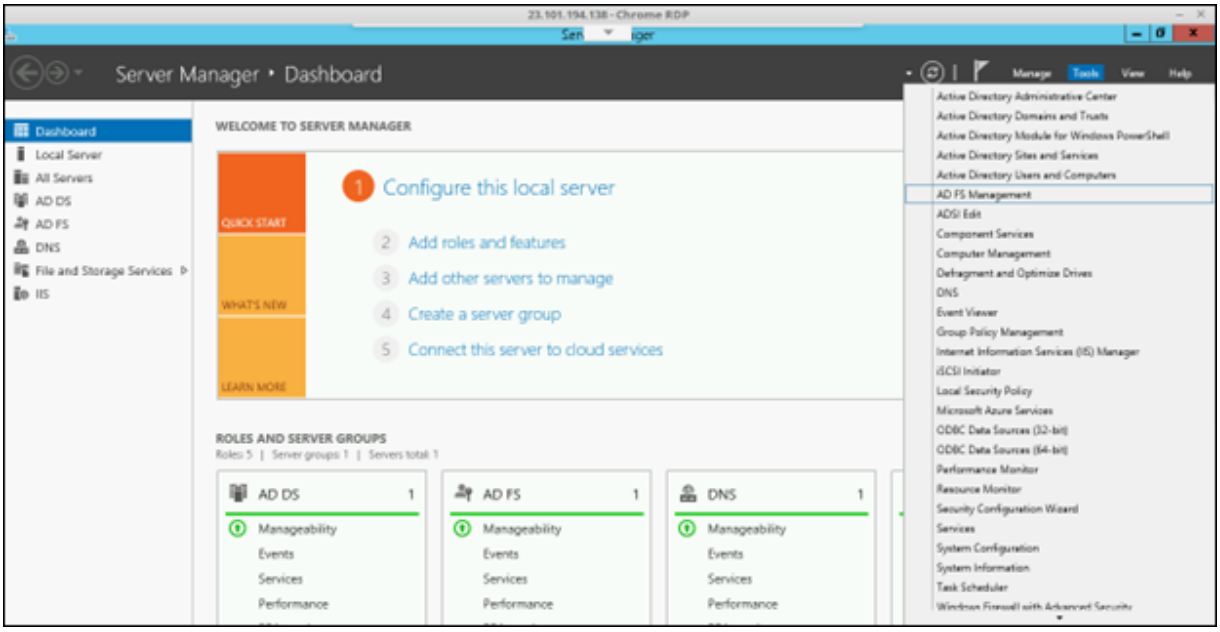
The below steps are performed at the IdP end. The navigation and screenshots might differ based on the version of the IdP. (This is just an example configuration)

Prerequisite

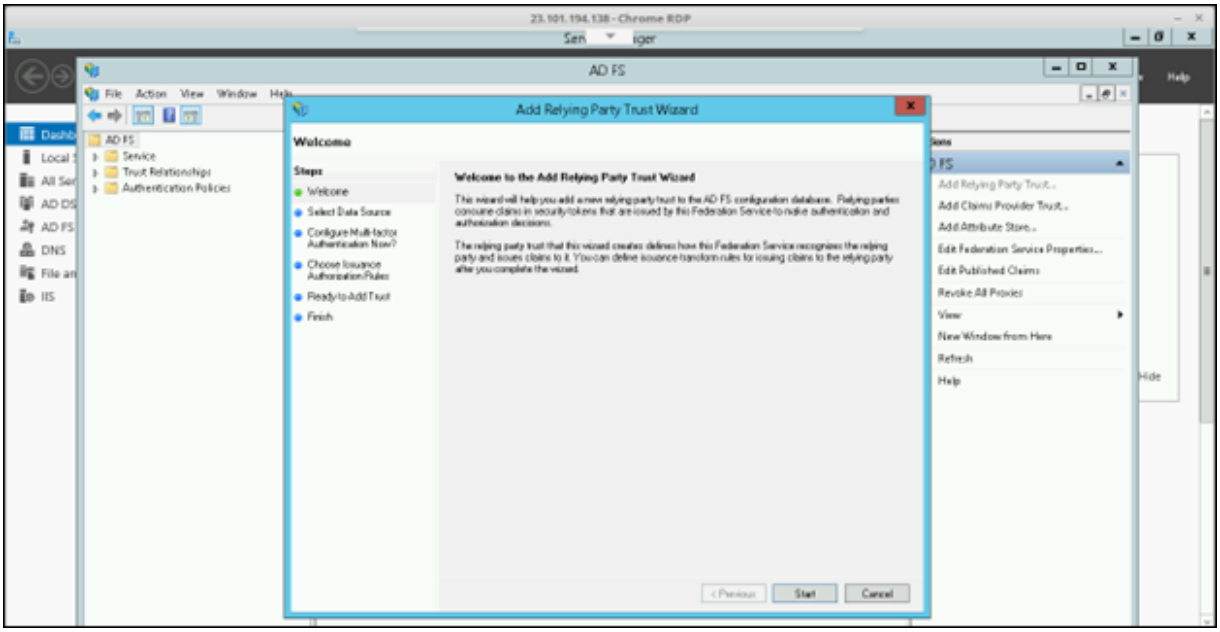
To enable ADFS based single sign-on, the ADFS service should be installed and configured with the respective Active Directory Domain.

Note: The steps are performed on the Windows 2012 R2 server with AD enabled in the same domain.

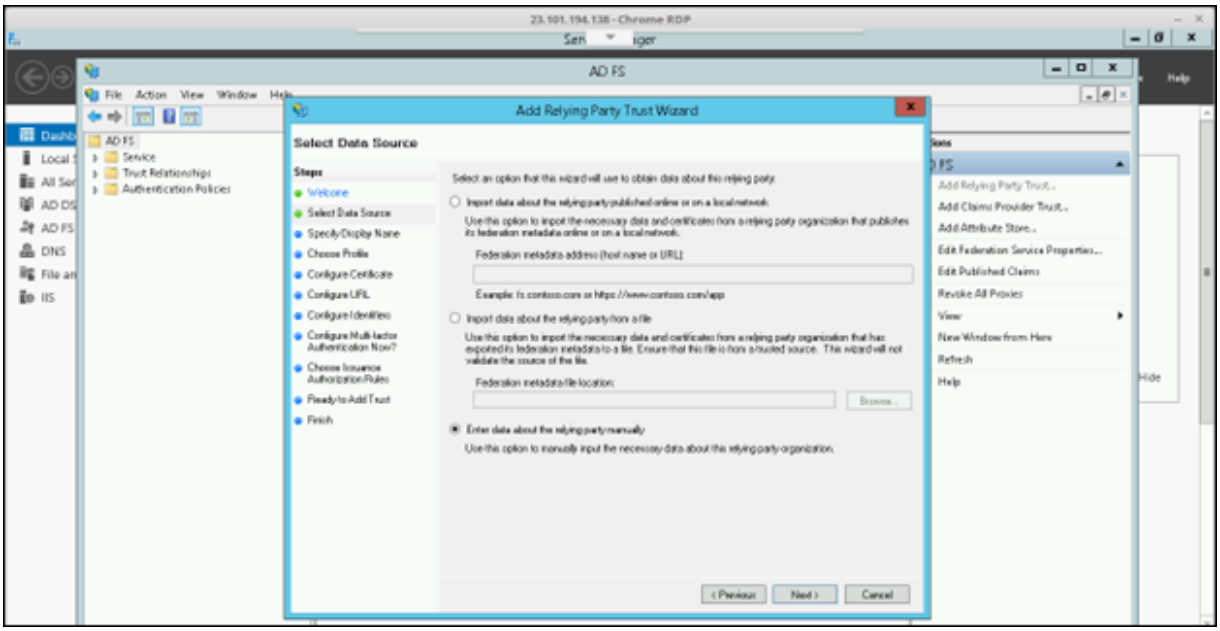
1. Navigate to **Server Manager** > **Tools** > **AD FS Management**.



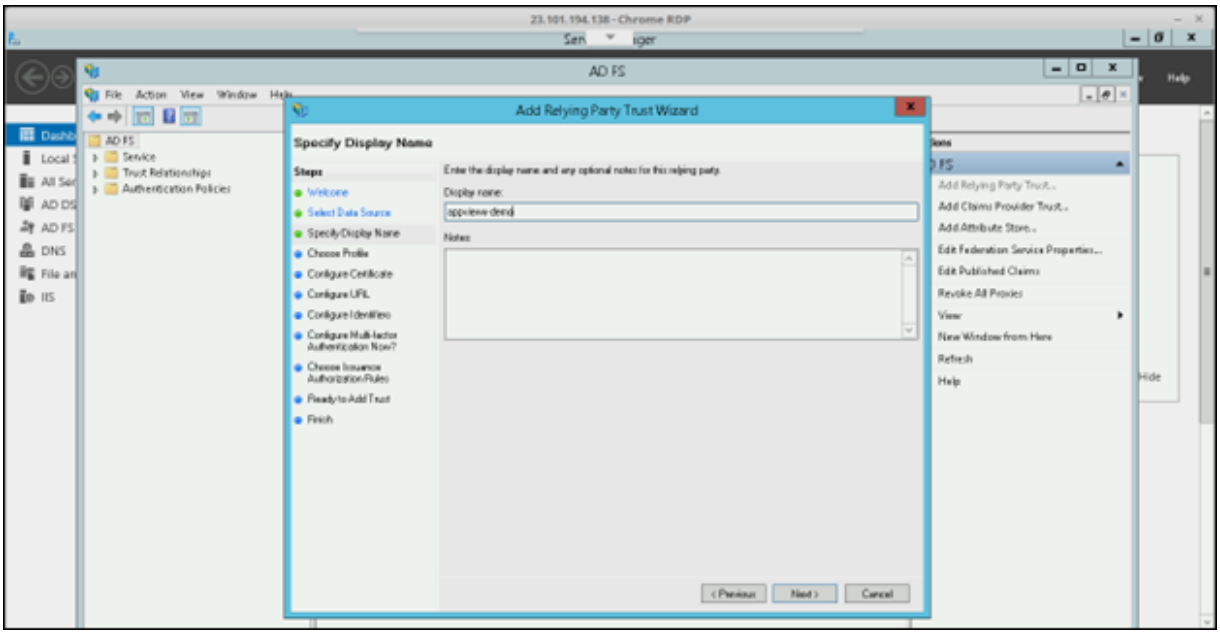
2. In the **AD FS** window, under **Actions** select **Add Relying Party Trust**.



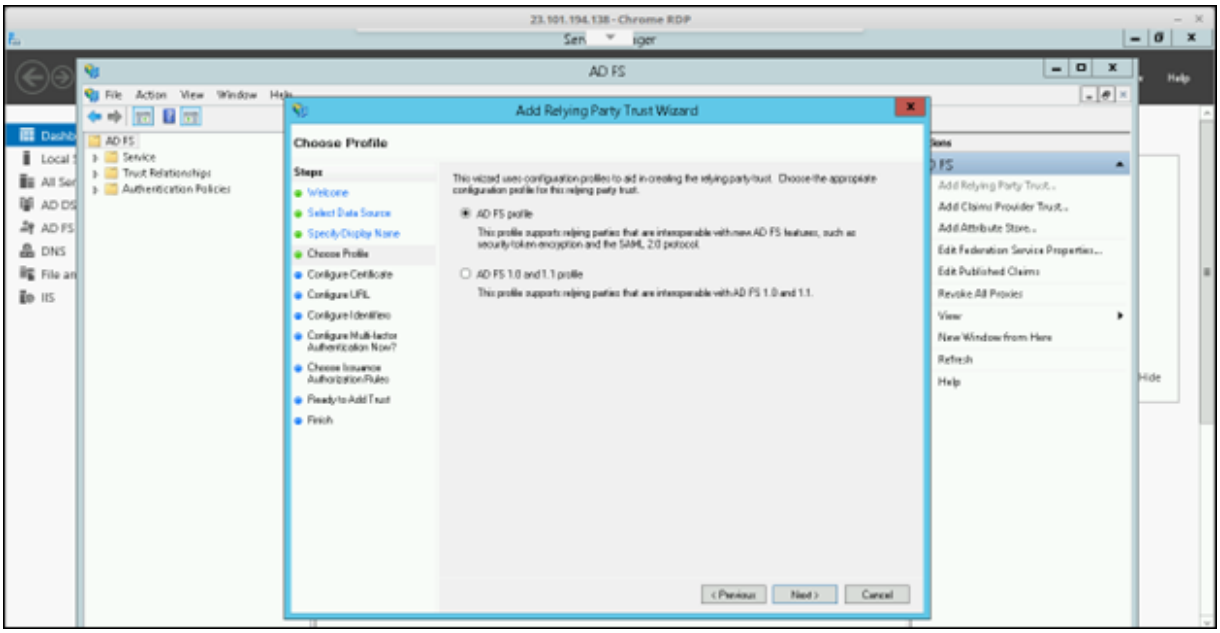
3. Click **Start** to **Add Relying Party Trust wizard**.
4. Under the **Select Data Source** section, select the **Enter data about the relying party manually** option, and then click **Next**.



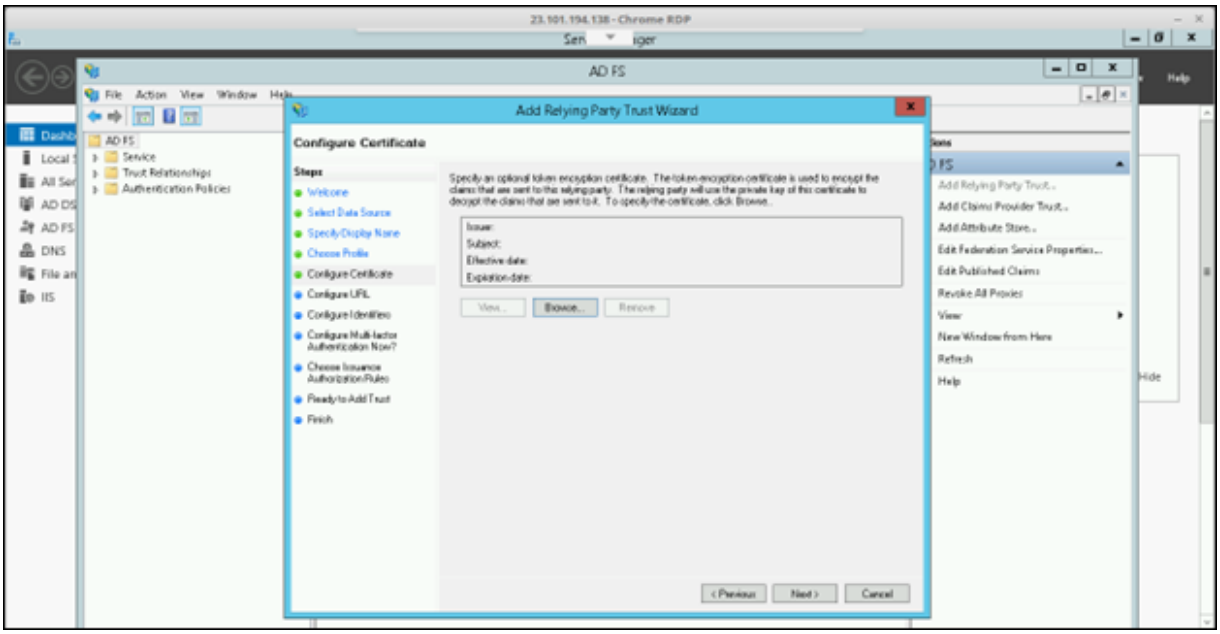
5. Enter a **Display Name** and click **Next**.



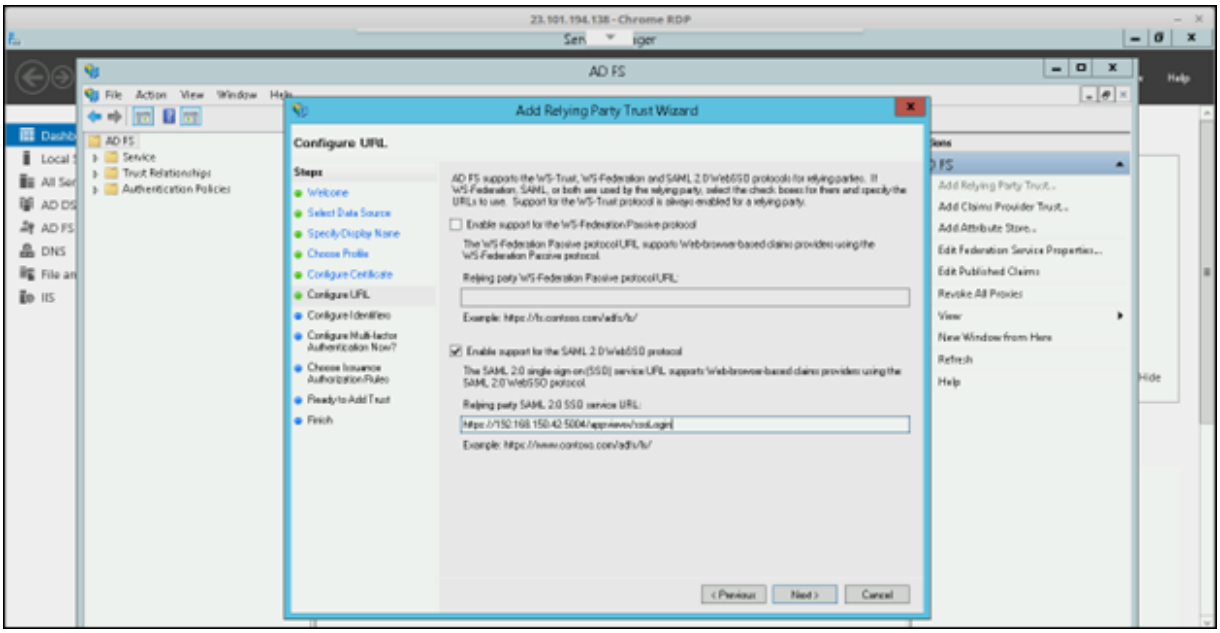
6. Under the **Choose Profile** section, select the **AD FS profile** option and click **Next**.



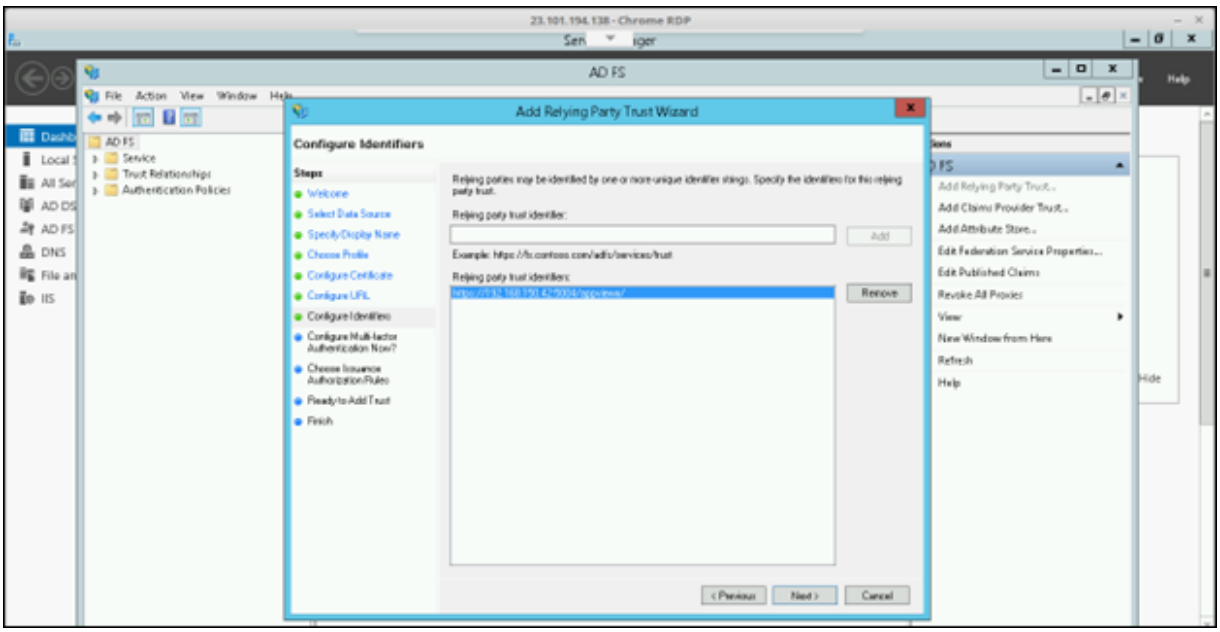
7. Add a new token encryption certificate if needed or leave it with the default setting and click **Next**.



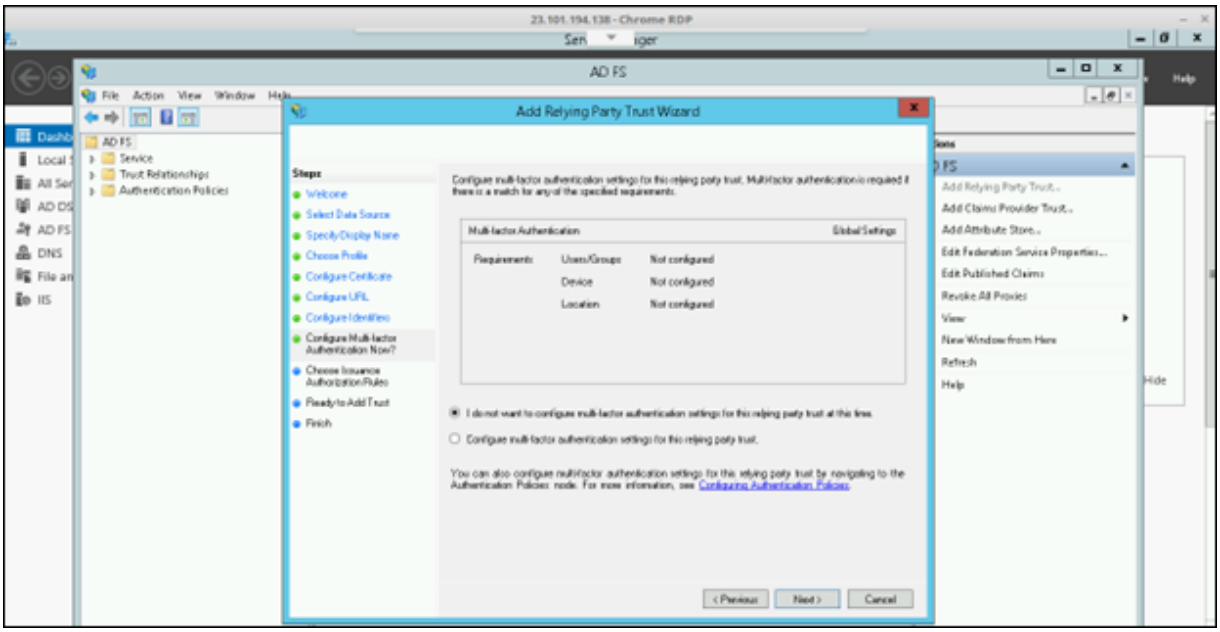
8. Under the **Configure URL** section, select the **Enable support for SAML 2.0 Web SSO protocol** option.
9. Enter the AppViewX Service URL which was copied in the previous step of Enabling SSO in AppViewX and click **Next**.



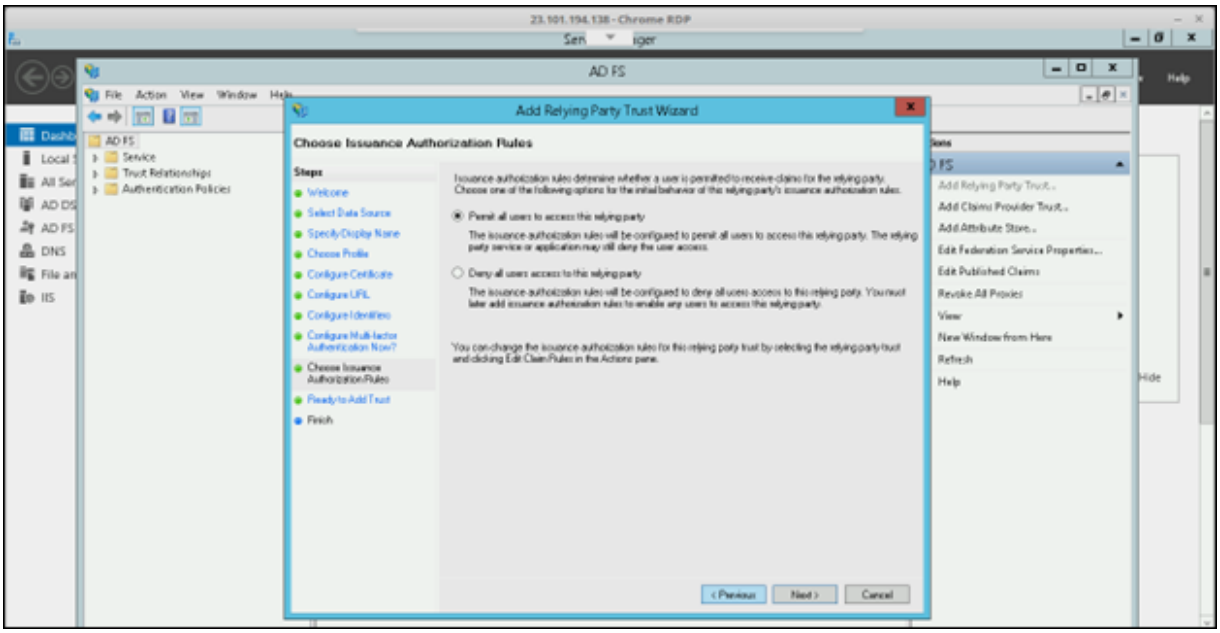
10. Under the **Configure Identifiers** section, enter the **AppViewX Entity ID** which was copied in the previous step of Enabling SSO in AppViewX and click **Add**.



11. Click **Next**.
12. Under the **Choose Multi-factor Authentication** section, select the **I do not want to configure multi-factor authentication settings at this time** option. If the organization has a multi-factor authentication setting, enable it and click **Next**.

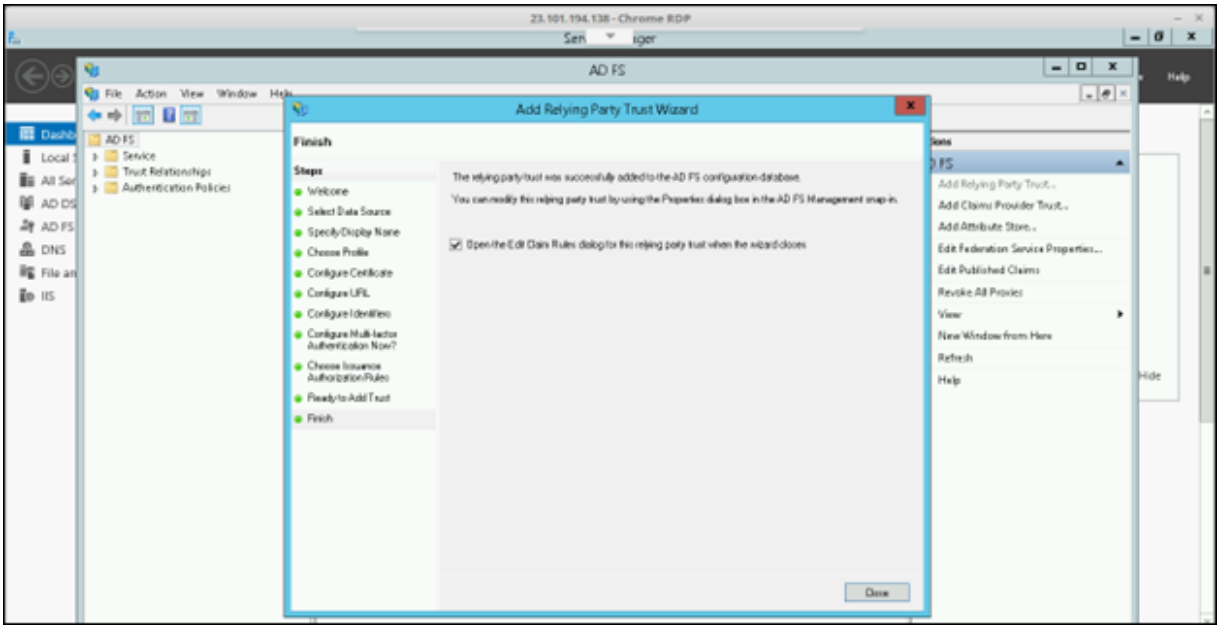


13. Under the **Choose Issuance Authorization Rules** section, select **Permit All Users to access this relying party** and then, click **Next**.



14. Under the **Ready to Add Trust** section, review the configuration done in the wizard and click **Next**.

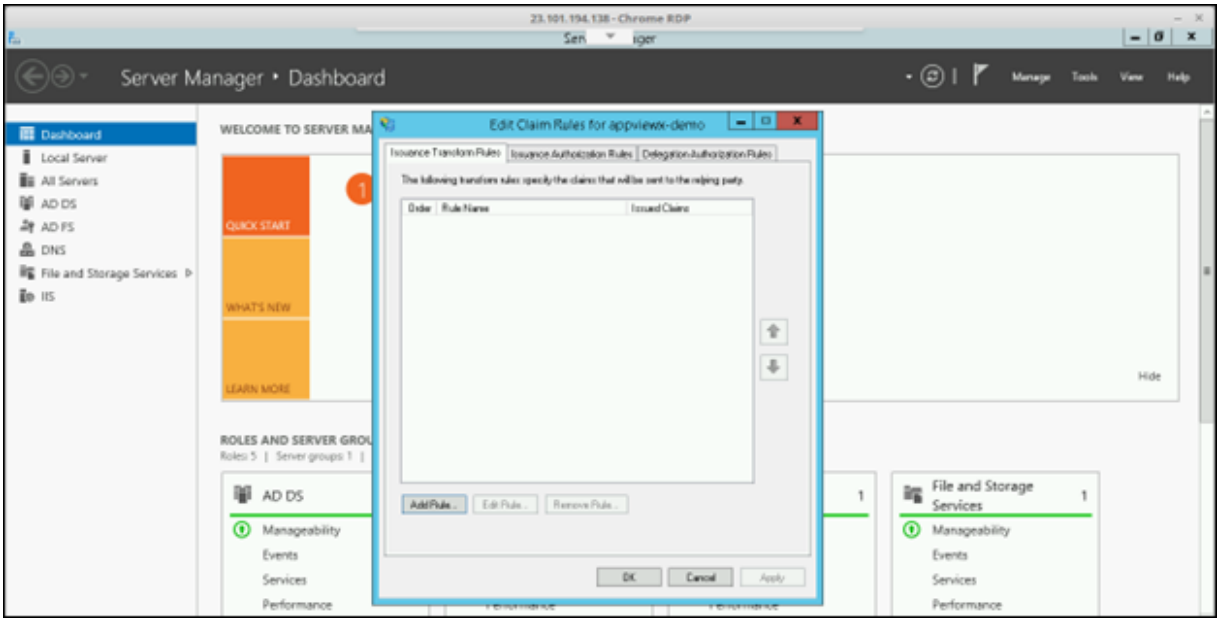
15. Under the **Finish** section, select the **Open the Edit Claims** checkbox and click **Close**.



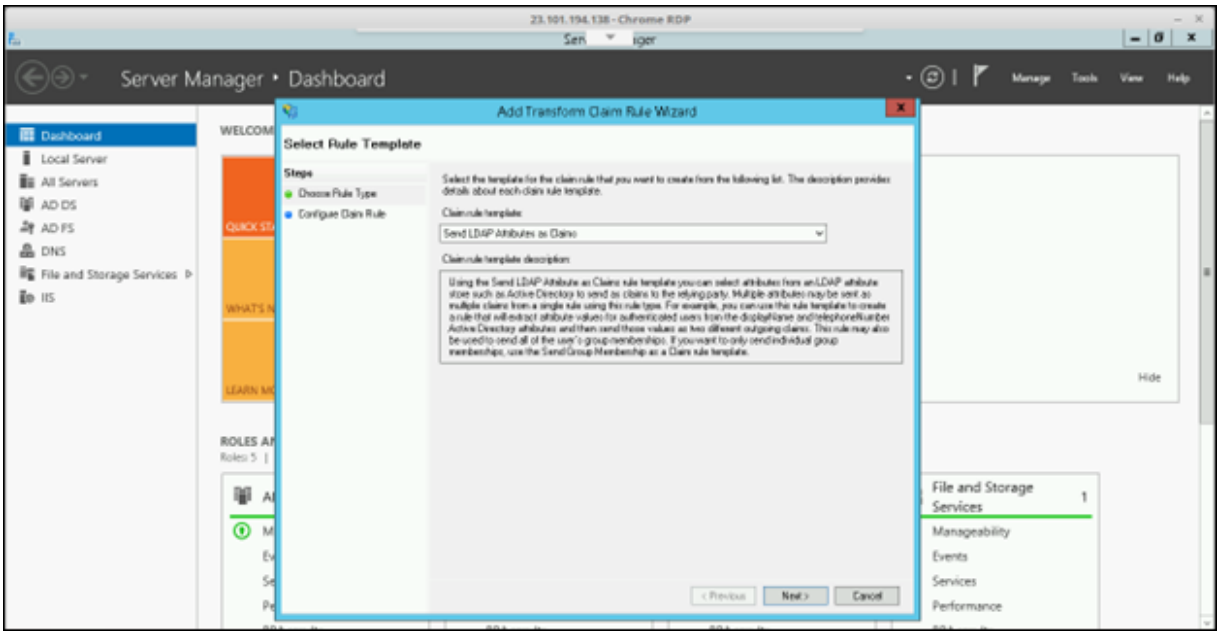
Add Claim Rules

To configure attributes or claims to be passed as an assertion Claim Rules should be created in ADFS.

1. In the **Edit Claim Rules** pane, click **Add Rule**.

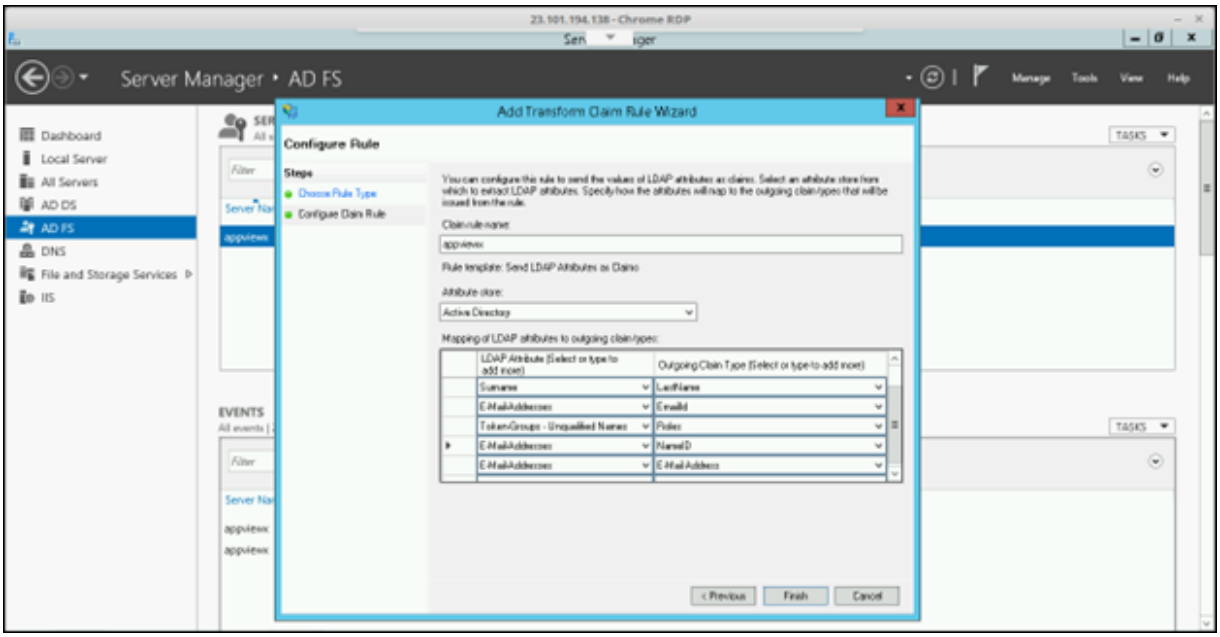


2. Under the **Select Rule Template** section, select **Rule Type** as **Send LDAP attributes as Claims** and click **Next**.

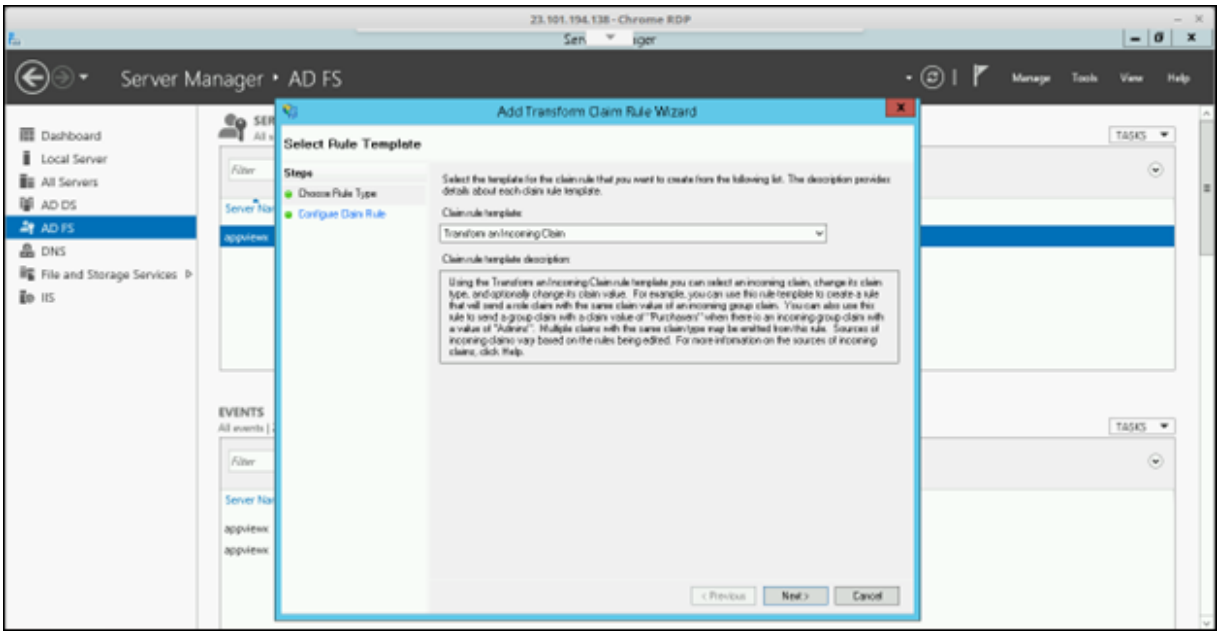


3. Enter a **Rule name** and select the **Attribute store** as **Active Directory**.
4. Enter the claim types as below, and then click **Finish**.

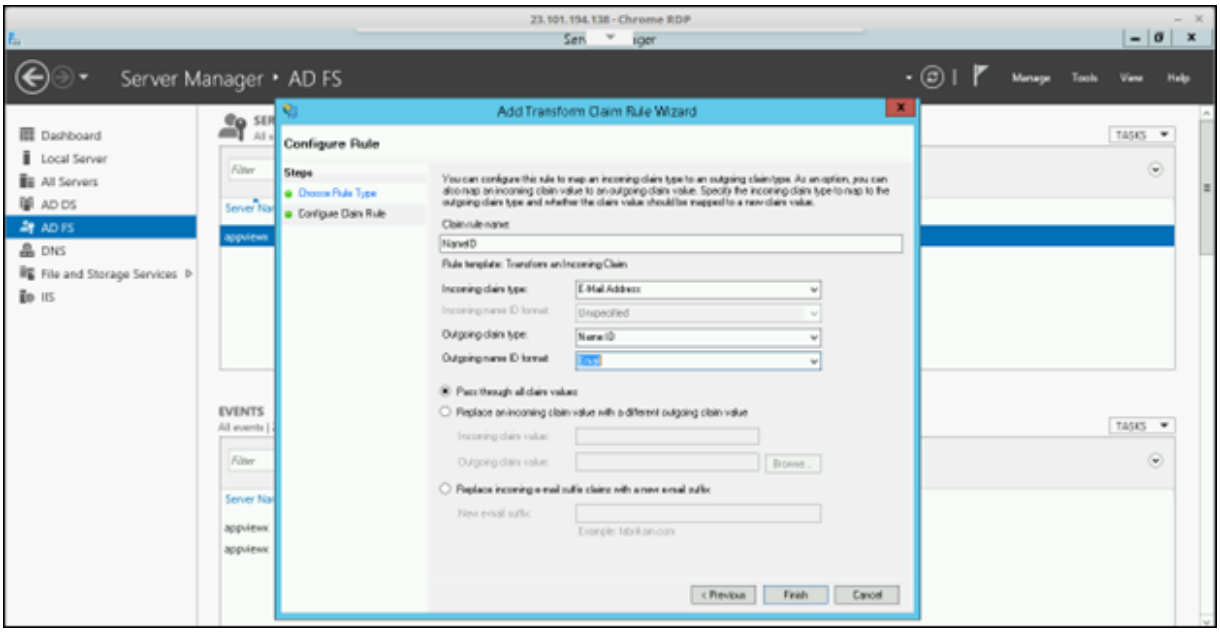
   Display-Name > FirstName, Surname > LastName, E-Mail-address > EmailId, Token-Groups-Unqualified Names > Roles, E-Mail-address > NameID, E-Mail-address > E-Mail-address.
5. Create another rule to transform the incoming claim by clicking **Add Rule** > **Rule Template** (Transform an Incoming Claim), and then click **Next**.



6. Enter a **Rule Name** and select the **Incoming Claim Type** as **E-Mail-Address**, **Outgoing Claim Type** as **Name ID**, and **Outgoing Name ID Format** as **Email**, and then click **Finish**.

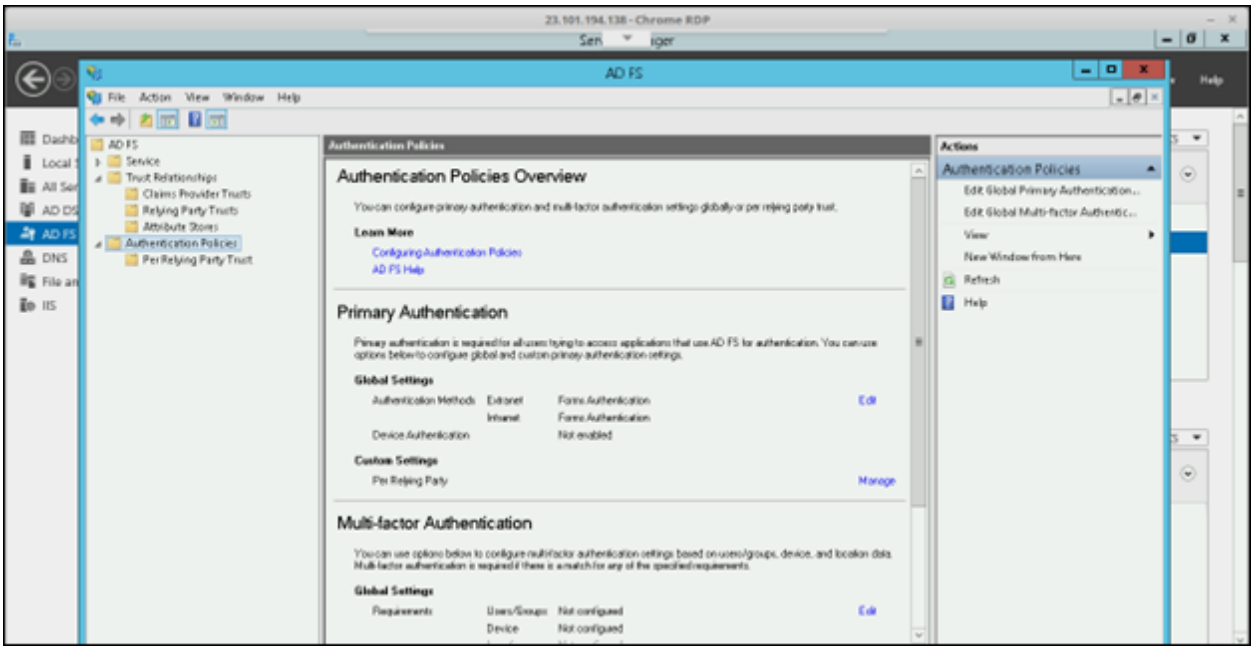


7. In the **Edit Claims** pane, click **Apply**, and then **OK**.



Enable Form-Based Authentication

For users to redirect from AppViewX to AD FS for authentication enable Form-based authentication as mentioned below. Under the AD FS menu > Authentication Policies the Primary Authentication should be Forms Authentication for Extranet and Intranet. If not select Edit and configure it as Forms Authentication.



Now AD FS is configured with all necessary details for SSO based authentication. To Export AD FS IDP metadata and upload in AppViewX SSO settings, export the metadata using the IDP URL and save it as an XML file.

Sample URL:

https://appviewx.westus.cloudapp.azure.com/federationmetadata/2007-06/federationmetadata.xml

Note: Role name passed in as a part of the SAML assertion should be configured in AppViewX on the Accounts > UserGroup and assign a role for accessing the application. For an IDP initiated SSO the following structure like URL should be used.

Sample IDP initiated URL: https://appviewx.westus.cloudapp.azure.com/adfs/ls/idpinitiatedsignon

Okta Integration

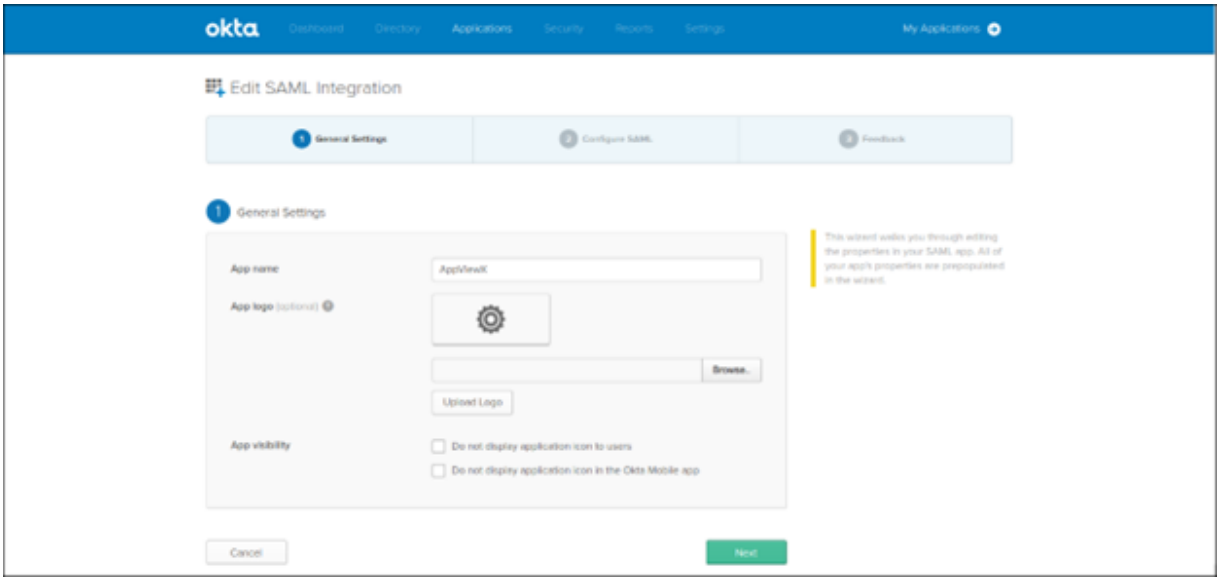
The below steps are performed at the IdP end. The navigation and screenshots might differ based on the version of the IdP.

Complete the following steps to begin the IDP configuration:

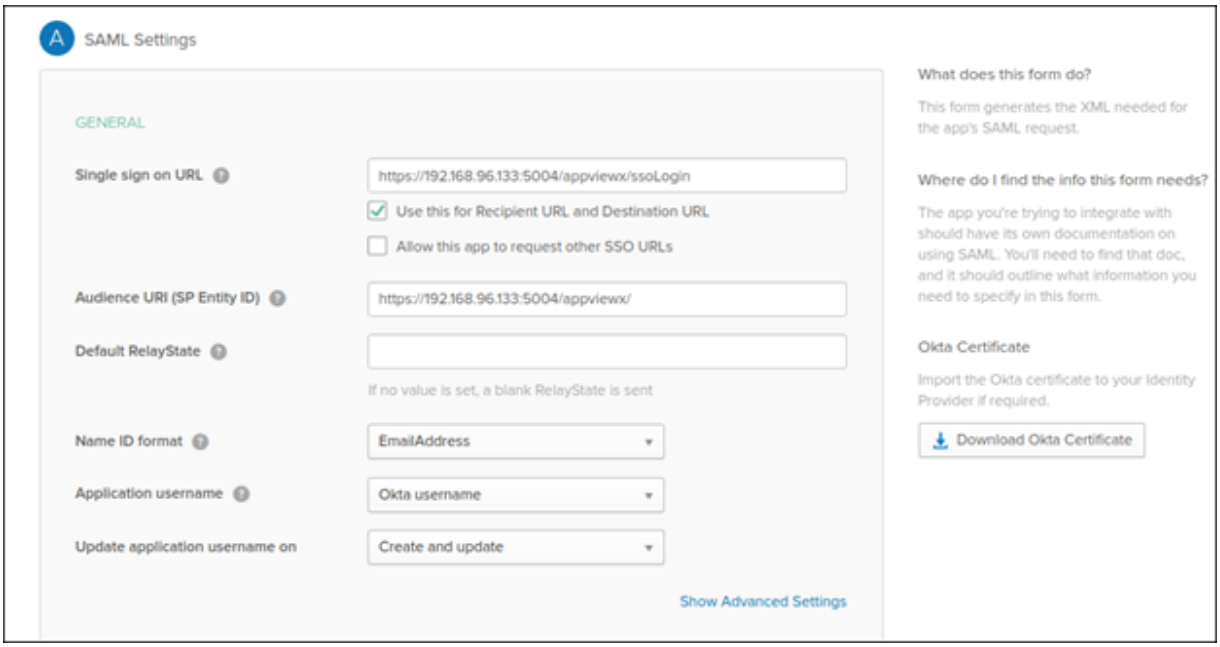
1. As an admin user or a user with the privilege to create an application, log in to the IDP and start creating the application.
2. Enter the basic details, name of the application, and logo update, if required.
3. Enter the configuration information of the service provider retrieved in the previous steps.
4. Enter the user attributes to be passed to AppViewX during the SAML assertion.
5. Download or copy the IDP metadata.
6. Map the Application to a user group or the user to the application.

Steps to add an application in OKTA:

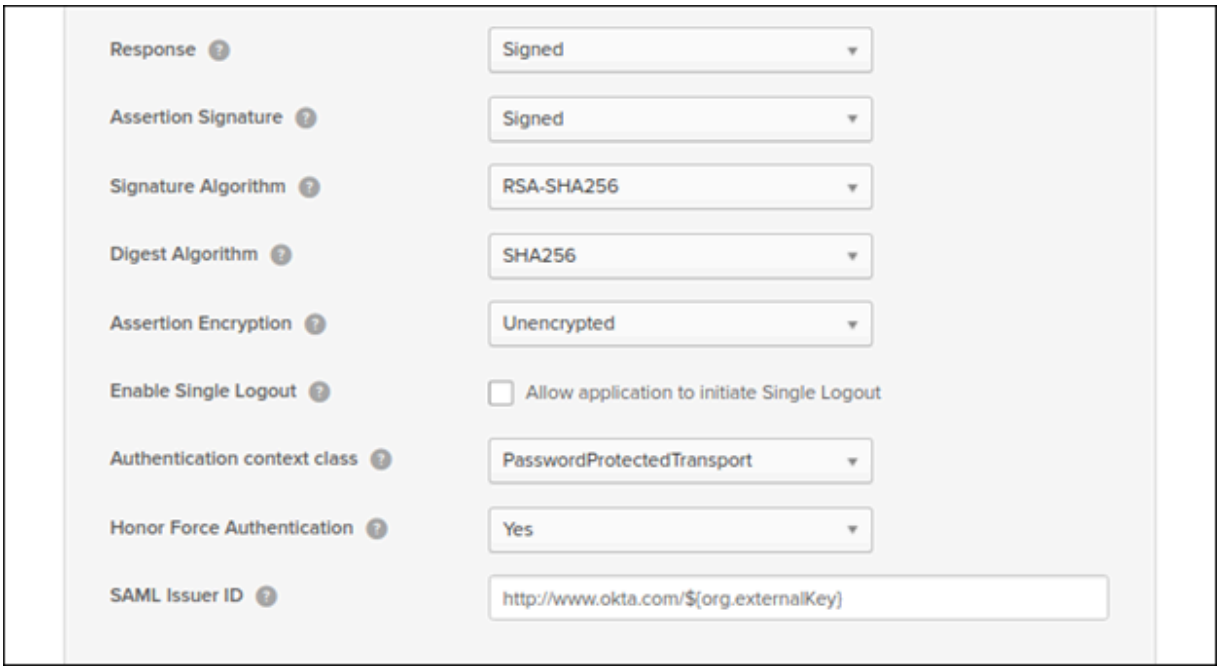
1. Create an application.



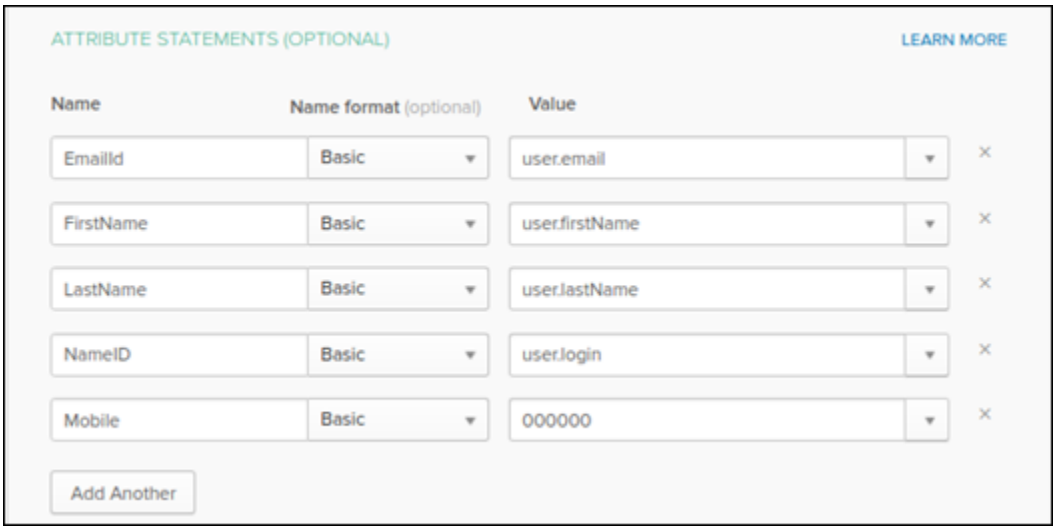
2. Configure service provider details.



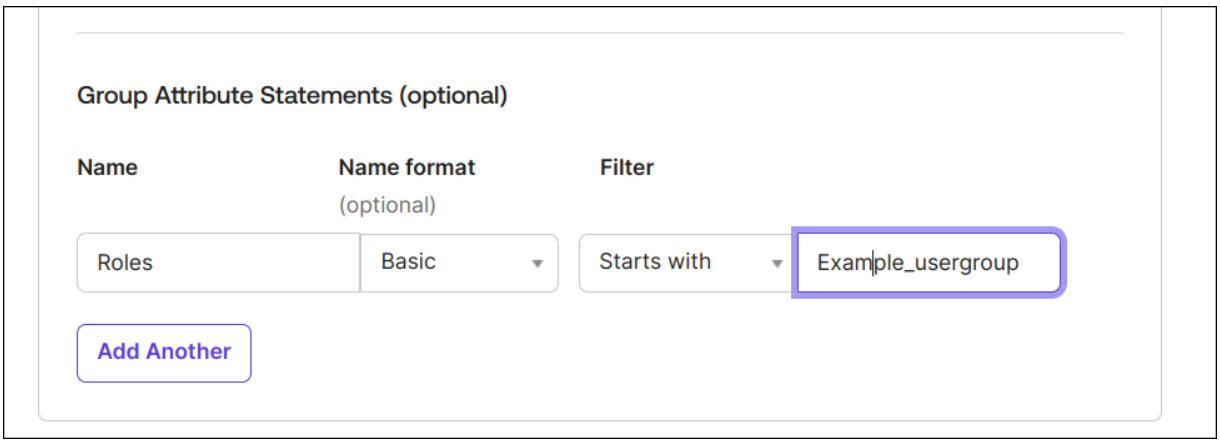
3. Show Advanced Settings screen.



4. Configure the User Attributes to be passed during the SAML assertion.

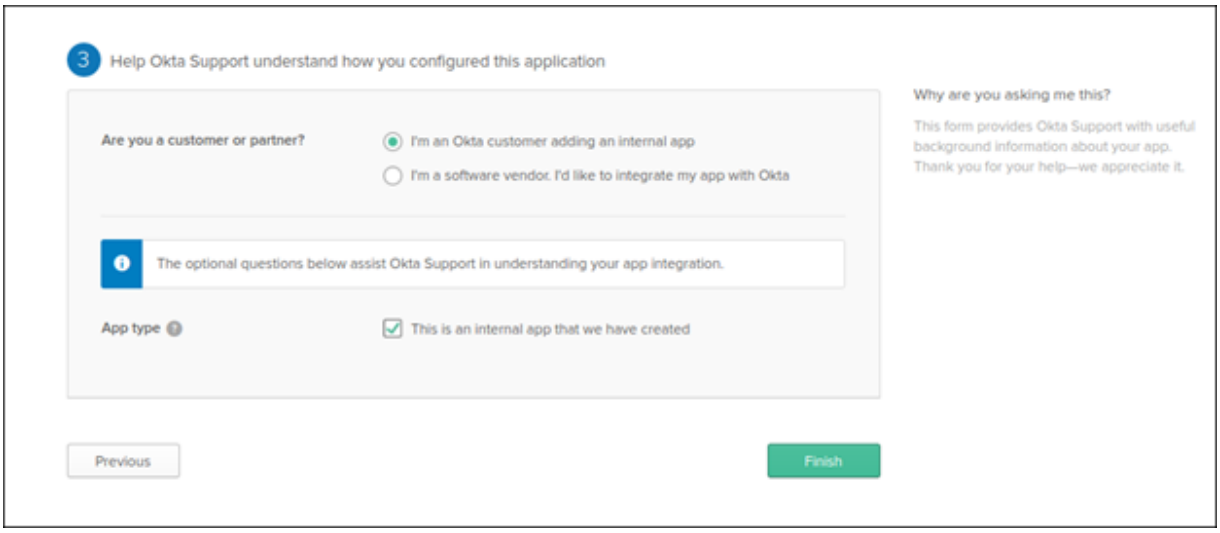


5. Create a user group within AppViewX using the identical group name as in OKTA. To access the instructions for creating a user group, click here.
6. Configure the User Group Attributes to be passed during the SAML assertion.

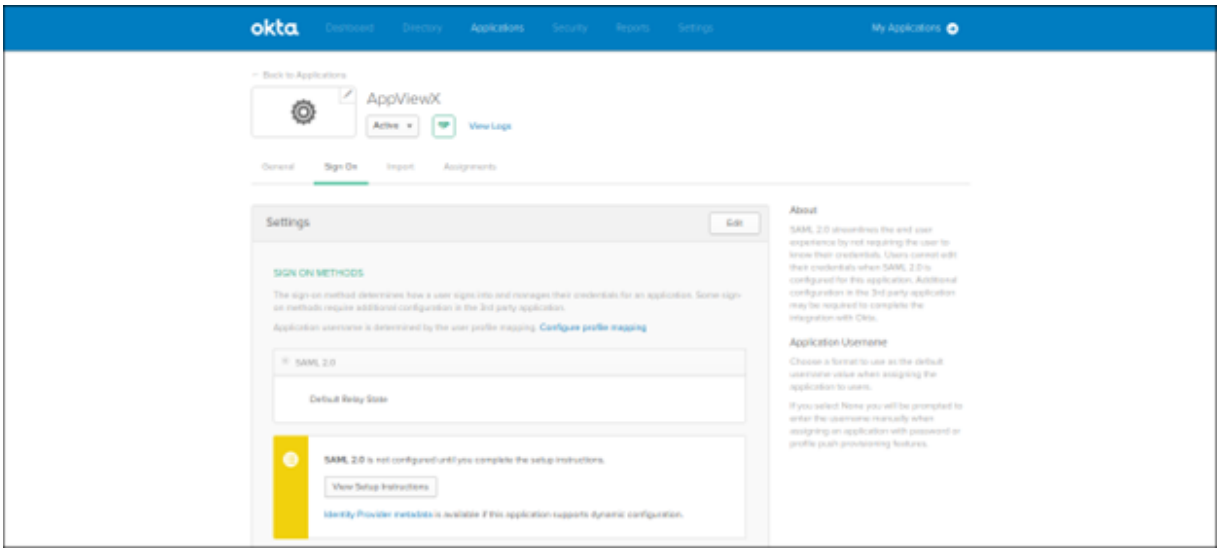


Choose Filter based on the requirement.

7. Finish the IDP configuration.

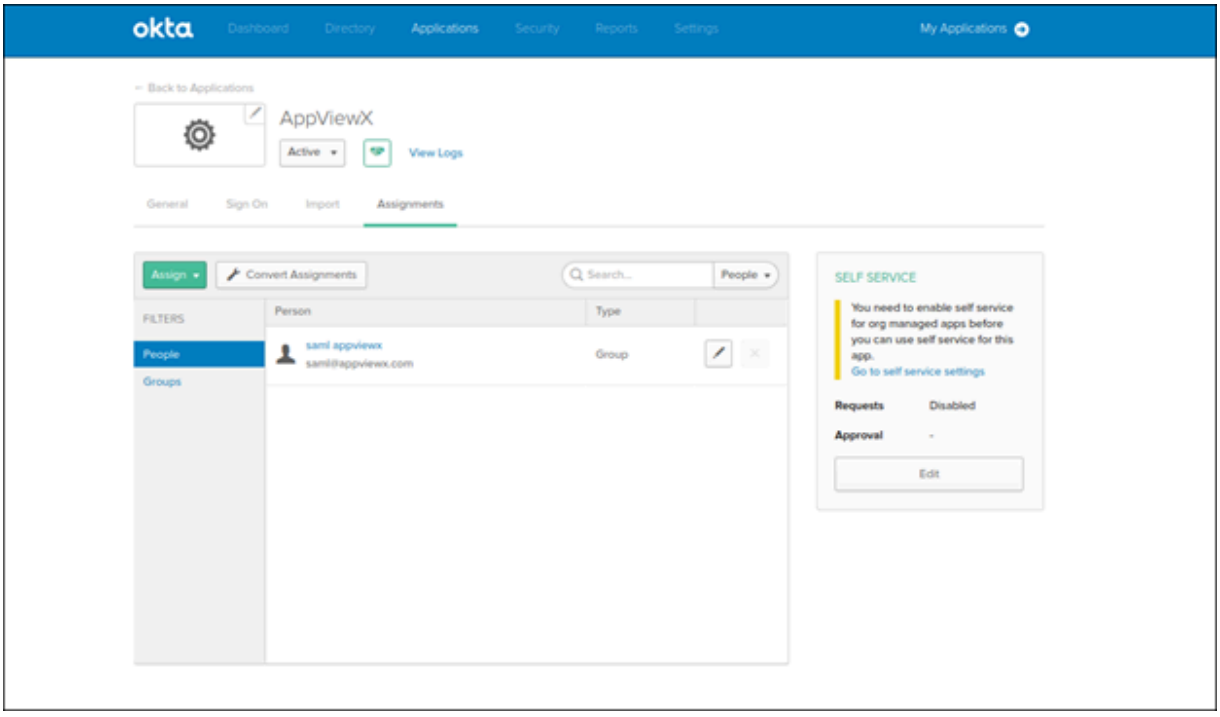


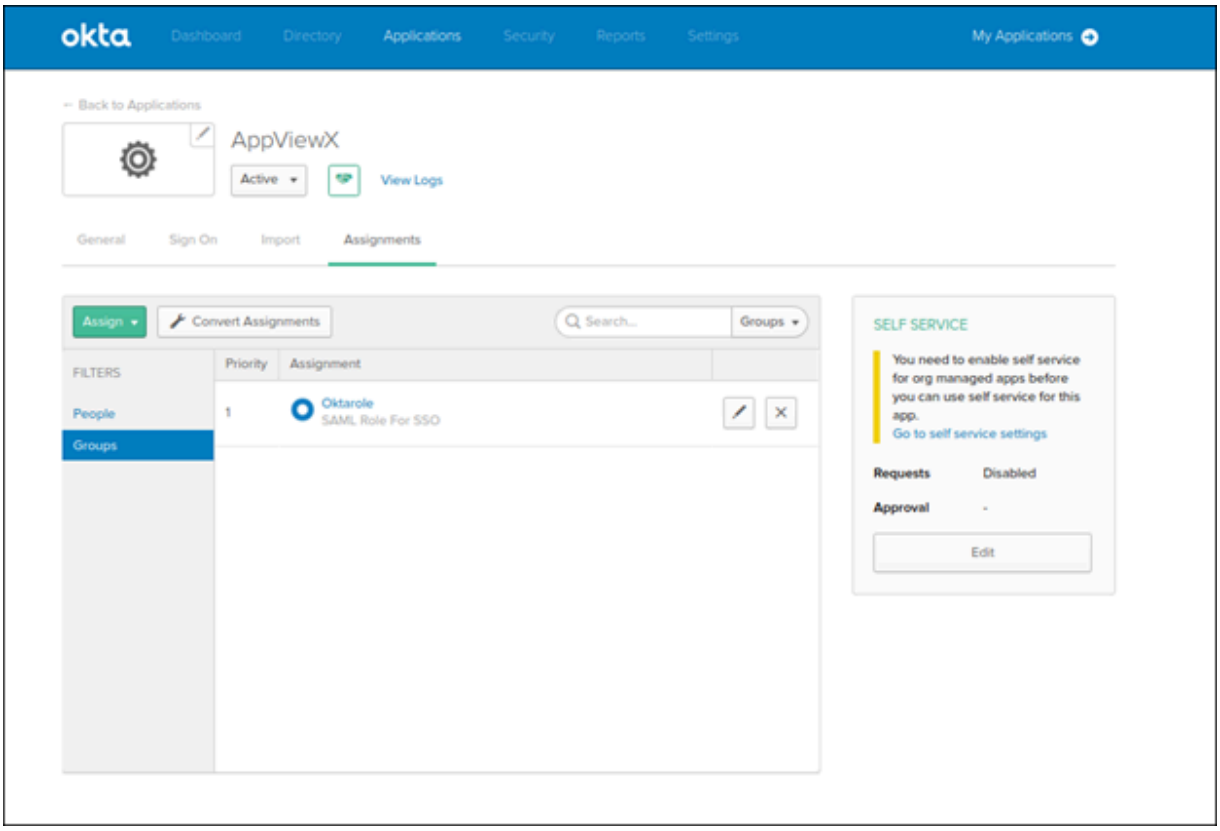
8. Click the View Setup Instructions in the Sign On tab.



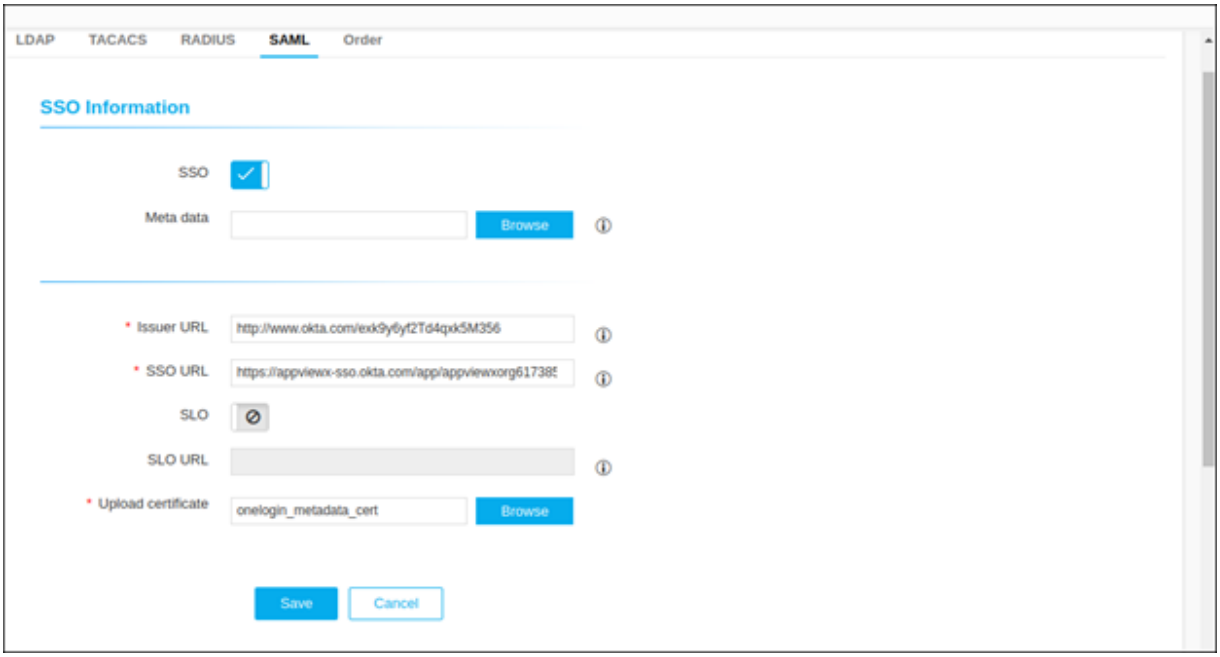
9. Copy and paste the content from the Optional section and save it as an XML file.

10. Map the application to a User or User Group.





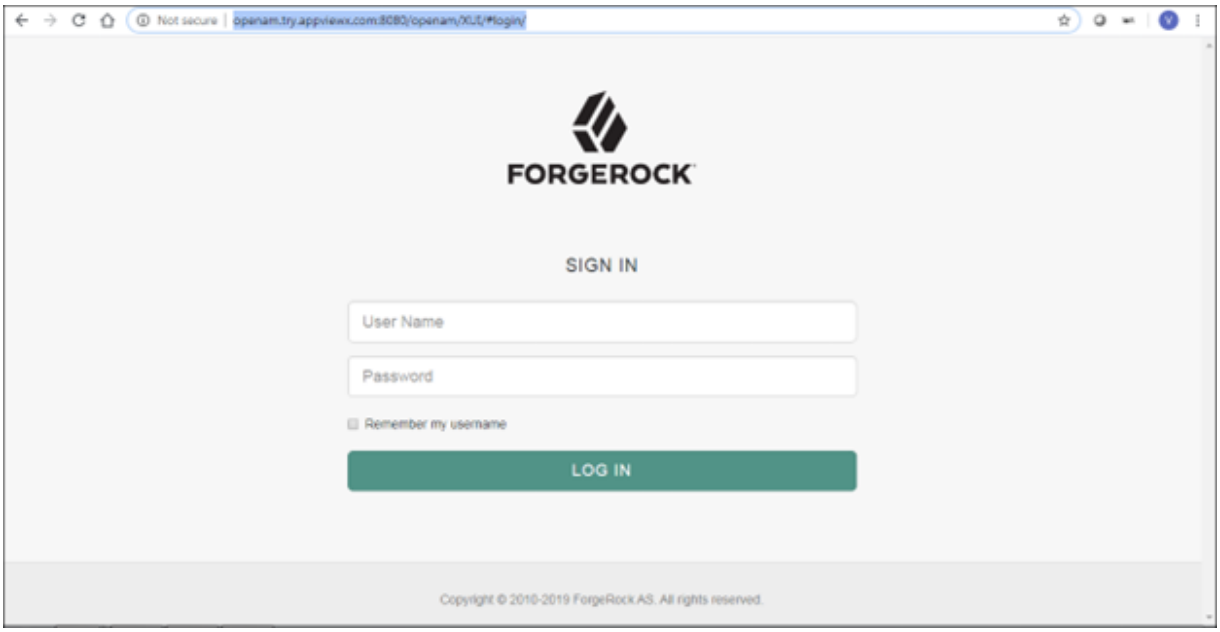
11. Browse and upload the IDP metadata to AppViewX.



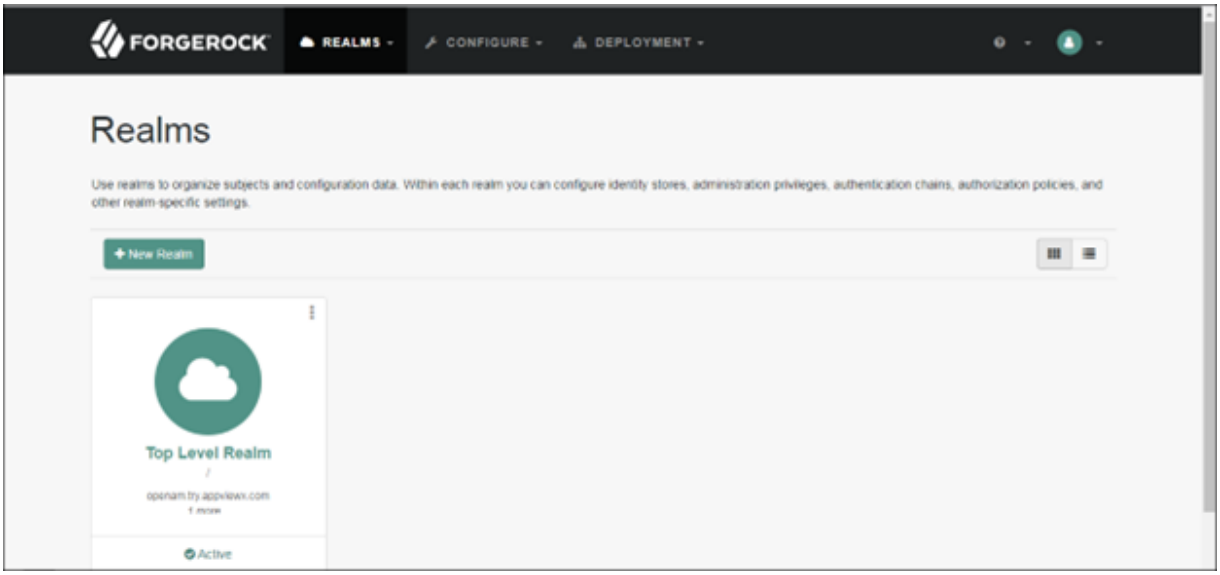
12. Click **Save**.

ForgeRock Integration

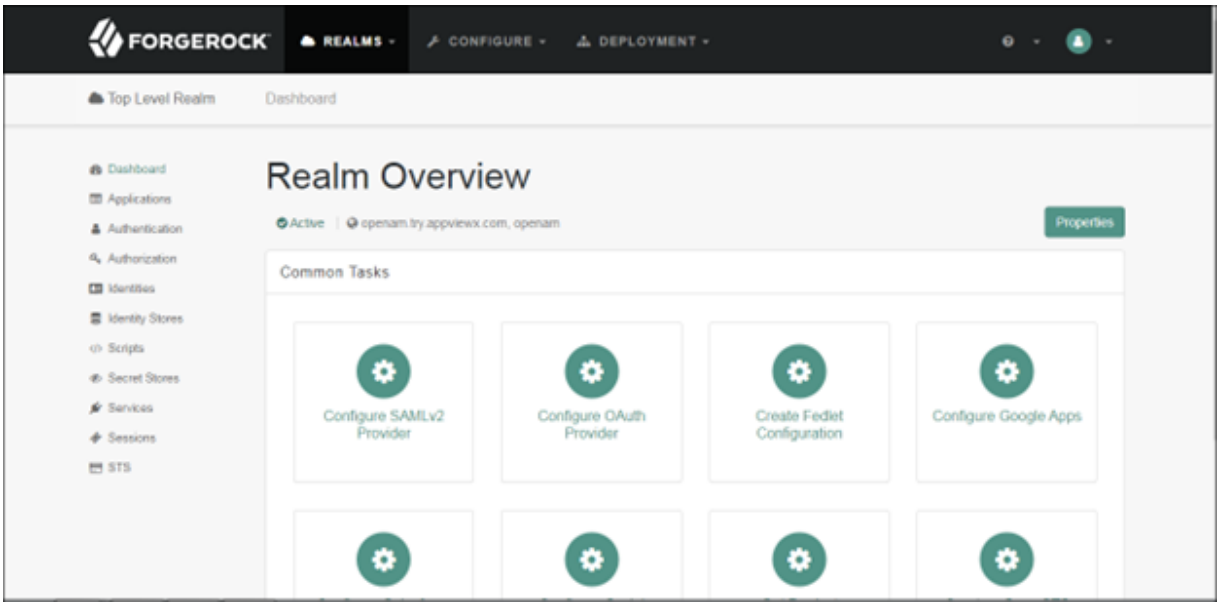
1. Login to the ForgeRock IDP Intense or Console.



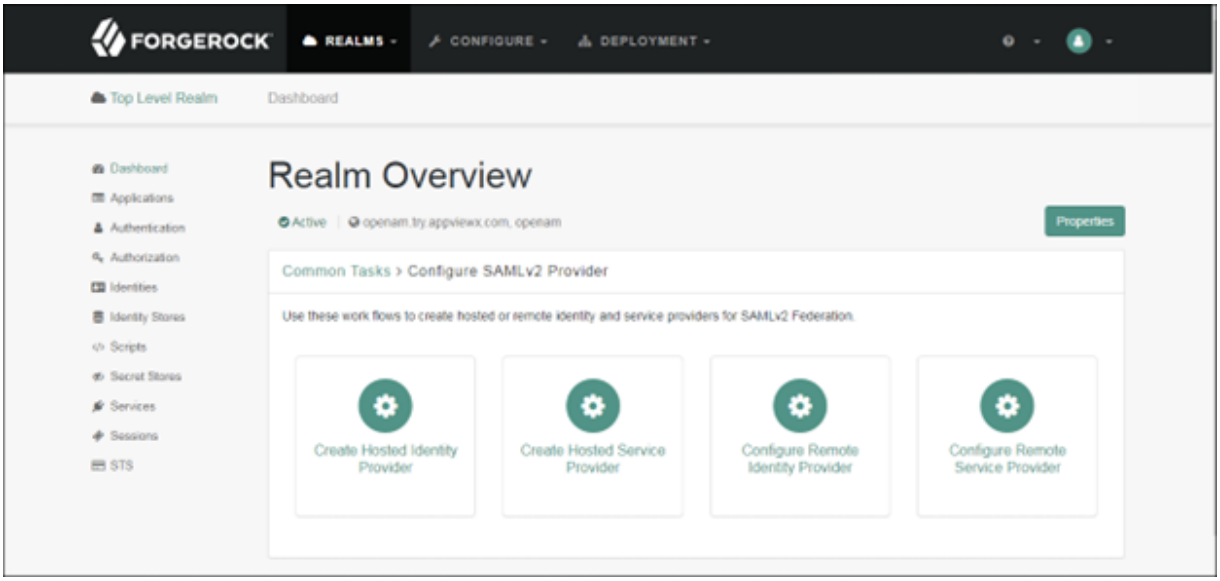
2. Select the respective Realm.



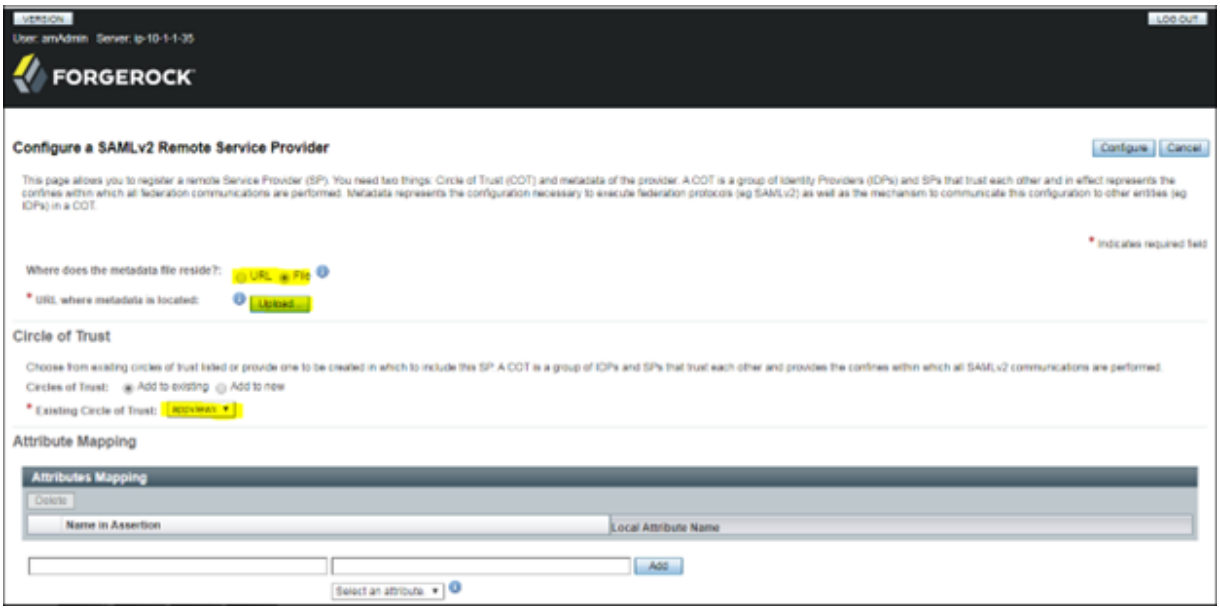
3. Under **Common Tasks**, select **Configure SAML v2 provider**.



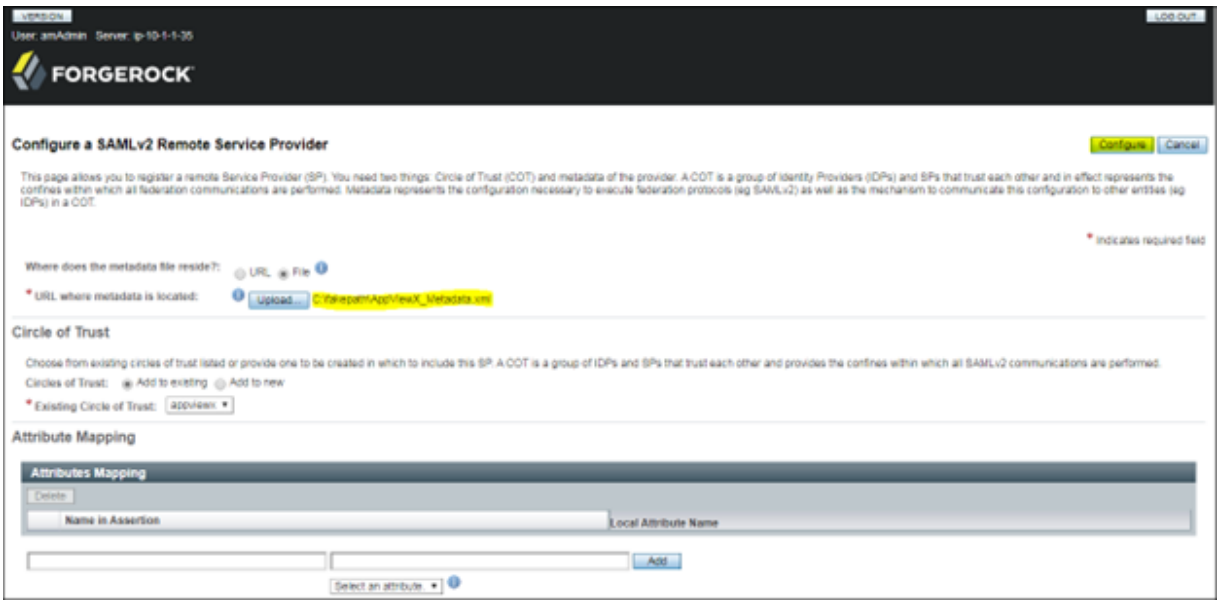
4. For Configuring AppViewX configuration, select **Configure Remote Service Provider**.



5. For metadata upload, select the **File** option.
6. Select or Create the circle of trust for mapping AppViewX to the IDP and then click **Upload**.

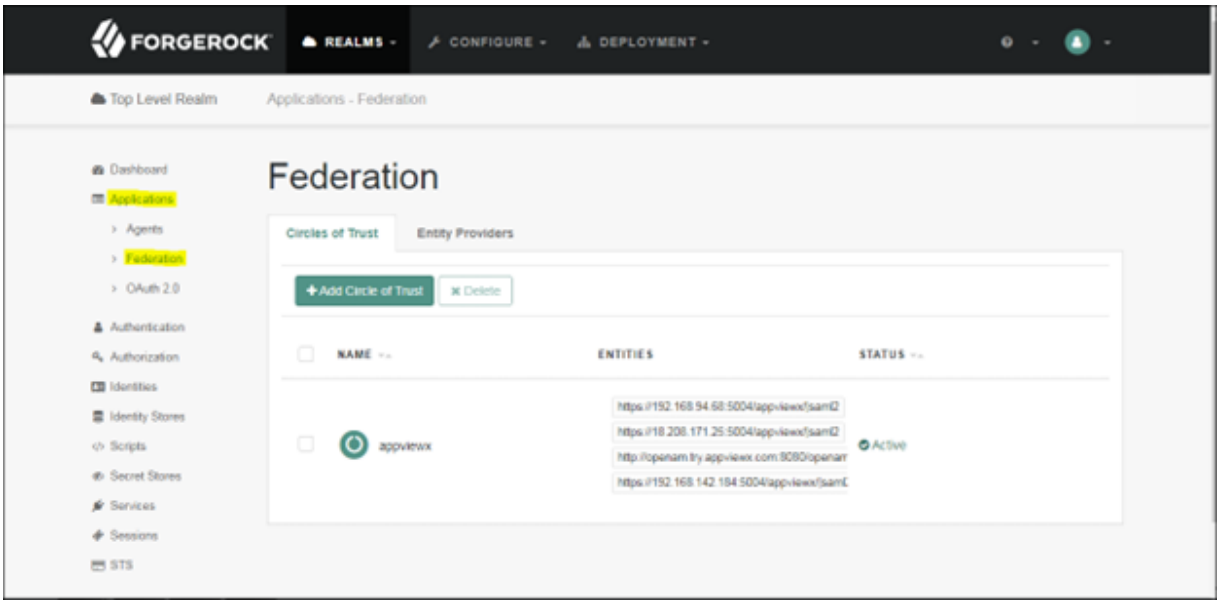


7. Upload the AppViewX metadata, which was downloaded earlier and click **Configure** to save the settings.

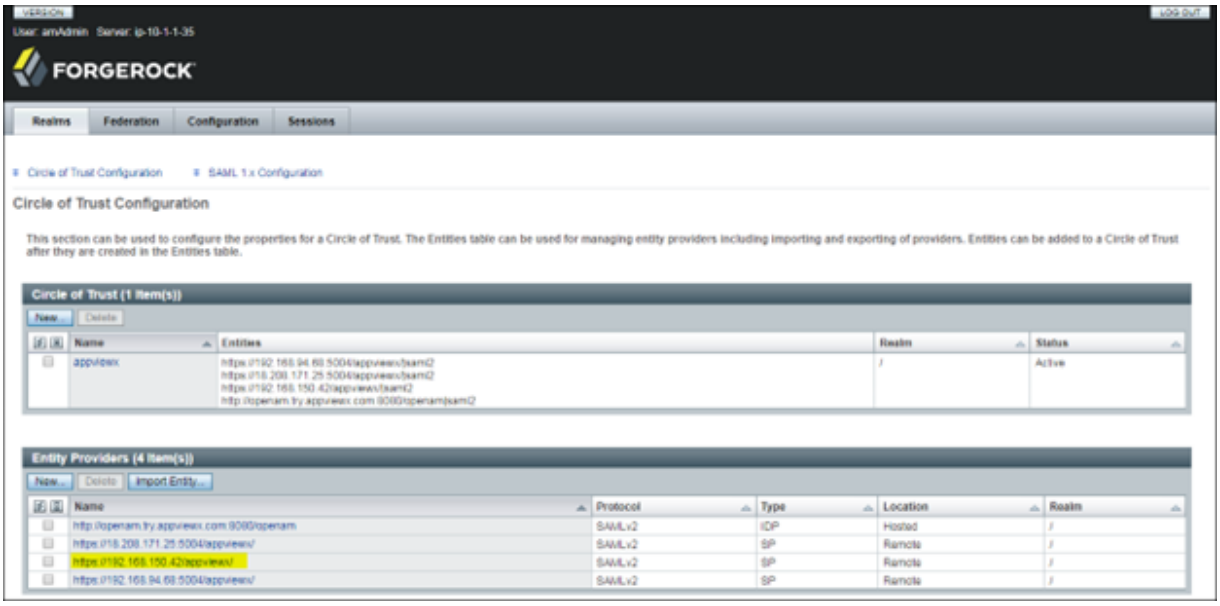


The page will redirect to the common tasks under the specific realm.

8. Access **Applications** > **Federation** from the left navigation pane.

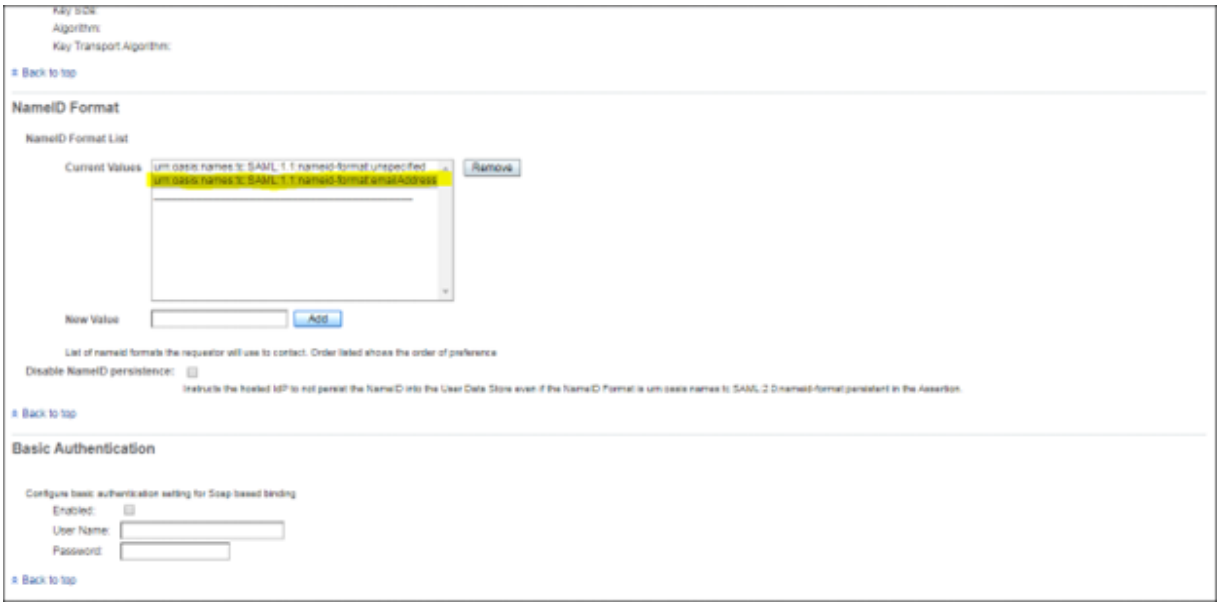


9. Select the entity providers tab.

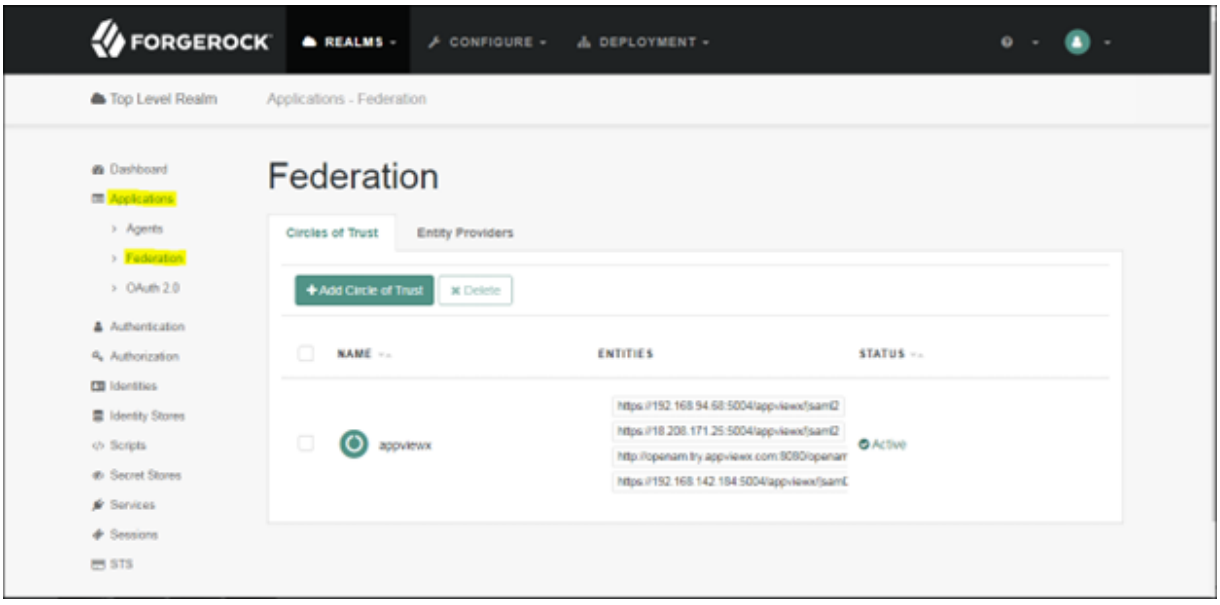


This action redirects to the **Federation** tab, displaying the service providers list and IDP configuration.

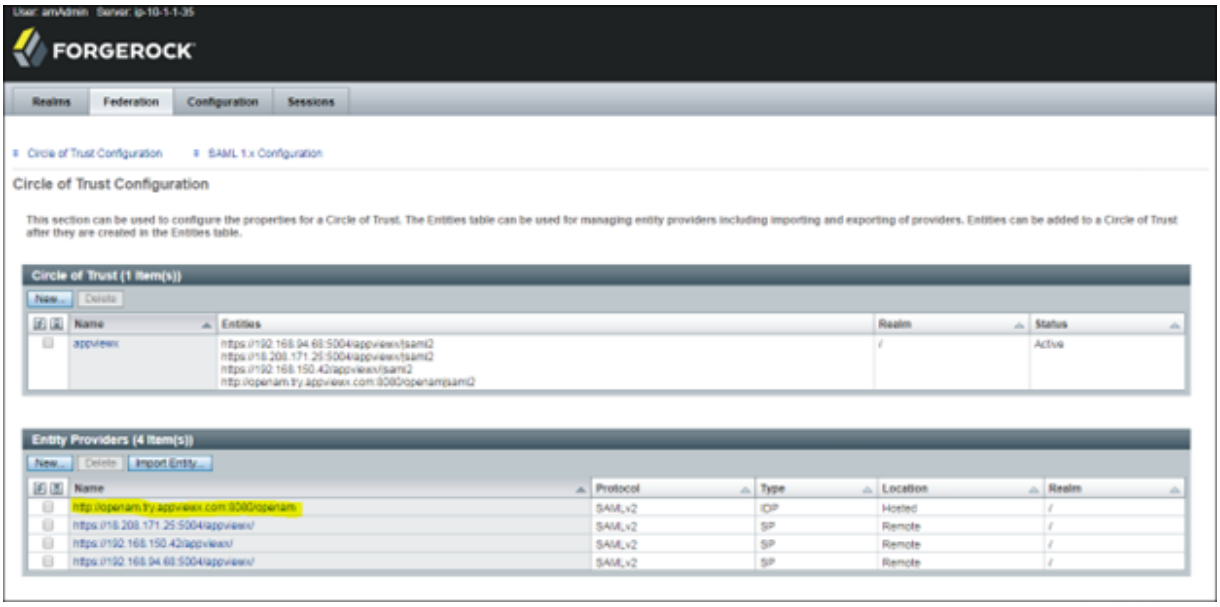
10. Select the respective Entity ID to navigate to the settings of the respective entity configuration.
11. On the **Assertion Content** tab, add the following in the **NameID Format** and then click **Save**.
    urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress



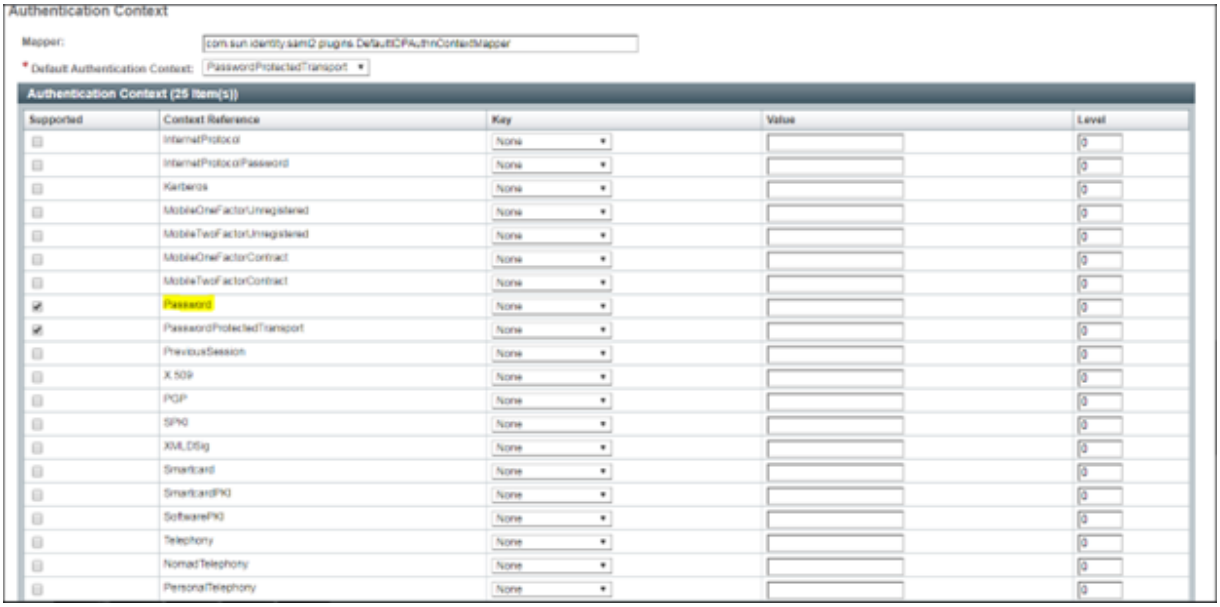
12. On the **Assertion Processing** tab, add the below assertion parameter that has to be passed as part of the SAML assertion and then click **Save**.
    EmailId=mail ; FirstName=cn ; LastName=sn ; NameID=mail ; Roles=isMemberOfAuthentication.
13. Modify IDP configuration to accept a password-based Authentication Context.
14. Navigate to **Applications** > **Federation**, and then select **Entity Providers** tab.



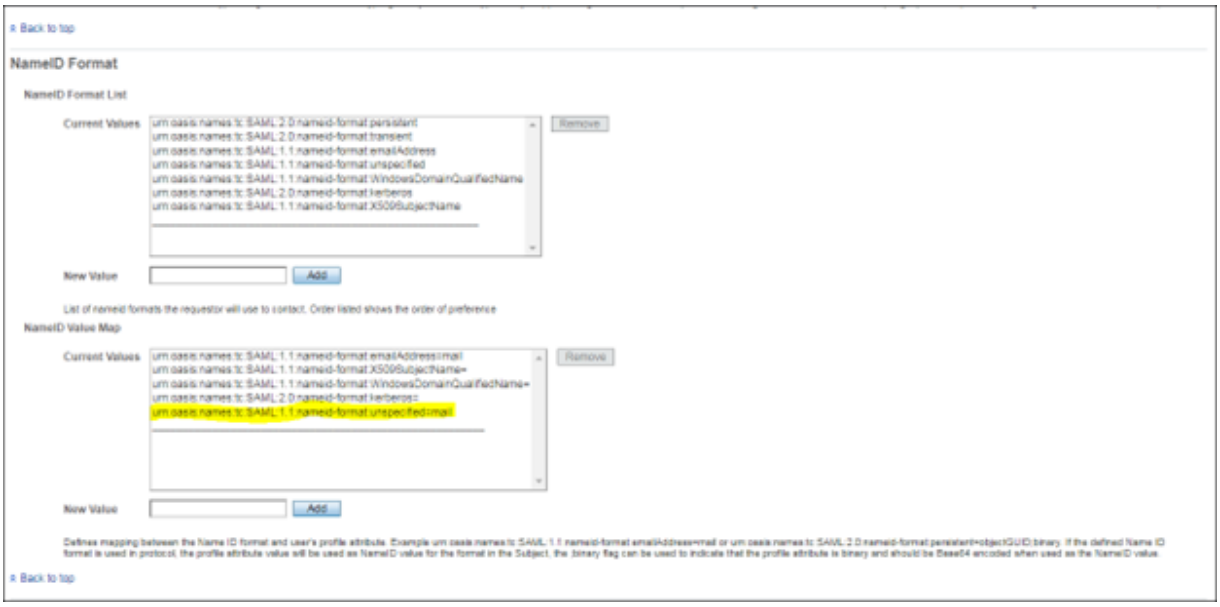
15. Under the **Federation** tab, select the IDP config under **Entity Providers**.



16. Under the **Authentication Context** section, check the password based context.



17. Above the Context, add the **NameID Value Map** and **Save** the settings.
    urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified=mail.



18. Access AppViewX with the SSO authentication and ForgeRock.
19. Export IDP metadata and upload it in AppViewX SSO settings.
20. To export metadata using the IDP URL and save it as an XML file. **Sample URL:**http://openam.try.appviewx.com:8080/openam/saml2/jsp/exportmetadata.jsp?entityid=http://openam.try.appviewx.com:8080/openam
21. Role name passed in as a part of the SAML assertion should be configured in appviewx on the **Accounts > UserGroup** and assign a role for accessing the application.

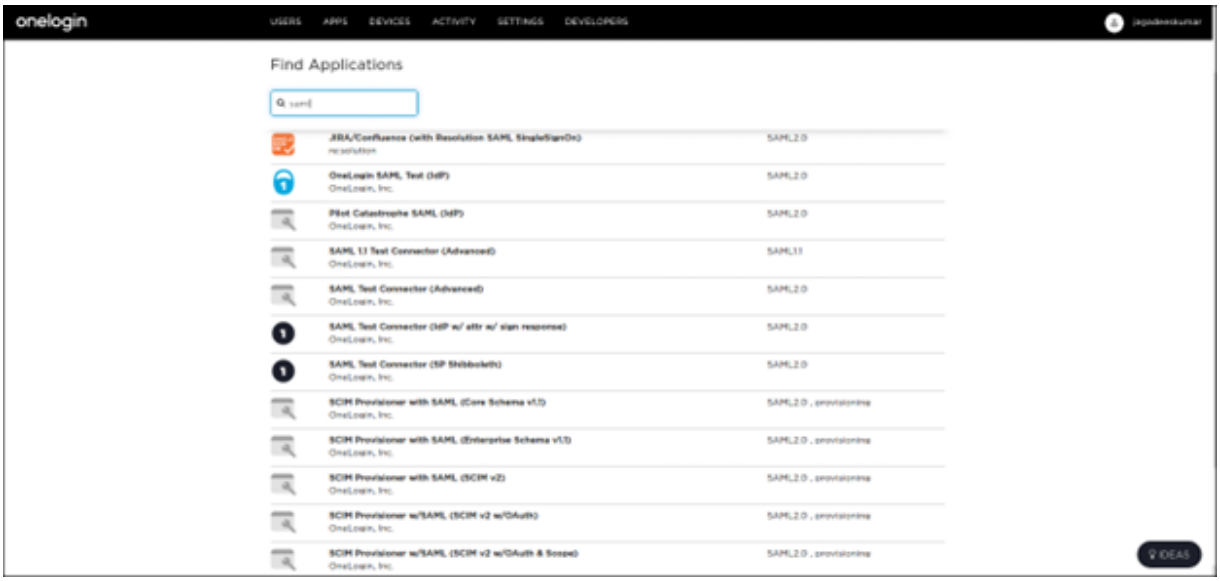
> **Note:** For an IDP initiated SSO the following structure like URL should be used. **Sample IDP initiated URL:** http://openam.try.appviewx.com:8080/openam/idpssoinit?metaAlias=/idp&spEntityID=https://192.168.x.x:31443/appviewx/

OneLogin Integration

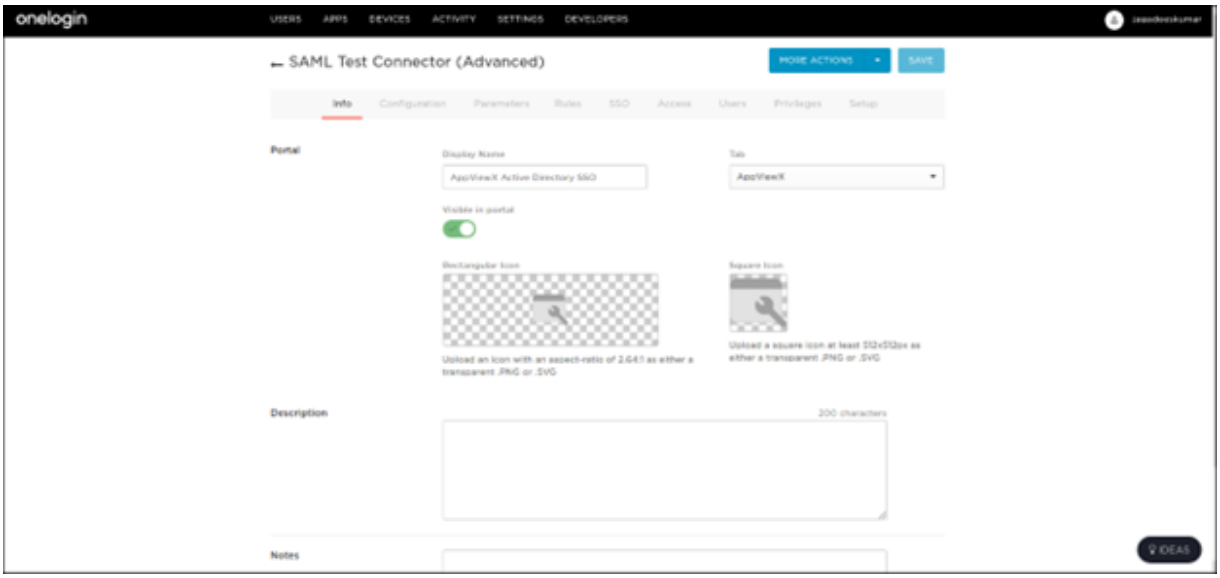
The below steps are performed at the IdP end. The navigation and screenshots might differ based on the version of the IdP.

The following are the steps to configure AppViewX SAML attributes in OneLogin.

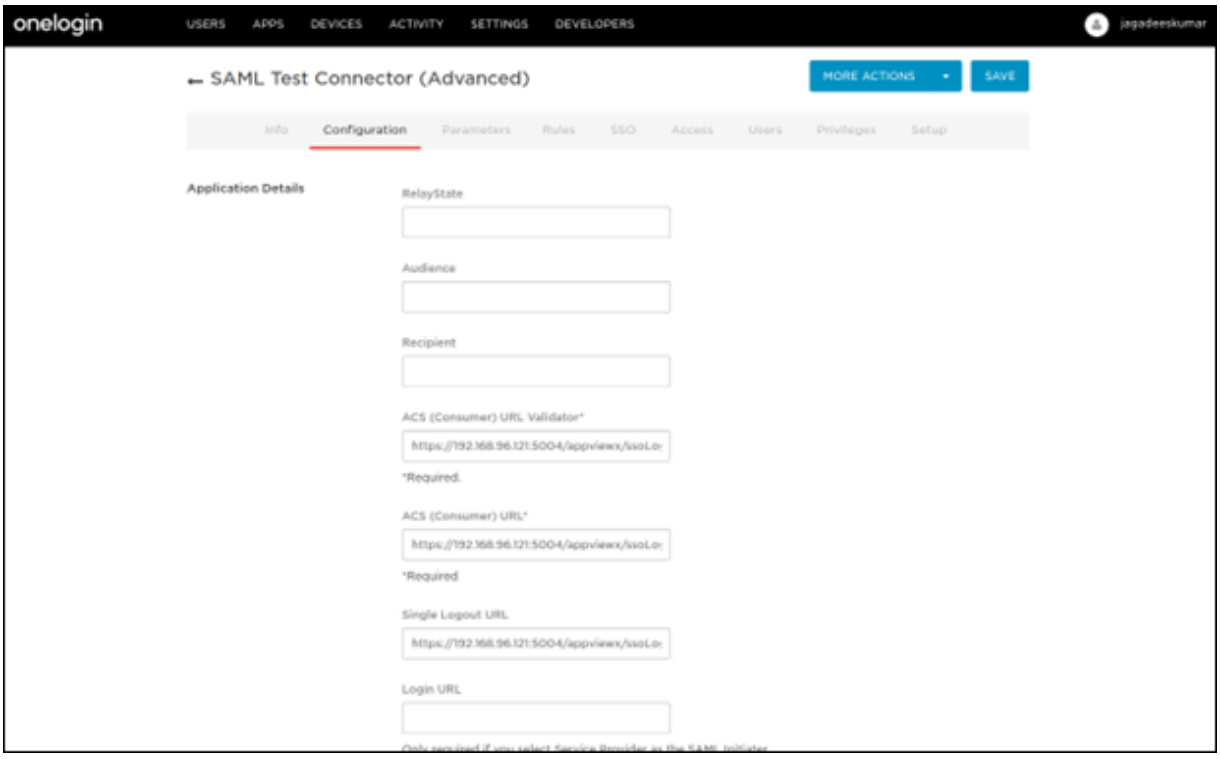
1. Create a new application.
2. Click Add application and search for SAML Test Connector.



3. Provide the application name and application details of AppViewX on the information page.

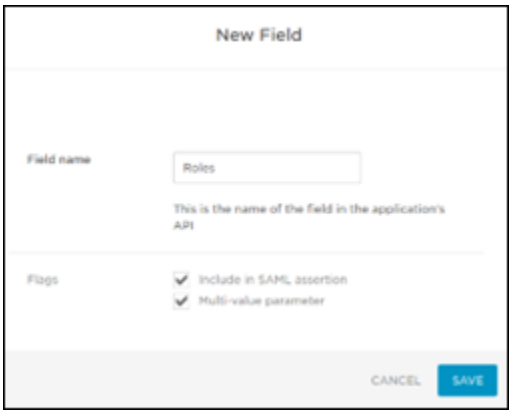


4. **AppViewX SAML attributes:** On the Configuration tab, provide the ACS consumer URL, single login URL, and single logout URL. This can be fetched by navigating to **AppViewX > Settings > General > Authentication > SAML > Enable SSO > Service URL** from the configuration found at the end of the page and specify the remaining settings to default.



5. **Parameters to be sent to AppViewX:** The following parameters are samples that have been sent to AppViewX.
6. Create a parameter called FirstName, which sends the user's first name to AppViewX in the SAML Assertion.

   Include the flag in SAML Assertion for all the added parameters.
7. **Sending User Groups to AppViewX:** To send User Groups to AppViewX from OneLogin via SAML Assertion, perform the following configuration:



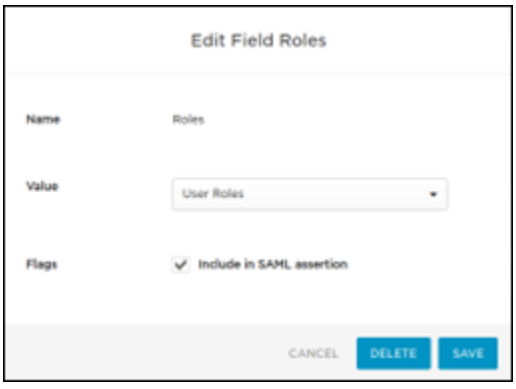
a. Integrate OneLogin with Active Directory.

b. Set the field name as **Roles**.

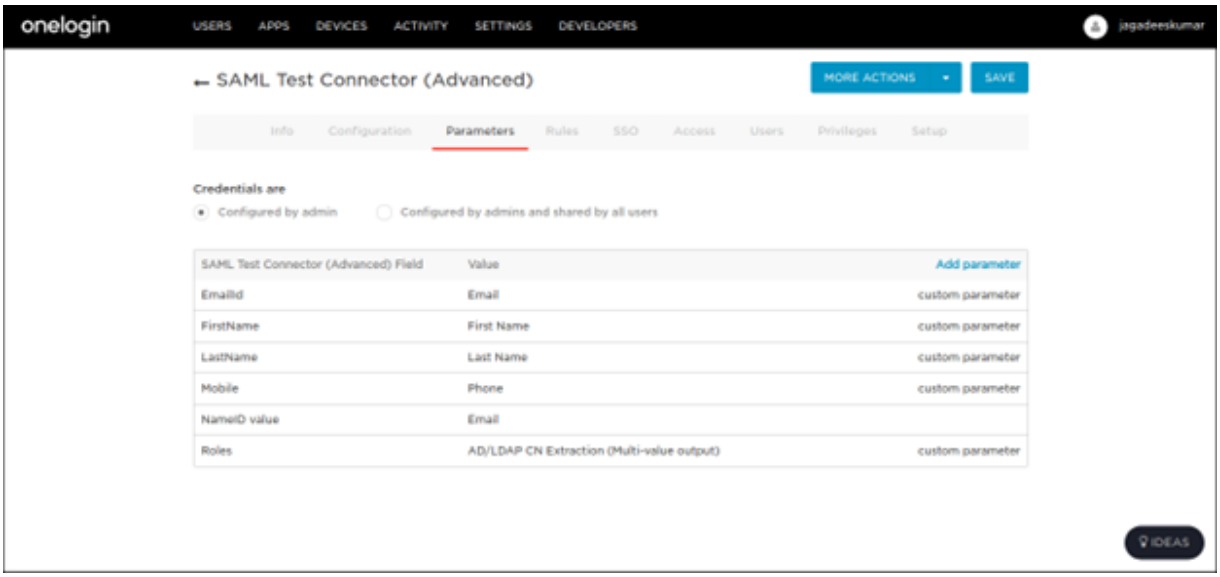
c. Enable the Flags for SAML assertion along with the multi-value parameter.

8. To utilize the user's **MemberOf** attribute as a role, enter the field name as **MemberOf** and select the **AD/LDAP CN Extraction**.

OneLogin without AD integration: Pass the roles field with user roles as value.



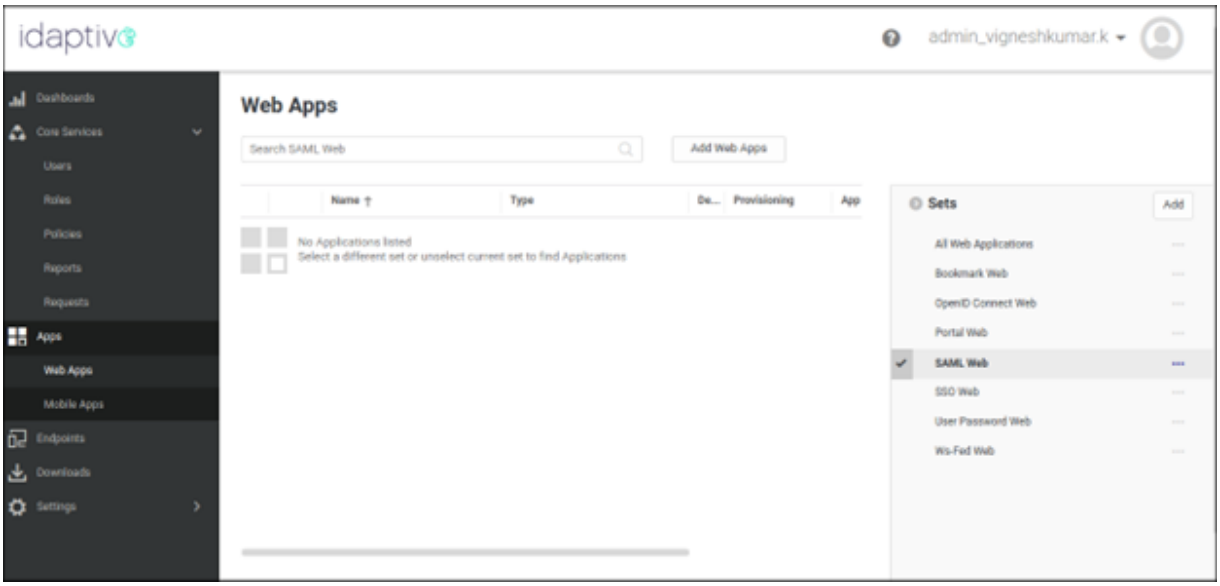
9. The following parameters have to be passed to AppViewX through the SAML assertion.



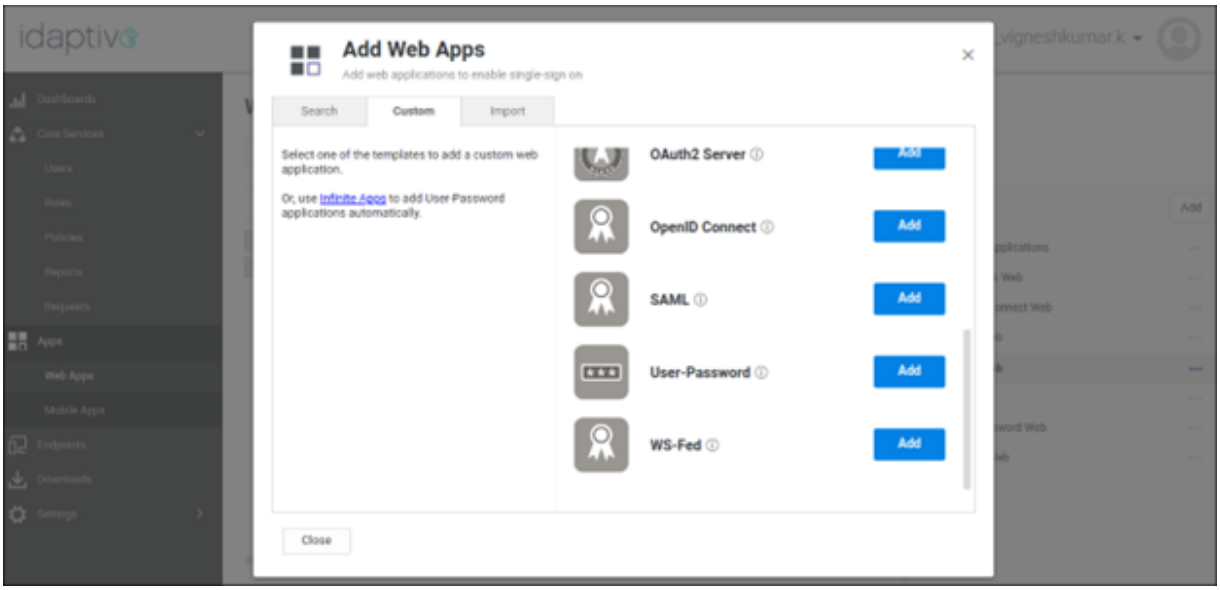
10. Assign application to User and Role.
    a. Download the federation metadata and click **Save**.
    b. Create the **UserGroup** within the roles in the administration section.
    c. Assign the created application to the user group.
    d. Sync users will subsequently be added to this user group.

Idaptive Integration

1. Login to the Idaptive SSO platform.
2. Navigate to **Apps** > **WebApps** > **Select SAML Web**.
3. Select **SAML Web**.

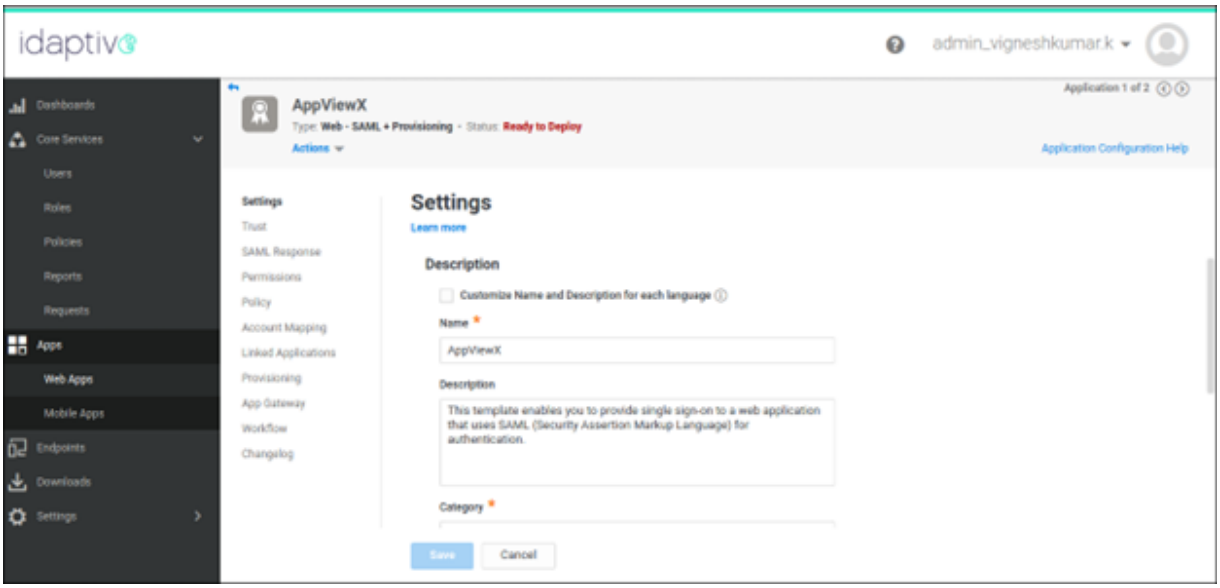


4. Click **Add Web Apps**.
5. In the **Add Web Apps** window, under the **Custom** tab, click **Add** for **SAML**.

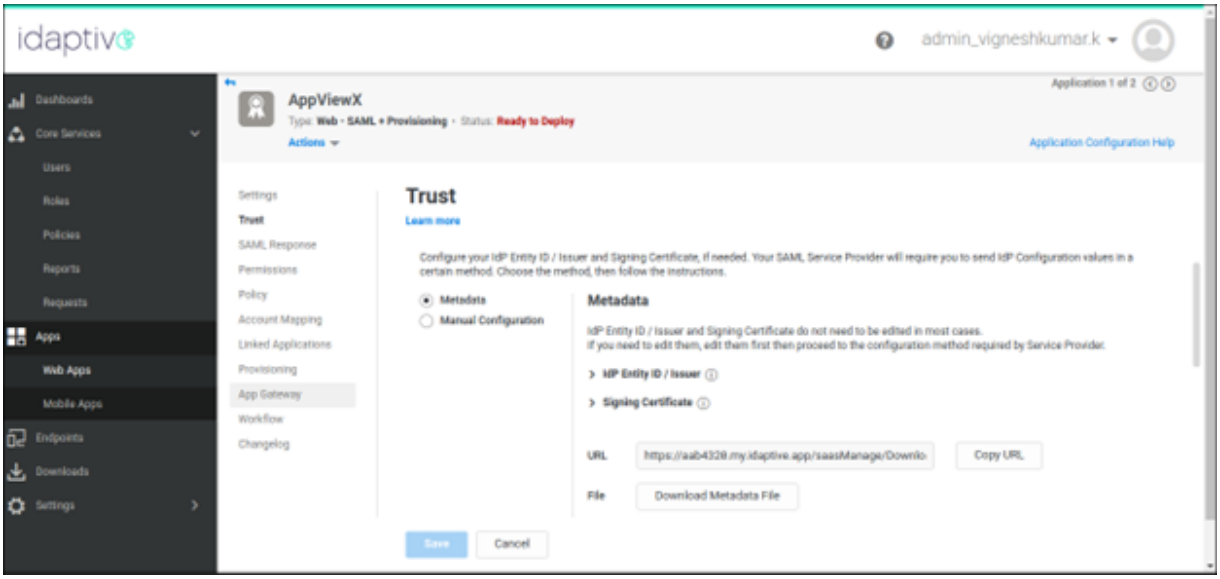


SAML app is added to the Web Apps Inventory.

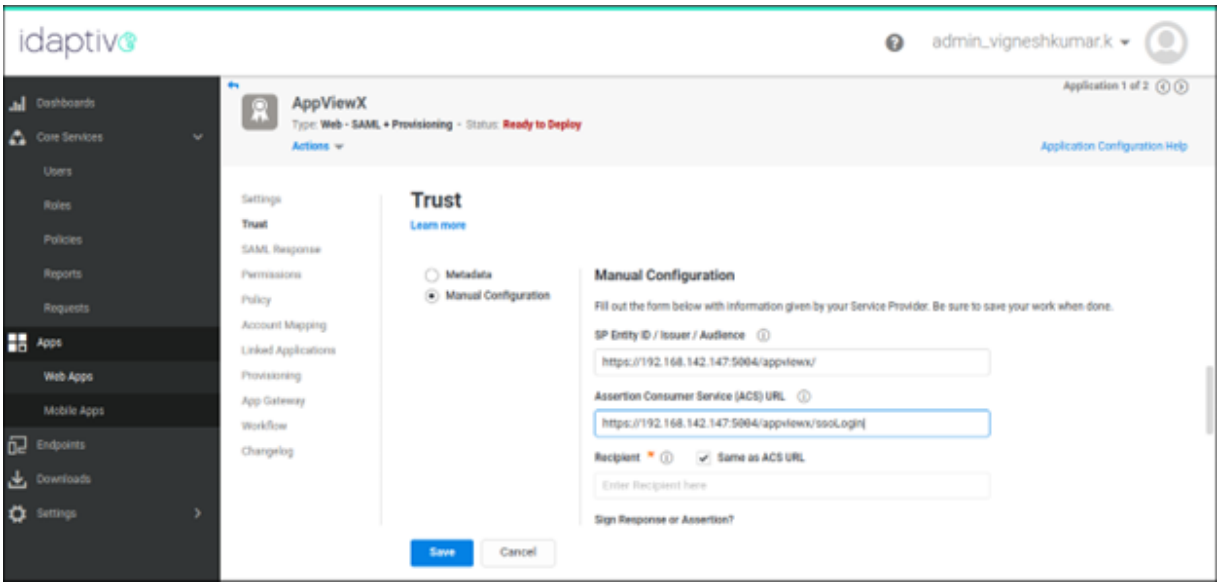
6. Select the SAML app in the Web Apps Inventory and proceed with the configuration.
7. In the **Settings** tab, enter **AppViewX** as the app name and save the configuration.



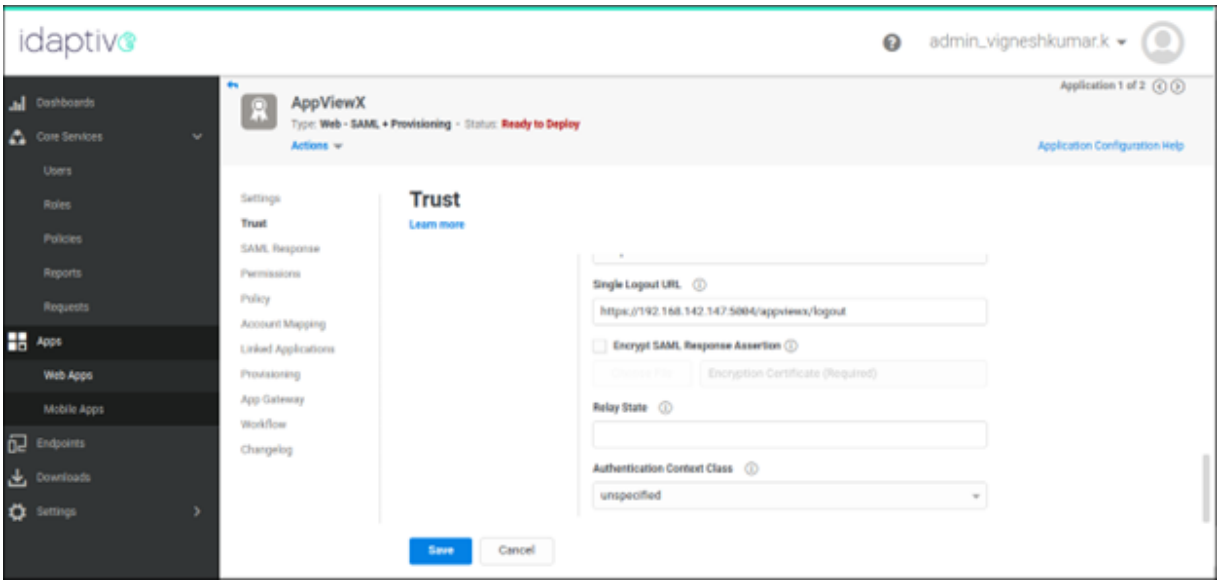
8. In the **Trust** tab, click **Download Metadata File**.



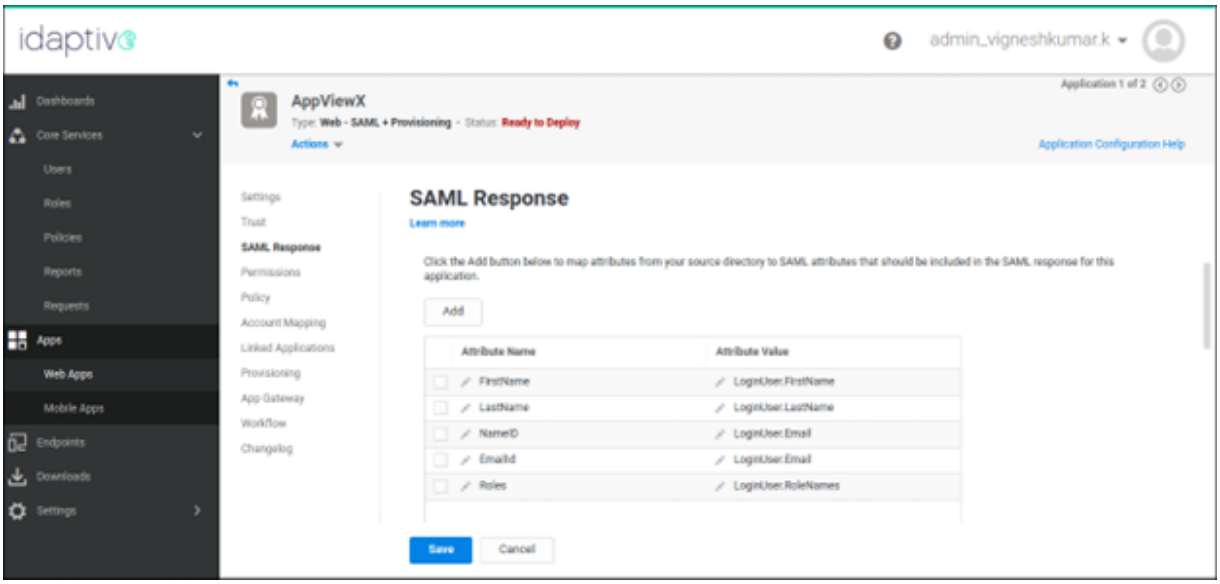
9. Select the **Manual Configuration** option.
10. Copy the **Entity ID URL** from AppViewX and paste it into the **SP Entity ID** field within the Idaptive portal. Similarly, copy the **Service URL** from AppViewX and paste it into the **ACS URL** field in the Idaptive portal.



11. Verify whether the Recipient checkbox matches the ACS URL. Retain the default settings for the remaining fields. Configure the Single Logout URL field with the copied value from the SLO URL in AppViewX. Finally, **Save** the configuration.



12. In the **SAML response** tab, add the below assertion attributes with the same format. FirstName > LoginUser.FirstName, LastName > LoginUser.LastName, NameID > LoginUser.Email, EmailId > LoginUser.Email, Roles > LoginUser.RoleNames (This should be the user associated User Groups or Security Groups).



13. Click **Save**.
14. Assign the application to the respective Role and the Role to the respective Users.
15. After configuration of role is done, proceed to set up the same role within AppViewX under the **Account > User Group** module. Assign the respective AppViewX role permissions to the User Group.
16. Access AppViewX with the help of External login using SAML.

OpenID Connect- Overview

OpenID Connect (OIDC) is an identity layer built on top of the OAuth protocol, which provides a modern and intuitive Single Sign-on (SSO) experience for you and your end-users. For example, administrators can configure Single Sign-on with a third-party identity provider that supports OpenID Connect. Users then have the option to log in to the application using their identity provider credentials.

- AppViewX Integration with OIDC Provider
- Login Workflow
- Steps to Integrate OIDC

Before you begin

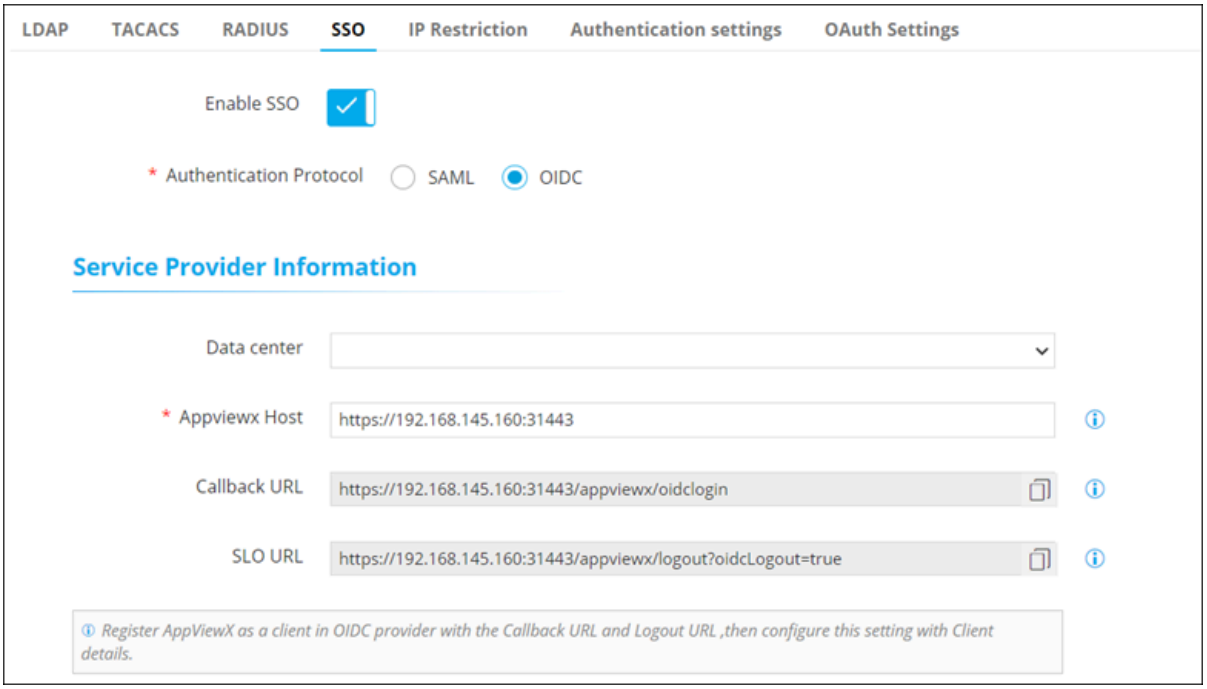
- Register AppViewX as an OIDC application with your Identity Provider (IdP) and note the Client ID, Client Secret, and Well-known configuration URL.
- The OIDC entity profile must be an authorization code grant type.
- Enable SSO with Authentication Protocol as OIDC in AppViewX.

- Role required: admin
- OIDC based SSO is supported from AppViewX release 21.1.X and above.

AppViewX Integration with OIDC Provider

To integrate AppViewX with OIDC provider, follow the below steps:

1. On the **Settings :: Authentication** page, under the **SSO** tab, turn on the **Enable SSO** toggle.
   The **Authentication Protocol** options are displayed.
2. Select **OIDC** as the **Authentication Protocol**.
   The **Service Provider Information** section will automatically populate based on the OIDC selection.
3. Copy the **Callback URL** and **SLO URL**, which has to be configured at the OIDC identity provider settings for AppViewX, from the **Service Provider Information** section.



4. Under the IDP Configuration section, enter the required field information.

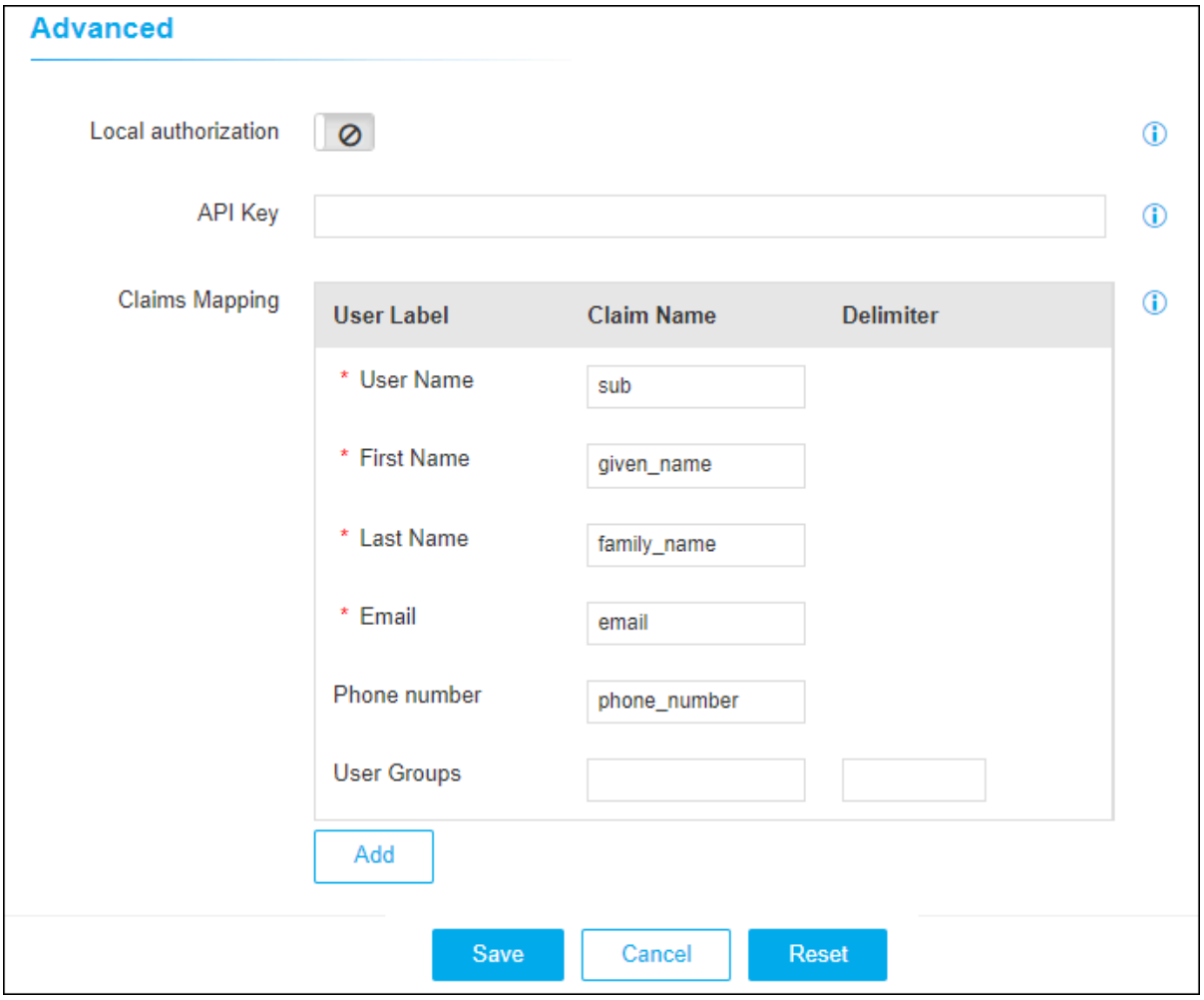
Field descriptions for IDP Configuration

Field	Description
***Client Name**	Unique name for the OIDC identity provider configuration.
***Client ID**	The client ID of the application that is registered in the third-party OIDC identity provider.

Field	Description
***Client Secret**	The client secret of the application that is registered in the third-party OIDC identity provider.
***Discovery Endpoint (Well known) URL**	The URL contains metadata about the third-party OIDC identity provider.

Note: The asterisk (*) symbol indicates mandatory fields.

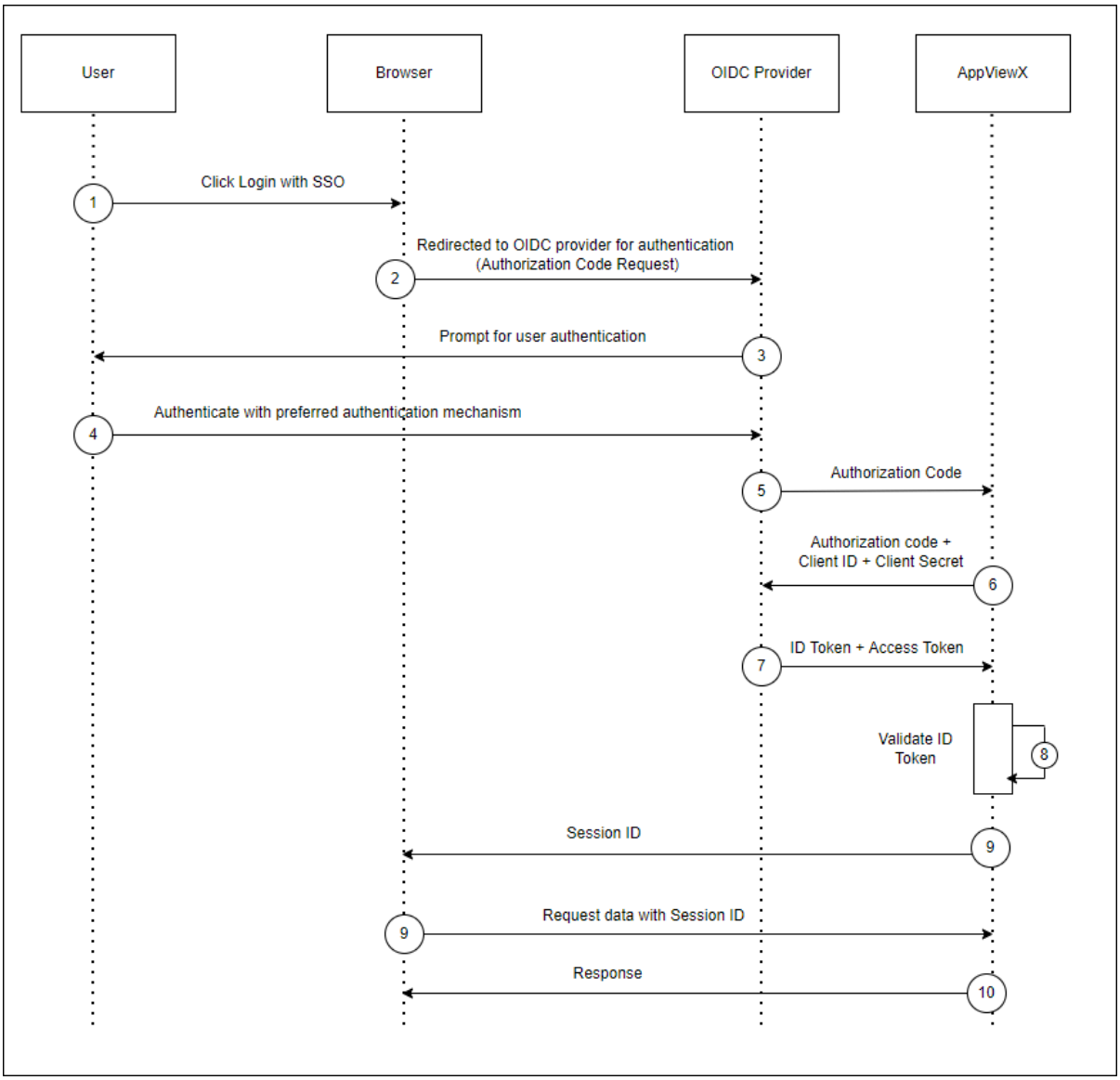
5. Under the **Advanced** section, turn the **Local Authorization** toggle on/off to define custom claim mapping based on the ID claims which are sent from the OIDC Identity provider.
   Turn the **Local Authorization** toggle **on** to define the following privileges:
   a. When a user from an OIDC provider tries to log in to AppViewX for the first time, the user account will be created under Account > User within AppViewX. But users will not be allowed to perform any operations until Admin assigns the user to the respective User Group.
   b. To enable the user with a successful login, an User Group must be created as a prerequisite, and the User Group must be assigned with Roles and Resources permissions for the SSO users and has to be assigned within AppViewX by mapping the users to the User Group.
   Turn the **Local Authorization** toggle **off** to define the following privileges:
   a. When a user from an OIDC provider tries to log in to AppViewX, with Local Authorization disabled it is assumed that the Security Groups are passed as a part of the ID token.
   b. Create the required Security Group under the **Menu > Account > User Groups** within AppViewX by assigning respective Roles and Resources.
6. Under the **Advanced** section, enter the API Key if provided by the OIDC provider.
7. Navigate to **Advanced > Claims Mapping**, enter the required field information to map the claim keys against the AppViewX User Label for the user profile information to be stored in the AppViewX expected format.



For example:

- An identity provider can send the user login name with the key called sub in the ID token and another identity provider can send the user login name with the key called upn.
- The administrator can configure/modify the claim setting against the User Name either as sub or upn based on the ID claim response sent by the OIDC vendor.
- Similarly, custom claims can be configured and additional claims for the user profile if required. Currently, these custom claims stored in the user profile will not be shown along with the user profile on the AppViewX web application.

Login Workflow



1. When user tries to login with SSO in AppViewX, user will be redirected to the OIDC provider's login page.
2. The user can now use the preferred authentication mechanism to login to the OIDC. After successful authentication, OIDC provider will send Authorization code to AppViewX.
3. AppViewX will then send the Client ID and Client Secret along with that Authorization code to the OIDC provider.
4. OIDC provider validates the client credentials and authorization. On successful validation, it returns ID Token and Access Token to AppViewX.
5. AppViewX validates the ID Token and uses the user information received in ID token.

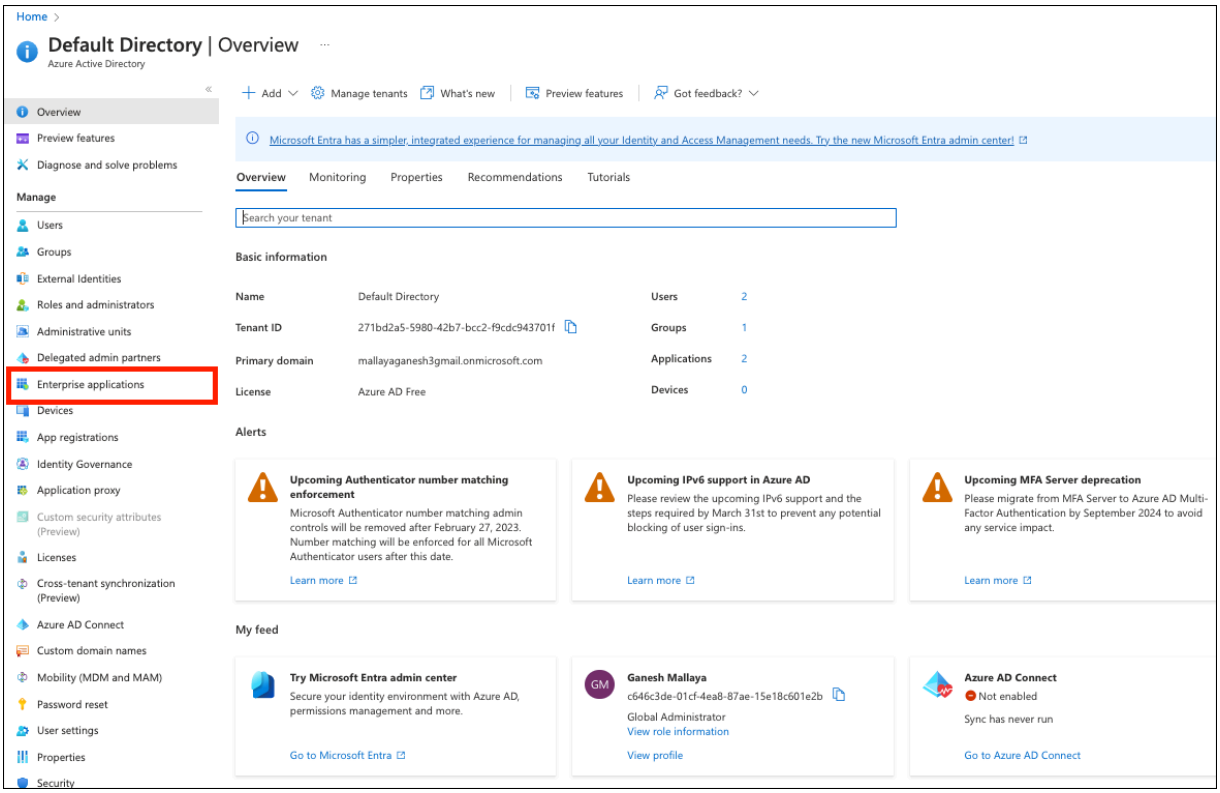
6. If a user tries to login for the first time, then that user account will be created in AppViewX using the details fetched from ID Token.
7. If Local Authorization is enabled, the admin must map the user to the respective user group to grant necessary permission and scope of management.
8. Upon completion of the user mapping, the user can access the AppViewX console. Any attempt to log in before this mapping results in an error.
9. If Local Authorization is disabled, then the authorization in AppViewX will be performed based on the groups the user exists in IDP.
10. AppViewX will compare the user group details available in the ID token with the existing user groups in AppViewX. If the same user groups exists in both, then the user will be assigned with permissions and the scope of those groups. Else, user will not have any permissions within AppViewX.

> **Note:** For Microsoft Azure, the token configuration should be configured with custom claims for sending user login name with the claim as upn and a group claim to send security groups as User Group.

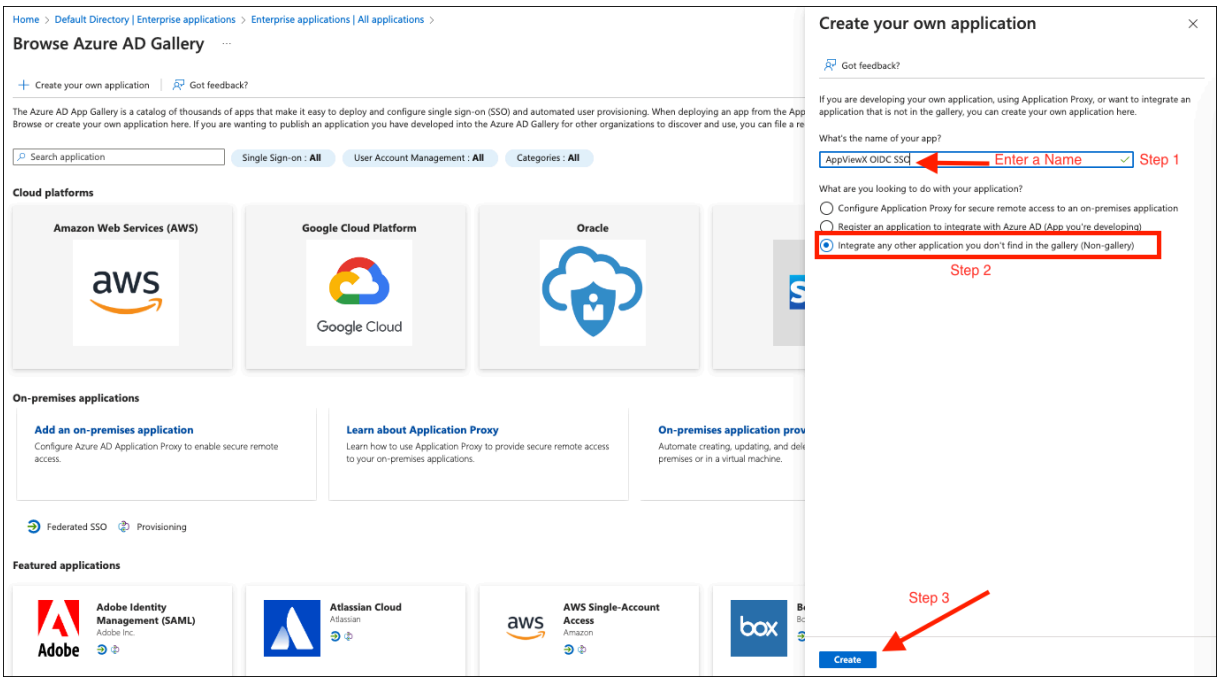
Steps to Integrate OIDC

To integrate with AppViewX – Azure using OIDC

1. From the Microsoft **Azure Home > Default Directory** Overview page, create an app under Enterprise Application within the **Azure Active Directory** (AAD).
2. Click **Enterprise applications**.



3. Click **New application**.
4. Click **Create your own application**.
5. In the Create your own application slider screen, perform the following:

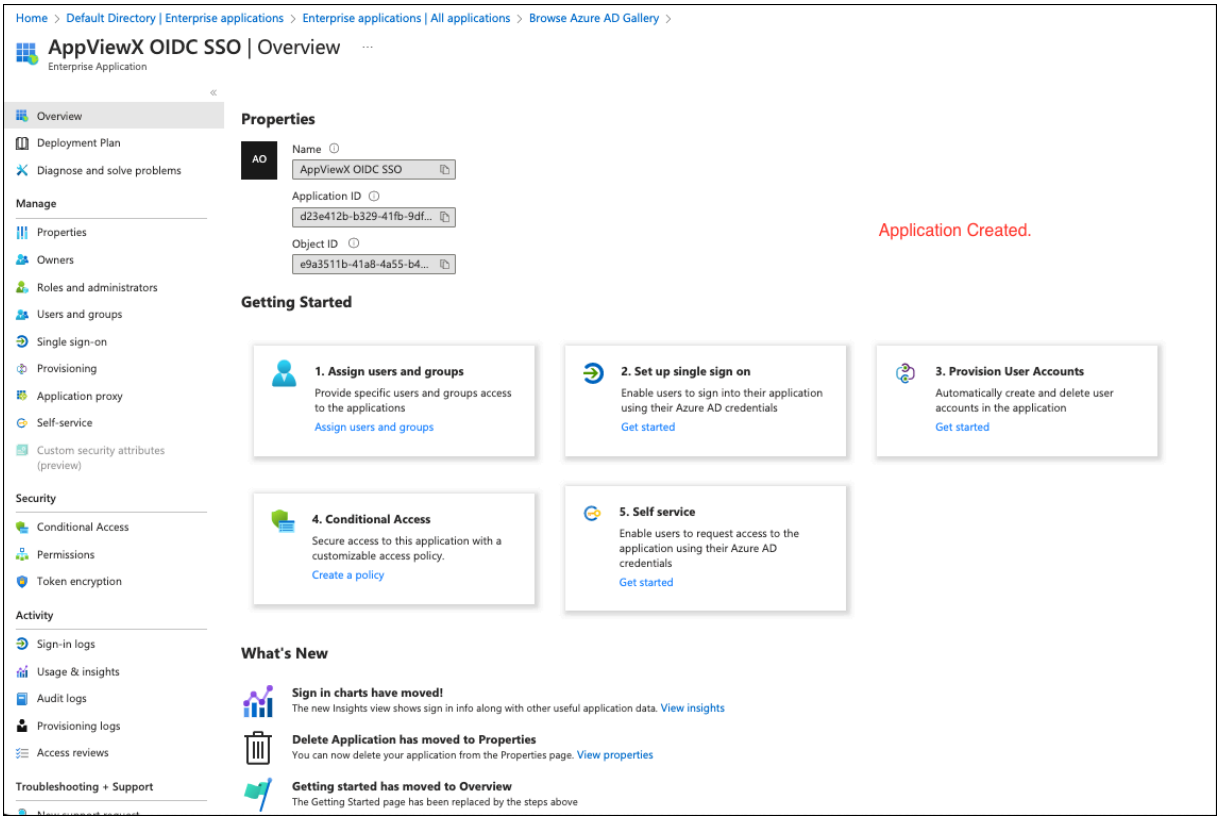


a. Enter a name in the **What's the name of your app?** field

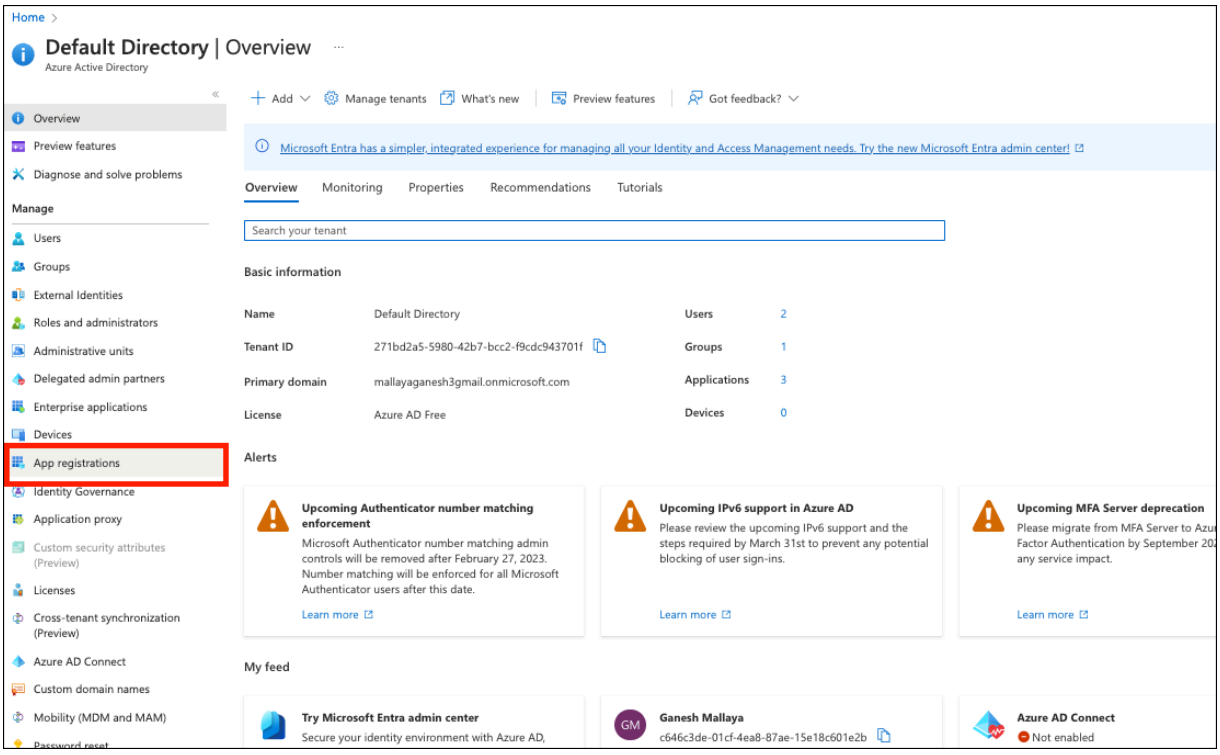
b. Select the radio button **Integrate any other application you don't find in the gallery**

c. Click **Create**

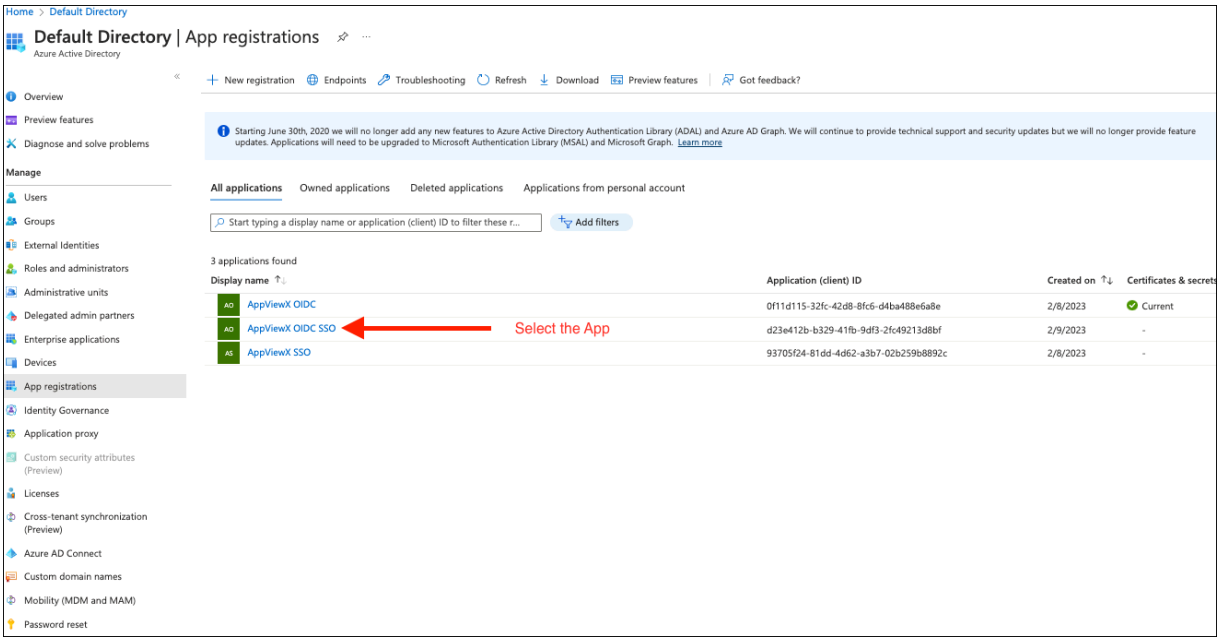
The application is created successfully and the details are displayed as shown below. Verify the details.



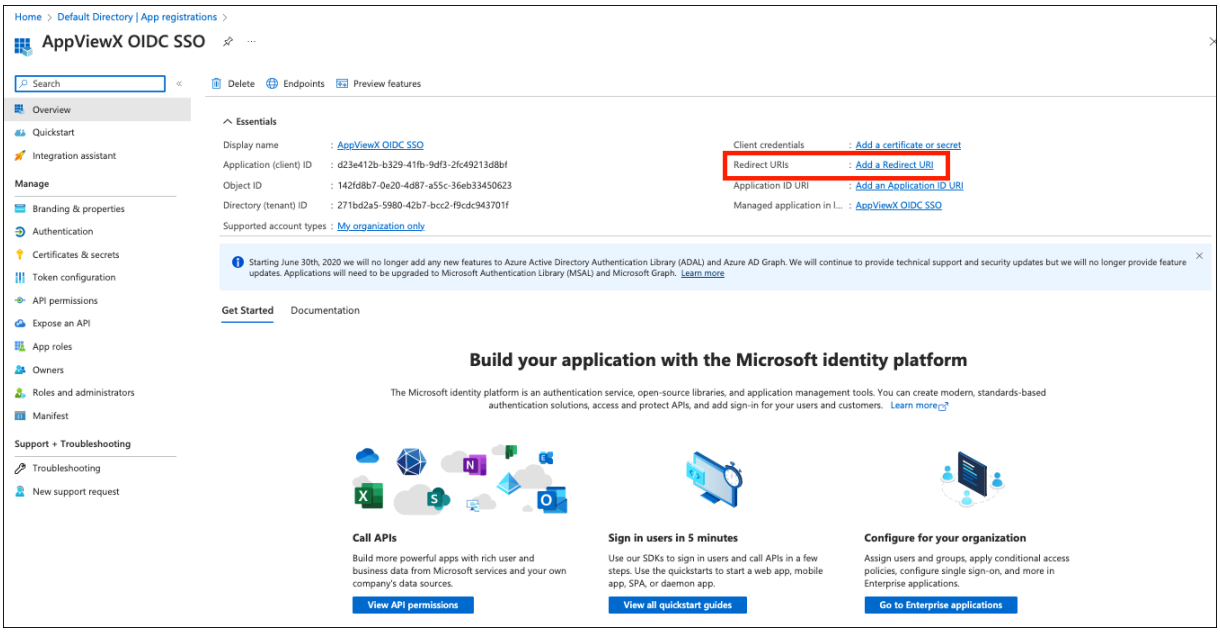
6. Navigate to **Overview**, and then click **App Registration**.



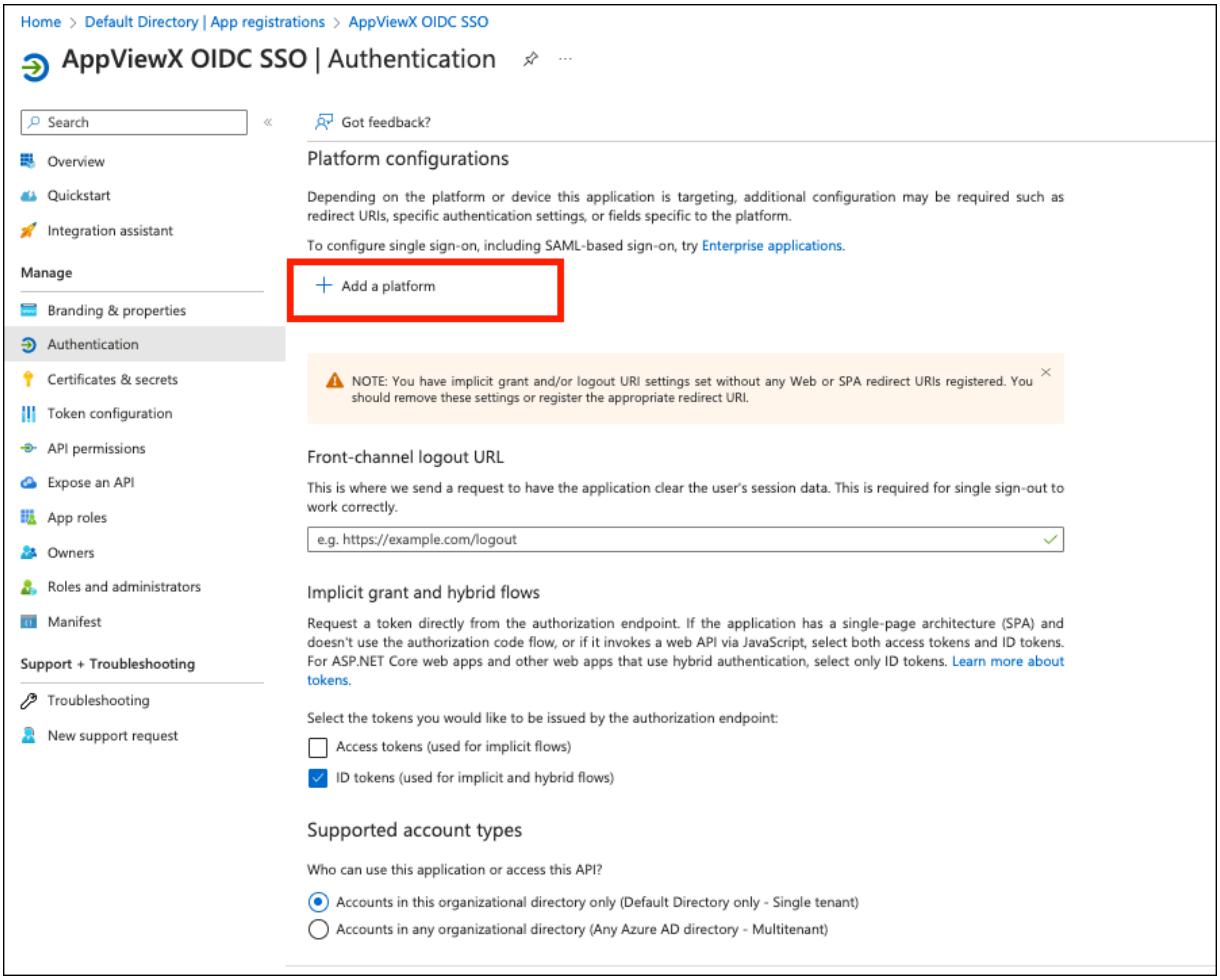
7. Select the App created.



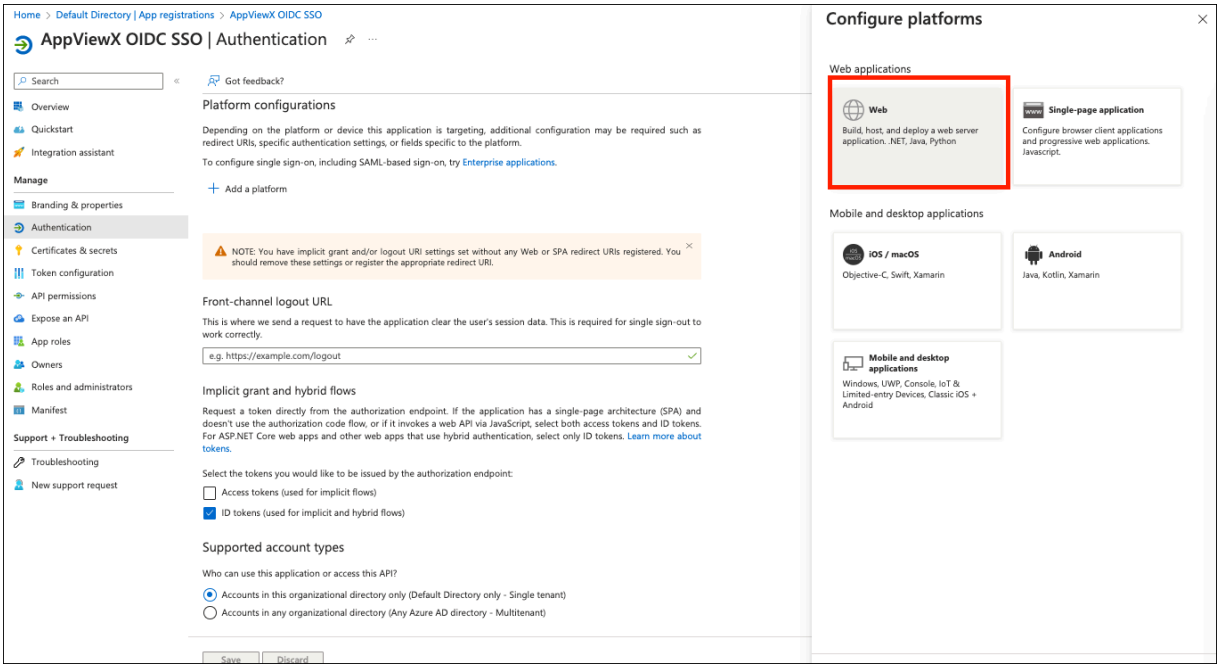
8. Setup the Redirect URI for web-based application.
9. Click **Redirect URI** from the overview page of the App.



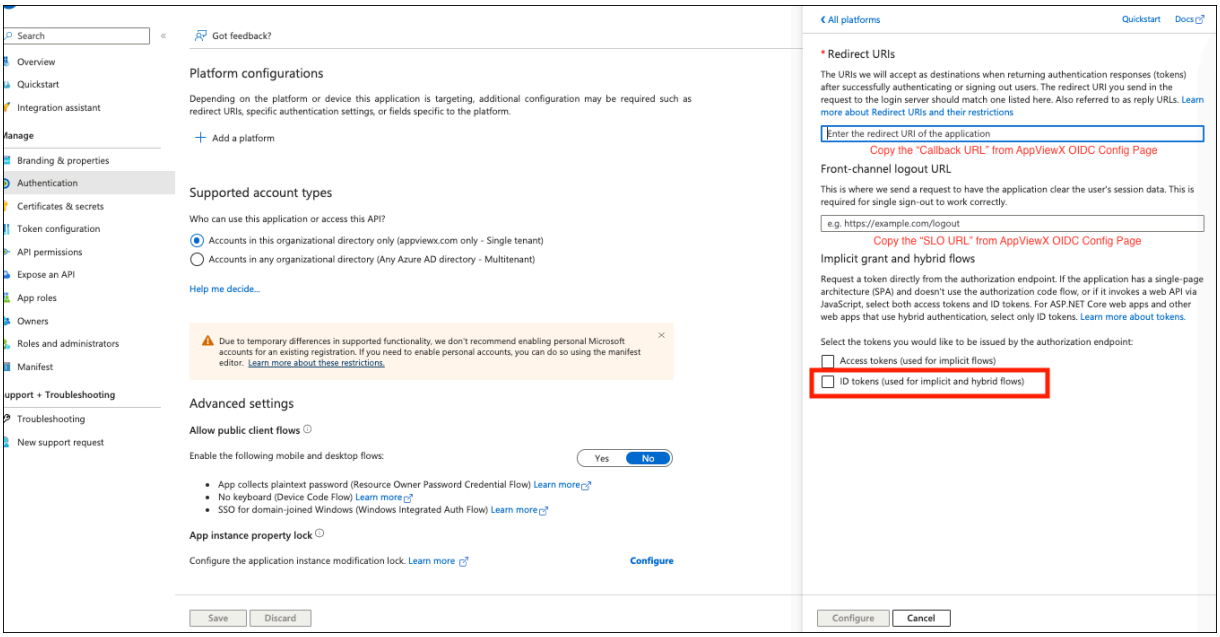
10. Click **Add a Platform**.



11. Select the **Web** platform and copy-paste the links from the AppViewX GUI.



12. Copy paste the URL from AppViewX GUI as follows:



a. Copy the Callback URL from the AppViewX GUI and paste it into the first field on the right.

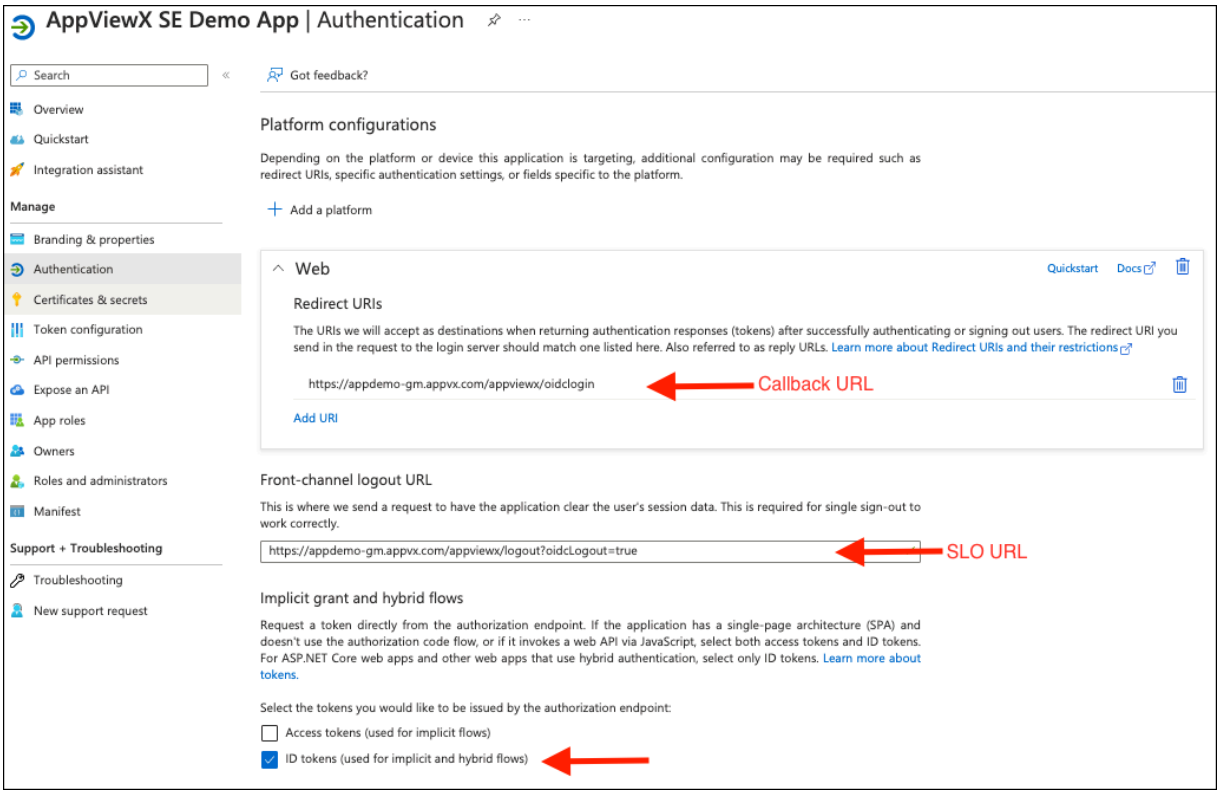
b. Copy the SLO URL from AppViewX GUI to the second field on the right.

c. Select the check box **ID Tokens**.

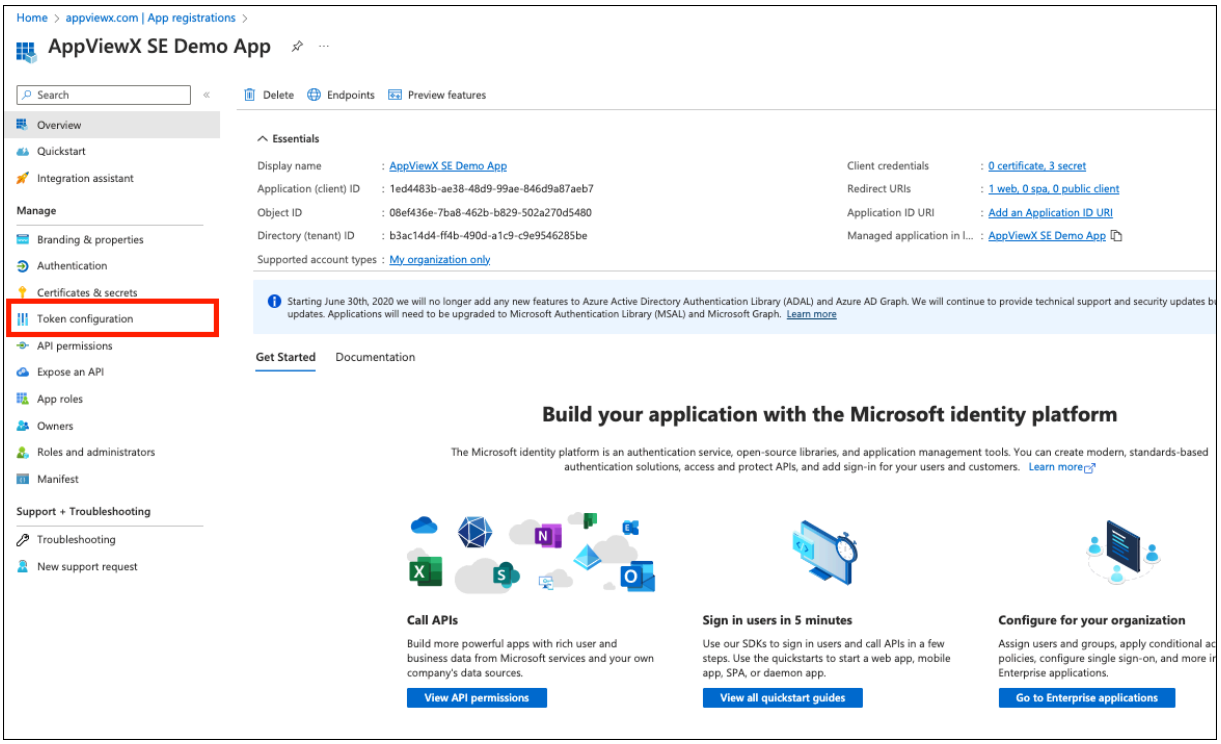
d. **Note:** Applicable for implicit and hybrid flows.

Click **Configure**.

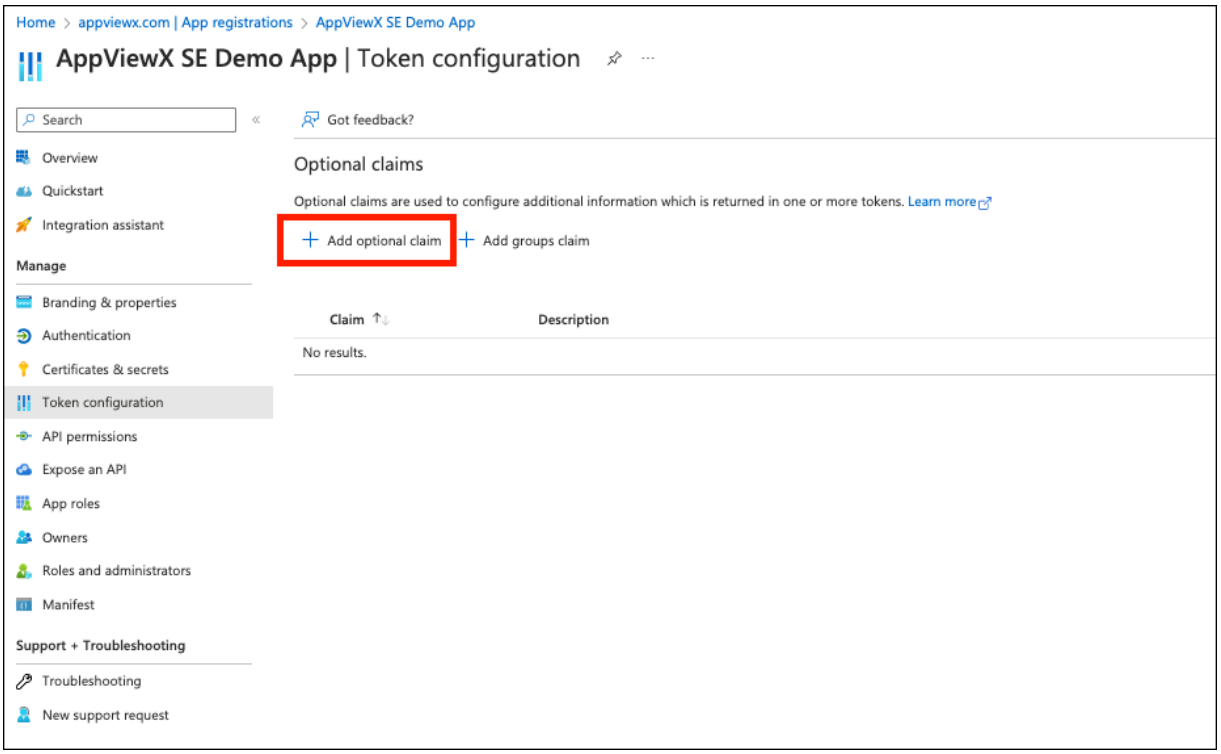
13. Verify the details of the Redirect URL.



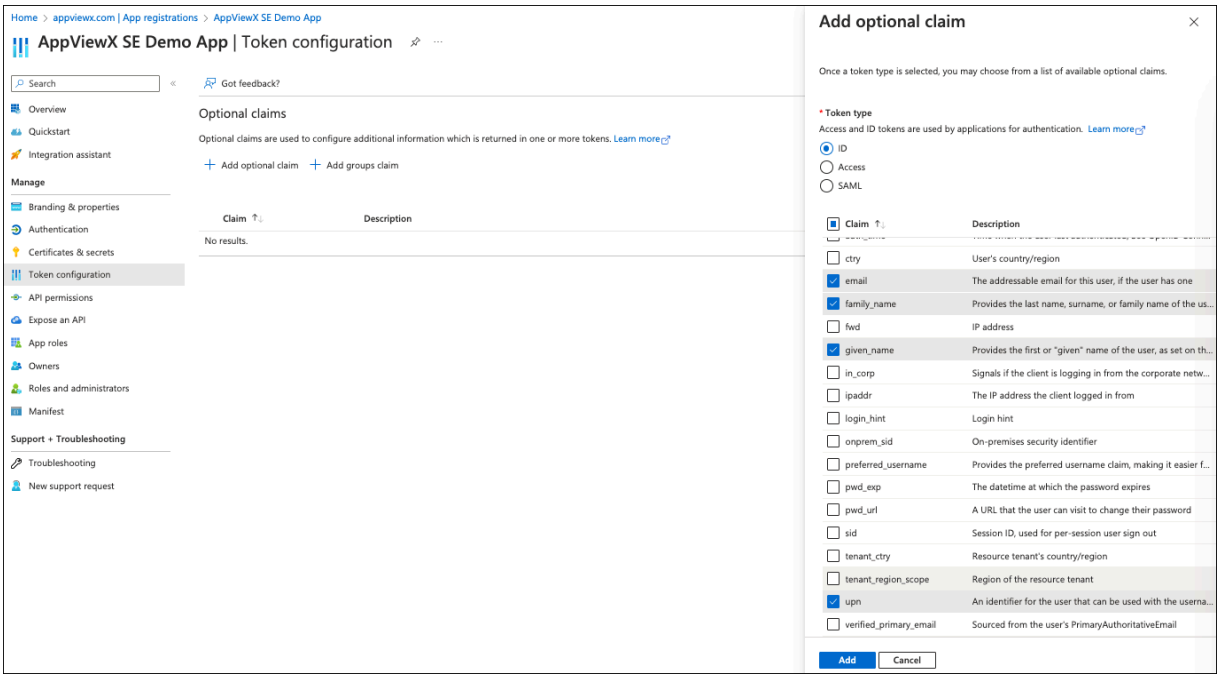
14. Click **Token configuration**.



15. In the Token configuration page, click **Add optional claim**.



Perform the following on the right slider screen:

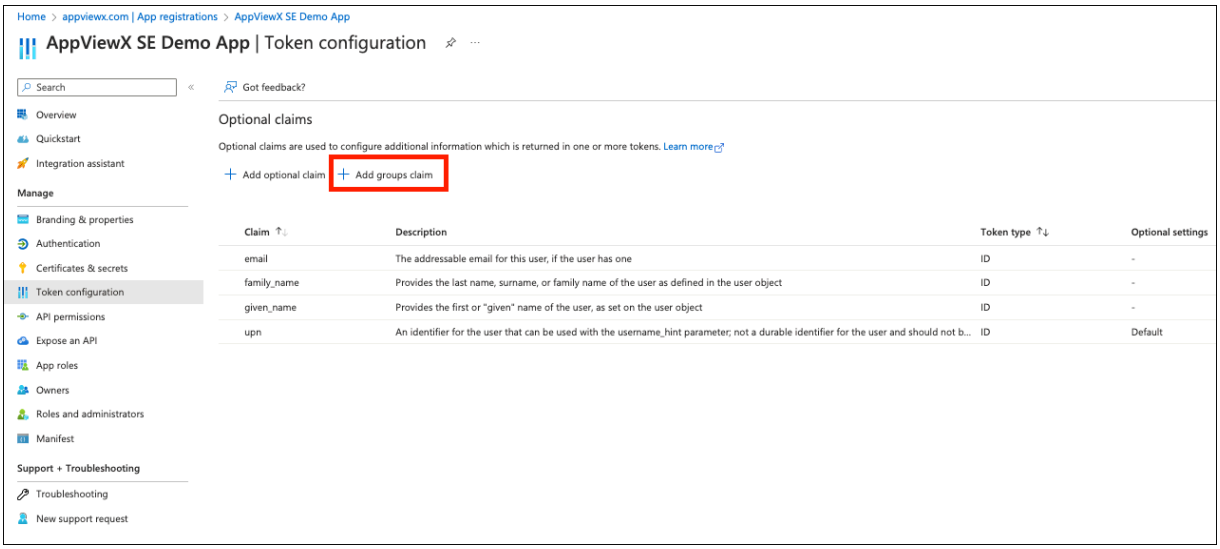


a. In the Token type, select the **ID** radio button.

b. Select the specified claims from the available list.

c. Click **Add**.

16. Click **Add group claims** and perform the following on the right slider page.



a. Select the **Security groups** checkbox.

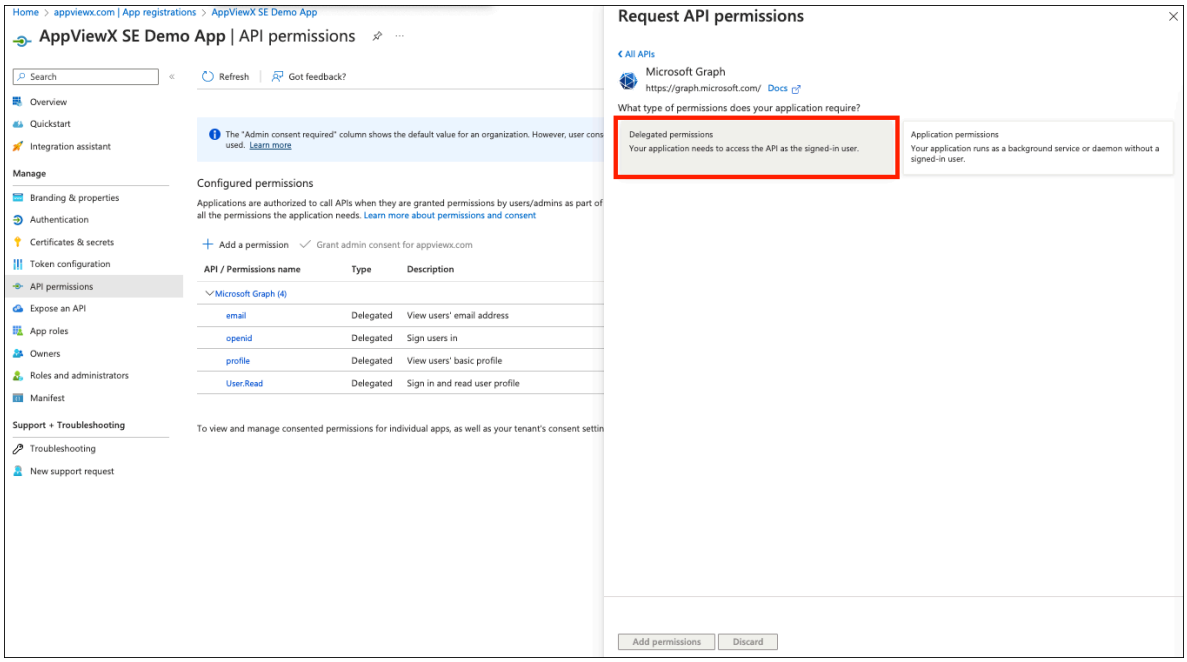
b. From the ID section select the radio button for **Account Name**.

17. Copy paste the Claims Mapping from Columns Claim in AppViewX as below.
18. To create API permissions for claim mapping, click **API Permissions**.
19. To configure the API Permissions from Microsoft Graph.

a. Click **Add a Permissions**.

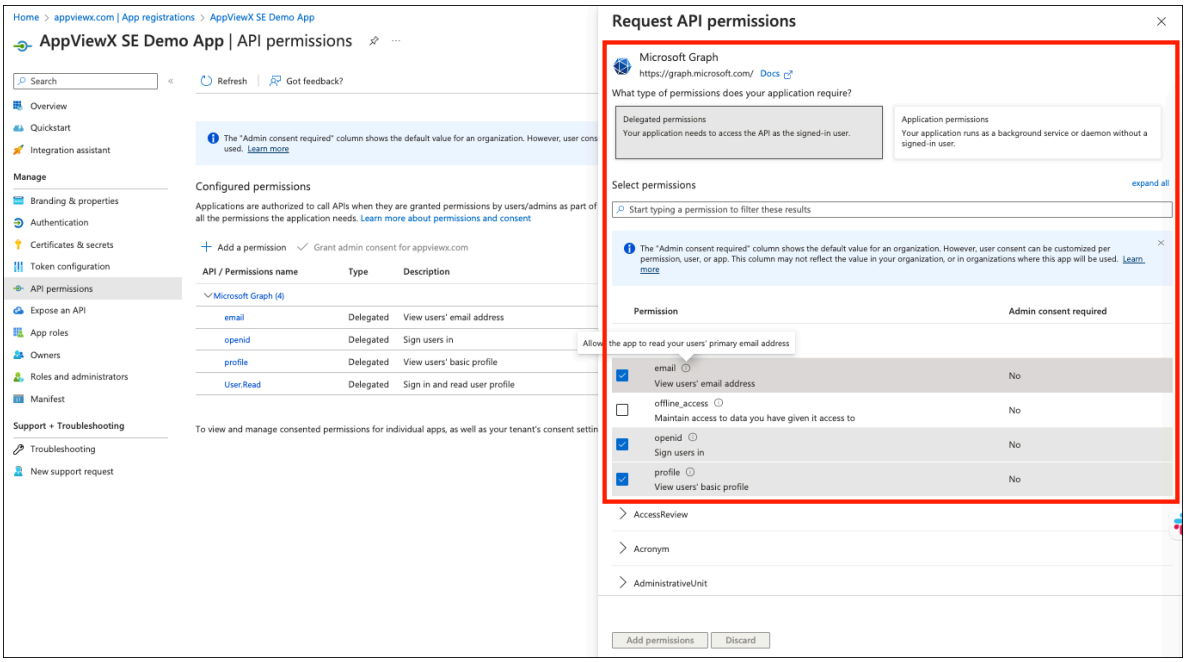
b. Select **Microsoft Graph**.

c. Select **Delegated permission**.

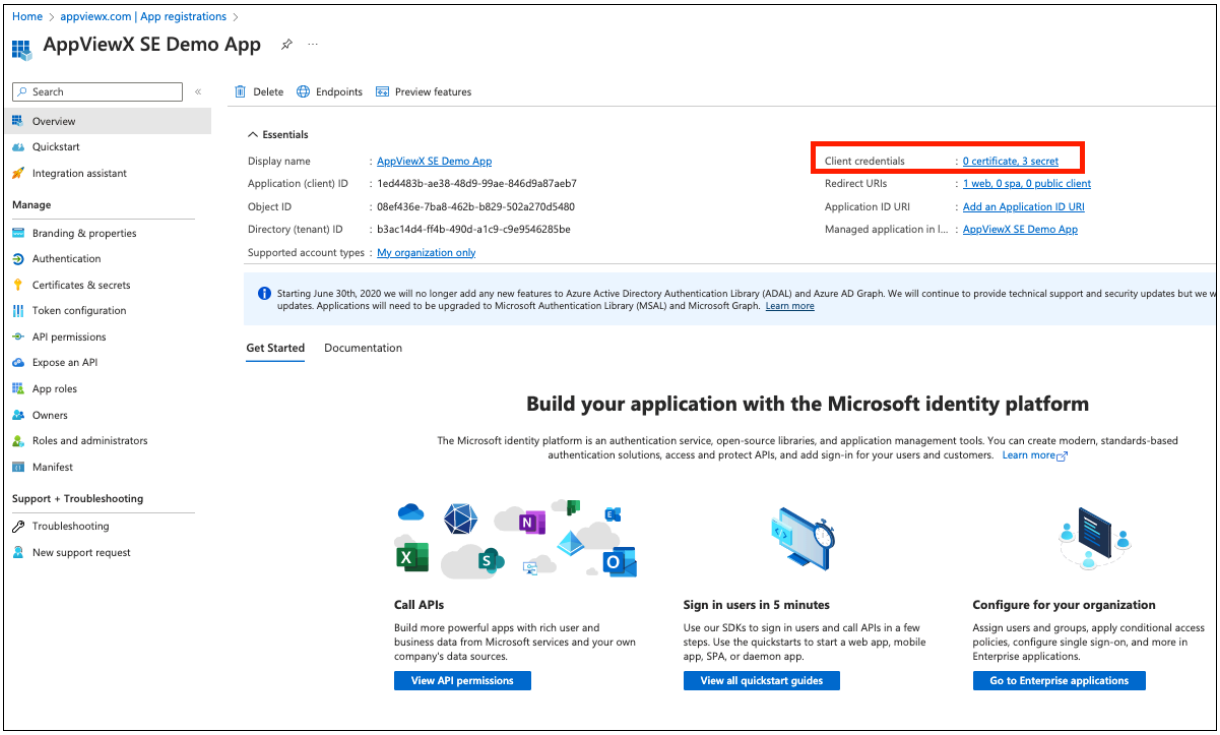


d. Click the following check-box on the Select Permissions section.

- email
- openid
- profile.

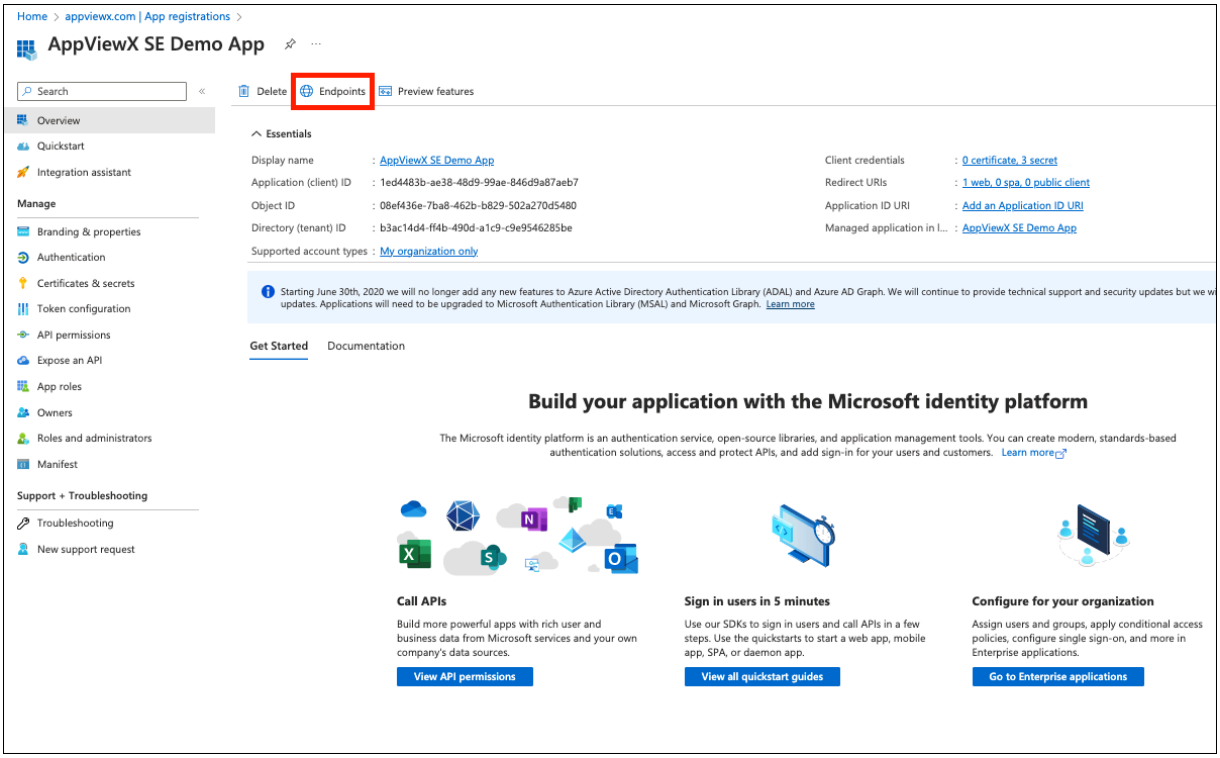


20. To create client secret for the App, click **Client credentials**.

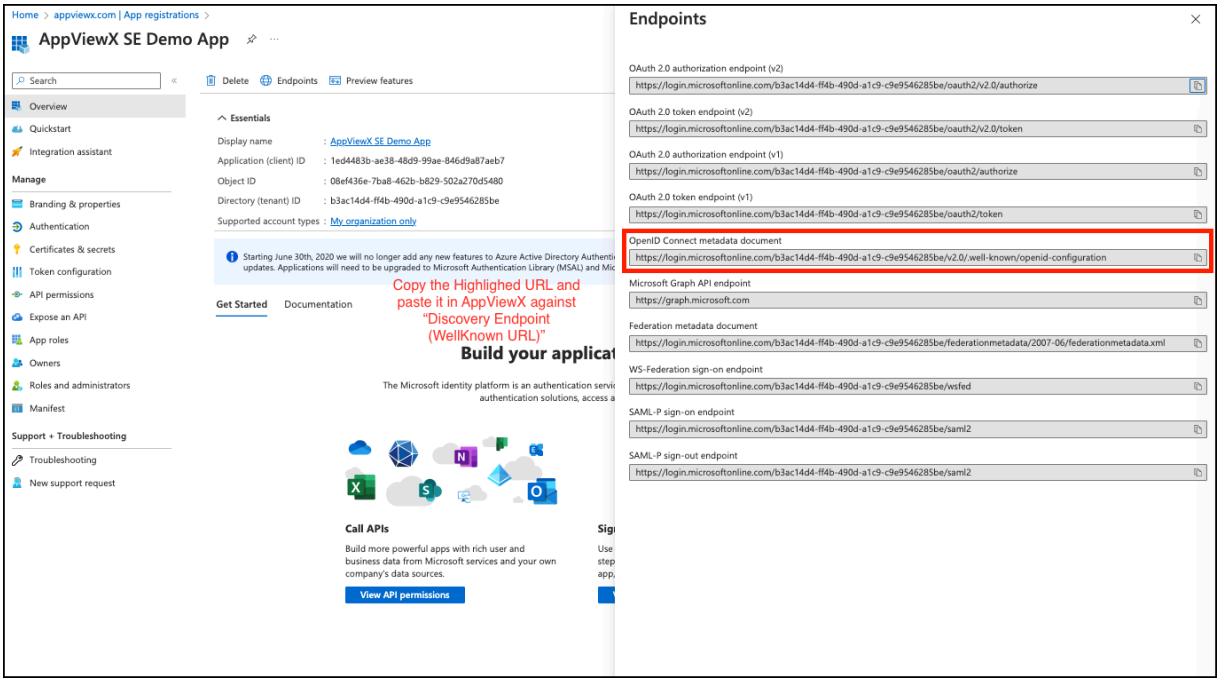


- Click **New client secret**, copy the secret and save it securely.

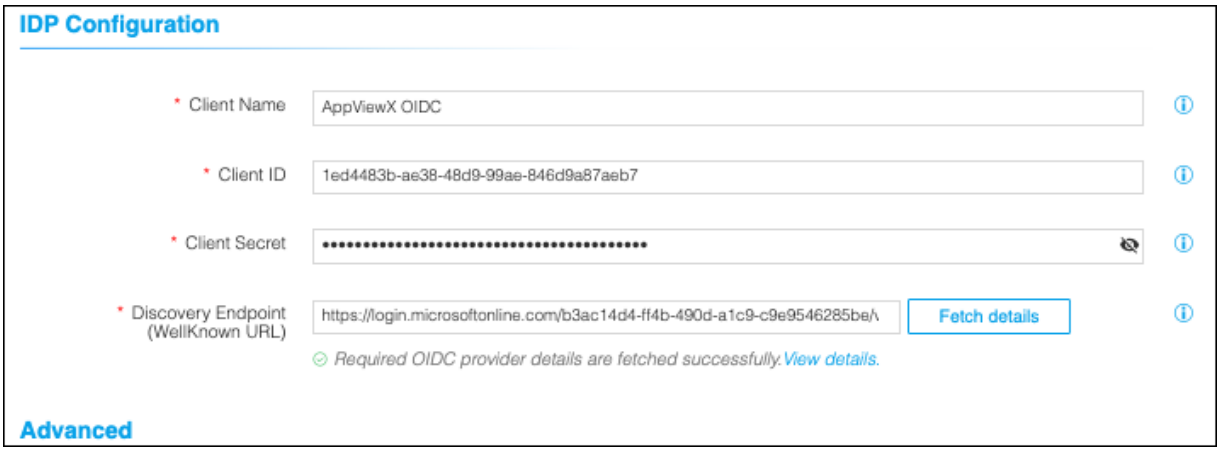
21. To copy the Endpoint Details from App Overview Page, click **Endpoints**.

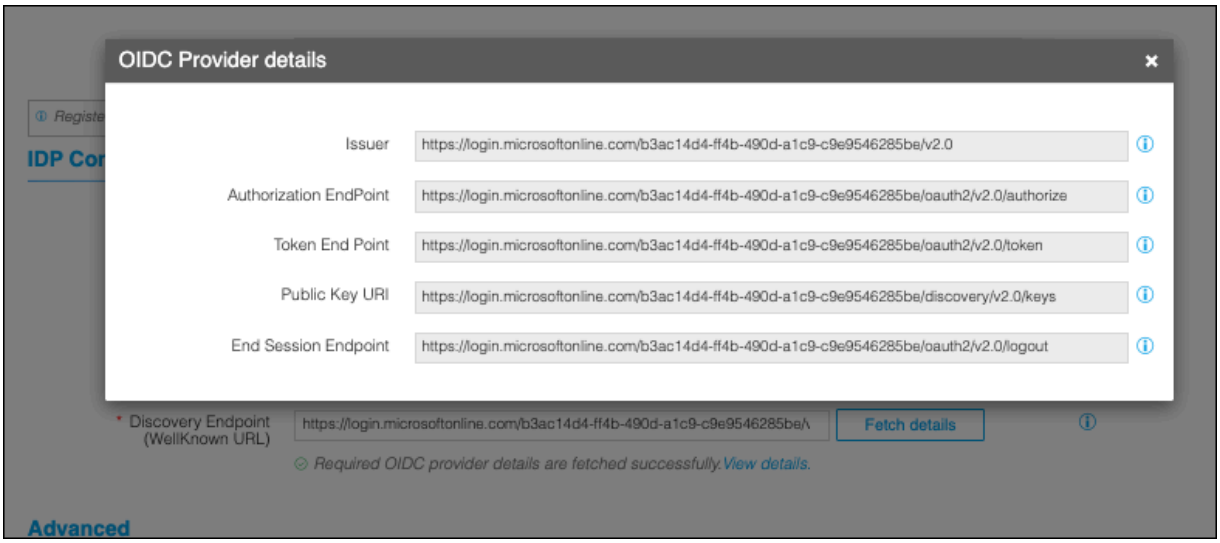


- Copy the URL from **OpenID Connect metadata document** field. **Discovery Endpoint (WellKnown URL)**.



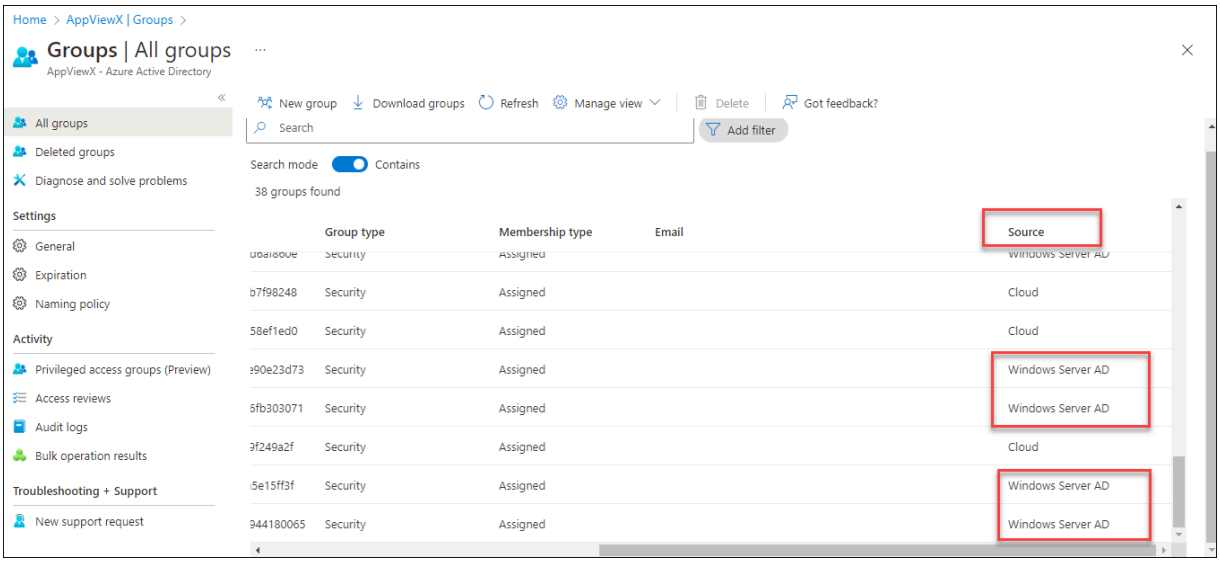
22. Configure the Client ID, Secret Key, and OpenID Wellknown URL in AppViewX GUI.





23. Create the Security Group within Azure, adding it in AppViewX under **Accounts > User groups**.
24. Proceed with user authentication, ensuring alignment of AppViewX roles with the designated user groups.

Note: Use the security groups with source as **Windows Server AD**.



IP Restriction Configuration

IP Restriction Configuration involves setting up limitations on network access based on specific IP addresses or ranges, controlling the ability to access a system, network, or application based on predefined rules or allowed IP ranges.

- Accessing the IP Restriction Configuration Settings
- Configuring the IP Restrictions

Accessing the IP Restriction Configuration Settings

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **ACCESS MANAGEMENT**, select **IP Restriction**. The **Settings :: Authentication** page is displayed with the **IP Restriction** tab open by default.	1. From the main navigation menu, click **Settings**. 2. On the **Settings** page, from the left menu, select **General** > **Authentication**.

New Menu	Old Menu
	The **Settings :: Authentication** page is displayed with the **LDAP** tab open by default. 3. Click the **IP Restriction** tab.

Note: For more information on how to switch between menus, click here.

Configuring the IP Restrictions

For enhanced security and if the administrator wants to whitelist specific IP addresses for user login, AppViewX lets you configure IP restrictions to allow access from whitelisted IP addresses/subnet ranges.

To configure IP restrictions:

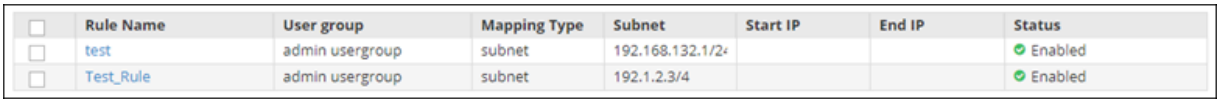
1. On the **Settings :: Authentication** page, under the **IP Restriction** tab, and **General Information** section, turn on the **Enable IP Restriction** toggle.
2. In the **IP/Subnet Configuration** section, enter the required field information.

Field descriptions for IP/Subnet Configuration

Field	Description
***Rule Name**	Rule name for a whitelisting condition.
***User group**	Select the user group to which this rule will apply, from the dropdown menu. **Note:** Only the users from the selected user group will be allowed to login to AppViewX from the whitelisted IP address/subnet range.
Mapping Type	Select one of the two mapping types: • **IP Range** • **Subnet**.
***Start IP**	Enter the starting IP address for the whitelisted IP/subnet range. **Note:** The IP/subnet range should be specified in the ascending order.

Field	Description
	Note: This field is displayed only when **Mapping Type** is selected as **IP Range**.
End IP	Enter the ending IP address for the whitelisted IP/subnet range. **Note:** The IP/subnet range should be specified in the ascending order. **Note:** This field is displayed only when **Mapping Type** is selected as **IP Range**.
***Subnet**	Enter the Subnet network range to whitelist. **Note:** This field is displayed only when **Mapping Type** is selected as **Subnet**.
Note: The asterisk (*) symbol indicates mandatory fields.	

3. To save the IP restriction settings, click **Add** or to reconfigure the settings, click **Reset**.
   The IP restriction settings thus configured are saved and displayed in the table shown at the end of the screen.



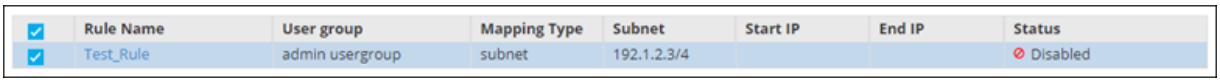
	Rule Name	User group	Mapping Type	Subnet	Start IP	End IP	Status
☐	test	admin usergroup	subnet	192.168.132.1/24			Enabled
☐	Test_Rule	admin usergroup	subnet	192.1.2.3/4			Enabled

- Enabling a IP Restriction Rule
- Disabling an IP Restriction Rule
- Deleting an IP Restriction Rule

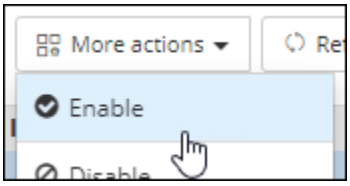
Enabling a IP Restriction Rule

To enable a IP restrictions rule:

1. On the **Settings :: Authentication** page, under the **IP Restriction** tab, from the table at the end of the page, for the IP restrictions rule you want to enable, select the check box corresponding to that rule.



2. From the **More actions** dropdown menu, click **Enable**.

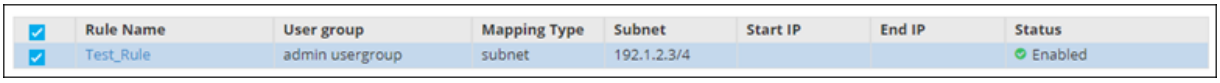


3. In the **Enable** dialog box, click **Yes**.

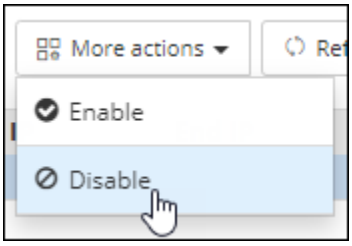
Disabling an IP Restriction Rule

To disable a IP restrictions rule:

1. On the **Settings :: Authentication** page, under the **IP Restriction** tab, from the table at the end of the page, for the IP restrictions rule you want to disable, select the check box corresponding to that rule.



2. From the **More actions** dropdown menu, click **Disable**.

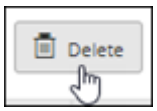


3. In the **Disable** dialog box, click **Yes**.
   The selected rule is disabled.

Deleting an IP Restriction Rule

To delete an IP restrictions rule:

1. On the **Settings :: Authentication** page, under the **IP Restriction** tab, from the table at the end of the page, for the IP restrictions rule you want to delete, select the check box corresponding to that rule.

2. Click 

(Delete).
3. In the **Confirmation** dialog box, click **Yes**.
   The selected rule is deleted.

Authentication Settings Configuration

Authentication Settings Configuration refers to the process of defining and customizing authentication mechanisms within a system or application. It involves configuring various authentication methods, settings, and security protocols to control user access and verify their identities during login or access attempts.

- Accessing the Authentication Settings Configuration Settings
- Configuring Authentication Settings

Accessing the Authentication Settings Configuration Settings

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **ACCESS MANAGEMENT**, select **Authentication settings**. The **Settings :: Authentication** page is displayed with the **Authentication settings** tab open by default.	1. From the main navigation menu, click **Settings**. 2. On the **Settings** page, from the left menu, select **General** > **Authentication**. The **Settings :: Authentication** page is displayed with the **LDAP** tab open by default. 3. Click the **Authentication settings** tab.
Note: For more information on how to switch between menus, click here.	

Configuring Authentication Settings

In addition to configuring authentication settings, AppViewX also lets you enable birthright provisioning for new users, configure the order in which user credentials are authenticated, enable/disable an authentication check, and other user and node settings.

To configure the authentication settings:

1. On the **Settings :: Authentication** page, under the **Authentication settings** tab, to enable **Birthright provisioning** for new users who log into the system with a predefined set of permissions (associated with the user group), turn on the **Enable Birthright** toggle.
   To do this, the admin should select the user group (Assigned with the defined permissions), which will act as a default user group for all the users logging in to AppViewX. For more details, refer to the content on creating a role and associating it with a user group.
2. To define the order in which the authentication settings will be checked, in the **Order** section, drag and drop the authentication labels to the required corresponding levels.
   If the level 1 check is set to Local and the level 2 check is set to LDAP, user credentials will be authenticated locally first and then on the LDAP server.

   Note: You can also disable, and then enable a level of authentication. To do this, click the green tick 

   next to the server name.

3. In the **User settings** section, enter the required field information.

Field descriptions for User settings

Field	Description
Create User an unique E-mail ID	To ensure that every AppViewX user has a unique email ID, turn on this toggle.
Create User on Authorization Failure	To create a user even if authorization fails (but the user is authenticated successfully), turn on this toggle.
Session Timeout	AppViewX lets you set a session timeout limit between 2 and 480 minutes. To set a web session timeout limit, enter the value in minutes.

4. If the AppViewX node password is updated, in the **Node Settings** section, enter the updated Node Password.

Note: The value entered in the Node Password field should be the same as the node password. To apply the changes, restart the avx-config-server pod in every datacenter.

5. Click **Save**.

- LDAP Authentication
- TACAS Authentication
- RADIUS Configuration
- Single Sign On Configuration
- IP Restriction Configuration
- Authentication Settings Configuration
- OAuth Settings
- MFA Settings Configuration
- SCIM Configuration

OAuth Settings

OAuth Settings typically refer to the configuration and management of OAuth (Open Authorization) protocols within an application or system. These settings encompass various parameters and configurations that govern OAuth-based authentication and authorization processes, including client IDs, client secrets, token lifetimes, scopes, and callback URLs, among others. Managing OAuth settings allows defining secure and authorized access for users or applications to protected resources.

- Accessing OAuth Settings Configuration
- Configuring External OAuth Settings
- Configuring Internal OAuth Settings

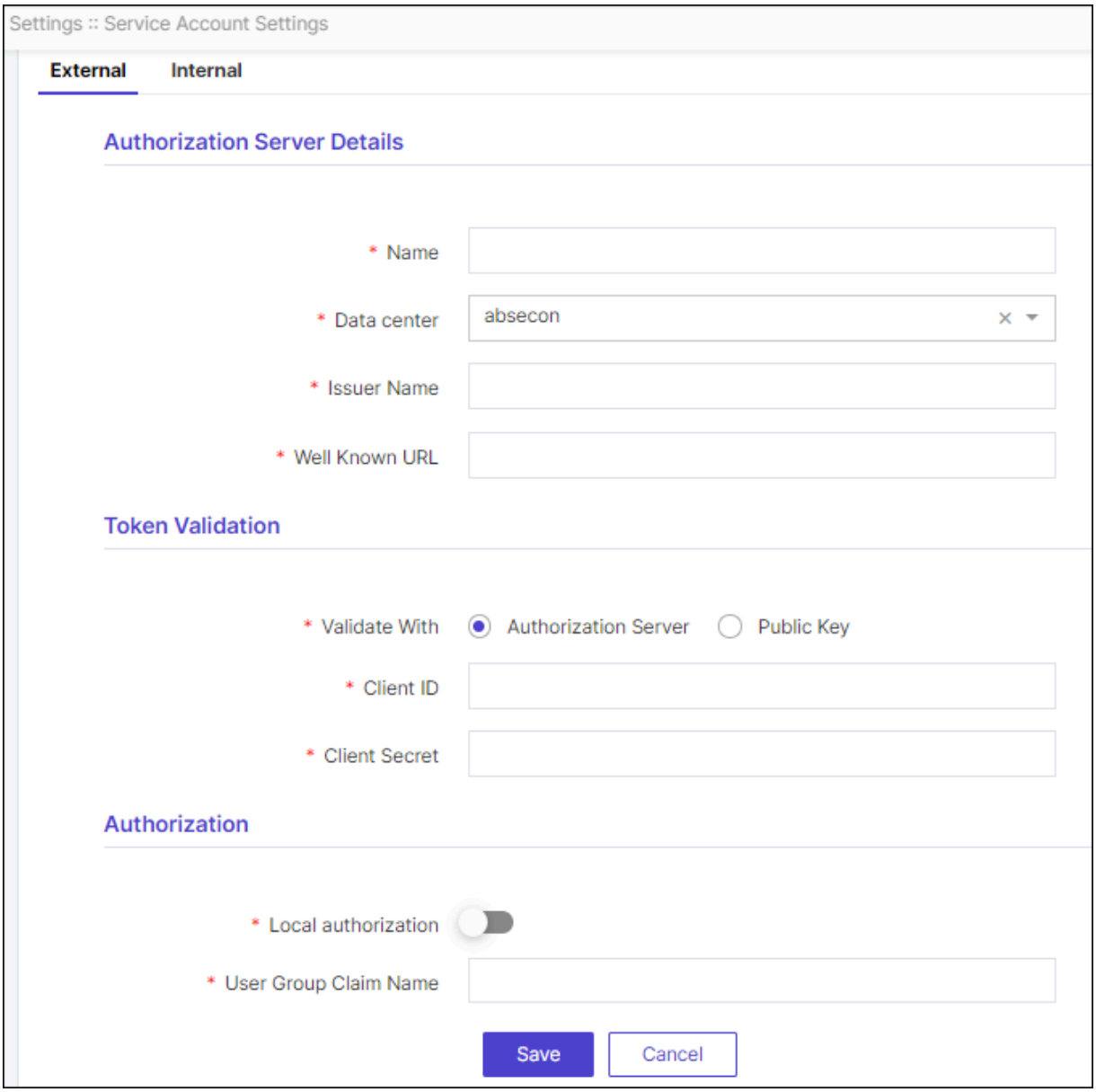
Accessing OAuth Settings Configuration

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **ACCESS MANAGEMENT**, select **OAuth Settings**. The **Settings :: Service Account Settings** page is displayed with the **External** tab open by default.	1. From the main navigation menu, click **Settings**. 2. On the **Settings** page, from the left menu, select **General** > **OAuth Settings**. The **Settings :: Service Account Settings** page is displayed with the **External** tab open by default.
Note: For more information on how to switch between menus, click here.	

Configuring External OAuth Settings

To configure External OAuth settings, follow the below steps:

1. On the **Settings :: Service Account Settings** page, under the **External** OAuth Settings tab, enter the required field information.



2. In the **Authorization Server Details** section, enter the following details.

Field descriptions for Authorization Server Details

Field	Description
***Name**	Enter the unique name for the Authorization server.
***Data center**	From the options available in the dropdown, select the data center.

Field	Description
***Issuer Name**	Enter the issuer name of the token, ensuring it matches the value in the issuer token claim.
***Well Known URL**	Enter the well known URL of the Authorization server.

Note: The asterisk (*) symbol indicates mandatory fields.

3. In the **Token Validation** section, enter the following details.

Field descriptions for Token Validation

Field	Description
***Validate With**	Select the **Validation** type: • **Authorization Server**: To validate with Client ID and Client Secret, Select **Authorization Server** option. • **Public Key**: To validate using a Public Key, Select **Public Key** option.
***Client ID**	**Note:** This field is displayed when **Validate With** is selected as **Authorization Server**. Enter the Client ID that is generated in the OAuth server when the OAuth client is created. **Note:** This client ID is generated in the OAuth server for AppViewX.
***Client Secret**	**Note:** This field is displayed when **Validate With** is selected as **Authorization Server**. Enter the Client Secret that is generated in the OAuth server when the OAuth client is created. **Note:** This client secret is generated in the OAuth server for AppViewX.

Field	Description
	Note: The asterisk (*) symbol indicates mandatory fields.

Note: If the token is valid and a service account has not been created, an automatic process will generate the service account, using the client ID as the login name.

Note: When the service account is automatically created, there is a chance of authorization failure resulting from unassigned user groups. To resolve this, manually assign the required user group to the service account.

4. In the **Authorization** section, enter the following details.

Field descriptions for Authorization

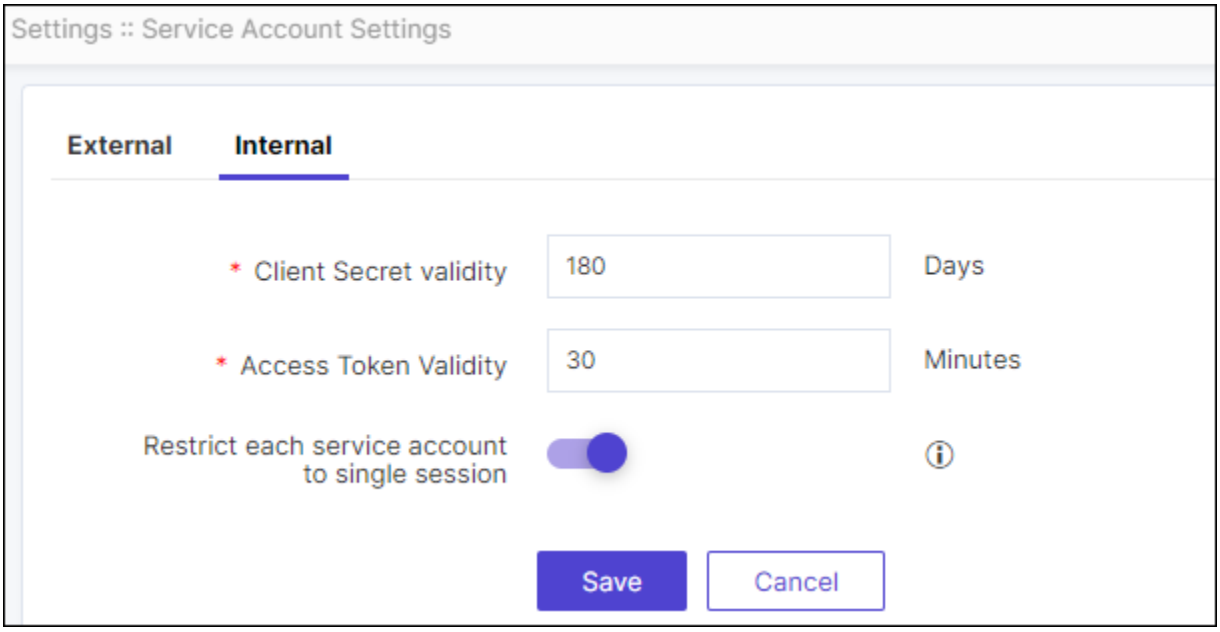
Field	Description
***Local authorization**	To enable or disable local authorization for authentication with the OAuth server and authorization within AppViewX, if the OAuth server is unable to pass the roles or user groups as part of the token and requires AppViewX to perform the authorization, then the above feature can be used.
***User Group Claim Name**	**Note:** This field is displayed when the **Local authorization** is disabled. Enter the user group's claim name from the token. **Note:** Ensure that the user group already exists in AppViewX; if it doesn't, create a new user group with the same name.
	Note: The asterisk (*) symbol indicates mandatory fields.

5. Click **Save**.

Configuring Internal OAuth Settings

To configure Internal OAuth settings, follow the below steps:

1. On the Settings :: Service Account Settings page, under the **Internal** OAuth Settings tab, enter the required field information.



Field descriptions for Internal OAuth Settings

Field	Description
***Client Secret validity**	Enter the secret validity in the number of days.
***Access Token Validity**	Enter the access token's validity in the number of minutes.
Restrict each service account to single session	Enable the toggle to limit each service account to have only one valid Access token at a time, thereby restricting them to use only one session at a time.

Field	Description
	Note: If the toggle is disabled, then a maximum of 100 Access tokens can be created in parallel for a single service account which allows using multiple sessions in parallel with the same service account.
Note: The asterisk (*) symbol indicates mandatory fields.	

Note: By default, the client secret expires in 180 days, and the access token expires in 30 minutes. It is customizable.

Note: Whenever an Access Token expires, an HTTP Error Code 401 is displayed in the API response. The client application can generate a new Access Token using the Client ID and Client Secret.

Note: When the Client Secret expires, you can regenerate a new Client Secret from AppViewX in **Service Account** > **Account Name** > **Client Secret** > **Regenerate**.

2. Click **Save**.

MFA Settings Configuration

MFA Settings Configurations refers to the process of configuring Multi-Factor Authentication (MFA) settings within a system or application. This involves setting up additional security measures beyond passwords, such as OTP (One-Time Password), biometric verification, or other methods, to enhance the authentication process and bolster security.

Accessing MFA Settings Configuration

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **ACCESS MANAGEMENT**, select **MFA**. The **Settings :: Authentication** page is displayed with the **MFA** tab open by default.	1. From the main navigation menu, click **Settings**. 2. On the **Settings** page, from the left menu, select **General** > **Authentication**. The **Settings :: Authentication** page is displayed with the **LDAP** tab open by default. 3. Click the **MFA** tab.
Note: For more information on how to switch between menus, click here.	

Configuring the MFA Settings

MFA is one of the most effective ways to prevent unauthorized access as it requires additional validation of login credentials during a user's authentication process. MFA can be as straightforward as a user providing their password, then entering an accompanying numeric code (OTP) from an Email Text.

Prerequisites for On-prem

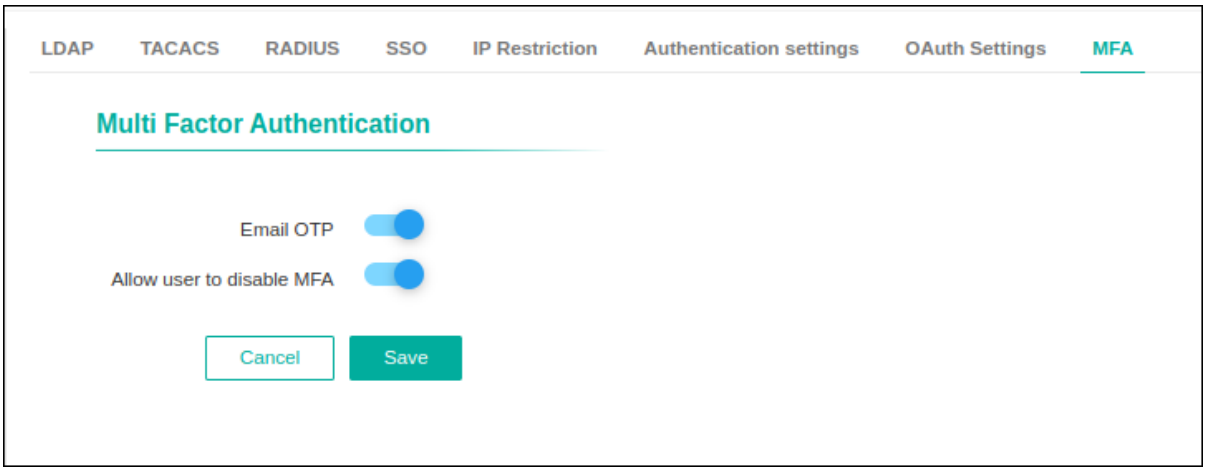
1. SMTP configuration should be done before enabling MFA.
2. Email should be configured for "Admin user" before enabling MFA.
3. **If there is communication or any other issue with SMTP, then local users cannot login to AppViewX if MFA is enabled. So, our recommendation is to maintain high availability for SMTP.**

Note: In **Onprem**, only the **"Admin user"** can configure MFA settings, and in **SaaS,** only the **"Account owner"** can configure MFA settings.

Note: For **SaaS** deployment, MFA is enabled by default for the Account Owner. You cannot disable MFA for the account owner.

To configure the MFA settings:

1. On the **Settings :: Authentication** page, under the **MFA** tab, select **Email OTP** to enable multi factor authentication.
2. The Audit logs for enable/disable **MFA** are `User: <Username> update MFA settings and enabled/disabled MFA`.
3. On selecting Email OTP, the **Allow user to disable MFA** option appears, which can be enabled or disabled based on the user's requirement.
4. If the admin disables the **Allow user to disable MFA** option, it will enforce MFA usage for all the users. If enabled by the admin, users can enable/disable MFA usage from their user profile settings.



5. The Audit logs for enable/disable **Allow user to disable MFA** are `User: <Username> updated MFA settings and enabled/disabled Allow user to disable MFA`.
6. Click **Save**.

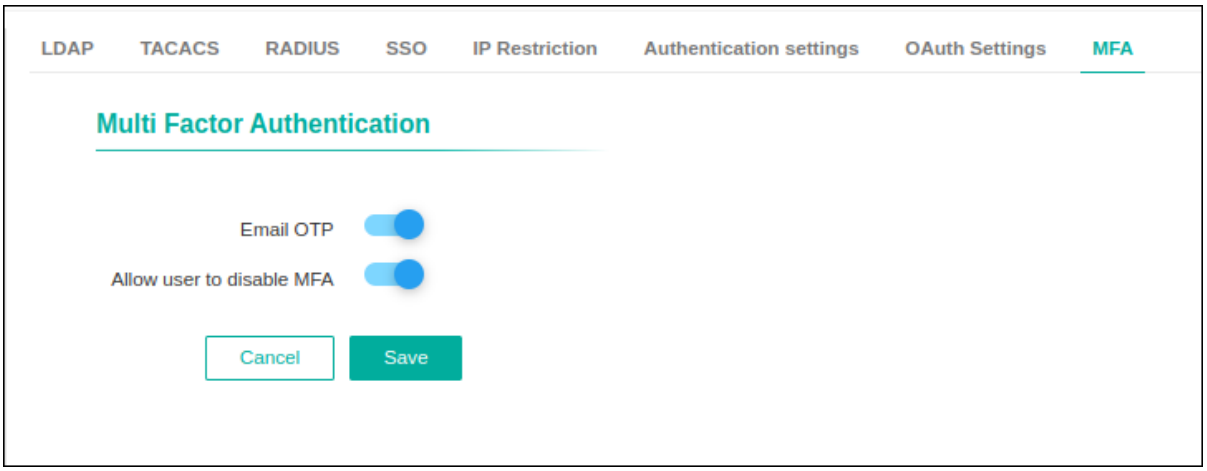
- MFA Settings for User Profile
- Logging in using MFA

MFA Settings for User Profile

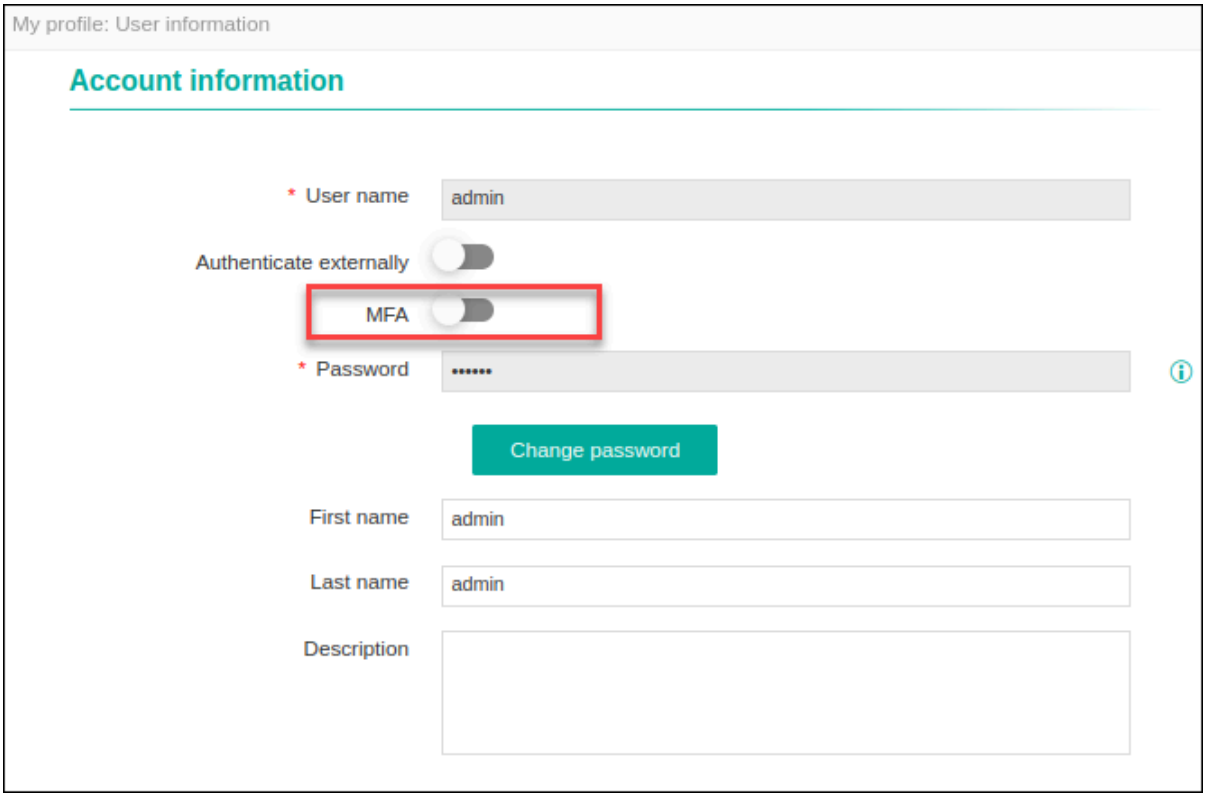
Admin has provision to control MFA feature for the user role.

The following steps explains access to enable/disable MFA from user profile:

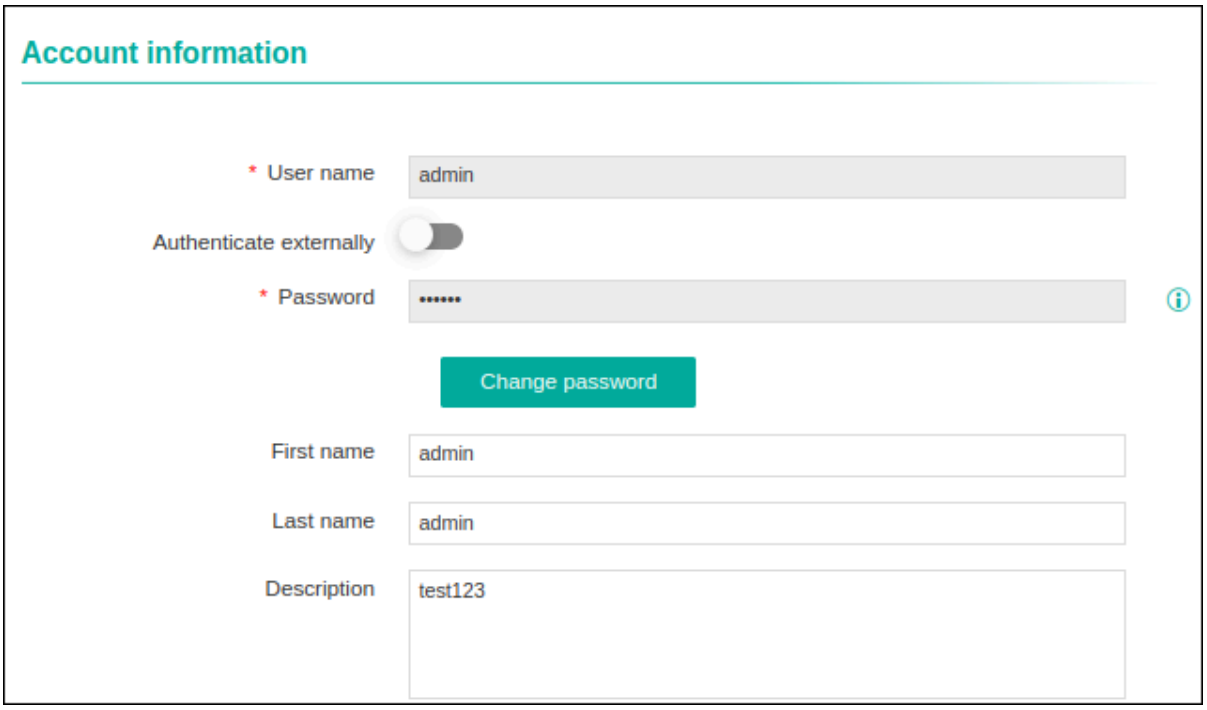
1. On selecting email OTP, the **Allow user to disable MFA** option appears. This can be enabled or disabled based on the user's requirement.



2. If the admin enables **Allow user to disable MFA**, then users have provision to enable/disable MFA and **MFA** option appears in user profile.



3. If the admin disables **Allow user to disable MFA**, then users can not see **MFA** option in the user profile.



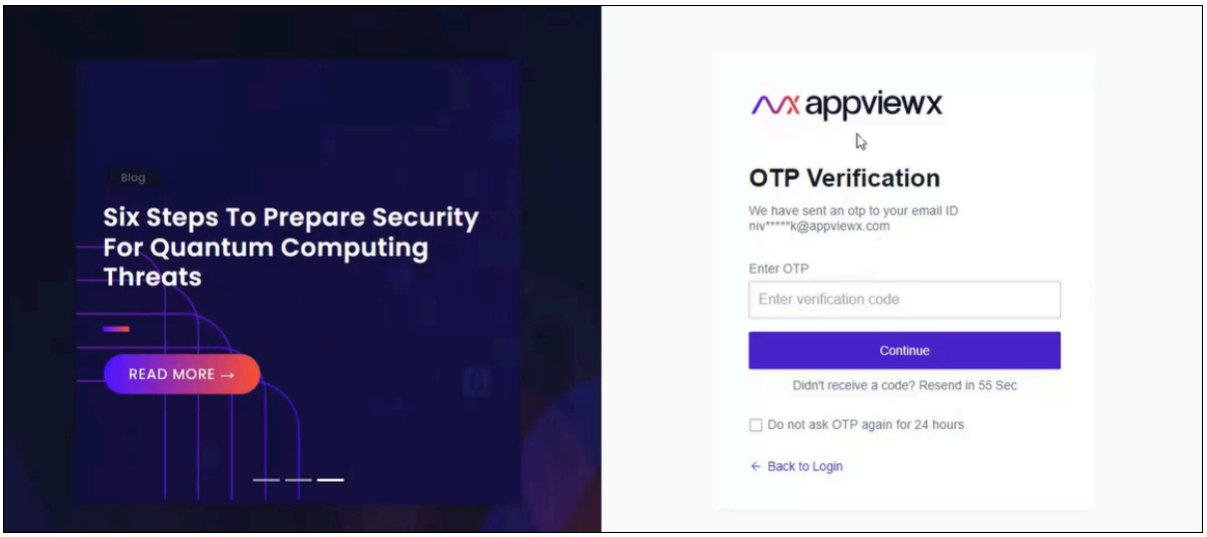
Logging in using MFA

The following steps explains access to AppViewX Login using MFA:

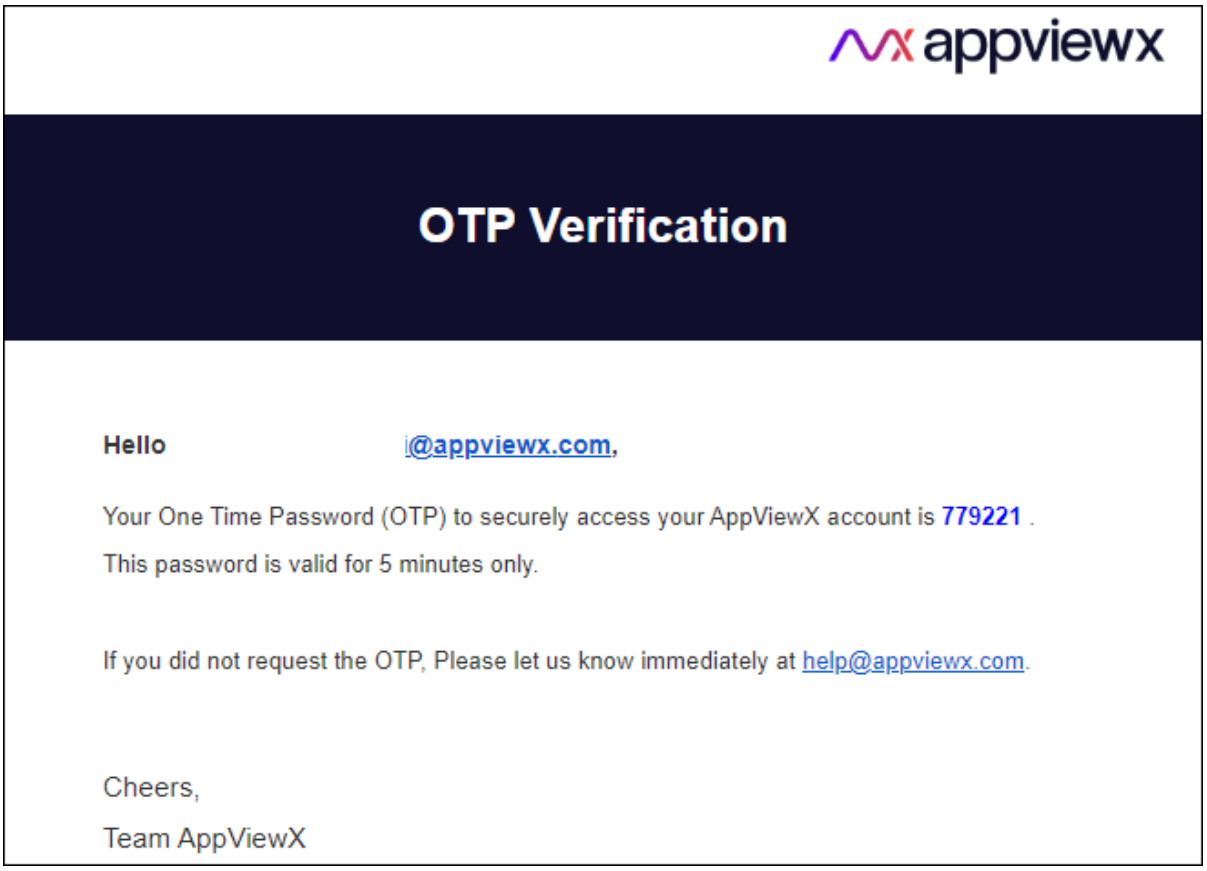
1. Log in using your user credentials.

   The MFA system generates a random six digit numeric value and sends OTP to the registered user's email ID.

2. User authentication (**OTP Verification**) screen is displayed.



3. Enter OTP which is sent to your registered email ID.



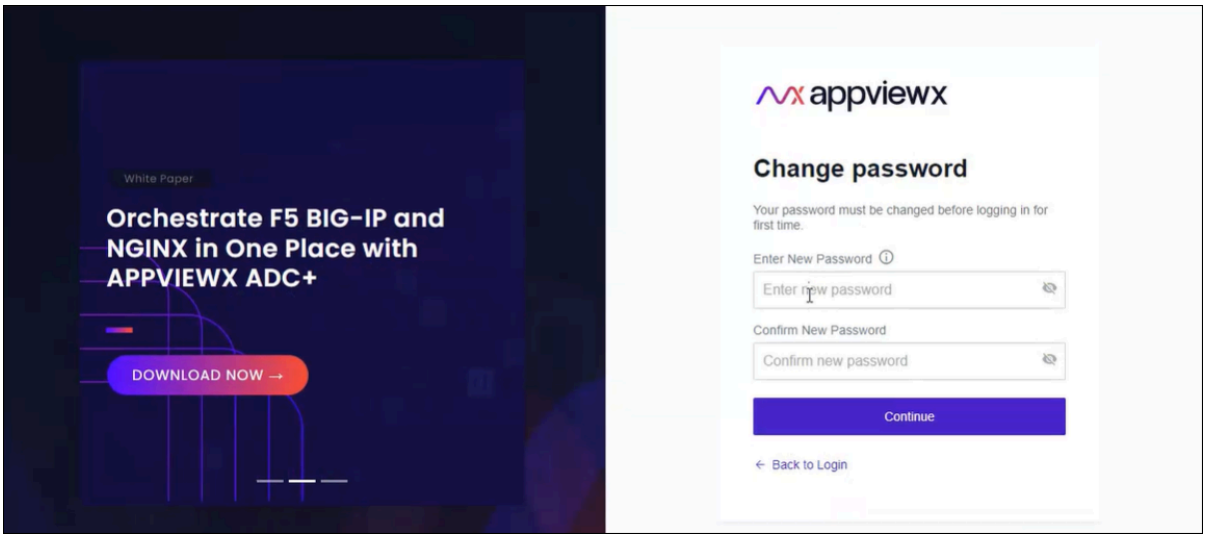
4. OTP Validation.

- OTP sent to Email will be valid only for next five minutes.
- Users will be locked if wrong OTP is entered more than five times.
- Once the user is locked for 15 minutes, an auto-generated Email is received asking to contact the administrator to unlock.

5. Resend OTP - MFA.
   - Resend option will be enabled after ***60 seconds***.
   - Resend option will be available only five times for wrong attempt.
   - Users will be locked if resend OTP is attempt for more than five times.
   - Once the user is locked for 15 min, an auto-generated Email is received asking to contact the administrator to unlock.

> **Note:** Users can select **Do not ask OTP again for 24 hours** during login and disable OTP Verification for next consecutive logins for 24 hours.

6. Click **Continue**.
7. The Audit log for invalid OTP is `Login failed for user: <Username> due to Invalid OTP`.
8. **Change Password** page is displayed for the users logging in for the first time.



9. Enter the details in the required fields.
10. Click **Continue**.

SCIM Configuration

SCIM, or System for Cross-domain Identity Management, is a standardized protocol designed for efficient management of user identities across different systems and platforms. It simplifies user provisioning

and deprovisioning processes by offering a consistent approach for user lifecycle management. SCIM operates over HTTP and uses JSON for data exchange, allowing seamless integration with various applications and services. Its core functions include user provisioning, updating user attributes, and deprovisioning users when they leave the organization. SCIM streamlines identity management, enhances security, and reduces administrative complexity through automated processes.

Accessing SCIM Configuration Settings

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **ACCESS MANAGEMENT**, select **SCIM**. The **Settings :: SCIM** page is displayed with the **SCIM** tab open by default.	1. From the main navigation menu, click **Settings**. 2. On the **Settings** page, from the left menu, select **General** > **SCIM**. The **Settings :: SCIM** page is displayed with the **SCIM** tab open by default.
Note: For more information on how to switch between menus, click here.	

Prerequisites

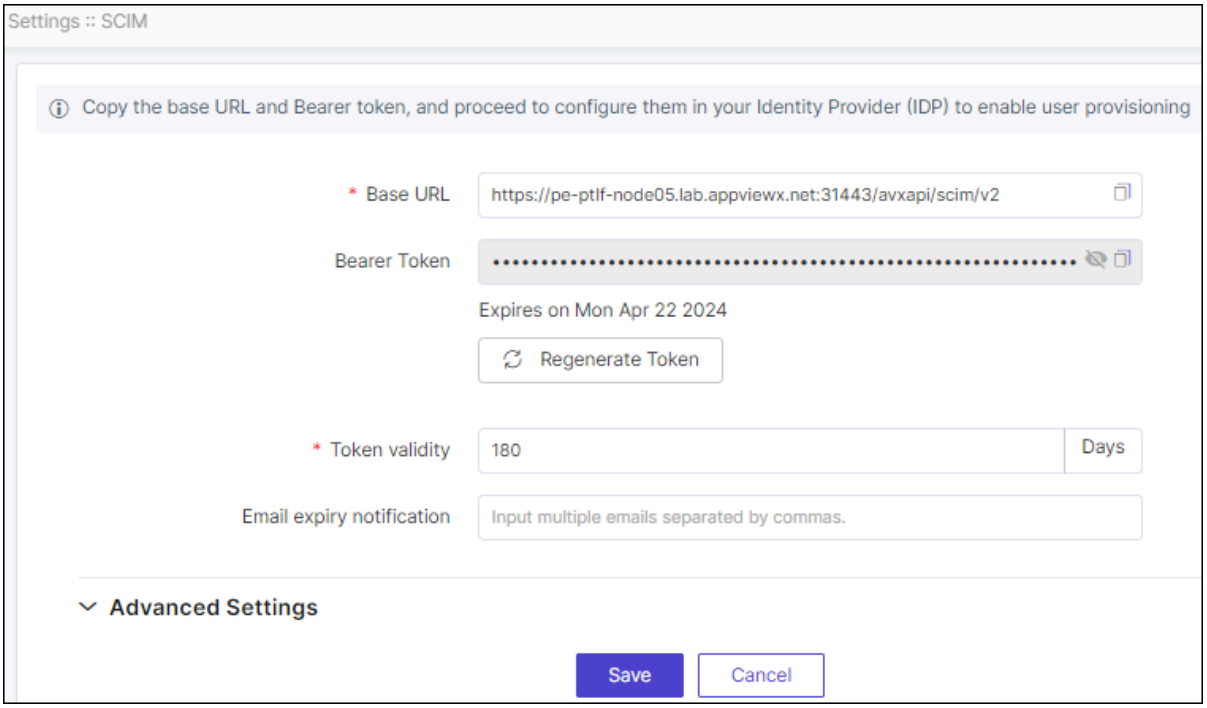
1. Ensure that the SSL certificate for the AppViewX website is sourced from a trusted public Certificate Authority (CA).
2. Verify that the IDP server supports SCIM 2.0.

Configuring SCIM Settings with AppViewX

To configure SCIM settings with AppViewX:

1. On the **Settings :: SCIM** page, Click **Generate Token**.

2. Once the bearer token is generated, the token validity and email expiry notification fields are visible.

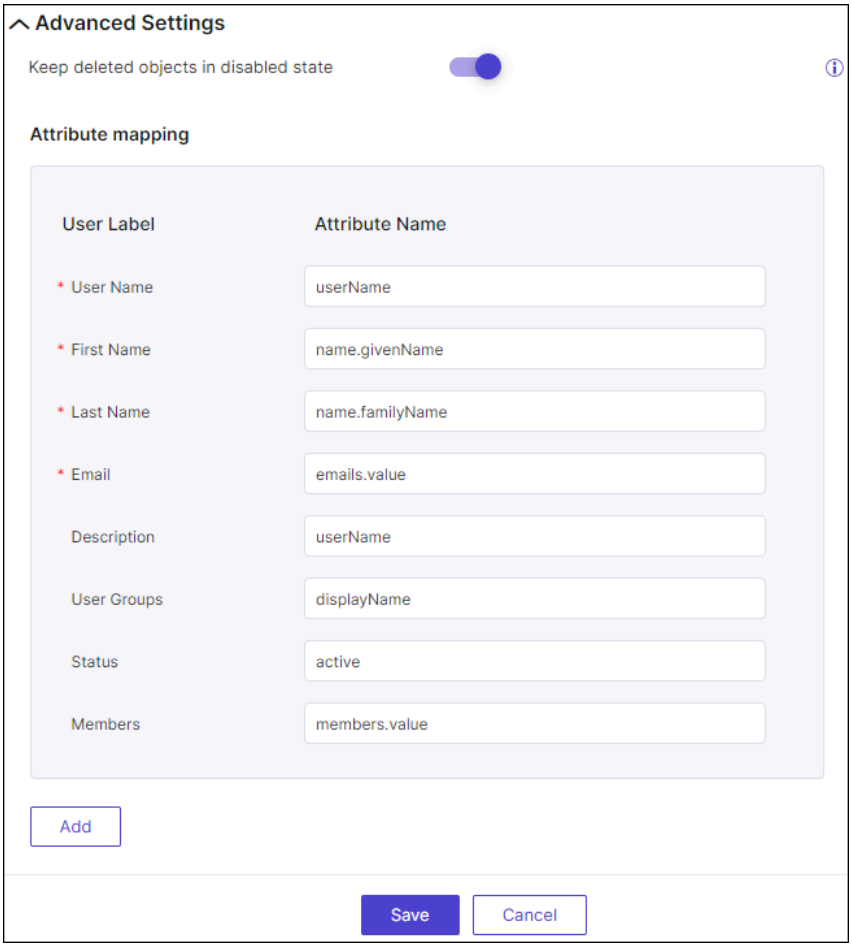


Field descriptions for SCIM

Fields	Description
***Base URL**	The Base URL is visible in this field.
Bearer Token	The generated bearer token is visible in this field. **Note:** The token's expiration date and day are shown below the field, along with the option to Regenerate the token.
***Token Validity**	Enter the validity period of the token in terms of the number of days. **Note:** By default, token validity is 180 days. It is customizable.

Fields	Description
Email expiry notification	To send the email notification for token expiry, enter the email address where the notification should be sent. **Note:** Separate multiple email addresses with a comma.
Note: The asterisk (*) symbol indicates mandatory fields.	

3. Enter the required field information.
4. Under the **Advanced Settings** section, enable the toggle to retain deleted objects in a disabled state. When a user or group is removed from the Identity Provider, instead of immediate deletion, the user or group will transition to a disabled state within AppViewX.
5. In the **Attribute Mapping** section, make the necessary changes to map the claim keys to the AppViewX **User Label** with the **Attribute Name**.



For example:

- An identity provider can send the user login name with the key called userName in the request and another identity provider can send the user login name with the key called upn.
- The administrator can configure or modify the claim setting against the User Name either as userName or upn based on the ID claim response sent by the SCIM vendor.
- Similarly, custom attributes can be configured and additional attributes for the user profile if required. Currently, these custom attributes stored in the user profile will not be shown along with the user profile on the AppViewX web application.

6. Click **Save**.

   Copy the base URL and bearer token, to configure them in your (IDP) to enable user provisioning.

What to do next:

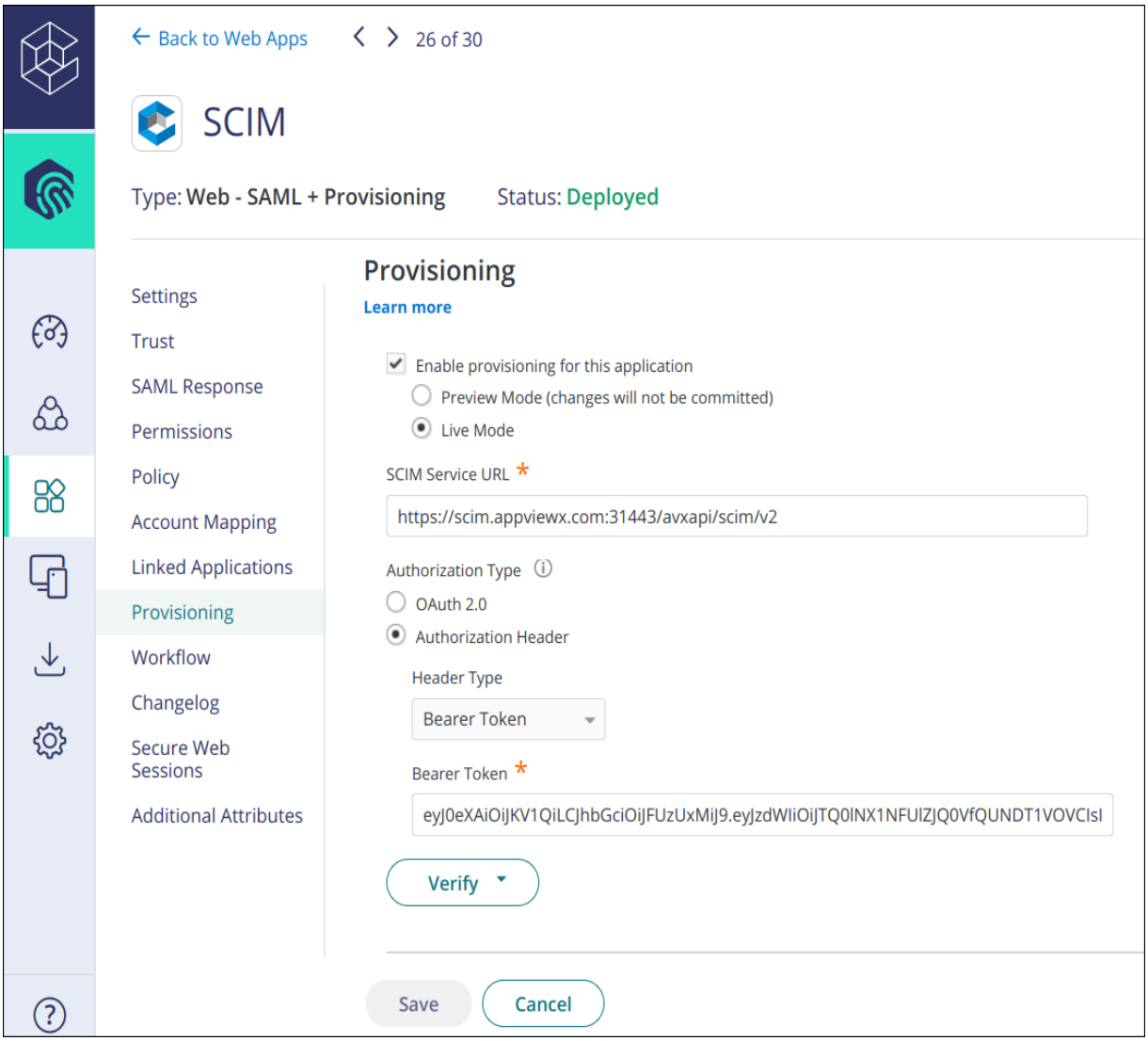
- Configure your (IDP) for SCIM provisioning using **Microsoft Azure** or **CyberArk**.
- Steps to Configure Microsoft Azure
- Steps to Configure CyberArk

Steps to Configure Microsoft Azure

1. Go to **Microsoft Azure** portal, click **Enterprise Applications**.
2. Click **+New Application**.
3. Click +Create your own application.
4. Enter a Name for the application.
5. Select “Integrate any other application you don't find in the gallery (Non-gallery)” and click Create.
6. Under the Manage menu, click **Provisioning**.
7. Upon opening the application, the "Get Started" page will be displayed. Click on "**Get Started**" to proceed.
8. Set Provisioning Mode to Automatic.
9. Enter the **Base URL** that was copied earlier.
10. Enter the **Bearer Token** that was generated earlier.
11. Click **Test Connection** and wait for the message that confirms that the credentials are authorized to enable provisioning.
12. Click **Save**.

Steps to Configure CyberArk

1. On the Identity Administration portal, go to the Provisioning page of your deployed application.

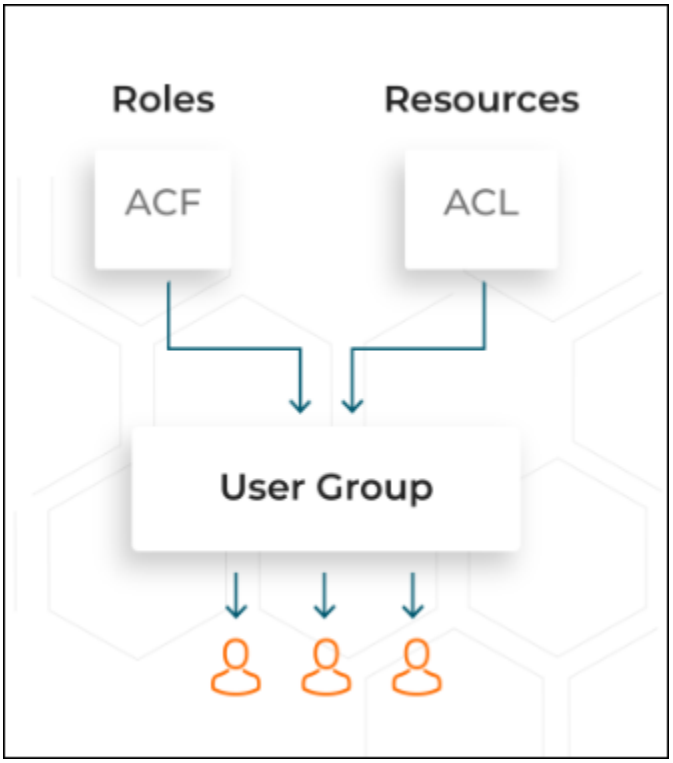


2. Select **Enable provisioning for this application**.
3. Select **Live Mode**.
4. Enter the service provider's SCIM URL for the **SCIM Service URL**.
5. Select **Authorization Type** as **Authorization Header**.
6. Select **Header Type** as **Bearer Token**.
7. Enter the Bearer Token to the Bearer Token field that you generated earlier.
8. Click **Verify** to have CyberArk Identity verify the connection and save the provisioning details.

For more details on steps for Configuring CyberArk.

Configuring Role and Resource-Based Access Control

AppViewX offers comprehensive support for Role and Resource-Based Access Control (RBAC). RBAC is a method of restricting AppViewX functions, network resources that can be managed and monitored in AppViewX based on the roles of individual users within an enterprise. It allows you to integrate with the existing identity stores such as Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) to enforce authorization policies. Roles and Resources can be customized to suit any organizational structure and user requirements.



RBAC lets employees have access rights only to the AppViewX functions and network resources they need to do their jobs and prevents them from accessing information that doesn't pertain to them.

Benefits of RBAC

Using RBAC should improve operational efficiency, enhance compliance, provide administrators increased visibility, reduction in costs, decrease in risk of breaches, and data leakage.

- RBAC: Predefined Roles, Resources, and User Groups
- Managing Users
- Service Accounts
- Managing User Groups
- Managing Roles

- Managing Resource
- RBAC Quick Configuration

RBAC: Predefined Roles, Resources, and User Groups

To expedite the RBAC configuration, AppViewX ships the following set of predefined roles, resources and user groups:

- **CLM Requester**
- **CLM Level 1 Approver**
- **CLM Level 2 Approver**
- **CLM Auditor**

On day 0 of your using the application, these, along with the **superadmin** role, will be available by default for you to map to your users, as well as to clone and/or modify as required.

CLM Requester

- **Role**: Low-level user allowed to submit requests to enroll, renew/regenerate, revoke, push to device, roll back on the resources assigned to the user
- **Resources**: CLM related visual workflows will be mapped and provided with the submit permission for the CLM actions. The default certificate group will be mapped.
- **User Group**: Mapping between the **CLM Requester** role and the **CLM Requestor** resource

Note: Once a request has been submitted, ensure that the requisite approvers are duly informed.

CLM Level 1 Approver

- **Role**: Level 1 approval role for all CLM actions
- **Resources**: CLM related visual workflows will be mapped and provided with the approve permission for CLM actions. The default certificate group will be mapped.
- **User Group**: Mapping between the **CLM Level 1 Approver** role and the **CLM Level 1 Approver** resource

Note: To check requests pending approvals, go to  (**Menu**) > **CERT+** > **Automation** > **My Requests** > **Open**.

Tip: You can also go to the certificate inventory and search for the common name of the certificate that needs to be approved. Click the common name to be redirected to the holistic view of the required certificate.

CLM Level 2 Approver

- **Role**: Level 2 approval role for all CLM actions
- **Resources**: CLM related visual workflows will be mapped and provided with the implement permission for CLM actions. The default certificate group will be mapped.
- **User Group**: Mapping between the **CLM Level 2 Approver** role and the **CLM Level 2 Approver** resource

Note: To check requests pending implementation approvals, go to (**Menu**) > **CERT+** > **Automation** > **My Requests** > **Open**.

Tip: You can also go to the certificate inventory and search for the common name of the certificate that needs to be approved for implementation. Click the common name to be redirected to the holistic view of the required certificate.

CLM Auditor

- **Role**: Auditor role for all CLM actions
- **Resources**: CLM related visual workflows will be mapped and provided with read permission for the CLM actions. The default certificate group will be mapped.
- **User Group**: Mapping between the **CLM Auditor** role and the **CLM Auditor** resource.

Note: To check requests raised/approved/open for approvals, go to (**Menu**) > **CERT+** > **Automation** > **My Requests** > **All**.

• Accessing the Predefined RBAC Configuration

Accessing the Predefined RBAC Configuration

Go to (**Menu**) > **Platform** > **Identity** > **Role**.

The **Role** page is displayed. The predefined roles are listed here.

The subsequent sections cover the instructions for cloning and modifying roles, resources, and user groups.

Managing Users

A user is an individual who has access to AppViewX using a unique username and password maintained internally or by an external enterprise server such as Active Directories (AD).

To create user accounts, you must be assigned the Administrator role. Administrators can define how users should be authenticated to AppViewX. User authentication can either be an internal authentication or external authentication via LDAP, RADIUS, TACACS, and Single Sign-on.

Note: You must add a user to the user group as the roles and resources cannot be directly associated with the user.

Accessing the User Page

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **IDENTITY**, select **User**. The **User** page is displayed, with all the user groups listed with their **Name**, **Full Name**, and other related information.	From the main navigation menu, select **Account** > **User**. The **User** page is displayed, with all the user groups listed with their **Name**, **Full Name**, and other related information.
Note: For more information on how to switch between menus, click here.	

Creating a User

To create a user:

1. On the **User** page, from the top right corner of the screen, click  **(Add)** icon.
   The **Add** page is displayed, with the **Information** tab open by default.
2. In the **Account Information** section, enter the following details:

Field descriptions for Account Information

Field	Description
***User name**	Enter the user name for the new user.
***Password**	Enter the password for the new user. **Note:** The new password should have: • At least one uppercase, lowercase, and numeric character • At least one special character (~!@#$^&*_-+=|()) • 6 to 24 characters. **Note:** The new password should not contain: • The user name • The same character more than three times consecutively • Blank spaces.
***Confirm Password**	Reenter the password for confirmation.
Authenticate externally	To allow authentication by external enterprise servers such as LDAP, TACACS, RADIUS, and so on, select this check box. **Note:** The **Password** and **Confirm Password** fields are disabled if **Authenticate externally** option is selected.
First name	New user's first name.
Last name	New user's last name.
Description	Descriptive information about the user such as their work location, workgroup, specialty, or any other details.

Field	Description
	Note: The asterisk (*) symbol indicates mandatory fields.

3. In the **Contact Information** section, enter the following details:

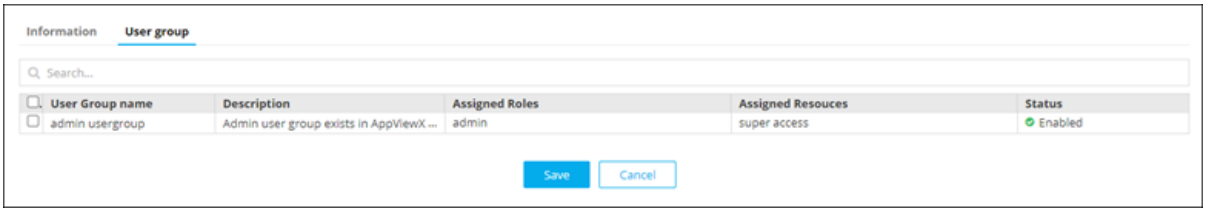
Field descriptions for Contact Information

Field	Description
***Preferred mode of contact**	From the following options, select the user's preferred mode of contact: • Email address • Phone number.
***Email address**	New user's email address.
***Phone number**	New user's phone number. **Note:** This field is required only when the preferred mode of contact is a phone number.
	Note: The asterisk (*) symbol indicates mandatory fields.

4. Click **Save**.

Note: To log into AppViewX and access the product, users need to be assigned or mapped to a user group.

5. To add the user to a group, click the **User group** tab.

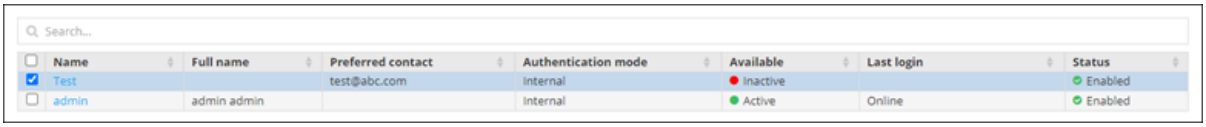


6. To add the user to a group, select the check box for that user group.
7. Click **Save**.

Modifying a User

To modify a user:

1. On the **User** page, select the check box against the user you want to modify.



2. From the top right corner of the screen, click 

(Modify) icon.
3. The **Modify** page is displayed, with the **Information** tab open by default.
4. In the **Account Information** section, update the required details:

Field descriptions for Account Information

Field	Description
***User name**	Enter the user name for the new user.
***Password**	Enter the password for the new user. **Note:** The new password should have: • At least one uppercase, lowercase, and numeric character • At least one special character (~!@#$^&*_-+=|()) • 6 to 24 characters. **Note:** The new password should not contain: • The user name • The same character more than three times consecutively • Blank spaces.
***Confirm Password**	Reenter the password for confirmation.
Authenticate externally	To allow authentication by external enterprise servers such as LDAP, TACACS, RADIUS, and so on, select this check box. **Note:** The **Password** and **Confirm Password** fields are disabled if **Authenticate externally** option is selected.

Field	Description
First name	New user's first name.
Last name	New user's last name.
Description	Descriptive information about the user such as their work location, workgroup, specialty, or any other details.

Note: The asterisk (*) symbol indicates mandatory fields.

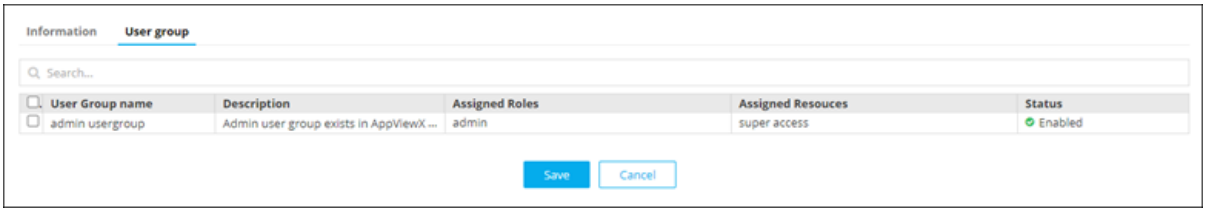
5. In the **Contact information** section, update the required details:

Field descriptions for Contact Information

Field	Description
***Preferred mode of contact**	From the following options, select the user's preferred mode of contact: • Email address • Phone number.
***Email address**	New user's email address.
***Phone number**	New user's phone number. **Note:** This field is mandatory only if the preferred mode of contact is Phone number.

Note: The asterisk (*) symbol indicates mandatory fields.

6. Click **Save**.
7. To modify the user and user group mapping, by adding a new user group/deleting an existing user group, click the **User group** tab.

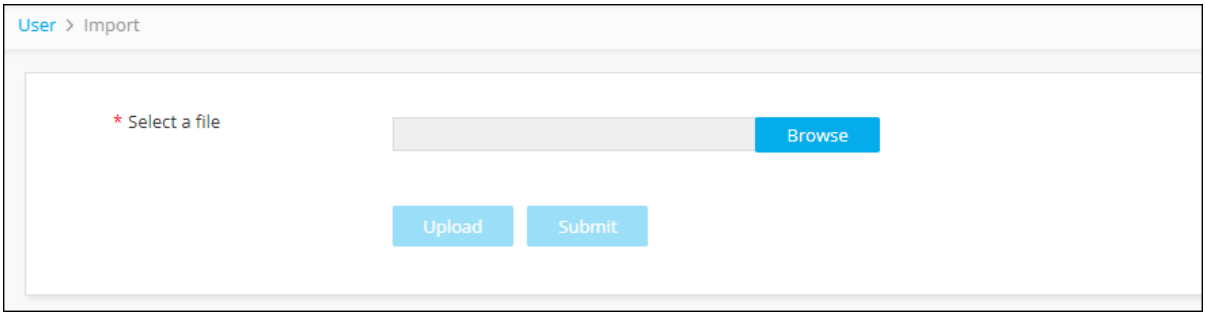


8. To add the user to a group, select the check box for that user group.
9. Click **Save**.

Importing a User

To import users into AppViewX:

1. On the **User** page, from the top right corner of the screen, click  **(Import)** icon.
   The **Import** screen is displayed.



2. Click **Browse**, and then select the user file to upload.

> **Note:** The file must be in .csv format. To download a sample template file click the  icon on the top-right corner.

> **Tip:** The most efficient way to import user details is to download the sample import file that is available by clicking the  (Sample file) icon in the Command bar of the Import screen, modify the contents, save it, and then import it into the system. This reduces the chance of error messages appearing during the import process.

3. Click **Upload** to see the user details displayed in the user interface.

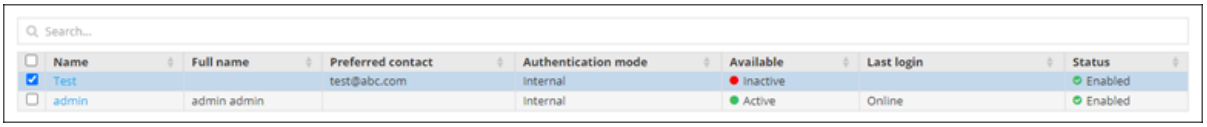
> **Note:** The user details displayed at this point are only for review; the user details have not been imported yet.

4. Review the details of each user in the import file. If you do not want to import specific users, deselect the checkboxes beside their names.
5. Click **Submit**.

Enabling a User

To enable a user:

1. On the **User** page, select the check box against the user you want to enable.



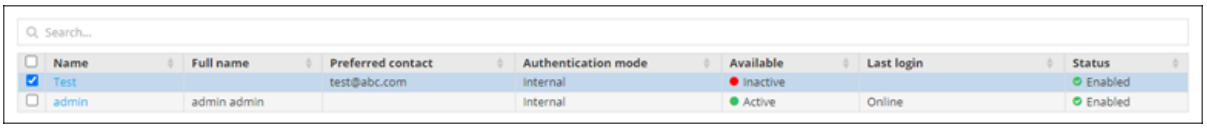
2. From the top right corner of the screen, click ✓ **(Enable)** icon.
3. In the **Confirmation** dialog box, click **Yes**.

   The selected user is enabled.

Disabling a User

To disable a user:

1. On the **User** page, select the check box against the user you want to disable.



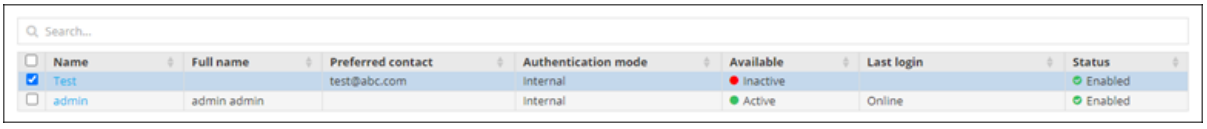
2. From the top right corner of the screen, click ⊘ **(Disable)** icon.
3. In the **Confirmation** dialog box, click **Yes**.

   The selected user is disabled.

Deleting a User

To delete a user:

1. On the **User** page, select the check box against the user you want to delete.



2. From the top right corner of the screen, click 🗑 **(Delete)** icon.
3. In the **Confirmation** dialog box, click **Yes**.

   The selected user is deleted.

Service Accounts

The service account is a special type of account intended to represent a non-human user. API endpoints will be consumed by non-human users. For example, automated applications are used to perform some operations. So, AppViewX introduced a new account type called Service Account. Using this, API endpoints can be accessed using oAuth based authentication.

Accessing the Service Account Page

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **IDENTITY**, select **Service Account**. The **Service Account** page is displayed, with all the service accounts listed with their **Name**, **Client Id**, and other related information.	From the main navigation menu, select **Account** > **Service Account**. The **Service Account** page is displayed, with all the service accounts listed with their **Name**, **Client Id**, and other related information.

Note: For more information on how to switch between menus, click here.

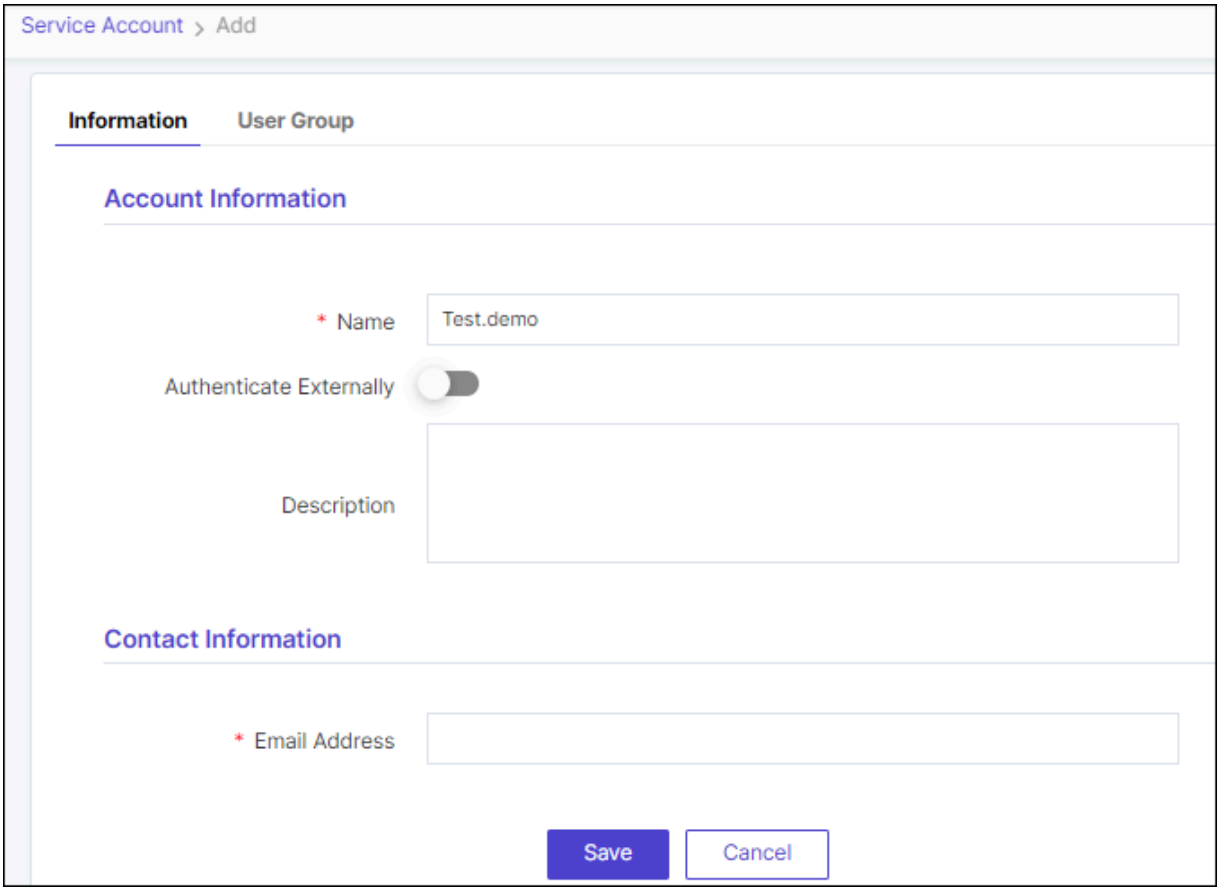
Client Credentials Grant Type

Client Credential Grant type is one of the grant types supported by oAuth 2.0. A Service Account is provided with a Client ID and Client Secret. Then, you can use this Client ID and Client Secret in client applications to get an Access token and perform API actions using the Access Token.

Create Service Account

To add a service account, follow the below steps:

1. Go to the **Service Account** page, click **+ Add Account**.
   The **Service Account > Add** page is displayed.



2. Enter/Select the following details in the **Account Information** section:

Field descriptions for Account Information

Fields	Description
***Name**	Name of service account.
Authenticate Externally	Enable the toggle to authenticate external service account using client Id.

Fields	Description
***Client Id**	**Note:** This field is displayed when **Authenticate Externally** toggle is enabled. Enter the external Client Id for authentication.
Description	Brief description of the service account.
Note: The asterisk (*) symbol indicates mandatory fields.	

3. Enter the **Email Address** details in the **Contact Information** section.

   Note: This section is displayed when **Authenticate Externally** toggle is disabled.

4. Click **Save**.
   The service account is created and included in the service account list.

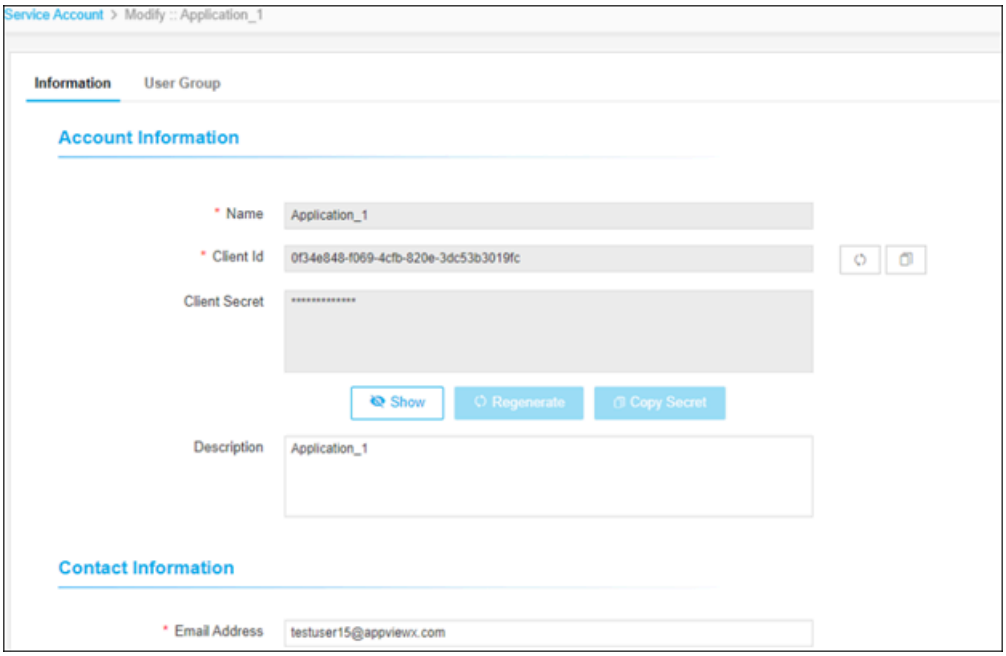
What to do next:

- Assign the necessary user group to the service account manually.

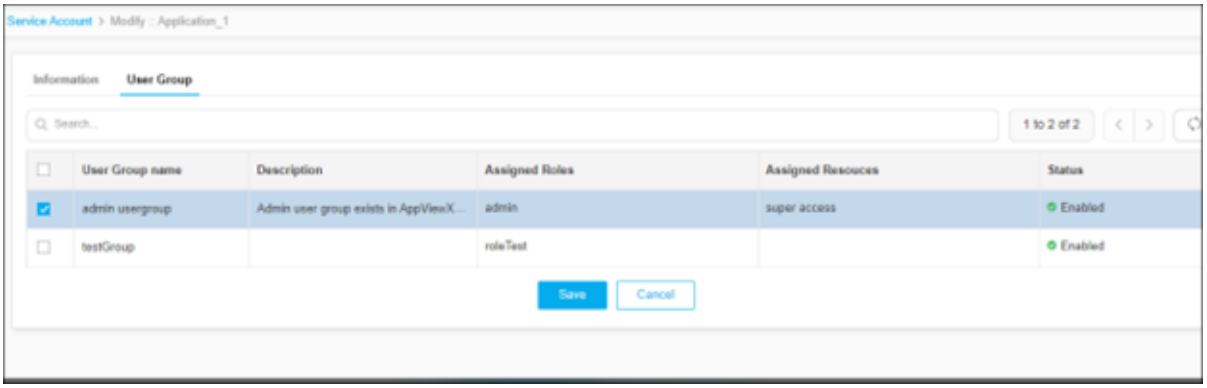
Managing Service Account

To configure managing service accounts, follow the below steps:

1. Go to the **Service Account** page.
   The screenshot below shows an existing Service Account. The secret is hidden by default. The client credentials can be copied using the corresponding copy buttons. The Client ID and Client Secret can be regenerated anytime using the corresponding regenerate buttons. When a Client ID is regenerated, the corresponding Client Secret is also regenerated. The Access tokens generated by the previous set of Client ID and Client Secret will still work until the token gets expired.



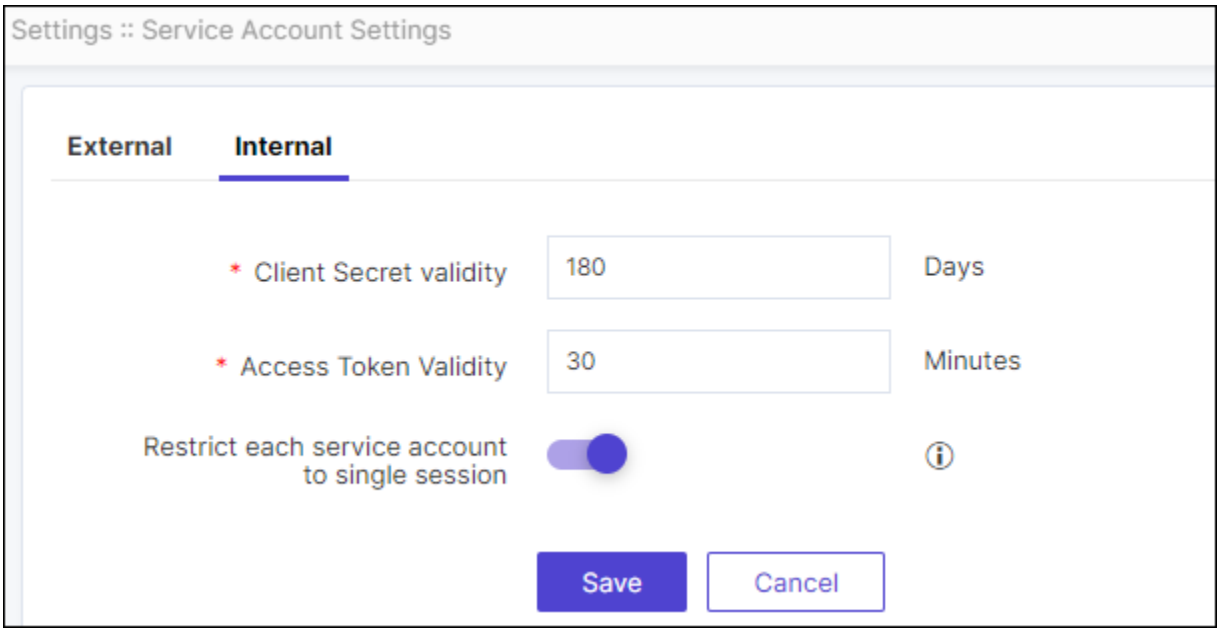
2. To define the access privileges and scope for this service account, assign the required User Groups to this account.



Configuring Internal OAuth Settings

To configure Internal OAuth settings, follow the below steps:

1. On the Settings :: Service Account Settings page, under the **Internal** OAuth Settings tab, enter the required field information.



Field descriptions for Internal OAuth Settings

Field	Description
***Client Secret validity**	Enter the secret validity in the number of days.
***Access Token Validity**	Enter the access token's validity in the number of minutes.
Restrict each service account to single session	Enable the toggle to limit each service account to have only one valid Access token at a time, thereby restricting them to use only one session at a time. **Note:** If the toggle is disabled, then a maximum of 100 Access tokens can be created in parallel for a single service account which allows using multiple sessions in parallel with the same service account.

Field	Description
Note: The asterisk (*) symbol indicates mandatory fields.	

Note: By default, the client secret expires in 180 days, and the access token expires in 30 minutes. It is customizable.

Note: Whenever an Access Token expires, an HTTP Error Code 401 is displayed in the API response. The client application can generate a new Access Token using the Client ID and Client Secret.

Note: When the Client Secret expires, you can regenerate a new Client Secret from AppViewX in **Service Account** > **Account Name** > **Client Secret** > **Regenerate**.

2. Click **Save**.

OAuth

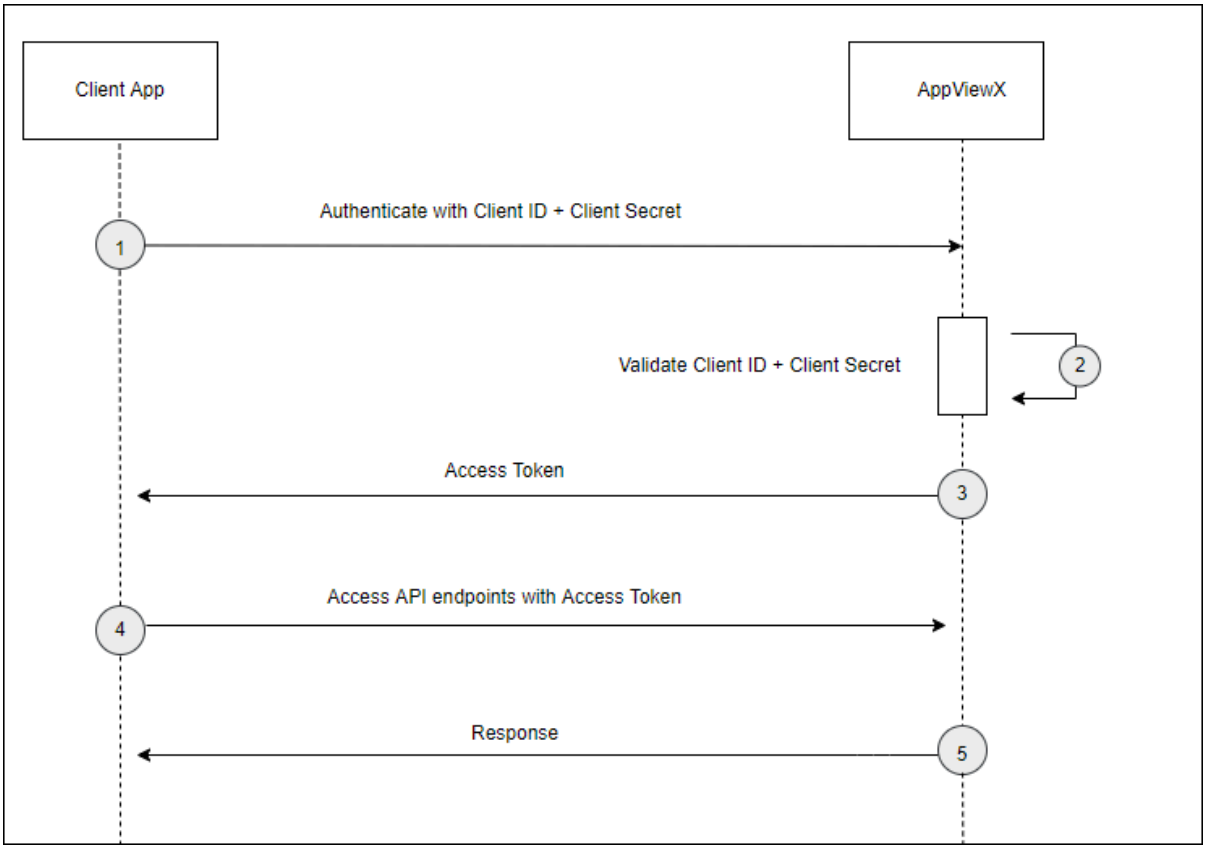
OAuth is a standard that applications can use to provide the client applications with **secure delegated access**. Using OAuth, access to client applications is delegated without sharing the password credentials.

AppViewX can be managed using web console and API endpoints.

To improve the security of the API endpoints access, AppViewX has introduced the oAuth Client Credentials Grant Type.

OAuth Workflow

1. Client application sends a request to the AppViewX server with a Client ID and Client Secret to get the Access Token.



API: acctmgmt-get-service-token

URL: http://localhost:5300/avxapi/acctmgmt-get-service-token?gwsource=web&gwkey=f000ca01

Method: POST

Header:

Basic Authentication : (base64(clientId:clientsecret))

Payload:

```
{
  "payload": {
    "grant_type":"client_credentials"
  }
}
```

2. AppViewX validates the Client ID and the Client Secret.
3. Once the Client ID and the Client Secret are validated by AppViewX, it returns the Access token with the expiry time. This is a JWT token. The client application can decode this JWT token to get all the claims including the expiry time of that token inside the exp claim.

Response:


```
{
"response":
 "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJBcHBsaWNhdGlvbl8xIiwiYXVkIjoiYXZ4IiwiY2xpZW50SWQiOiIwZjM0ZTg0OC1mMDY5LTRjZmItO
DlwZS0zZGM1M2IzMDE5ZmMiLCJpc3MiOiJhdngiLCJleHAiOjE2NDMxMDc3OTQsImdyYW50IHR5cGUiOiJjbGllbnRfY3JlZGVudGlhbHMifQ.EC6my35MCU
sMVC0gsylFqWVzqjgs5Js87Owf1esoano",
"message": null,
"appStatusCode": null,
"tags": null,
"headers": null
}
```

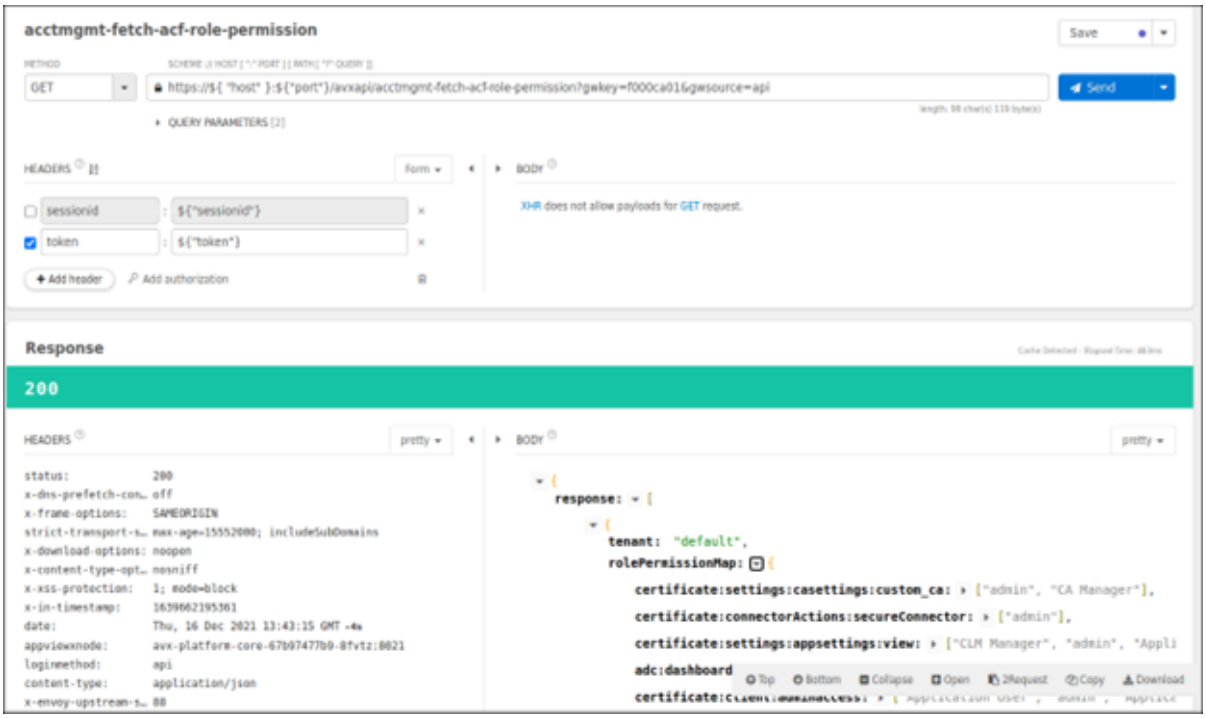

Access Token JWT Claims:


```
 "sub": "Application_1",
 "aud": "avx",
 "clientId": "0f34e848-f069-4cfb-820e-3dc53b3019fc",
 "iss": "avx",
 "exp": 1643107794,
 "grant type": "client_credentials"
}
```


4. The client application then accesses the API endpoints with the access token in the **“token”** header of the API. AppViewX provides the response.

Example

Refer to the below sample screenshot for reference.



Managing User Groups

A user group is a set of individual users assigned with the same roles and resources. You can associate one or more roles and resources to a user group. Users within that user group are granted the role and resource permissions.

Note: You can associate roles and resources only with user groups.

- Accessing the User group Page
- Creating a User Group
- Cloning a User Group
- Modifying a User Group
- Enabling a User Group
- Disabling a User Group
- Deleting a User Group

Accessing the User group Page

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **IDENTITY**, select **User group**. The **User Group** page is displayed, with all the user groups listed with their **Name**, **Description**, and other related information.	From the main navigation menu, select **Account** > **User group**. The **User Group** page is displayed, with all the user groups listed with their **Name**, **Description**, and other related information.
Note: For more information on how to switch between menus, click here.	

Creating a User Group

To create a user group:

1. On the User group page, from the top right corner of the screen, click 

(Add) icon.
2. The **Add** page is displayed with the **Information** tab open by default.

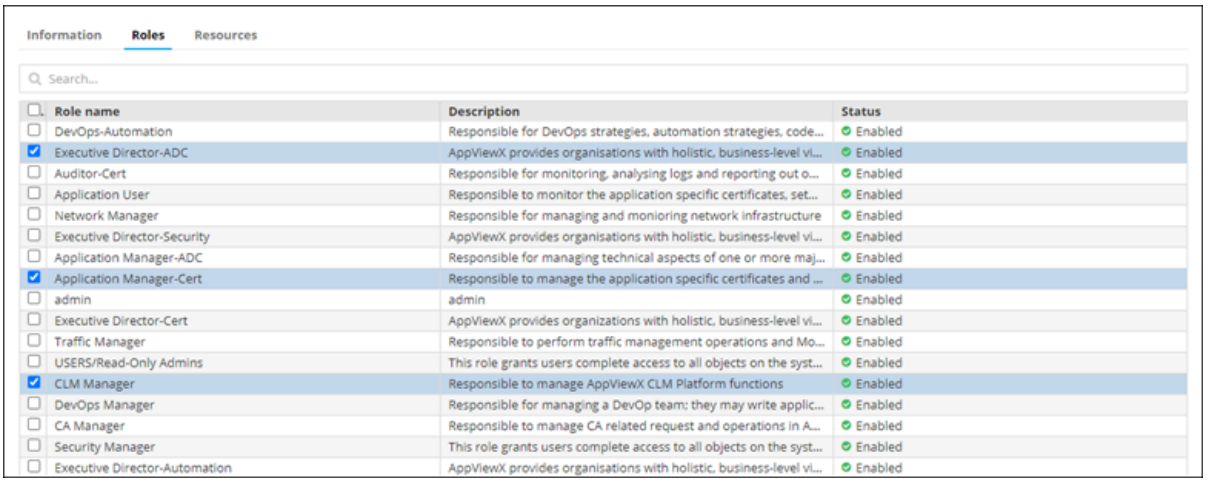
3. Enter the following details:

Field descriptions for Information

Field	Description
***Name**	User group name.
Description	Brief description of the group (which makes it easy for the administrators to decide if a user should be assigned to this group or not).

Field	Description
	Note: The asterisk (*) symbol indicates mandatory fields.

4. Click **Save**.
5. To assign roles to this user group, in the **Roles** tab, select the check boxes against the required roles.



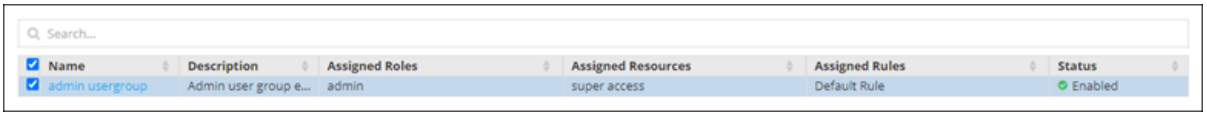
Note: A user group can be assigned to more than one role and resource in the system. A user assigned to a user group with more than one role or resource has all of the permissions of all of the roles and resources to which he or she is assigned. If one resource has only Read access to a component and another resource has Read/Write access to the same component, the higher-level access permissions (Read/Write) take precedence and the user has Read/Write access.

Note: Admins who associate User Groups to Roles and Resources may skip/forget to associate User Groups to a user. To overcome this, an alert icon has been added to the User Group inventory to notify if the group is not associated with a role, resource, or both.

Cloning a User Group

To clone a user group:

1. On the User group page, select the user group you want to clone.



2. From the top right corner of the screen, click 

(Clone) icon.
3. The **Cloning** page is displayed, with the **Information** tab open by default. Update the required details.

Field descriptions for Information

Field	Description
***Name**	User group name.
Description	Brief description of the group (which makes it easy for the administrators to decide if a user should be assigned to this group or not).

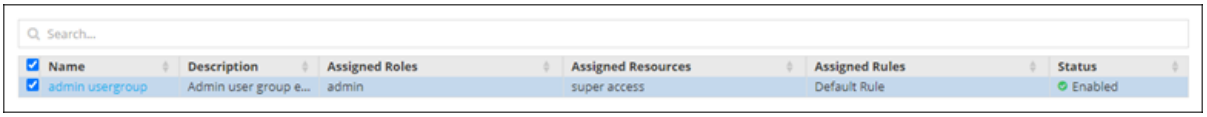
Note: The asterisk (*) symbol indicates mandatory fields.

4. Click **Save**.

Modifying a User Group

To create a user group:

1. On the User group page, select the user group you want to modify.



2. From the top right corner of the screen, click 

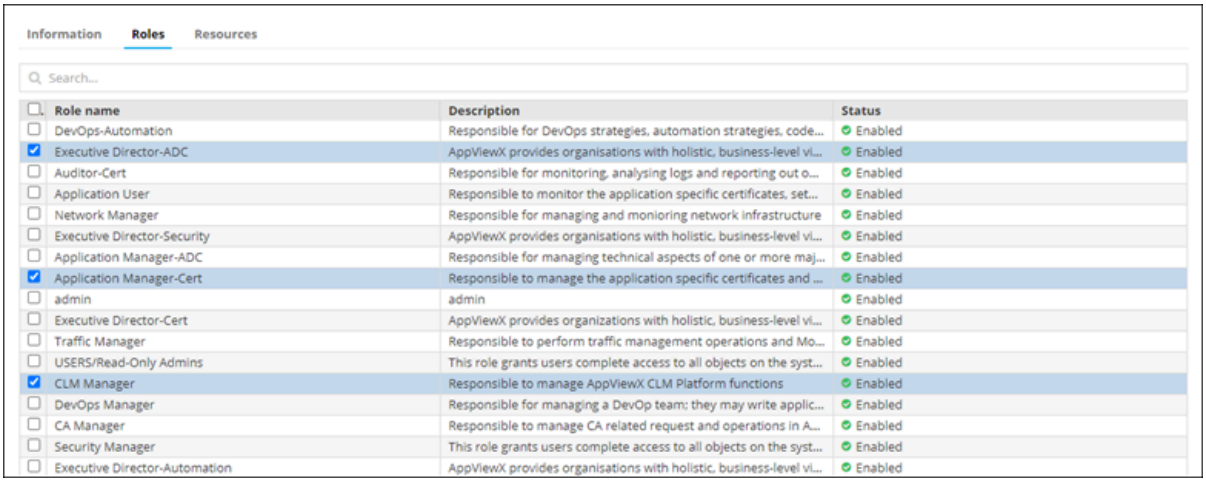
(Modify) icon.
3. The **Modify** page is displayed, with the **Information** tab open by default. Update the required details.

Field descriptions for Information

Field	Description
***Name**	User group name.
Description	Brief description of the group (which makes it easy for the administrators to decide if a user should be assigned to this group or not).

Note: The asterisk (*) symbol indicates mandatory fields.

4. Click **Save**.
5. To modify the role assignment for this user group, in the **Roles** tab, select/clear the check boxes against the required roles and resources

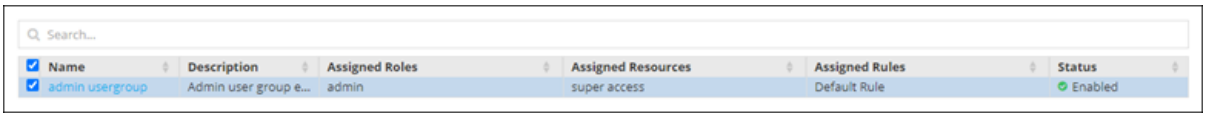


.

Enabling a User Group

To enable a user group:

1. On the User group page, select the user group you want to enable.

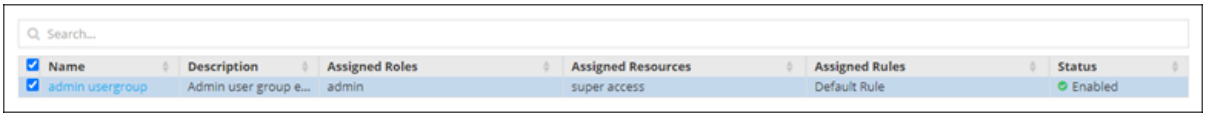


2. From the top right corner of the screen, click ✓ **(Enable)** icon.
3. In the **Confirmation** dialog box, click **Yes**.

Disabling a User Group

To disable a user group:

1. On the User group page, select the user group you want to disable.

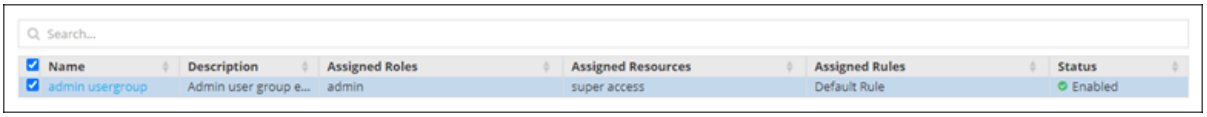


2. From the top right corner of the screen, click ⊘ **(Disable)** icon.
3. In the **Confirmation** dialog box, click **Yes**.

Deleting a User Group

To delete a user group:

1. On the User group page, select the user group you want to delete.



2. From the top right corner of the screen, click 🗑 **(Delete)** icon.
3. In the **Confirmation** dialog box, click **Yes**.

Managing Roles

A set of permissions to execute specific tasks in the application is termed as Roles in AppViewX. Roles can be assigned only to a user group. Users within user groups will inherit role permissions assigned to that group. User groups can be assigned more than one role. A default set of roles is available within the application as per the industry standards.

Accessing the Role Page

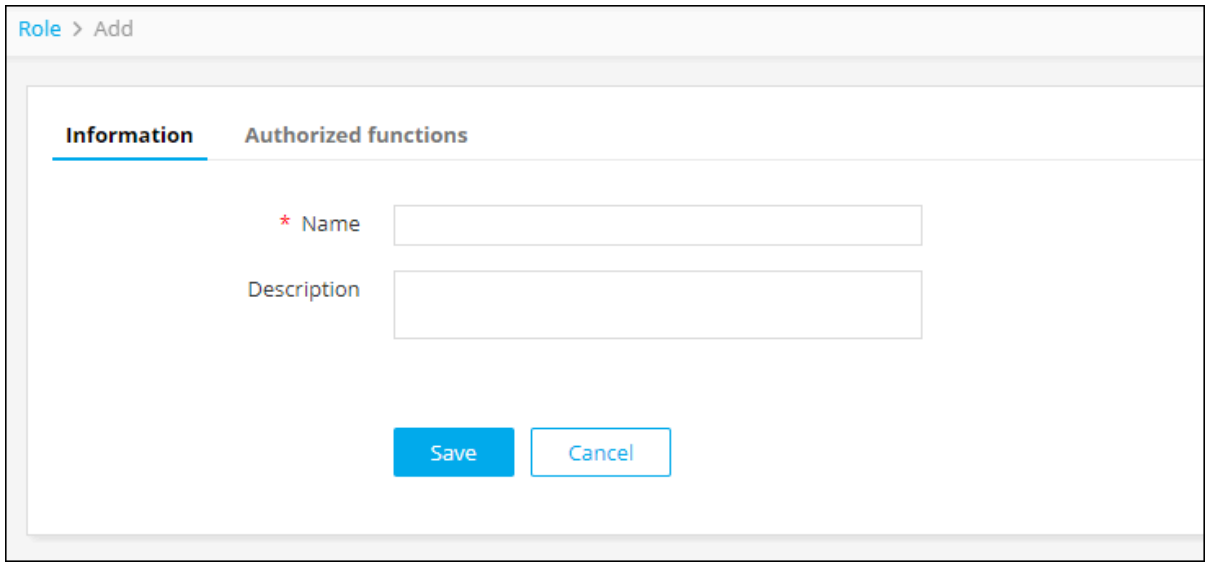
New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **IDENTITY**, select **Role**. The **Role** page is displayed, with all the roles listed with their **Name**, **Description**, and **Status**.	From the main navigation menu, select **Account** > **Role**. The **Role** page is displayed, with all the roles listed with their **Name**, **Description**, and **Status**.

Note: For more information on how to switch between menus, click here.

Creating a Role

To create a role:

1. On the Role page, from the top right corner of the screen, click  **(Add)** icon.
   The **Add** page is displayed.



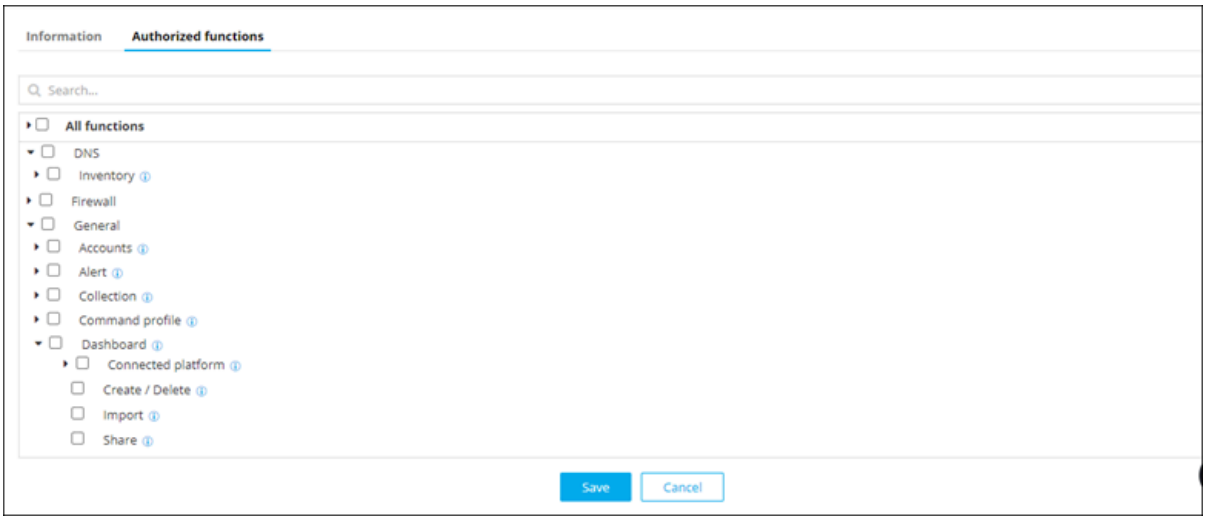
2. Under the **Information** tab, enter the following details:

Field descriptions for Information

Field	Description
***Name**	Name of the role.
Description	Role/features/functionalities associated with the role.

Note: The asterisk (*) symbol indicates mandatory fields.

3. Click **Save**.
4. In the **Authorized functions** section, select the checkbox beside the functionalities that you want to associate with the role.
5. To assign functions at a granular level, click the icon for the functions' check box and then select individual sub-options within the functions.



6. Click **Save**.

   Details of the new role are displayed in the list on the **Role** page.

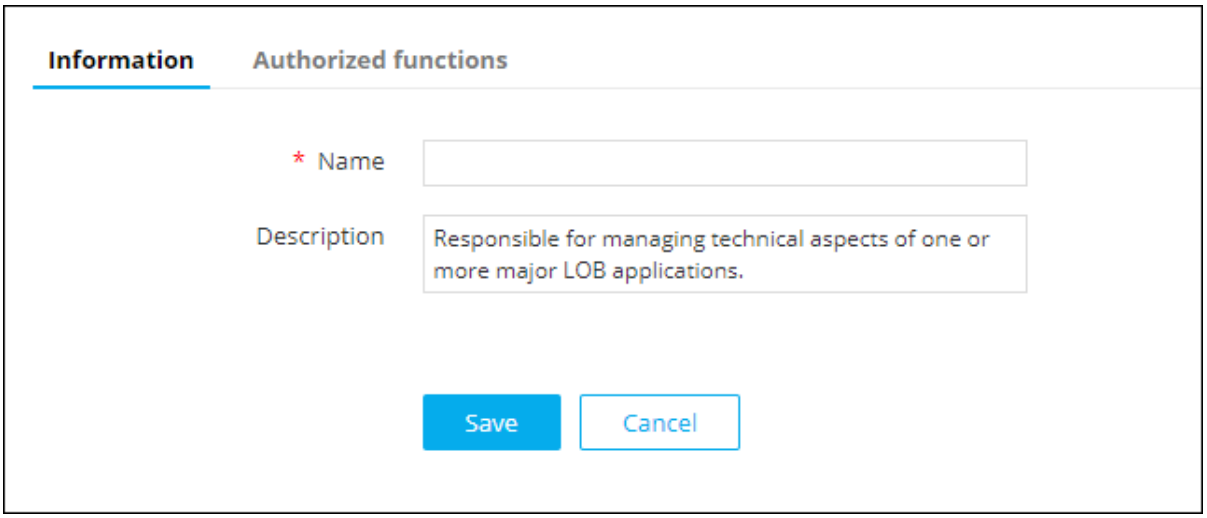
Cloning a Role

Cloning lets you create a copy of an existing role with a different name. You can modify the permissions and tasks that can be performed while cloning a role.

To clone a role:

1. On the Role page, for the role you want to clone, select the corresponding check box.
2. From the top right corner of the screen, click 

(Clone) icon.
3. In the **Information** section, enter a new **Name** for the role.



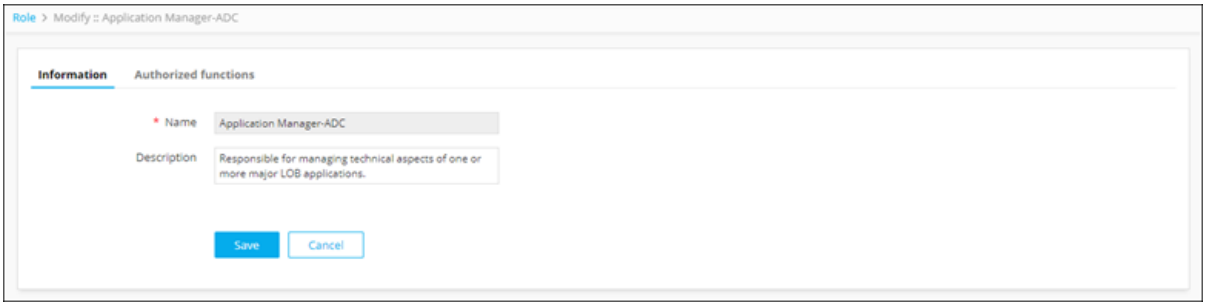
4. Click **Save**.
   The selected role is cloned.

Modifying a Role

To modify a role:

1. On the Role page, from the top right corner of the screen, click 

(Modify) icon.
2. The **Modify :: Application Manager-ADC** page is displayed (because we selected the Application Manager role).
3. Modify the details in the **Information** and **Authorized functions** as required.



4. Click **Save**.
   The selected role is modified.

Enabling a Role

To enable a role:

1. On the Role page, for the role you want to enable, select the corresponding check box.
2. From the top right corner of the screen, click ✓ **(Enable)** icon.
3. In the **Confirmation** dialog box, click **Yes**.
   The selected role is enabled.

Disabling a Role

To disable a role:

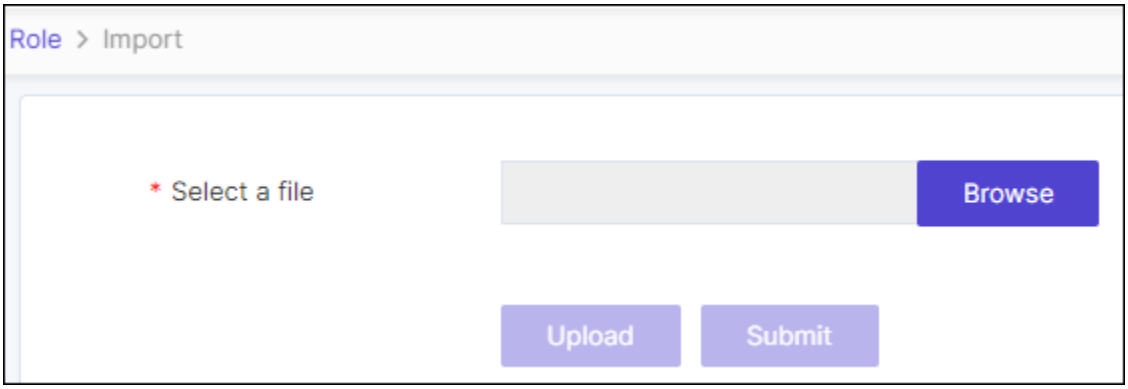
1. On the Role page, for the (enabled) role you want to disable, select the corresponding check box.
2. From the top right corner of the screen, click ⃠ **(Disable)** icon.

3. In the **Confirmation** dialog box, click **Yes**.
   The selected role is disabled.

Importing Roles

To import a role:

1. On the Role page, from the top right corner of the screen, click  **(Import)** icon.
   The **Import** page is displayed.

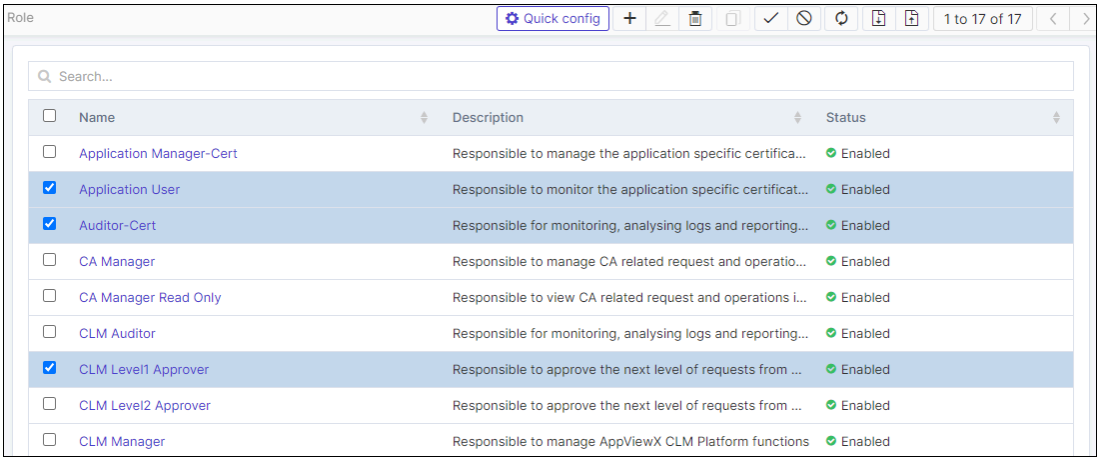


2. Click **Browse**.
   Choose the .csv file for import.
3. Click **Upload**.
   The imported file will be displayed in the list below.
4. Click **Submit**.
   The Role page displays the details of the imported role in the list.

Exporting Roles

To export a role:

1. On the Role page, choose the roles that need to be exported.



Note: The export roles functionality allows exporting a maximum of ten roles at a time.

2. From the top right corner of the screen, click **(Export)** icon.
   Selected roles will be exported in .csv format.

Deleting a Role

Note: A role that has active users belonging to it cannot be deleted.

To delete a role:

1. On the Role page, for the role you want to delete, select the corresponding check box.
2. From the top right corner of the screen, click **(Delete)** icon.
3. In the **Confirmation** dialog box, click **Yes**.
   The selected role is deleted.

Managing Resource

All the devices and objects that are configured within AppViewX are termed as Resources. The resource allows you to specify access at a granular level across all the devices and modules of AppViewX. Resources can be assigned to a user group. Users within a user group will inherit resources assigned to that group. User groups can be assigned more than a resource. To enforce authorization policies on object levels such as for devices, certificates, and sub-objects such as wide-IP, virtual server, and so on

users can configure resources and restrict user access to specific resources by mapping the resources to the respective user groups.

Accessing the Resource Page

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **IDENTITY**, select **Resource**. The **Resource** page is displayed, with all the resource listed with their **Name**, **Description**, and **Status**.	From the main navigation menu, select **Account** > **Resource**. The **Resource** page is displayed, with all the resource listed with their **Name**, **Description**, and **Status**.

Note: For more information on how to switch between menus, click here.

Create a Resource

To create a resource:

1. On the Resource page, from the top right corner of the screen, click 

(Add) icon.
   The **Add** page is displayed.
2. The following table describes the options available on the Add page:

Field	Description
* **Name**	Enter the name of the resource.

Field	Description
Description	Enter a brief description of the resource and granular-level access associated with the resource. (You can enter a maximum of 255 words in the field.)
*: *Mandatory fields*	

3. Click **Save**.
   The pop-up message is displayed as **Resource added successfully**.
4. Click **Access control** to associate the required resources and to provide permission.
   The **Access control** tab lists the categories that can be controlled by RBAC using resources.
5. From the **List** pane, select one of the required resources. The available resources are,
   a. Cloud
   b. Application Security Policy
   c. Proxy List
   d. Device (to filter and select the devices that need to be assigned to a resource, click the icon.)
   e. ADC (to filter the ADC objects that need to be assigned to the resource, click the icon.)
   f. Certificate
   g. SSH Key Groups
   h. SSH Infra Access Groups
   i. Command Session Control
   j. Workflow Studio
   k. Workflow Requests.

Note: AppViewX is packaged with default certificate groups (Certificate-Gateway and Default).

   The items of the selected resource is displayed on the right with a checkbox for each.
6. To associate the items to the resource and assign permission, first select the checkbox, then
   a. Click R (Read-only) to assign read-only permissions.
   b. Click RW (Read and Write) to assign read and write permissions.
   c.

Note: On clicking R or RW the item is associated with the resource. Provide RW (Read and Write) permission for the resource associate with the root user and R (Read-only) for others.

7. Use regular expression (regex) to identify and associate the items to the resource:
   a. Enter the **regex** in the Search field. For example, enter CA in the search field and click **R or RW** to assign Read-only or Read and Write permission respectively.
   b. Click the **Add as regex** button. All the certificate groups that match the regex will auto associate to the resource with the relevant permission. For example, all the certificate groups with CA in their name, such as CA-Digicert, CA-Entrust, CA-Sectigo will auto associate to the resource with R read permission.
   c. One or more than one regex can be added.

   Note: The purpose of the regex is, the search string continues to work in the background and auto-associate all the new certificate groups to the resource when the certificate group matches the regex you created.

8. Click **Save**.

Modify a Resource

To modify Read (R) and Read/Write (R/W) permissions of devices, device objects, certificate groups, provisioning requests, or provisioning templates associated with a resource, modify a resource.

1. Navigate to the Resource page.
   The Resource inventory page is displayed.
2. In the resource inventory, select the check box against the resource you want to modify.
   The options on the top menu are enabled.
3. Click  **(Modify)** icon.
   The **Information** tab is displayed.
4. Click the **Access control tab** to add/ remove the items from the resource.
5. Click the respective resource in the left pane.
   The list of items is displayed on the right with the checkboxes and the R or RW options enabled/ disabled for the items .

   Note: You can also modify Read (R) and Read/Write (RW) permissions associated with a resource.

6. Select the check box against the items you want to add to associate the items to the resource OR if the checkbox is already selected, uncheck the item to remove the association.

a. Click **R (Read-only)** to assign read-only permissions.
b. Click **RW (Read and Write)** to assign read and write permissions.

7. Click **Save**.

Delete a Resource

To delete a resource:

1. Navigate to the Resource page.
   The Resource inventory page is displayed.
2. In the resource inventory, select the check box against the resource you want to delete.
   The options on the top menu are enabled.
3. Click the  **(Delete)** icon.
   A confirmation pop-up window is displayed with Are you sure you want to delete? with the **Yes** and **No** buttons.
4. Click **Yes.**
   The resource is deleted and a pop-up message is displayed Operation performed successfully.

Clone a Resource

Clone allows you to create an exact copy of an existing resource with all the access control permissions.

To clone a resource:

1. Navigate to the Resource page.
   The Resource inventory page is displayed.
2. In the resource inventory, select the check box against the resource you want to clone.
   The options on the top menu are enabled.
3. Click the  **(Clone)** icon.
   The **Information** tab is displayed.
4. The following table describes the options available on the Cloning page:

Field	Description
* **Name**	Enter the name of the resource.
Description	Enter a brief description of the resource and granular-level access associated with the resource. (You can enter a maximum of 255 words in the field.)

Field	Description
Note: The asterisk (*) symbol indicates a mandatory field.	

5. Click **Save**.
   The resource is cloned and a pop-up message is displayed as Resources has been cloned successfully.
6. Click the **Access control tab** to add/remove the items from the resource.
7. Click the respective resource in the left pane.
   The list of items is displayed on the right with the checkboxes and the R or RW options enabled/ disabled for the items .
8. Select the check box against the items you want to add to associate the items to the resource OR if the checkbox is already selected, uncheck the item to remove the association.
   a. Click **R (Read-only)** to assign read-only permissions.
   b. Click **RW (Read and Write)** to assign read and write permissions.
9. Click **Save**.

Enable a Resource

To enable a resource:

1. Navigate to the Resource page.
   The Resource inventory page is displayed.
2. In the resource inventory, select the check box against the resource with **Status** as **Disabled**.
   The options on the top menu are enabled.
3. Click the  **(Enable)** icon.
   A confirmation pop-up window is displayed with Confirm enable with the **Yes** and **No** buttons.
4. Click **Yes**.
   The resource is enabled and a confirmation message displays as **Operation performed successfully**.

Disable a Resource

To disable a resource:

1. Navigate to the Resource page.
   The Resource inventory page is displayed.
2. In the resource inventory, select the check box against the resource with **Status** as **Enabled**.

The options on the top menu are enabled.

3. Click the  **(Disable)** icon.
   A confirmation pop-up window is displayed with Confirm disable with the **Yes** and **No** buttons.
4. Click **Yes**.
   The resource is disabled and a confirmation message displays as **Operation performed successfully**.

RBAC Quick Configuration

Simplified RBAC Configuration in AppViewX

To simplify existing RBAC Configuration in AppViewX for the Account Administrator, the Quick Config wizard flow option has been introduced in the existing Authentication, User groups, Roles and Resources. Using the Quick Config option, users should be able to perform all the following actions in the same wizard flow:

- Configure external authentication or single-sign-on for users to log in to AppViewX
- Add users groups into AppViewX by pulling specific user groups from AD into AppViewX based on specific patterns/keywords/codes and support Bulk Export/Import option to onboard user groups
- Pre-packaged roles for ADC, Cert, Security, and Automation modules to assign permissions to user groups
- Simplifying custom role creation by providing information help against each ACF explaining the significance of the functionality
- Dynamic rule-based resource tagging of newly discovered ADC objects, Certificates based on Query or using a script and assigning permissions to user groups dynamically.

- Accessing Quick Config Settings
- Authentication
- Resource
- Role
- User Group

Accessing Quick Config Settings

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **ACCESS MANAGEMENT**, select **Quick Config**. The **RBAC Journey :: Authentication** page is displayed with the **LDAP** tab open by default.	1. From the main navigation menu, click **Settings**. 2. On the **Settings** page, from the left menu, select **General** > **Authentication**. The **Settings :: Authentication** page is displayed with the **LDAP** tab open by default. 3. From the top right corner of the screen, click **Quick Config**. The **RBAC Journey :: Authentication** page is displayed with the **LDAP** tab open by default.
Note: For more information on how to switch between menus, click here.	

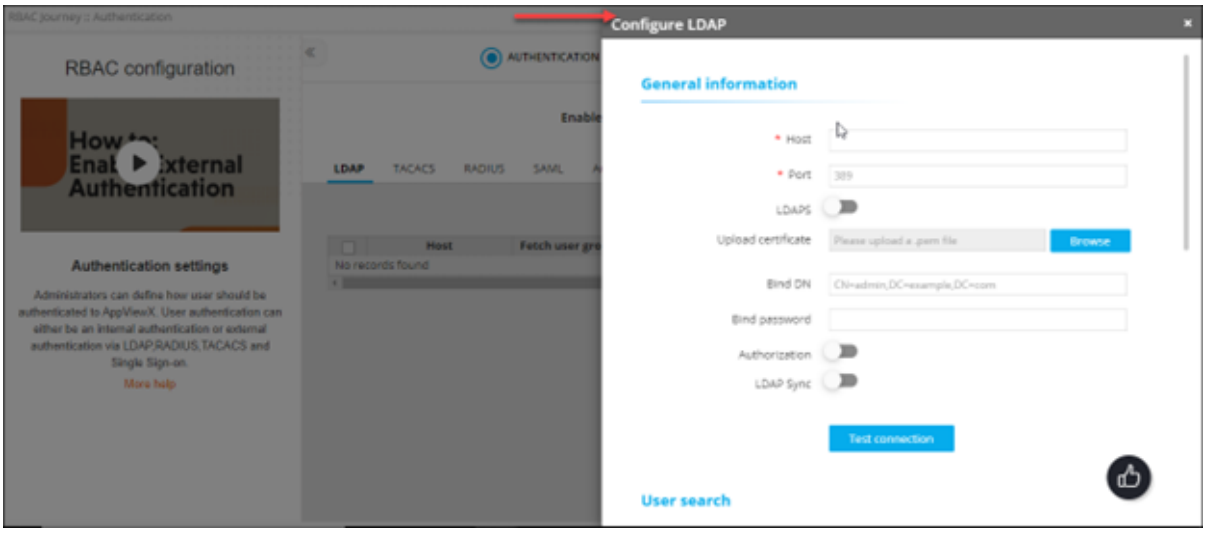
Authentication

- Configure the Role-Based Access Control for LDAP
- Configuring Role-Based Access Control for TACACS
- Configuring Role-Based Access Control for RADIUS
- Configuring Single Sign On Settings with AppViewX
- Configuring Authentication Settings RBAC quick config

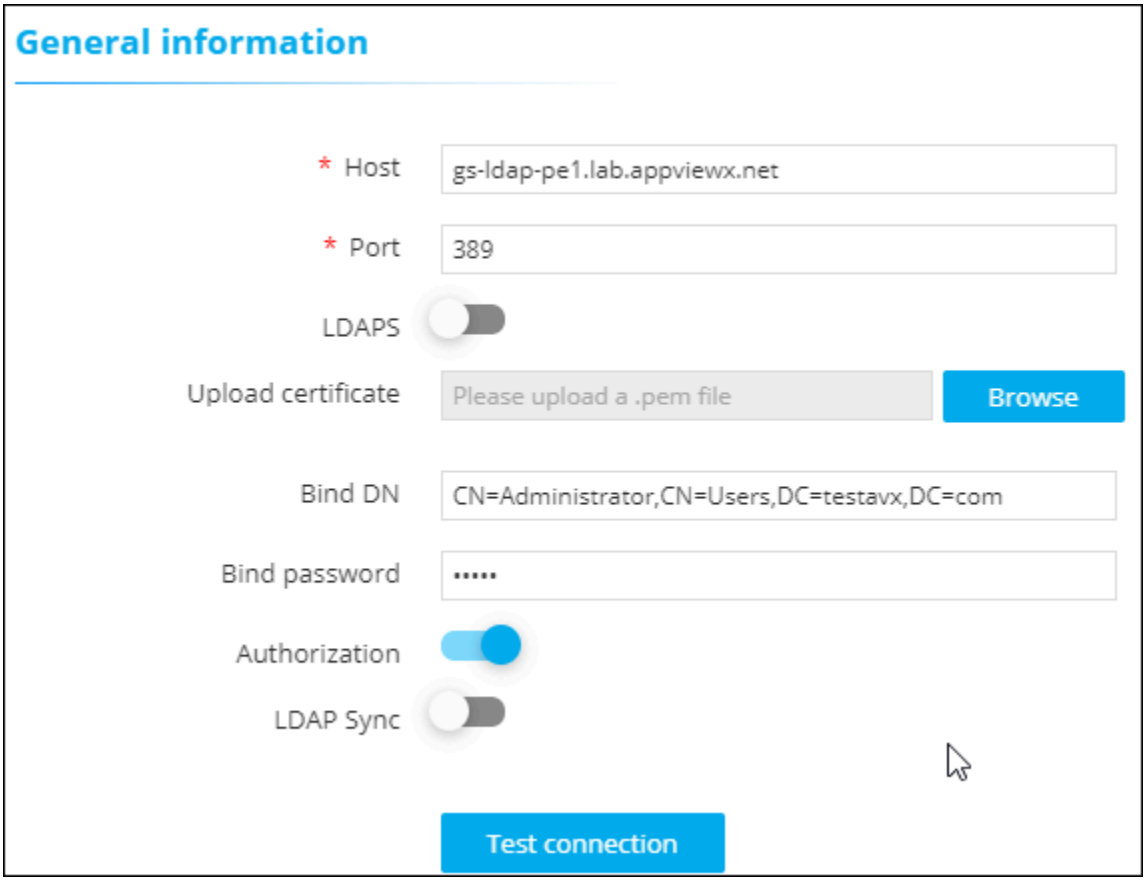
Configure the Role-Based Access Control for LDAP

To configure the RBAC settings for LDAP:

1. On the **RBAC Journey :: Authentication** page, click **Configure LDAP**.
   The **Configure LDAP** action pane is displayed.



2. In the **General Information** section, enter the following details (sample values are shown in the image).



Field descriptions for General Information

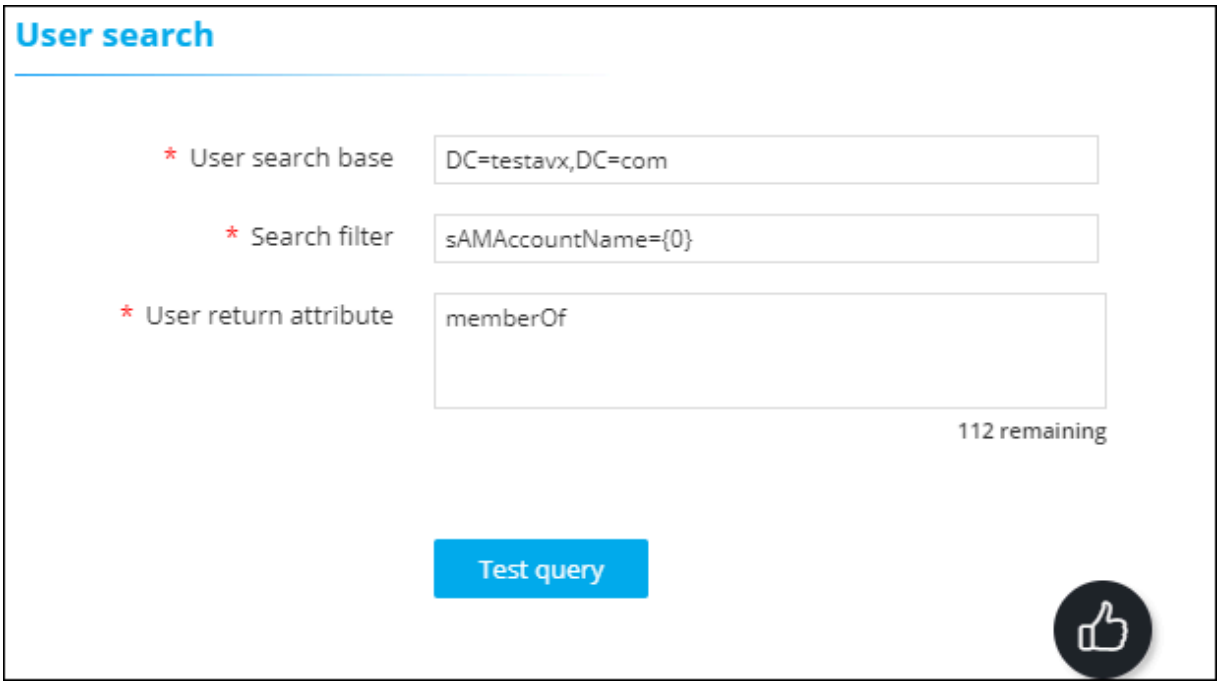
Field	Description
***Host**	Host name (domain name) of the LDAP server.
Port	Port number of the LDAP server. **Note:** This value is entered based on the port number used in your deployment. By default, port number **389** is used for a LDAP configuration and port number 636 is used for a LDAPS configuration.
LDAP	The LDAPS protocol is used for secure communication between AppViewX and Active Directory/Open LDAP. To enable use of the LDAPS protocol authentication, instead of the LDAP protocol, turn on this toggle.
Upload certificate	**Note:** This field is enabled only when the **LDAPS** is enabled. To upload a LDAP server certificate: a. Click **Browse Certificate**. b. Navigate to the location of the **.pem** certificate file. **Note:** If the LDAP servers are load balanced with VIP, upload the root certificate of the LDAP server instead of the server certificate. c. Select the certificate to be uploaded and click **Open**. The selected certificate is uploaded. **Note:** Only a single certificate can be uploaded for each server.
Bind DN	Username of the base authentication endpoint that will be used to connect to LDAP.
Bind Password	The password of the base authentication endpoint that will be used to connect to LDAP.

Field	Description
Authorization	To check user permissions at the time of authentication, select this check box. In addition to authentication, AppViewX also lets you perform user authorization against the LDAP server. To enable authorization along with authentication, select this check box. **Note:** If Authorization is not enabled, AppViewX will only carry out LDAP authentication for the given user.
LDAP Sync	To enable the use of the SSH module in AppViewX for SSH key discovery use case, turn on this toggle.
Note: The asterisk (*) symbol indicates mandatory fields.	

3. After entering the above connection details, to test if the host is reachable and the port is valid for establishing an LDAP/LDAPS connection, click **Test Connection**.

Note: You can test the connection of LDAPS only when you save all of the configuration details. Bind DN and Bind password details cannot be validated through a test connection.

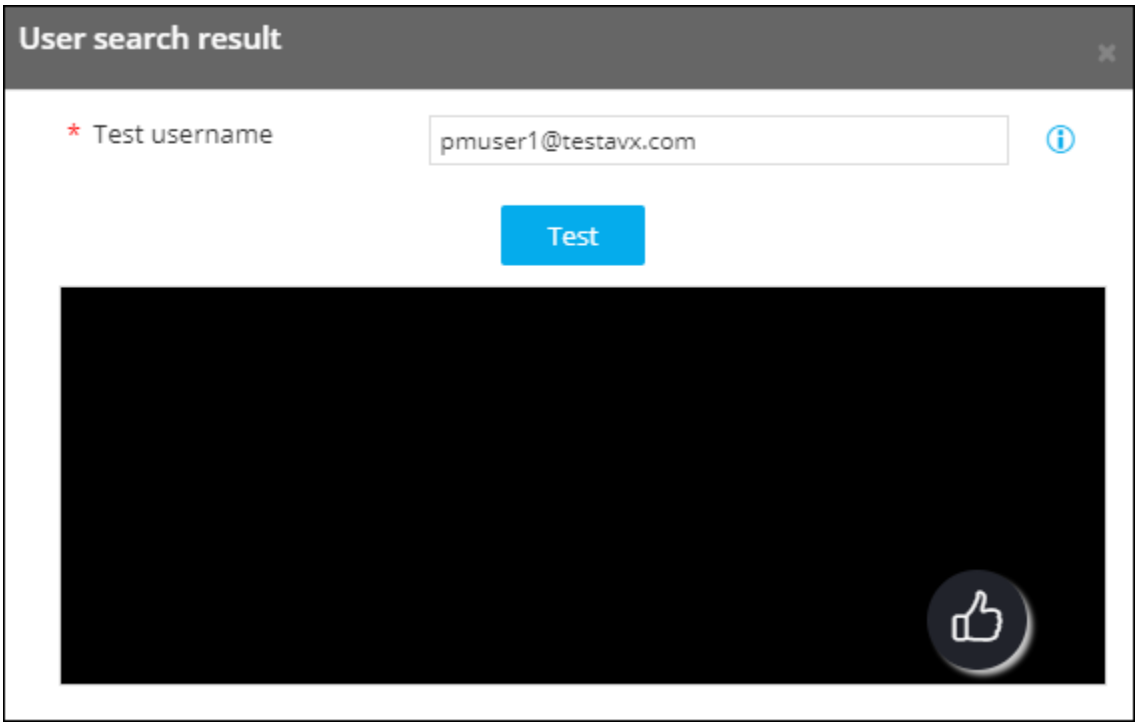
4. The **User Search** section collects information to validate a user's presence in the Active Directory. In the **User Search** section, enter the following details(sample values are shown in the image).



Field descriptions for User search

Field	Description
***User search base**	Base directory where the user is present.
***Search filter**	Criteria for searching for the user from the search base.
***User return attribute**	User information to be retrieved from the search base. **Note:** This field is enabled only when the **Authorization** toggle (in the **General Information** section) is turned on. **Note:** You can specify only User return attribute.
Note: The asterisk (*) symbol indicates mandatory fields.	

5. After entering the above details, to test if the user is present in the Active Directory, click **Test query**.
6. In the **User search result** action pane, enter the **Test username** and click **Test**.



Note: You are allowed to check the query response for User search and Group search only when the connection is valid.

7. To test which user group the user belongs to, in the **Group search** section, enter the following details:

Note: This section is enabled only when the **Authorization** toggle (in the **General Information** section) is turned on.

Field descriptions for Group search

Field	Description
Group search base	Base directory where the user group is present.
Search filter	Criteria to search the user group from the search base.
Group return attribute	User group information to be retrieved from the search base.

Note: You are allowed to check the query response for User search and Group search only when the connection is valid.

Note: Group search can be performed only if the customer's LDAP is of type Open LDAP. Microsoft Active Directory does not need group search configuration. For Open LDAP, group search needs to be configured mandatorily. The User return attribute in the User search section does not return the group membership details.

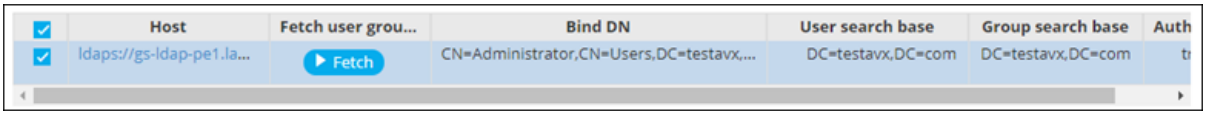
Note: In the case of multiple LDAP servers, to define/update the order in which the servers will be authenticated, drag and drop the entries in this table.

• Deleting a LDAP Configuration

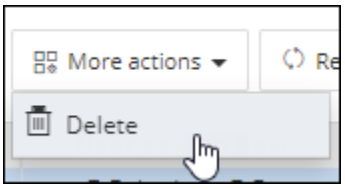
Deleting a LDAP Configuration

To delete a LDAP configuration:

1. On the **RBAC Journey :: Authentication** page, from the table of LDAP configurations, to delete a LDAP configuration, select the check box corresponding to that entry.



2. From the **More actions** drop-down menu, click **Delete**.

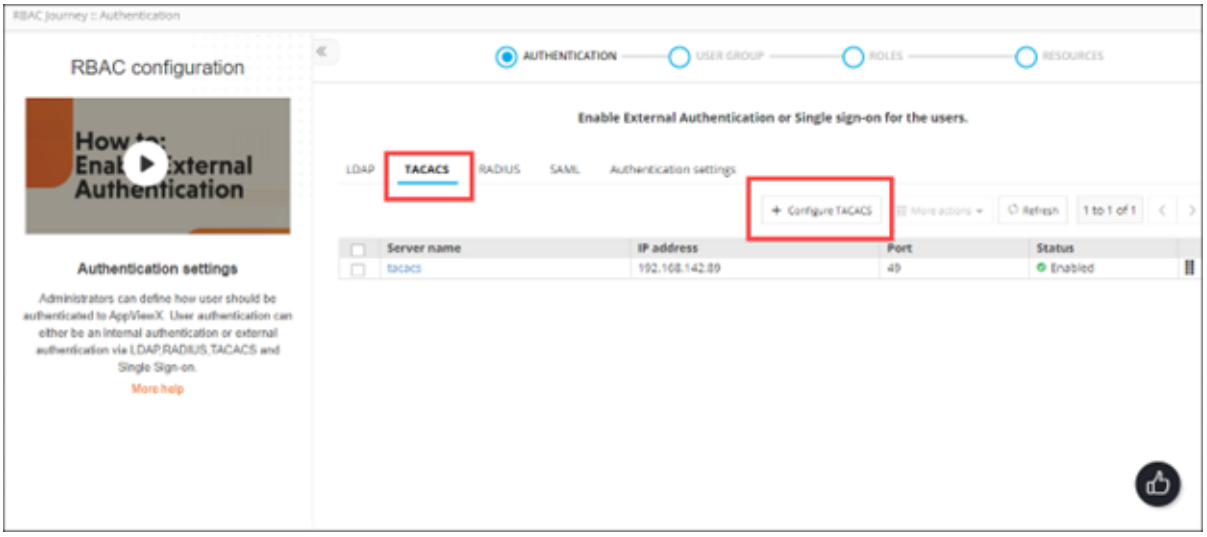


3. In the **Confirmation** dialog box, click **Delete**.
   The selected configuration is deleted.

Configuring Role-Based Access Control for TACACS

To configure RBAC for TACACS authentication:

1. On the **RBAC Journey :: Authentication** page, click the **TACACS** tab and click **Configure TACACS**.



The **Configure TACACS** action pane is displayed.

2. Enter the field information as shown in the table below:

Field descriptions for TACACS Test connection

Field	Description
***Server name**	Name of the TACACS server.
***IP address**	IP address of the TACACS server.
***Port**	Port number of the TACACS server

Note: The asterisk (*) symbol indicates mandatory fields.

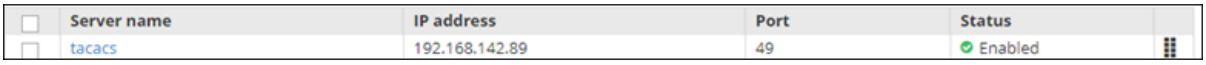
3. To test the connectivity between AppViewX and the IP address mentioned above, click **Test connection**.
4. Enter the field information as shown in the table below::

Field descriptions for TACACS

Field	Description
***Secret key**	A unique key for authentication between the AppViewX server and the TACACS server.
***Service**	Name of the service used by the user requested to be authorized.

Field	Description
	Specifying the service name is mandatory because it enables the TACACS + server to behave according to the type of each authorization request. Commonly, the Point-to-Point Protocol (PPP) is used for authorization checks.
***Protocol**	The protocol associated with the value specified in Service Name, which is a subset of the associated service being used for client authorization or system accounting Commonly, the Internet Protocol (IP) is used as the modifier with PPP to indicate the protocol layer for authorization check.
***Authorization Attribute Name**	Attribute that will be returned from the TACACS server to authenticate and authorize the connection between the AppViewX server and the TACACS server.
Note: The asterisk (*) symbol indicates mandatory fields.	

5. To save the TACACS authentication settings, click **Add** and to reconfigure the settings, click **Reset**. The TACACS authentication settings thus configured are saved and displayed in the table as shown in the image below:



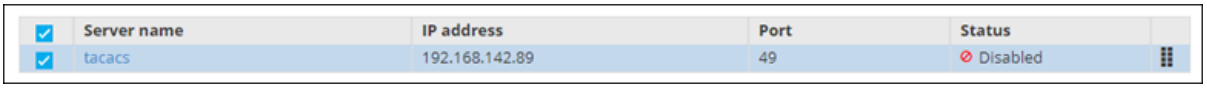
Note: In the case of multiple TACACS servers, to define/update the order in which the servers will be authenticated, drag and drop the entries in this table.

- Enabling a TACACS Configuration
- Disabling a TACACS Configuration
- Deleting a TACACS Configuration

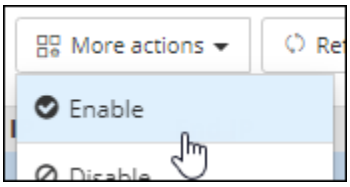
Enabling a TACACS Configuration

To enable a TACACS configuration:

1. On the **RBAC Journey :: Authentication** page, click the **TACACS** tab.
2. From the table of TACACS configurations, for the configuration you want to enable, select the check box corresponding to that entry.



3. From the **More actions** drop-down menu, click **Enable**.

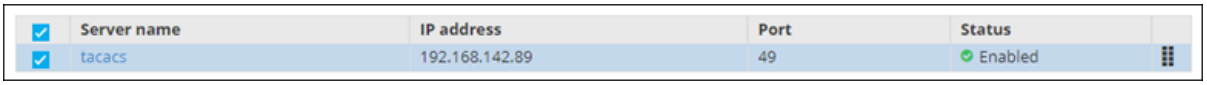


4. In the **Confirmation** message dialog box, click **Proceed**.
   The selected configuration is enabled.

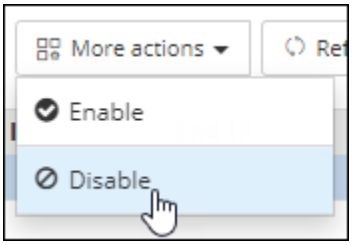
Disabling a TACACS Configuration

To disable a TACACS configuration:

1. On the **RBAC Journey :: Authentication** page, click the **TACACS** tab.
2. From the table of TACACS configurations, for the configuration you want to disable, select the check box corresponding to that entry.



3. From the **More actions** drop-down menu, click **Disable**.

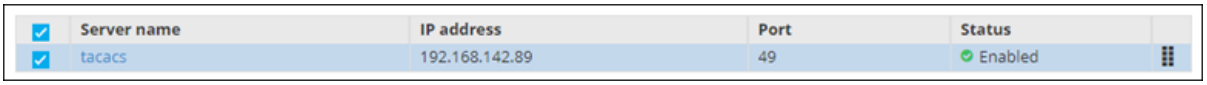


4. In the **Confirmation** message dialog box, click **Proceed**.
   The selected configuration is disabled.

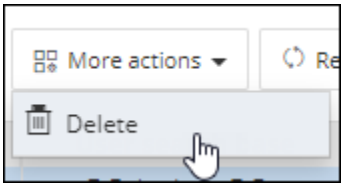
Deleting a TACACS Configuration

To delete a TACACS configuration:

1. On the **RBAC Journey :: Authentication** page, click the **TACACS** tab.
2. From the table of TACACS configurations, for the configuration you want to delete, select the check box corresponding to that entry.



3. From the **More actions** drop-down menu, click **Delete**.

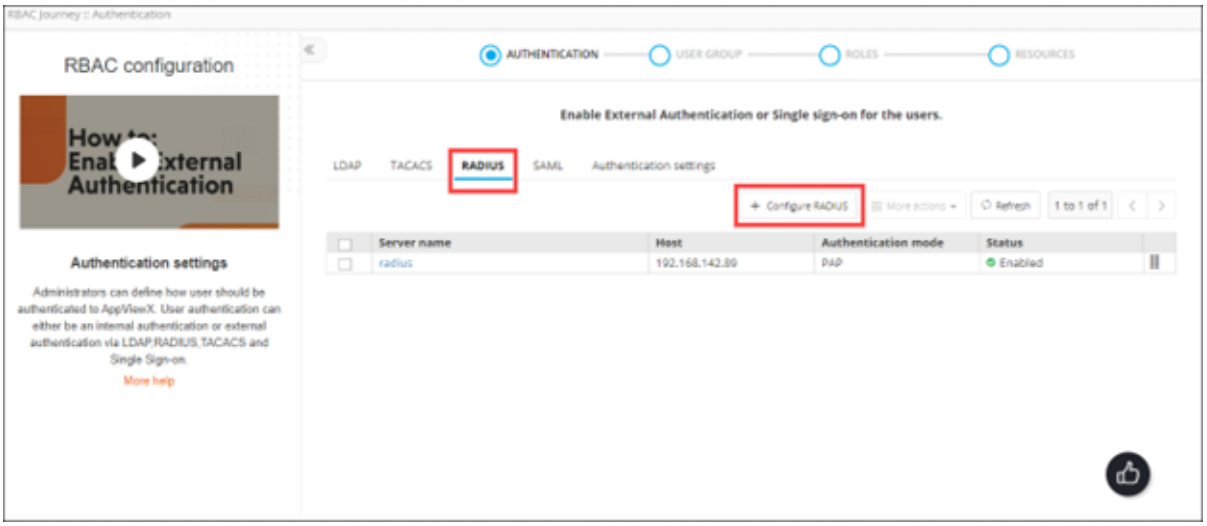


4. In the **Confirmation** message dialog box, click **Proceed**.
   The selected configuration is deleted.

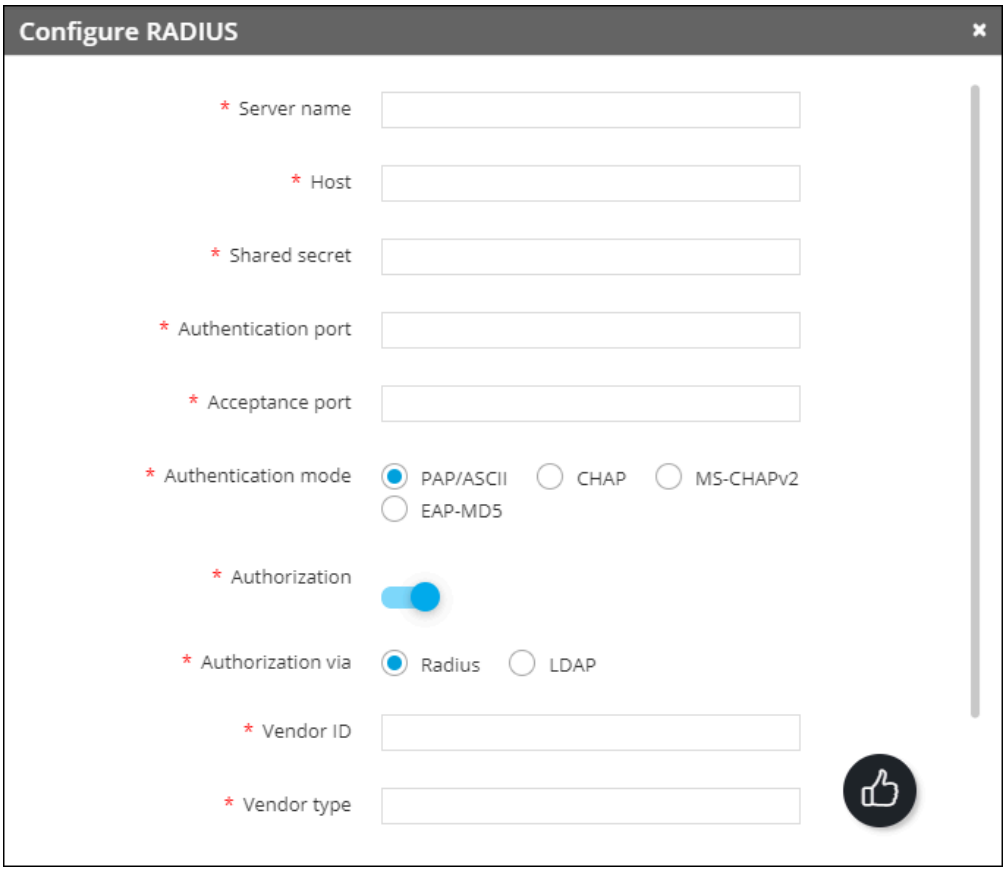
Configuring Role-Based Access Control for RADIUS

To configure RBAC for RADIUS authentication:

1. On the **RBAC Journey :: Authentication** page, click the **RADIUS** tab and click **Configure RADIUS**.



   The Configure RADIUS action is displayed.



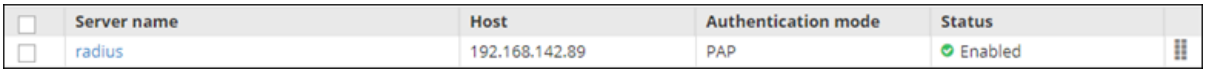
Field descriptions for RADIUS

Field	Description
***Server Name**	Name of the RADIUS server.
***Host**	The IP address of the RADIUS server.
***Shared secret**	A unique key for authentication between the AppViewX server and the RADIUS server.
***Authentication port**	Port number that AppViewX will use for authentication. **Note:** The default authentication port number is 1812. Please check with your system admin if your organization uses a different port number.
***Acceptance port**	Port number that AppViewX will use to accept a response from the RADIUS server.

Field	Description
	Note: The default acceptance port number is 1813. Please check with your system admin if your organization uses a different port number.
***Authentication mode**	Select one of the following authentication modes: • PAP/ASCII • CHAP • MS-CHAPv2 • EAP-MD5. **Note:** Ensure that the selected authentication mode is also confirmed in the RADIUS server settings.
Authorization via	Select from one of the following authorization modes: • RADIUS • LDAP. **Note:** This field is enabled only when the Authorization toggle is turned on.
***Vendor ID**	Enter the vendor ID. **Note:** This field is enabled only when the Authorization toggle is turned on and authorization is done via the RADIUS server. **Note:** AppViewX does not have a unique vendor ID. We use a free vendor ID: **500**. Ensure that this is configured as part of the RADIUS server settings.
***Vendor type**	Enter the vendor type. **Note:** This field is enabled only when the Authorization toggle is turned on and authorization is done via the RADIUS server.

Field	Description
	Note: AppViewX does not have a unique vendor type. We use a free vendor ID: **200**. Ensure that this is configured as part of the RADIUS server settings.
***LDAP**	From the dropdown menu, select the LDAP server to be used for the authorization. **Note:** This field is enabled only when the Authorization toggle is turned on and authorization is done via the LDAP server.
Note: The asterisk (*) symbol indicates mandatory fields.	

2. To save the RADIUS authentication settings entered above, click **Add** or to reconfigure the settings, click **Reset**.
   The RADIUS authentication settings thus configured are saved and displayed in the table as shown in the image given below:



Note: In the case of multiple RADIUS servers, to define/update the order in which the servers will be authenticated, drag and drop the entries in this table.

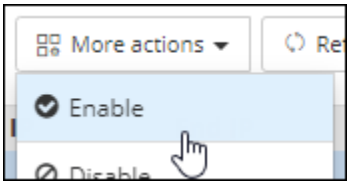
- Enabling a RADIUS Configuration
- Disabling a RADIUS Configuration
- Deleting a RADIUS Configuration

Enabling a RADIUS Configuration

To enable a RADIUS configuration:

1. On the **RBAC Journey :: Authentication** page, click the **RADIUS** tab.
2. From the table of RADIUS configurations, for the configuration you want to enable, select the check box corresponding to that entry.

3. From the **More actions** drop-down menu, click **Enable**.

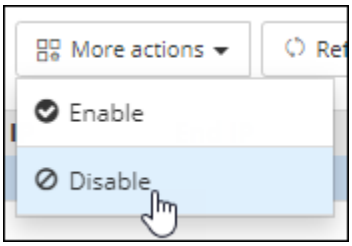


4. In the **Confirmation** message dialog box, click **Proceed**.
   The selected configuration is enabled.

Disabling a RADIUS Configuration

To disable a RADIUS configuration:

1. On the **RBAC Journey :: Authentication** page, click the **RADIUS** tab.
2. From the table of RADIUS configurations, for the configuration you want to disable, select the check box corresponding to that entry.
3. From the **More actions** drop-down menu, click **Disable**.

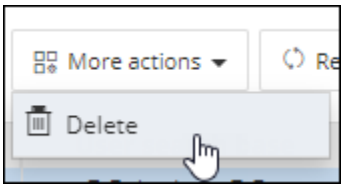


4. In the **Confirmation** message dialog box, click **Proceed**.
   The selected configuration is disabled.

Deleting a RADIUS Configuration

To delete a RADIUS configuration:

1. On the **RBAC Journey :: Authentication** page, click the **RADIUS** tab.
2. From the table of RADIUS configurations, for the configuration you want to delete, select the check box corresponding to that entry.
3. From the **More actions** drop-down menu, click **Delete**.

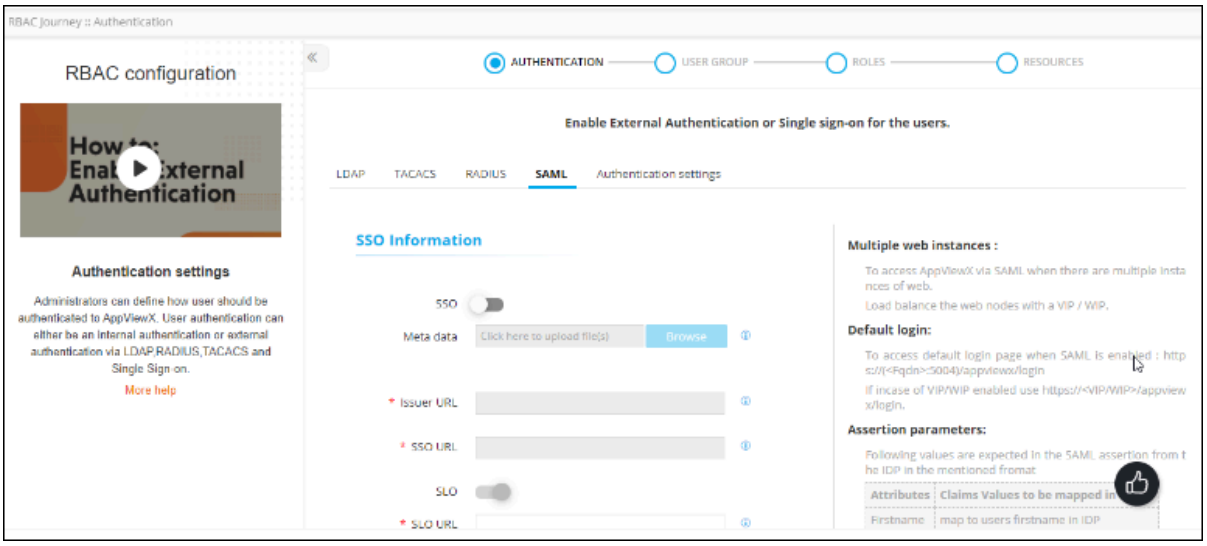


4. In the **Confirmation** message dialog box, click **Proceed**.
   The selected configuration is deleted.

Configuring Single Sign On Settings with AppViewX

To configure single sign on settings with AppViewX:

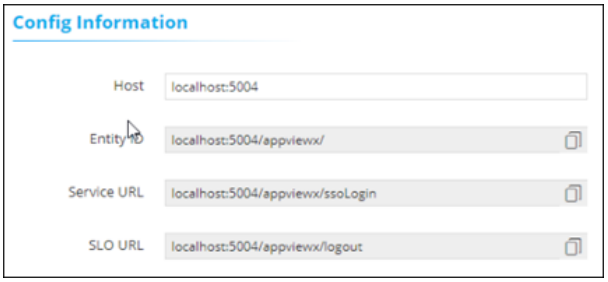
1. On the **RBAC Journey :: Authentication** page, click the **SAML** tab.



2. In the **SSO Information** section, enter the following details:

Field descriptions for SSO Information

Field	Description
SSO	To use SAML authentication for Single Sign On, turn on the **SSO** toggle. The **Config Information** section is displayed with the field information auto-populated as shown below:

Field	Description
	
Metadata	To import an identity provider (IdP): a. Click **Browse**. b. Navigate to the location where the XML metadata file is stored. c. To upload the file, click **Open**. **Note:** You can also copy and paste the metadata information from the XML file into the metadata contents text boxes in the **Config Information** section.
***Issuer URL**	Entity ID of the IdP. **Note:** This field is enabled only when the **SSO** toggle in the **SSO Information** section is turned on.
***SSO URL**	For AppViewX to send the authentication request, enter the URL of the protected endpoint provided by your IdP. **Note:** This field is enabled only when the **SSO** toggle in the **SSO Information** section is turned on.
SLO	To enable single log out, turn on the **SLO** toggle. This will log out the user from AppViewX and the IdP.
***SLO URL**	URL of the IdP protocol endpoint. **Note:** This field is enabled only when the **SSO** toggle in the **SSO Information** section is turned on.

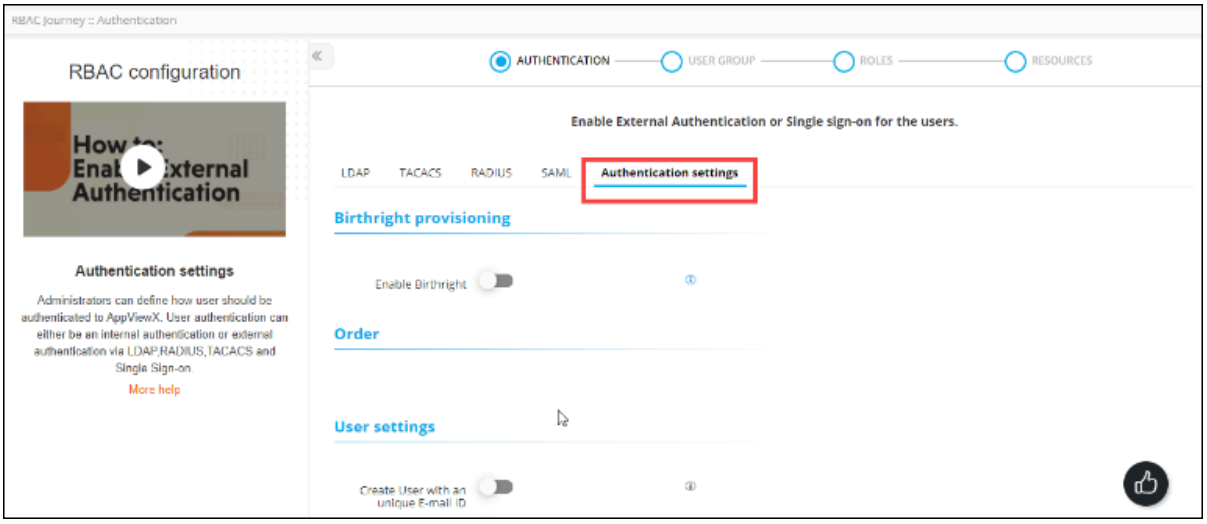
Field	Description
	Note: This field is mandatory only when the **SLO** toggle in the **SAML details** section is turned on.
***Upload certificate**	To upload a certificate: a. Click **Browse Certificate**. b. Navigate to the location of the **.pem** certificate file. c. Select the certificate file to be uploaded and click **Open**. The selected certificate is uploaded. **Note:** A certificate is to be uploaded only when the certificate of the IDP is not available as a part of the metadata. **Note:** This field is enabled only when the **SSO** toggle in the **SSO Information** section is turned on.
Local authorization	To enable SAML only authentication in IdP and for authorization to be carried out in AppViewX, enable this toggle key. **Note:** Authorization can be done by assigning user groups manually to the user or enabling birthright role.
Note: The asterisk (*) symbol indicates mandatory fields.	

3. To save the SAML authentication settings, click **Save**.
4. To cancel the authentication settings, click **Cancel**.

Configuring Authentication Settings RBAC quick config

To configure the authentication settings:

1. On the **RBAC Journey :: Authentication** page, click the **Authentication Settings** tab.



2. To enable **Birthright provisioning** for new users who log into the system with a predefined set of permissions (associated with the user group), turn on the **Enable Birthright** toggle.
3. To define the order in which the authentication settings will be checked, in the **Order** section, drag and drop the authentication labels to the required corresponding levels.
   If the level 1 check is set to Local and the level 2 check is set to LDAP, user credentials will be authenticated locally first and then on the LDAP server.

> **Note:** You can also disable, and then enable a level of authentication. To do this, click the green tick 
>
> next to the server name.

4. In the **User settings** section, enter the required field information.

Field descriptions for User settings

Field	Description
Create User an unique E-mail ID	To ensure that every AppViewX user has a unique email ID, turn on this toggle.
Create User on Authorization Failure	To create a user even if authorization fails (but the user is authenticated successfully), turn on this toggle.
Session Timeout	AppViewX lets you set a session timeout limit between 2 and 480 minutes. To set a web session timeout limit, enter the value in minutes.

5. If the AppViewX node password has been changed, in the **Node Settings** section, enter the updated Node Password.

   Note: The value entered in the Node Password field should be the same as the node password. To apply the changes, restart the avx-config-server pod in every datacenter.

6. Click **Save**.

Resource

The resource allows you to specify access at a granular level across all the devices and modules of AppViewX listed in this section, where the permission definitions are independent of each other. The resources can be assigned only to a User group. The resources that are assigned to the user groups will automatically inherit the permissions associated with that resource. User groups can be assigned more than one resource.

AppViewX enables the following resource-related features:

- Dynamic rule-based resource tagging of newly discovered ADC objects, Certificates based on Query using object/Certificate fields available within in AppViewX.
- Dynamic rule-based resource tagging of newly discovered ADC objects, Certificates using a script to tag based on data available with external tools (SNOW, Other CMDB, etc.).
- Rule templates are pre-shipped to ease the rule creation to dynamically tag resources.
- Dynamically created resources can be assigned to user groups dynamically by mapping the respective rule to the required user groups as part of the Rules in Use inventory in the wizard flow.
- Manage the order of execution for the RBAC rules.
- Manage short circuit option to dynamically tag ADC objects

Note: This dynamic resource tagging is only for newly discovered ADC objects and certificates.

Note: Objects/Certificates and the respective permissions part of the existing resources will not be updated/changed.

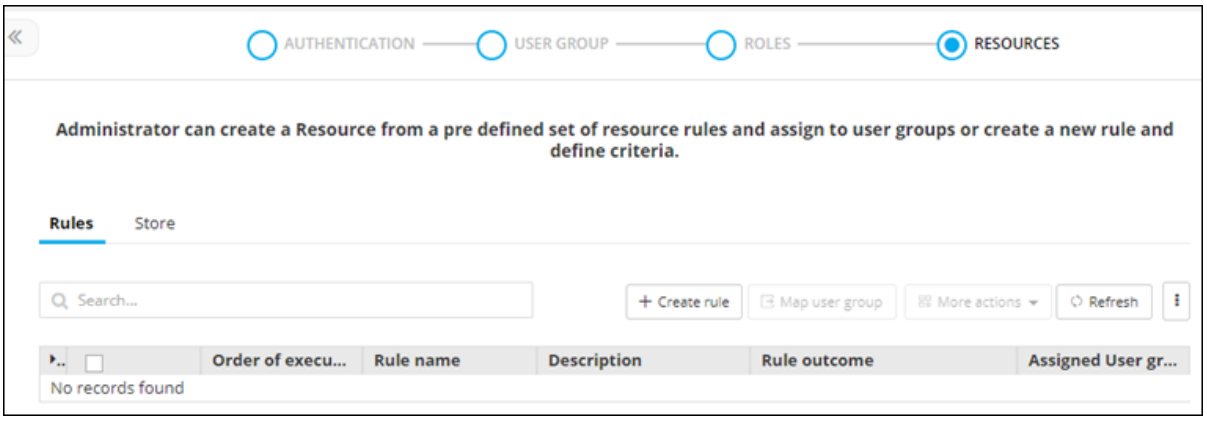
- Create an RBAC Rule to Tag ADC Objects Using a Query
- Configuring a Variable as a Filter Condition Value based on Patterns
- Configuring the Resource Name
- Create an RBAC Rule to Tag ADC Objects/Certificates using a Script

- Configuring the Certificate Group Name
- Configuring the Resource Name Based on Patterns
- Clone a Rule
- Delete a Rule
- RBAC Rule Mapping to User Groups to Dynamically Provide Access for Resources to User Groups
- Managing Order of Execution and Short Circuit Configuration for Rules

Create an RBAC Rule to Tag ADC Objects Using a Query

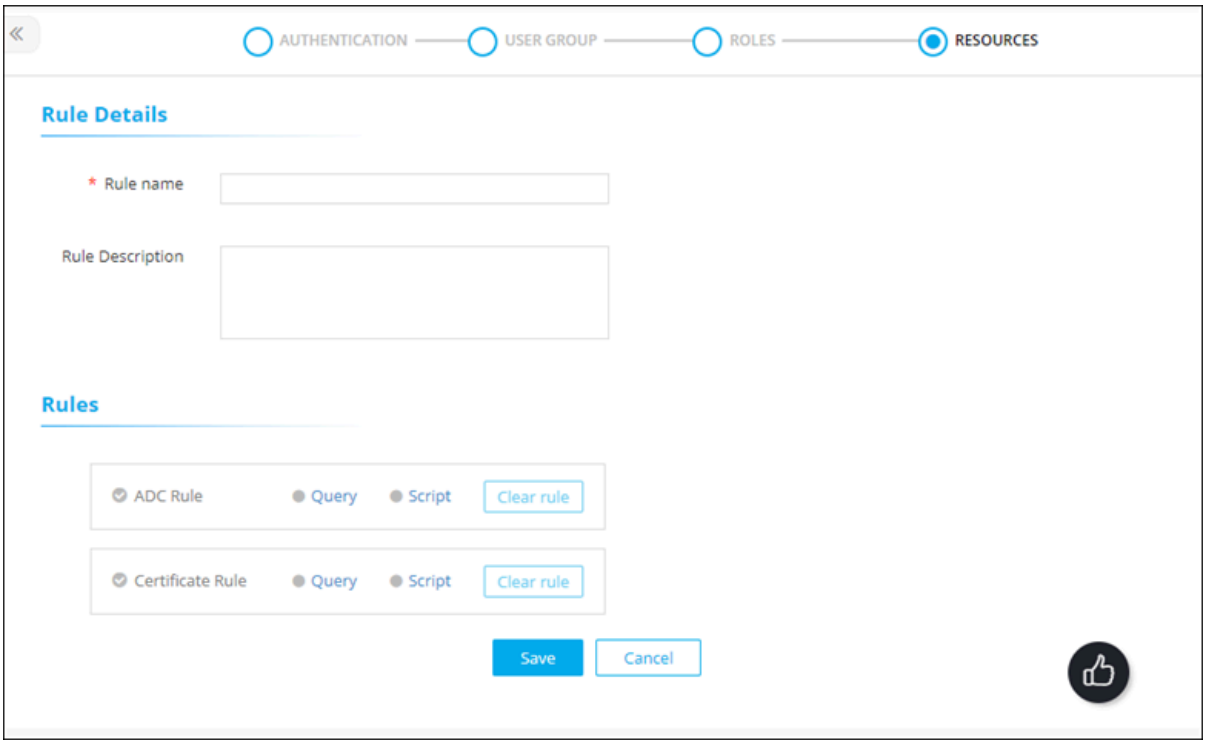
To create a RBAC rule to tag resources using a query:

1. On the **RBAC Journey :: Authentication** page, navigate to the **RESOURCES** stage as part of the wizard flow to add roles into AppViewX, with the **Rules** tab displayed by default.



2. Click + Create rule.

   The **Rules :: Create** screen is displayed.



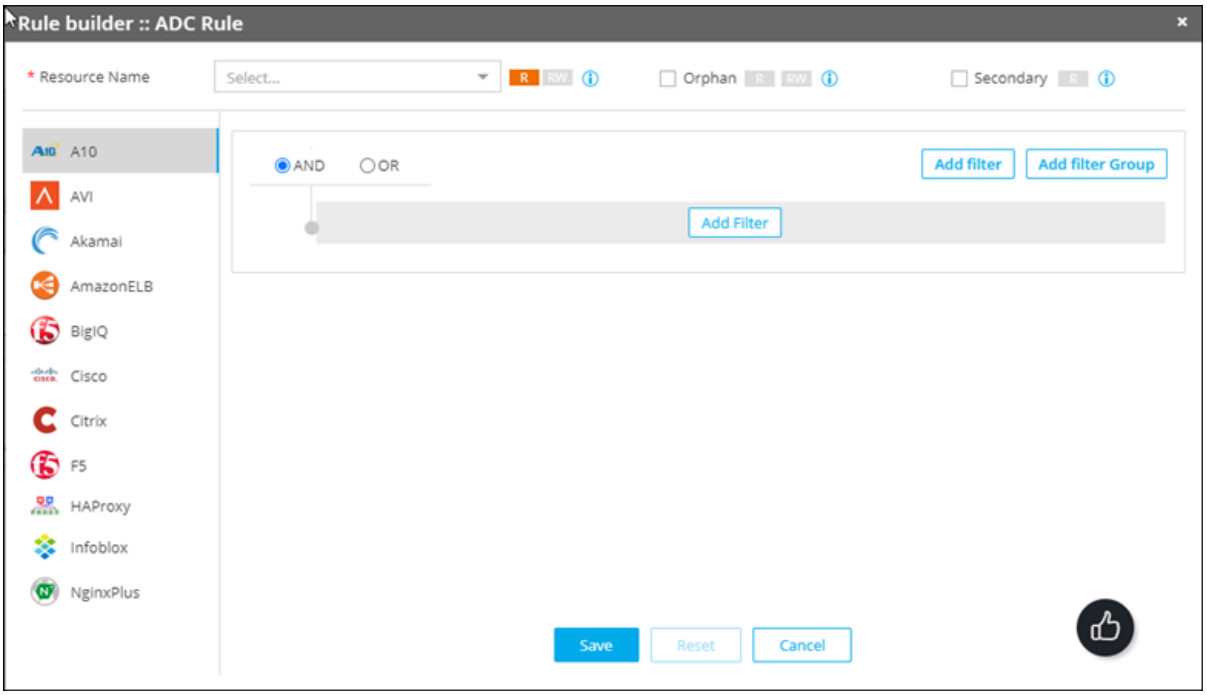
3. In the **Rule Details** section, enter the following details:

Field descriptions for Rule Details

Field	Description
***Rule Name**	Resource name.
Rule Description	Brief description of the resource/granular level accesses associated with the resource.

Note: The asterisk (*) symbol indicates mandatory fields.

4. To configure a rule to dynamically tag ADC objects using Query, in the **Rules** section, for the **ADC Rule**, select **Query**.
5. The **Rule builder :: ADC Rule** action pane is displayed.



6. On the **Rule builder :: ADC Rule** action pane, click **Add Filter**.
7. Select the field, condition and enter the value to be monitored for dynamic tagging of ADC objects based on rule condition.

Configuring a Variable as a Filter Condition Value based on Patterns

A variable can be defined with a pattern as specified below:

1. Select any one required field, then select condition as “Variable”, define value in the format of <%variable%>. Example: A virtual server configured with the pattern vs_prod_support.appviewx.com can be defined as vs_<%variable1%>_support.appviewx.com [where <%variable1%> can match to name UAT, DEV, etc.].
2. Multiple variable definitions for the same object pattern can be defined as. vs_<%variable1%>_<%variable2%>_support.appviewx.com [where <%variable1%> can match to name UAT, DEV etc and <%variable2%> can match to name sales, marketing etc].
3. Variables can be used only across one field in a Rule.
4. Variable name should follow the below standards:
   - Only alphanumeric [A-Z, a-z, 0-9].
   - Special characters underscore [_].
   - Placeholder is <% for beginning and %> for ending.
5. Specify a resource name.

Configuring the Resource Name

To create resources dynamically based on patterns, resource name can be configured in the following ways:

1. Provide the resource name of an existing resource by choosing the resource name from dropdown.
2. Provide a static name to the resource. [when rule matches the resource name would be created on demand].
3. Provide a pattern for the resource name. [provide the variable pattern defined in the query as the resource name].
4. Click either the R (Read-only) or RW (Read/Write) button to designate whether user groups assigned to the resource have read-only or read/write permissions on the ADC objects.

   Note: The ADC objects tagging has two additional fields that allow you to assign global permissions for orphan and secondary ADC objects to the resource you are creating. Users cannot assign individual permissions to orphan and secondary objects.

   To enable this:

   a. Next to the **Resource** name, select the checkbox beside Orphan if you want to assign global permissions for orphan objects.
   b. Click either the **R** or **RW** icon to give users assigned to the resource Read-Only or Read/Write permissions on all orphan objects.
   c. Select the checkbox beside **Secondary** if you want to assign global permissions for secondary objects.
   d. Click the **R** icon to give user groups assigned to the resource Read-Only permissions on all secondary objects. The **RW** icon is not available because you cannot grant Read/Write access to secondary objects.
   e. Click **Save**.

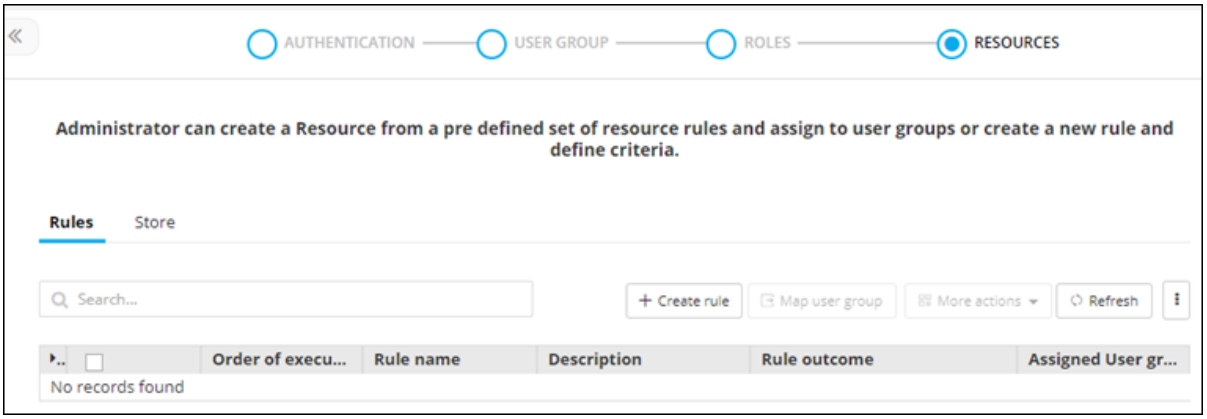
      Saved rules will be displayed in the **Rules** tab.

   f. Go to the Rules tab by clicking on Resource in the breadcrumb.
   g. Rule Summary details (Rule Name, Description, Rule Outcome) are displayed in the Rule Inventory table.
   h. Enable the rule by clicking on the respective status icon for the rule to be actively running.

Create an RBAC Rule to Tag ADC Objects/Certificates using a Script

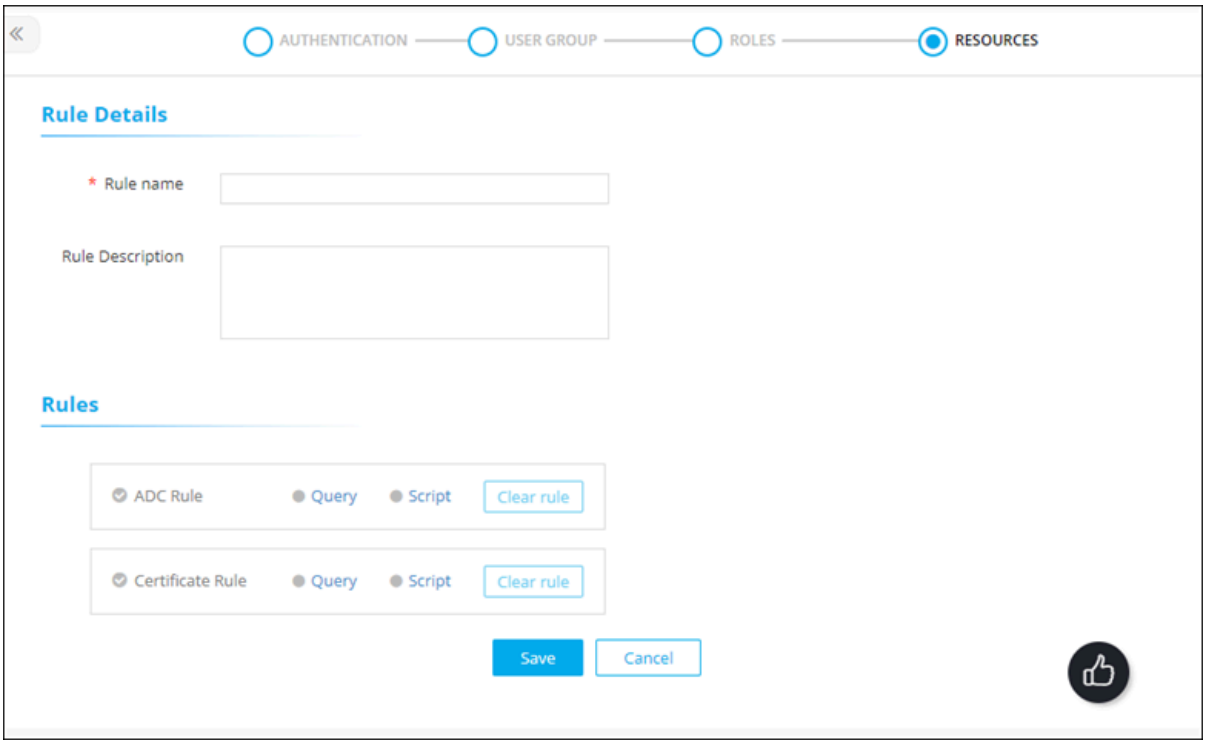
To create a RBAC rule to tag ADC objects/certificates using a script:

1. On the **RBAC Journey :: Authentication** page, navigate to the **RESOURCES** stage as part of the wizard flow to add roles into AppViewX, with the **Rules** tab displayed by default.



2. Click + Create rule.

The **Rules :: Create** screen is displayed.



3. In the **Rule Details** section, enter the following details:

Field descriptions for Rule Details

Field	Description
***Rule Name**	Resource name.
Rule Description	Brief description of the resource/granular level accesses associated with the resource.

Note: The asterisk (*) symbol indicates mandatory fields.

4. In the Rules section, choose the ADC Rule and select 'Script' to configure a rule for dynamically tagging ADC objects using a Query.
5. Configure the details of the script, provide a resource name and assign required permissions. For ADC Objects, Orphan and Secondary objects need to be assigned globally. For Certificates, Certificate Group Name need to be provided.
6. Click **Save**.
   Saved rules will be displayed in the **Rules** tab.
7. Go to the Rules tab by clicking on Resource in the breadcrumb. Rule Summary details (Rule Name, Description, Rule Outcome) are displayed in the Rule Inventory table.
8. Enable the rule by clicking on the respective status icon for the rule to be actively running.

Configuring the Certificate Group Name

To create certificate groups dynamically based on patterns, the certificate group name can be configured in the following ways:

1. Provide the certificate group name of an existing resource by choosing the certificate group name from the dropdown menu.
2. Provide a static name to the certificate group name. [When rule matches the resource name would be created on demand].
3. Provide a pattern for the certificate group name. [Provide the variable pattern defined in the query as the resource name].

For example, Resource_<%variablename%> | <%variablename%>_Resource | <%variablename%>

Configuring the Resource Name Based on Patterns

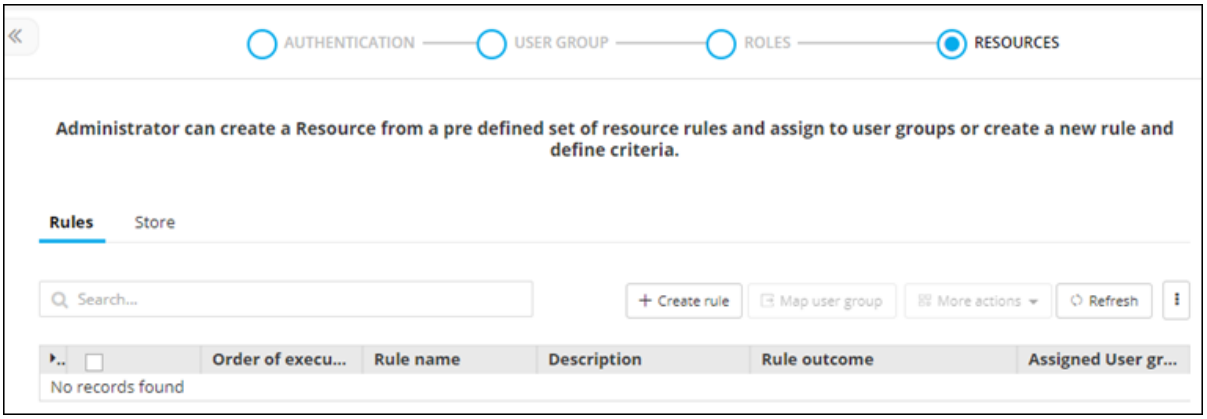
To create resources dynamically based on patterns, the resource name can be configured in the following ways:

1. Provide the Resource Name of an existing resource by choosing the Resource Name from Drop Down.
2. Provide a Static Name to the Resource. [When Rule matches the Resource Name would be created on Demand].
3. Provide a Pattern for the Resource Name. [Provide the variable pattern defined in the Query as the Resource Name]. For example, Resource_<%variablename%> | <%variablename%>_Resource | <%variablename%>.
4. Click either the R (Read-only) or RW (Read/Write) button to designate whether user groups assigned to the resource have read-only or read/write permissions on the certificate groups.
5. When you are finished configuring the Certificate rule, click Save. Saved rules will be displayed in the Rules tab.
6. Go to the Rules tab by clicking on Resource in the breadcrumb. Rule Summary details (Rule Name, Description, Rule Outcome) are displayed in the Rule Inventory table.
7. Enable the rule by clicking on the respective status icon for the rule to be actively running.

Clone a Rule

To clone a rule:

1. On the **RBAC Journey :: Authentication** page, navigate to the **RESOURCES** stage as part of the wizard flow to add roles into AppViewX, with the **Rules** tab displayed by default.



2. For the resource you want to clone, select the check box against that resource.
3. From the **More actions** drop-down menu, click **Clone**.
4. In the **Clone** rules dialog box, enter a name for the cloned rule and click **Save**.

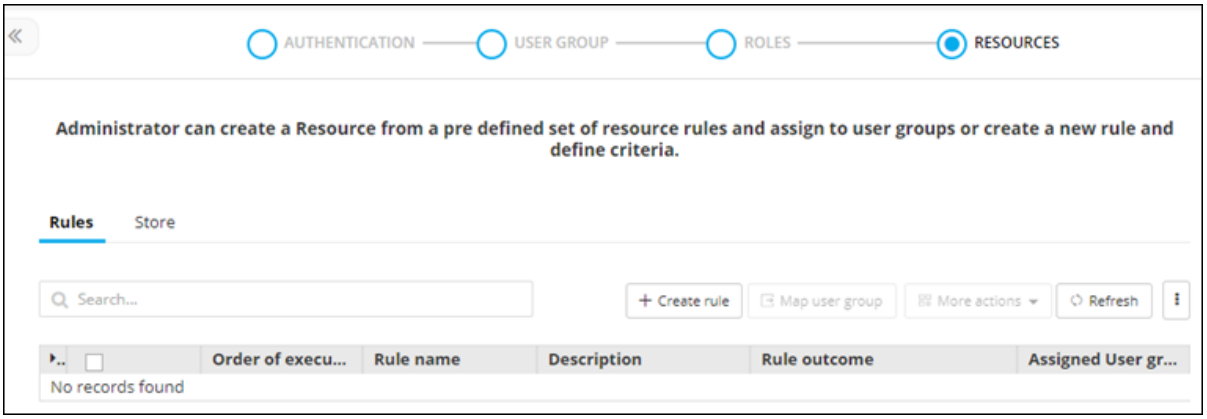
Rule details will be closed and will be opened in edit mode for any further modification on description/ rule conditions.

5. Once the rule is saved, enable the rule by clicking on the respective status icon for the rule to be actively running in the rules inventory table.

Delete a Rule

To delete a rule:

1. On the **RBAC Journey :: Authentication** page, navigate to the **RESOURCES** stage as part of the wizard flow to add roles into AppViewX, with the **Rules** tab displayed by default.

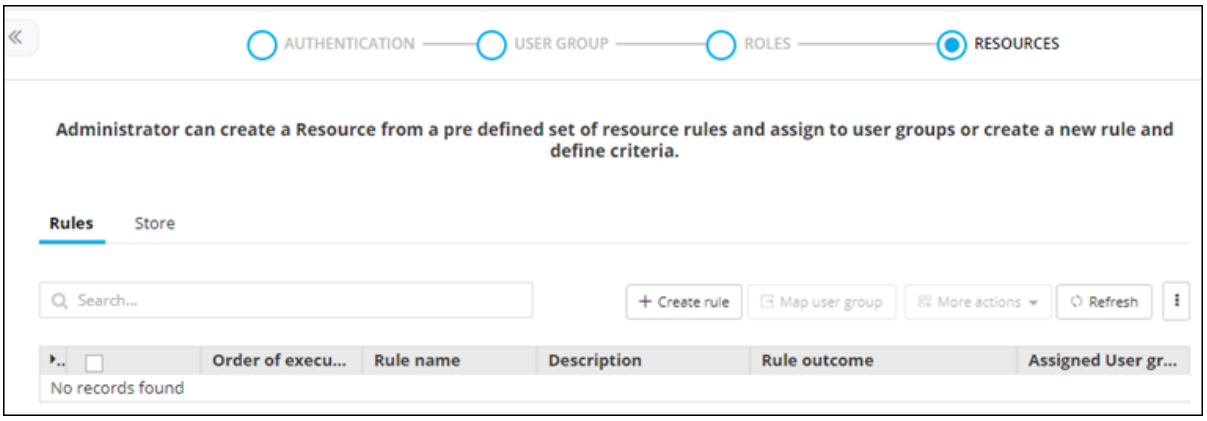


2. For the resource you want to delete, select the check box against that resource.
3. From the **More actions** drop-down menu, click **Delete**.
4. In the **Confirmation** dialog box, click **Yes**.

RBAC Rule Mapping to User Groups to Dynamically Provide Access for Resources to User Groups

To create a RBAC rule to dynamically provide access for resources to user groups:

1. On the **RBAC Journey :: Authentication** page, navigate to the **RESOURCES** stage as part of the wizard flow to add roles into AppViewX, with the **Rules** tab displayed by default.



2. For the resource you want to map to user groups, select the check box against that resource.
3. Click 

.
4. In the **Map user group** action pane, select the user groups the resource will be mapped to.
5. Click **Save**.

Managing Order of Execution and Short Circuit Configuration for Rules

For managing the order of rule execution to avoid conflicts across multiple rules matching similar conditions and tag to expected resources:

1. In the rule inventory table, click and hold a rule name and drag it up or down to change the order of execution of rules in use in the system.
2. The order will be automatically saved or click the up or down arrows beside each rule name to update the rule execution order.

Key points for consideration:

- Order of execution needs to be maintained by the user only to manage certificates tagged to expected certificate groups configured part of a rule, as certificates can’t be part of multiple certificate groups.
- Based on the order of execution and matching rule condition, certificates will be only tagged to the certificate group at the top of rule execution order even though other RBAC rules down the order have a matching condition.
- Order of execution also needs to be maintained by the user for ADC objects tagging to a specific resource only when Short circuit option is turned on for ADC.

- By default, a short circuit will be turned off for ADC as ADC objects can be tagged to multiple resources. There is no such restriction for ADC as it is existing for a certificate tagging. For certificates, a short circuit will always be turned on and can't be changed by the user.
- To enable a short circuit for ADC, click More icon under the Rules Inventory>> Enable Short Circuit for ADC.

Role

Each role assigns a specific set of permissions relating to the modules that can be accessed and the tasks that can be performed in each AppViewX module. The roles can be assigned only to a User group. The user groups that are assigned with a role will automatically inherit all the associated permissions. User groups can be assigned more than one role.

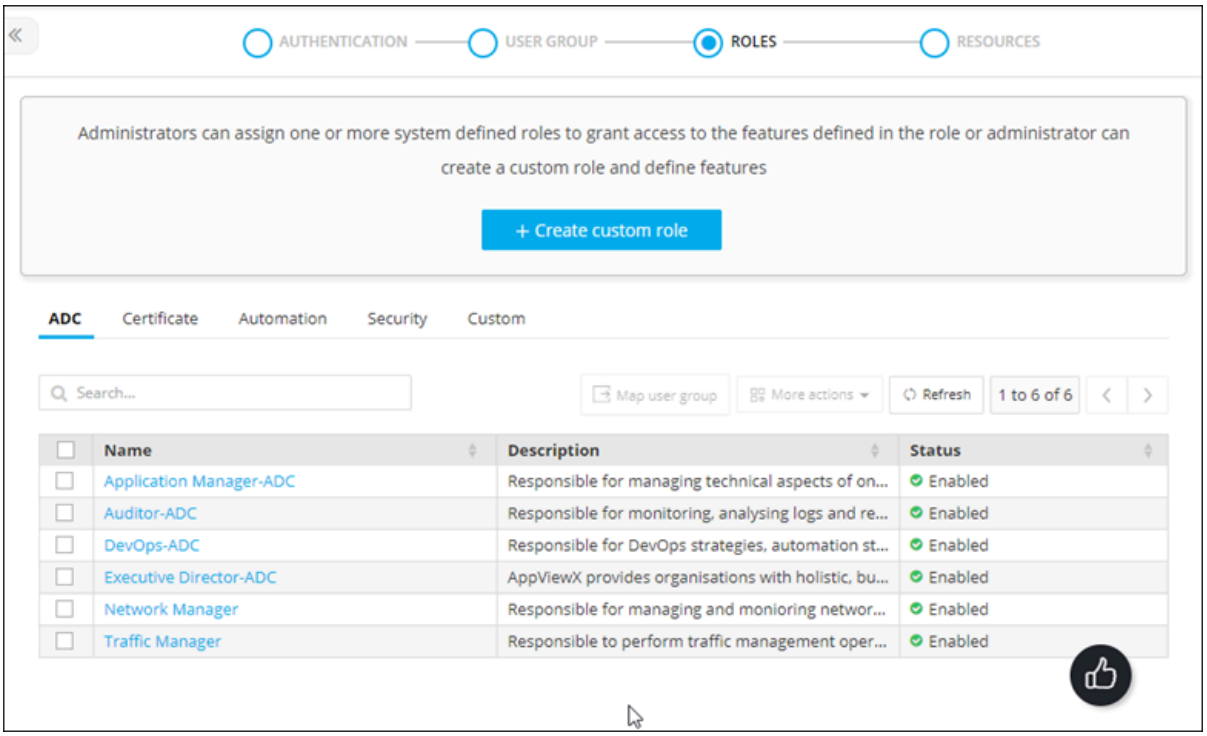
AppViewX enables the following role-related features:

- Out of the Box (OOB) roles are available for ADC, Certificates, Security, and Automation modules.
- OOB roles can be cloned, enabled, and disabled. OOB roles can't be updated/deleted.
- Administrators can also create custom roles. Custom roles can be updated, deleted, enabled and disabled.
- Users can either use OOB roles (if suits their needs) or custom roles to map to user groups.

Creating a Custom Role

To create a custom role:

1. On the **RBAC Journey :: Authentication** page, navigate to the **ROLES** stage as part of the wizard flow to add roles into AppViewX.



2. Click **Create custom role**.
   The **Create custom role** action pane is displayed.
3. Under the **Information** tab, enter the following details:

Field descriptions for Information

Field	Description
***Name**	Role name.
Description	Brief description of what users assigned to the role can do and/or what features or functionalities are associated with the role.

Note: The asterisk (*) symbol indicates mandatory fields.

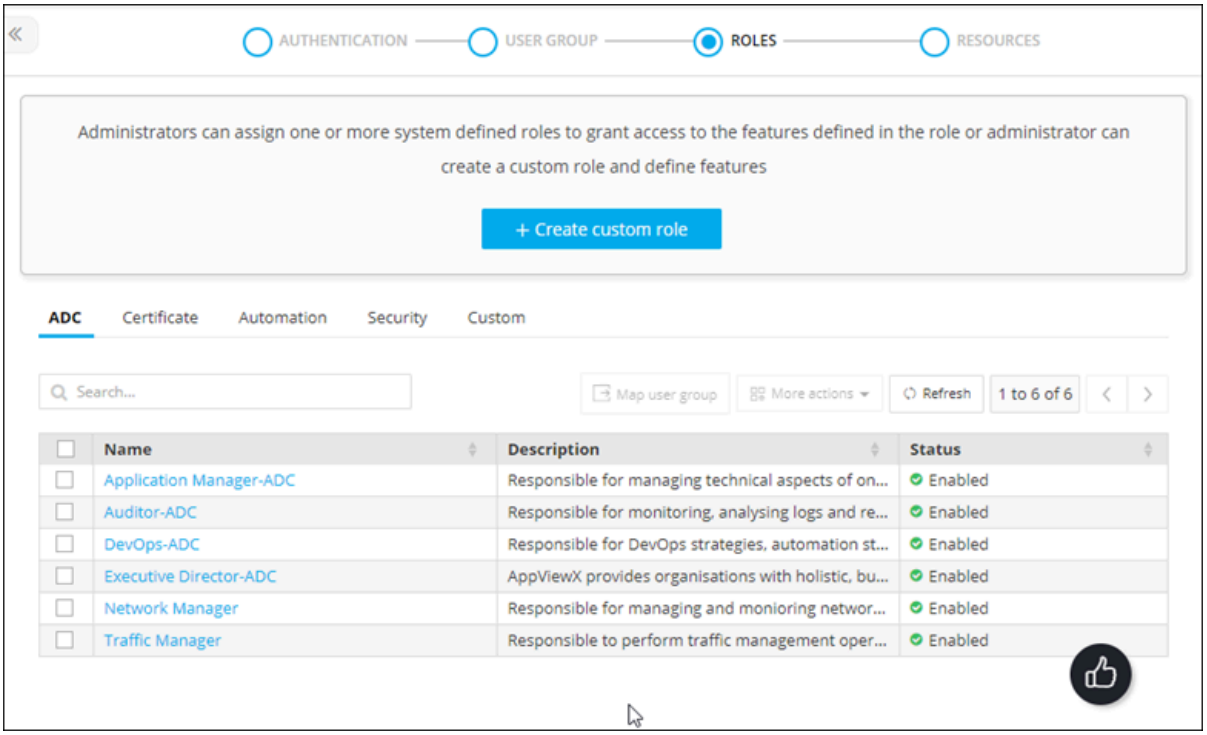
4. Click **Save**.
5. In the **Authorized functions** section, select the check box against the functionalities that you want to associate with the role.

6. To assign functions at a granular level, click the icon for the functions check box and then select individual sub-options within the functions.
7. Click **Save**.

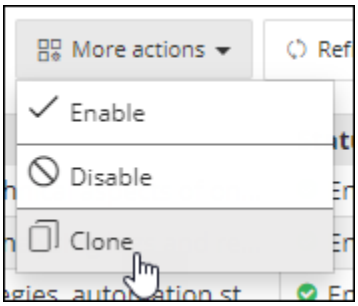
Cloning a Role

To clone an existing role to a custom role:

1. On the **RBAC Journey :: Authentication** page, navigate to the **ROLES** stage as part of the wizard flow to add roles into AppViewX.



2. For the role, you want to clone, select the check box against that role.
3. From the **More actions** drop-down menu, select **Clone**.

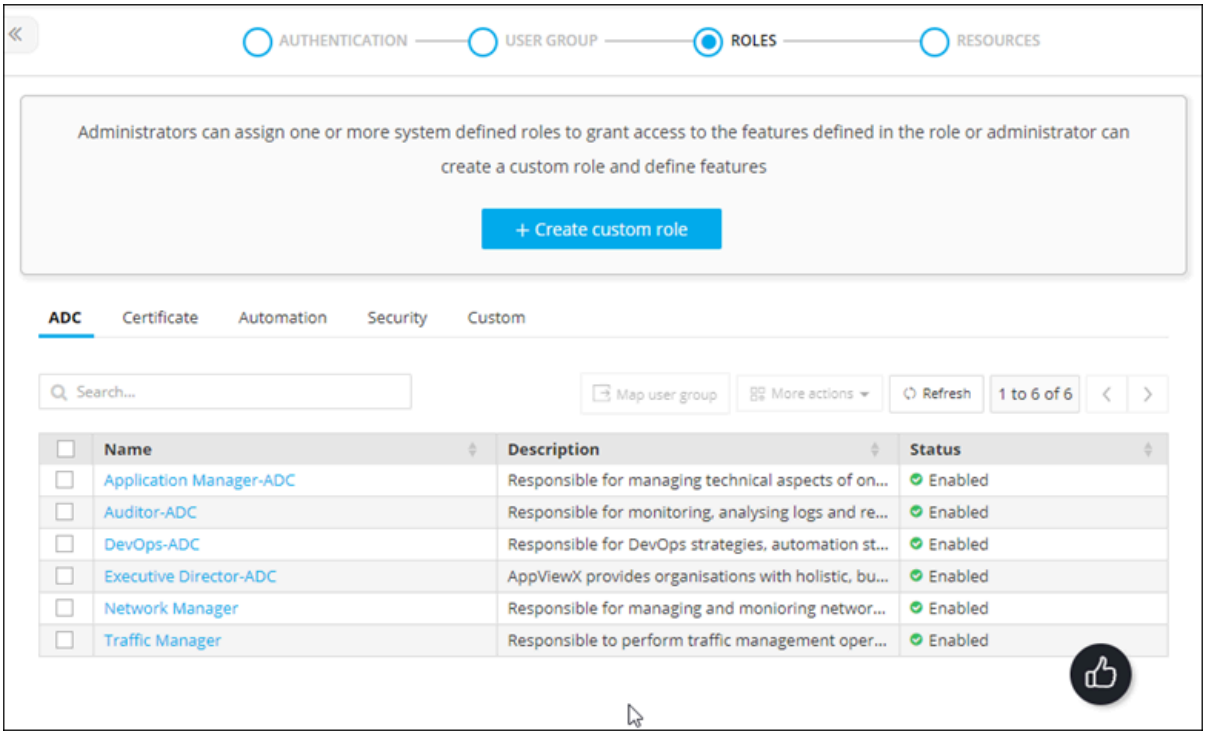


4. In the **Clone** action pane, modify the details in the **Information** and **Authorized functions** sections as required.
5. Click **Save**.

Modifying a Role

To modify a custom role:

1. On the **RBAC Journey :: Authentication** page, navigate to the **ROLES** stage as part of the wizard flow to add roles into AppViewX.



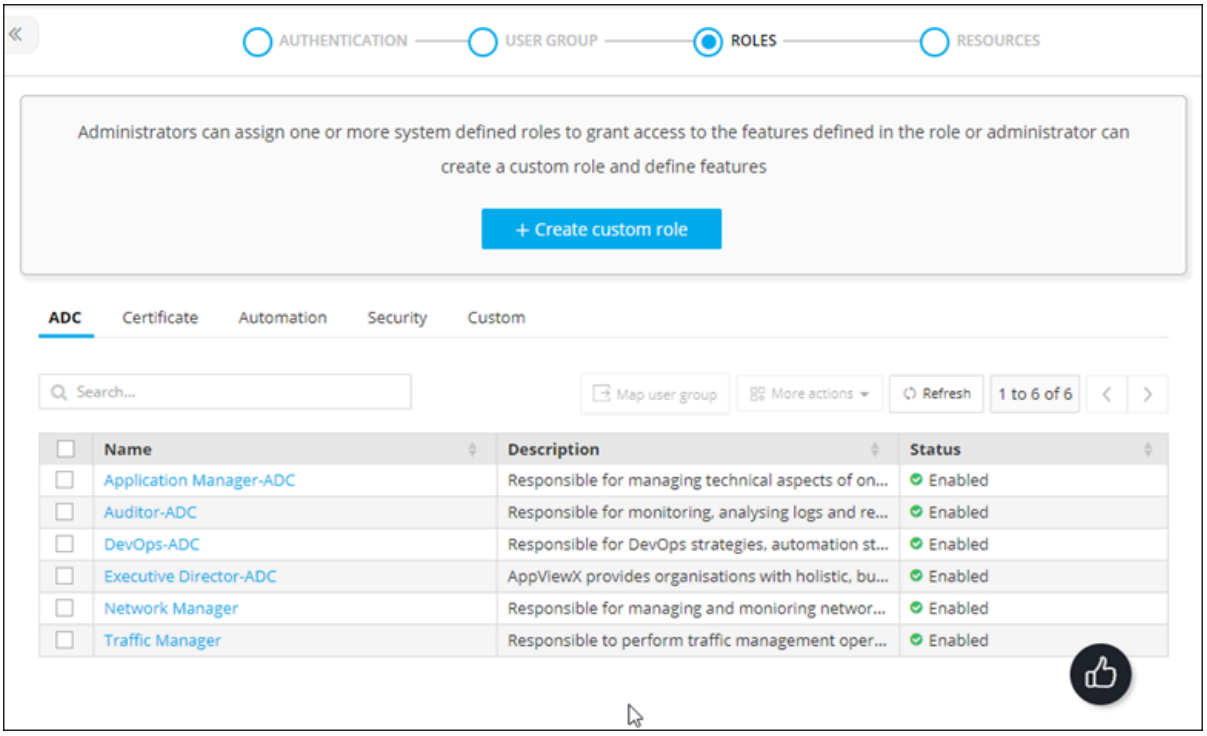
2. Click the role name you want to modify.
3. The **Edit role** action pane is displayed for the selected role.
4. Modify the details in the **Information** and **Authorized functions** sections as required.
5. Click **Save**.

> **Note:** Out of the box role functions can not be edited. Only custom role functions can be edited.

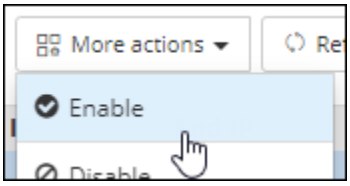
Enabling a Role

To enable a role:

1. On the **RBAC Journey :: Authentication** page, navigate to the **ROLES** stage as part of the wizard flow to add roles into AppViewX.



2. To enable a role, select the check box against that role.
3. From the **More actions** dropdown menu, select **Enable**.



4. In the **Enable** role(s) dialog box, click **Yes**.

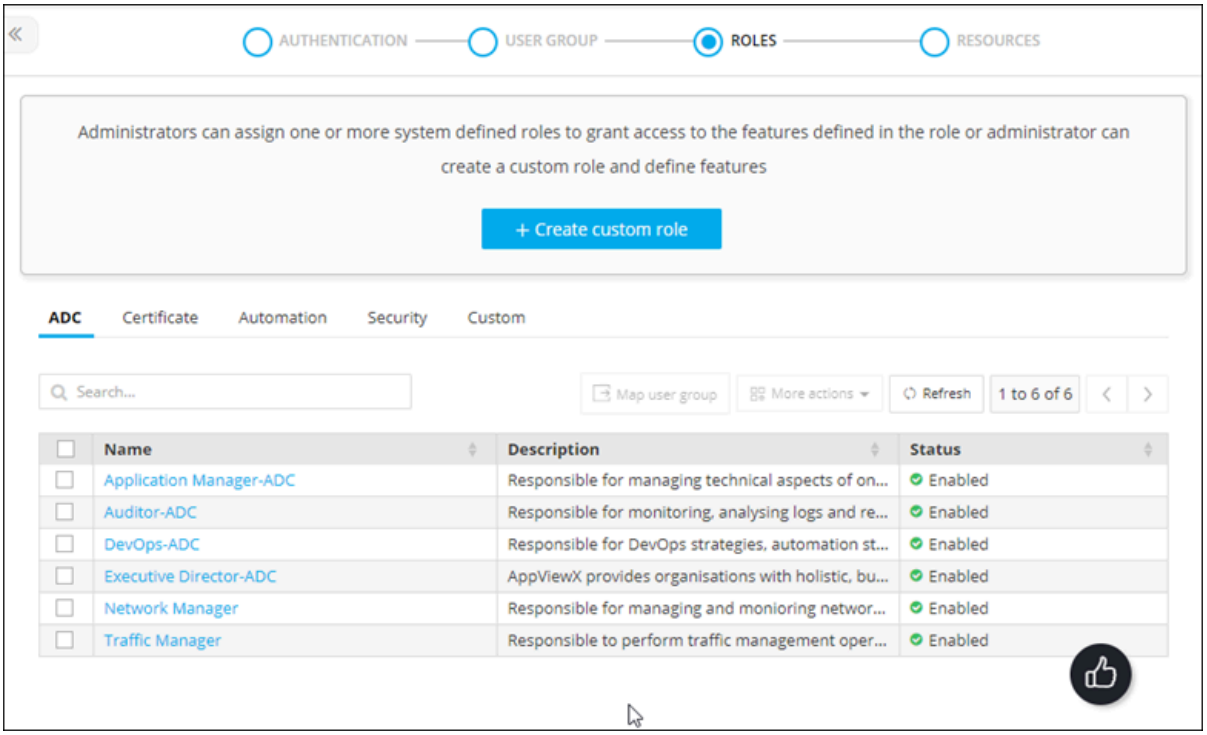
Disabling a Role

Note: You cannot disable roles that have active users associated with them.

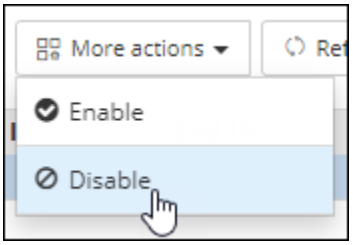
Note: The users associated with a disabled role through a user group will not be allowed to log in to AppViewX.

To disable a role:

1. On the **RBAC Journey :: Authentication** page, navigate to the **ROLES** stage as part of the wizard flow to add roles into AppViewX.



2. To disable a role, select the check box against that role.
3. From the **More actions** dropdown menu, select **Disable**.

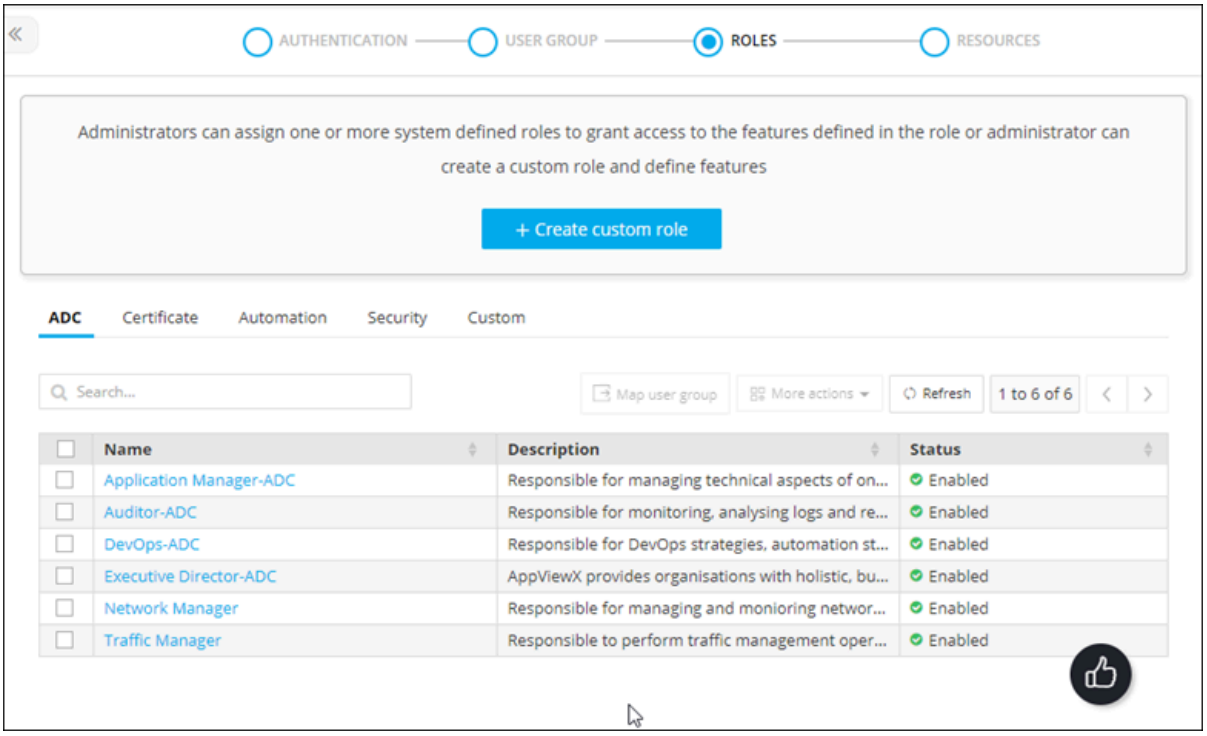


4. In the **Disable** role(s) dialog box, click **Yes**.

Mapping Role to User Groups

To map roles to user groups:

1. On the **RBAC Journey :: Authentication** page, navigate to the **ROLES** stage as part of the wizard flow to add roles into AppViewX.



2. For the role, you want to map to user groups, select the check box against that role.
3. Click 

.
4. In the **Mapping user group** action pane, select the user groups the role will be mapped to.
5. Click **Save**.

   The saved list of user groups will be displayed as a hyperlink in the rule inventory for each group.

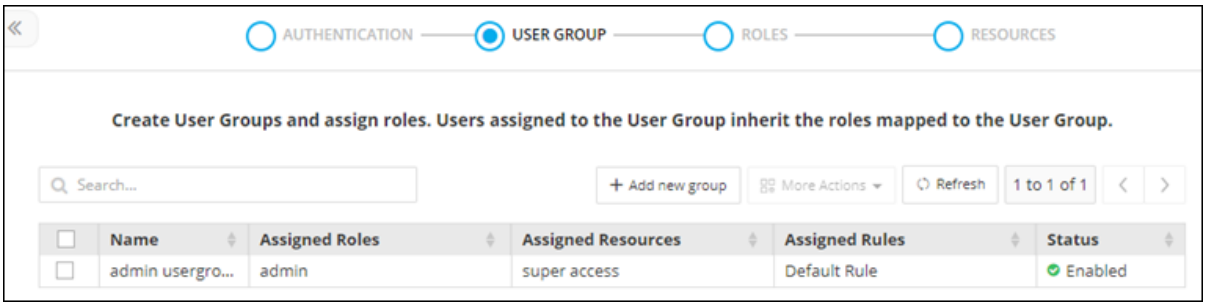
User Group

A user group is a group of individuals that have access to the same roles and resources. When you associate a role and resource with a user group, the users within that user group are granted all of the roles and resources' corresponding privileges and permissions. User Groups can be created manually or synced from the Active Directory or can be bulk uploaded using a spreadsheet.

Note: You can associate the roles and resources only with the user groups.

Once Authentication details are configured:

1. Go to the **User Group** stage as part of the wizard flow to add user groups into AppViewX.



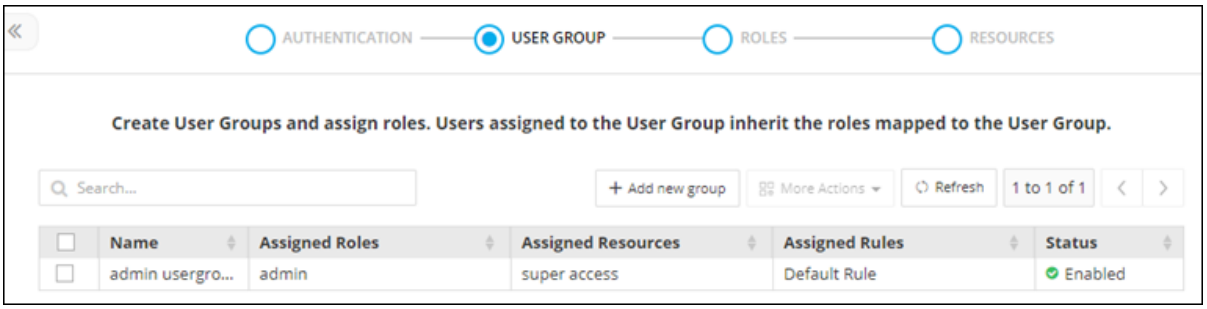
   The User group inventory table is displayed with the list of available user groups in AppViewX along with corresponding roles and resources mapping.
2. In the User group stage, user group creation can be done by fetching groups from LDAP or through bulk import.
3. In addition to this, existing user groups can be cloned, enabled, disable, and deleted.

- Adding a New User Group by Syncing Groups from LDAP
- Adding a New User Group using the TACACS/RADIUS/SAML/AppViewX Option
- Add New User Group by Bulk Import
- Cloning a User Group
- Enabling a User Group
- Disabling a User Group
- Deleting a User Group

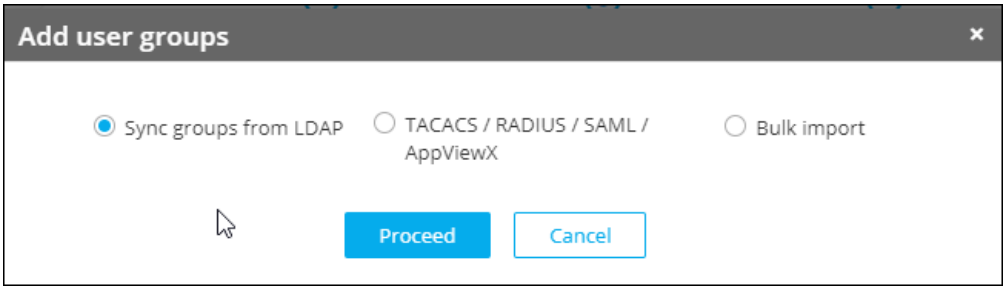
Adding a New User Group by Syncing Groups from LDAP

To create a new user group by syncing groups from LDAP:

1. On the **RBAC Journey :: Authentication** page, navigate to the **USER GROUP** stage as part of the wizard flow to add user groups into AppViewX.

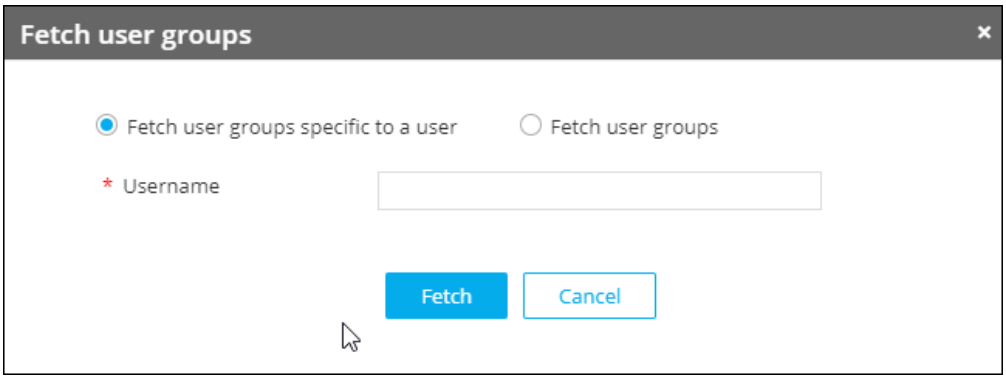


2. Click + Add new group.
3. From the **Add user groups** dialog box, select **Sync groups from LDAP** and click **Proceed**.



The LDAP inventory table is displayed.

4. To view the user groups available in the AD and create or map them with the existing user groups in AppViewX, from the LDAP inventory table, click Fetch.
The **Fetch user groups** dialog box is displayed.

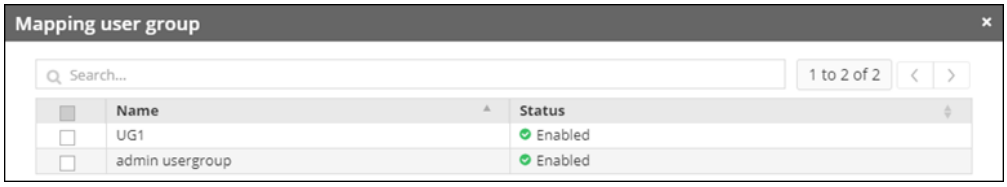


5. In the **Fetch user groups** dialog box:

- To fetch user groups according to a specific user, select **Fetch user groups specific to a user** and enter the **Username** of the AD user.
- To fetch user groups by a specific name, select **Fetch user groups** and type the **User group name** from the AD.

> **Note:** You can search the user group either by entering the complete user group name or using wild card characters (*).

6. Click **Fetch**.
   A table containing the AD group names and their corresponding AppViewX user group names is displayed.
7. Select the AD user group(s) that must be created with the same name in AppViewX and click Save to Appviewx.
8. To select the AD user group(s) to be mapped with the existing AppViewX user group:
   a. Select the user group to be mapped with the existing AppViewX user group.
   b. From the **More actions** list, select **Create Map**.
   c. From the **Mapping user group** action pane, select the existing AppViewX user group to be mapped.



   d. Click **Save**.

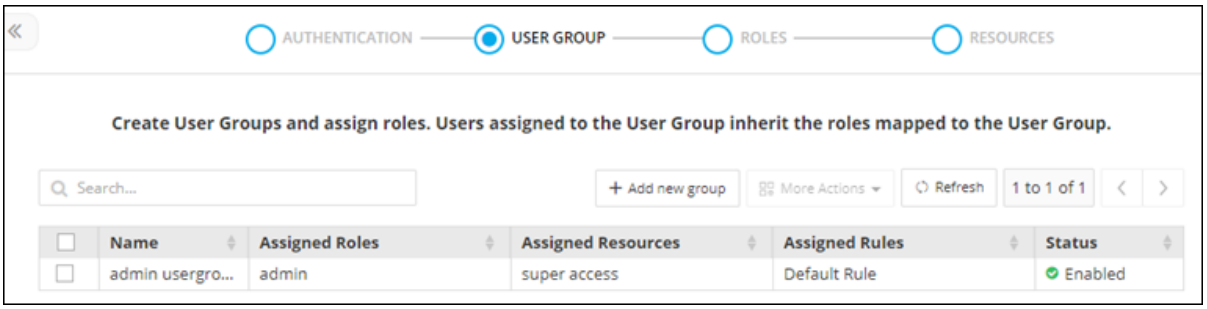
   Selected AD user group(s) will be now mapped to the existing AppViewX user group and the same mapping will reflect in the AD group names table.

9. To export specific AD groups:
   a. Select the user group to be mapped with the existing AppViewX user group. From the **More actions** list, select **Export**.
   b. From the **Export user groups** action pane, select the **Selected group (S)** option and click **Yes**.
   c. To export all user groups, select the **All User Group(s)** option and click **Yes**.
   d. The selected/all user group(s) should be automatically exported in (.CSV) Format.

Adding a New User Group using the TACACS/RADIUS/SAML/AppViewX Option

To create a new user group using the TACACS/RADIUS/SAML/AppViewX option:

1. On the **RBAC Journey :: Authentication** page, navigate to the **USER GROUP** stage as part of the wizard flow to add user groups into AppViewX.

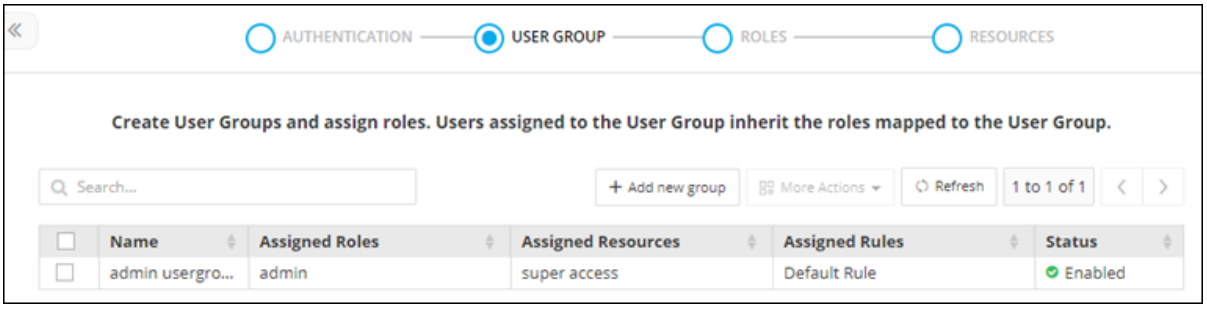


2. Click + Add new group.
3. From the **Add user groups** dialog box, select **TACACS/RADIUS/SAML/AppViewX** and click **Proceed**.
4. Enter the **Name** and **Description** for the user group.
5. Click **Submit**.

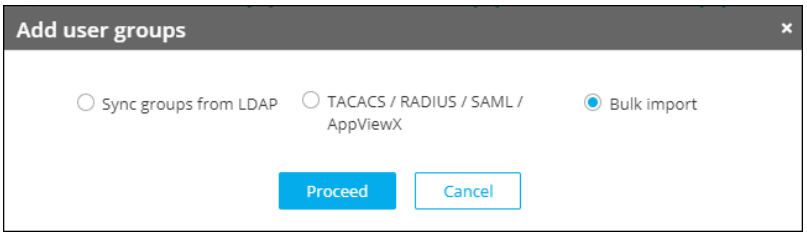
Add New User Group by Bulk Import

To add a new user group using the bulk import feature:

1. On the **RBAC Journey :: Authentication** page, navigate to the **USER GROUP** stage as part of the wizard flow to add user groups into AppViewX.



2. Click + Add new group.
3. From the **Add user groups** dialog box, select **Bulk import**, and then click **Proceed**.



4. Click **Browse**.
5. To upload your CSV file, in the **Select a file** field, click **Browse**.

> **Note:** To view the sample file for the formatting of the CSV file, click .

6. Click **Upload**. User group validation is performed on the imported user groups and the validation status (Valid/Invalid) is displayed.

> **Note:** The validation status can be invalid for reasons like duplicate group name, invalid group name (group name does not meet the group naming criteria, and so on).

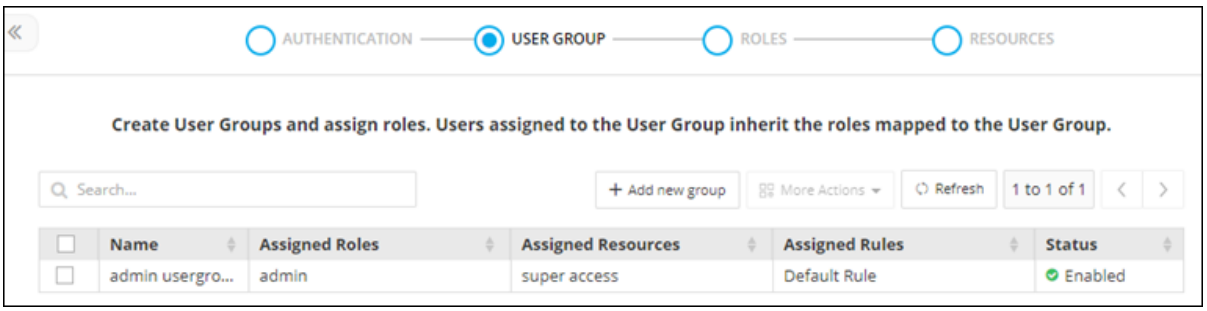
7. To save the user groups, select the list of user groups and click **Submit**.
   All user groups with the valid status will be saved into AppViewX.

> **Note:** Once you go back to the User group inventory table, you need to re-upload the file to add the user group.

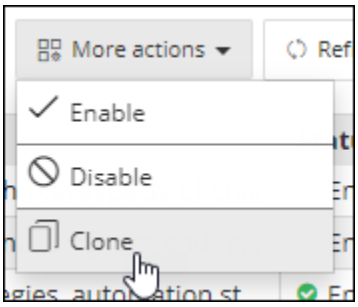
Cloning a User Group

To clone a user group:

1. On the **RBAC Journey :: Authentication** page, navigate to the **USER GROUP** stage as part of the wizard flow to add user groups into AppViewX.



2. From the inventory table, select the user group to be cloned.
3. From the **More Actions** drop-down menu, select **Clone**.

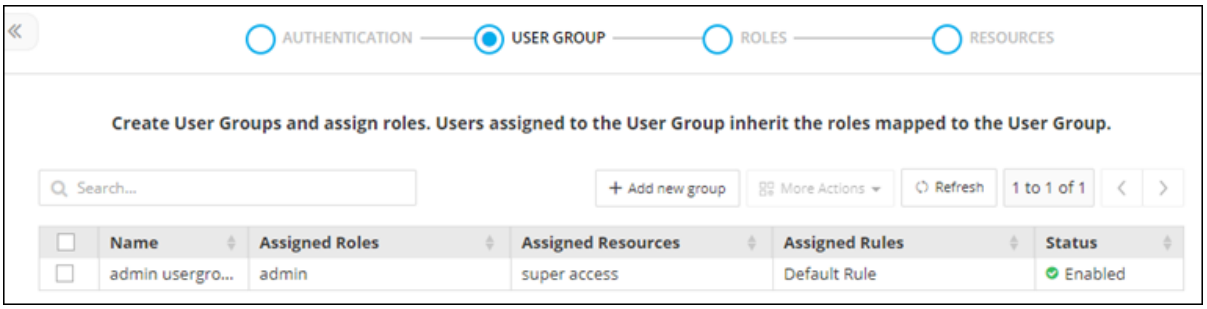


4. In the **Clone** dialog box, enter a name for the cloned user group and update the description, if required.
5. Click **Save**.

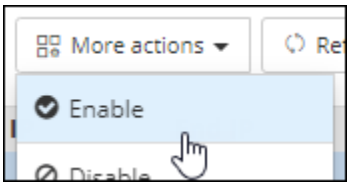
Enabling a User Group

To enable a user group:

1. On the **RBAC Journey :: Authentication** page, navigate to the **USER GROUP** stage as part of the wizard flow to add user groups into AppViewX.



2. From the inventory table, select the user group to be enabled.
3. From the **More Actions** drop-down menu, select **Enable**.

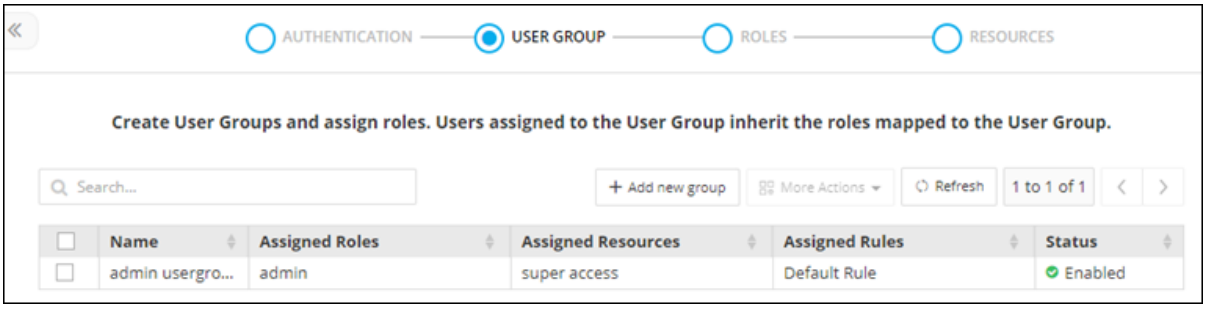


4. From the **Enable user group** dialog box, click **Yes**.

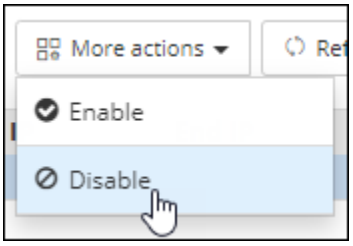
Disabling a User Group

To disable a user group:

1. On the **RBAC Journey :: Authentication** page, navigate to the **USER GROUP** stage as part of the wizard flow to add user groups into AppViewX.



2. From the inventory table, select the user group to be disabled.
3. From the **More Actions** drop-down menu, select **Disable**.

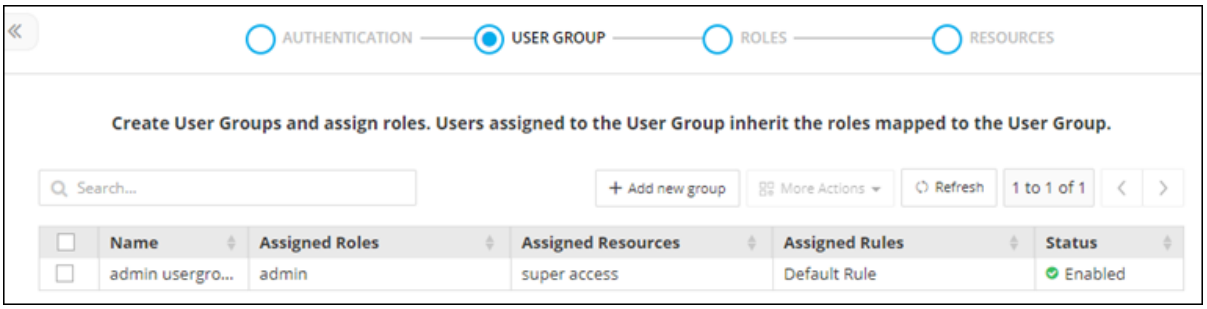


4. From the **Disable user group** dialog box, click **Yes**.

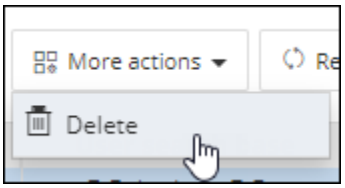
Deleting a User Group

To delete a user group:

1. On the **RBAC Journey :: Authentication** page, navigate to the **USER GROUP** stage as part of the wizard flow to add user groups into AppViewX.



2. From the inventory table, select the user group to be deleted.
3. From the **More Actions** drop-down menu, select **Delete**.



4. From the **Delete user group** dialog box, click **Yes**.

Configuring Privileged Access Management

For a more sophisticated management of critical data and infrastructure, AppViewX allows for Privileged Access Management (PAM). In simple words, PAM is the practice of managing users/devices/ applications that have elevated access to an organization's most confidential and critical resources.

To configure PAM settings:

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **VAULT & SECURITY**, select **PAM**. The **PAM** page is displayed with a list of devices/ objects/applications with Privileged Access Management.	From the main navigation menu, select **Inventory** > **Device**. The **Device :: ADC** page is displayed with the **ADC** tab open by default.
Note: For more information on how to switch between menus, click here.	

1. From the command bar in the top right corner of the page, click  **(Add Credentials)** icon.
2. From the left pane, select the vendor for whom you want to configure PAM.

   Credential details fields are displayed for the selected vendor.
3. Enter the **Credential details** for the vendor.
   - To enter the credential details for AppViewX, click here.
   - To enter the credential details for CyberArk, click here.
   - To enter the credential details for Thycotic, click here.

- To enter the credential details for Hashicorp, click here.
- To enter the credential details for BeyondTrust, click here.

4. Click **Save**.

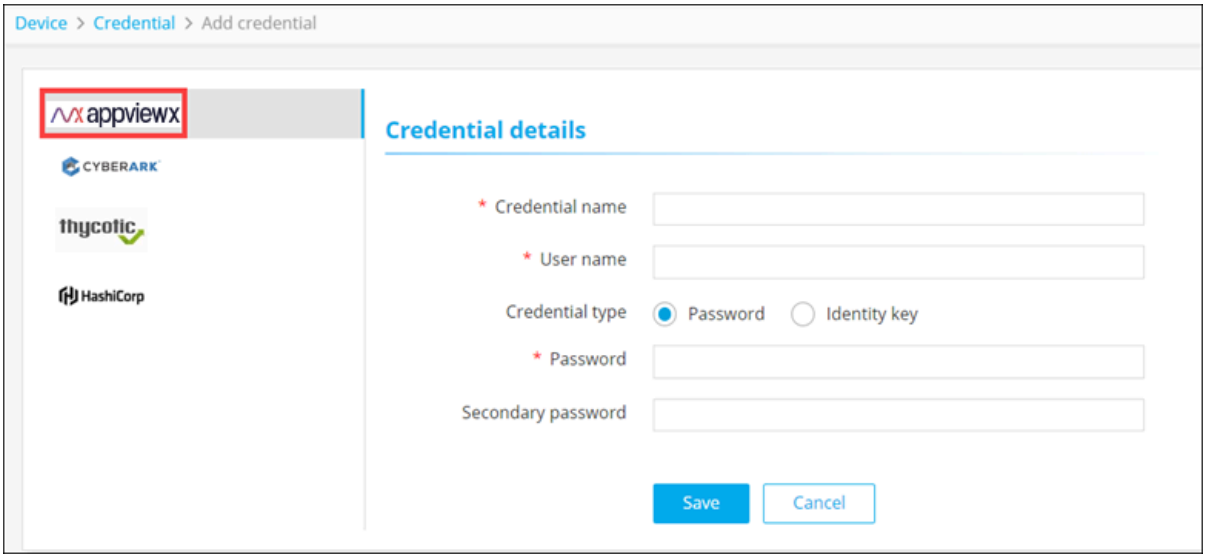
- AppViewX
- CyberArk
- Thycotic
- HashiCorp
- BeyondTrust

AppViewX

AppViewX is shipped with a built-in integration with HashiCorp Vault for software level security to secure the private keys and device credentials onboarded to the product.

To configure credential details for the AppViewX vault:

1. Go to **Platform > VAULT & SECURITY > PAM**.
2. The **PAM** page is displayed with a list of devices/objects/applications with Privileged Access Management.
3. On the **+ Add credential** page, select **AppViewX** from the left menu.
4. In the **Credential details** section, enter the required field information.



Field descriptions for Credential details

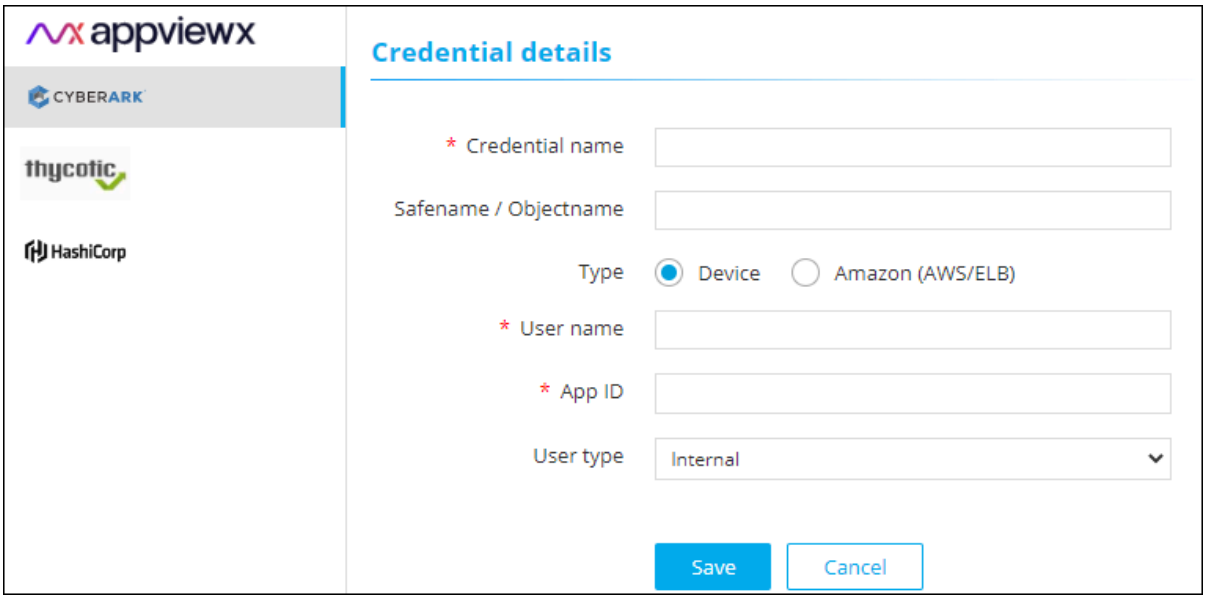
Field	Description
***Credential name**	Name for the credential for the users to identify it.
***User name**	User name used for device onboarding.
Credential type	Select the type of authentication from one of the following: • Password • Identity key.
***Password**	Password configured at the time of device onboarding. **Note:** This field is displayed only when the **Credential type** is selected as **Password**.
Secondary password	Additional password enabled by vendors for specific operations. **Note:** This field is displayed only when the **Credential type** is selected as **Password**.
***Identity key**	Credentials (upload private key in the **.pem** or **.txt** or **.rsa** or **.ppk** format only) for enabling device communication via SSH. **Note:** This field is displayed only when the **Credential type** is selected as **Identity key**.
Passphrase	Key to protect the private key files. **Note:** This field is displayed only when the **Credential type** is selected as **Identity key**.
Note: The asterisk (*) symbol indicates mandatory fields.	

5. Click **Save**.

CyberArk

To configure credential details for the CyberArk vault:

1. Go to **Platform > VAULT & SECURITY > PAM**.
2. The **PAM** page is displayed with a list of devices/objects/applications with Privileged Access Management.
3. On the **+ Add credential** page, select **CyberArk** from the left menu.
4. In the **Credential details** section, enter the required field information.



Field descriptions for Credential details

Field	Description
***Credential name**	Name for the credential for the users to identify it.
Safename / Objectname	Name of the safe/object where the password is stored.
Type	To retrieve a credential from the CyberArk vault, select one of the following options: • Device (default) • Amazon (AWS/ELB).
***User name**	User name that has been added in CyberArk. **Note:** This field is displayed when the **Device** type is selected.

Field	Description
***App ID**	App ID that has been authorized to provide access to CyberArk and retrieve credentials. **Note:** This field is displayed when the **Device** type is selected.
User type	From the drop-down menu, select one of the following: • Internal (user created directly in the device) • External (user created in the Active Directory). **Note: *Server IP Address** field is displayed when the **User type** is selected **External**.
***Server IP Address**	The server IP Address has to be entered if the user has created an external active directory. It is utilized for integrating service accounts, particularly when external integration is required. By selecting "external," the input of the server's (LDAP/AD) IP address is taken, which manages the service account. **Note:** This field is displayed when the User type is selected as **External**.
***AWS IAM username**	User name that has been added in CyberArk. **Note:** This field is displayed when the **Amazon** (AWS/ELB) type is selected.
***App ID**	Reference ID provided by CyberArk for the corresponding application. **Note:** This field is displayed when the **Amazon** (AWS/ELB) type is selected.
***AWS access key ID**	Access key ID generated from the AWS management console. **Note:** This field is displayed when the **Amazon** (AWS/ELB) type is selected.

Field	Description
Note: The asterisk (*) symbol indicates mandatory fields.	

5. Click **Save**.

• Steps for Integration

Steps for Integration

To configure credential details for the CyberArk vault:

1. On the **Add credential** page, select **CyberArk** from the left menu.
2. From the top right corner of the page, click **CyberArk API Settings**.
   The **CyberArk API Settings** pop-up window is displayed.

Field descriptions for CyberArk API Settings

Field	Description
***IIS-Server IP/Hostname**	Hostname or IP address of the CyberArk application.
***Port**	Port number on which CyberArk is running.
***Client certificate**	Upload the Client Certificate needed to authenticate the CyberArk API service.
***Passkey**	Enter the passkey for Client Certificates uploaded in the .pfx format.
Note: The asterisk (*) symbol indicates mandatory fields.	

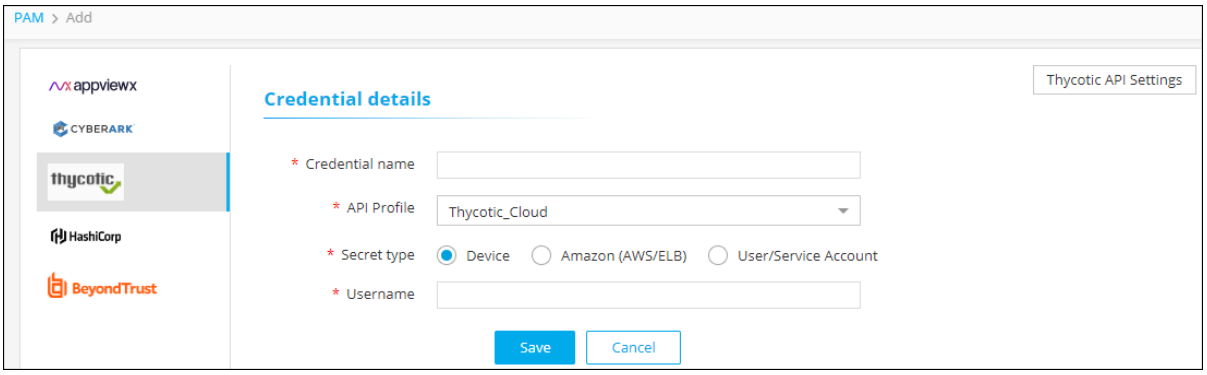
3. Once the details are entered, click **Update**.

Note: Multiple vaults can not be added by configuring multiple profiles.

Thycotic

To configure credential details for the Thycotic vault:

1. Go to **Platform > VAULT & SECURITY > PAM**.
2. The **PAM** page is displayed with a list of devices/objects/applications with Privileged Access Management.
3. On the **+ Add credential** page, select **Thycotic** from the left menu.
4. In the **Credential details** section, enter the required field information.



Field descriptions for Credential details

Field	Description
***Credential name**	Reference name for Thycotic in AppViewX.
***API Profile**	If you have more than one Thycotic Server added as profiles, select the respective profile while adding credentials.
***Secret Type**	The "Secret Type - Device" works if the Thycotic secret contains both the username and device name. This option is beneficial if you have multiple secrets in your Thycotic vault that share a username but have different device names associated with them. You can add a single secret to AppViewX with the username, and when fetching the credential from the vault, AppViewX will automatically send the corresponding device name or IP along with the username to retrieve the correct credentials. For this option to work, the device name or IP in the secret must match the device name or IP used in AppViewX. If the secret in the Thycotic vault does not have a device name associated with it, this option will not work, and you will need to use the "User/Service Account" service type instead. For example, you can use Thycotic secret templates such as "Windows Account" or "Unix Account (SSH)" that require a device name.

Field	Description
	The "Secret Type - Amazon (AWS/ELB)" is useful for adding Amazon credentials to AppViewX. You can use the Thycotic secret template "Amazon IAM Key" with this option. The "Secret Type - User/Service Account" is beneficial if you have a common secret in your Thycotic vault that works across multiple devices. This type of Thycotic secret template does not have a device name associated with it because it works across multiple devices. Therefore, when fetching the credential, AppViewX will only send the username of the credential to the Thycotic vault. For example, you can use Thycotic secret templates such as "Active Directory Account," "Azure AD Account," or "CISCO Account (SSH)," which do not require a device name in the secret template.
Username	Enter the username of the secret if you selected the Secret Type as Device.
AWS IAM Username	Enter the AWS IAM username if you selected the Secret Type as Amazon.

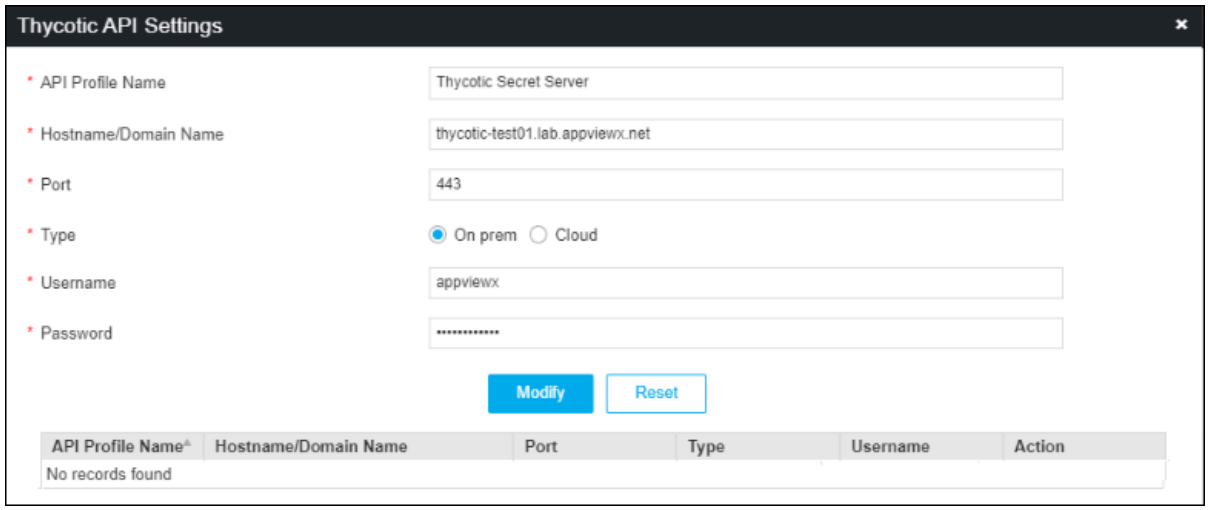
Note: The asterisk (*) symbol indicates mandatory fields.

5. Click **Save**.

• Steps for Integration

Steps for Integration

1. On the **Add credential** page, select **Thycotic** from the left menu.
2. From the top right corner of the page, click **Thycotic API Settings**.
   The **Thycotic API Settings** pop-up window is displayed.



Field descriptions for Thycotic API Settings

Field	Description
***API Profile Name**	Reference name for the vault in AppViewX.
***Hostname/Domain Name**	Enter the Hostname of the Thycotic Secret Server if it is hosted in an on-prem environment or the Domain name can be include or exclude in the user name during synchronization of the Thycotic Secret Server if it is the cloud version.
***Port**	Port number of the Thycotic Secret Server.
***Type**	Select if Thycotic Secret Server is hosted in an On prem or Cloud environment.
***Username**	Username of Thycotic Secret Server.
***Password**	Password of Thycotic Secret Server.

Note: The asterisk (*) symbol indicates mandatory fields.

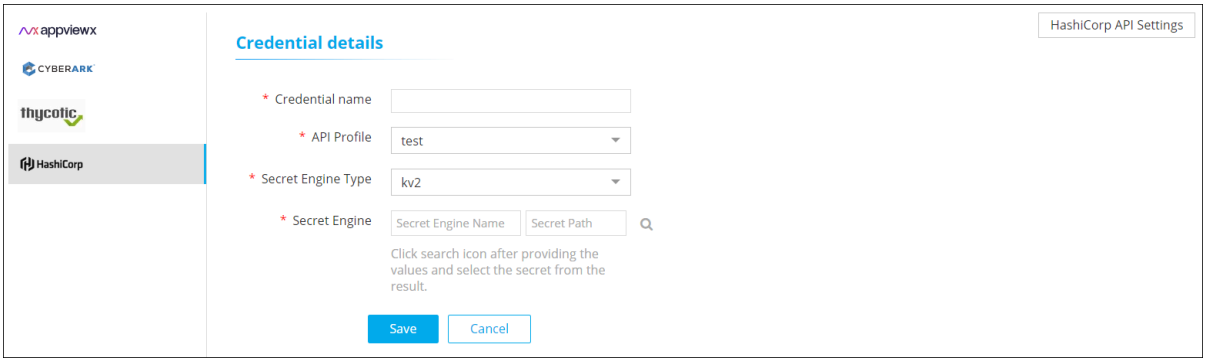
Note: You can add multiple Thycotic Secret Servers as different Profiles. Each Thycotic Secret Sever will be added to the Thycotic API settings page.

3. Once the details are entered, click **Add.**
4. To modify the details of any profiles, click name of profile, modify the details and click **Modify**.
5. To delete any profile, click **(Delete)** icon in Action column of profiles.

HashiCorp

To configure credential details for the HashiCorp vault:

1. Go to **Platform > VAULT & SECURITY > PAM**.
2. The **PAM** page is displayed with a list of devices/objects/applications with Privileged Access Management.
3. On the **+ Add credential** page, select **HashiCorp** from the left menu.
4. In the **Credential details** section, enter the required field information.



Field descriptions for Credential details

Field	Description
***Credential name**	Unique name for the credential for the users to identify it.
***API Profile**	Select the API profile from the dropdown list which is configured in HashiCorp API settings.
***Secret Engine**	Type path and click enter. It will suggest a list of secrets and the desired secret can be selected.

Note: The asterisk (*) symbol indicates mandatory fields.

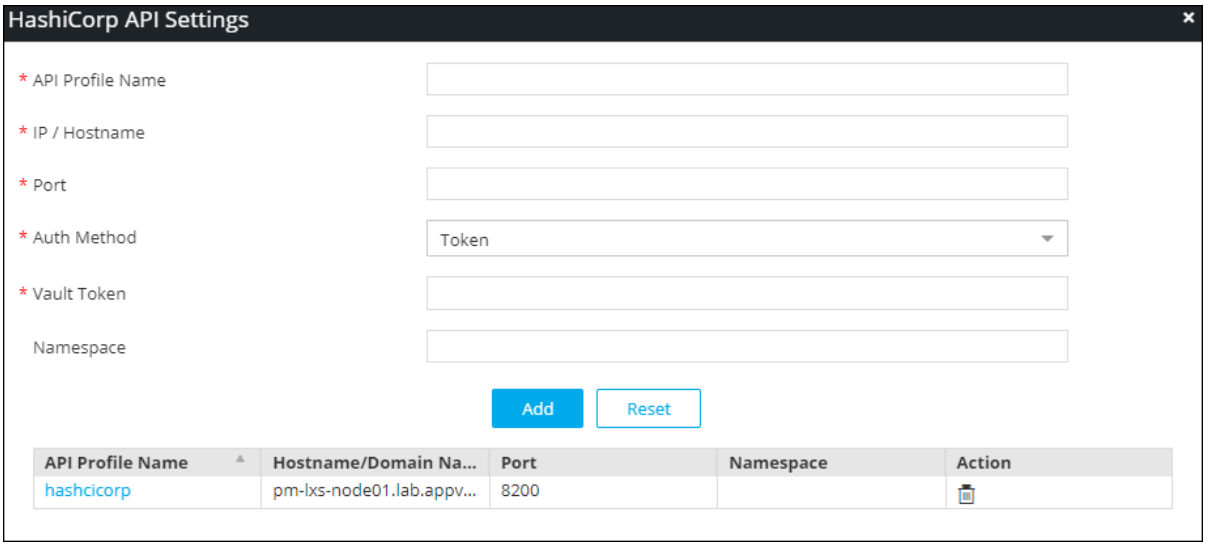
5. Click **Save**.

• Linking Credentials in AppViewX from Hashicorp Vault

Linking Credentials in AppViewX from Hashicorp Vault

To configure credential details for the HashiCorp vault:

1. On the **Add credential** page, from the top-right corner of the page, click **HashiCorp API Settings**.
   The **HashiCorp API Settings** window is displayed.



Field descriptions for HashiCorp API Settings

Field	Description
***API Profile Name**	Enter a unique API profile name.
***IP/Hostname**	Enter the HashiCorp vault hosted IP address or hostname.
***Port**	Enter the port in which the HashiCorp vault is running.
***Auth Method**	From the drop-down list, select either **Token/AppRole.** • If **Token** is selected, enter the **Vault Token** for the authentication.  • If **AppRole** is selected, enter the following:  • Enter the **RoleID** • Enter the **SecretID**.
Namespace	Enter a namespace.

Field	Description
	Note: The asterisk (*) symbol indicates mandatory fields.

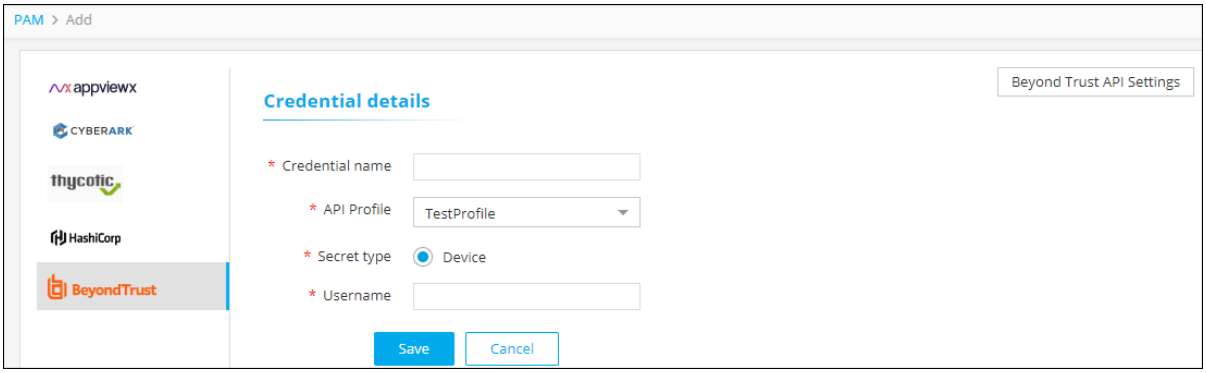
2. Once the details are entered, click **Add.**

Note: Multiple vaults can be added by configuring multiple profiles.

BeyondTrust

To configure credential details for the BeyondTrust vault:

1. Go to **Platform > VAULT & SECURITY > PAM**.
2. The **PAM** page is displayed with a list of devices/objects/applications with Privileged Access Management.
3. On the **+ Add credential** page, select **BeyondTrust** from the left menu.
4. In the **Credential details** section, enter the required field information.



Field descriptions for Credential details

Field	Description
***Credential name**	Reference name for BeyondTrust in AppViewX.
***API Profile**	If you have more than one BeyondTrust Server added as profiles, select the respective profile while adding credentials.
***Secret Type**	Select the secret type as Device. Only secrets associated with any device can be added with this secret type. Secret should contain the device name.

Field	Description
***Username**	Enter the username of the secret if you selected the Secret Type as Device. When this secret is used in any device, respective device name will be automatically send as one of the argument when AppViewX fetches credential from Vault.

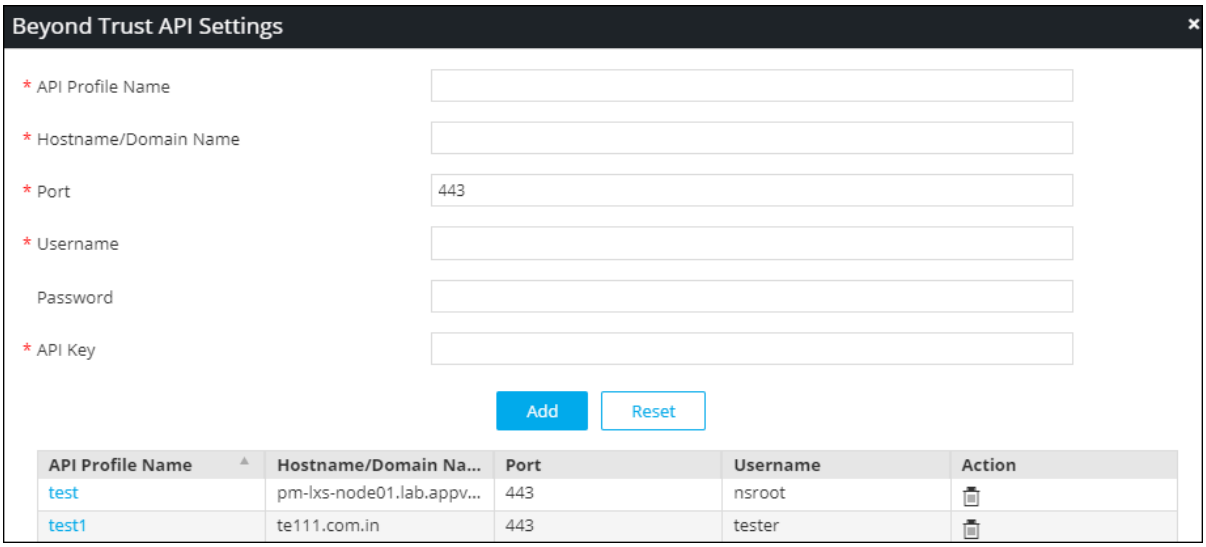
Note: The asterisk (*) symbol indicates mandatory fields.

5. Click **Save**.

• Steps for Integration

Steps for Integration

1. On the **Add credential** page, select **BeyondTrust** from the left menu.
2. From the top right corner of the page, click **BeyondTrust API Settings**.
   The **BeyondTrust API Settings** pop-up window is displayed.



Field descriptions for BeyondTrust API Settings

Field	Description
***API Profile Name**	Reference name for the vault in AppViewX.

Field	Description
***Hostname/ Domain Name**	Enter the Hostname of the BeyondTrust Secret Server if it is hosted in an on-prem environment or the Domain name of the BeyondTrust Secret Server if it is the cloud version.
***Port**	Port number of the BeyondTrust Secret Server.
***Username**	Username of BeyondTrust Secret Server.
Password	Password of BeyondTrust Secret Server.
***API Key**	It is the security key provided for authentication.

Note: The asterisk (*) symbol indicates mandatory fields.

Note: You can add multiple BeyondTrust Secret Servers as different Profiles. Each BeyondTrust Secret Server will be added to the BeyondTrust API settings page.

3. Once the details are entered, click **Add**.
4. To modify the details of any profile, click on the name of the profile, modify the details and click **Modify**.
5. To delete any profile, click **(Delete)** icon in the **Action** column of the profiles.

Configuring General Settings

- Configuring the SMTP Settings
- Managing Proxy Settings
- Setting the Cryptographic Policy
- Enabling Dashboard View for the User
- Managing the Login Configuration

Configuring the SMTP Settings

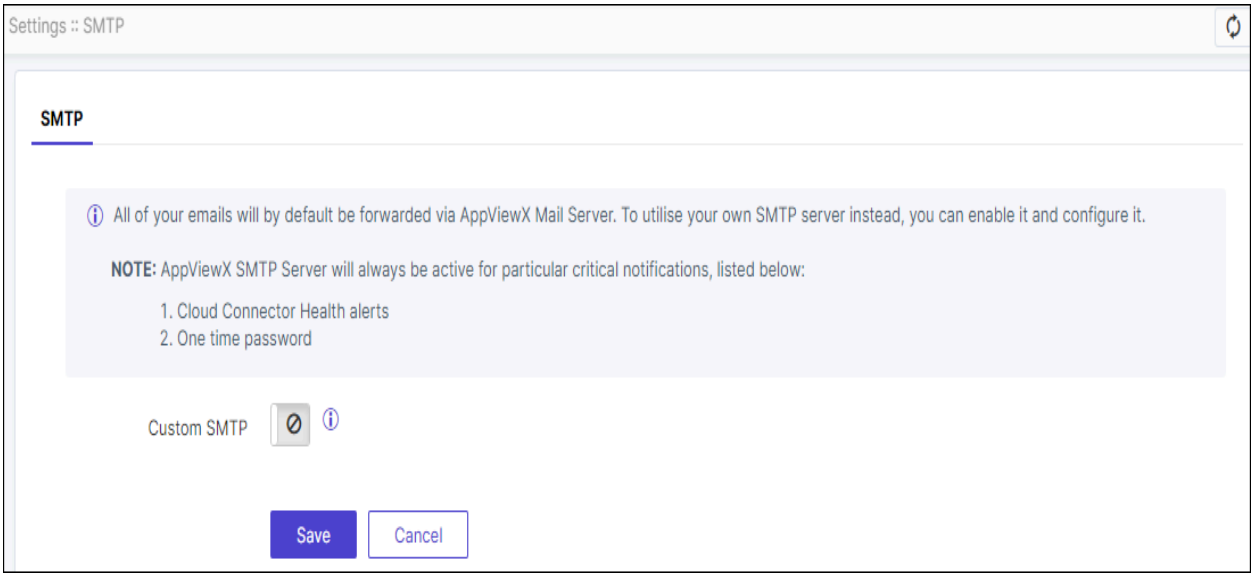
Accessing SMTP Settings Page

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **SYSTEM ADMINISTRATION**, select **SMTP**. The **Settings :: SMTP** page is displayed.	1. From the main navigation menu, click **Settings**. 2. On the **Settings** page, from the left menu, select **General** > **SMTP**. The **Settings :: SMTP** page is displayed.

Note: For more information on how to switch between menus, click here.

Configuring the SMTP Settings

When accessing the Settings :: SMTP page in SAAS, the following screen will be displayed.



1. Enable the **Custom SMTP** toggle to use your own SMTP server.
2. Configure **Custom SMTP** settings if the toggle is enabled; otherwise, emails will be sent through the AppViewX mail server by default.

   Note: AppViewX SMTP server will remain active for specific critical notifications, such as cloud connector health alerts and one-time passwords.

3. Click **Save**.

Configuring the SMTP Settings for Google

The SMTP configuration is required for AppViewX to be able to send logs and alerts via email and for other email related activities such as sending and receiving notifications and so on.

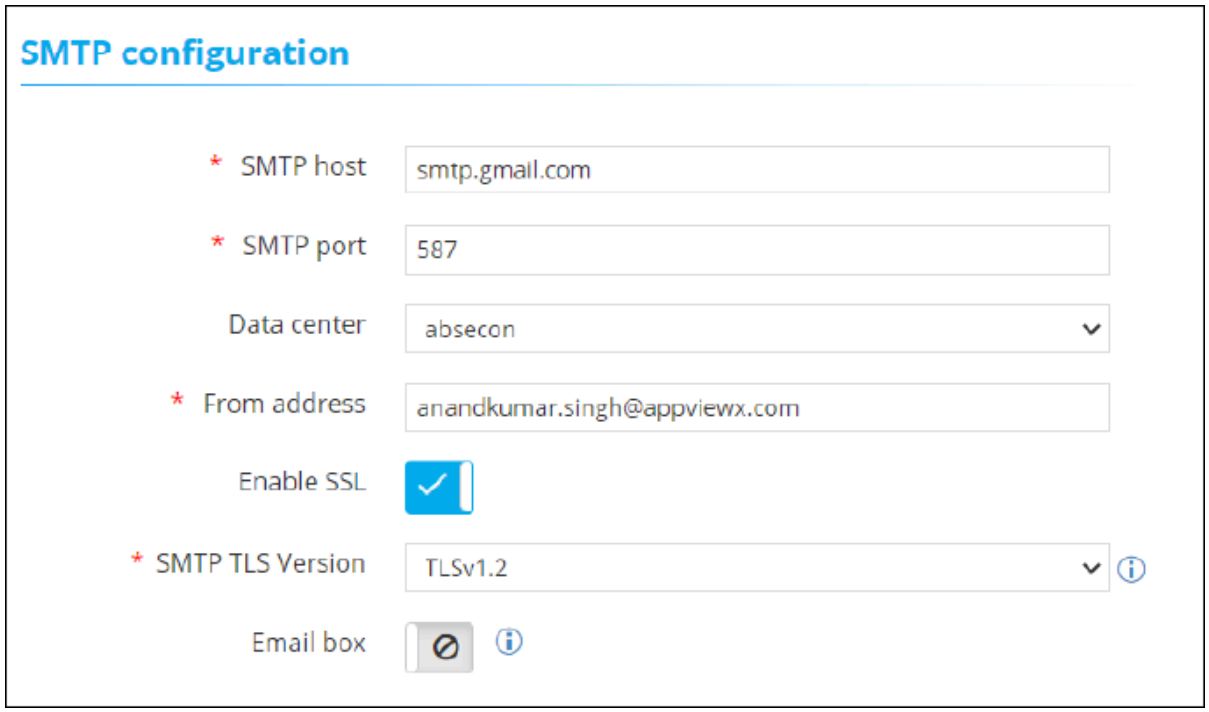
The SMTP oAuth uses an access token instead of a password to send email. The access token works as a temporary password with fixed validity and has permissions delegated by the user.

To get the access token you must provide details such as username, client-id, secret, Authorization endpoint, token Endpoint and scope. Once these details are submitted, you will be redirected to the oAuth server login page. Once the user authorization is done here, the oAuth server returns the Auth code.

The Auth code is exchanged with the access token and refresh token in the backend and saved in DB.

To configure the SMTP server:

1. On the **Settings :: SMTP** page, in the **SMTP configuration** section, enter the required field information.

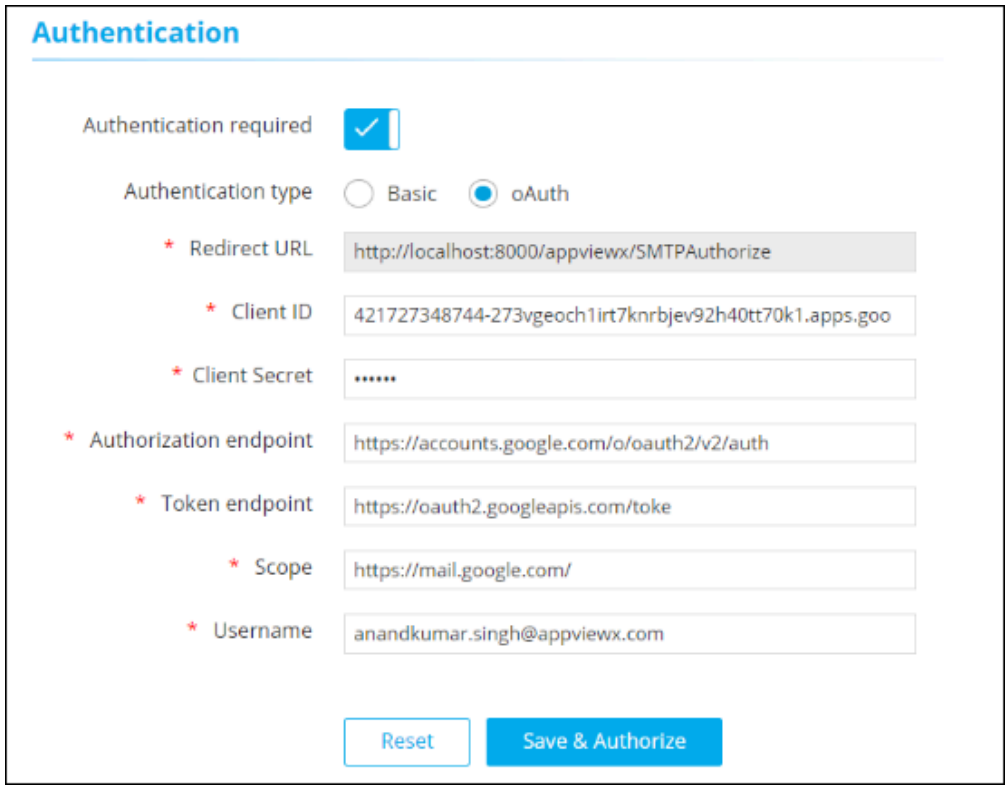


Field descriptions for SMTP configuration

Field	Description
***SMTP host**	Host name of the SMTP server.
***SMTP port**	Port number of the SMTP server.
Data center	From the options available in the dropdown, select the data center.
***From address**	Enter the email address that will be used to email the logs and alerts.
Enable SSL	To allow SSL encryption, enable this toggle key.
***SMTP TLS Version**	From the options available in the dropdown, select the TLS version of the SMTP server. **Note:** Versions 1.2 and higher are recommended.
Email box	To use the mailbox feature to read emails in Visual Workflow, enable this toggle key.

Field	Description
***Email**	Email address of the IMAP server used for the mailbox feature. **Note:** This field is displayed only if the **Email box** key is enabled.
***Password**	Password of the IMAP server used for the mailbox feature. **Note:** This field is displayed only if the **Email box** key is enabled.
***Host name**	Host name of the IMAP server used for the mailbox feature. **Note:** This field is displayed only if the **Email box** key is enabled.
***Port**	Enter the Port number. **Note:** This field is displayed only if the **Email box** key is enabled.
Note: The asterisk (*) symbol indicates mandatory fields.	

2. In the **Authentication** section, enter the required field information.

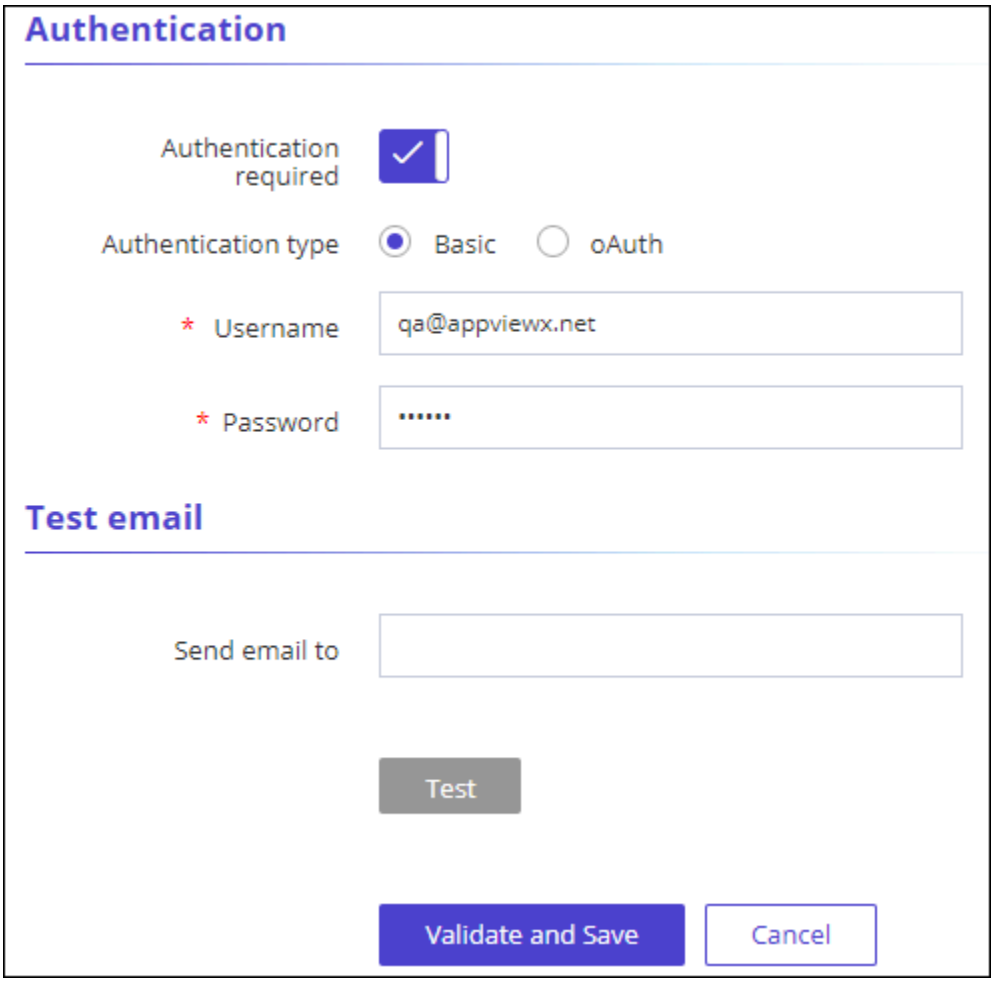


Field descriptions for Authentication

Field	Description
Authentication required	To enable authenticated mail server communication, enable this toggle.
Authentication type	Select the Authentication type as Basic. **Note:** Selecting Basic displays the Username and Password fields. Select the Authentication type as oAuth. **Note:** Selecting oAuth displays the fields that are described below.
***Redirect URL**	This field is auto-populated from the address bar of the browser.
***Client ID**	Enter the Client ID that is generated in the oAuth server when the oAuth client is created.

Field	Description
	Note: The steps to create an oAuth client are different for Google and Microsoft. For more information on steps for Google, click here. For more information on steps for Microsoft click here.
***Client Secret**	Enter the Client Secret that is generated in the oAuth server when the oAuth client is created.
***Authorization endpoint**	Enter the authorization endpoint where the user authorizes and gives permission to the oAuth client to send email on behalf of the user.
***Token endpoint**	Enter the token endpoint to get Access Token and Refresh Token. You can get the endpoint by providing Client ID, Secret, and other relevant values based on oAuth 2.0 specifications.
***Scope**	The permission required to send email. **Note:** For Google, enter **https://mail.google.com/**.
***Username**	**Note:** This field is enabled only if the **Authentication required** key is enabled. Username for the authenticated mail server
***Password**	**Note:** This field is enabled if you select **Basic** as your **Authentication type**. Enter the valid password associated with the username.
Note: The asterisk (*) symbol indicates mandatory fields.	

3. If the **Authentication type** is selected as **Basic**, displays the username and password attributes.
4. In the **Test email** section, enter the email address to which a test email should be sent and click **Test**.

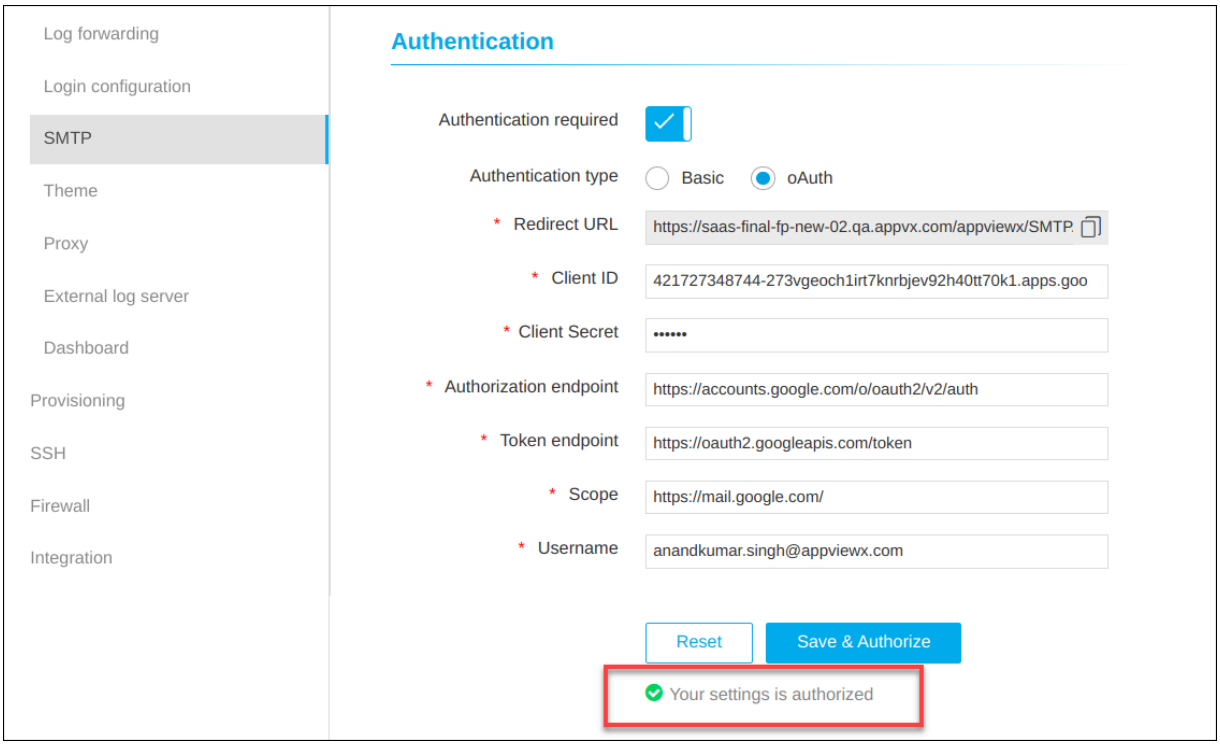


5. To save the SMTP configuration settings, click **Validate and Save**.
   Upon clicking "Validate and Save," an email will be sent to the user's email address for validation.

> **Note:** If the user does not have an email ID configured, an error will be displayed, prompting them to set up an email address.

> **Note:** In case of validation failure, the SMTP settings will not be saved.

6. If the **Authentication type** is selected as **oAuth**, To save the SMTP configuration settings, click **Save & Authorize**.
7. Displays confirmation of SMTP Settings Authorized.



A new tab will open, prompting for sign-in.

Once authorization is done the user receives an access token and a refresh token from the token endpoint. The access token is used for sending email and the refresh token is used for renewing the access token upon its expiry.

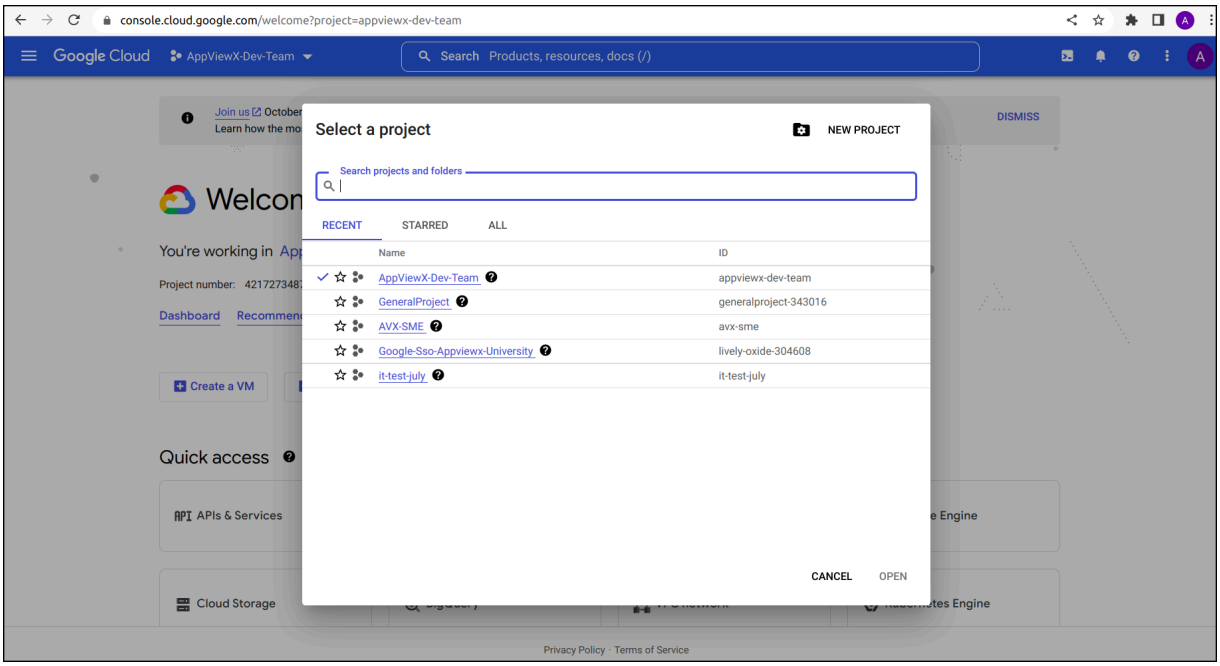
- Authentication for Google SMTP Settings

Authentication for Google SMTP Settings

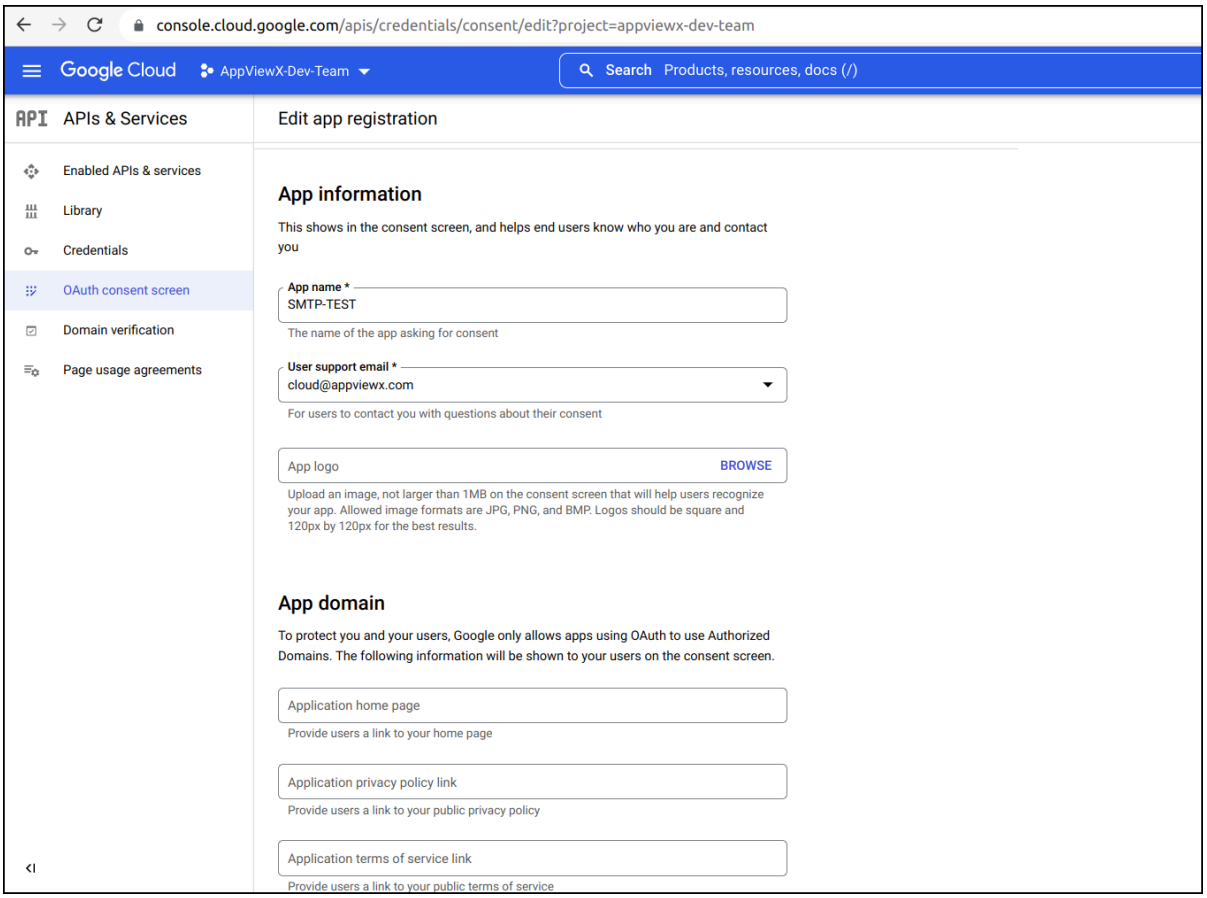
Create authorization credentials

Any application that uses OAuth 2.0 to access Google APIs must have authorization credentials that identify the application to Google's OAuth 2.0 server. The following steps explain how to create credentials for your project. Your applications can then use the credentials to access APIs that you have enabled for that project.

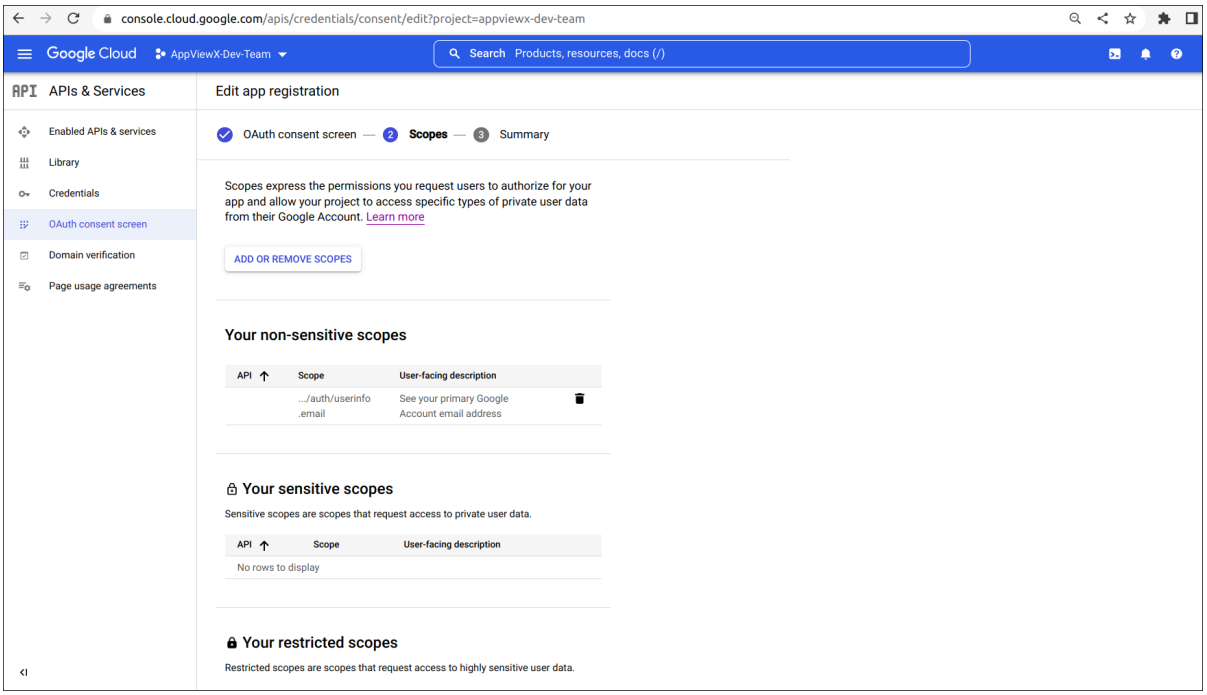
1. Sign in to Google using valid credentials for **App Registration** using the following URL: https://console.cloud.google.com/.



2. From the project drop-down, select an existing project, or create a new one by clicking on **NEW PROJECT**.
3. In the sidebar hover the mouse pointer over the "APIs & Services", click **OAuth consent screen**. The **OAuth consent screen:: App information** page is displayed.

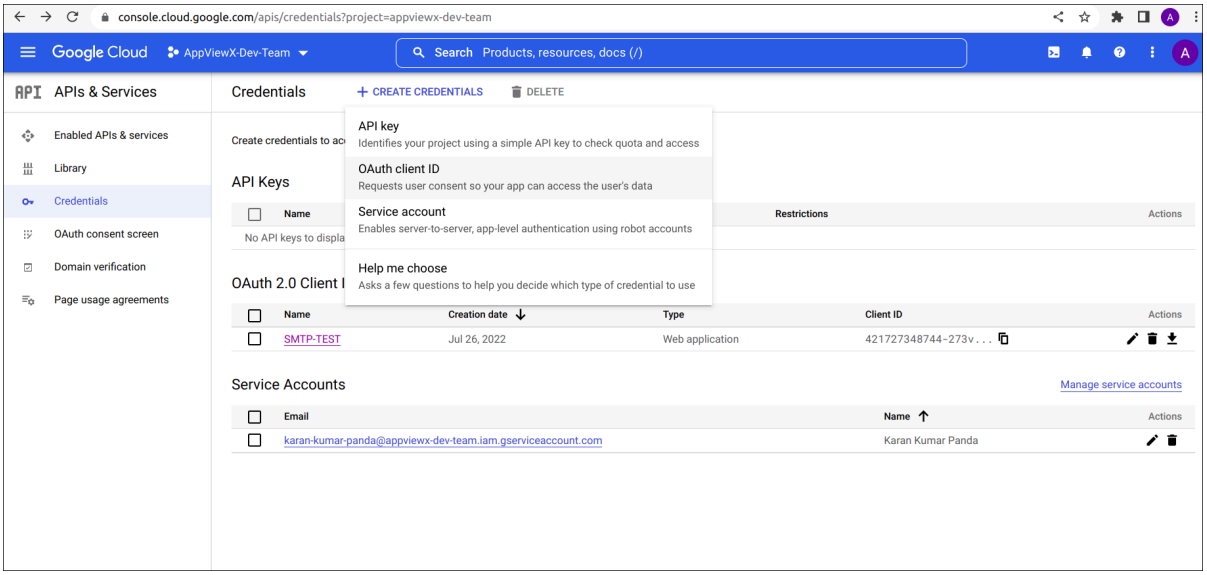


4. In the **App information** section, enter the required field information. **App name***, **User support email***, **Authorized domains**, **and Developer contact information**, then click **Save & Continue**. The **Save & Continue :: Scopes** page is displayed.



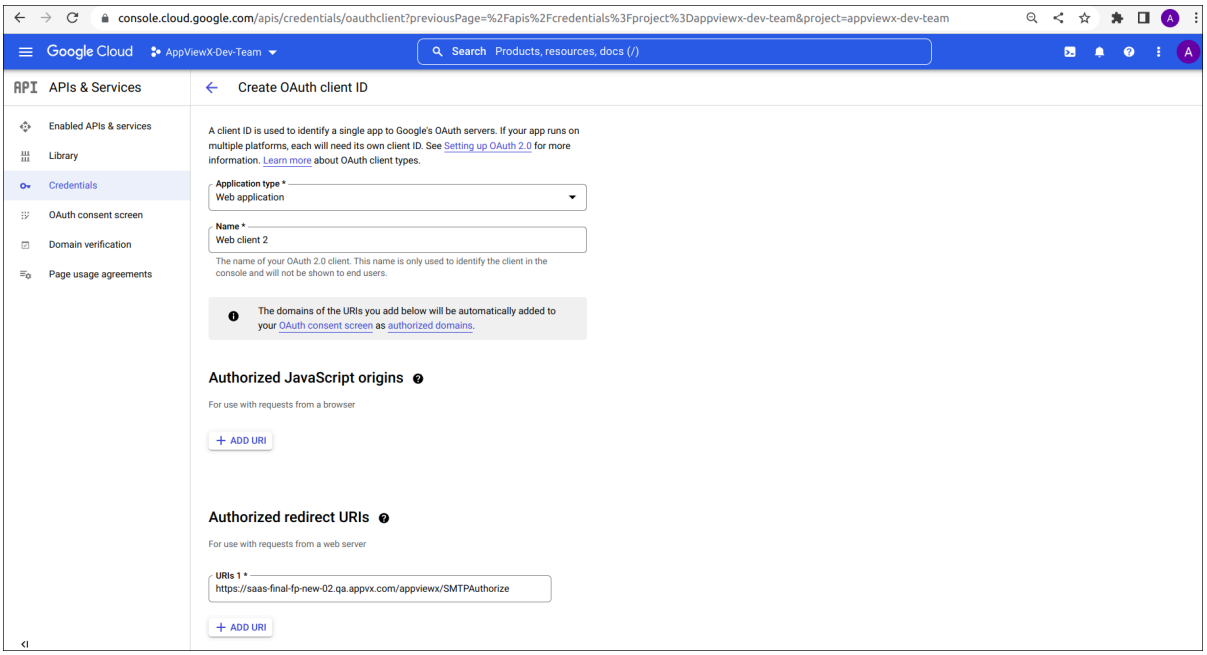
5. Under **Scopes** section, **ADD SCOPES** required information.
6. In the sidebar hover the mouse pointer over the "APIs & Services", click **Credentials**.

   The **APIs & Services :: Credentials** page is displayed.

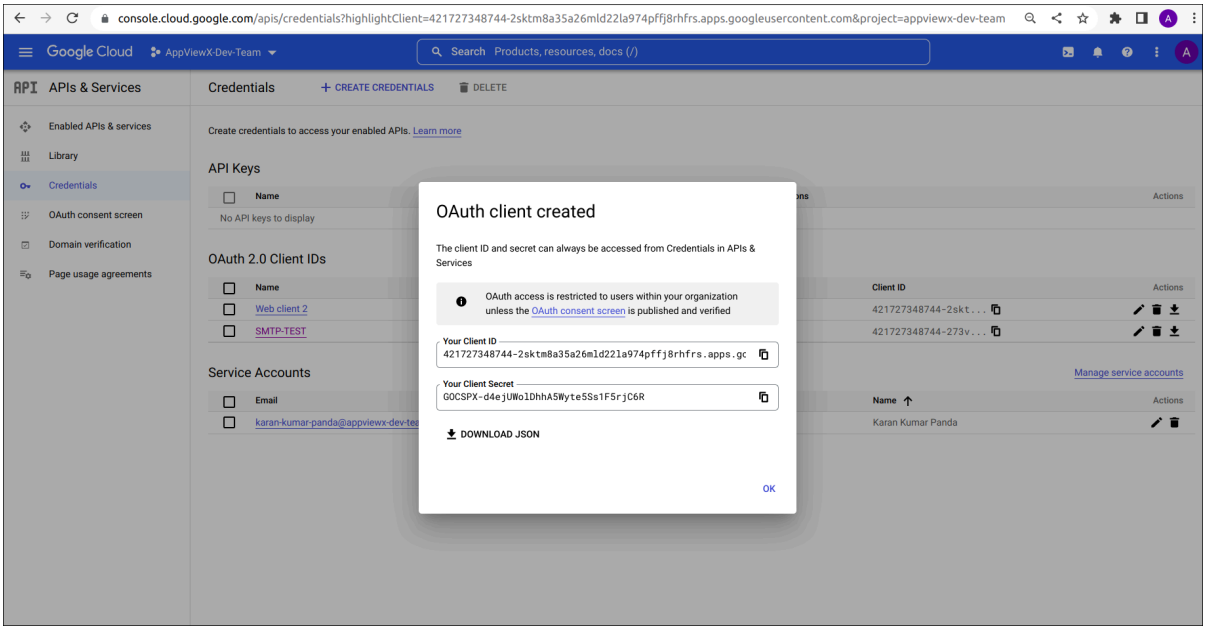


7. In the **Credentials** tab, click the **+CREATE CREDENTIALS**, from the drop-down list, choose **OAuth client ID**.

   The **CREATE CREDENTIALS :: Create OAuth client ID** page is displayed.



8. Enter the required field information, for **Application type*** select **Web application** and specify **Name*** then click **Save**.
9. Displays confirmation of **OAuth client Created**, with Your Client ID and Your Client Secret.



10. Copy the **Client ID** and **Client Secret** for authentication of SMTP server settings.
    - Authorization endpoint URL: https://accounts.google.com/o/oauth2/v2/auth.
    - Token endpoint URL: https://oauth2.googleapis.com/token.

Configuring the SMTP Settings for Microsoft

Prerequisites

- Ensure connectivity of the SMTP Server from the selected Data Center.
- Verify unrestricted connectivity between the Data Center and SMTP Server by checking for any firewall restrictions.
- For Microsoft SMTP OAuth.
  - Ensure the SMTP OAuth is enabled. For more details, refer to "Enable or Disable SMTP AUTH in Exchange Online" to enable it.
  - Ensure that a valid license is available for the mailbox.
- Validate the accuracy of the configuration details provided on the settings page.
- Prior to saving the configuration, verify the functionality of the Test Mail feature.

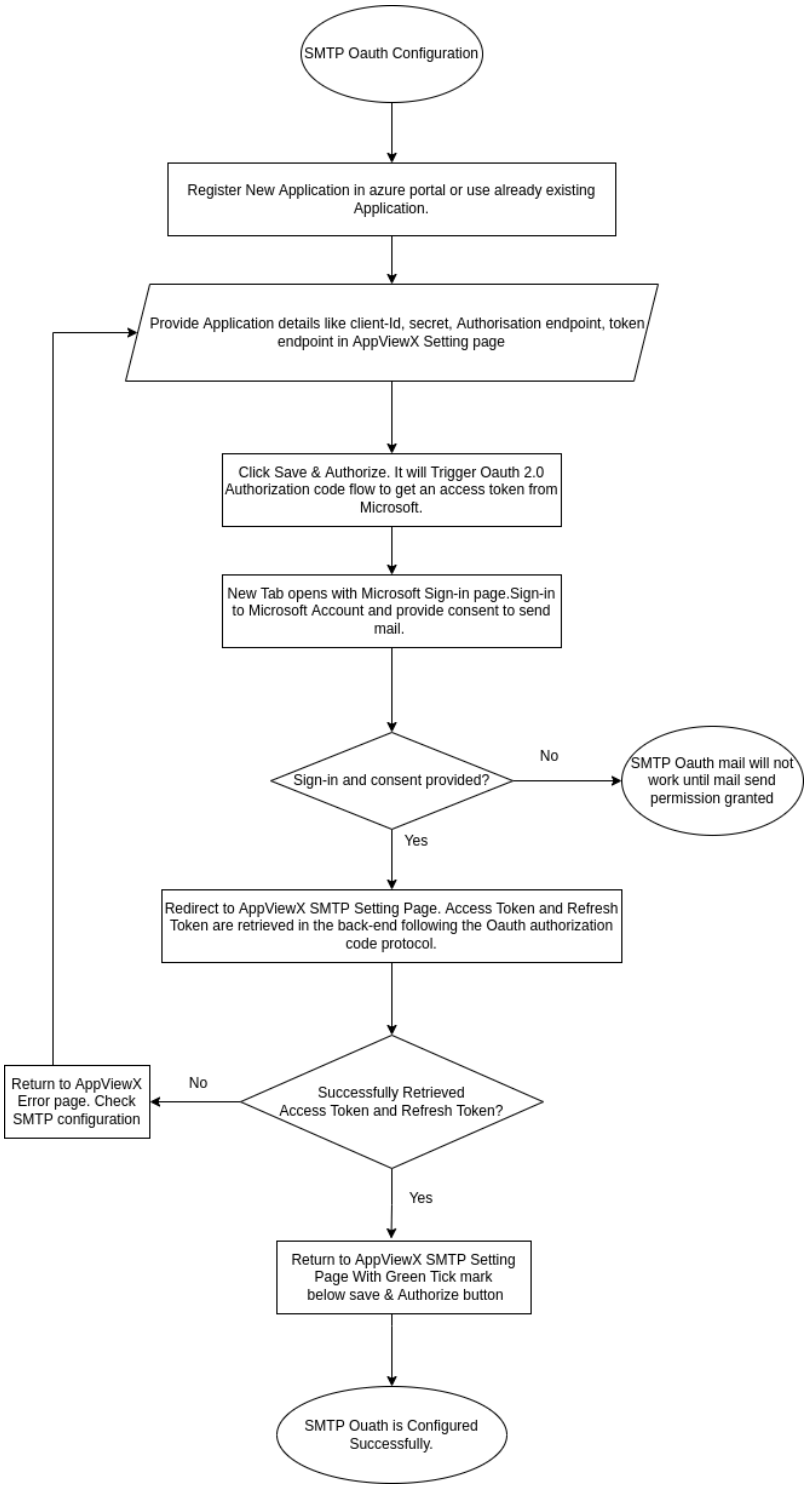
The SMTP configuration is required for AppViewX to be able to send logs and alerts via email and for other email related activities such as sending and receiving notifications and so on.

The SMTP oAuth uses an access token instead of a password to send email. The access token works as a temporary password with fixed validity and has permissions delegated by the user.

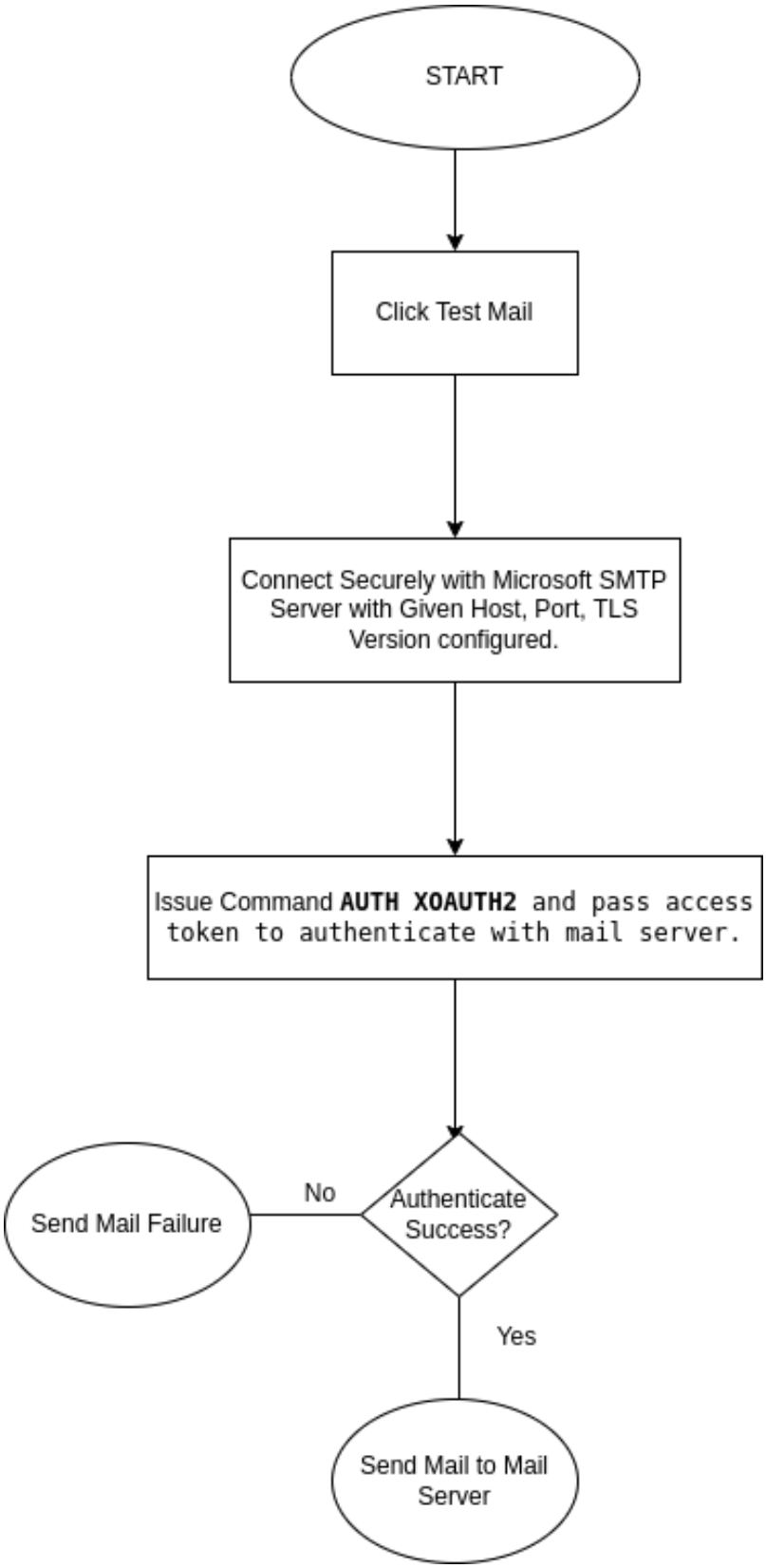
To get the access token you must provide details such as username, client-id, secret, Authorization endpoint, token Endpoint and scope. Once these details are submitted, you will be redirected to the oAuth server login page. Once the user authorization is done here, the oAuth server returns the Auth code.

The Auth code is exchanged with the access token and refresh token in the backend and saved in DB.

Flow Chart for SMTP Oauth Configuration.

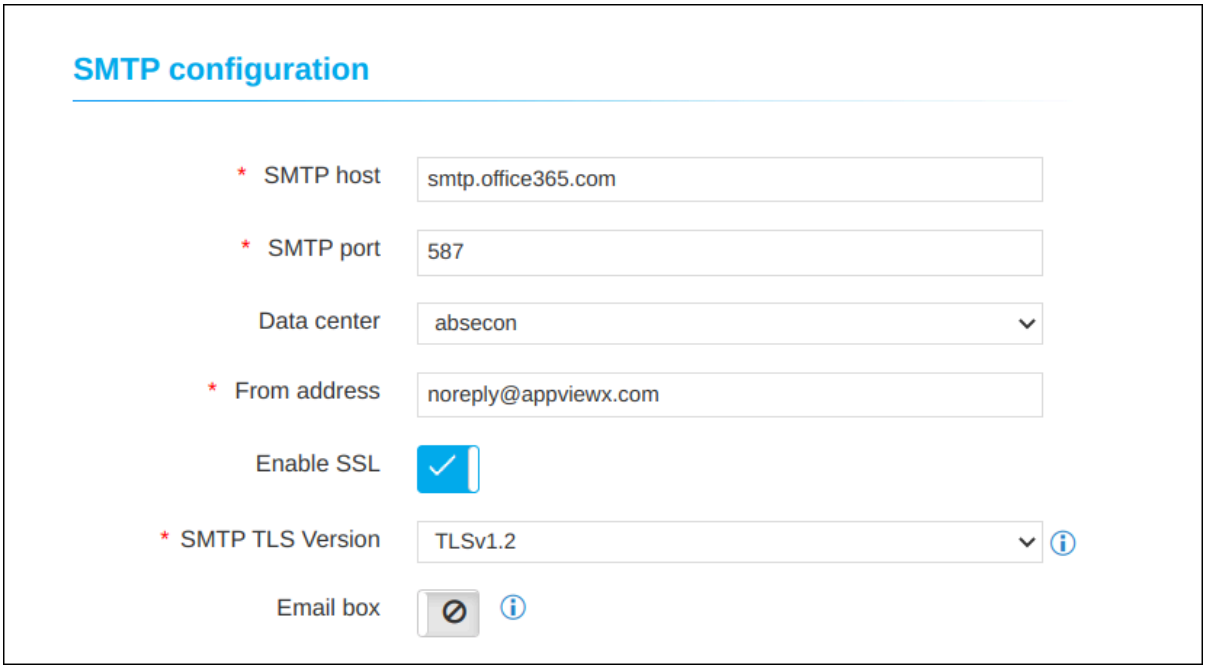


Flow Chart for Test Mail.



To configure the SMTP server:

1. On the **Settings :: SMTP** page, in the **SMTP configuration** section, enter the required field information.

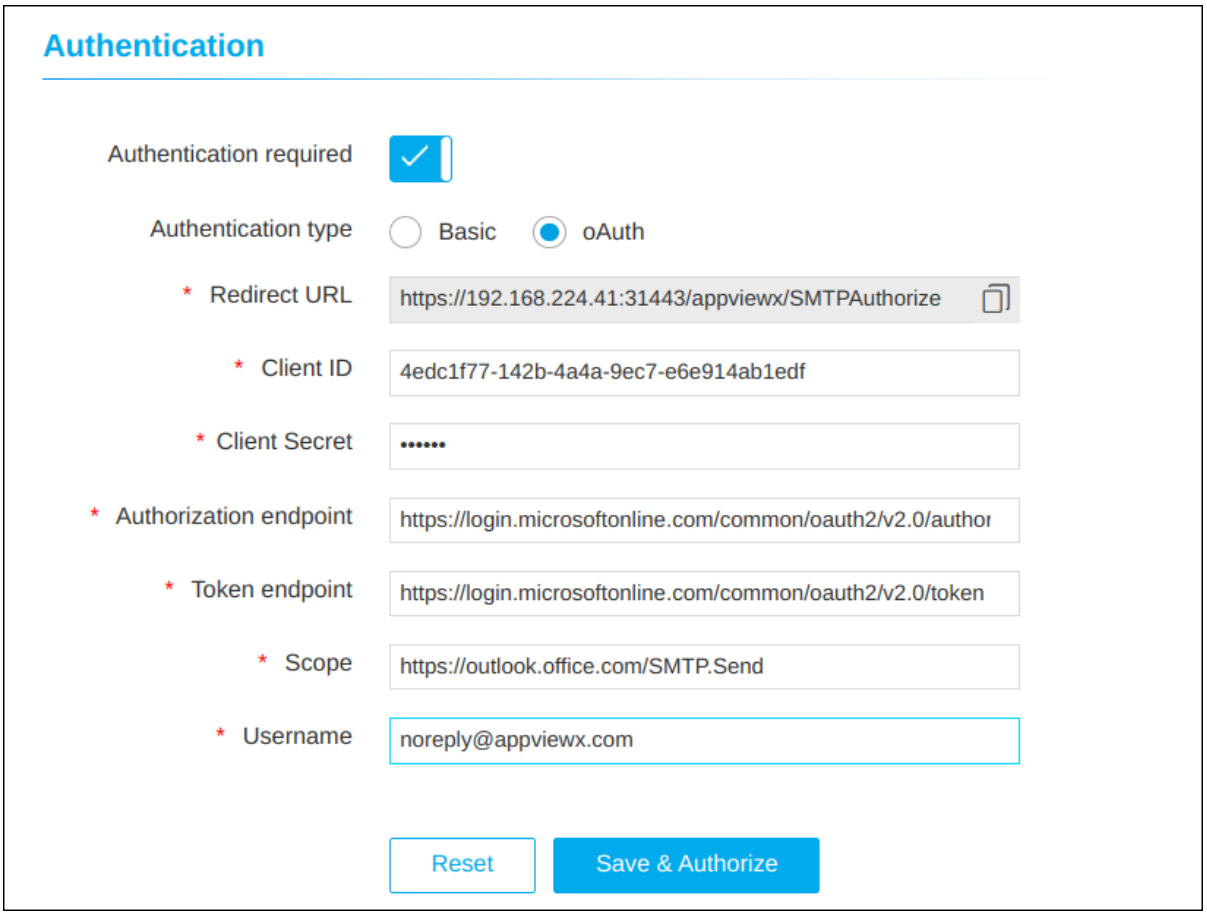


Field descriptions for SMTP configuration

Field	Description
***SMTP host**	Host name of the SMTP server.
***SMTP port**	Port number of the SMTP server.
Data center	From the options available in the dropdown, select the data center.
***From address**	Enter the email address that will be used to email the logs and alerts.
Enable SSL	To allow SSL encryption, enable this toggle key.
***SMTP TLS Version**	From the options available in the dropdown, select the TLS version of the SMTP server. **Note:** Versions 1.2 and higher are recommended.
Email box	To use the mailbox feature to read emails in Visual Workflow, enable this toggle key.

Field	Description
***Email**	Email address of the IMAP server used for the mailbox feature. **Note:** This field is displayed only if the **Email box** key is enabled.
***Password**	Password of the IMAP server used for the mailbox feature. **Note:** This field is displayed only if the **Email box** key is enabled.
***Host name**	Host name of the IMAP server used for the mailbox feature. **Note:** This field is displayed only if the **Email box** key is enabled.
***Port**	Enter the Port number. **Note:** This field is displayed only if the **Email box** key is enabled.
Note: The asterisk (*) symbol indicates mandatory fields.	

2. In the **Authentication** section, enter the required field information.



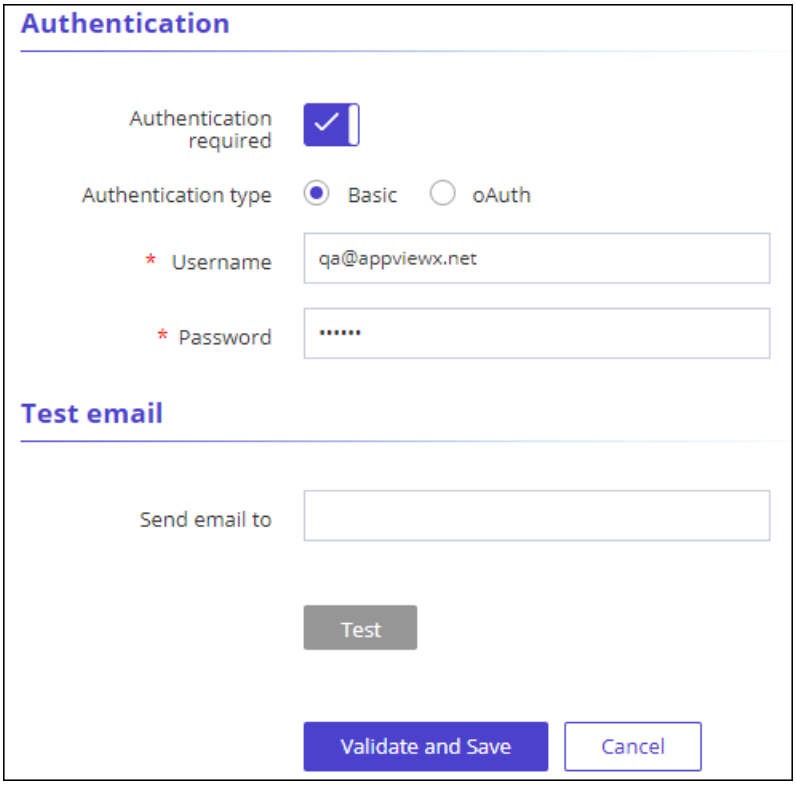
Field descriptions for Authentication

Field	Description
Authentication required	To enable authenticated mail server communication, enable this toggle.
Authentication type	Select the Authentication type as Basic. **Note:** Selecting Basic displays the Username and Password fields. Select the Authentication type as oAuth. **Note:** Selecting oAuth displays the fields that are described below. SMTP oAuth method to send email, we can't use a different address in From field. The sending address must be the same with the authenticated account.

Field	Description
***Redirect URL**	This field is auto-populated from the address bar of the browser.
***Client ID**	Enter the Client ID that is generated in the oAuth server when the oAuth client is created. **Note:** The steps to create an oAuth client are different for Google and Microsoft. For more information on steps for Google, click here. For more information on steps for Microsoft click here.
***Client Secret**	Enter the Client Secret that is generated in the oAuth server when the oAuth client is created.
***Authorization endpoint**	Enter the authorization endpoint where the user authorizes and gives permission to the oAuth client to send email on behalf of the user.
***Token endpoint**	Enter the token endpoint to get Access Token and Refresh Token. You can get the endpoint by providing Client ID, Secret, and other relevant values based on oAuth 2.0 specifications.
***Scope**	The permission required to send email. **Note:** For Microsoft, enter https://outlook.office.com/SMTP.Send.
***Username**	**Note:** This field is enabled only if the **Authentication required** key is enabled. Username for the authenticated mail server If the Authentication is chosen as oAuth the **Username** and **From address** should be the same.

Field	Description
***Password**	**Note:** This field is enabled if you select **Basic** as your **Authentication type**. Enter the valid password associated with the username.
Note: The asterisk (*) symbol indicates mandatory fields.	

3. If the **Authentication type** is selected as **Basic**, displays the Username and Password attributes.
4. In the **Test email** section, enter the email address to which a test email should be sent and click **Test**.

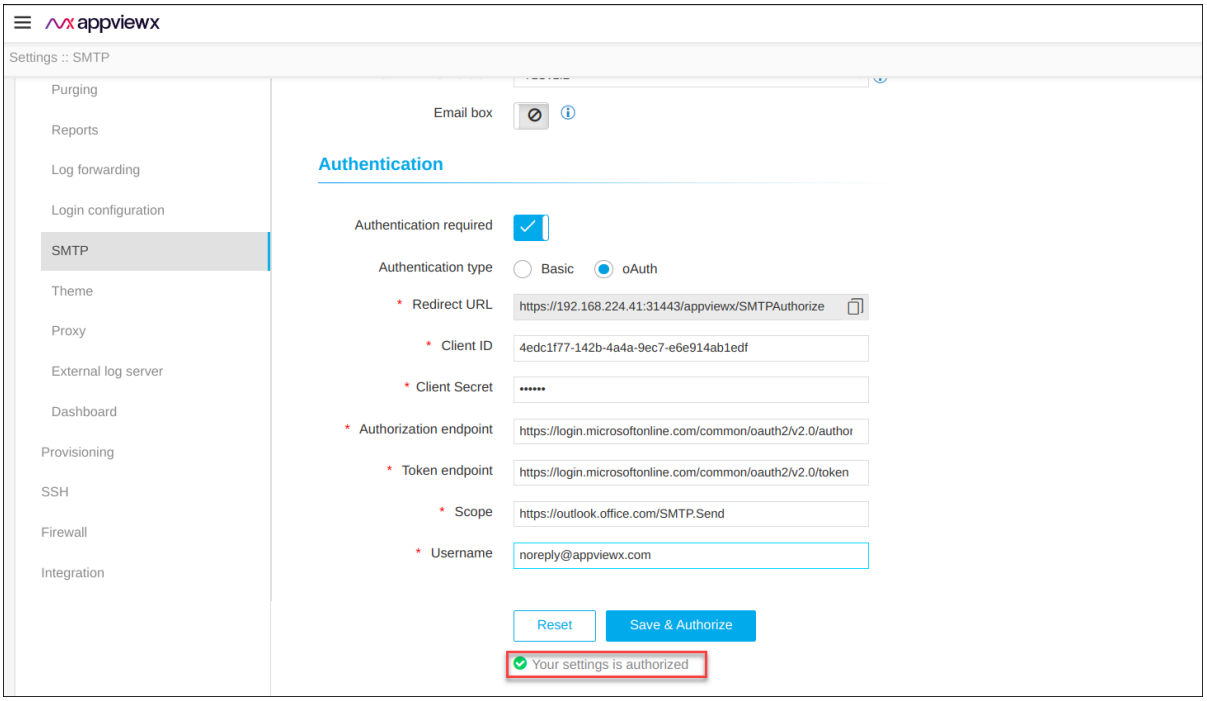


5. To save the SMTP configuration settings, click **Validate and Save**.
   Upon clicking "Validate and Save," an email will be sent to the user's email address for validation.

Note: If the user does not have an email ID configured, an error will be displayed, prompting them to set up an email address.

Note: In case of validation failure, the SMTP settings will not be saved.

6. If the **Authentication type** is selected as **oAuth**, To save the SMTP configuration settings, click **Save & Authorize**.
   New Tab is displayed for Single Sign On (SSO) with microsoft.
7. Provide your login credentials and submit your consent for the mentioned permissions. The login credential should be the same as the username configured in the SMTP Authentication.
8. Displays confirmation of SMTP Settings Authorized.



9. AppViewX can send an email on behalf of the authorized user as the user has given the consent to send email on his behalf during authentication.

Note: The **Username** should have a mailbox assigned, and it should also have all the necessary permissions for web sign-in as per the oAuth 2.0 authorization code flow.

A new tab will open, prompting for sign-in.

Once authorization is done the user receives an access token and a refresh token from the token endpoint. The access token is used for sending email and the refresh token is used for renewing the access token upon its expiry.

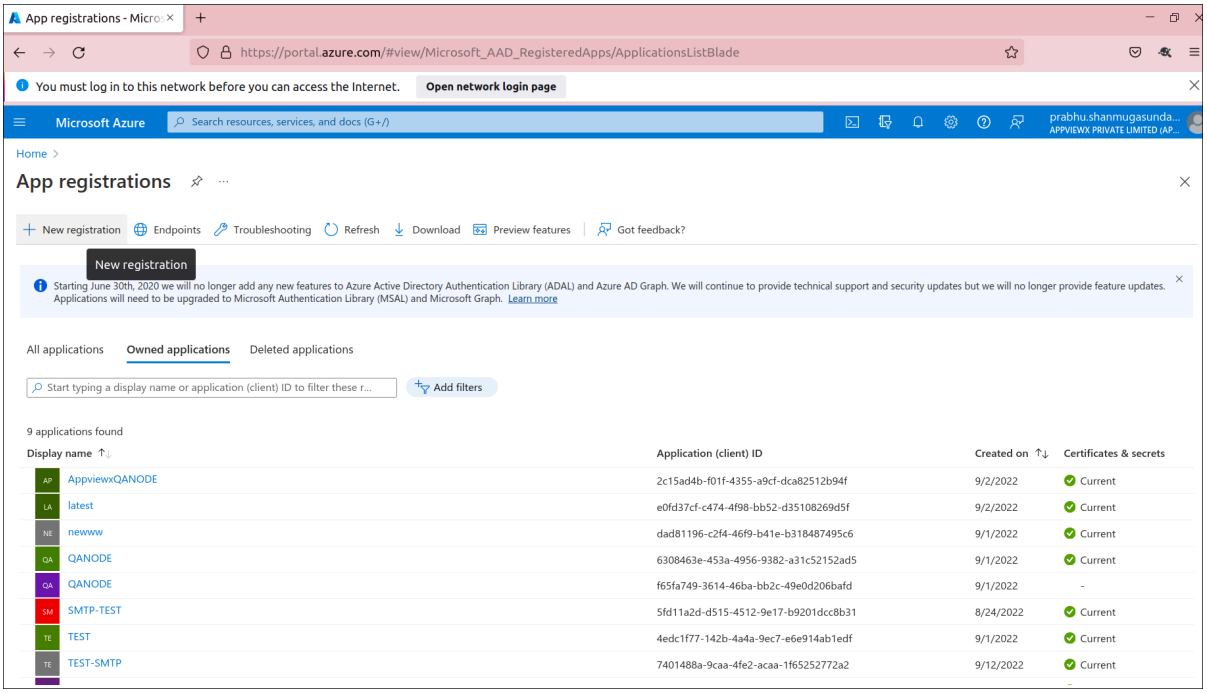
Authentication for Microsoft SMTP Settings

Create authorization credentials.

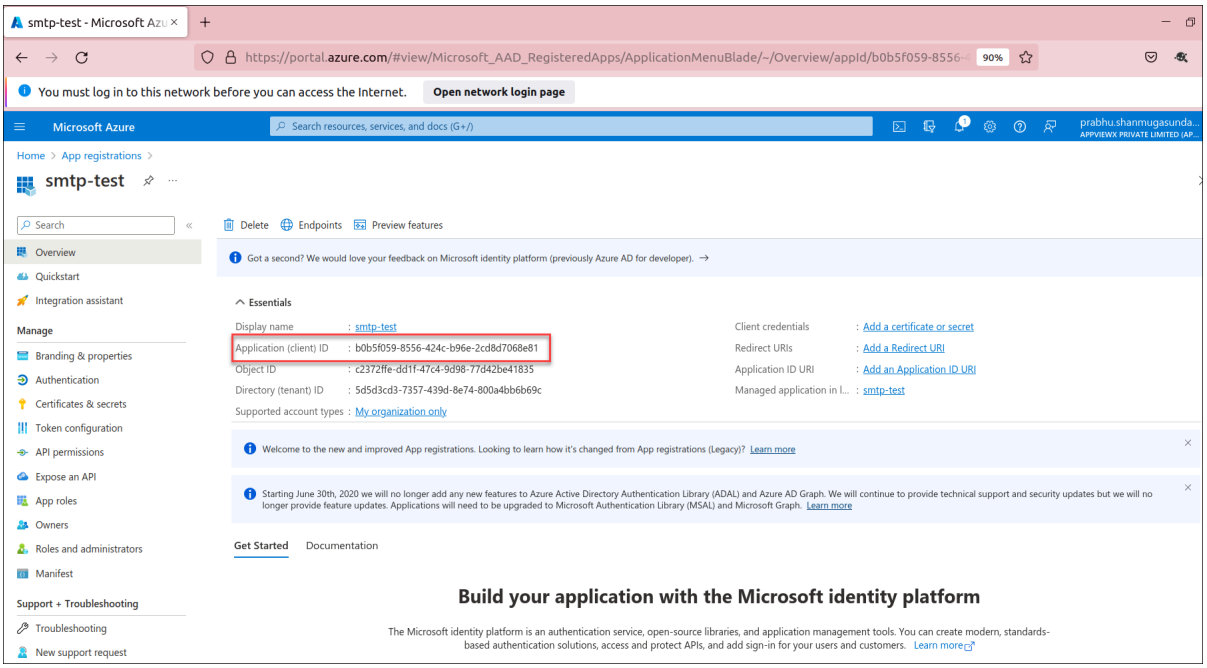
Registering your application establishes a trust relationship between your app and the Microsoft identity platform. The trust is unidirectional: your app trusts the Microsoft identity platform, and not the other way around.

Follow these steps to create the app registration:

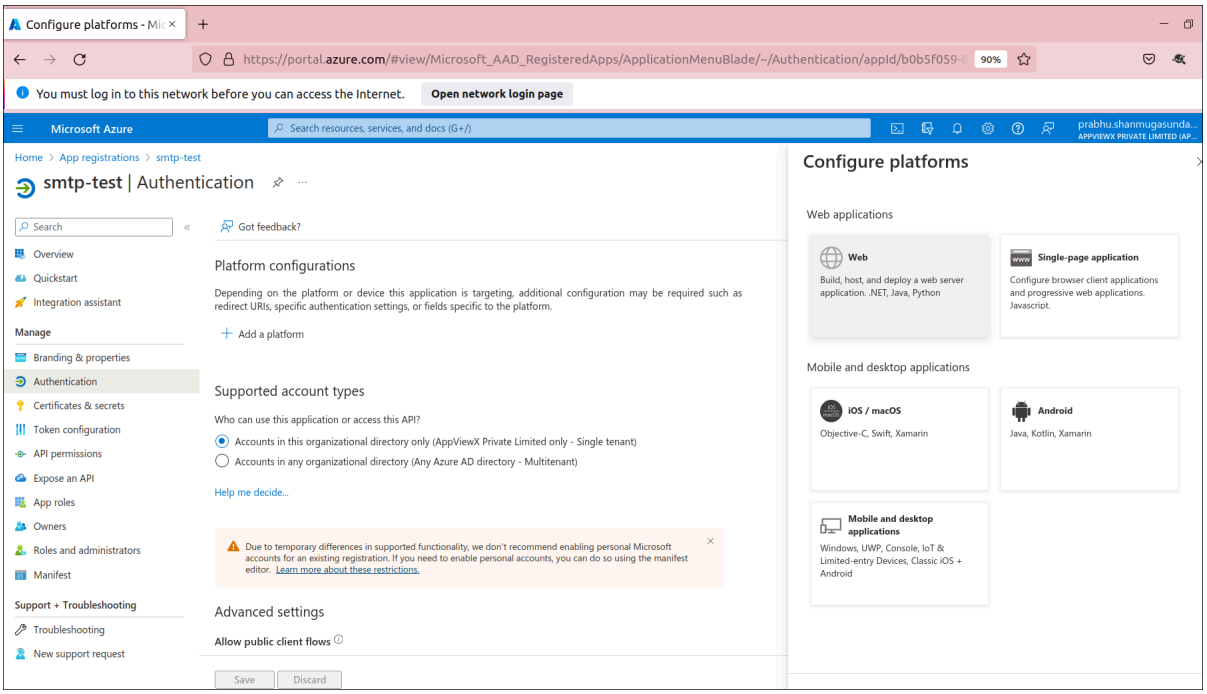
1. Sign in to Microsoft using valid credentials for App Registration using the following URL: https://portal.azure.com/.
2. Under **Manage**, click **App registrations** > **New registration**.



3. In the **Register an Application** section, enter the required field information.
4. Click **Register** to complete the initial app registration.
5. When registration finishes, the Azure portal displays the app registration's Overview pane. You see the **Application (client) ID**.

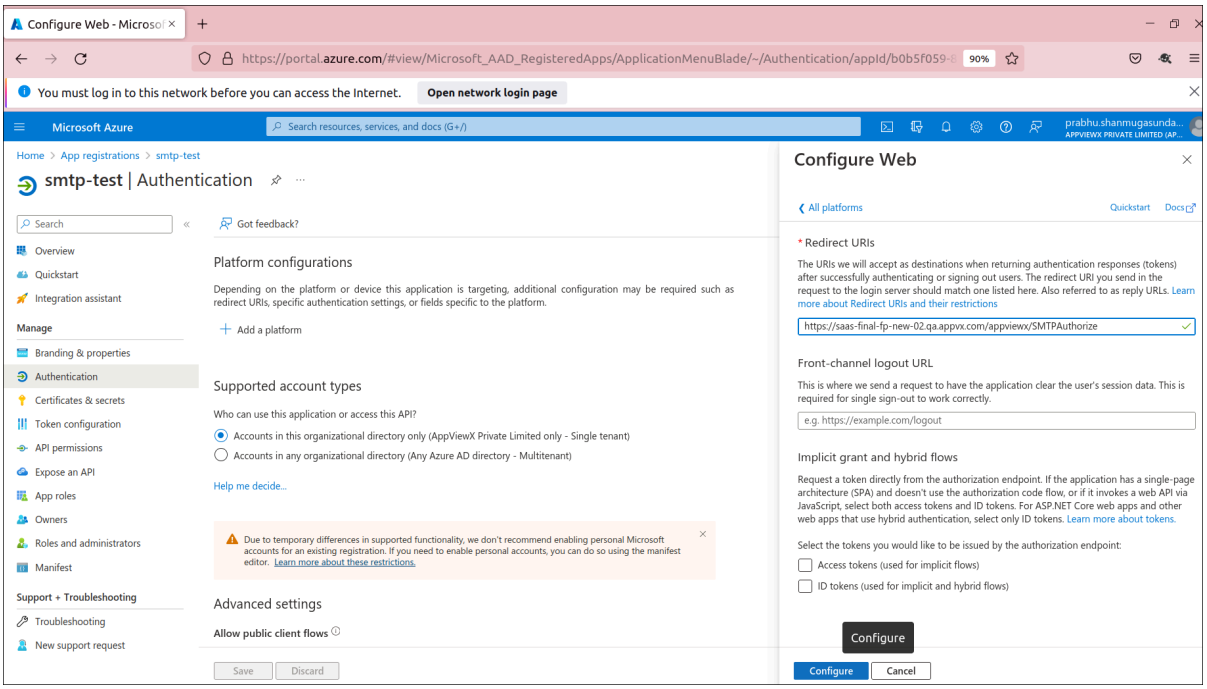


6. Under **Manage**, select **Authentication**.
7. Under **Platform configurations**, select **Add a platform**.

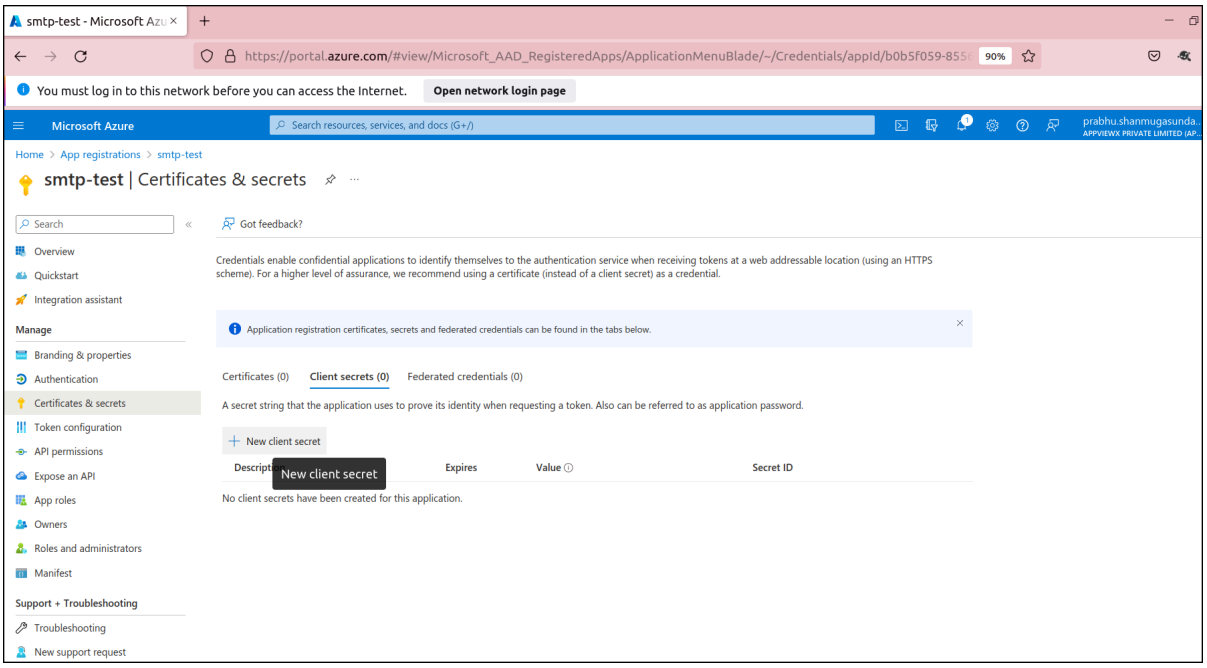


8. Under **Configure platforms**, select **Web** for application type (platform) to configure its settings.

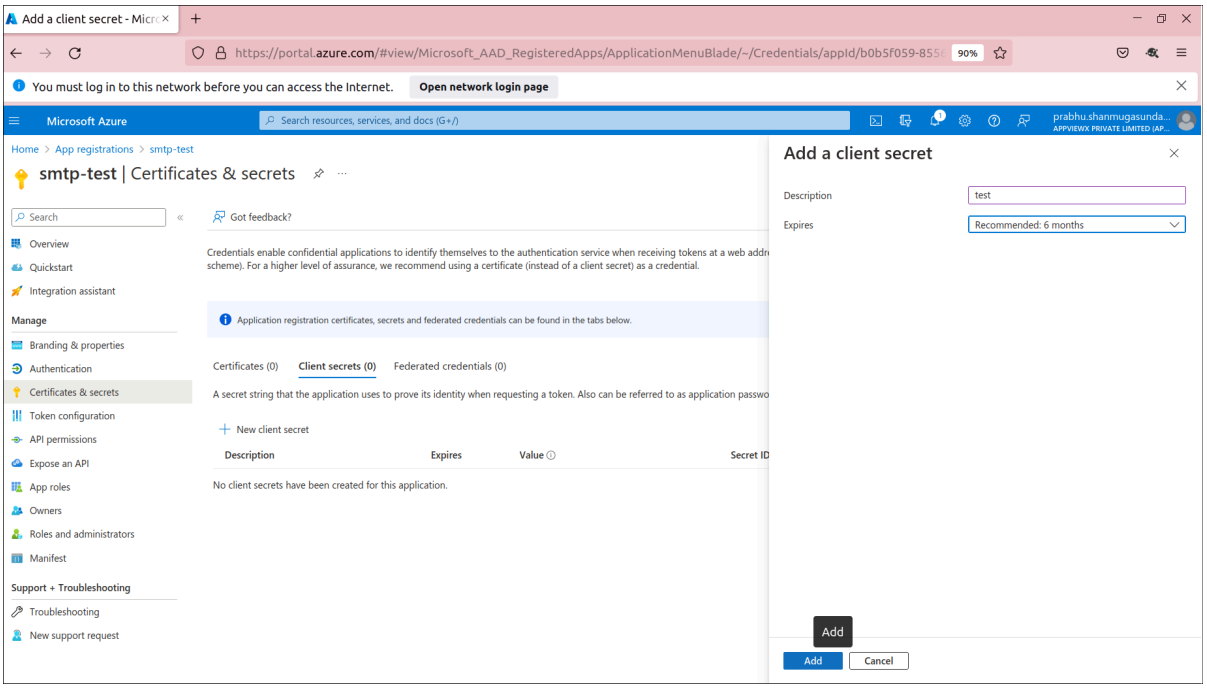
   The **Redirect URI :: Configure Web** page is displayed.



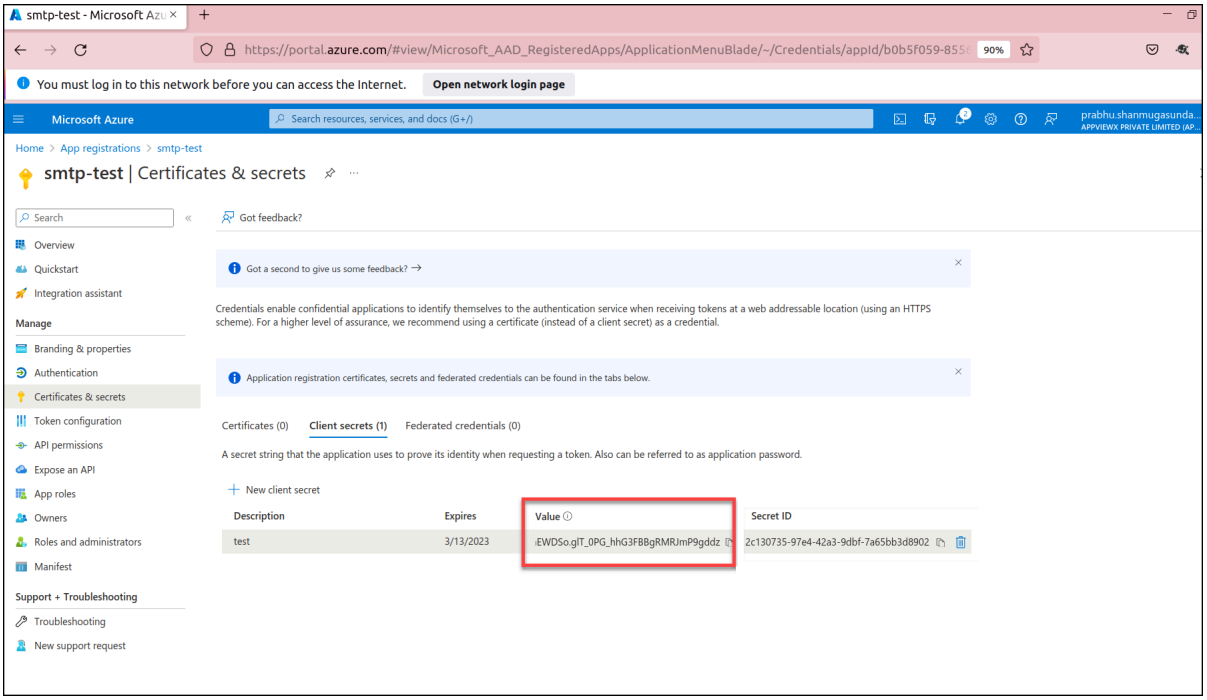
9. Enter a Redirect URI for your app. This URI is the location where the Microsoft identity platform redirects a user's client and sends security tokens after authentication.
10. Click **Configure** to complete the platform configuration.
11. Select **Certificates & secrets** > **Client secrets** > **New client secret**.



The **New client secret :: Add a client secret** page is displayed.

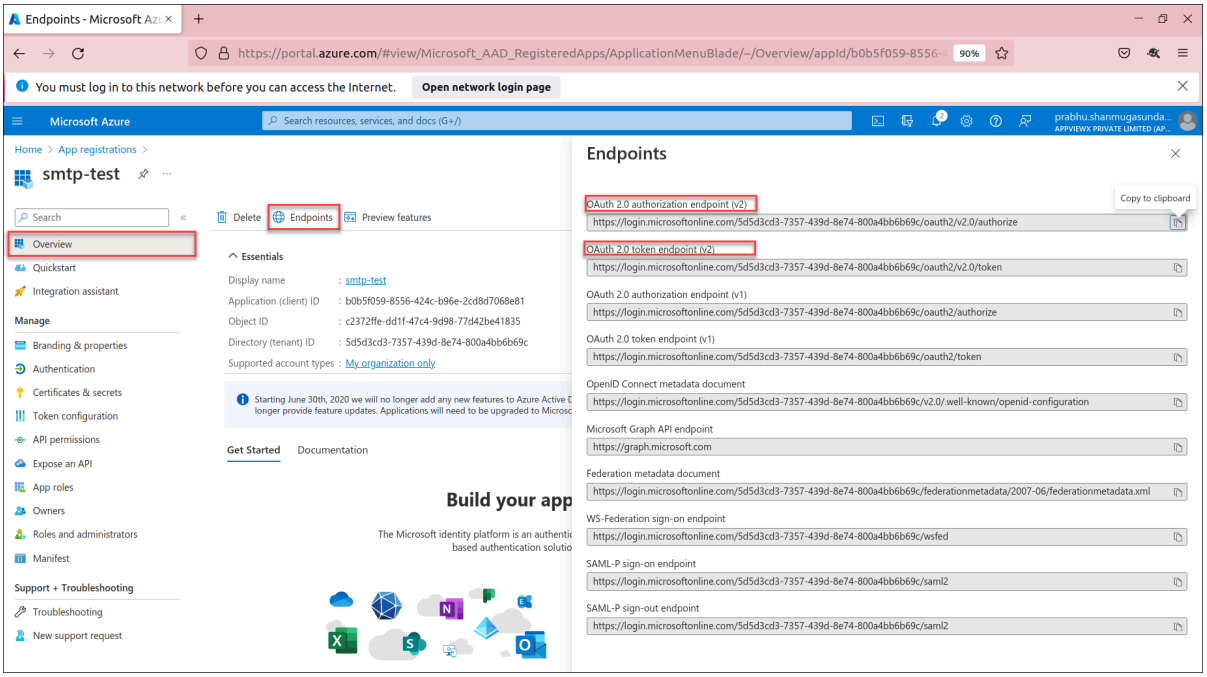


12. Add a **Description** for your client secret.
13. Select an **Expiration** for the secret or specify a custom lifetime.
14. Click **Add**.
15. Record the **Secret value** for use in your client application code. This secret value is never displayed again after you leave this page.



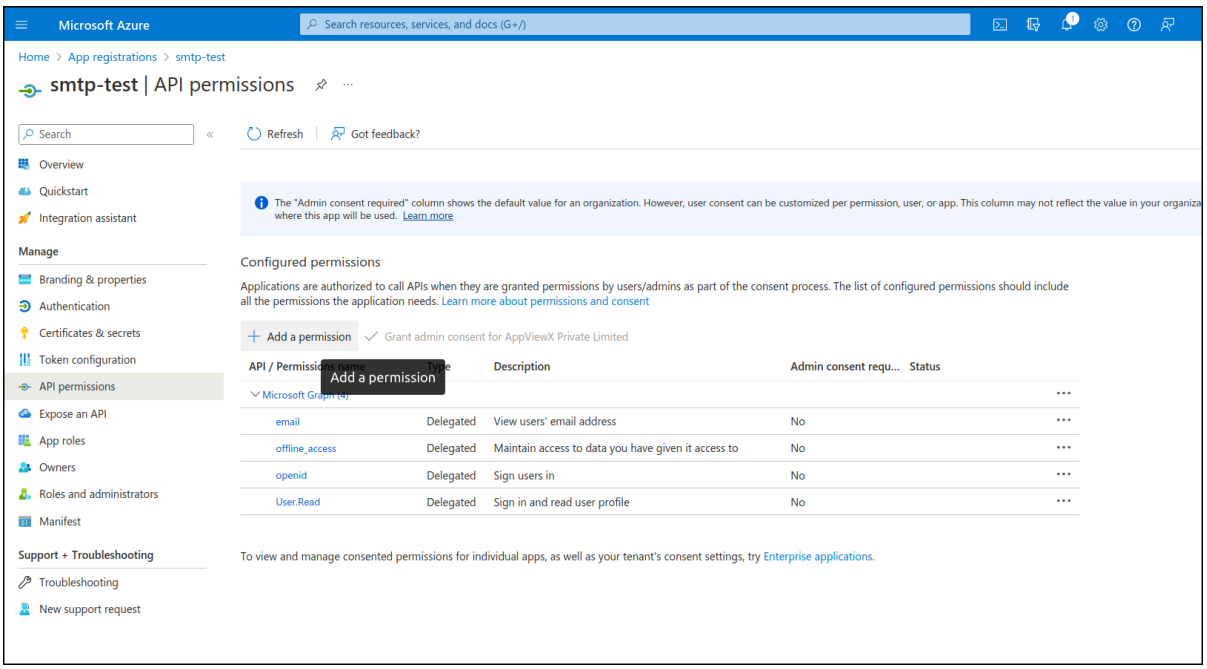
16. Under **App Registration**, click **Overview**.
17. Click **Endpoints**.

    The **Overview :: Endpoints** page is displayed.



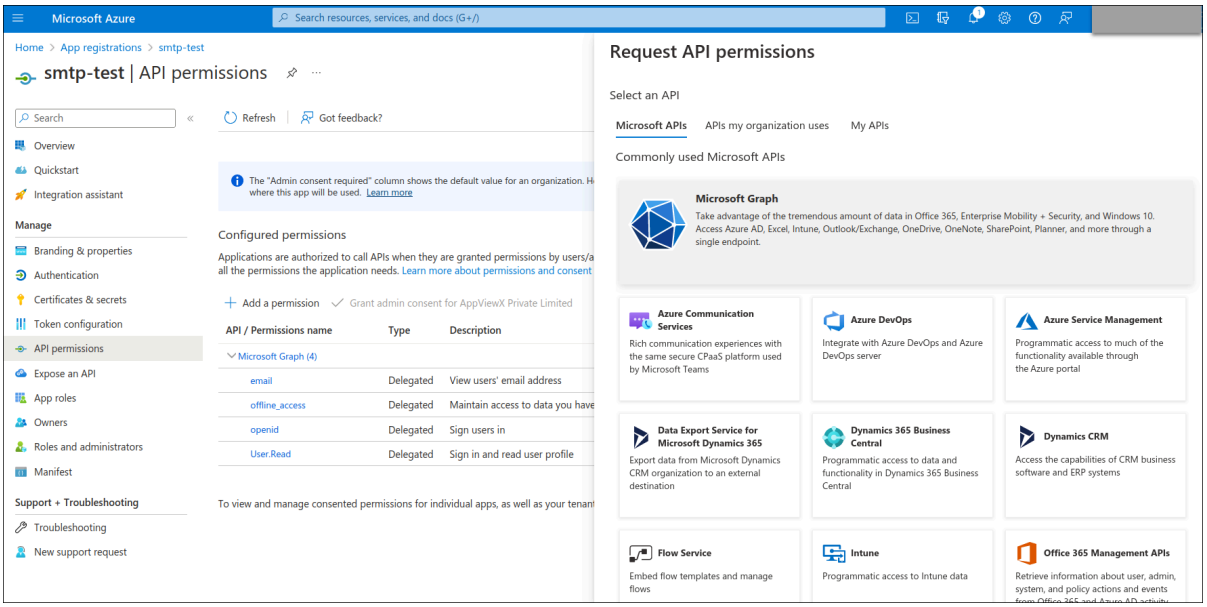
18. Copy **authorization endpoint** and **token endpoint** for Authentication of SMTP Server Settings.
19. Under **Manage**, click **API permissions**.

    The **API permissions** page is displayed.

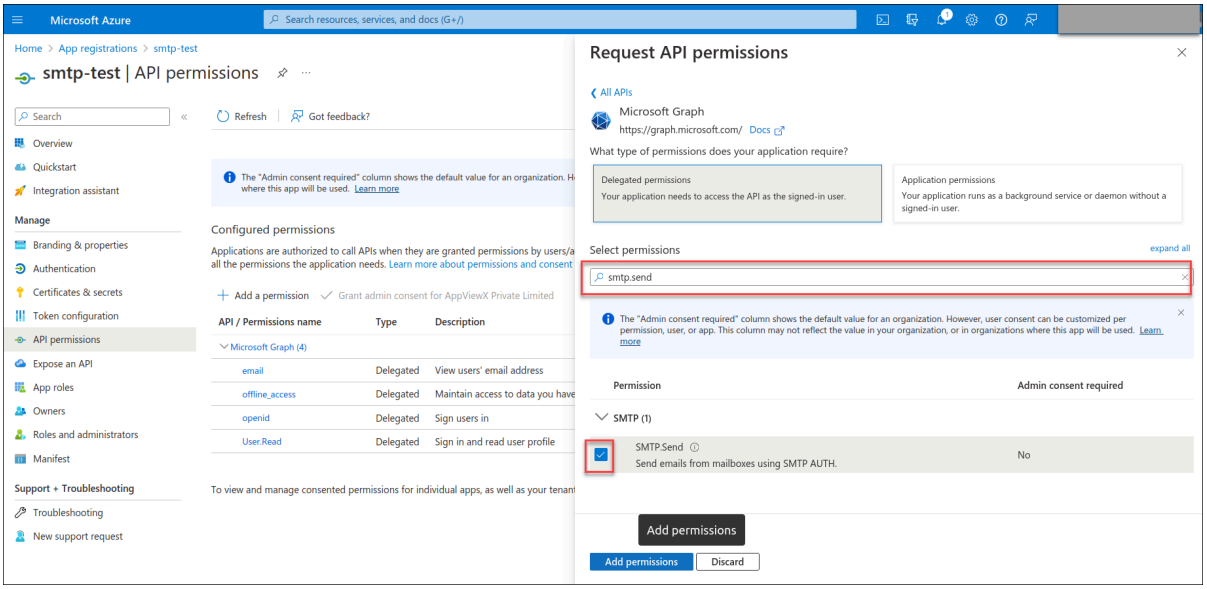


20. To add required permissions, click **Add a permission**.

    The **Request API permissions** page is displayed.

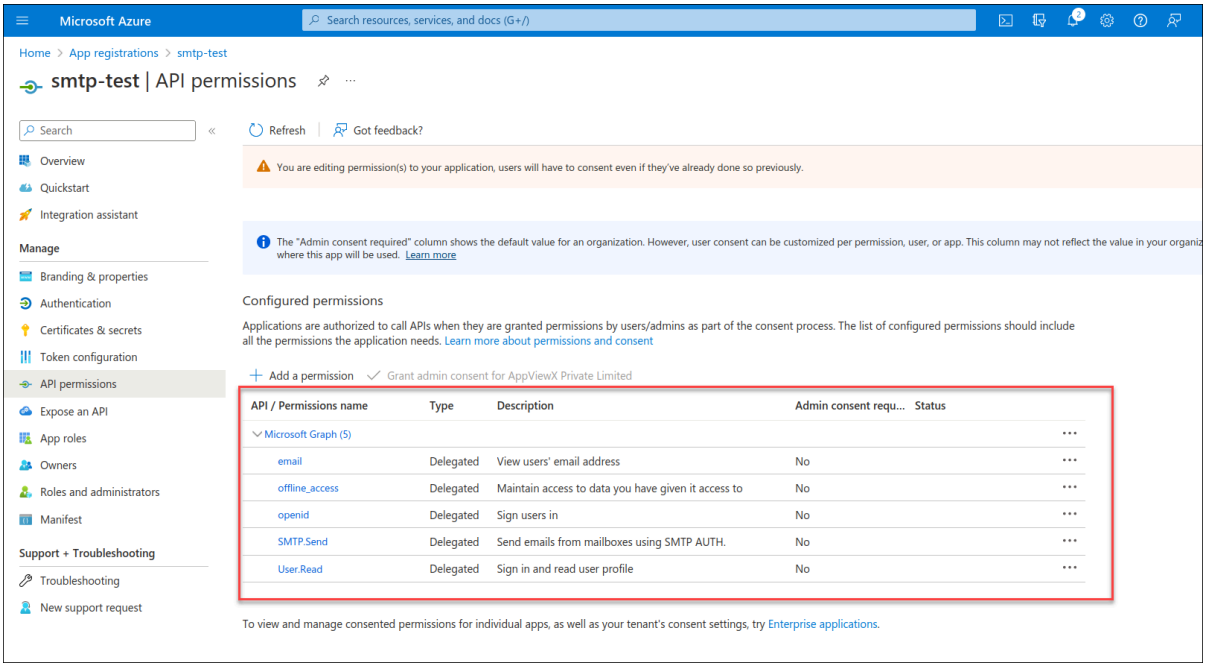


21. Click **Microsoft Graph > Delegated permissions**.



22. Under **Select permissions** search box, search for the **smtp.send** and select the **SMTP.Send** from the dropdown.
23. Similarly search for **email, offline_access, openid, User.Read** and select the **email, offline_access, openid, User.Read** from the respective dropdowns.
24. Click **Add permissions**.

The **API permissions** added will be Displayed below **API / Permissions name**.

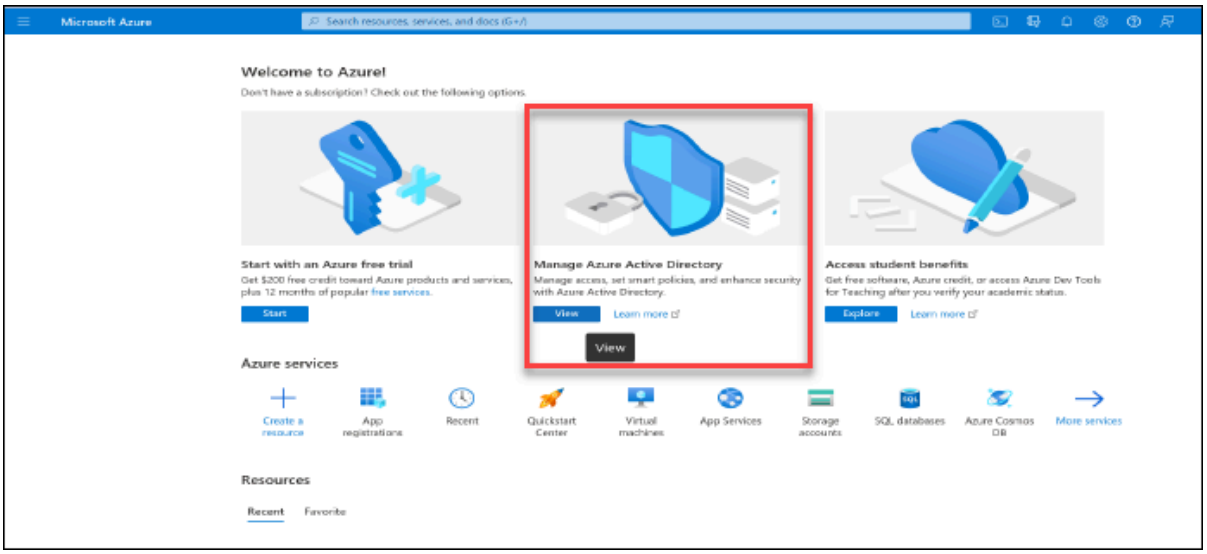


Frequently Asked Questions

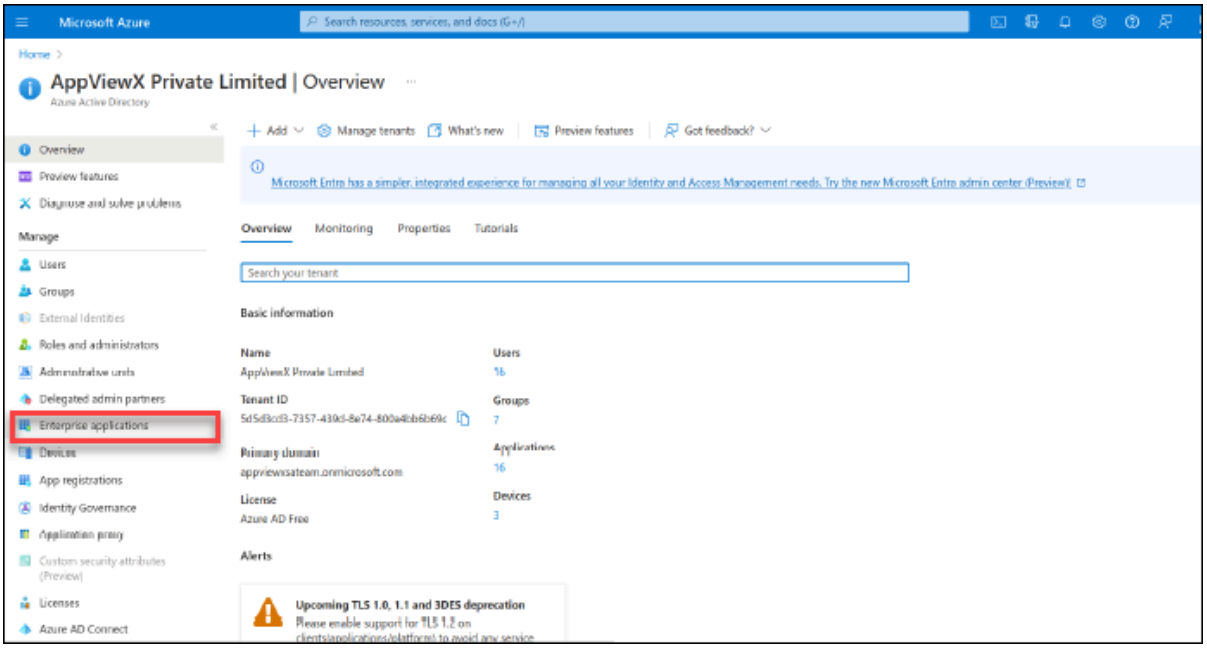
While adding **API permissions** Owner Consent Error is shown, to avoid this error following changes have to be done.

Follow these steps to overcome Owner Consent Error:

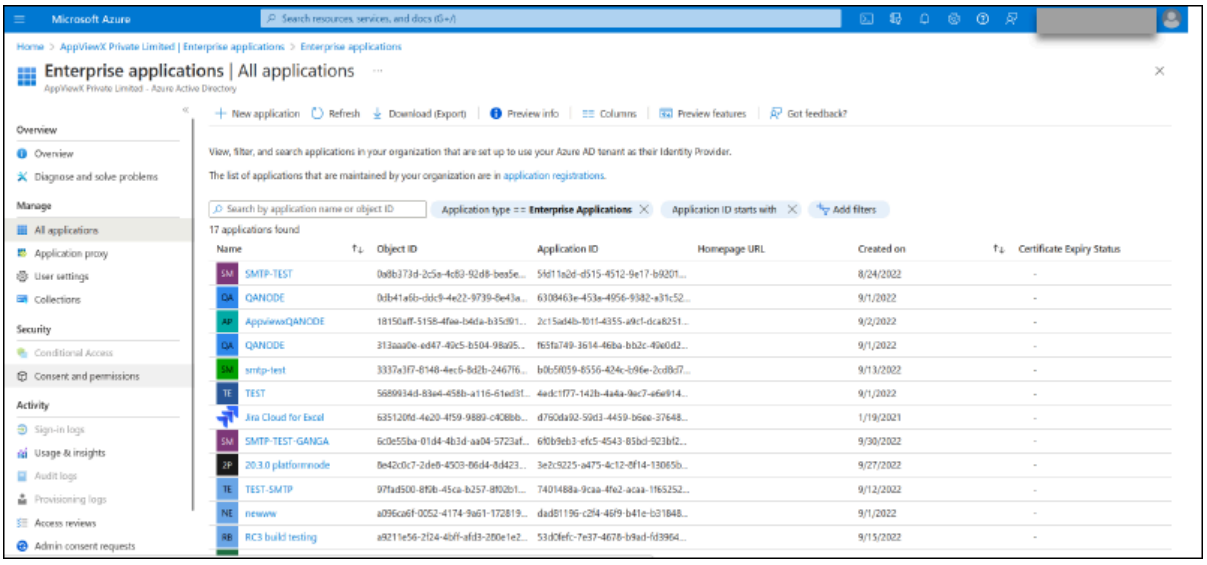
1. Sign in to Microsoft using valid credentials for App Registration using the following URL: https://portal.azure.com/.
2. Click **Manage Azure Active Directory**.



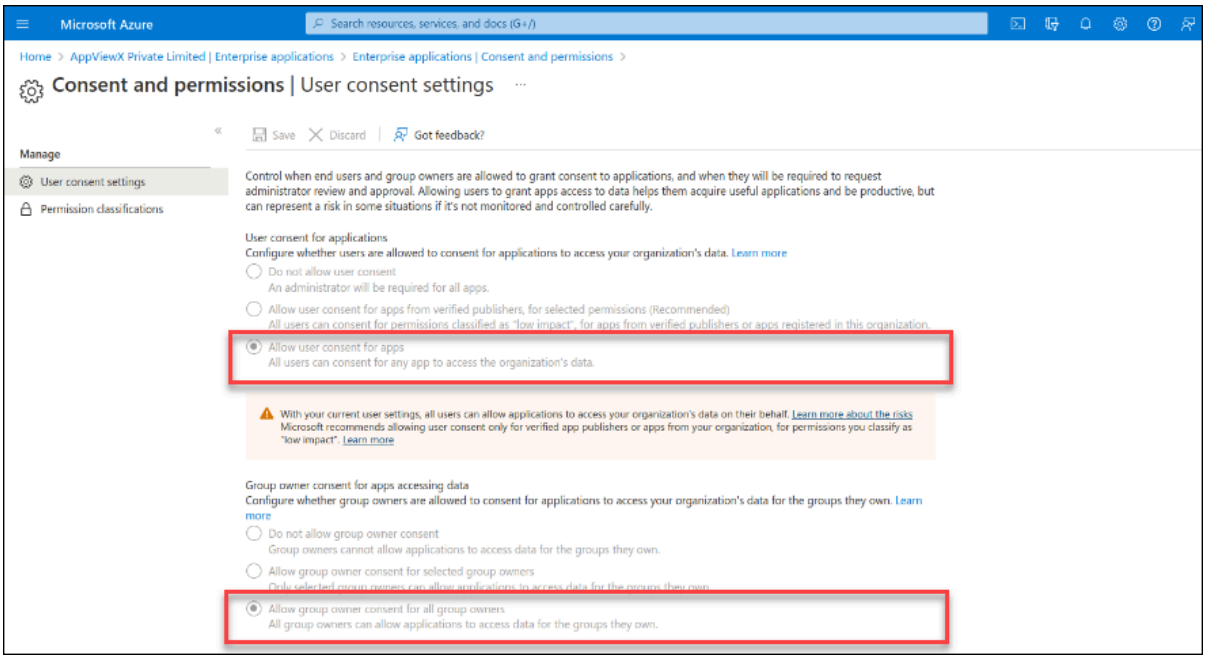
3. Click **Enterprise applications** in the left menu.



4. Click **Consent and permissions** in the left menu.



5. Change the **User Consent Settings** for user consent for applications from **Do not allow user consent** to **Allow user consent for apps**.
6. Change the **User Consent Settings** for group owner consent for apps accessing data from **Do not allow group owner consent** to **Allow group owner consent for all group owners**.



Managing Proxy Settings

When deployed at a customer's site, AppViewX communicates with the internet through a proxy server to shield the customer's IP address from exposure.

To configure the proxy settings:

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **SYSTEM ADMINISTRATION**, select **Proxy**. The **Settings :: Proxy** page is displayed.	1. From the main navigation menu, click **Settings**. 2. On the **Settings** page, from the left menu, select **General** > **Proxy**. The **Settings :: Proxy** page is displayed.
Note: For more information on how to switch between menus, click here.	

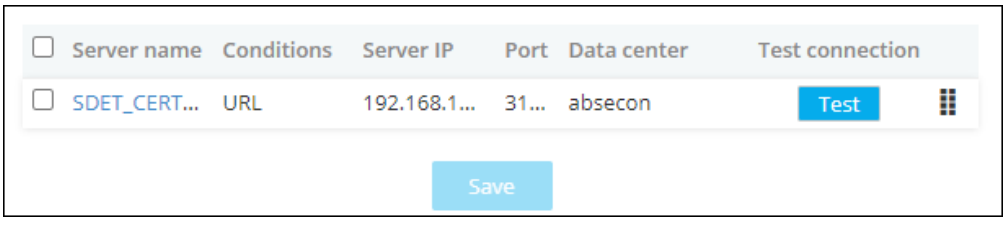
1. On the **Settings :: Proxy** page, enter the following details:

Field descriptions for Proxy Settings

Field	Description
***Proxy Settings**	Select the Proxy settings from the following options: • Cloud Connector When choosing Cloud Connector as your proxy setting, the settings will be shown on the Cloud Connector addition page. To distinguish between the Cloud Connector and AppViewX, not all proxy settings are applicable for the Cloud Connector connectivity. • AppViewX If you choose AppViewX as your proxy setting, the settings will not be visible within the CC addition page.
***Server name**	Name of the proxy server.
***Server IP**	IP address of the proxy server.
***Port**	Port number of proxy server.
Advanced	To enable advanced settings, select this check box.
Data center	From the drop-down menu, select a data center.

Field	Description
	Note: This field is displayed only when the **Advanced** check box is selected.
URL	From the drop-down menu, select the URL. **Note:** This field is displayed only when the **Advanced** check box is selected.
Authentication	To enable authentication, select this check box.
***Username**	Enter the username. **Note:** This field is displayed only when the **Authentication** check box is selected.
***Password**	Enter the password. **Note:** This field is displayed only when the **Authentication** check box is selected.
Note: The asterisk (*) symbol indicates mandatory fields.	

2. To save the proxy settings configured above, click **Add**.
   The settings are saved and displayed in the table.



3. To reconfigure the proxy settings, click **Reset**.

Setting the Cryptographic Policy

AppViewX enforces a SFTP-based cryptographic policy for protection of sensitive data. Ciphers are used for performing any file operations within AppViewX's functionality and to communicate with devices added in AppViewX.

To set the cryptographic policy:

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **SYSTEM ADMINISTRATION**, select **Crypto Policy**. The **Settings :: Advanced Settings** page is displayed.	1. From the main navigation menu, click **Settings**. 2. On the **Settings** page, from the left menu, select **General** > **Advanced**. The **Settings :: Advanced Settings** page is displayed.
Note: For more information on how to switch between menus, click here.	

1. On the **Settings :: Advanced Settings** page, in the **SFTP Cryptographic Policy** section, enter the following details:

   Field descriptions for SFTP Cryptographic Policy

Field	Description
Key Exchange Algorithms	Algorithms used to exchange keys for a successful handshake between the client and the server.
Cipher parameters	Parameters to encrypt the connection between the client and the server.
HMAC parameters	Parameters to ensure that the received message is intact and not tampered during its delivery from the client to the server and vice versa.
Connection retry limit	Number of attempts to retry establishing a connection between the client and the server.

2. Click **Save**.

Enabling Dashboard View for the User

To prevent loss of control over organizational data in the event that a resource leaves the organization, AppViewX lets the admin user have default access to all user dashboard, private as well as public.

To enable default admin access to all dashboards:

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **SYSTEM ADMINISTRATION**, select **Dashboard**. The **Settings :: Dashboard** page is displayed.	1. From the main navigation menu, click **Settings**. 2. On the **Settings** page, from the left menu, select **General** > **Dashboard**. The **Settings :: Dashboard** page is displayed.
Note: For more information on how to switch between menus, click here.	

1. On the **Settings :: Dashboard** page, turn on the **Dashboard view for admin** toggle.
2. Click **Save**.

Managing the Login Configuration

- Restricting the Number of User Sessions
- Restricting the Number of Login Attempts
- Managing User Inactivity
- Managing Password Policy

Restricting the Number of User Sessions

The **Restrict each user to a single session** toggle is turned off be default. The number of user sessions can be restricted by enabling this feature.

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **SYSTEM ADMINISTRATION**, select **Login Policy**. The **Settings :: Login configuration** page is displayed.	1. From the main navigation menu, click **Settings**. 2. On the **Settings** page, from the left menu, select **General** > **SMTP**. The **Settings :: SMTP** page is displayed.
Note: For more information on how to switch between menus, click here.	

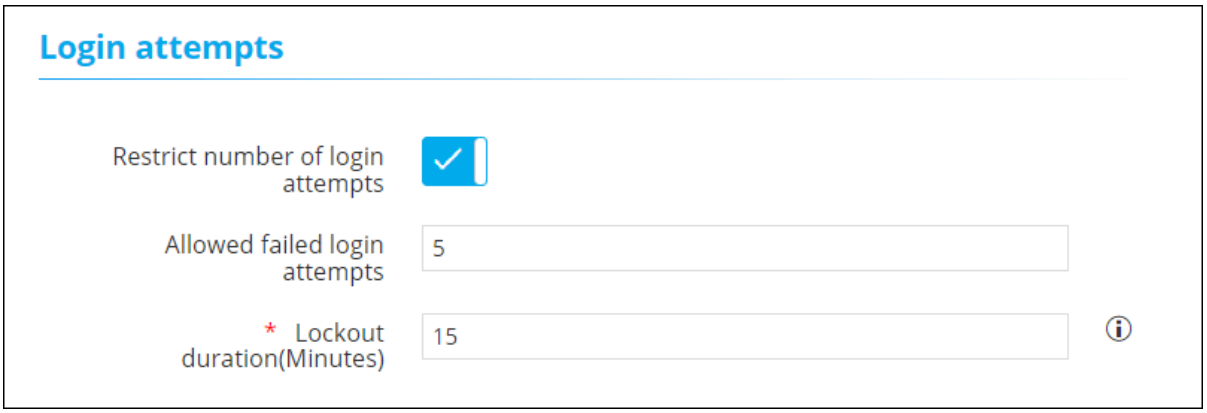
1. On the **Settings :: Login configuration** page, in the **Session** section, turn on the **Restrict each user to a single session** toggle.
2. Click **Save**.
3. In the **Confirmation** pop-up, click **OK**.
   The Login setting is modified and will be applied from next login for internal users.

Restricting the Number of Login Attempts

The **Restrict number of login attempts** toggle is turned off be default. The number of login attempts can be restricted by enabling this feature.

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **SYSTEM ADMINISTRATION**, select **Login Policy**. The **Settings :: Login configuration** page is displayed.	1. From the main navigation menu, click **Settings**. 2. On the **Settings** page, from the left menu, select **General** > **SMTP**. The **Settings :: SMTP** page is displayed.
Note: For more information on how to switch between menus, click here.	

1. On the **Settings :: Login configuration** page, in the **Login attempts** section, enter the following field information:



Field descriptions for Login attempts

Field	Description
Restrict number of login attempts	Turn on this toggle to restrict the number of login attempts by a user.
Allowed failed login attempts	Enter any number between 0 and 99 to set the number of login attempts permitted. **Note:** By default, this value is set to 5. If the user enters incorrect details more than 5 times, he/she will get locked out.
***Lockout duration (Minutes)**	Enter a value for the duration for which the account will be locked after the specified number of failed attempts. If the value entered is 0, then the account will remain locked until the administrator unlocks it manually.

Note: The asterisk (*) symbol indicates mandatory fields.

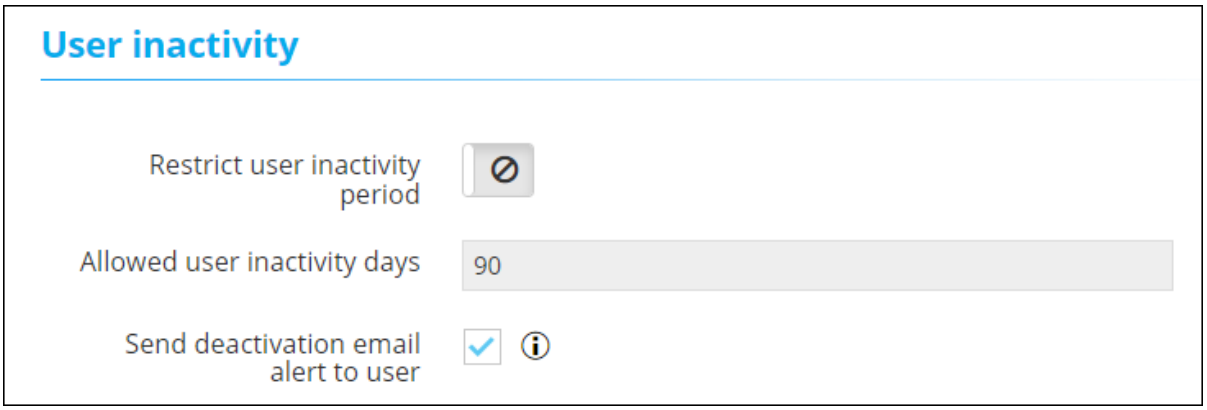
2. Click **Save**.

Managing User Inactivity

AppViewX lets you restrict a user from logging in to the system if they have been inactive for a predefined duration.

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **SYSTEM ADMINISTRATION**, select **Login Policy**. The **Settings :: Login configuration** page is displayed.	1. From the main navigation menu, click **Settings**. 2. On the **Settings** page, from the left menu, select **General** > **Login configuration**. The **Settings :: Login configuration** page is displayed.
Note: For more information on how to switch between menus, click here.	

1. On the **Settings :: Login configuration** page, in the **User inactivity** section, turn on the **Restrict user inactivity period** toggle.



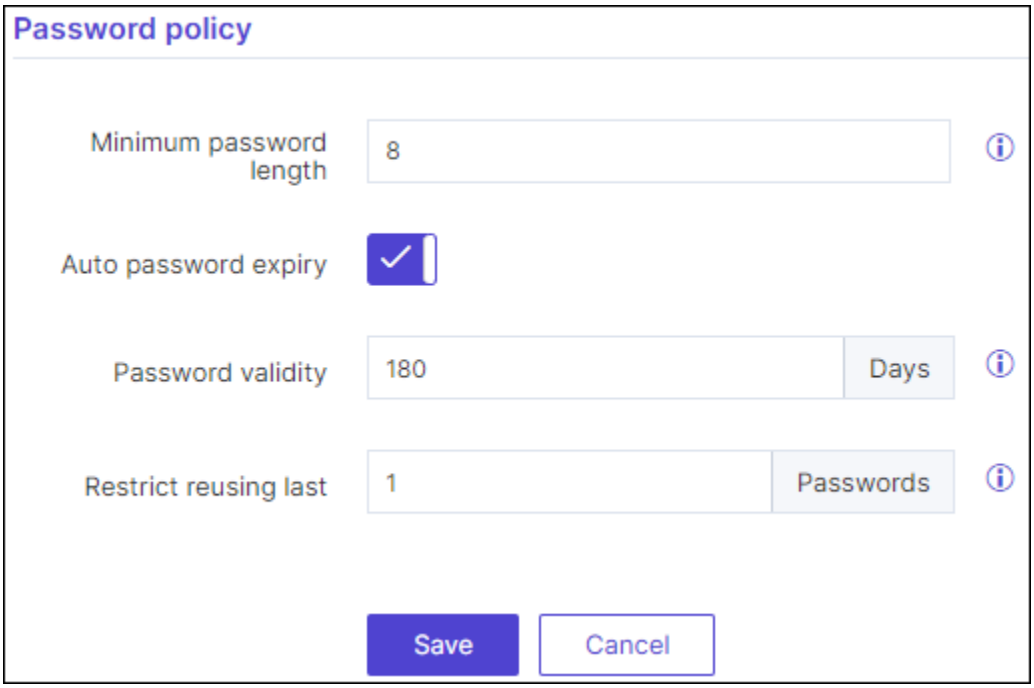
2. To set the number of days for which a user can remain inactive, in the **Allowed user inactivity days** text field, enter the required value (between 0 and 99).
3. To send the user an email when they are deactivated, select the **Send deactivation email alert to user** check box.
   An email alert is sent to the user for three consecutive days before deactivation.
4. Click **Save**.

Managing Password Policy

AppViewX allows you to manage password policies, enabling the configuration and enforcement of rules for minimum password length, automatic password expiry, setting password validity, and restricting the reuse of the last password. These measures enhance security within the system.

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **SYSTEM ADMINISTRATION**, select **Login Policy**. The **Settings :: Login configuration** page is displayed.	1. From the main navigation menu, click **Settings**. 2. On the **Settings** page, from the left menu, select **General** > **Login configuration**. The **Settings :: Login configuration** page is displayed.
Note: For more information on how to switch between menus, click here.	

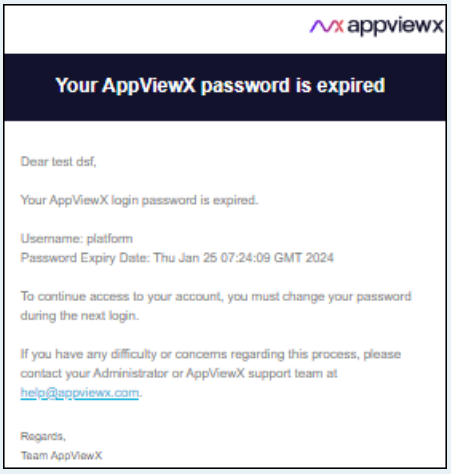
1. On the **Settings :: Login configuration** page, within the Password Policy section, adjust the Minimum password length from a minimum of 6 characters to a maximum of 128 characters.



Note: Users should reset the password for new password length to be effective and the minimum password length will be applicable only to internal users.

2. Enable or Disable the **Auto password expiry** toggle for automatic expiration of user passwords for enhanced security.
3. Define the **Password validity** duration in days, with a maximum limit of 1098 days.

Note: Users will start receiving email notification seven days prior to their password expiration date and we enforce the user to change the password if it has expired.



4. Define the number to **Restrict reusing last** passwords. This prevents users from reusing the last five passwords when changing it.
5. Click **Save**.
   It will save all the login configuration changes.

Managing Logs

Log management is an integral part of any customer-serving application. Monitoring and analyzing user activity logs helps in preventing security breaches, provides an insight into the performance of the applications, and contributes to troubleshooting.

As a part of log management, AppViewX tracks user activities and creates device and object level logs. For all recorded logs, it lets you:

- View logs
- Filter logs
- Forward logs
- Export logs
- Purge logs.

AppViewX lets you view all logs in one place as well as groups them under the following types for a segregated viewing:

- All
- Audit
- Self Audit
- Certificate
- ADC
- AppViewX
- Syslog
- SSH.

Accessing the Logs

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **OBSERVE & EXPLORE**, select **Logs**. The **Logging :: All** page is displayed with the **All** tab open by default.	From the main navigation menu, select **Logging**. The **Logging :: All** page is displayed with the **All** tab open by default.

New Menu	Old Menu

Note: For more information on how to switch between menus, click here.

Viewing Audit Logs

To view the audit logs:

1. Go to the **Logging :: All** page.
2. From the **Logging :: All** page, from the log categories, click **Audit**.
   The **Logging :: Audit** page is displayed. This page displays the following details:

Field descriptions for Audit Logs

Fields	Description
Time	Date and time at which the activity was carried out
User	Username of the user who performed the activity.
Device name	Name of the device, if the log is of a device-related activity
Object details	Name of the object, if the log is of a object-related activity
Source IP	IP address of the system that was the source of the activity.
AppViewX node	IP address of the installed AppViewX node.
Method of login	The method used for logging in to the AppViewX node, from one of the following: • UI • AppViewX (used for cronjob-related activities).
Comments	Comments related to the activity logged.
Log Message	Description of the activity logged

Viewing Self-Audit Logs

To view the self-audit logs:

1. Go to the **Logging :: All** page.
2. From the **Logging :: All** page, from the log categories, click **Self Audit**.
   The **Logging :: Self Audit** page is displayed. This page displays the following details:

Field descriptions for Self-Audit Logs

Fields	Description
Time	Date and time at which the activity was carried out
User	Username of the user who performed the activity.
Device name	Name of the device, if the log is of a device-related activity
Object details	Name of the object, if the log is of a object-related activity
Source IP	IP address of the system that was the source of the activity.
AppViewX node	IP address of the installed AppViewX node.
Method of login	The method used for logging in to the AppViewX node, from one of the following: • UI • AppViewX (used for cronjob-related activities)
Comments	Comments related to the activity logged.
Log Message	Description of the activity logged

Viewing Workflow Logs

To view the workflow logs:

1. Go to the **Logging :: All** page.
2. From the **Logging :: All** page, from the log categories, click **Workflow**.
   The **Logging** page is displayed. This page displays the following details:

Field descriptions for Workflow Logs

Fields	Description
Time	Date and time at which the activity was carried out.
Request ID	Workflow Request ID
User	Username of the user who performed the activity.

Fields	Description
Work order stage	The stage at which an action is performed on the workflow.
Alert severity	Severity of the workflow.
Log Message	Description of the activity logged.

Viewing Certificate Logs

To view the certificate logs:

1. Go to the **Logging :: All** page.
2. From the **Logging :: All** page, from the log categories, click **Certificate**.
   The **Logging :: Certificate** page is displayed. This page displays the following details:

Field descriptions for Certificate Logs

Fields	Description
Time	Date and time at which the activity was carried out
User	Username of the user who performed the activity.
Device name	Name of the device, if the log is of a device-related activity.
Object details	Name of the object, if the log is of a object-related activity.
Purpose/Usage	Certificate type (server, client, device, code signing) associated with the logged activity.
severity	Severity of the activity logged (Notification, Debug, Warn, Error, Fatal, Critical).
Log Message	Description of the activity logged.

Viewing Cloud Logs

To view the cloud logs:

1. Go to the **Logging :: All** page.
2. From the **Logging :: All** page, from the log categories, click **Cloud**.
   The **Logging :: Cloud** page is displayed. This page displays the following details:

Field descriptions for Cloud Logs

Fields	Description
Time	Timestamp of the event logged
User	Login name of the user that triggered the event
Source IP	IP address of the system from which the event was triggered
Cloud Account	Cloud device name for the event that is being logged
Cloud Vendor	Cloud device vendor
Cloud Service	Cloud service associated with the event **Note:** This field displays the name of the service(s) associated with the event that is being logged. However, there can be instances where events are independent of services. For example, credential validation for the master account is not related to any one service. If an event is independent of services, then all the services associated with the cloud account are listed for ease of searching the logs based on service name.
Cloud Region	Cloud region associated with the event **Note:** This field displays the name of the region(s) associated with the event that is being logged. However, there can be instances where events are independent of regions. For example, credential validation for the master account may not be related to any one region. If an event is independent of regions, then all the regions associated with the cloud account are listed for ease of searching the logs based on region name.
Event Source	Source (AppViewX UI or API) from where the event was triggered
Event Type	Type of the event being logged
Severity	Severity of the event triggered

Fields	Description
	This field can have one of the following values: • **Critical** • **Warning** • **Notification** • **Debug**.
Log Message	Details of the event outcome
Log Statement	Additional details related to the event outcome (optional)

Viewing ADC Logs

To view the ADC logs:

1. Go to the **Logging :: All** page.
2. From the **Logging :: All** page, from the log categories, click **ADC**.
   The **Logging :: ADC** page is displayed. This page displays the following details:

Field descriptions for ADC Logs

Fields	Description
Time	Date and time at which the activity was carried out
User	Username of the user who performed the activity
Device name	Name of the device, if the log is of a device-related activity
Object details	Name of the object, if the log is of a object-related activity
Alert severity	Severity of the activity logged (Notification, Debug, Warn, Error, Fatal, Critical)
Log Message	Description of the activity logged

Viewing AppViewX Logs

To view the AppViewX logs:

1. Go to the **Logging :: All** page.
2. From the **Logging :: All** page, from the log categories, click **AppViewX**.

The **Logging :: AppViewX** page is displayed. This page displays the following details:

Field descriptions for AppViewX Logs

Fields	Description
Time	Date and time at which the activity was carried out
Device name	Name of the device, if the log is of a device-related activity
Object details	Name of the object, if the log is of a object-related activity
Severity	Severity of the activity logged (Notification, Debug, Warn, Error, Fatal, Critical)
Log Message	Description of the activity logged

Viewing Syslog Logs

To view the syslog logs:

1. Go to the **Logging :: All** page.
2. From the **Logging :: All** page, from the log categories, click **Syslog**.
   The **Logging :: Syslog** page is displayed. This page displays the following details:

Field descriptions for Syslog

Fields	Description
Time	Date and time at which the activity was carried out.
Host name	Host name of the Syslog server.
Log Message	Description of the activity logged.

Viewing Firewall Logs

To view the firewall logs:

1. Go to the **Logging :: All** page.
2. From the **Logging :: All** page, from the log categories, click **Firewall**.
   The **Logging :: Firewall** page is displayed. This page displays the following details:

Field descriptions for Firewall Logs

Category	Description
Time	Date and time at which the activity was carried out.
User	Username of the user who performed the activity.
Device name	Name of the device, if the log is of a device-related activity
Object details	Name of the object, if the log is of a object-related activity
Log Message	Description of the activity logged.

Viewing Sign Logs

1. Go to **Logging :: All** page.
2. From the **Logging :: All** page, from the log categories, click **Sign**.
   The **Logging :: Sign** page is displayed.
3. Use the following filters to display limited data:
   - Search by text field
   - Search by time icon (date and time)
   - Search by **Method of Login** dropdown.

   This page displays the following details:

Field descriptions for Sign Logs

Fields	Description
Time	Date and time at which the activity was carried out.
User	Username of the user who performed the activity.
Severity	Severity of the activity logged (Notification, Debug, Warn, Error, Fatal, Critical).
Category	Name of the module. In this case - Sign.
Method of login	Indicates the type of signing. UI is for a file-based signing (File upload and sign) and API is for a hash-based signing.
Log message	Description of the activity logged.

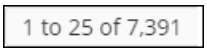
Fields	Description
Source IP	IP of the device from where the action was performed.
AppViewX node	IP:node of the AppViewX server from where the action was performed.

Setting the Record Count Preference for Logs

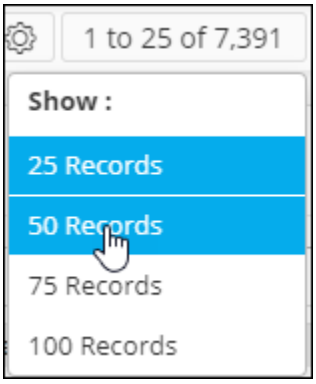
For easier viewing of records, AppViewX lets you set the record count preference, which is the number of log records that will be displayed on one page.

Note: By default, 100 records are shown on one page (which is why the control reads 1 to 100).

To set the record count preference:

1. On the **Logging :: All** page, from the top-right corner of the screen, click 

.
2. From the **Show** menu displayed, select your record count preference (for example, 25 records).



3. The Logging page is updated according to the record count preference selected. A message, **Record count preference saved successfully**, is displayed. The UI control is also updated to display the current selection, as shown in the following image:

Searching for Logs

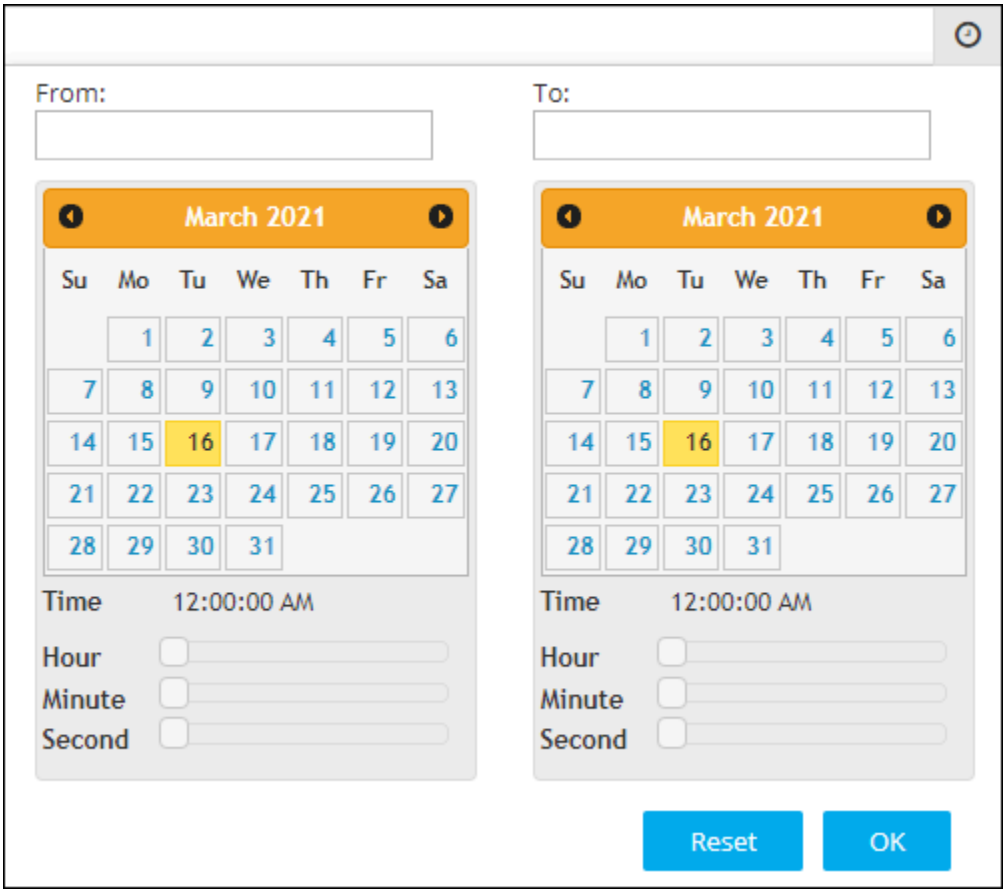
AppViewX lets you search for logs in two ways:

- Based on a timestamp
- Based on the values recorded for each log.

Based on a Timestamp

To search for logs based on a timestamp:

1. From the **Search** field on the **Logging** page, click  **(Clock)** icon.
2. Widgets to select the date and time are displayed.



3. To select a date range, in the **From** and **To** fields, select the required dates.
4. To set a time, use the **Hour**, **Minute**, and **Second** slider controls.
5. Click **OK**.

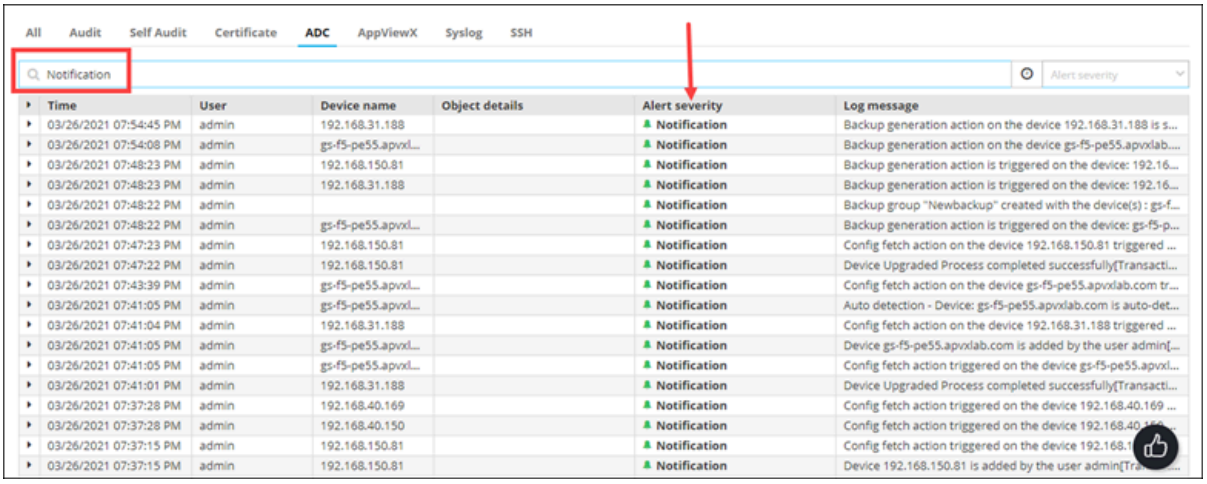
The page is updated to display log records from the selected timestamp.

Note: To view records from a specific date to the current date, select only the From date. When the To field is left blank, by default, it is set to the current date.

Based on the Values Recorded for each Log

To search for logs based on a value for one of the categories, for example, to search for ADC logs with the severity Notification:

1. Go to the **Logging :: All** page and click the **ADC** tab.
2. From the drop-down menu in the **Search** field, select a category, for example, **Alert Severity**, for searching the required logs.
3. In the **Search** field, enter a search value. for example, **Notification**.
   The page is updated to display logs that fulfill the search criteria.



Forwarding Logs

Before logs are purged, AppViewX enables forwarding logs to external servers, like SIEM, that allows for a detailed analysis and, therefore, better identification of problem areas. This gives an advantage when configuring alerts; new alerts can be created to target and resolve the problem areas identified.

- Configuring Server Inventory Settings
- Configuring Forwarding Settings

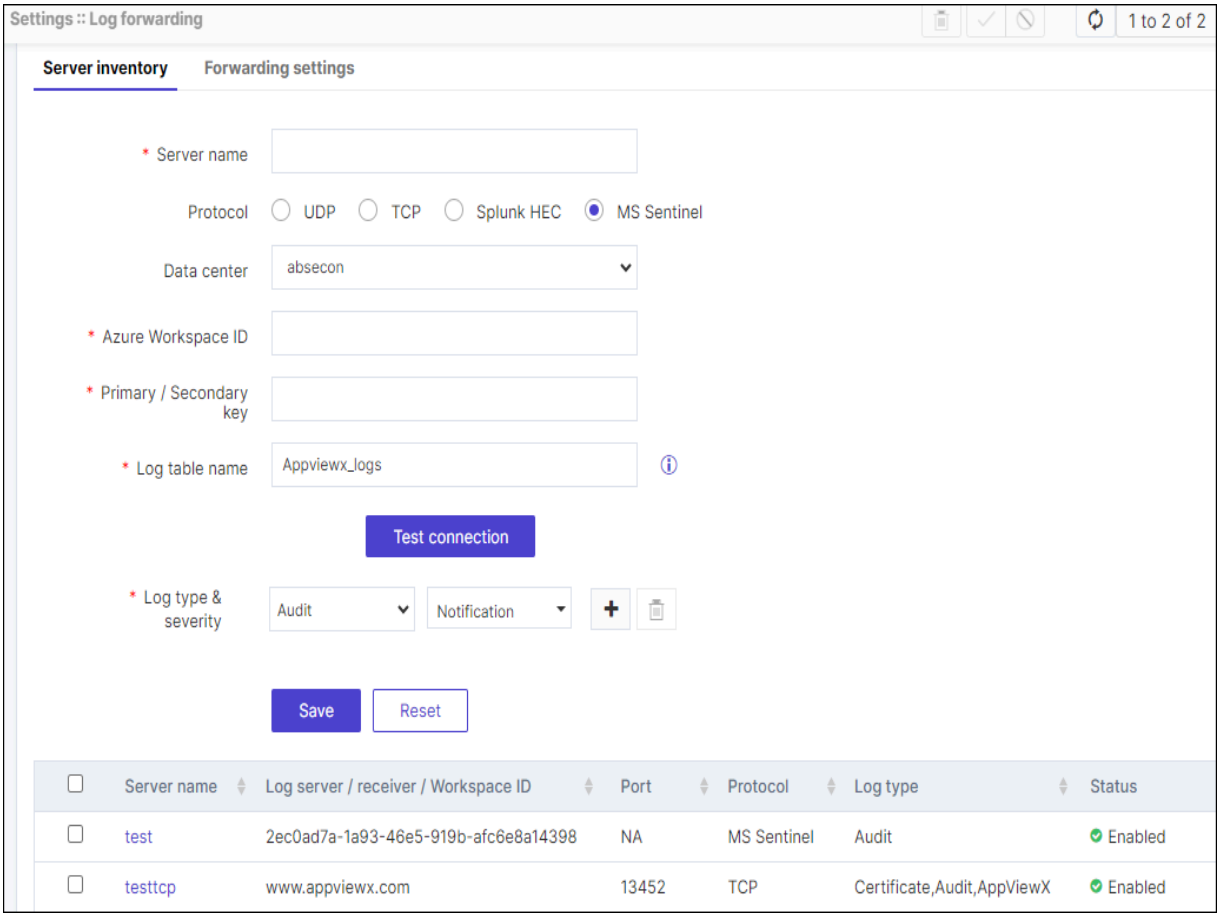
Configuring Server Inventory Settings

Server inventory settings are used to configure settings for forwarding logs to a specific external server.

To configure server inventory settings:

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **OBSERVE & EXPLORE**, select **Log Forwarding**. The **Settings :: Log Forwarding** page is displayed with the **Server inventory** tab open by default.	1. From the main navigation menu, click **Settings**. 2. On the **Settings** page, select **General** > **Log Forwarding** The **Settings :: Log Forwarding** page is displayed with the **Server inventory** tab open by default.
Note: For more information on how to switch between menus, click here.	

1. On the **Settings :: Log Forwarding** page, in the **Server inventory** tab, enter the following details.



Field descriptions for Server inventory

Field	Description
***Server name**	Name of the external server to which the logs will be forwarded
***Log server / receiver**	The IP address of the external server to which the logs will be forwarded
***Protocol**	Select a protocol from the following options: • UDP (default) • TCP • Splunk HEC • MS Sentinel.
***Port**	Enter the port number to be used for the server.
Data center	From the options available in the dropdown, select the data center.
Enable HTTPS	For more details on steps for Configuring Splunk HEC.

Field	Description
	Note: This field is enabled if you select **Splunk HEC** as your **Protocol**. Enable the HTTPS toggle button if the exposed hostname needs SSL verification.
Validate Certificate	**Note:** This field is enabled if you enable the **HTTPS toggle** button. • If you select **Global Root CA's** as **Validate Certificate** type there is no additional validation required. • If you select **Custom CA Certificate** as **Validate Certificate** type there is an additional validation of Uploading certificate is required.
***Upload certificate**	Click on **Browse** to Upload the certificate created from the **HTTP Event Collector** URL. **Note:** Certificate has to be uploaded in the **.pem** format.
Index	**Note:** This field is enabled if you select **Splunk HEC** as your **Protocol**. Enter the indexer created while creating the HTTP Event Collector token on Splunk Enterprise for log forwarding on the server. If Indexer is not created and set to default, then it can be left blank.
***Authentication Token**	**Note:** This field is enabled if you select **Splunk HEC** as your **Protocol**. Enter the HTTP Event Collector token value generated while creating the HTTP Event Collector token on Splunk Enterprise for log forwarding on the server.
***Azure Workspace ID**	For more details on steps for Configuring MS Sentinel.

Field	Description
	For more detailed steps on Creating a resource group during the configuration of MS Sentinel. **Note:** This field is enabled if you select **MS Sentinel** as your **Protocol**. The unique identifier for the Log Analytics workspace.
***Primary / Secondary key**	**Note:** This field is enabled if you select **MS Sentinel** as your **Protocol**. A security key providing access to a range of management and data operations.
***Log table name**	**Note:** This field is enabled if you select **MS Sentinel** as your **Protocol**. The default name of the log table is “Appviewx_logs”, which can be changed as per user requirements.
***Log type & severity**	You can choose to forward logs of a specific type and a specific severity to an external server. **To add a log type and severity entry:** a. From the first drop-down menu, select a log type from the following: • Audit (default) • Certificate • ADC • AppViewX • VisualWorkflow. b. From the second drop-down menu, select the severity of the log type from the following: • Notification (default) • Debug • Warning

Field	Description
	• Error • Fatal • Critical. **Note:** You can select more than one severity value for a log type. **To add multiple log types and severity entries:** a. From the **Log type & severity** field, click **(Add)** icon. b. From the first drop-down menu, select a log type. c. From the second drop-down menu, select a severity for the log type. d. To add another log type and severity entry, repeat steps **a** to **c**. **To delete a log type and severity entry,** from the **Log type & severity** field, click **(Delete)** icon. **Note:** It is mandatory to have at least one log type and severity entry.
Note: The asterisk (*) symbol indicates mandatory fields.	

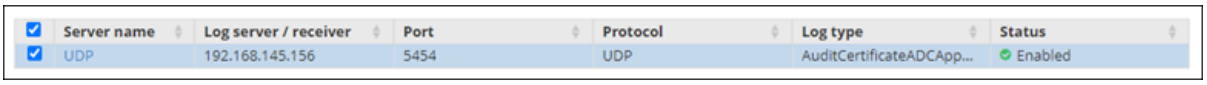
2. To save the server inventory settings, click **Save**.
   The settings configured in the fields above are displayed in the table shown at the end of the page.

• Enabling Server Inventory Settings
• Disabling Server Inventory Settings
• Deleting Server Inventory Settings

Enabling Server Inventory Settings

To enable a server inventory setting:

1. From the table at the bottom of the **Server inventory** page, select the server inventory setting you want to enable.



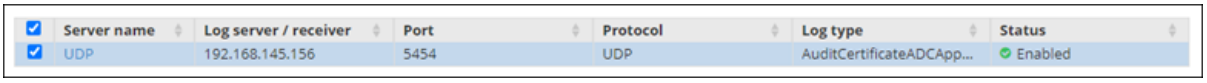
2. From the top right corner of the screen, click **(Enable)** icon.

> **Note:** You can enable multiple server inventory settings by selecting the check box against all the settings you want to enable.

Disabling Server Inventory Settings

To disable a server inventory setting:

1. From the table at the bottom of the **Server inventory** page, select the server inventory setting you want to disable.



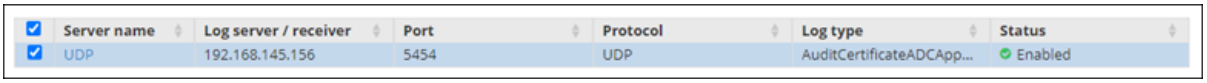
2. From the top right corner of the screen, click **(Disable)** icon.

> **Note:** You can disable multiple server inventory settings by selecting the check box against all the settings you want to disable.

Deleting Server Inventory Settings

To delete a server inventory setting:

1. From the table at the bottom of the **Server inventory** page, select the server inventory setting you want to delete.



2. From the top right corner of the screen, click **(Delete)** icon.

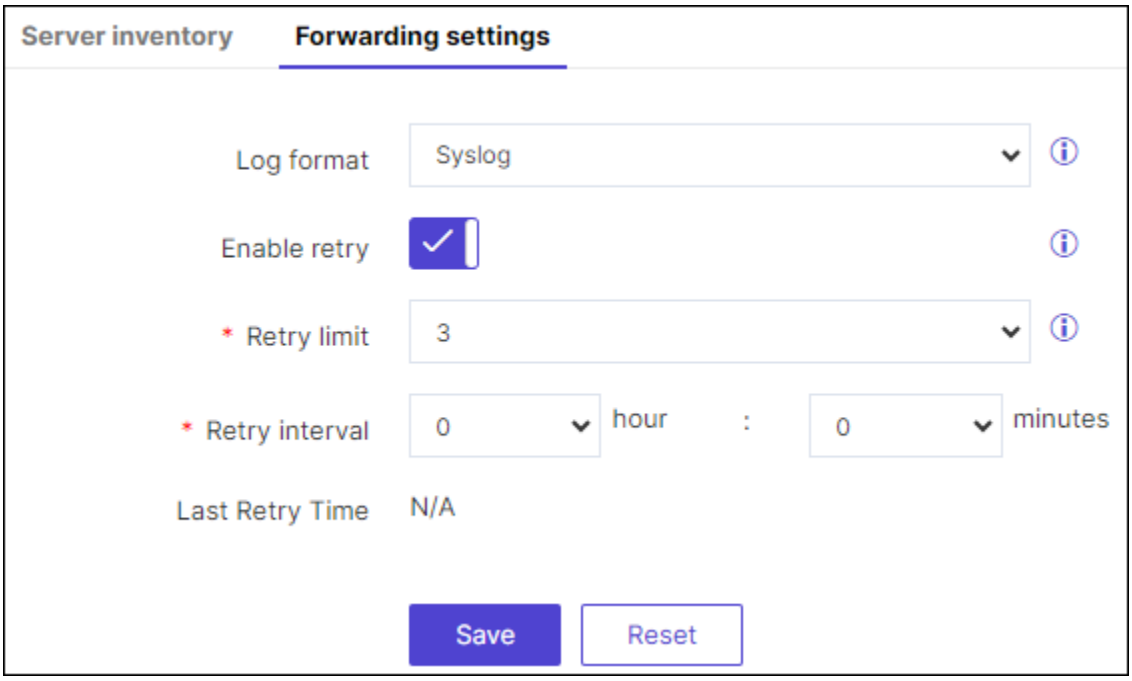
> **Note:** You can delete multiple server inventory settings by selecting the check box against all the settings you want to delete.

Configuring Forwarding Settings

To configure the forwarding settings follow the below steps:

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **OBSERVE & EXPLORE**, select **Log Forwarding**. The **Settings :: Log Forwarding** page is displayed with the **Server inventory** tab open by default.	1. From the main navigation menu, click **Settings**. 2. On the **Settings** page, select **General** > **Log Forwarding** The **Settings :: Log Forwarding** page is displayed with the **Server inventory** tab open by default.
Note: For more information on how to switch between menus, click here.	

1. On the **Settings :: Log Forwarding** page, under the **Forwarding settings** tab, enter the following details:



Field descriptions for forwarding settings

Field	Description
Log format	To select the format in which logs should be forwarded to the external server, from the drop-down menu, select one of the following options: • Syslog • CEF. **Note:** CEF is the most recent industry standard for forwarding logs.
Enable retry	If an attempt to forward logs fails because of server unavailability, AppViewX lets you set a retry interval the duration after which logs will be forwarded again. To enable this retry, turn on the **Enable retry** toggle.
***Retry limit**	Configure this value to provide maximum retry attempts for forwarding the logs when server(s) are down/unreachable.
***Retry interval**	To set a retry interval, from the **hour** and **minutes** drop-down menus, select the required values.

Field	Description
	Note: This field is displayed when the **Enable retry** toggle is turned on.
Last Retry Time	Displays the date and time of the previous attempt of log forwarded.

Note: The asterisk (*) symbol indicates mandatory fields.

2. To set a retry interval, from the hour and minutes drop-down menus, select the required values.

Exporting Logs

AppViewX lets you export logs as Excel sheets.

1. Go to the **Logging :: All** page for the log type you want to export.
2. From the top right corner of the page, click **(Export)** icon.
3. Navigate to the location to save the log file, and click **Save**.
   All logs of the selected log type are downloaded and saved.

HSM Integration for AppViewX

An HSM (Hardware Security Module) is a piece of hardware and associated software or firmware that usually resides in a PC or server and provides at least the minimal cryptographic functions. These functions include encryption, decryption, key generation, and hashing. The physical device offers physical tamper-resistance and has a user interface and a programmable interface. Other names for an HSM include Personal Computer Security Module (PCSM), Secure Application Module (SAM), Hardware Cryptographic Device, or Cryptographic Module.

For the deployment, AppViewX enables support for integrating all HSMs that support the PKCS11 library, an interface that facilitates interaction between the HSM and AppViewX. This eliminates the need to deploy vendor-specific SDKs and JAR files, thus significantly reducing the time it takes for integrating and installing an HSM.

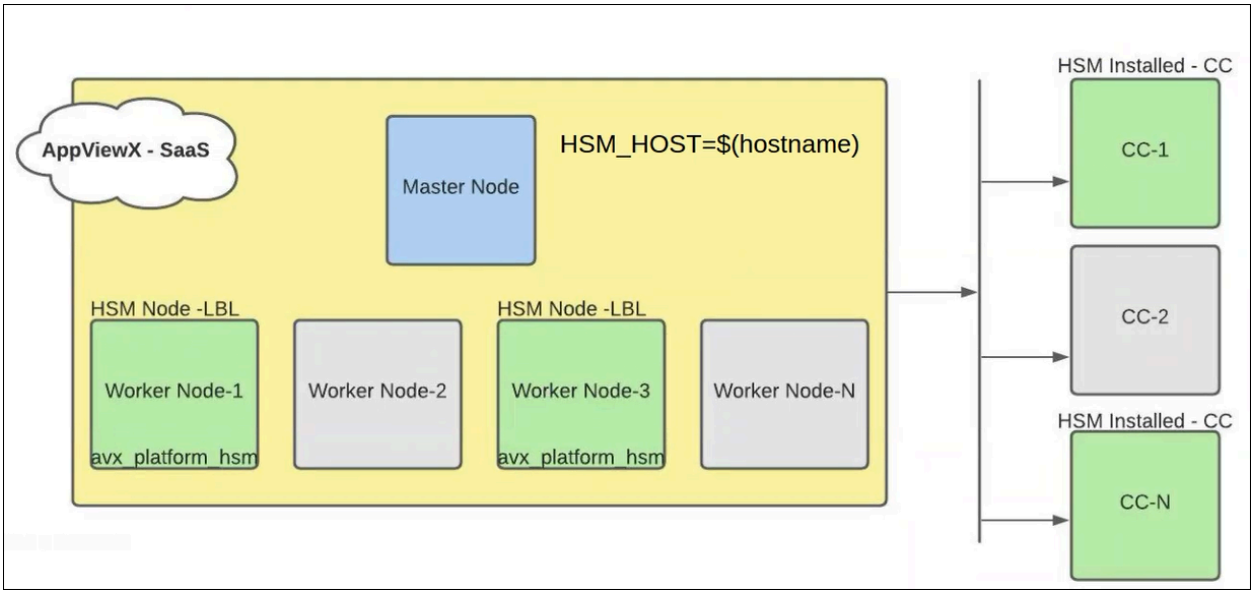
The deployment currently supports the following four HSM vendors:

- Utimaco
- Fortanix
- Thales TCT
- Thales - DPoD
- Thales - GPN.

Accessing HSM

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **VAULT & SECURITY**, select **HSM**. The **HSM** page is displayed.	1. From the main navigation menu, select **Inventory** > **HSM**. 2. The **HSM** page is displayed.
Note: For more information on how to switch between menus, click here.	

HSM Architecture for the SaaS Deployment



In the SaaS deployment, all necessary configuration files enabling integration and communication with HSM are installed on the AppViewX Cloud Connector.

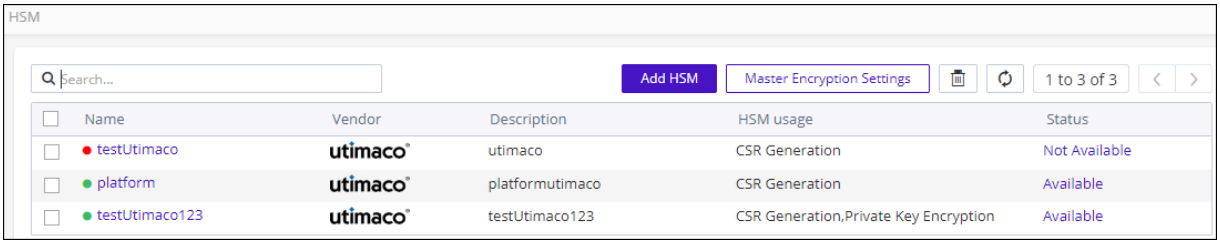
In a SaaS deployment, the chosen cloud connector used for HSM communication should have strict routing enabled.

HSM Inventory

The Inventory section allows you to add and configure HSM vendors such Utimaco, Fortanix, Thales TCT, Thales DPoD, and Thales GPN. By default the Inventory displays the HSM vendors that have already been configured. However, you can add and configure a vendor of your choice.

To configure HSM for a vendor:

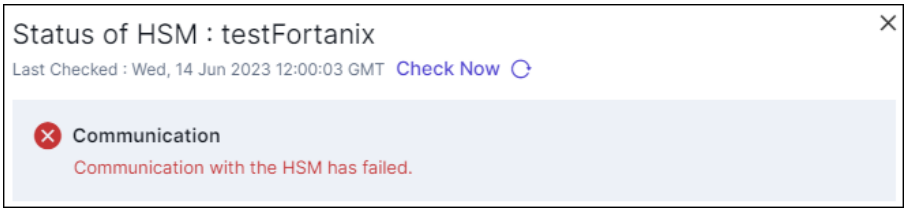
1. On the **HSM** page, the inventory of all added HSMs, displays details such as name, vendor, description, HSM Usage, and status.



   You can use the search bar.

The inventory table provides essential details about the integrated HSM.

Field descriptions for HSM Inventory

Field	Description
Name	Displays the name of integrated HSM.
Vendor	Displays the vendor name of integrated HSM.
Description	Displays the description of integrated HSM.
HSM usage	It displays the usage of HSM. **Note:** If you opt to use the HSM for Master Key Encryption in SaaS, its reflection in the HSM Usage column will occur only after the Account Owner has selected that HSM in the Master Encryption Settings Page.
Status	Displays the current status of the HSM. • **Available** To know the details about the communication and last checked date and time, click on the "Available" status. • **Not Available** To know the details about the reason for communication failure and last checked date and time, click on the "Not Available" status.  • **In Progress** To know the details about the communication In progress, click on the "In-progress" status.

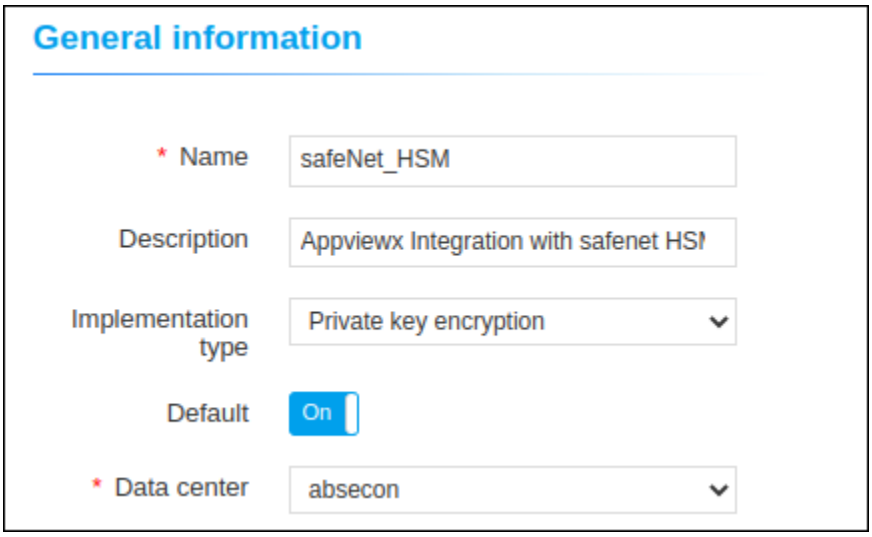
2. On the **HSM** page, from the top-right corner of the screen, click Add HSM.
3. From the left pane, select the vendor for whom you want to integrate HSM.
   HSM integration details fields are displayed for the selected vendor.

4. Enter the **HSM details** for the vendor.
   - To enter the HSM details for Utimaco, click here.
   - To enter the HSM details for Fortanix, click here.
   - To enter the credential details for Thales TCT, click here.
   - To enter the credential details for Thales DPoD, click here.
   - To enter the credential details for Thales GPN, click here.
5. Click **Save**.

- Adding HSM in the inventory
- HSM Encryption Settings

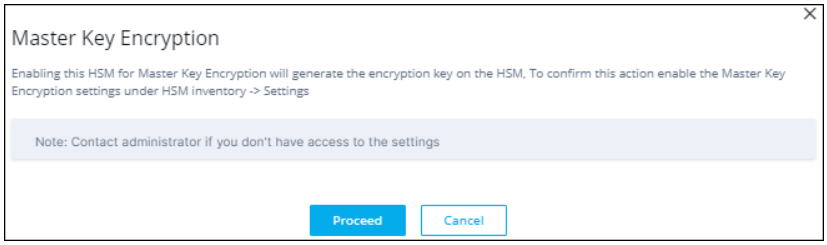
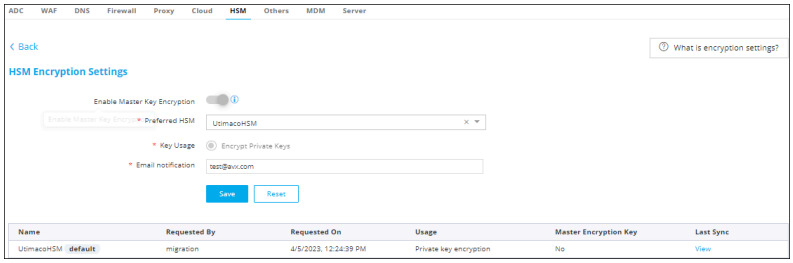
Adding HSM in the inventory

1. Login to the AppViewX UI using valid credentials.
   The **Dashboard** page is displayed by default.
2. On **HSM** page, click **Add HSM**, from the navigation pane on the left, select **Thales TCT**.
   The **HSM > Add** page is updated to display the fields required to integrate Thales TCT with the AppViewX.
3. In the **General Information** section, enter/select the required field information.

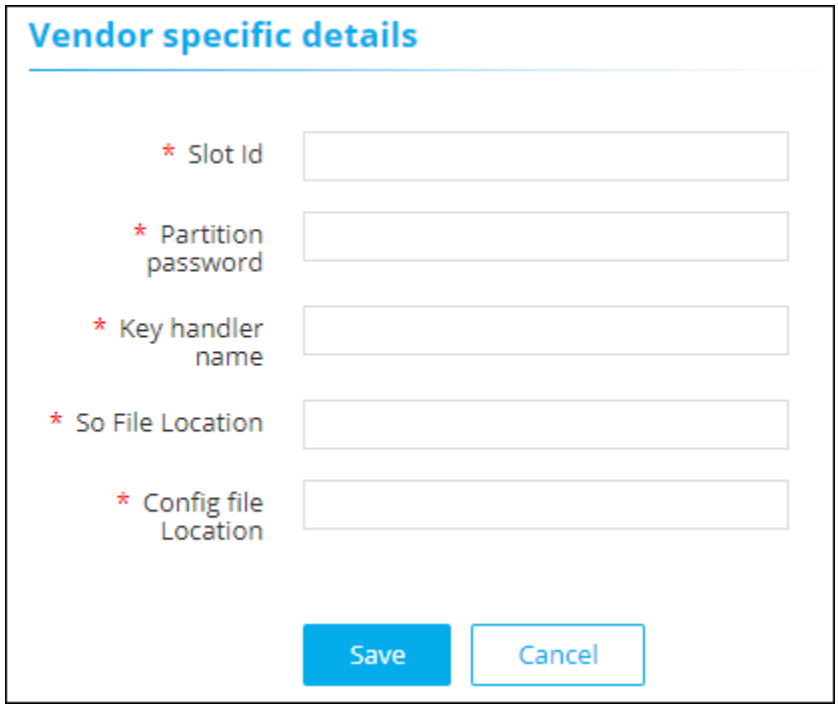


Field descriptions for General Information

Field	Description
***Name**	Enter a name for this integration.
Description	Enter a description for the integration.

Field	Description
Implementation type	Select an implementation type from the following options: • CSR generation • Master key encryption • Both  a. Click **Proceed**. b. To confirm this action enable the **Master Key Encryption settings** under **HSM inventory** > **Settings**. 
***Data center**	From the dropdown list, from the list of applicable values, select the required data center. **Note:** The data center selected here is used to map the AppViewX Cloud Connector for this integration.
Note: The asterisk (*) symbol indicates mandatory fields.	

4. In the **Vendor specific details** section, enter/select the required field information.



Field descriptions for Vendor specific details

Field	Description
***Slot Id**	Unique identification number of the slot in the HSM will be used to communicate with the end HSM device.
***Partition password**	Password of the HSM partition for the specific slot mentioned above.
***Key handler name**	A reference name to create a Master Encryption key in HSM. This enables us to pick the right MEK for crypto operations over KEK.
***So File**	The SO file is used to facilitate the communication between the HSM and AppViewX. Enter the .so file location hsm/safenet/lunaclient/lib/libCryptoki2_64.so. So File Location:
***Config file**	The Config file is used to facilitate the communication between the HSM and AppViewX. Enter the .conf file location hsm/Chrystoki.conf.

Note: The asterisk (*) symbol indicates mandatory fields.

5. Click **Save**.
6. Scroll to the end of this page to view the table/navigate to HSM inventory to view the HSM status. If the HSM has been configured correctly, the Status for the HSM will be set to **Available** (after checking the encryption and decryption logic). If the Status is **Not Available**:
   a. Check the installation path for the HSM.
   b. Ensure that all required permissions have been enabled.
   c. Go to **Logs** > **Logging :: All**. Search with HSM and see the **Log message**.
7. If the implementation type is CSR Generation, refer to the Cert+ User Guide for steps on how to generate a CSR.

HSM Encryption Settings 

To secure certificates with a private key, enable private key encryption in the Master Encryption Settings page. Follow the steps below to enable private key encryption.

1. Add a new HSM to the HSM inventory by selecting Master Key Encryption as the HSM usage.
2. In the top-right corner of the HSM inventory page, select the Master Encryption Settings button.
3. Enable the Master Key Encryption Toggle under the HSM Settings.
4. Select the added HSM from the preferred HSM dropdown and set the key usage to encrypt private keys.
5. Provide notification emails or email distro, in the case of HSM connectivity or key not accessible failures to the administrators.

> **Note:** To receive default HSM health status emails, set up the email address in the settings page. Ensure SMTP settings are configured in **Platform** > **System Administration** > **SMTP** for email functionality.

6. Save the Settings for the HSM to be marked as default HSM for storing encryption keys.

HSM Installation and Configuration

- Utimaco
- Fortanix
- Thales TCT

- Thales DPoD
- Thales GPN

Utimaco

Prerequisites

1. The Utimaco HSM device setup should be available.
2. HSM slot initialization and crypto user credential creation should be done.
3. Communication to the hsm and appviewx nodes in the case of  and the cloud connector in the case of  should be available to integrate with AppViewX.
4. Slot id and partition password from the Utimaco device should be available to use in the AppViewX.

   ```
   pkcs11_Utimaco.so
   ```

   and

   ```
   cs_pkcs11_R2.cfg
   ```

   file should be available; a sample format of a cfg file is available here.

- Integrating the Utimaco HSM with the AppViewX Onprem
- Integrating the Utimaco HSM with the AppViewX SaaS

Integrating the Utimaco HSM with the AppViewX Onprem

To integrate the Utimaco HSM with the AppViewX:

1. Login to the AppViewX server on which the AppViewX is installed.
2. From the command line interface, navigate to the properties folder path:
   {APPVIEWX_INSTALLATION_PATH}/appviewx_dependencies/properties
3. Open the **hsm** file using the following command:

   ```
   vi hsm
   ```

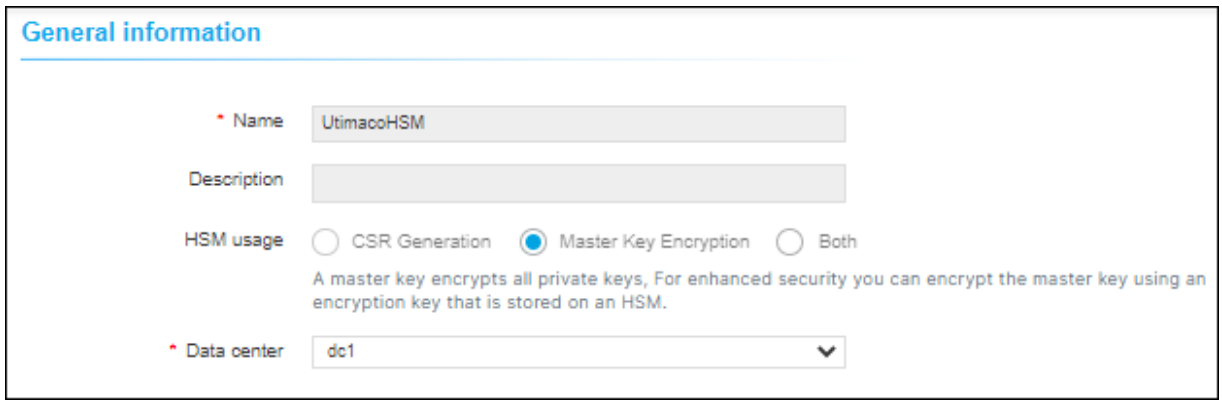
4. Check and confirm if the HSM file has the following lines. If not, uncomment the following lines:

   ```
   export CS_PKCS11_R2_CFG=/appviewx/dependencies/hsm/utimaco/cs_pkcs11_R2.cfg

   echo "UTIMACO Config Path : $CS_PKCS11_R2_CFG"
   ```

5. If the file is edited, you have to restart the avx-platform-hsm pod, using the following commands:

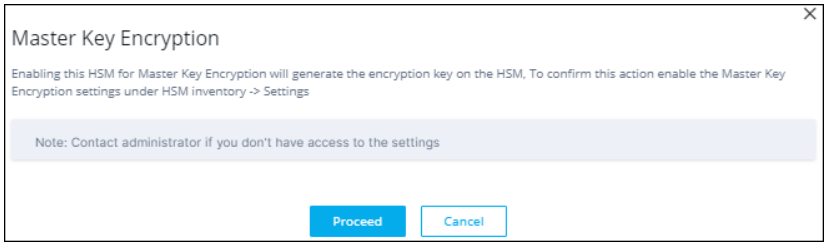
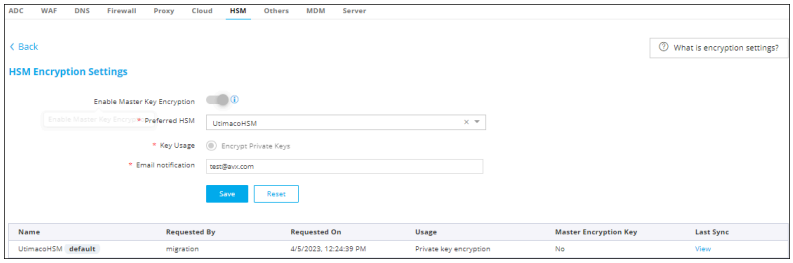
```
kubectl get pods -n <namespace>

kubectl delete pods -n <namespace> <PodName>
```

6. Login to the AppViewX UI using valid credentials.
   The **Dashboard** page is displayed by default.
7. On **HSM** page, click **Add HSM**, from the navigation pane on the left, select **Utimaco**.
   The **HSM > Add** page is updated to display the fields required to integrate Utimaco with the AppViewX.
8. To integrate the utimaco hsm device with appviewx, please get the following details from the hsm device.
9. In the **General Information** section, enter/select the required field information.

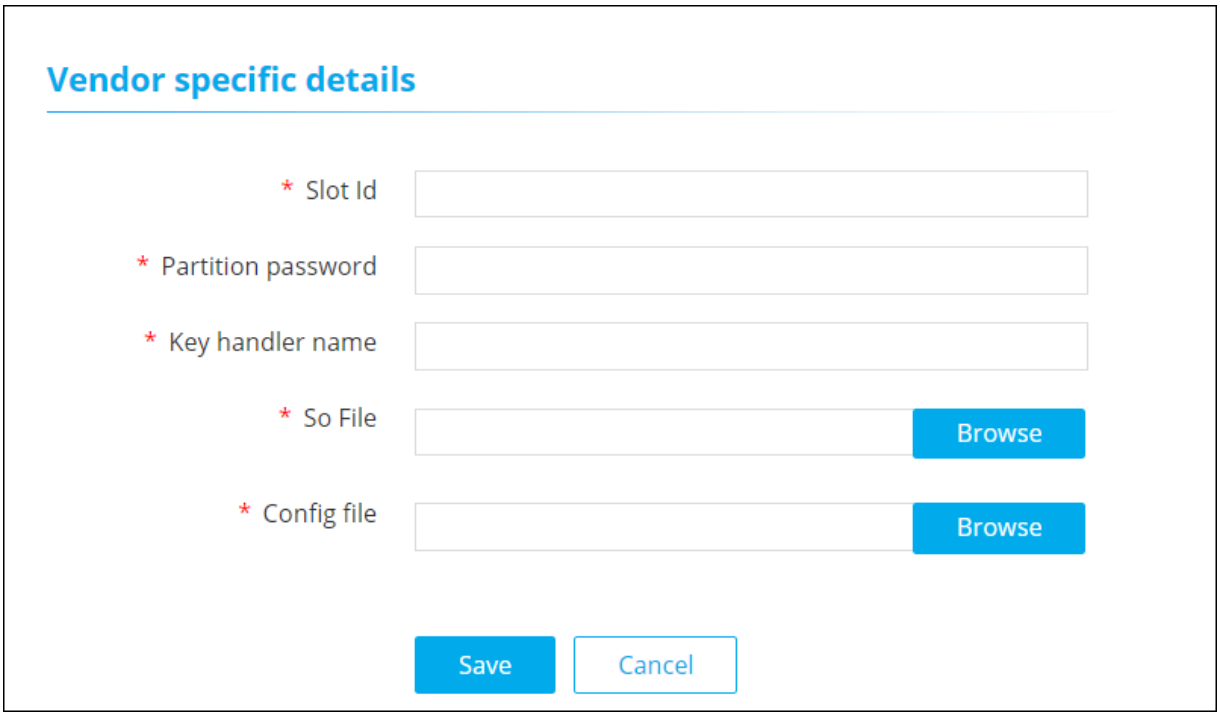


Field descriptions for General Information

Field	Description
***Name**	Enter a name for this integration.
Description	Enter a description for the integration.
Implementation type	Select an implementation type from the following options: • CSR generation • Master key encryption

Field	Description
	 a. Click **Proceed**. b. To confirm this action enable the **Master Key Encryption settings** under **HSM inventory** > **Settings**.  • Both
***Data center**	From the dropdown list, from the list of applicable values, select the required data center. **Note:** The data center selected here is used to map the AppViewX Cloud Connector for this integration.
Note: The asterisk (*) symbol indicates mandatory fields.	

10. In the **Vendor specific details** section, enter/select the required field information.



Field descriptions for Vendor specific details

Field	Description
***Slot Id**	Unique identification number of the slot in the HSM will be used to communicate with the end HSM device.
***Partition password**	Password of the HSM partition for the specific slot mentioned above.
***Key handler name**	A reference name to create a Master Encryption key in HSM. This enables us to pick the right MEK for crypto operations over KEK.
***So File**	The SO file is used to facilitate the communication between the HSM and AppViewX. To upload the .so file: a. Click **Browse**. b. Navigate to the location of the .so file. c. Select the .so file, and click **Open**.
***Config file**	The Config file is used to facilitate the communication between the HSM and AppViewX. To upload the .conf file: a. Click **Browse**. b. Navigate to the location of the .conf file. c. Select the .conf file, and click **Open**.

Field	Description
	Note: The asterisk (*) symbol indicates mandatory fields.

11. Click **Save**.
12. Scroll to the end of this page to view the table or navigate to HSM inventory to view the HSM status. If the HSM has been configured correctly, the status for the HSM will be set to **Available** after checking the encryption and decryption logic. If the Status is **Not Available**:
    a. Check the installation path for the HSM.
    b. Ensure that all required permissions have been enabled.
    c. Go to **Logs** > **Logging :: All**. Search with HSM and see the **Log message**.
13. If the implementation type is CSR Generation, refer to the Cert+ User Guide for steps on how to generate a CSR.

Integrating the Utimaco HSM with the AppViewX SaaS

To integrate the Utimaco HSM with the AppViewX:

1. Login to the AppViewX server on which the Cloud Connector is installed.
2. From the command line interface, navigate to the properties folder path:
   {CC_INSTALLATION_PATH}/deps/properties
3. Open the **hsm** file using the following command:

```
vi hsm
```

4. Check and confirm if the HSM file has the following lines. If not, uncomment the following lines:

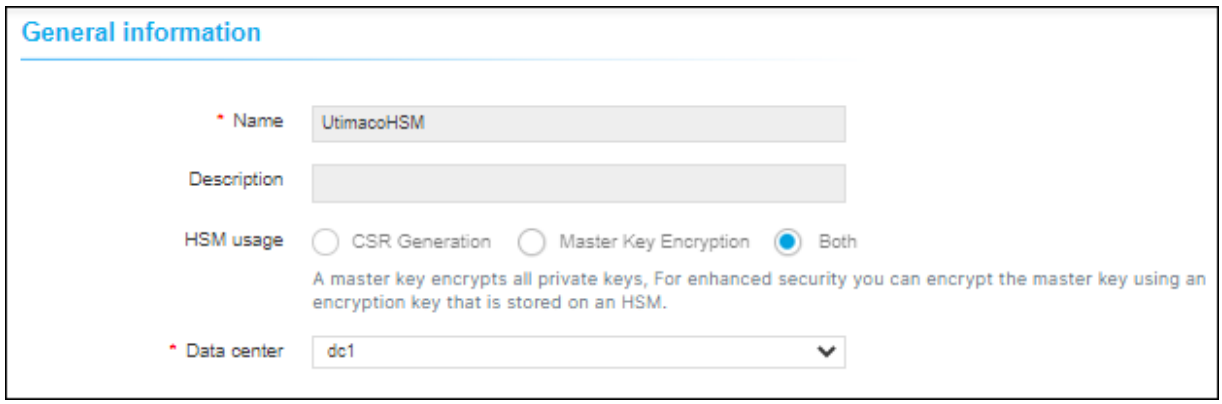
```
export CS_PKCS11_R2_CFG= /appviewx/dependencies/external_libs/hsm/utimaco/cs_pkcs11_R2.cfg

echo "UTIMACO Config Path : $CS_PKCS11_R2_CFG"
```

5. If the file is edited, you have to restart the avx-mid-server-platform pod, using the following commands:

```
kubectl get pods -n <namespace>

kubectl delete pods -n <namespace> <PodName>
```

6. Login to the AppViewX UI using valid credentials.
   The **Dashboard** page is displayed by default.
7. On HSM page, click **Add HSM**, from the navigation pane on the left, select **Utimaco**.
   The **HSM > Add** page is updated to display the fields required to integrate Utimaco with the AppViewX.

8. To integrate the utimaco hsm device with appviewx, please get the following details from the hsm device.
9. In the **General Information** section, enter/select the required field information.

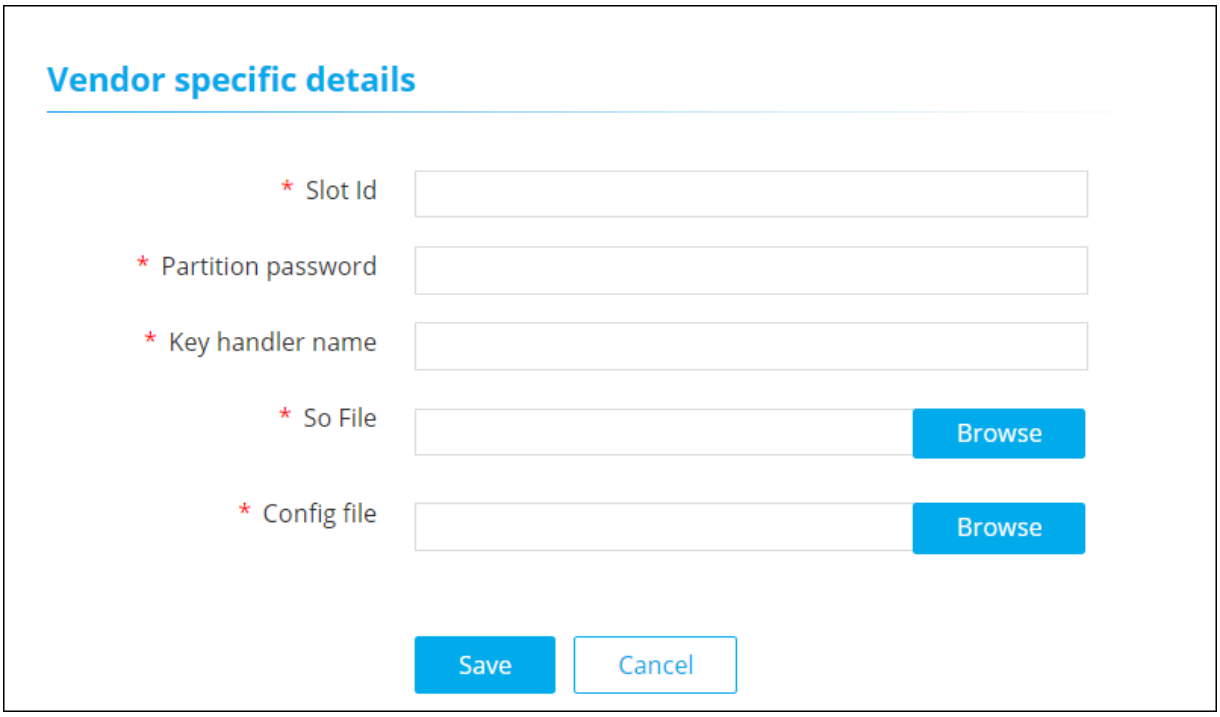


Field descriptions for General Information

Field	Description
***Name**	Enter a name for this integration.
Description	Enter a description for the integration.
Implementation type	Select an implementation type from the following options: • CSR generation • Master key encryption • Both
***Data center**	From the dropdown list, from the list of applicable values, select the required data center. **Note:** The data center selected here is used to map the AppViewX Cloud Connector for this integration.

Note: The asterisk (*) symbol indicates mandatory fields.

10. In the **Vendor specific details** section, enter/select the required field information.



Field descriptions for Vendor specific details

Field	Description
***Slot Id**	Unique identification number of the slot in the HSM will be used to communicate with the end HSM device.
***Partition password**	Password of the HSM partition for the specific slot mentioned above.
***Key handler name**	A reference name to create a Master Encryption key in HSM. This enables us to pick the right MEK for crypto operations over KEK.
***So File**	The SO file is used to facilitate the communication between the HSM and AppViewX. To upload the .so file: a. Click **Browse**. b. Navigate to the location of the .so file. c. Select the .so file, and click **Open**.
***Config file**	The Config file is used to facilitate the communication between the HSM and AppViewX. To upload the .conf file: a. Click **Browse**. b. Navigate to the location of the .conf file. c. Select the .conf file, and click **Open**.

Field	Description
	Note: The asterisk (*) symbol indicates mandatory fields.

11. Click **Save**.
12. Scroll to the end of this page to view the table or navigate to HSM inventory to view the HSM status. If the HSM has been configured correctly, the status for the HSM will be set to **Available** after checking the encryption and decryption logic. If the Status is **Not Available**:
    a. Check the installation path for the HSM.
    b. Ensure that all required permissions have been enabled.
    c. Go to **Logs** > **Logging :: All**. Search with HSM and see the **Log message**.
13. If the implementation type is CSR Generation, refer to the Cert+ User Guide for steps on how to generate a CSR.

Fortanix

Prerequisites

1. The Fortanix HSM device setup should be available.
2. HSM slot initialization and crypto user credential creation should be done.
3. Communication to the hsm and appviewx nodes in the case of and the cloud connector in the case of should be available to integrate with Appviewx.
4. The slot id and partition password from the Fortanix device should be available to use in the appviewx.

- Integrating the Fortanix HSM with the AppViewX Onprem
- Integrating the Fortanix HSM with the AppViewX SaaS

Integrating the Fortanix HSM with the AppViewX Onprem

To integrate the Fortanix HSM with the AppViewX:

1. Login to the AppViewX server on which the AppViewX is installed.
2. From the command line interface, navigate to the properties folder path: **{APPVIEWX_INSTALLATION_PATH}/appviewx_dependencies/properties**
3. Open the **hsm** file using the following command:

```
vi hsm
```

4. Check and confirm if the HSM file has the following lines. If not, uncomment the following lines:

```
export FORTANIX_PKCS11_CONFIG_PATH= /appviewx/dependencies/hsm/fortanix/pkcs11.conf

echo "FORTANIX Config Path : $FORTANIX_PKCS11_CONFIG_PATH"
```

5. If the file is edited, you have to restart the avx-platform-hsm pod, using the following commands:

```
kubectl get pods -n <namespace>

kubectl delete pods -n <namespace> <PodName>
```

6. Login to the AppViewX UI using valid credentials.

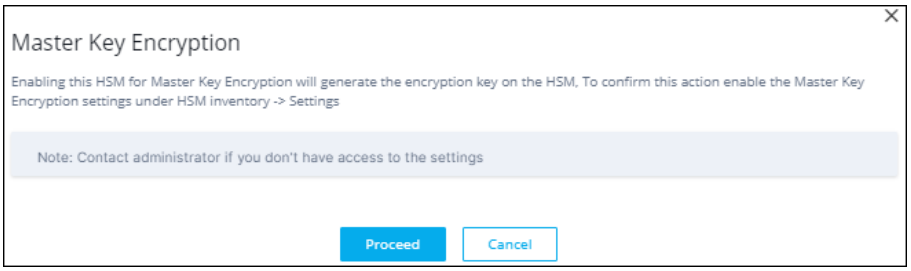
   The **Dashboard** page is displayed by default.

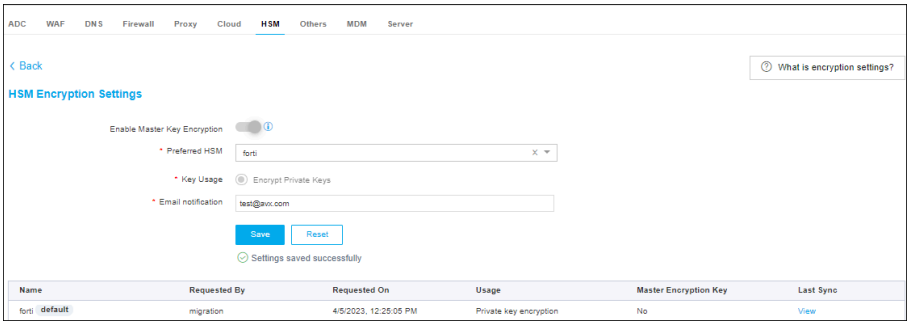
7. On HSM page, click **Add HSM**, from the navigation pane on the left, select **Fortanix**.

   The **HSM > Add** page is updated to display the fields required to integrate Fortanix with the AppViewX.

8. In the **General Information** section, enter/select the following details:

Field descriptions for General Information

Field	Description
***Name**	Enter a name for this integration.
Description	Enter a description for this integration.
Implementation type	Select an implementation type from the following options: • CSR generation • Master key encryption  Click **Proceed**. To confirm this action enable the **Master Key Encryption settings** under **HSM inventory** > **Settings**

Field	Description
	 • Both
***Data center**	Select the required data center from the list of applicable values in the dropdown menu.

Note: The asterisk (*) symbol indicates mandatory fields.

9. In the **Vendor specific details** section, enter/select the following details:

Field descriptions for Vendor specific details

Field	Description
FIPS Mode	Enable the toggle to switch On for FIPS mode.
***API Key**	Unique identification number of the slot in the HSM will be used to communicate with the end HSM device. Enter the API key.
***Key handler name**	A reference name to create a Master Encryption key in HSM. This enables us to pick the right MEK for crypto operations over KEK.
***So file**	The SO file is used to facilitate the communication between the HSM and AppViewX. To upload the .so file: a. Click **Browse**. b. Navigate to the location of the .so file. c. Select the .so file, and click **Open**.

Field	Description
***Config file**	The Config file is used to facilitate the communication between the HSM and AppViewX. To upload the .conf file: a. Click **Browse**. b. Navigate to the location of the .conf file. c. Select the .conf file, and click **Open**.
Note: The asterisk (*) symbol indicates mandatory fields.	

10. Click **Save**.
11. Scroll to the end of this page to view the table or navigate to HSM inventory to view the HSM status. If the HSM has been configured correctly, the status for the HSM will be set to **Available** after checking the encryption and decryption logic. If the Status is **Not Available**:
    a. Check the installation path for the HSM.
    b. Ensure that all required permissions have been enabled.
    c. Go to **Logs** > **Logging :: All**. Search with HSM and see the **Log message**.
12. If the implementation type is CSR Generation, refer to the Cert+ User Guide for steps on how to generate a CSR.

Integrating the Fortanix HSM with the AppViewX SaaS

To integrate the Fortanix HSM with the AppViewX:

1. Login to the AppViewX server on which the Cloud Connector is installed.
2. From the command line interface, navigate to the properties folder path: **{CC_INSTALLATION_PATH}/deps/properties**
3. Open the **hsm** file using the following command:

```
vi hsm
```

4. Check and confirm if the HSM file has the following lines. If not, uncomment the following lines:

```
export FORTANIX_PKCS11_CONFIG_PATH= /appviewx/dependencies/external_libs/hsm/fortanix/pkcs11.conf

echo "FORTANIX Config Path : $FORTANIX_PKCS11_CONFIG_PATH"
```

5. If the file is edited, you have to restart the avx-mid-server-platform pod, using the following commands:

```
kubectl get pods -n <namespace>

kubectl delete pods -n <namespace> <PodName>
```

6. Login to the AppViewX UI using valid credentials.
   The **Dashboard** page is displayed by default.
7. On HSM page, click **Add HSM**, from the navigation pane on the left, select **Fortanix**.
   The **HSM > Add** page is updated to display the fields required to integrate Fortanix with the AppViewX.
8. In the **General Information** section, enter/select the following details:

Field descriptions for General Information

Field	Description
***Name**	Enter a name for this integration.
Description	Enter a description for this integration.
Implementation type	Select an implementation type from the following options: • CSR generation • Master key encryption • Both
***Data center**	Select the required data center from the list of applicable values in the dropdown menu.

Note: The asterisk (*) symbol indicates mandatory fields.

9. In the **Vendor specific details** section, enter/select the following details:

Field descriptions for Vendor specific details

Field	Description
FIPS Mode	Enable the toggle to switch On for FIPS mode.
***API Key**	Unique identification number of the slot in the HSM will be used to communicate with the end HSM device. Enter the API key.
***Key handler name**	A reference name to create a Master Encryption key in HSM. This enables us to pick the right MEK for crypto operations over KEK.
***So file**	The SO file is used to facilitate the communication between the HSM and AppViewX. To upload the .so file: a. Click **Browse**. b. Navigate to the location of the .so file. c. Select the .so file, and click **Open**.

Field	Description
***Config file**	The Config file is used to facilitate the communication between the HSM and AppViewX. To upload the .conf file: a. Click **Browse**. b. Navigate to the location of the .conf file. c. Select the .conf file, and click **Open**.

Note: The asterisk (*) symbol indicates mandatory fields.

10. Click **Save**.
11. Scroll to the end of this page to view the table or navigate to HSM inventory to view the HSM status. If the HSM has been configured correctly, the status for the HSM will be set to **Available** after checking the encryption and decryption logic. If the Status is **Not Available**:
    a. Check the installation path for the HSM.
    b. Ensure that all required permissions have been enabled.
    c. Go to **Logs** > **Logging :: All**. Search with HSM and see the **Log message**.
12. If the implementation type is CSR Generation, refer to the Cert+ User Guide for steps on how to generate a CSR.

Thales TCT

Prerequisites

- Ensure the HSM service/pod is up and running before integrating HSM with Appviewx.
  - If on-prem, use avx_platform_hsm as plugin.
  - If SaaS, use avx_platform_hsm & all Cloud Connector instances for HSM DC.
- Users need to provide both the client and Thales server certificates for agent installation. The installation of the agent and verification of the connection should be carried out by the customer with the assistance of HSM vendors.
- Add server and client certificates to establish a connection between AppViewX and HSM.
- From the AppViewX perspective, appviewx has prepared a sample agent installation guide for Thales. Please refer to it for guidance.

Sample agent installation

To establish communication between the HSM and AppViewX, the installation of the Thales Luna agent is required. The following steps outline the process followed in our lab setup using LunaClient-7.12.0-18.zip.

1. Copy the LunaClient.zip file to the appviewx server and unzip it.
2. Go to LunaClient location

```
cd /LunaClient-7.12.0-18/linux/64
```

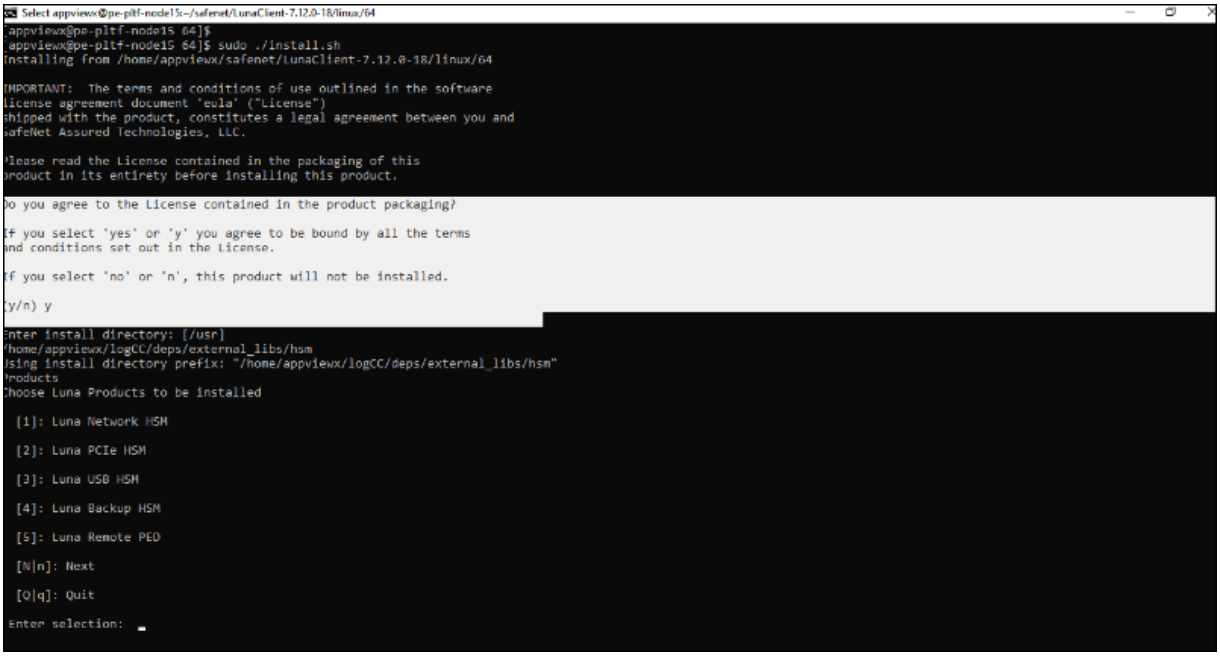
3. Execute the chmod command as shown below:

```
sudo chmod 777 install.sh

sudo chmod 777 common
```

4. Run the install.sh file using the command given below:

```
sudo ./install.sh
```

5. User will be prompted with the following:



Select Y in the prompt

Enter the install directory as - "/usr"

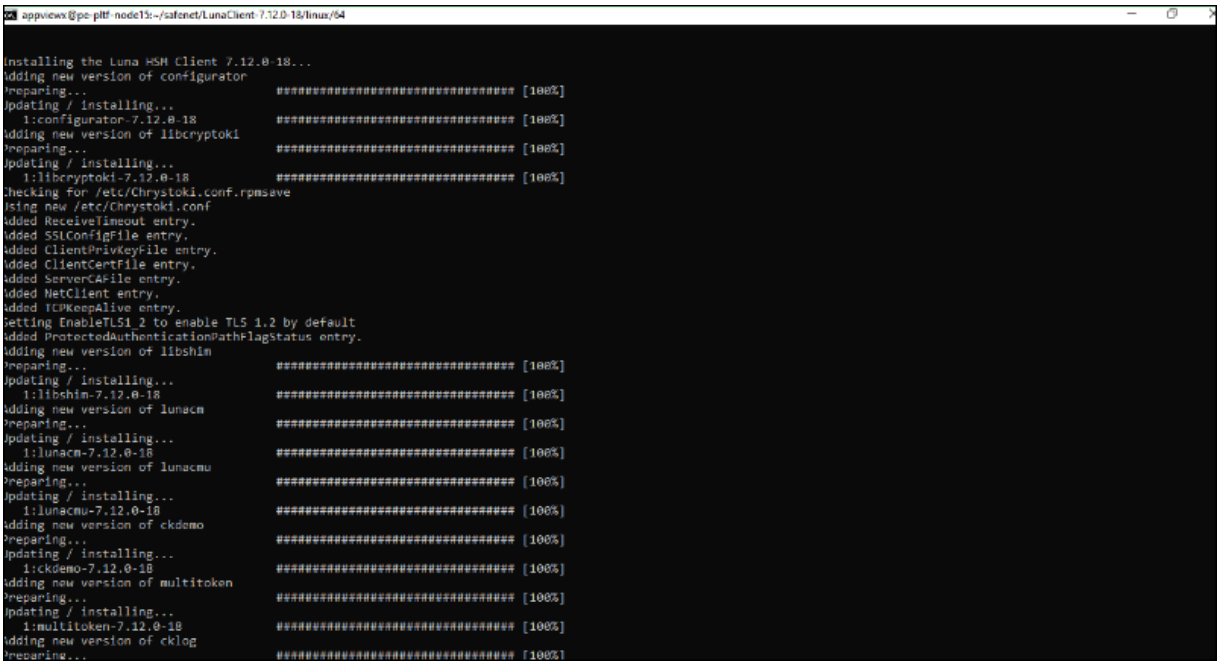
6. Choose Luna Products to be installed, select the Network HSM (Enter 1) and select next (N).

```
Products

Choose Luna Products to be installed
```

```
*[1]: Luna Network HSM

 [2]: Luna PCIe HSM

 [3]: Luna USB HSM

 [4]: Luna Backup HSM

 [5]: Luna Remote PED

 [N|n]: Next

 [Q|q]: Quit

Enter selection:
```

7. Advanced - Choose Luna Components to be installed, select Luna SDK (Enter 1) and select install (I) to install the client.

```
Advanced

Choose Luna Components to be installed

 *[1]: Luna SDK

 [2]: Luna JSP (Java)

 [3]: Luna JCProv (Java)

 [B|b]: Back to Products selection

 [I|i]: Install

 [Q|q]: Quit

Enter selection:  i
```



Installation of the Luna HSM Client 7.12.0-18 completed message should be displayed.

8. Copy server.pem file and place it in the bin directory of the luna client installed path.

```
sudo cp server.pem /usr/safenet/lunaclient/bin
```

9. Register the HSM server certificate with the client using the following command:

```
sudo /usr/safenet/lunaclient/bin/vtl addServer -n <safenet hsm ip> -c server.pem
```

10. Copy the client certificate created to the path.

```
sudo cp <Generated certname>Key.pem <Generated certname>.pem /usr/safenet/lunaclient/cert/client/
```

- HSM Integration with AppViewX - Manual
- HSM Agent Installation and Configuration in AppViewX - Automation

HSM Integration with AppViewX - Manual

To establish communication between the HSM and AppViewX, it is necessary to follow the installation steps provided below.

Installation for onprem

1. Validate the availability of the .so files in the specified path. (libCryptoki2_64.so)

```
<APPVIEWX_INSTALLATION_PATH>/appviewx/hsm/safenet/lunaclient/lib/
```

2. After successful installation, copy the Chrystoki.conf to the below directory from /etc folder

```
On-prem : "cp /etc/Chrystoki.conf  {APPVIEWX_INSTALLATION_PATH}/hsm/"
```

Update the permissions for the Chrystoki.conf file and safenet folder using the command given below:

```
chown appviewx:appviewx Chrystoki.conf

chown -R appviewx:appviewx safenet
```

3. Edit Chrystoki.conf file and replace all custom to mount path.

> **Note:** You have to change in all the places wherever we see local path to mount path.

4. Change local path to mount path

```
LibUNIX =/home/appviewx/hsm/safenet/lunaclient/lib/libCryptoki2.so;
```

to

```
LibUNIX = /appviewx/dependencies/hsm/safenet/lunaclient/lib/libCryptoki2.so;
```

- Verify the certificate names in the Chrystoki.conf file to the ones that were copied manually.
- Update if the names are incorrect and replace them with mount path in all places.
- Save the Chrystoki.conf file.

Installation for SaaS

1. Validate the availability of the .so files in the specified path. (libCryptoki2_64.so)

```
<CC_INSTALLATION_PATH>/deps/external_libs/hsm/safenet/lunaclient/lib/
```

2. After successful installation, copy the Chrystoki.conf to the below directory from /etc folder

```
cp /etc/Chrystoki.conf {CC Installed Path}/deps/external_libs/hsm
```

Update the permissions for the Chrystoki.conf file and safenet folder using the command given below:

```
chown appviewx:appviewx Chrystoki.conf

chown -R appviewx:appviewx safenet
```

3. Edit Chrystoki.conf file and replace all custom to mount path.

> **Note:** You have to change in all the places wherever we see local path to mount path.

4. Change local path to mount path

```
LibUNIX =/home/appviewx/cc/deps/external_libs/hsm/safenet/lunaclient/lib/libCryptoki2.so;
```

to

```
LibUNIX = /appviewx/dependencies/external_libs/hsm/safenet/lunaclient/lib/libCryptoki2.so;
```

- Verify the certificate names in the Chrystoki.conf file to the ones that were copied manually.
- Update if the names are incorrect and replace them with mount path in all places.
- Save the Chrystoki.conf file.

• Integrating the Thales TCT HSM with the AppViewX onprem

• Integrating the Thales TCT HSM with the AppViewX SaaS

Integrating the Thales TCT HSM with the AppViewX onprem

To integrate the Thales TCT HSM with the AppViewX:

1. Login to the AppViewX server on which the AppViewX is installed.
2. From the command line interface, navigate to the properties folder path:
   {APPVIEWX_INSTALLATION_PATH}/appviewx_dependencies/properties
3. Open the hsm file using the following command:

```
vi hsm
```

4. Check and confirm if the HSM file has the following lines. If not, uncomment the following lines:

```
export ChrystokiConfigurationPath=/appviewx/dependencies/hsm/
```

5. If the file is edited, you have to restart the avx-platform-hsm pod, using the following commands:

```
kubectl get pods -n <namespace>

kubectl delete pods -n <namespace> <PodName>
```

6. AppViewX can now communicate with HSM devices.

Integrating the Thales TCT HSM with the AppViewX SaaS

To integrate the Thales TCT HSM with the AppViewX:

1. Login to the AppViewX server on which the Cloud Connector is installed.
2. From the command line interface, navigate to the properties folder path:
   {CC_INSTALLATION_PATH}/deps/properties
3. Open the **hsm** file using the following command:

```
vi hsm
```

4. Check and confirm if the HSM file has the following lines. If not, uncomment the following lines:

```
export ChrystokiConfigurationPath=/appviewx/dependencies/external_libs/hsm/
```

5. If the file is edited, you have to restart the avx-mid-server-platform pod, using the following commands:

```
kubectl get pods -n <namespace>

kubectl delete pods -n <namespace> <PodName>
```

6. AppViewX can now communicate with HSM devices.

HSM Agent Installation and Configuration in AppViewX - Automation

To avoid above steps of "Sample Agent Installation - Manual" section, appviewx has introduced an automation script that streamlines the installation of the Thales agent and its configuration with AppViewX.

Automation script for onprem

1. Go to the path /home/appviewx/appviewx_kubernetes/yaml/appviewx_plugins/avx_platform_hsm/hsm.
2. Ensure the availability of the following files:
   - avx_hsm_integration.sh
   - thales_safenet_hsm_configuration.sh
3. Run the command "chmod 777 *" or apply "chmod" specifically for avx_hsm-integration.sh and the required HSM agent.
4. Execute "sudo ./avx_hsm_integration.sh".
5. Choose the required HSM to configure and select the "Configure" option.
6. Proceed with the subsequent steps using the script.

Automation script for SaaS

1. Go to the path <cloud connector installed path>/deps/utils/avx-platform-hsm.
2. Ensure the availability of the following files:
   - hsm-integration.sh
   - safenet_config.sh
3. Run the command "chmod 777 *" or apply "chmod" specifically for hsm-integration.sh and the required HSM agent.
4. Execute "sudo ./hsm-integration.sh".
5. Choose the required HSM to configure and select the "Configure" option.
6. Proceed with the subsequent steps using the script.

Thales DPoD

Prerequisites

- Ensure the HSM service/pod is up and running before integrating HSM with Appviewx.
  - If on-prem, use avx_platform_hsm as plugin
  - If SaaS, use avx_platform_hsm & all Cloud Connector instances for HSM DC.
- DPOD client package to be downloaded and copied in the appviewx node where HSM connection is to be established.
- Connectivity for the DPOD URL to be established.
- HSM slot and PIN should be available for communication.

Sample agent installation

The following steps outline the process followed in installing the DPOD Client Package.

1. Go to the hsm folder for Path: **{APPVIEWX_INSTALLATION_PATH}/hsm/** and for Path: **{CC_INSTALLATION_PATH}/deps/external_libs/hsm/**.
2. Create a new folder as a safenet.
3. Untar the **DPoD** tar file inside safenet folder.
4. Once extracted inside the safenet, make sure a new folder, dpod, is created and all the extracted files are present.

> **Note:** From the extracted client package, if the dpod folder is not present, please create a folder named dpod inside the safenet and then extract the files.

5. Untar the **cvclient-min.tar** file.

• HSM Integration with AppViewX - Manual

• HSM Agent Installation and Configuration in AppViewX - Automation

HSM Integration with AppViewX - Manual

To establish communication between the HSM and AppViewX, it is necessary to follow the installation steps provided below.

1. Go to the hsm folder for path : **{APPVIEWX_INSTALLATION_PATH}/hsm/safenet/dpod/** and : **{CC_INSTALLATION_PATH}/deps/external_libs/hsm/safenet/dpod**.
2. Provide chmod 755 permission to the Chrystoki.conf file.
3. Edit the Chrystoki.conf file to replace the custom path with the above specified mount path.
4. Change the path value in the Chrystoki.conf file to match the mount.

   Check the .so file location mentioned in Chrystoki.conf file LibUNIX64 = ./libs/64/libCryptoki2.so

   Replace the dot with mount path for as **/appviewx/dependencies/hsm/safenet/dpod/**

   Sample: /appviewx/dependencies/hsm/safenet/dpod/libs/64/libCryptoki2.so

   Replace the dot with mount path for as **/appviewx/dependencies/external_libs/hsm/safenet/dpod/**

   Sample: /appviewx/dependencies/external_libs/hsm/safenet/dpod/libs/64/libCryptoki2.so
5. Update the **Chrystoki.conf** file by modifying all instances where the path is specified.

6. From the command line interface, navigate to the properties folder path.
   - For : **{AppViewX_INSTALLATION_PATH}/appviewx_dependencies/properties**
   - For : **<Cloud connector installed path >/deps/properties**.
7. Open the **hsm** file, using the following command:

```
vi hsm
```

8. Check and confirm if the HSM file has the following lines.
   - For :

```
cd /appviewx/dependencies/hsm/safenet/dpod/

source setenv
```

   - For :

```
cd /appviewx/dependencies/external_libs/hsm/safenet/dpod/

source setenv
```

9. Uncomment all the above lines if commented, and save the file for .
10. Add the below command for and then save the file.

```
export ChrystokiConfigurationPath=/appviewx/dependencies/external_libs/hsm/safenet/dpod/
```

```
# ====== Gemalto / thales - DPOD ====== #
cd /appviewx/dependencies/external_libs/hsm/safenet/dpod/
source setenv
export ChrystokiConfigurationPath=/appviewx/dependencies/hsm/safenet/dpod/

# ====== Gemalto / thales - GPN ====== #
#export ChrystokiConfigurationPath=/appviewx/dependencies/external_libs/hsm/

# ====== Utimaco config file variable  ====== #
export CS_PKCS11_R2_CFG=/appviewx/dependencies/external_libs/hsm/utimaco/cs_pkcs11_R2.cfg
echo "UTIMACO Config Path : $CS_PKCS11_R2_CFG"

# ====== fortanix config file variable  ====== #
export FORTANIX_PKCS11_CONFIG_PATH=/appviewx/dependencies/external_libs/hsm/fortanix/pkcs11.conf
echo "FORTANIX Config Path : $FORTANIX_PKCS11_CONFIG_PATH"
```

11. Restart the **avx-platform-hsm** pod for , and **avx-mid-server-platform** pod for , using the following commands:

```
kubectl get pods -n <namespace>

kubectl delete pods -n <namespace> <PodName>
```

12. AppViewX can now communicate with HSM devices.

- Integrating the Thales GPN HSM with the AppViewX onprem
- Integrating the Thales GPN HSM with the AppViewX SaaS

HSM Agent Installation and Configuration in AppViewX - Automation

To avoid above steps of "Sample Agent Installation - Manual" section, we have introduced an automation script that streamlines the installation of the Thales agent and its configuration with AppViewX.

Automation script for onprem

1. Go to the path /home/appviewx/appviewx_kubernetes/yaml/appviewx_plugins/avx_platform_hsm/hsm.
2. Ensure the availability of the following files:
   - avx_hsm_integration.sh
   - thales_dpod_hsm_configuration.sh
3. Run the command "chmod 777 *" or apply "chmod" specifically for avx_hsm-integration.sh and the required HSM agent.
4. Execute "sudo ./avx_hsm_integration.sh".
5. Choose the required HSM to configure and select the "Configure" option.
6. Proceed with the subsequent steps using the script.

Automation script for SaaS

1. Go to the path <cloud connector installed path>/deps/utils/avx-platform-hsm.
2. Ensure the availability of the following files:
   - hsm-integration.sh
   - dpod_config.sh
3. Run the command "chmod 777 *" or apply "chmod" specifically for hsm-integration.sh and the required HSM agent.
4. Execute "sudo ./hsm-integration.sh".
5. Choose the required HSM to configure and select the "Configure" option.
6. Proceed with the subsequent steps using the script.

Thales GPN

Prerequisites

- Ensure the HSM service/pod is up and running before integrating HSM with Appviewx.
  - If on-prem, use avx_platform_hsm as plugin
  - If SaaS, use avx_platform_hsm & all Cloud Connector instances for HSM DC.
- The Alien and RPM packages should be installed in the environment.
- Environment should be able to communicate with the HSM.
- Users should have either root access or sudo access.
- HSM slot and PIN should be available to establish a connection between AppViewX and HSM.
- From the AppViewX perspective, appviewx has prepared a sample agent installation guide for Thales. Please refer to it for guidance.

Sample agent installation

To establish communication between the HSM and AppViewX, the installation of the Thales Luna agent is required. The following steps outline the process followed in our lab setup using LunaClient-7.12.0-18.zip.

1. Copy the LunaClient.zip file to the appviewx server and unzip it.
2. Go to LunaClient location

```
cd <untarred Luna-client-path>/64/
```

3. Execute the chmod command as shown below:

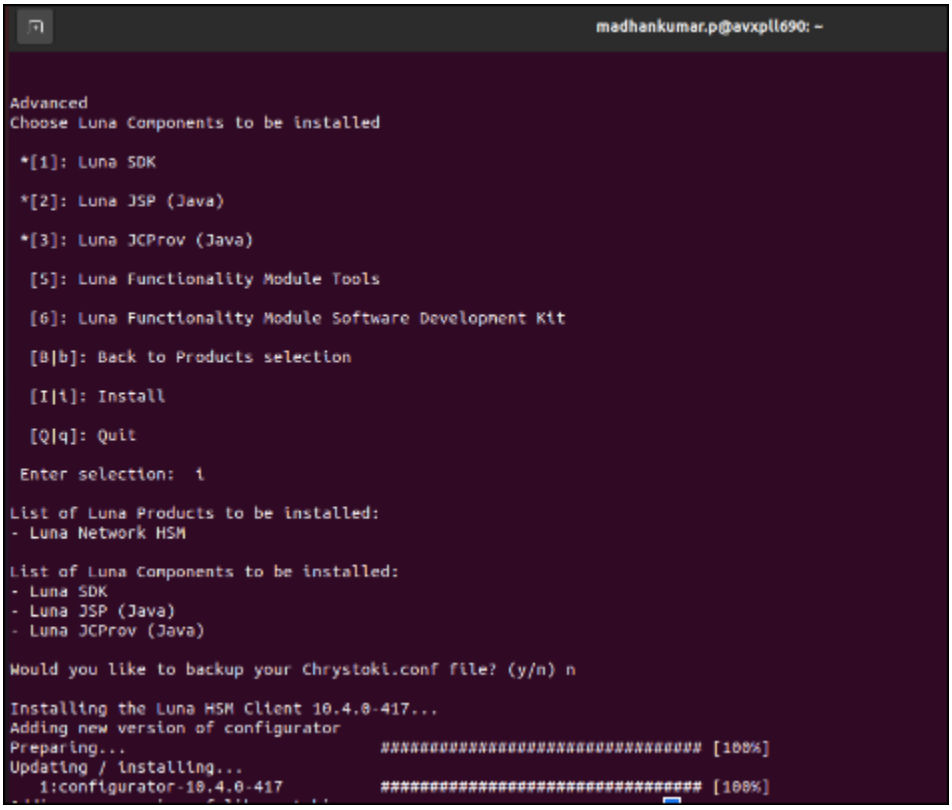
```
sudo chmod 755 install.sh

sudo chmod 755 common
```

4. Run the install.sh file using the command given below:

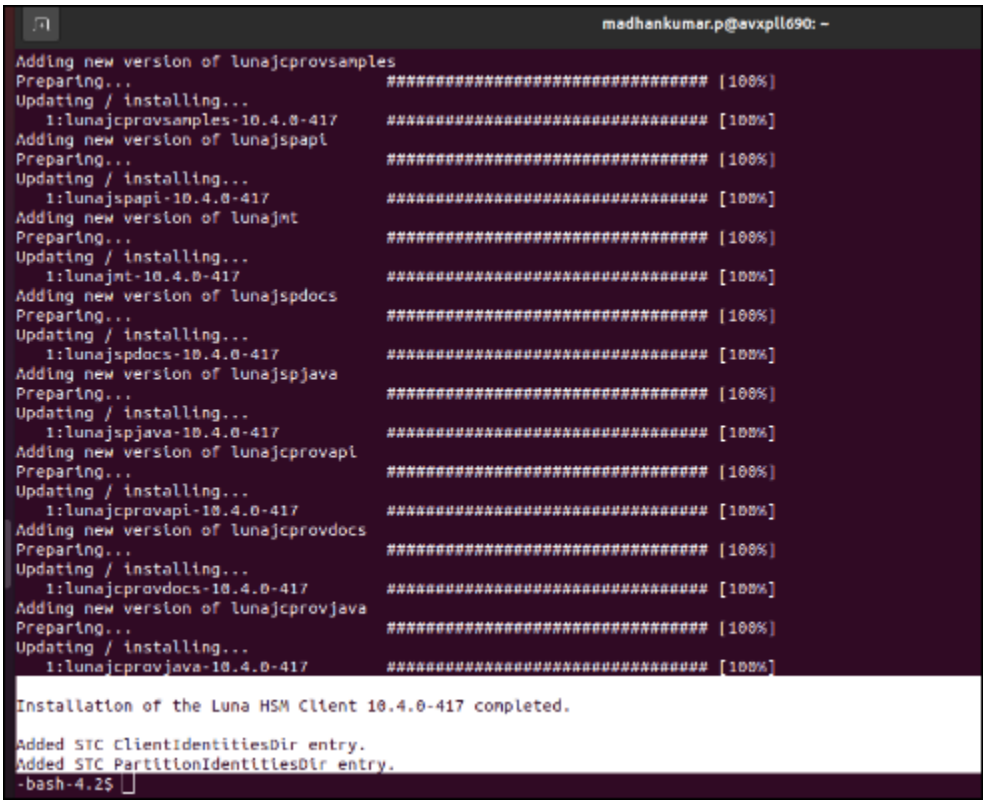
```
sudo ./install.sh
```

5. When directed, as input for Enter install directory: [/usr], enter the following custom path: **<APPVIEWX_INSTALLATION_PATH >/appviewx/hsm**
6. When directed, as input for Enter install directory: [/usr], enter the following custom path: **<CC_INSTALLATION_PATH>/deps/external_libs/hsm**
7. When prompted to choose the Luna products to be installed, select Luna Network HSM and enter next (n).
8. When prompted to choose the Luna components to be installed, choose the following packages:
   a. Luna Software Development Kit (SDK)
   b. Luna JSP (Java)
   c. Luna JCProv (Java)
   d. Crypto Command Center Provisioning Client (Not applicable for Luna client v7.2)

To select a Luna component, Enter the number marked against it and press **Enter**. To select multiple Luna components, repeat the above step. Once the required components are selected, enter (I/i) and press enter to initiate the installation process.



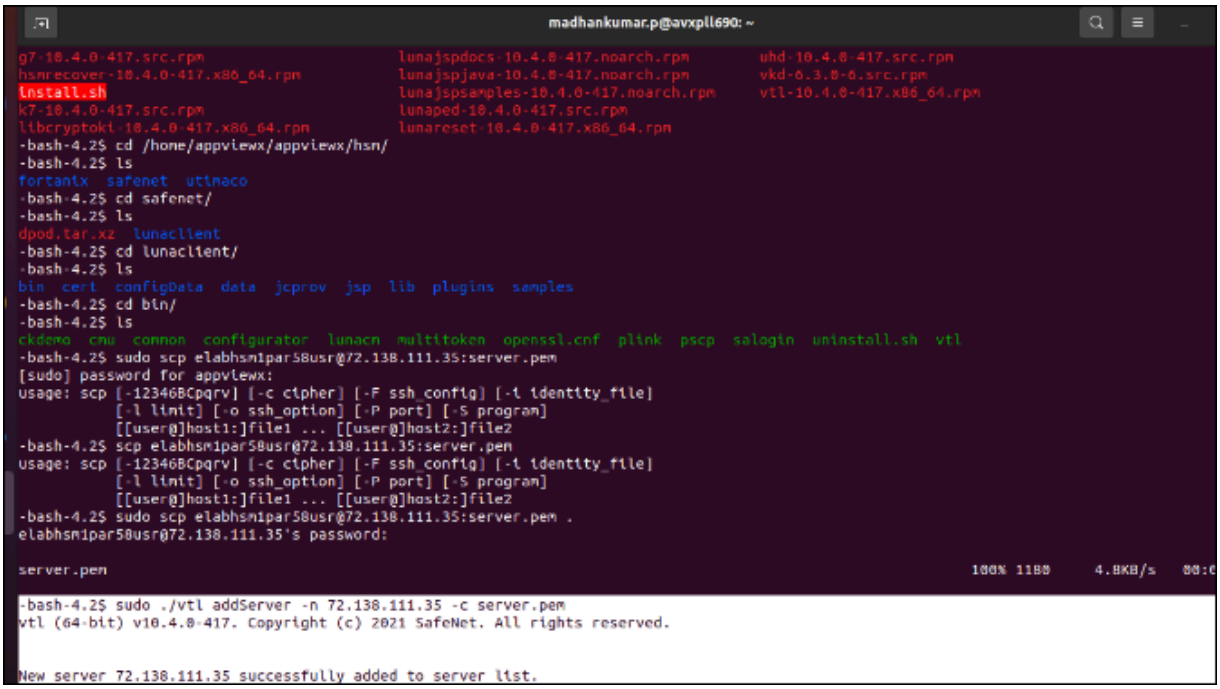
Once the Luna client is installed successfully, you will get the following message in the terminal:



9. After installing the Luna client, navigate to the directory in which the Luna client is installed. path: **<APPVIEWX_INSTALLATION_PATH>/appviewx/hsm/safent/lunaclient/bin**
10. After installing the Luna client, navigate to the directory in which the Luna client is installed. path: **<CC_INSTALLATION_PATH>/deps/external_libs/hsm/safenet/lunaclient/bin**
11. This is a sample HSM device IP, and it will vary according to the IP of the HSM in the customer environment.
12. Import the server certificate of the HSM device to the Luna client using the following command: **sudo scp <username>@<HSM device IP>:server.pem**

> **Note:** Sample value mentioned above are Host IP: **<HSM device IP>** of HSM, Client credentials of HSM device is - **<username>**

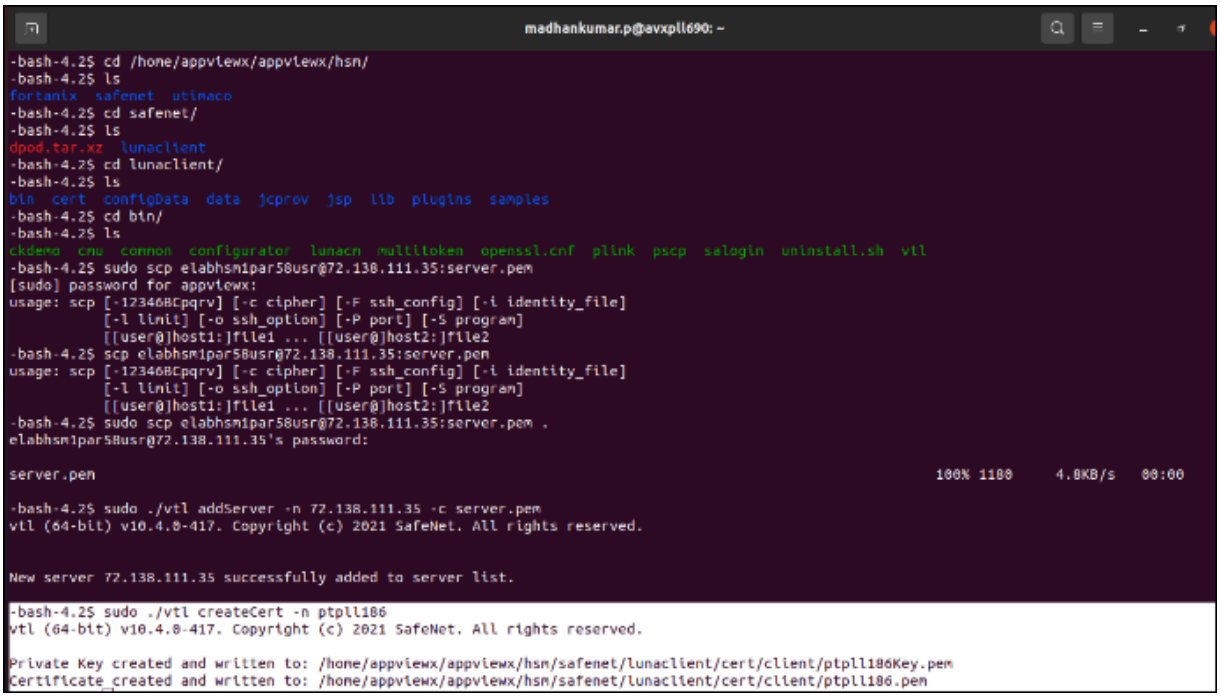
After successfully adding the server, you will get the message as follows:



13. Register the HSM server certificate with the client using the following command: **sudo ./vtl addServer -n <HSM Device IP> -c server.pem**
14. Create a client certificate in the node from which we are trying to communicate with the HSM (AppViewX): **sudo ./vtl createCert -n <hostname of node>**

> **Note:** Sample value **<hostname of node>** here is client certificate name.

After the certificates are created, you will get the output as follows:

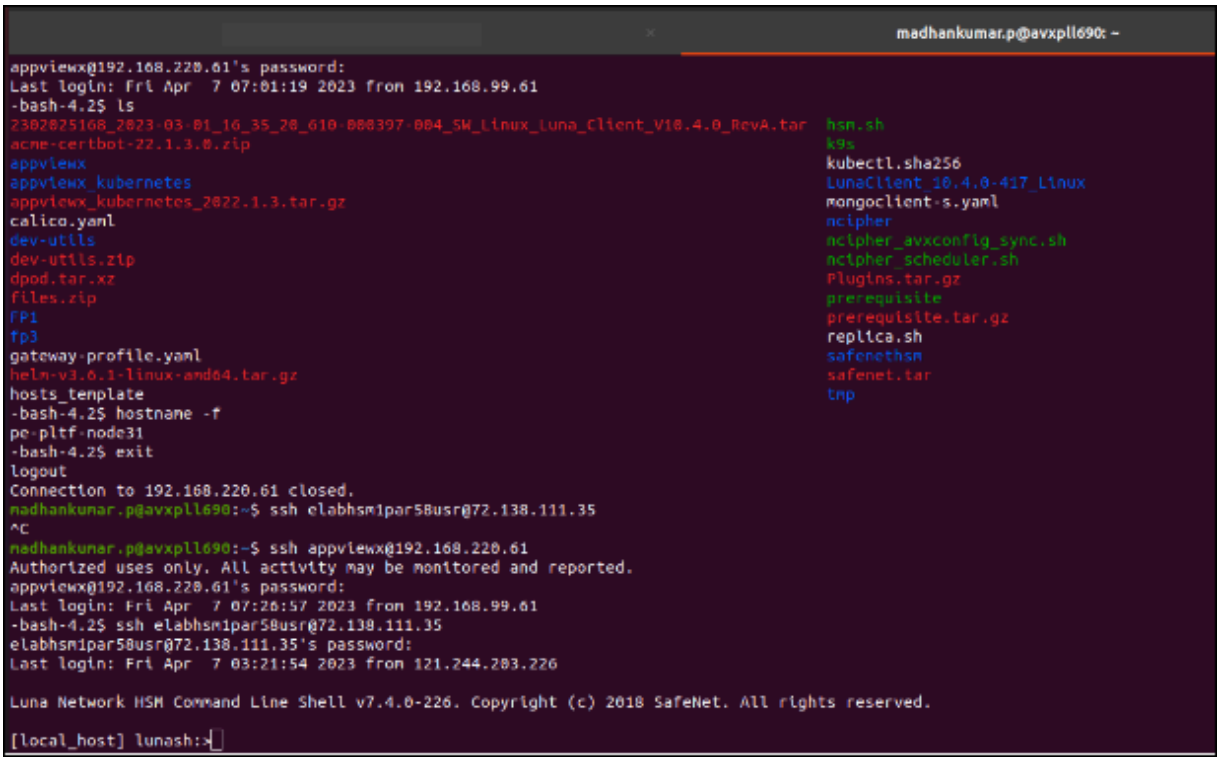


15. Export the Client certificate to the node where the HSM is to be configured:

```
sudo scp /usr/safenet/lunaclient/cert/client/ptpll186.pem <username>@<HSM device IP>:
```

Use the certificate created and written to the path obtained from the previous step, as shown in the screenshot in the scp command.

After logging into the HSM, the prompt will appear as below:



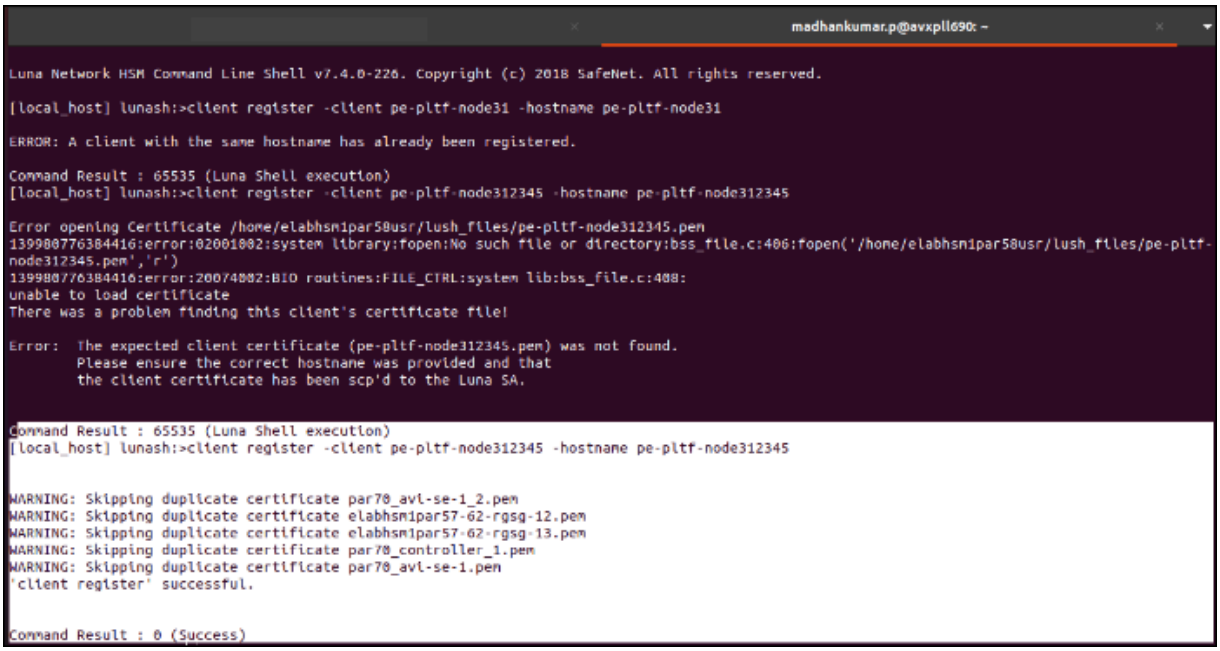
16. Register the client certificate on the HSM Machine.

    (This command to be run in HSM device using SSH login.)

```
client register -client <hostname> -hostname <hostname>
```

> **Note: *hostname** - Is the node from where you are trying to communicate with the HSM.

After registering the client certificate, you will get the following output at the command prompt:

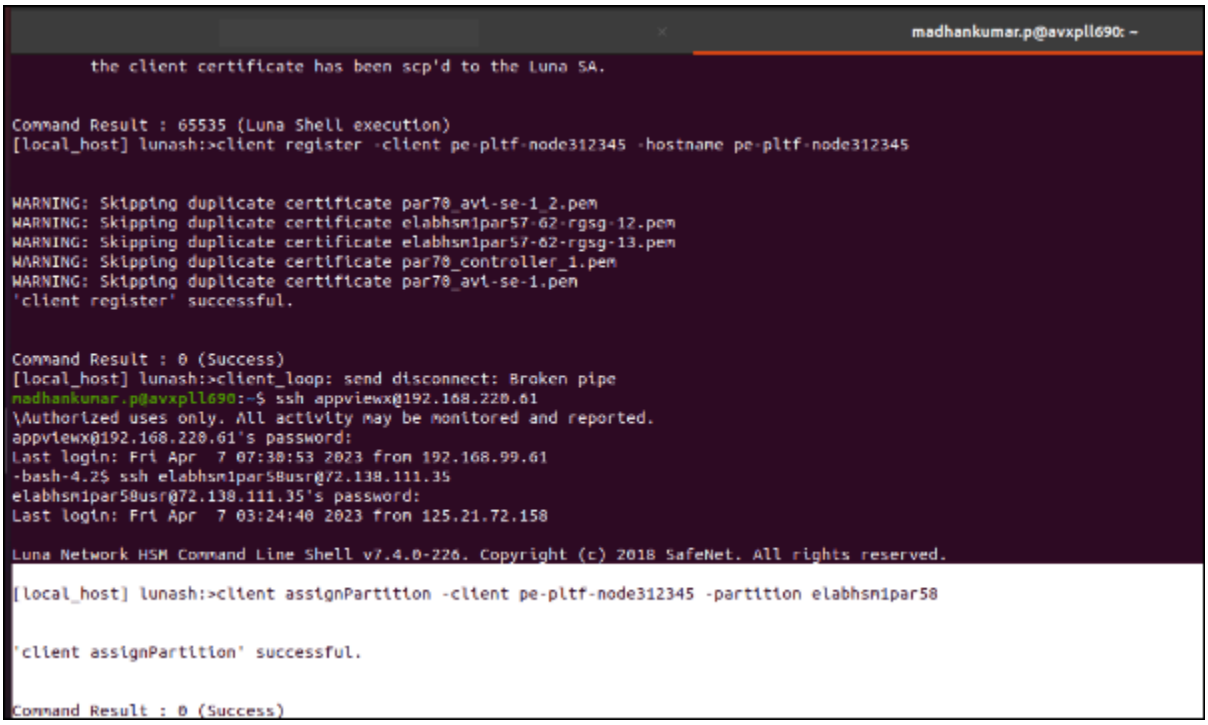


17. Assign the client to a partition using the following command:

    (This command to be run in HSM device using SSH login.)

    ```
    client assignPartition -client <host name of node trying to connect> -partition <Partition name of the hsm device>
    ```

    After assigning the client partition, the output will be as follows:



HSM Integration with AppViewX - Manual

To establish communication between the HSM and AppViewX, it is necessary to follow the installation steps provided below.

1. Go to the hsm folder for path : **{APPVIEWX_INSTALLATION_PATH}/hsm/safenet/dpod/** and : **{CC_INSTALLATION_PATH}/deps/external_libs/hsm/safenet/dpod**.
2. Provide chmod 755 permission to the Chrystoki.conf file.
3. Edit the Chrystoki.conf file to replace the custom path with the above specified mount path.
4. Change the path value in the Chrystoki.conf file to match the mount.

   Check the .so file location mentioned in Chrystoki.conf file LibUNIX64 = ./libs/64/libCryptoki2.so

   Replace the dot with mount path for as **/appviewx/dependencies/hsm/safenet/dpod/**

   Sample: /appviewx/dependencies/hsm/safenet/dpod/libs/64/libCryptoki2.so

   Replace the dot with mount path for as **/appviewx/dependencies/external_libs/hsm/safenet/dpod/**

   Sample: /appviewx/dependencies/external_libs/hsm/safenet/dpod/libs/64/libCryptoki2.so
5. Update the **Chrystoki.conf** file by modifying all instances where the path is specified.
6. From the command line interface, navigate to the properties folder path.
   - For : **{AppViewX_INSTALLATION_PATH}/appviewx_dependencies/properties**
   - For : **<Cloud connector installed path >/deps/properties**.
7. Open the **hsm** file, using the following command:

   ```
   vi hsm
   ```

8. Check and confirm if the HSM file has the following lines.
   - For :

   ```
   cd /appviewx/dependencies/hsm/safenet/dpod/

   source setenv
   ```

- For :

```
cd /appviewx/dependencies/external_libs/hsm/safenet/dpod/

source setenv
```

9. Uncomment all the above lines if commented, and save the file for .
10. Add the below command for and then save the file.

```
export ChrystokiConfigurationPath=/appviewx/dependencies/external_libs/hsm/safenet/dpod/
```

```
# ====== Gemalto / thales - DPOD ====== #
cd /appviewx/dependencies/external_libs/hsm/safenet/dpod/
source setenv
export ChrystokiConfigurationPath=/appviewx/dependencies/hsm/safenet/dpod/

# ====== Gemalto / thales - GPN ====== #
#export ChrystokiConfigurationPath=/appviewx/dependencies/external_libs/hsm/

# ====== Utimaco config file variable  ====== #
export CS_PKCS11_R2_CFG=/appviewx/dependencies/external_libs/hsm/utimaco/cs_pkcs11_R2.cfg
echo "UTIMACO Config Path : $CS_PKCS11_R2_CFG"

# ====== fortanix config file variable  ====== #
export FORTANIX_PKCS11_CONFIG_PATH=/appviewx/dependencies/external_libs/hsm/fortanix/pkcs11.conf
echo "FORTANIX Config Path : $FORTANIX_PKCS11_CONFIG_PATH"
```

11. Restart the **avx-platform-hsm** pod for , and **avx-mid-server-platform** pod for , using the following commands:

```
kubectl get pods -n <namespace>

kubectl delete pods -n <namespace> <PodName>
```

12. AppViewX can now communicate with HSM devices.

- Integrating the Thales GPN HSM with the AppViewX onprem
- Integrating the Thales GPN HSM with the AppViewX SaaS

Integrating the Thales GPN HSM with the AppViewX onprem

To integrate the Thales GPN HSM with the AppViewX:

1. Login to the AppViewX server on which the AppViewX is installed.
2. From the command line interface, navigate to the properties folder path: **{APPVIEWX_INSTALLATION_PATH}/appviewx_dependencies/properties**
3. Open the **hsm** file, using the following command:

```
vi hsm
```

4. Check and confirm if the HSM file has the following lines. If not, uncomment the following lines:

```
export ChrystokiConfigurationPath=/appviewx/dependencies/hsm/
```

> **Note:** The given path is only for reference, if there is change in the installed path the same has to be updated in the above commands.

5. If the file is edited, you have to restart the avx-platform-hsm pod, using the following commands:

```
kubectl get pods -n <namespace>

kubectl delete pods -n <namespace> <PodName>
```

6. AppViewX can now communicate with HSM devices.

Integrating the Thales GPN HSM with the AppViewX SaaS

To integrate the Thales GPN HSM with the AppViewX:

1. Login to the AppViewX server on which the Cloud Connector is installed.
2. From the command line interface, navigate to the properties folder path: **{CC_INSTALLATION_PATH}/deps/properties**
3. Open the **hsm** file using the following command:

```
vi hsm
```

4. Check and confirm if the HSM file has the following lines. If not, uncomment the following lines:

```
export ChrystokiConfigurationPath=/appviewx/dependencies/external_libs/hsm/
```

> **Note:** The given path is only for reference, if there is change in the installed path the same has to be updated in the above commands.

5. If the file is edited, you have to restart the avx-mid-server-platform pod, using the following commands:

```
kubectl get pods -n <namespace>

kubectl delete pods -n <namespace> <PodName>
```

6. AppViewX can now communicate with HSM devices.

HSM Configuration in AppViewX - Automation

To streamline the integration of HSM with AppViewX, we've introduced an automation script for configuration. (Make sure that the Thales agent is manually installed).

Automation script for onprem

1. Go to the path /home/appviewx/appviewx_kubernetes/yaml/appviewx_plugins/avx_platform_hsm/hsm.
2. Ensure the availability of the following files:
   - avx_hsm_integration.sh
   - thales_gpn_hsm_configuration.sh
3. Run the command "chmod 777 *" or apply "chmod" specifically for avx_hsm-integration.sh and the required HSM agent.
4. Execute "sudo ./avx_hsm_integration.sh".
5. Choose the required HSM to configure and select the "Configure" option.
6. Proceed with the subsequent steps using the script.

Automation script for SaaS

1. Go to the path <cloud connector installed path>/deps/utils/avx-platform-hsm.
2. Ensure the availability of the following files:
   - hsm-integration.sh
   - gpn_config.sh
3. Run the command "chmod 777 *" or apply "chmod" specifically for hsm-integration.sh and the required HSM agent.
4. Execute "sudo ./hsm-integration.sh".
5. Choose the required HSM to configure and select the "Configure" option.
6. Proceed with the subsequent steps using the script.

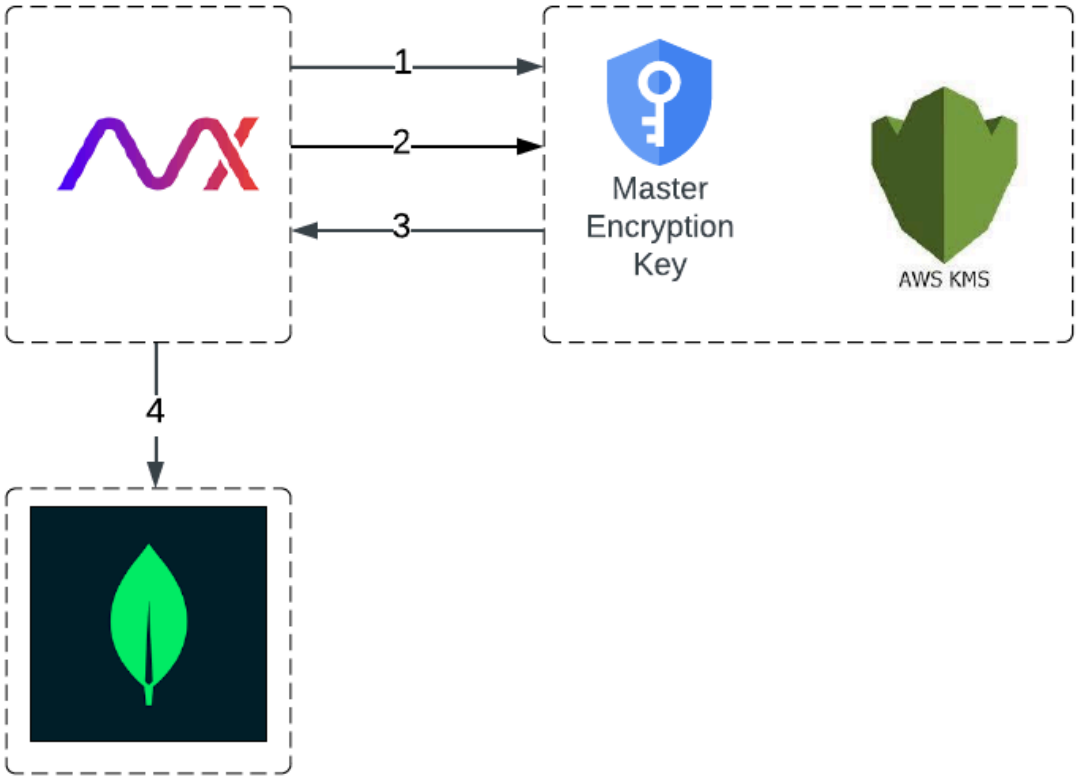
Managing Master Encryption Key

AppViewX employs an envelope encryption technique to protect all sensitive information, using the AWS Key Management Service (KMS) keys. This process involves encrypting plaintext data using an encryption key, called the AppViewX Master Encryption Key (MEK). The AppViewX MEK is encrypted with a Master Encryption Key (KMS-MEK) maintained in the AWS KMS when storing it at rest or during transit. User's can choose to encrypt the AppViewX MEK with an encryption key stored in their HSM. This encryption key is the user’s Master Encryption Key. As a result, the AppViewX MEK used to encrypt secure materials is encrypted twice; first, using the Master Key stored in KMS, and then using the user’s

Master Key stored in the HSM. If the user's Master Key is removed from the HSM, the AppViewX MEK cannot be used to access the data, making it inaccessible and irrecoverable.

Generating the User's Master Encryption Key

The user's Master Encryption key generation process is initiated after they have been successfully onboarded. The following is a graphical representation of the key generation process is outlined in the image:



1. Upon the onboarding of a tenant, AppViewX initiates a request to AWS KMS to generate a Master Encryption Key (KMS-MEK) and a Data Encryption Key for the tenant.

   AppViewX refers to this Data Encryption Key as its internal Master Encryption Key and utilizes it to encrypt all sensitive information.

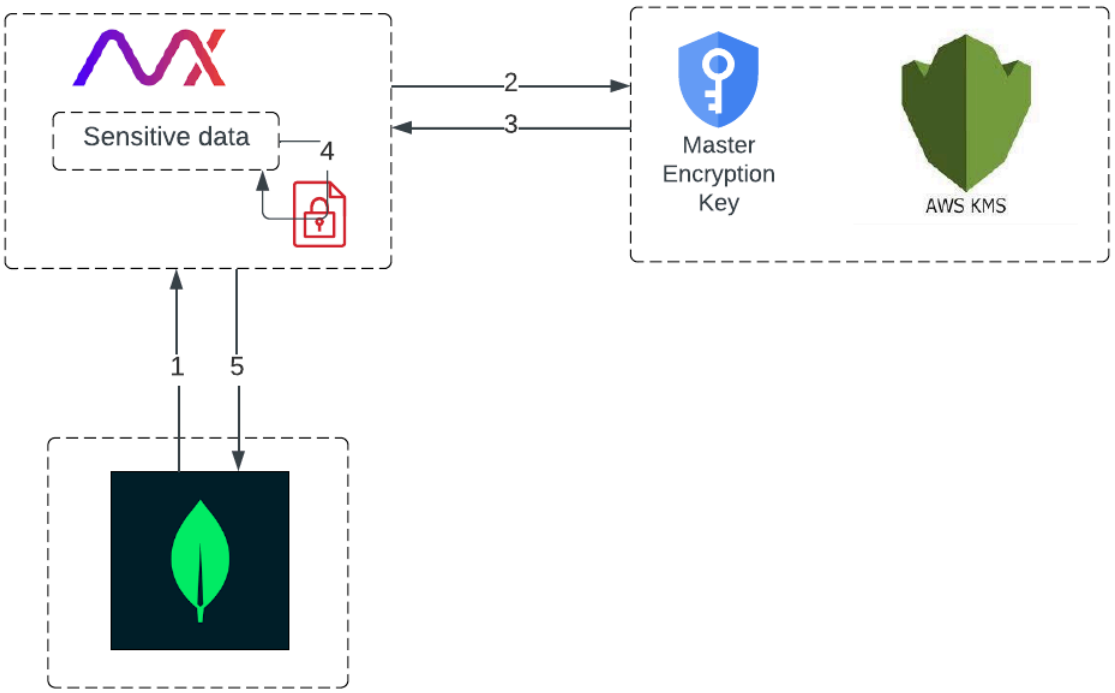
2. AWS KMS generates the AppViewX MEK and encrypts it using the KMS-MEK stored in KMS.
3. AWS KMS returns the encrypted AppViewX MEK.
4. The encrypted AppViewX MEK is stored in the tenant's database.

   All encryption and decryption processes take place within AppViewX, and the key used for these operations is supplied by AWS KMS.

> **Note:** It is important to note that the AWS KMS generates the Master Encryption Keys (KMS-MEK, AppViewX MEK) for each tenant. The tenant's database (in which the encrypted AppViewX MEK is securely stored) is encrypted at rest for added security.

Encrypting Data Using the AppViewX MEK

To ensure the protection of sensitive data, it should be encrypted. To securely encrypt the data, AppViewX executes the following steps:



1. Retrieve the encrypted MEK from the in-memory cache.

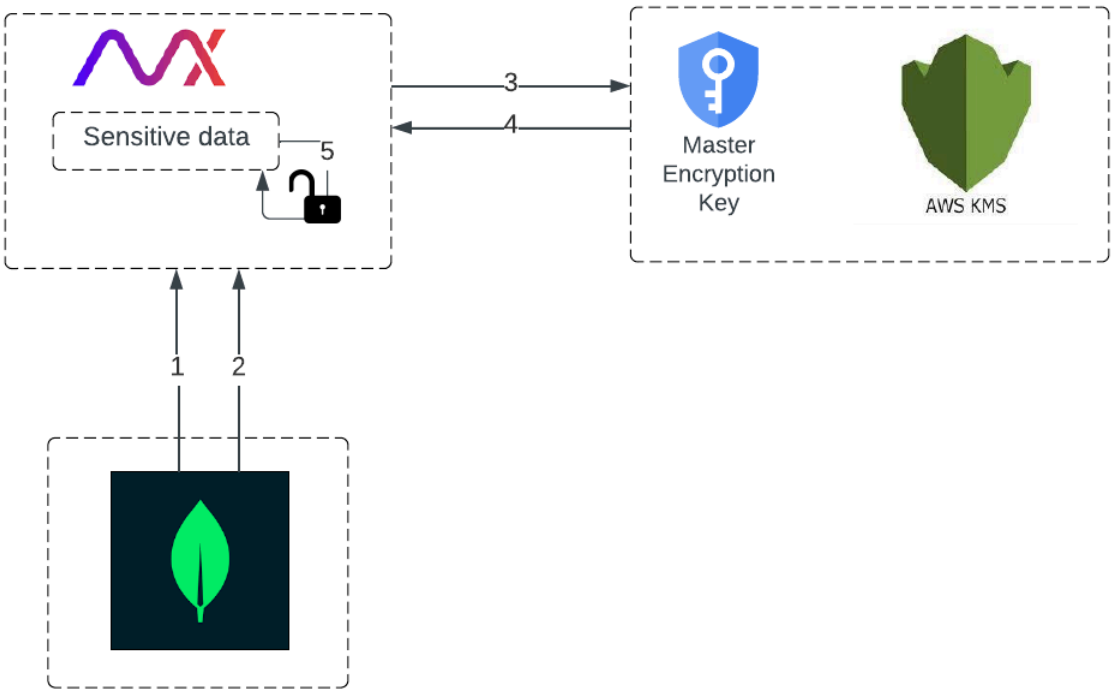
   If the AppViewX Master Encryption Key (MEK) necessary for encryption is not yet available in the in-memory cache, it is retrieved from the tenant's database.

2. Send a request to the AWS KMS to decrypt the MEK.
3. Retrieve the decrypted plaintext AppViewX MEK and cache it in memory.
4. Encrypt sensitive data using AppViewX MEK.
5. Once the plaintext MEK has been retrieved, store it in memory for future sensitive data encryptions.

   This helps to improve performance by reducing the number of calls to AWS KMS for each encryption/ decryption request.

Decrypting Data Using the AppViewX MEK

To decrypt the sensitive information stored in the tenant database, AppViewX executes the following steps:



1. Retrieve the encrypted sensitive data (ciphertext).

   This ciphertext can only be decrypted using the AppViewX Master Encryption Key (MEK).

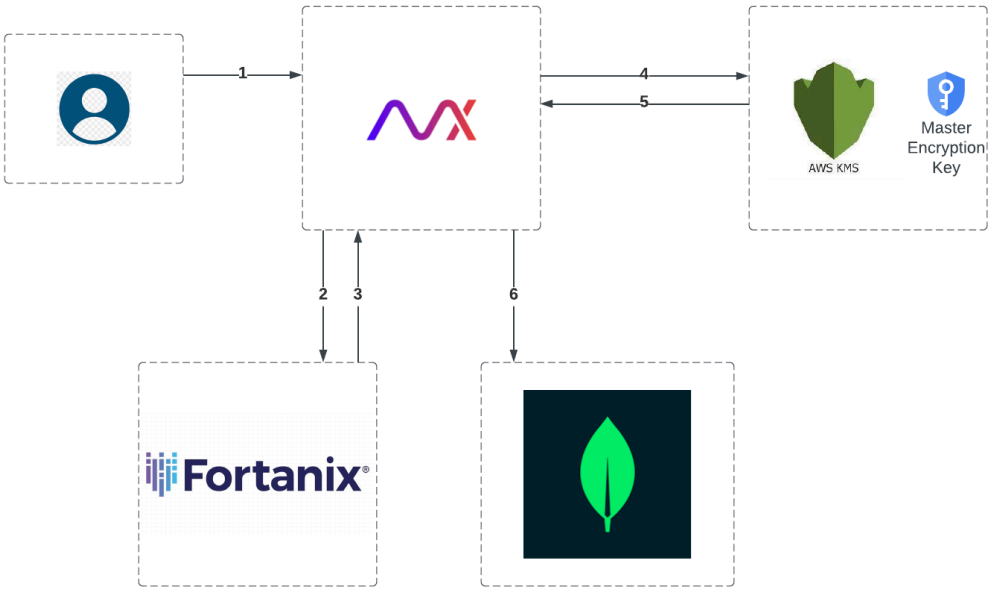
2. Retrieve the encrypted AppViewX MEK from the in-memory cache.

   If the plaintext AppViewX MEK is unavailable in memory, it is retrieved from the tenant database.

3. Initiate a request to AWS KMS to decrypt the encrypted MEK.
4. Retrieve the plaintext MEK from the AWS KMS.
5. Decrypt the sensitive data using this plaintext MEK.

Setting up the HSM to Facilitate using the AppViewX MEK

To facilitate the encryption of the AppViewX Master Key with the User's Master Key, AppViewX executes the following steps:



1. Set up an HSM.

   Note: For instructions on setting up the HSM, click here.

2. After successful configuration of the HSM in AppViewX, conduct a health check on the HSM through the Cloud Connector to verify the configuration's validity.
3. If the configuration is valid, add the HSM to AppViewX.

   AppViewX receives success response from the HSM.

4. Encrypt the secure material required for communication with HSM (API Key, partition password, and so on.) using the KMS-MEK instead of the standard AppViewX MEK.

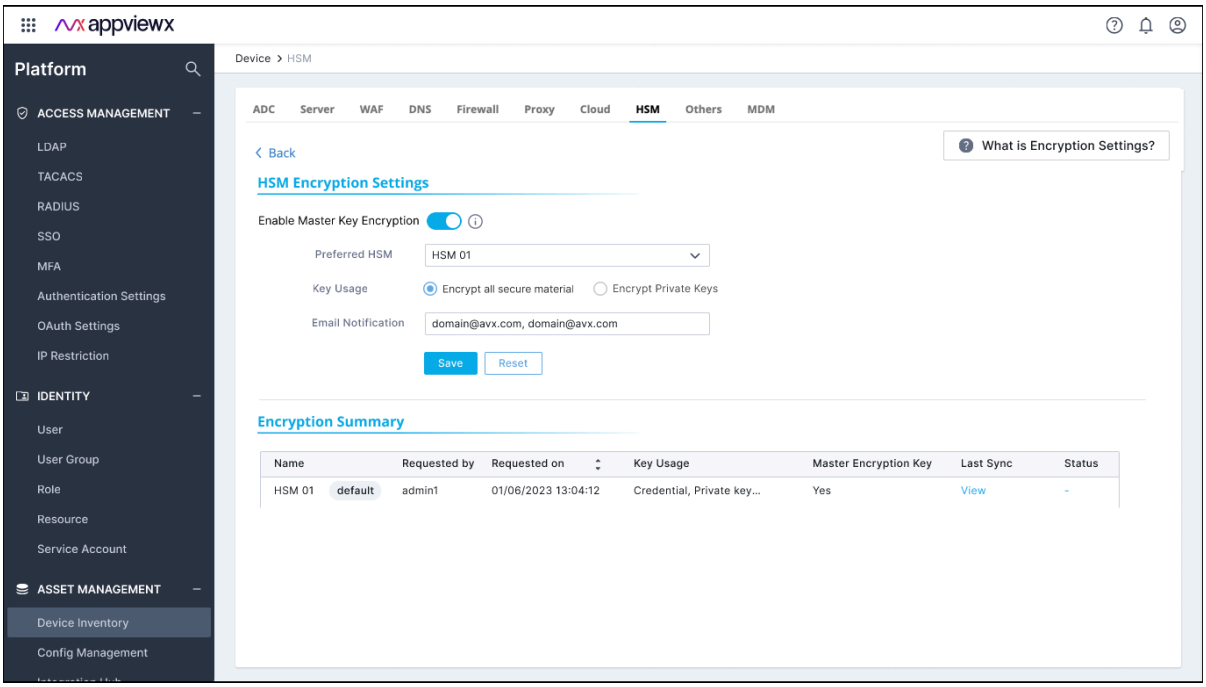
   This deviation is to allow for the encryption of the AppViewX MEK using the User's Master Key stored in the HSM.

5. Retrieve the Encrypted HSM Password/API Key from AWS KMS.
6. Persist the HSM Settings in the tenant’s database.

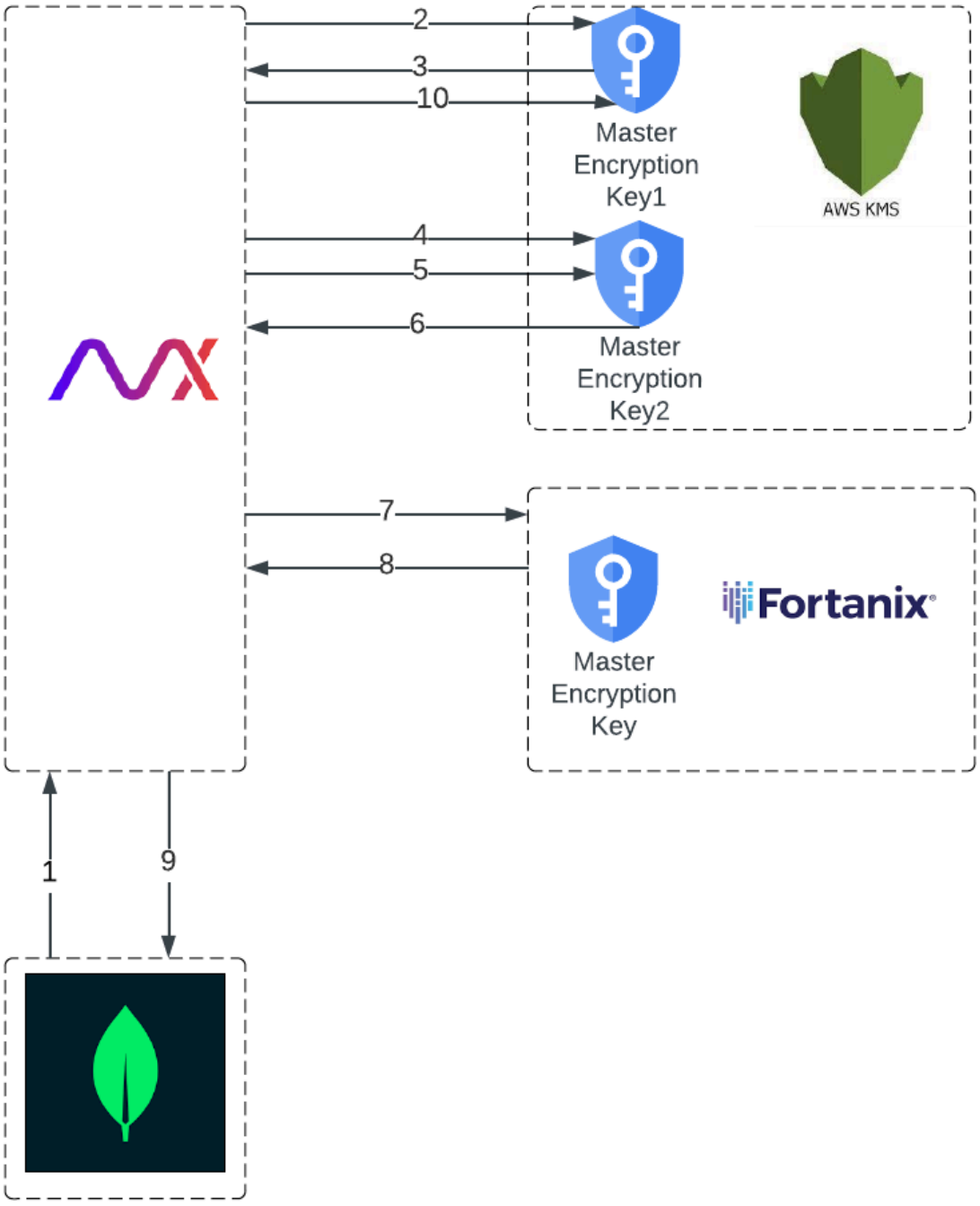
Enabling AppViewX Master Key Encryption

Encrypting the AppViewX Master Key using the User's Master Key

AppViewX offers the ability to encrypt the AppViewX Master Key using the User's Master Key stored in the User's Hardware Security Module (HSM). This delegation of control over all data to the user enhances the confidentiality and security of sensitive information. With this option enabled, AppViewX can only access sensitive data if the User's Master Key is available and valid.



When the user chooses to encrypt the AppViewX Master Key using the User's Master Key stored in the HSM, AppViewX executes the following steps:



1. Retrieve the existing KMS-encrypted Master Encryption Key (MEK) from the tenant's database.
2. Decrypt the AppViewX MEK using the MEK (Master Encryption Key 1) created during tenant onboarding in the KMS.
3. Retrieve the plaintext AppViewX MEK.

4. Generate a new **MEK (Master Encryption Key 2)** in the KMS.
5. Encrypt the AppViewX MEK using the MEK 2 in the KMS.
6. Retrieve the KMS-encrypted AppViewX MEK.
7. Encrypt the KMS-encrypted AppViewX MEK using the User's Master Key in the HSM.
8. Retrieve the double-encrypted AppViewX MEK.
9. Update the new double-encrypted AppViewX MEK in the database, replacing the previous KMS MEK encrypted ciphertext in the tenant's database.
10. Schedule the **Master Encryption Key 1** for deletion to ensure that any previous data backups are invalidated.

Note: It is important to note that the AppViewX Master Encryption Key is stored only in its encrypted form within the tenant's database and is not paged or stored elsewhere.

Why is there a dependency on AWS KMS?

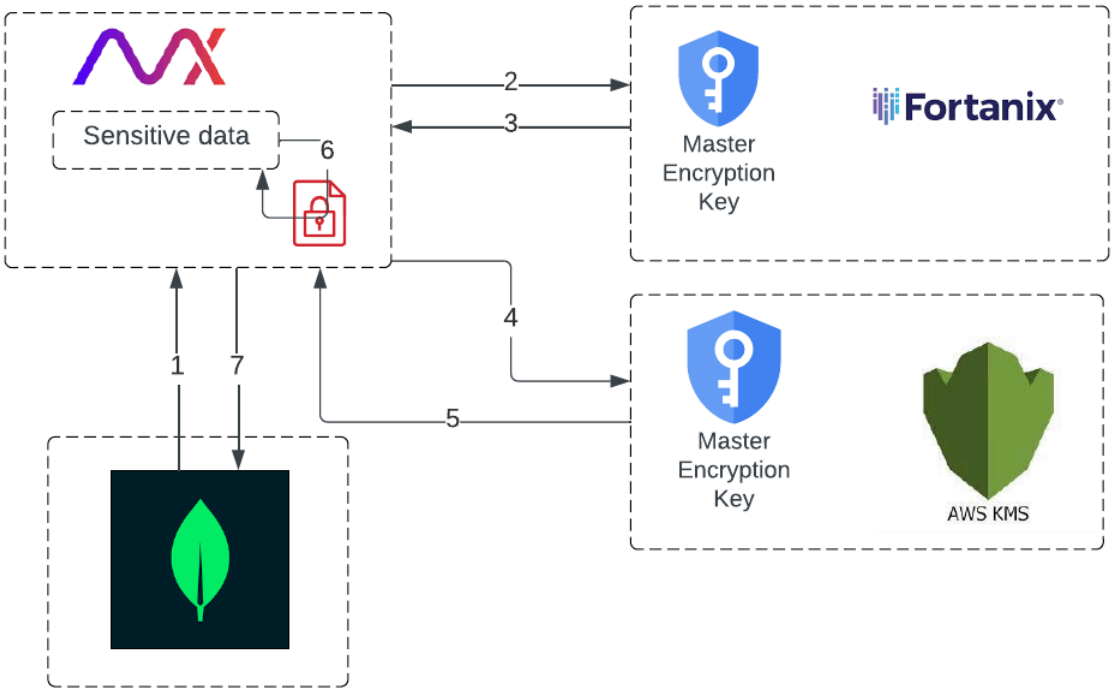
AppViewX uses the AWS KMS for two main purposes:

- To retain a key for encrypting the AppViewX Master Encryption Key (MEK) when it is sent to the user's HSM through the AppViewX Cloud Connector
- To encrypt sensitive information related to the HSM.

Although the AWS KMS continues to be utilized, the AppViewX MEK is encrypted using the user's Master Key stored in the HSM. This means that if the Master Key is removed from the HSM, the data will become inaccessible.

New Encryption/Decryption Flow

When sensitive data is fed into AppViewX after enabling AppViewX MEK encryption via the HSM, to ensure data security, AppViewX executes the following steps:



Note: The AppViewX Master Encryption Key (MEK) is required to encrypt/decrypt the sensitive data, but it is not readily available. The process of retrieving the AppViewX MEK involves two steps, with the HSM initially in control.

1. Retrieve the encrypted AppViewX MEK from the tenant's database.
2. Send a request to the HSM, which decrypts the encrypted MEK and sends back a response. This response is a ciphertext encrypted using the KMS MEK.
3. Retrieve the decrypted value (KMS encrypted).
4. Send a request to the AWS KMS to decrypt the KMS-encrypted AppViewX MEK using the KMS's MEK.
5. Retrieve the plaintext AppViewX MEK.
6. Encrypt/Decrypt sensitive data using the plaintext AppViewX MEK.
7. Persist the encrypted sensitive data in the tenant database.

Warning:

- After enabling AppViewX Master Key encryption, if the User’s Master Key is removed from the HSM, all data becomes inaccessible and irrecoverable. There is no way for the recovery of this data.
- Once AppViewX Master Key encryption is enabled, there is no option to roll back to the default approach of using AWS-KMS.

Understanding the HSM Health Check and Sync Status Functionalities

To ensure the proper functioning of the HSM, a health check of the HSM is scheduled to occur every hour after the encryption of AppViewX's MEK is enabled. If the HSM is deemed unhealthy for three consecutive checks, the plaintext MEK will be purged from AppViewX's in-memory cache, failing most system functions. The affected use cases are listed here .

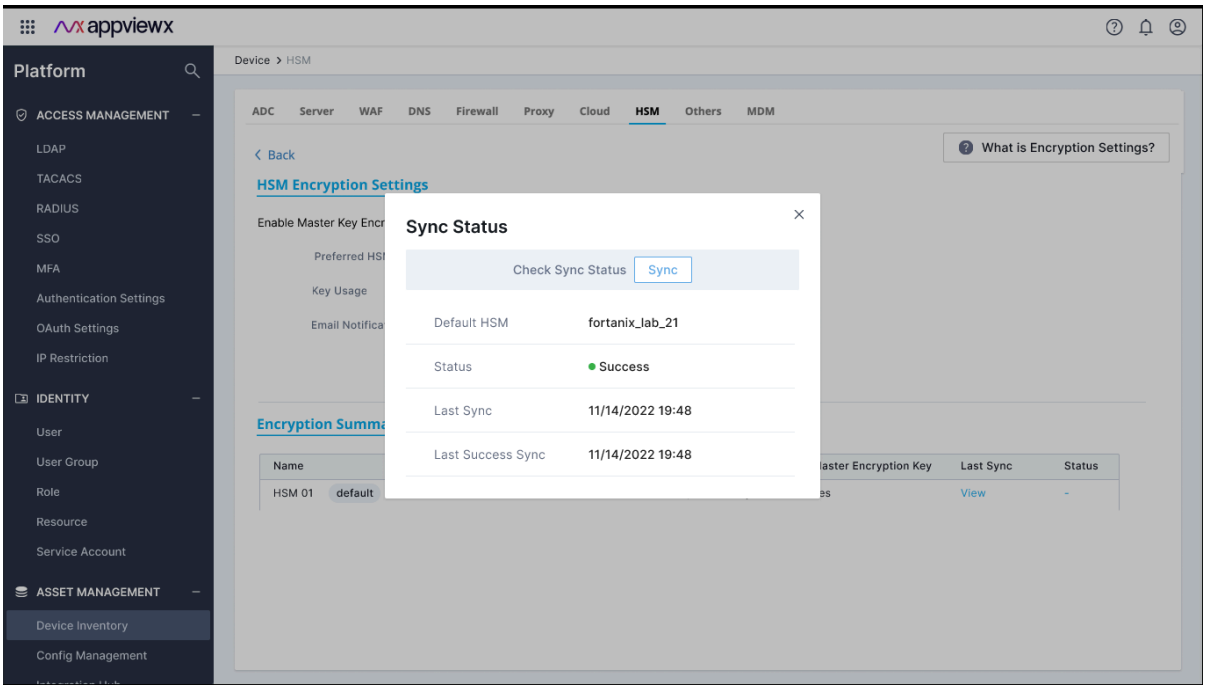
The HSM is considered unhealthy:

- If the Master Encryption Key has been removed

or

- The HSM credentials have been changed and not updated in AppViewX.

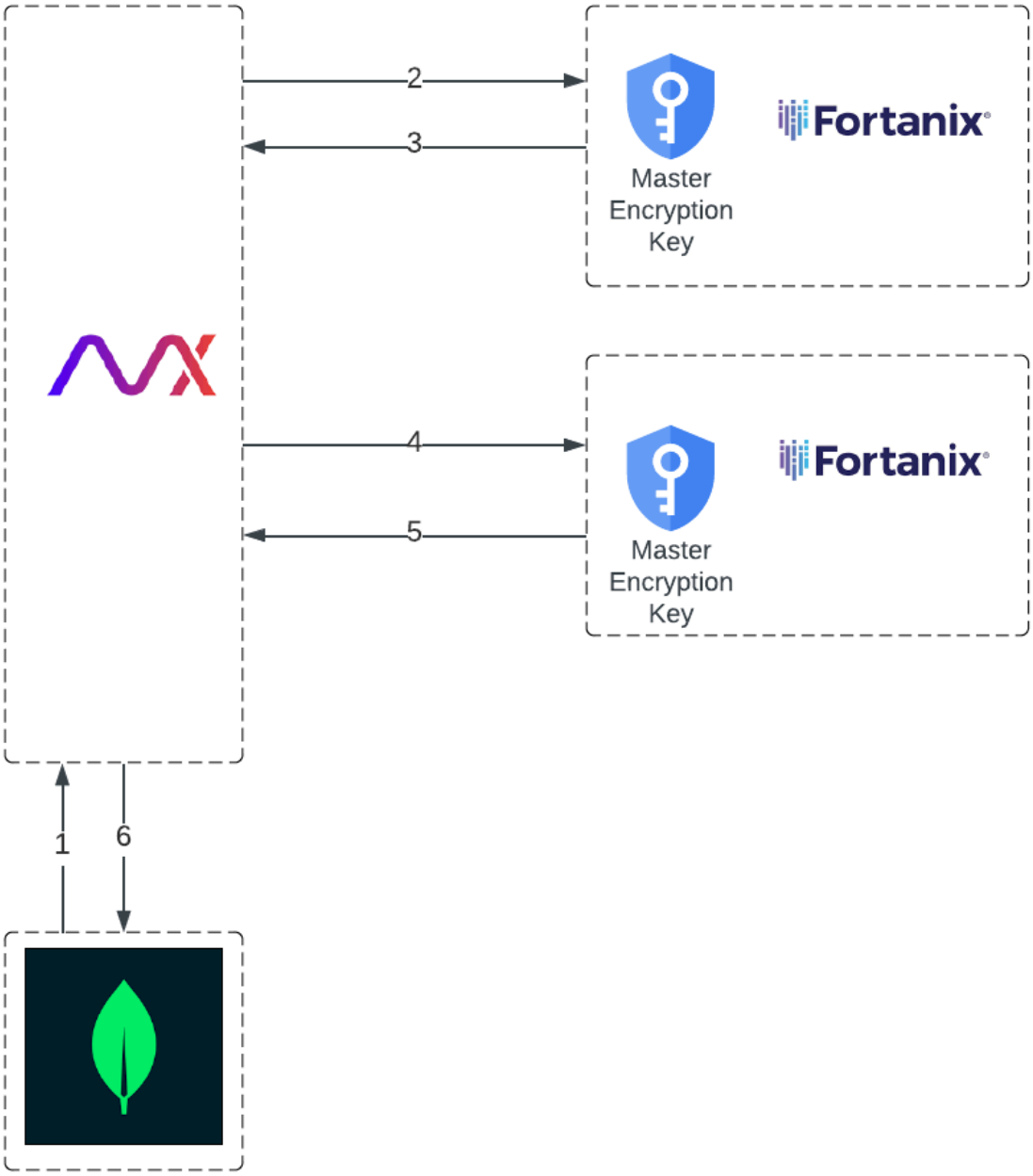
In addition to the regular health checks, AppViewX provides an option in the GUI to manually initiate a health check. If the user selects to sync their HSM and the HSM is found to be unhealthy, the MEK stored in AppViewX's cache will be immediately purged.



Note: The in-memory cache functionalities will start to fail, even without flushing, if the key is not available in the cache. This is because the key retrieval will not succeed when the HSM is unhealthy.

Switching between HSMs

Once the encryption of the AppViewX MEK has been enabled, it cannot be disabled. However, it is possible to switch between the HSMs used for encryption. The process involves decrypting the MEK using the current HSM and then re-encrypting it using the new HSM. To switch between HSMs, AppViewX executes the following steps:



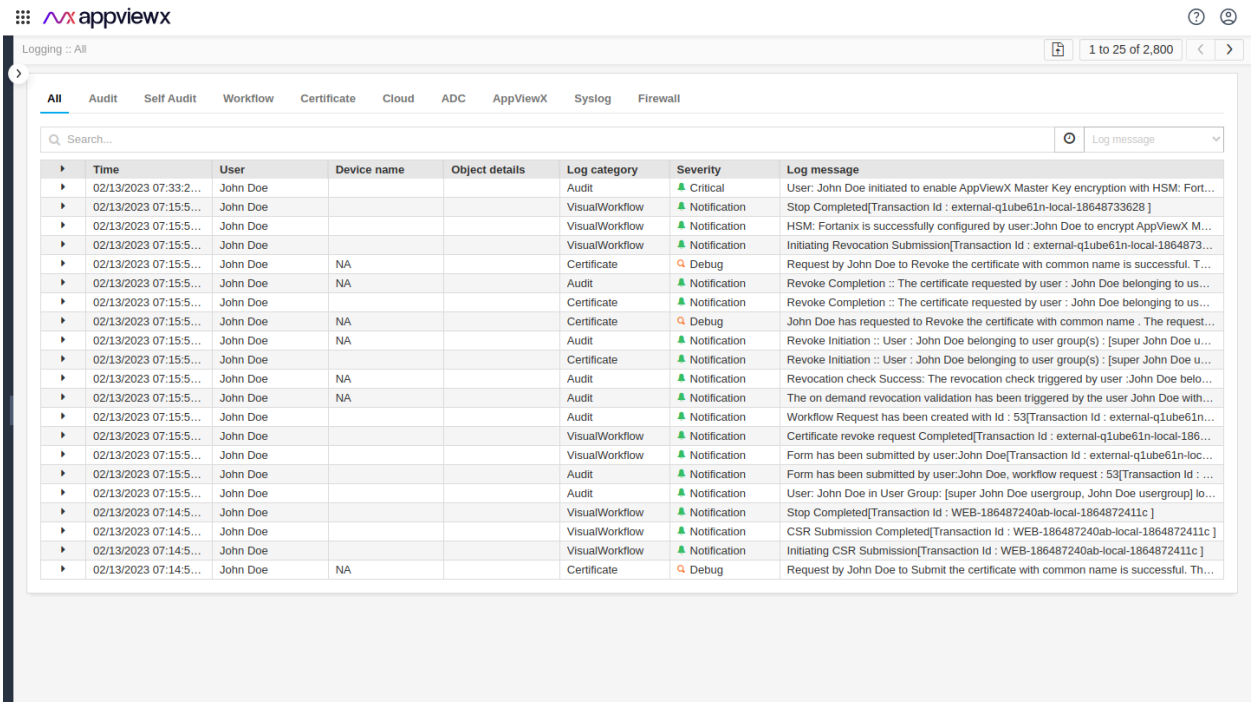
1. Retrieve the encrypted AppViewX MEK from the tenant database.
2. Decrypt the AppViewX MEK using the current HSM.
3. Retrieve the KMS-encrypted AppViewX MEK.
4. Encrypt the AppViewX MEK using the new HSM.
5. Retrieve the double-encrypted AppViewX MEK.
6. Persist the encrypted AppViewX MEK in the tenant database.

Warning: When switching between HSMs, the User's Master Key in the existing HSM should be retained till the process is complete, failing which can result in a failure in the switch operation.

Viewing Audit Logs for Encryption Operations

The AppViewX audit logs provide a comprehensive view of system activity, allowing users to track and monitor various events. Whenever the tenant administrator enables the encryption of the AppViewX Master Key, all subsequent operations are also recorded in the logs.

Note: For instructions on viewing and reading the audit logs, click here.



The following table lists the log events recorded in the context of the AppViewX Master Key Encryption:

Actions with Log Message

Action	Log Message
Tenant Admin initiates encryption of AppViewX Master Key.	User:<User Name> initiated to enable AppViewX Master Key encryption with HSM:<HSM Name>
AppViewX Master Key encryption is successful	HSM:<HSM Name> is successfully configured by user:<User Name> to encrypt sensitive data.

Actions with Log Message (continued)

Action	Log Message
AppViewX Master Key encryption has failed	HSM:<HSM Name> configuration to encrypt sensitive data failed due to <reason>.
AppViewX retrieved the plaintext AppViewX MEK successfully.	Connected with HSM:<HSM Name> for decrypting AppViewX MEK and it is a success.
AppViewX failed to retrieve the plaintext AppViewX MEK.	Connected with HSM:<HSM Name> for decrypting AppViewX MEK and it failed.
KMS Key created during onboarding is scheduled for deletion after enabling AppViewX MEK encryption.	KMS Key will be deleted within seven days as AppViewX Master Key encryption through HSM is enabled.
Scheduled health check of HSM is successful.	Scheduled validation of Master Key with HSM:<HSM Name> is successful.
Scheduled health check of HSM failed.	Scheduled validation of Master Key with HSM:<HSM Name> is failed due to <reason>.
Scheduled health check of the HSM failed due to removal of the User's Master Key.	Scheduled validation of Master Key with HSM:<HSM Name> is failed because MEK is not available. So, AppViewX MEK is flushed from memory.
Scheduled health check of the HSM failed due to three continuous failures.	Scheduled validation of Master Key with HSM:<HSM Name> is failed continuously for the third time. So, AppViewX MEK is flushed from memory.
The user initiated a health check from the GUI and it succeeded.	User:<User Name> initiated validation of Master Key with HSM:<HSM Name> and it is a success.
The user initiated a health check from the GUI and it failed.	User:<User Name> initiated validation of Master Key with HSM:<HSM Name> and it failed due to <reason>.
The user initiated a health check from the GUI and it failed due to removal of the User's Master Key.	User:<User Name> initiated validation of Master Key with HSM:<HSM Name> and it is failed because MEK not available. So, AppViewX MEK is flushed from memory.

Impacted Use Cases if the Customer's Master Key is Removed

Overview

If the customer's Master Key in the HSM is removed and the AppViewX MEK is purged from AppViewX's in-memory cache, logging into AppViewX using LDAP/SSO and local accounts with multi-factor authentication (MFA) will be disabled.

Note: Multi-factor authentication (MFA) is planned for a future release.

For users currently logged/users logged in using a local account without MFA, the functions listed in the following sections will become unavailable. Additionally, personally identifiable information such as the user's first and last name, email address, and phone number will be displayed as ciphertext in the product's user interface.

User Management

- Login as local user when MFA is enabled
- Change Password for local account
- Create service account
- Authorize service account
- Change Client ID/ Secret for service account
- Configure LDAP
- Login with AD
- Configure TACACS

- Login with TACACS
- Configure RADIUS
- Login with RADIUS
- Configure SAML
- Login with SAML
- Configure OIDC
- Login with OIDC

Vault

- Add credential in AppViewX vault
- Add credential with Other vaults
- Integrate vaults
- Add device using credential in vault
- Perform other operations in device with credential in vault
- Perform operations in cloud account using credential in vault
- Perform operations in CA using credential in vault

HSM

- Add HSM
- Delete HSM
- Configure Private KEY in HSM
- Configure All encryption in HSM
- Change default HSM
- Enable CSR in HSM
- Rotate HSM key

Log Forwarding

- Configure log forwarding with Splunk HEC
- Forward logs using Splunk

Alerts

- Configure alerts
- Send alerts

License

- Apply License

Mail Server

- Configure mail server using SMTP
- Configure mail server using OAuth
- Send email using SMTP credentials
- Send email using OAuth credentials

Certificate Management

- Upload CA certificate
- Generate custom CA certificate
- Add MDM devices to inventory
- Update MDM device(s)
- Import MDM Devices
- Save intermediate and root cert in DB if new certificate
- Create client certificate
- Upload client authentication json into CA settings
- Symantec CA: Challenge password functionality
- API to persist credentials of certificates in the Vault
- Update CA connector info with challenge password during revoke
- Auto enrollment: Create/Update agent settings
- Encrypt the intune client secret: update agent setting
- Auto enrollment create certificate: Perform Client Authentication
- Save external vault details in inventory
- Save HSM settings
- Update CA settings: secret access key in VendorSpecific Settings
- Retrieve CA specific values from certificate authority

- Authenticate vendor for server
- Update GCP cloud connector
- Cloud vendor details in view device
- Get vendor details for AWS, Azure, GCP
- Misc: Fetch credentials from credential store
- Encrypt device password or get access details from the credential store for device
- API to encrypt plain text using HSM Utimaco
- HSM Thales encryption service
- HSM SafeNet encryption service
- Upload certificate via holistic view
- Upload client authentication certificate
- Upload server certificate
- Discovery via upload
- Bulk upload
- Application connector: Profile and user preference properties
- Discovery: Password protected certificate parsing

AppViewX Cloud Connector

- Add a cloud connector

FAQs-Supporting User Master Key

- **How does AppViewX connect with the HSM?**

  The cloud connector facilitates all communication and interactions between AppViewX and the User's resources, which includes the Hardware Security Module (HSM).

- **Is the data that is sent to the Cloud Connector encrypted during transit?**

  Yes. The communication between AppViewX and the AppViewX cloud connector is through a TLS-encrypted channel.

- **What is the impact after enabling AppViewX Master Key Encryption if the virtual machine or server hosting the AppViewX Cloud Connector experience health issues?**

  The AppViewX cloud connector is required for any communication with the HSM. If there are issues between AppViewX and the AppViewX cloud connector, it can result in a service disruption. To ensure

high availability, it is recommended to deploy multiple cloud connectors across various data centers and also ensure that all deployed cloud connectors can interact with the HSM.

- **Can you explain the reason for not rotating the AppViewX Master Key when the User opts to utilize a User Master Key?**

  AppViewX uses envelope encryption to enhance the security of confidential data. This technique involves encrypting the AppViewX Master Key with the User's Master Key, thus allowing the User to retain control over their data. To ensure the security of the AppViewX Master Key, AppViewX never stores it in plain text format and instead uses AWS KMS to encrypt it. When the user opts to encrypt the AppViewX Master Key, all existing keys of that tenant in the KMS are discarded, rendering any previous data backups useless. The tight security measures in place eliminate the need for rotating the AppViewX Master Key, saving the cost and effort of re-encrypting all secure materials.

- **Can you provide an overview of the actions that an MFA-disabled local user can carry out if the User Master Key is removed from the HSM?**

  In the event that the Master Key is removed, AppViewX will be in a near-read-only state, where only non-sensitive data, such as audit logs, can be viewed. Any actions requiring access to sensitive information will be disabled, even for a local user without multi-factor authentication. This added layer of security ensures the protection of confidential data and reinforces AppViewX's commitment to data privacy and security.

- **What are the consequences if the password for the HSM is modified and not updated within AppViewX?**

  AppViewX conducts regular health checks on the HSM where the User Master Key is stored. In the event that the HSM is deemed unhealthy after three consecutive failures, AppViewX will flush the plain text AppViewX MEK from its cache. This measure is necessary to protect the confidentiality of the data, but it may result in a temporary service disruption.

- **Are there any notifications to alert us in the event that the HSM is not functioning optimally or if the Master Key is removed?**

  When enabling the AppViewX MEK encryption, users can set up notifications for the health of the Hardware Security Module (HSM). By configuring a list of email addresses, users can stay informed about the status of the HSM.

- **Since there is a dependency on the AWS KMS, is the service highly available?**

  Yes AWS KMS is highly available within an AWS region.

- **After enabling AppViewX Master Key encryption by User Master Key do we have the option to revert back?**

No. After enabling AppViewX MEK encryption there is no option to revert back to using the AWS KMS. We can switch the HSM that stores the User's Master Key.

- **Does AppViewX support rotating the User Master Key stored in the HSM?**

  Currently, we do not support the rotation of the User Master Key.

- **Does AppViewX rotate the Master Key stored in the AWS KMS?**

  Yes, the Master Key stored in the AWS KMS is rotated every 90 days.

- **Can you provide details regarding the algorithm and size of the AppViewX Master Key?**

  Algorithm: AES

  Size: 256-Bit Key

Rotation Settings

HSM key rotation involves the regular replacement of cryptographic keys used by a Hardware Security Module (HSM) to bolster security and safeguard sensitive data. This process includes generating new keys and securely substituting the current ones.

Accessing Rotation Settings

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **VAULT & SECURITY**, select **Rotation Settings**. The **Settings :: Key Rotation** page is displayed.	1. From the main navigation menu, select **Settings** > **General** > **Key Rotation**. 2. The **Settings :: Key Rotation** page is displayed.
Note: For more information on how to switch between menus, click here.	

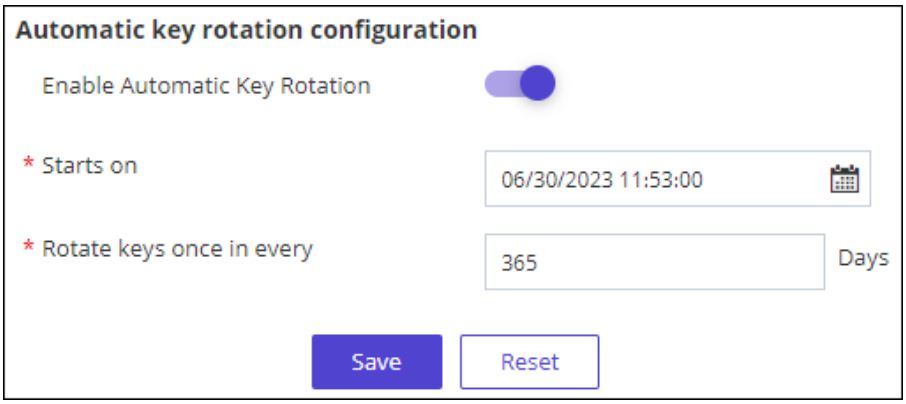
- Automatic key rotation configuration
- On Demand Key Rotation

Automatic key rotation configuration

"Automatic key rotation" configuration involves the automatic rotation of cryptographic keys at predefined intervals, ensuring the automatic replacement of encryption keys without manual intervention.

To configure the Automatic key rotation settings:

1. On the **Settings :: Key Rotation** page, from the left corner of the screen, navigate to the **Automatic key rotation configuration**.



2. Enable the toggle to **Enable Automatic Key Rotation**.

> **Note:** On selecting **Enable Automatic Key Rotation**, the ***Starts on** and ***Rotate keys once in every** attribute appears.

Field descriptions for Automatic Key rotation configuration

Field	Description
*** Starts on**	This field provides a calendar option to specify the start date and time of the key rotation.
*** Rotate keys once in every**	This field enables you to define the rotation frequency of keys in terms of the number of days.

> **Note:** The asterisk (*) symbol indicates mandatory fields.

3. Click **Save**.

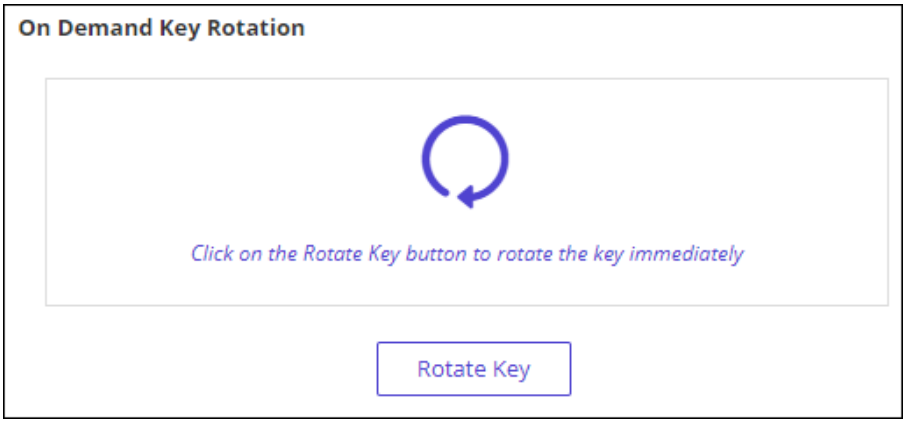
   A Confirmation message indicating 

is displayed on the screen.

On Demand Key Rotation

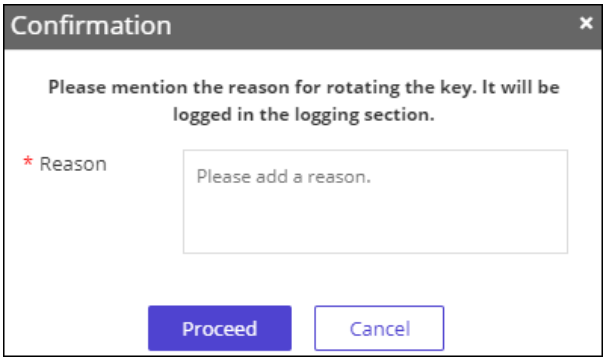
"On Demand Key Rotation" is a process of manually rotating cryptographic keys as necessary, providing flexibility in key management based on specific requirements. This approach empowers organizations to initiate key rotation at any time to meet their needs.

1. On the **Settings :: Key Rotation** page, from the right corner of the screen, navigate to the **On Demand Key Rotation**.



2. Click **Rotate Key** to rotate the key immediately.

   A pop-up window of **Confirmation** is displayed.



3. Enter the **Reason** for rotating the key. It will be logged in the logging section.

4. Click **Proceed**.

A Confirmation message indicating **Key rotation triggered successfully** is displayed on the screen.

Managing Alerts

Alert management is important for an organization to monitor and respond to security concerns before they become a threat to the organization's security.

As part of its alert management, AppViewX enables you to identify complications that may occur within an application. Alerts can then be configured, to notify the users of these complications, and send a predetermined date and time using email and SNMP configurations.

AppViewX enables managing alerts in the following categories

Alert type	Description
Certificate	Alerts triggered when a certificate is invalid, about to expire, or out of sync
SSH	Alerts related to SSH components
ADC	ADC alerts for changes that are triggered through AppViewX
AppViewX	Alerts related to AppViewX-specific components
Syslog	Syslog alerts of critical applications and devices for changes that are executed on the device and execute workflow as an action

For each alert type, AppViewX defines the following severity levels

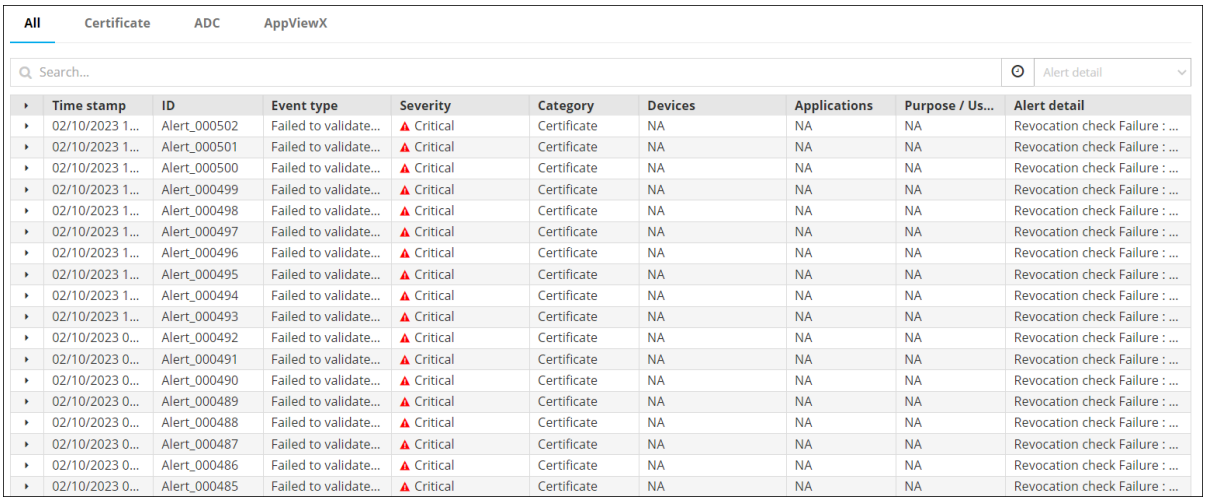
Severity level	Description
Critical	Alerts for issues that can disastrously impact functionality are marked as critical alerts. These are top priority and must be resolved immediately.
Fatal	Alerts for issues that can disastrously impact functionality are marked as fatal alerts. These are top priority and must be resolved immediately.
Major	Alerts for issues that are important and require a resolution, but are not a top priority, are marked as major alerts.
Minor	Alerts for issues that are low priority are marked as minor alerts.
Notification	Alerts for issues that users have to only be notified/warned of are marked as notifications.

For these alerts, AppViewX lets you:

- View alerts
- Configure alerts
- Search for alerts
- Purge alerts
- Delete alerts.

Accessing the Alerts Page

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **OBSERVE & EXPLORE**, select **Alerts**. The **Alerts :: All** page is displayed with the **All** tab open by default.	From the main navigation menu, select **Alert**. The **Alert :: All** page is displayed with the **All** tab open by default.
Note: For more information on how to switch between menus, click here.	

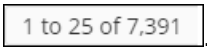


Time stamp	ID	Event type	Severity	Category	Devices	Applications	Purpose / Us...	Alert detail
02/10/2023 1...	Alert_000502	Failed to validate...	Critical	Certificate	NA	NA	NA	Revocation check Failure : ...
02/10/2023 1...	Alert_000501	Failed to validate...	Critical	Certificate	NA	NA	NA	Revocation check Failure : ...
02/10/2023 1...	Alert_000500	Failed to validate...	Critical	Certificate	NA	NA	NA	Revocation check Failure : ...
02/10/2023 1...	Alert_000499	Failed to validate...	Critical	Certificate	NA	NA	NA	Revocation check Failure : ...
02/10/2023 1...	Alert_000498	Failed to validate...	Critical	Certificate	NA	NA	NA	Revocation check Failure : ...
02/10/2023 1...	Alert_000497	Failed to validate...	Critical	Certificate	NA	NA	NA	Revocation check Failure : ...
02/10/2023 1...	Alert_000496	Failed to validate...	Critical	Certificate	NA	NA	NA	Revocation check Failure : ...
02/10/2023 1...	Alert_000495	Failed to validate...	Critical	Certificate	NA	NA	NA	Revocation check Failure : ...
02/10/2023 1...	Alert_000494	Failed to validate...	Critical	Certificate	NA	NA	NA	Revocation check Failure : ...
02/10/2023 1...	Alert_000493	Failed to validate...	Critical	Certificate	NA	NA	NA	Revocation check Failure : ...
02/10/2023 0...	Alert_000492	Failed to validate...	Critical	Certificate	NA	NA	NA	Revocation check Failure : ...
02/10/2023 0...	Alert_000491	Failed to validate...	Critical	Certificate	NA	NA	NA	Revocation check Failure : ...
02/10/2023 0...	Alert_000490	Failed to validate...	Critical	Certificate	NA	NA	NA	Revocation check Failure : ...
02/10/2023 0...	Alert_000489	Failed to validate...	Critical	Certificate	NA	NA	NA	Revocation check Failure : ...
02/10/2023 0...	Alert_000488	Failed to validate...	Critical	Certificate	NA	NA	NA	Revocation check Failure : ...
02/10/2023 0...	Alert_000487	Failed to validate...	Critical	Certificate	NA	NA	NA	Revocation check Failure : ...
02/10/2023 0...	Alert_000486	Failed to validate...	Critical	Certificate	NA	NA	NA	Revocation check Failure : ...
02/10/2023 0...	Alert_000485	Failed to validate...	Critical	Certificate	NA	NA	NA	Revocation check Failure : ...

Setting the Record Count Preference for Viewing Alerts

For easier viewing of records, AppViewX lets you set the record count preference, which is the number of alert records that will be displayed on one page.

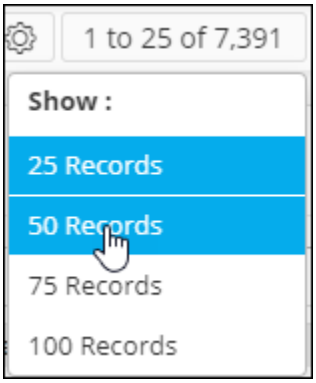
To set the record count preference:

1. On the **Alert :: All** page, from the top-right corner of the screen, click 

.

> **Note:** By default, 25 alert records are displayed on one page (which is why the control reads 1 to 25).

2. From the **Show** menu displayed, select your record count preference (for example, 50 records).



3. The Alert page is updated according to the record count preference selected. A message, **Record count preference saved successfully**, is displayed. The UI control is also updated to display the current selection, as shown in the following image:

Configuring Alerts

AppViewX lets you configure alerts to define when the event type that will trigger an alert, the severity of the alert, the message to describe the alert, settings for sending alert notifications, and so on. The subsequent sections outline the instructions for configuring the following types of alerts:

- Certificate
- Syslog
- SSH
- AppViewX
- ADC.

- Configuring Certificate Alerts
- Configuring Syslog Alerts
- Configuring AppViewX Alerts
- Configuring ADC Alerts

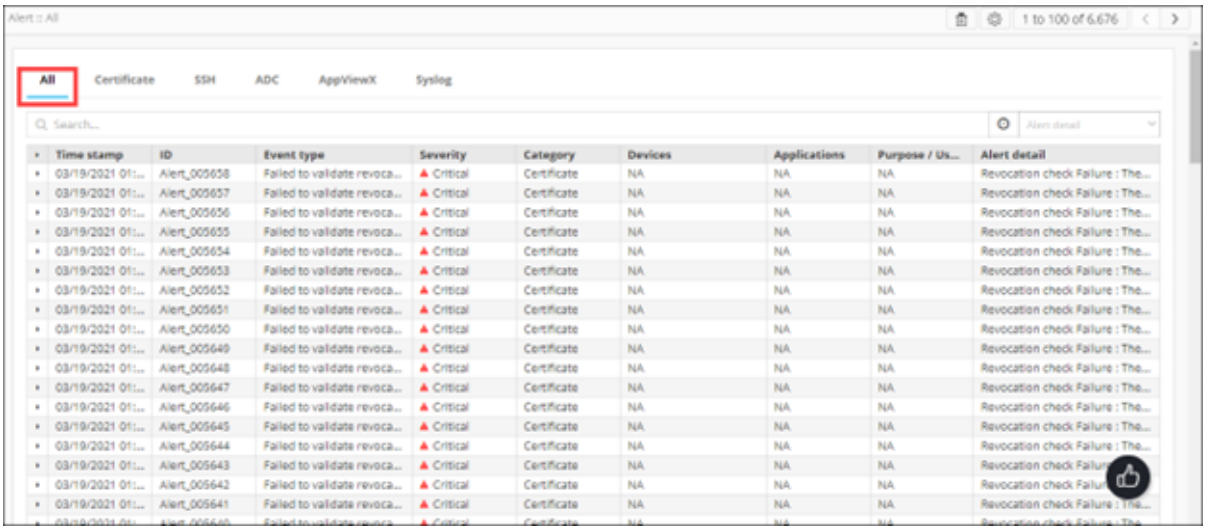
Configuring Certificate Alerts

Certificate alerts are generated to notify users of certificate events that require the user to take a remedial action. Certificate alerts are sent when:

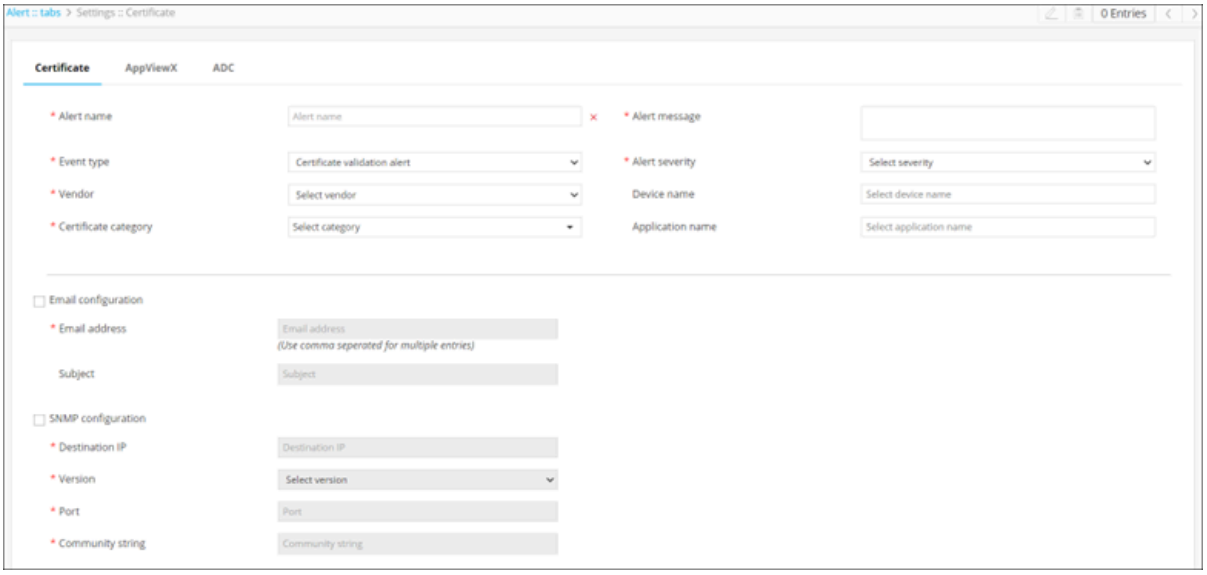
- Certificates need to be validated
- Certificates are set to expire
- Certificates cannot be synchronized.

To configure certificate alerts:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the **(Menu)** icon.
2. From the menu displayed, click **Alert**.
   The **Alert :: All** page is displayed (by default).



3. From the top-right corner of the screen, click **(Settings)** icon.
4. The **Settings :: Certificate** page is displayed, with the **Certificate** tab open by default.



5. To configure certificate alerts, enter the following details:

Field descriptions for Certificate Alerts

Field	Description
***Alert name**	Enter the name you want to give this alert.
***Alert message**	Enter the message that will be displayed with the alert, to describe the alert.

Field	Description
	Note: This field is not displayed when configuring the certificate expiry alert. **Note:** The alert message cannot be longer than 64 words.
***Event type**	From the drop-down menu, select the event type that will trigger this alert from the following options: • Certificate validation alert (default) • Certificate expiry alert • Certificate sync alert.
***Alert severity**	From the drop-down menu, select a severity for the alert from the following options: • Critical • Major • Notification.
Vendor	From the drop-down menu, select the vendor name for whose device/ application you are creating the alert. **Note:** This field is not displayed when configuring the certificate expiry alert.
Device name	Enter the name of the device associated with the certificate you are creating the alert for. **Note:** This field is not displayed when configuring the certificate expiry alert.
***Certificate category**	From the drop-down menu, select a certificate category from the following options: • Server • Client • Device • Code Signing.

Field	Description
***Expires in (days)**	Enter the number of days till the certificate expires. **Note:** This field is displayed only when configuring certificate expiry alerts.
Email configuration	To send the certificate alert as an email, select this check box.
***Email address**	To send the certificate alert as an email, enter the email address to which this specific certificate alert will be sent. **Note:** Separate multiple email addresses with a comma.
Subject	To send the certificate alert as an email, enter a subject line.
SNMP configuration	To use the Simple Network Management Protocol for sending the alert, select this check box.
***Destination IP**	Enter the destination IP address for the alert.
***Version**	From the drop-down menu, from the following options, select the SNMP version to be used: • V1 • V2.
***Port**	Enter the port number to be used for the alert.
***Community string**	Enter the community string for the alert. The community string is similar to a user ID or password that allows users access to the requested information on the device.
Note: The asterisk (*) symbol indicates mandatory fields.	

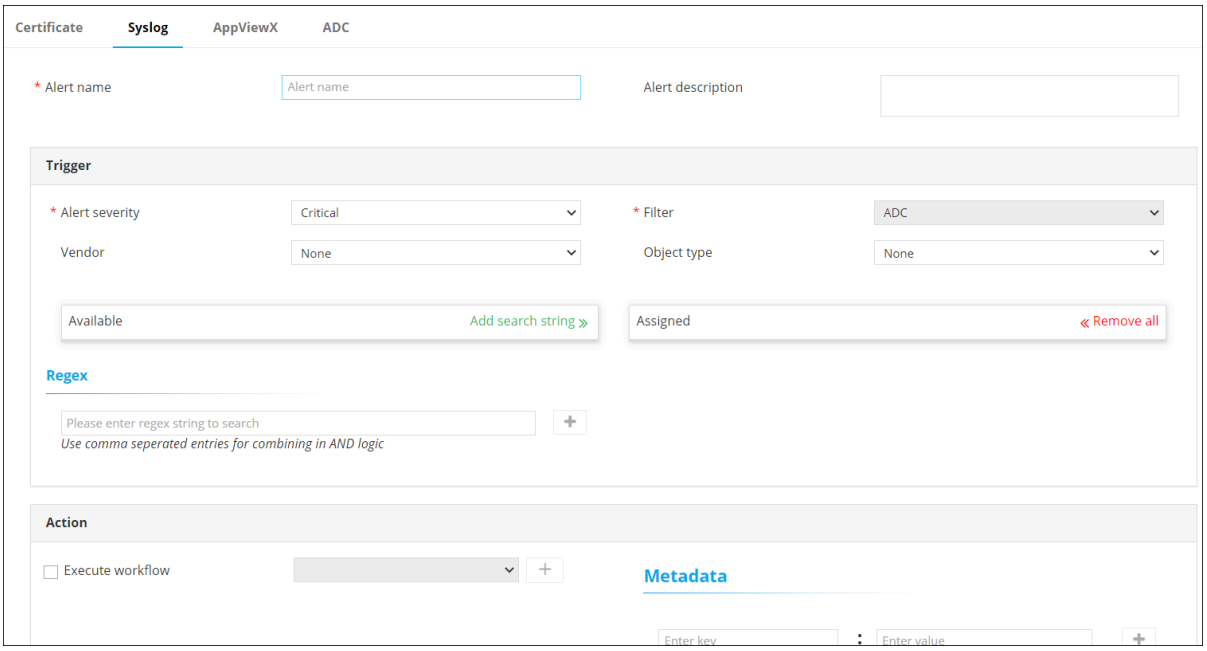
6. To save the certificate alerts configuration details, click **Add**.
   The saved details are displayed in the table shown at the bottom of the screen.

Configuring Syslog Alerts

AppViewX subscribes to all device-level alerts, where it acts as a syslog listener. Logs of any device added in AppViewX can be viewed as syslog. However, devices tend to generate a huge amount of data. To resolve this, a Syslog Alert is a convenient way to notify about specific syslog information that is of importance to you.

To configure syslog alerts:

1. On the **Alert :: All** page, from the top-right corner of the screen, click **(Settings)** icon.
   The **Settings :: Certificate** page is displayed with the **Certificate** tab open by default.
2. To configure Syslog alerts, click **Syslog**.
   The **Settings :: Syslog** page is displayed.



3. Enter the following details:

Field descriptions for Syslog

Field	Description
***Alert name**	Enter the name you want to give this alert.
Alert description	Enter a description for the alert.

Field	Description
	Note: The asterisk (*) symbol indicates mandatory fields.

4. In the **Trigger** section, enter the following details:

Field descriptions for Trigger

Field	Description
***Alert severity**	From the drop-down, from the options given below, select a severity for the alert: • Critical • Fatal • Major • Minor • Notification.
Filter	For syslog alerts, the filter is set to ADC, because syslog alerts are parsed only through ADC devices.
Vendor	ADC module vendor (**A10**, **Citrix**, or **F5**)
Object type	Object type for ADC (**FQDN**, **Service IP**, **VirtualService**, **ServiceGroup**, **Server**, **VirtualServer**, or **Device**)
Available	Depending on the **Object type** and **Vendor** selected, a list of all available ADC objects or devices is displayed here.
Add search string	Instead of adding devices manually, AppViewX lets you automatically assign all existing devices or objects that match your criteria. To do this: a. In the **Available** section, in the **Search** field, enter the search criteria. b. Click **Add search string**. **Note:** The benefit of using a search string rather than selecting devices manually is that the search string continues to work in the background and auto-assigns all new devices that match the search criteria.

Field	Description
Assigned	To add an object to the Assigned column, click the check box corresponding to that object.
Regex	Enter single/multiple regex patterns/strings. **Note:** When entering multiple regex patterns/strings, separate the regex strings using commas. The comma works as the **BOOLEAN AND** operator.
Note: The asterisk (*) symbol indicates mandatory fields.	

5. In the **Action** section, enter the following details:

Field descriptions for Action

Field	Description
Execute workflow	To select the workflow to trigger: a. Select the **Execute workflow** check box. b. From the drop-down menu, select the workflow to trigger.
Metadata	AppViewX lets you define a metadata condition based on which the workflow will be triggered. To define a metadata key-value pair for this condition: a. In the **Enter key** field, enter the key. b. In the **Enter value** field, enter the key value. To add another key-value pair: a. Click **(Add)** icon. b. In the **Enter key** field, enter the key. c. In the **Enter value** field, enter the key value. To delete a key-value pair: For the key-value pair you want to delete, click **(Delete)** icon.

6. To send the Syslog alert as an email, execute the steps for configuring SMTP for email alerting.
7. Enter the following details:

Field descriptions for SMTP email alerting

Field	Description
Email configuration	To send the syslog alert as an email, select this check box.
Email configuration	To send the syslog alert as an email, enter the email address to which this specific syslog alert will be sent. **Note:** Separate multiple email addresses with a comma.
Email configuration	To send the syslog alert as an email, enter a subject line.
Note: The asterisk (*) symbol indicates mandatory fields.	

8. To use the Simple Network Management Protocol (SNMP) to send the alert, enter the following details:

Field descriptions for Simple Network Management Protocol

Field	Description
SNMP configuration	To use the Simple Network Management Protocol for sending the alert, select this check box.
***Destination IP**	Enter the destination IP address for the alert.
***Version**	From the drop-down menu, from the following options, select the SNMP version to be used: • V1 • V2.
***Port**	Enter the port number to be used for the alert.
***Community string**	Enter the community string for the alert. The community string is similar to a user ID or password that allows users access to the requested information on the device.

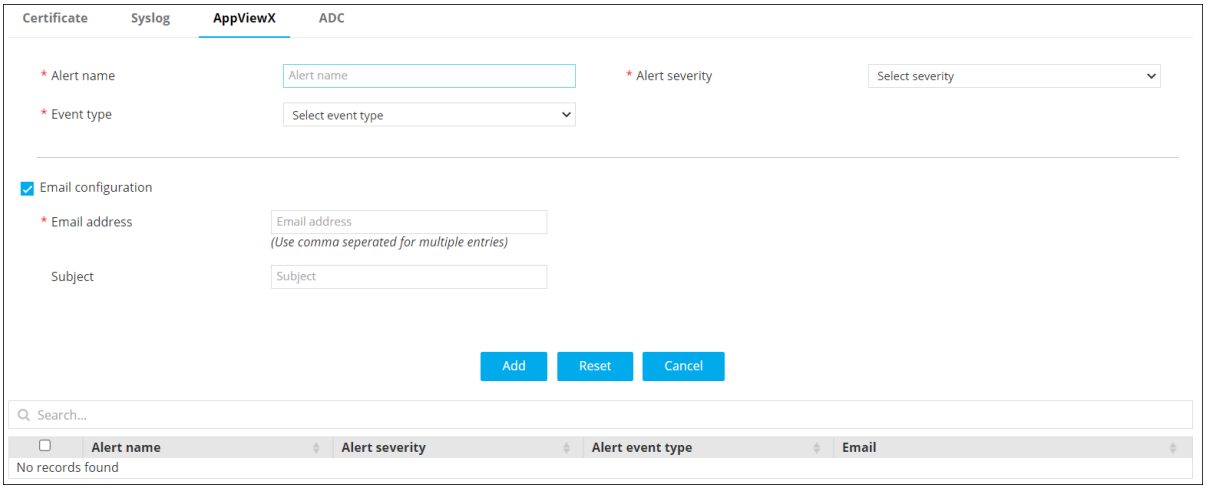
Field	Description
	Note: The asterisk (*) symbol indicates mandatory fields.

9. To save the Syslog alerts configuration details, click **Add**.
   The saved details are displayed in the table shown at the bottom of the screen.

Configuring AppViewX Alerts

To configure AppViewX alerts:

1. On the **Alert :: All** page, from the top-right corner of the screen, click **(Settings)** icon.
   The **Settings :: Certificate** page is displayed with the **Certificate** tab open by default.
2. To configure AppViewX alerts, click **AppViewX**.
   The **Settings :: AppViewX** page is displayed.



3. Enter the following details:

Field descriptions for AppViewX Alerts

Field	Description
***Alert name**	Enter the name you want to give this alert.

Field	Description
***Alert severity**	From the drop-down menu, select a severity for the alert from the following options: • Critical • Fatal • Major • Minor • Notification.
***Event type**	From the drop-down menu, from the following options, select the event type that will trigger this alert: • Infrastructure • Application Discovery.
Email configuration	To send the certificate alert as an email, select this check box. **Note:** For AppViewX alerts, this feature is enabled by default.
***Email address**	To send the certificate alert as an email, enter the email address to which this specific certificate alert will be sent. **Note:** Separate multiple email addresses with a comma.
Subject	To send the certificate alert as an email, enter a subject line.
Note: The asterisk (*) symbol indicates mandatory fields.	

4. To save the alert to the AppViewX system, click **Add**.
   The saved details are displayed in the table shown at the bottom of the screen.

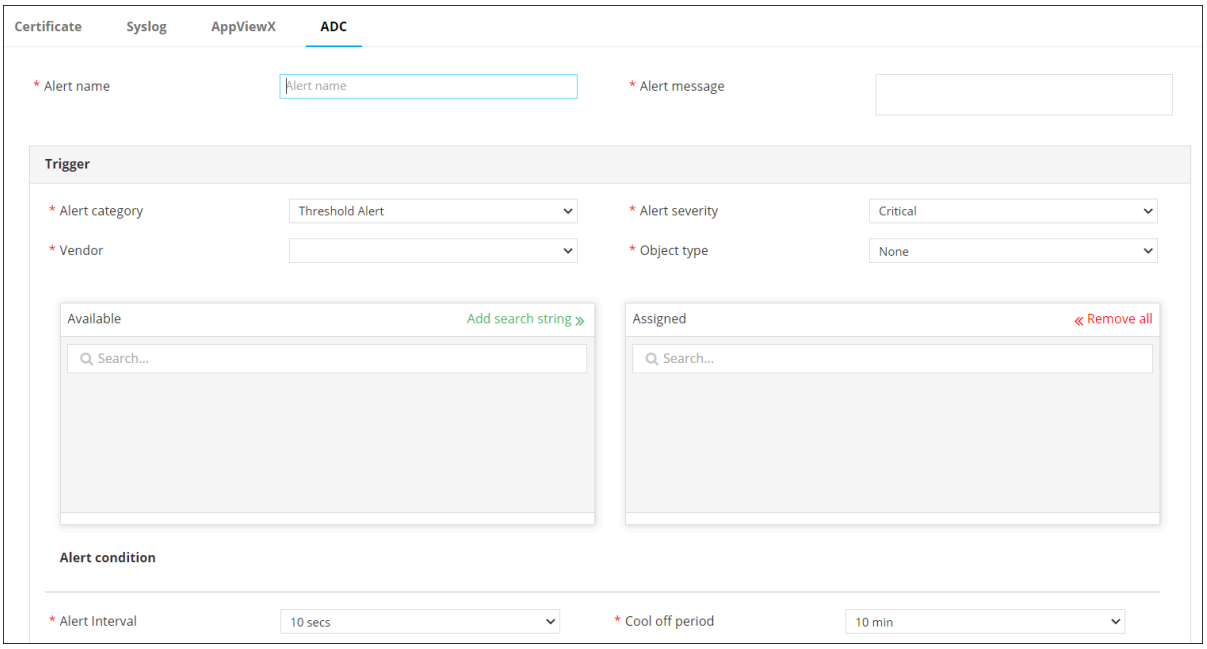
Configuring ADC Alerts

To configure ADC alerts:

1. On the **Alert :: All** page, from the top-right corner of the screen, click **(Settings)** icon.
   The **Settings :: Certificate** page is displayed with the **Certificate** tab open by default.

2. To configure ADC alerts, click **ADC**.

   The **Settings :: ADC** page is displayed.



3. Enter the following details:

Field descriptions for ADC alerts

Field	Description
***Alert name**	Enter the name you want to give this alert.
***Alert message**	Enter the message that will be displayed with this alert.

Note: The asterisk (*) symbol indicates mandatory fields.

4. In the **Trigger** section, enter the following details:

Field descriptions for Trigger

Field	Description
***Alert category**	From the drop-down menu, select one of the following alert categories: • Threshold alert • Application alert • Device alert.

Field	Description
***Alert severity**	From the drop-down, from the options given below, select a severity for the alert: • Critical • Fatal • Major • Minor • Notification.
Vendor	From the drop-down menu, select the vendor whose device or devices you want to set an alert for.
Object type	From the drop-down menu, select the vendor object that you want to set an alert for. **Note:** The contents of this field will vary depending on the vendor selected.
Detail contains	**Note:** This field is applicable only for the **Device Alert** category.
Available	Depending on the **Object type** and **Vendor** selected, a list of all available ADC objects or devices is displayed here. To add an object/device to the alert, click » for that object/device.
Add search string	Instead of adding devices manually, AppViewX lets you automatically assign all existing devices or objects that match your criteria. To do this: a. In the **Available** section, in the **Search** field, enter the search criteria. b. Click **Add search string**. **Note:** The benefit of using a search string rather than selecting devices manually is that the search string continues to work in the background and auto-assigns all new devices that match the search criteria.

Field	Description
Assigned	To add an object to the Assigned column, click the check box corresponding to that object.

5. In the **Alert condition** section, enter the following details:

Field descriptions for Alert condition

Field	Description
***Alert interval**	From the drop-down menu, from the following options, select how often you want the system to check for breaches of the threshold levels that you are about to define: • 10 seconds • 20 seconds • 30 seconds • 40 seconds • 50 seconds • 60 seconds.
***Cool off period**	From the drop-down menu, from the following options, select how much time the system should wait before sending another alert about a continuing threshold breach: • 10 minutes • 20 minutes • 30 minutes.

Note: The asterisk (*) symbol indicates mandatory fields.

Note: This section is applicable only for the Threshold Alert category.

6. In the **Statistics** section, define the conditions that will generate an alert by selecting values in the Statistics, Operator, and Value fields.
   - To add more than one Statistics conditions, click **(Add)** icon.
   - To delete a condition, click **(Delete)** icon.
7. In the **Action** section, to send the syslog alert as an email, execute the steps for configuring SMTP for email alerting.

8. Enter the following details:

Field descriptions for Action

Field	Description
Email configuration	To send the syslog alert as an email, select this check box.
***Email address**	To send the syslog alert as an email, enter the email address to which this specific syslog alert will be sent. **Note:** Separate multiple email addresses with a comma.
Subject	To send the syslog alert as an email, enter a subject line.
Note: The asterisk (*) symbol indicates mandatory fields.	

9. To use the Simple Network Management Protocol (SNMP) to send the alert, enter the following details:

Field descriptions for Simple Network Management Protocol

Field	Description
SNMP configuration	To use the Simple Network Management Protocol for sending the alert, select this check box.
***Destination IP**	Enter the destination IP address for the alert.
***Version**	From the drop-down menu, from the following options, select the SNMP version to be used: • V1 • V2.
***Port**	Enter the port number to be used for the alert.
***Community string**	Enter the community string for the alert. The community string is similar to a user ID or password that allows users access to the requested information on the device.
Note: The asterisk (*) symbol indicates mandatory fields.	

10. To save the ADC alert configure above, click **Add**.
    The saved details are displayed in the table shown at the bottom of the screen.

Editing Alerts

To edit an alert:

1. Go to the **Alert :: All** page and select the relevant tab for the alert you want to edit.
2. Scroll to the bottom of the page for the table that records all the alerts that have been configured for that category.
3. From the table, to select the alert you want to edit, select the check box corresponding to that alert.
4. From the top-right corner of the screen, click  **(Edit)** icon.
5. The fields are populated with the details of the alert.
6. Update the required fields and click **Update**.

Deleting Alerts

To delete an alert:

1. Go to the **Alert :: All** page and select the relevanr tab for the alert you want to delete.
2. Scroll to the bottom of the page for the table that records all the alerts that have been configured for that category.
3. From the table, to select the alert you want to delete, select the check box corresponding to that alert.
4. From the top-right corner of the screen, click  **(Delete)** icon.
5. In the **Confirmation** dialog box, click **Yes**.

Searching for Alerts

AppViewX lets you search for alerts in two ways:

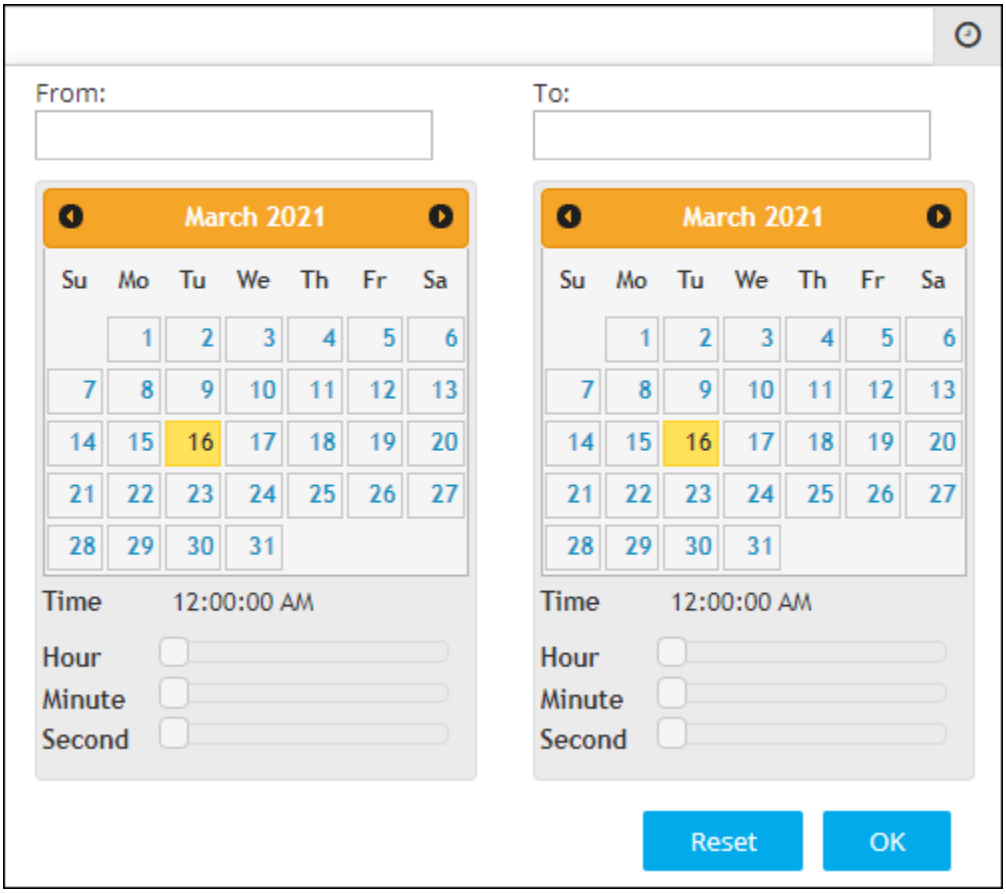
- Based on a timestamp
- Based on the values recorded for each alert.

- Based on a Timestamp
- Based on the Values Recorded for each Alert

Based on a Timestamp

To search for alerts based on a timestamp:

1. From the **Search** field on the **Alert** page, click **(Clock)** icon.
   Widgets to select the date and time are displayed.

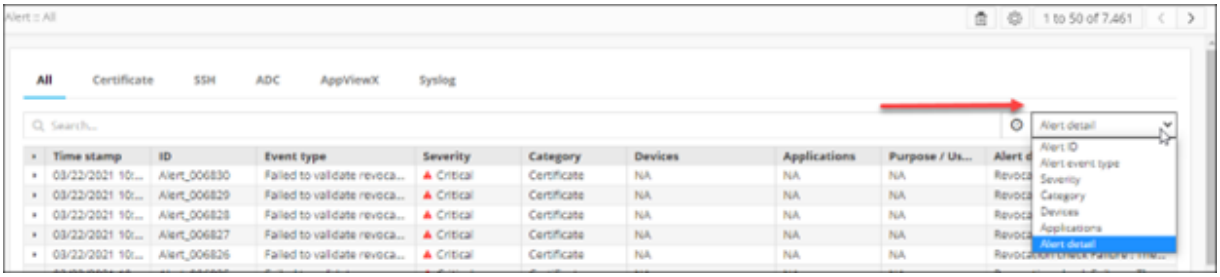


2. To select a date range, in the **From** and **To** fields, select the required dates.
3. To set a time, use the **Hour**, **Minute**, and **Second** slider controls.
4. Click **OK**.
5. The page is updated to display alerts from the selected timestamp.

> **Note:** To view alerts from a specific date to the current date, select only the From date. When the To field is left blank, by default, it is set to the current date.

Based on the Values Recorded for each Alert

1. From the drop-down menu in the **Search** field, select the category for searching alerts. For example, to search for alerts with a specific alert ID, from the drop-down menu, select **Alert ID**.



2. In the **Search** field , enter the search value. For our example, in the Search field, enter the required alert ID.

   The page is updated to display alerts that fulfil the search criteria.

Data Retention/Purging Alerts

- Accessing Data Retention/Purging Settings
- Purging Alerts

Accessing Data Retention/Purging Settings

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **OBSERVE & EXPLORE**, select **Data Retention**. The **Settings :: Purging** page is displayed with the **Alert** tab open by default.	1. From the main navigation menu, click **Settings**. 2. On the **Settings** page, from the left menu, select **General** > **Purging**. The **Settings :: Purging** page is displayed with the **Alert** tab open by default.

Note: For more information on how to switch between menus, click here.

Purging Alerts

With a large number of alerts being recorded each day, a system can soon become vulnerable to threats like compromise of confidential information, a surplus of outdated information, and so on. For security reasons, regular purging of old data comes as a highly recommended practice.

To enable purging of alert records:

1. On the **Settings :: Purging** page, enter the following details:

Field descriptions for Purging alert

Field	Description
***Alert Purge Duration (in Days)**	Enter the number of days, the interval, after which the alerts will be purged.
***Maximum Alert count**	Enter the maximum number of the most recent alerts that have to be retained. For example, if you set this value to 10,000, all alerts after the most recent 10,000 alerts will be purged.

Note: The asterisk (*) symbol indicates mandatory fields.

Note: Excess alerts will be purged even if the maximum alert count is exceeded before the next purging cycle is scheduled.

2. Click **Save**.

Syslog Reception Settings

- Accessing Syslog Reception Settings
- Syslog Reception

Accessing Syslog Reception Settings

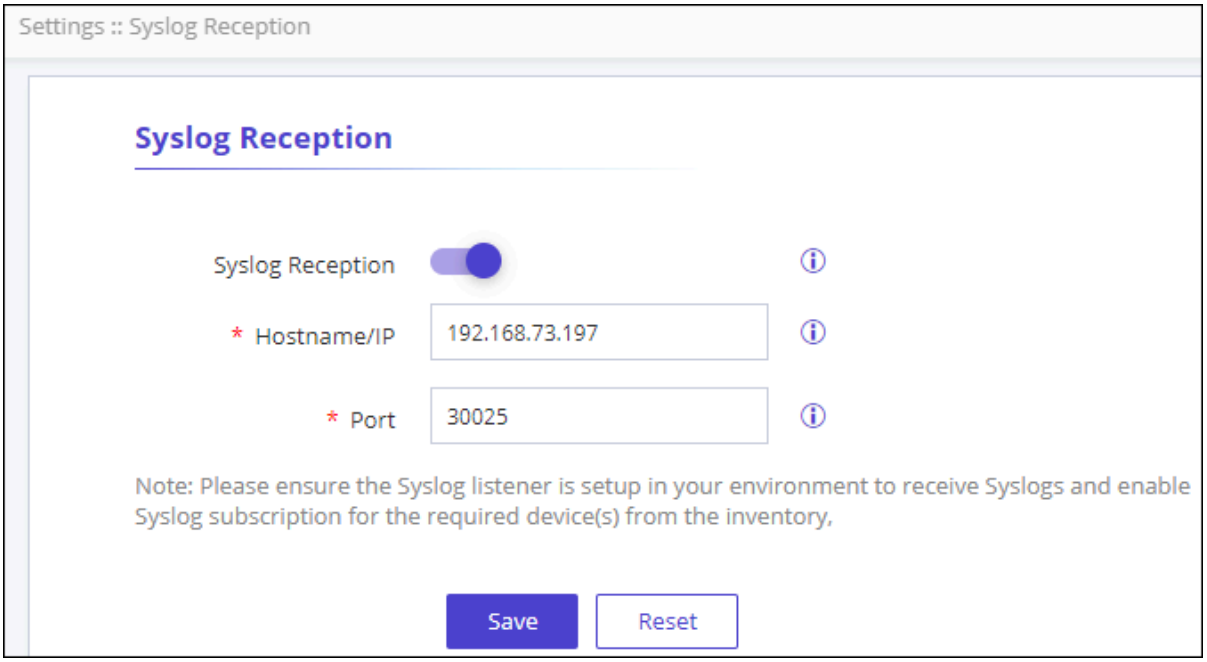
New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **OBSERVE & EXPLORE**, select **Syslog Reception**. The **Settings :: Syslog Reception** page is displayed by default.	1. From the main navigation menu, click **Settings**. 2. On the **Settings** page, from the left menu, select **General** > **Syslog Reception**. The **Settings :: Syslog Reception** page is displayed by default.
Note: For more information on how to switch between menus, click here.	

Syslog Reception

With Syslog reception, changes in ADC devices are dynamically updated in AppViewX, which supports Syslog in ADC.

Note: Please ensure the Syslog listener is setup in your environment to receive Syslogs and enable Syslog subscription for the required device(s) from the inventory.

1. On the **Settings :: Syslog Reception** page, enter the following details:

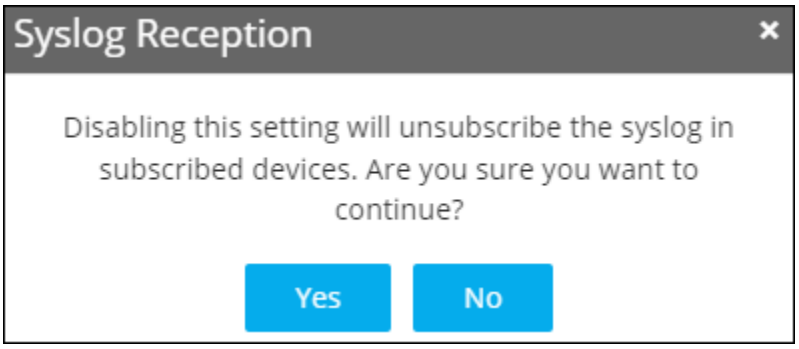


Field descriptions for Syslog Reception

Field	Description
Syslog Reception	Enable the toggle to enable Syslog reception for real time configuration updates from the subscribed devices.
***Hostname/IP**	Enter the Hostname or IP address of the Syslog listner. Incase of a multi node or multi cloud connector setup, provide virtual IP(VIP). **Note:** This field is displayed when the **Syslog Reception** toggle is enabled.
***Port**	The default port value is set to 30025. However, if a virtual IP or host is used, the port can be customized. **Note:** This field is displayed when the **Syslog Reception** toggle is enabled.
Note: The asterisk (*) symbol indicates mandatory fields.	

2. Click **Save**.
   If the Syslog reception is enabled, the following header notification is displayed on the top of your screen in green.

3. To disable **Syslog reception**, disable the toggle and click **Save**.
   The **Syslog Reception** pop-up is displayed.



4. Click **Yes** to continue.
   If the Syslog reception is disabled, the following header notification is displayed on the top of your screen in green.

Managing Licenses

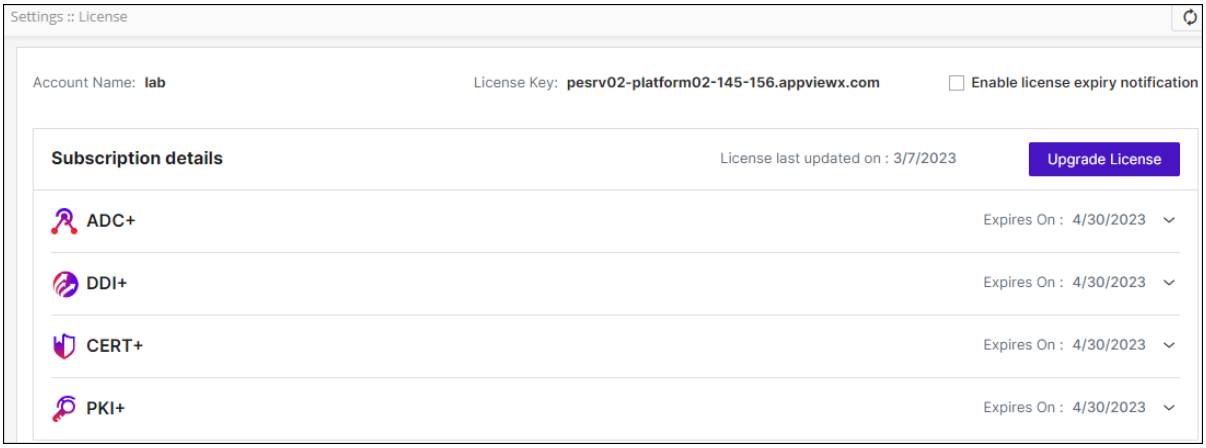
Note: AppViewX blocks the usage/upload of the old license. If an organization uploads an old license, an error message is displayed. **LICENSE_ERROR_037: Unsupported version of the license file. Please contact AppViewX support**. The AppViewX support team will help with the new and latest supported versions of the license.

Note: AppViewX blocks the usage of the product if the license has expired. If an organization exceeds the threshold of license (maximum number of ADC+ objects, CERT+ certificates, and/or PKI+ Certificates allowed), a warning is issued as a reminder. A pop-up warning is issued for both scenarios.

Accessing the License Page

New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **SYSTEM ADMINISTRATION**, select **License**. The **Settings :: License** page is displayed with the **License** tab open by default.	1. From the main navigation menu, click **Settings**. 2. On the **Settings** page, from the left menu, select **General** > **License**. The **Settings :: License** page is displayed with the **License** tab open by default.
Note: For more information on how to switch between menus, click here.	

The **Settings :: License** page shows the following details.



Note: The License page screen displays details of those license that are purchased or subscribed by the user. The following image shows all products under the **Products** section ADC +, DDI+, CERT+, KUBE+, PKI+.

Descriptions of License section

License Detail	Description
Account Name	Displays the associated account name.
License Key	Displays the License key details of the user. The key is generated by the customer perspective. Using which License Key of "16 digit Alphanumeric" value is generated by the sales team. Only License Key generated with installation key can be applied in the respective instance of the product. **Note:** Consider only the license key which is provided by the sales team.
Enable license expiry notification	This option can be enabled by adding the Email addresses to get the license expiry related notifications from AppViewX.  **Note:** Multiple Email addresses can be added using comma (,). The following license expiry notifications are sent to the email address: 1. **License expiry alert**: Your AppViewX license for the products [ADC+, DDI +, CERT+, KUBE+, PKI+] is about to expire. Kindly upgrade the license. This notification is sent to the user two days before the license expires. 2. **License limit reaching**: Your AppViewX License usage limit subscribed for the products [ADC+, DDI+, CERT+, KUBE+, PKI+] is about to be exceeded. Kindly upgrade the license. 3. **License limit reached**: Your AppViewX License usage limit subscribed for the products [ADC+, DDI+, CERT+, KUBE+, PKI+] has been exceeded. Kindly upgrade the license.
Subscription details	This includes the details of licenses of AppViewX products subscribed by the user.

Descriptions of License section (continued)

License Detail	Description
License last updated on	Displays the date on which the license was last updated.
Product Name	This includes the details of subscribed licenses of all AppViewX products.
Expires on	Date of expiry of the respective products.
ADC+	
Nodes	All the ADC devices (Independent devices, Controllers, Nodes within controllers) that are onboarded in the inventory.
Firewall Devices 	Devices integrated with firewall network topology.
Objects	All the ADC Applications (Unique GTM WideIPs, LTM VIPs) discovered from the onboarded ADC devices.
DDI+	
Managed Domains	Each DDI+ license subscription allows the user a number of managed domains that can be used. The number displays DDI+ managed domains currently in use.
CERT+	
Managed Server Certificates Instances	All the server certificate instances managed on server.
Managed Device Certificates Instances	All the device certificate instances managed on device.
Managed Certificates Instances	All the certificate instances in the certificate inventory with Managed Status.
Monitored Certificates Instances	All the certificate instances in the certificate inventory with Monitored Status.
PKI+	
Certificates Issued	Certificates issued are the total number of certificates which includes the number of certificates issued and all CAs created in PKI.

Descriptions of License section (continued)

License Detail	Description
	Note: The certificate count begins from the day the project is initialized in Google Cloud Platform (GCP)and is maintained for a year from that date. The count is reset annually.
Total CA(s)	Total CA is Number of CA's created from AppViewX. Each PKI+ license subscription allows the user a number of total CA's using this license. This is the number of total CA's used.

• License Alerts

License Alerts

Following are the system alerts which indicates the product usage limit.

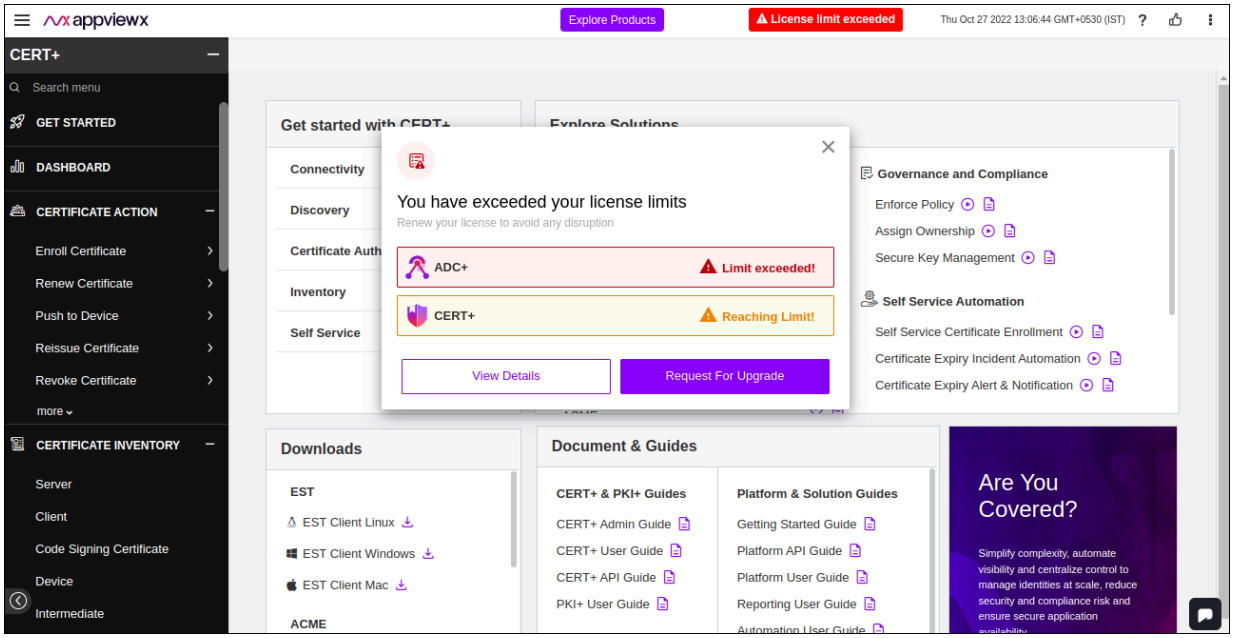
- **Reaching Limit!**

  If the usage reaches 90% of the threshold limit, then **“Reaching Limit!”** alert will be displayed.

- **Limit exceeded!**

  If the usage exceeds the threshold limit, then **“Limit exceeded!”** alert will be displayed.

• You will see a header alert message while logging In, if the license limit is exceeded.



Upgrading Licenses for On-prem

Note: AppViewX blocks the usage of the license if the license has expired. If an organization exceeds the threshold of license (maximum number of ADC+ objects, CERT+ certificates, and/or PKI+ Certificates allowed), a warning is issued as a reminder. A pop-up warning is issued for both the scenarios.

To upgrade a license:

1. On the **Settings :: License** page, to upgrade a license, from the top right corner of the screen, click **Upgrade License**.
   A screen that lets you upload the license file is displayed.
2. In the **Upload License** dialog box, to upload a license file, click **Browse**.

   Note: License files only in the following formats can be uploaded: .txt and .zip.

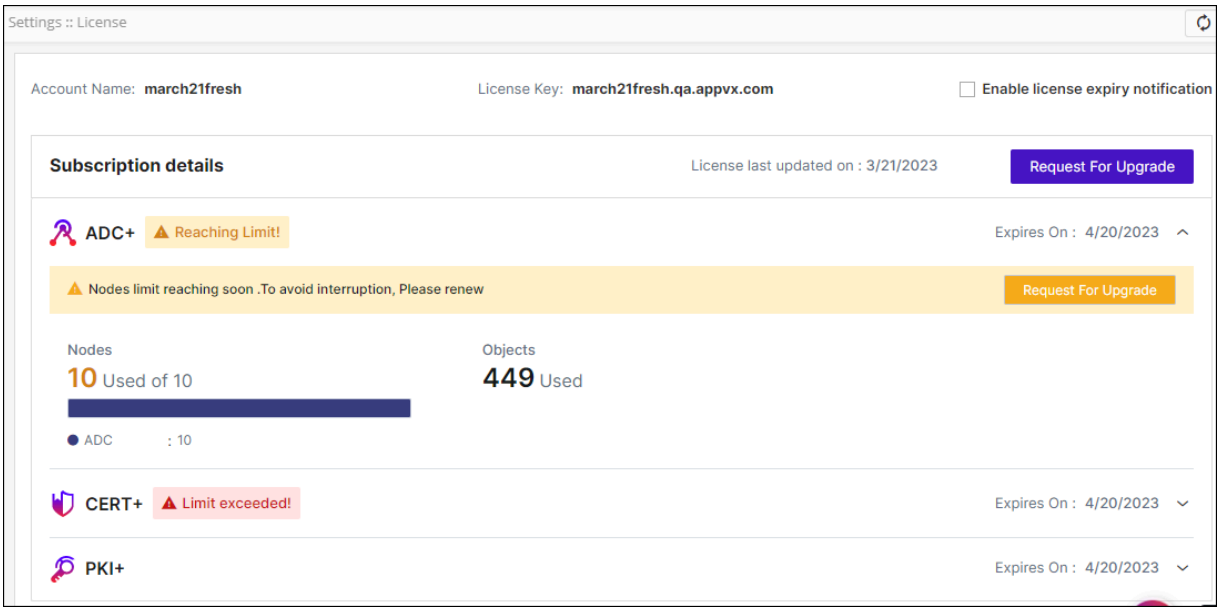
3. Go to the location of the license file, select the file, and click **Open**.
4. Click **Upload**.

Upgrading Licenses for SaaS

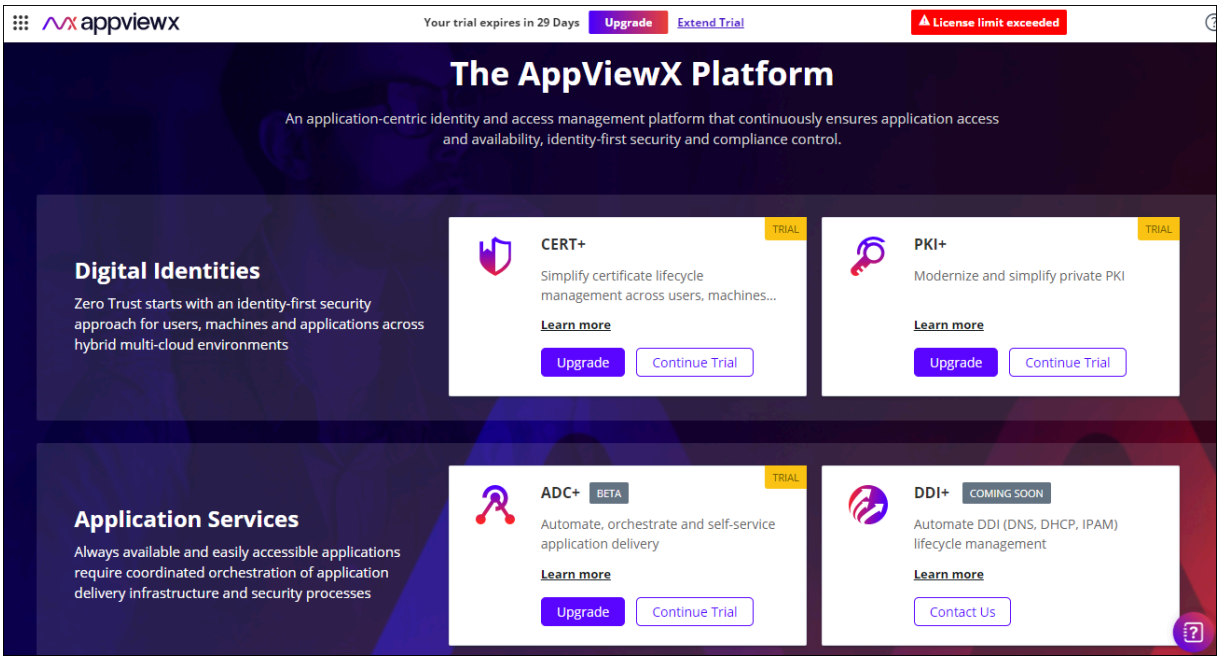
Note: AppViewX blocks the usage of the license if the license has expired. If an organization exceeds the threshold of license (maximum number of ADC+ objects, CERT+ certificates, and/or PKI+ Certificates allowed), a warning is issued as a reminder. A pop-up warning is issued for both the scenarios.

To upgrade a license:

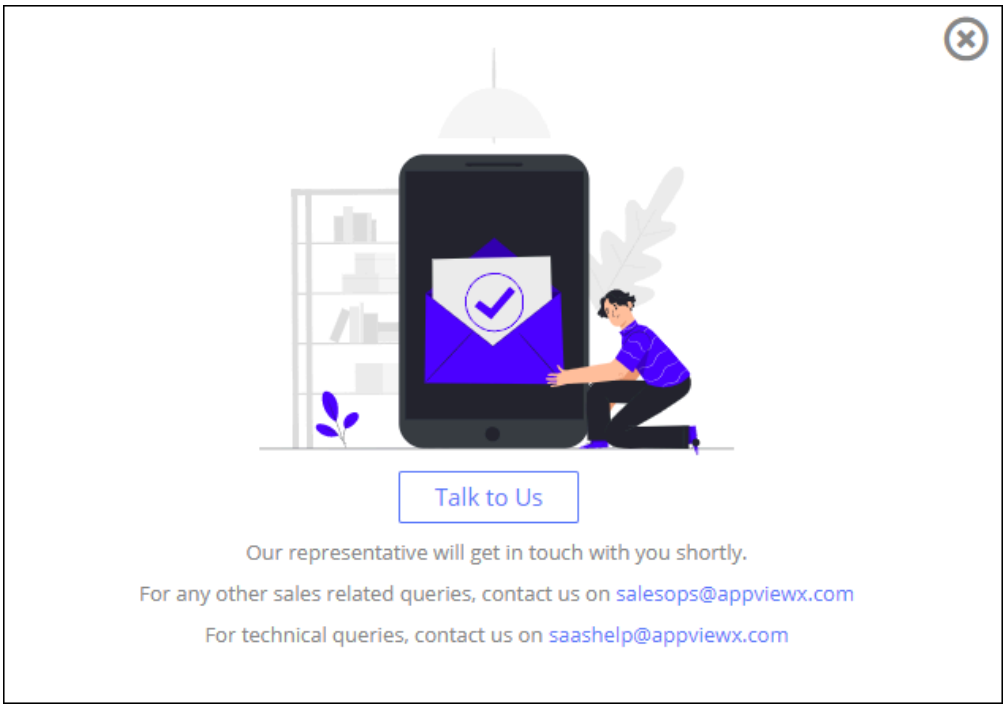
1. On the **Settings :: License** page, to upgrade a license, from the top right corner of the screen, click **Request For Upgrade**.



2. Click **Upgrade**, on the corresponding product to request for upgrade.



3. The **“Talk to us”** page will be displayed. You can click that and submit the upgrade request. Our representative will get in touch with you shortly.



Customizing the AppViewX User Interface

AppViewX lets you create a custom theme by customizing the following UI elements:

- Logo
- Screenheader
- Login screen
- Email attachment representation.

Accessing Themes and Personalization Settings

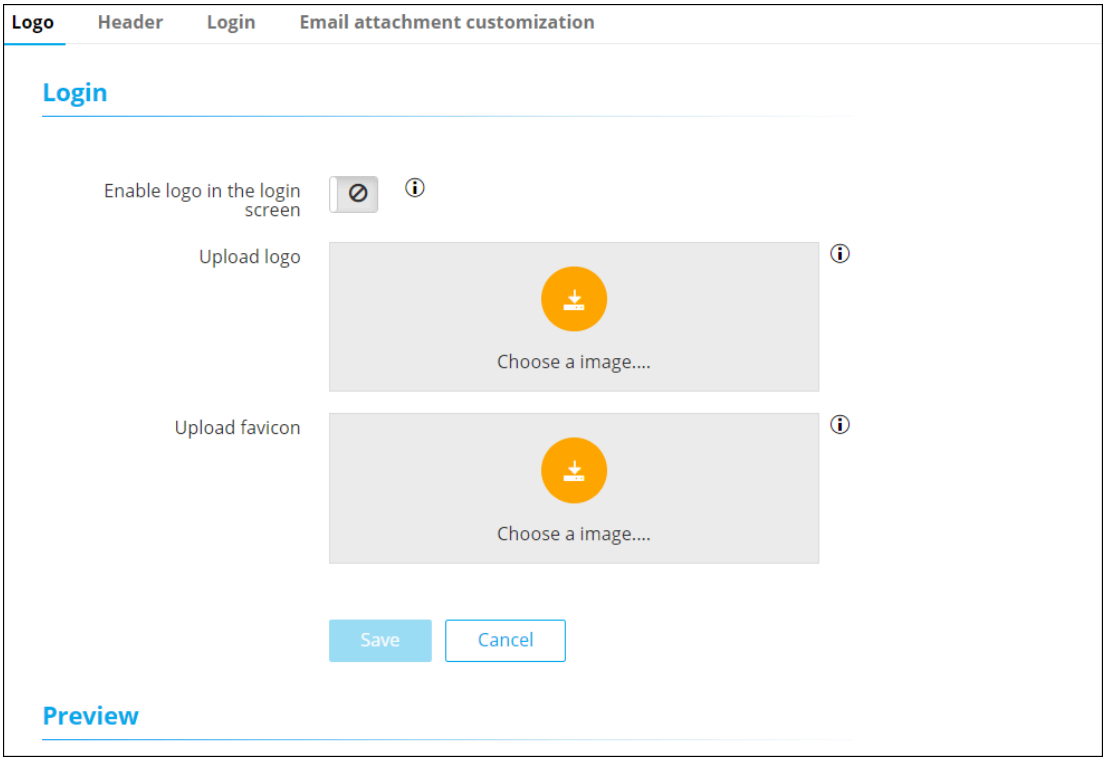
New Menu	Old Menu
In the **Platform** module, from the navigation pane on the left, under **SYSTEM ADMINISTRATION**, select **Themes and Personalization**. The **Settings :: Theme** page is displayed with the **Logo** tab open by default.	1. From the main navigation menu, click **Settings**. 2. On the **Settings** page, from the left menu, select **General** > **Theme**. The **Settings :: Theme** page is displayed with the **Logo** tab open by default.
Note: For more information on how to switch between menus, click here.	

Customizing the Logo

You can replace the AppViewX logo with the logo of your organization.

To add a custom logo:

1. On the **Settings :: Theme** page, under the Logo tab, enter the **Login** section details:



Field descriptions for Login section

Field	Description
Enable logo in the login screen	To display your organization's logo on the AppViewX screen, turn on this toggle. **Note:** If this toggle key is disabled, AppViewX's default theme settings are applied.
Upload logo	**Note:** This field is enabled only when the Enable logo in the toggle screen toggle is turned on. To choose a logo image: a. Click  **(Upload)** icon. b. From Windows Explorer, navigate to the location of the logo image, select the image, and click **Open**.

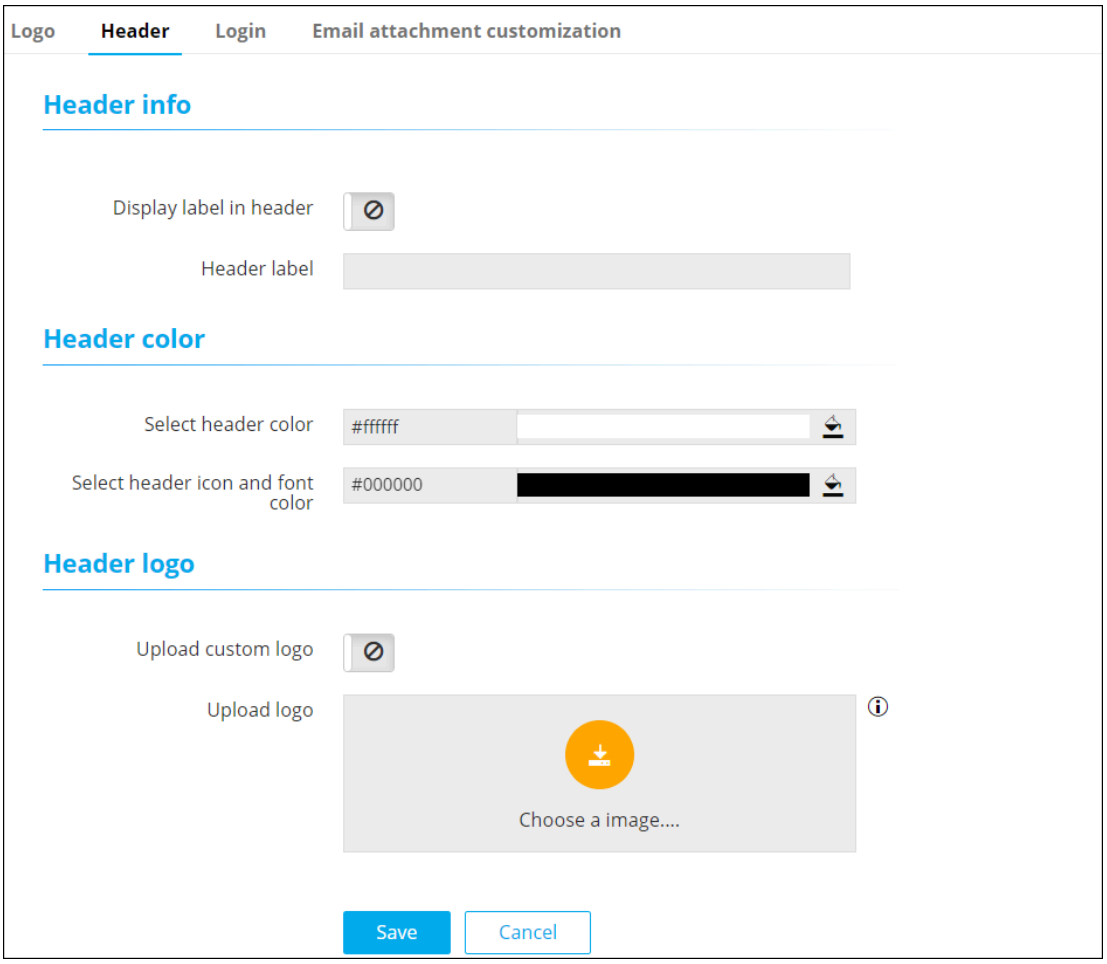
Field	Description
	Note: • Image formats allowed for upload: **.png** and **.svg** • Maximum image resolution allowed: 865 X 185 (width X height) • Image size: < 5 MB • Recommended image dimensions: 175 X 37 (width X height) c. In the **Confirmation Message** dialog box, click **Yes**.
Upload favicon	**Note:** This field is enabled only when the Enable logo in the toggle screen toggle is turned on. To choose a favicon image: a. Click  **(Upload)** icon. b. From Windows Explorer, navigate to the location of the logo image, select the image, and click **Open**. **Note:** • Image formats allowed for upload: **.png** • Maximum image resolution allowed: 64 X 64 (width X height) • Image size: < 5MB c. In the **Confirmation Message** dialog box, click **Yes**.

2. In the **Preview** section, view a preview of the login screen after your custom logo and favicon have been uploaded.
3. To apply the changes, click **Save**.

Customizing the Screen Header

To customize the screen header:

1. On the **Settings :: Theme** page, to customize the screen header, click **Header** tab, enter the **Header Info**, **Header color** and **Header logo** section details:



Field descriptions for Header Info section

Field	Description
Display label in header	To display custom header text, turn on this toggle.
Header label	Enter the custom header text. **Note:** This field is enabled only when the **Display label in header** toggle is turned on.

Field descriptions for Header color section

Field	Description
Select header color	To set a color for the header text: a. Enter the hex code of the required header color. **OR** b. To select a color, click  .
Select header icon and font color	To set a color for the header icon and the font: a. Enter the hex code of the required color. **OR** b. To select a color, click  .

Field descriptions for Header logo section

Field	Description
Upload custom logo	To insert a custom logo image in the header, turn on this toggle.
Upload logo	**Note:** This field is enabled only when the Upload custom logo toggle is turned on. To upload a logo image: a. Click  **(Upload)** icon. b. From Windows Explorer, navigate to the location of the image, select the image, and click **Open**.

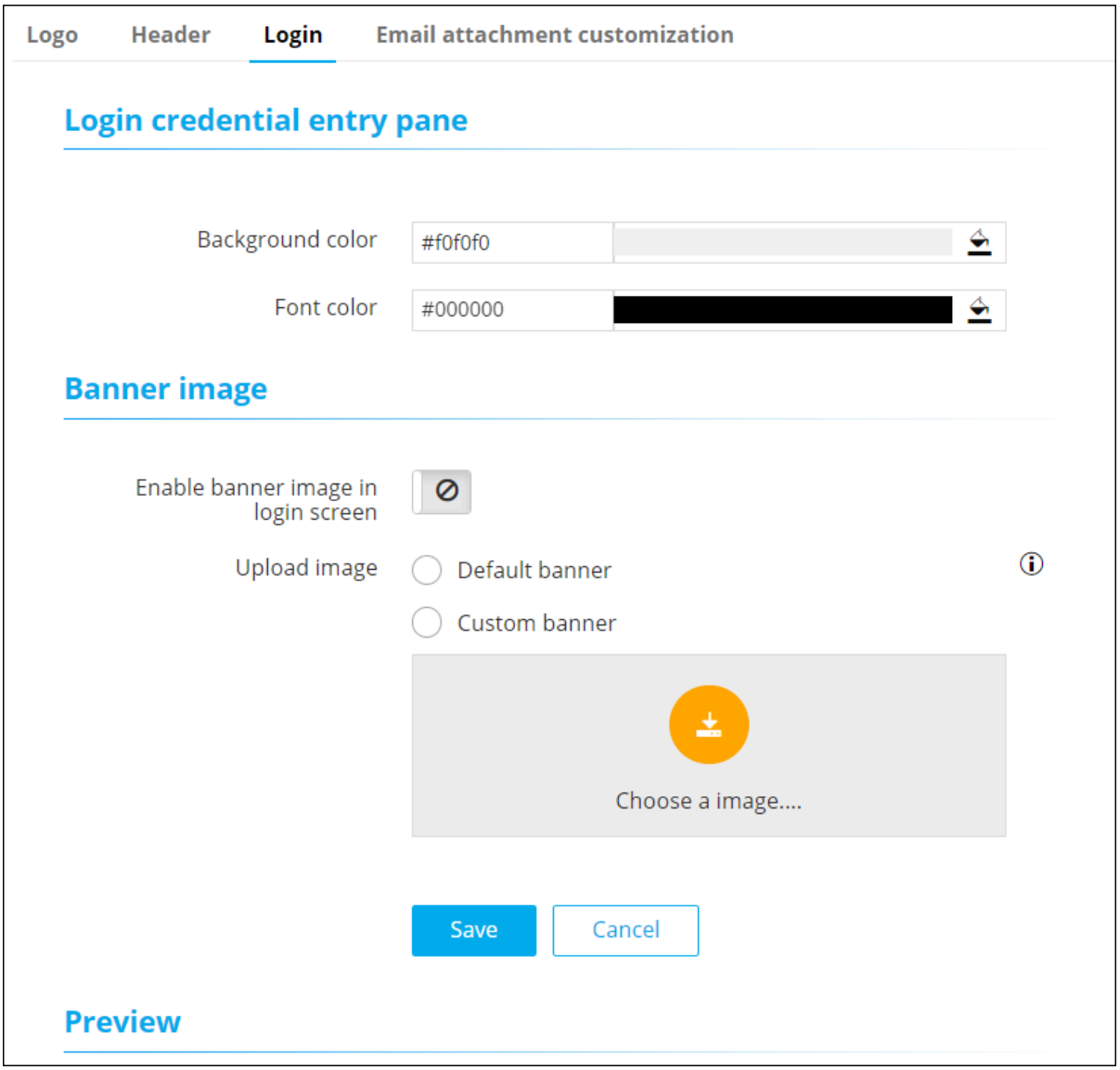
Field	Description
	Note: • Image formats allowed for upload: **.png** and **.svg** • Maximum image resolution allowed: 865 X 185 (width X height) • Image size: < 5 MB • Recommended image dimensions: 175 X 37 (width X height) c. In the **Confirmation Message** dialog box, click **Yes**.

2. In the **Preview** section, view a preview of your header customization.
3. To apply the changes, click **Save**.

Customizing the Login Screen

To customize the login screen:

1. On the **Settings :: Theme** page, to customize the login screen, click the **Login** tab, enter the **Login credential entry pane** and **Banner image** section details:



Field descriptions for Login credential entry pane section

Field	Description
Background color	To set a background color for the login screen: a. Enter the hex code of the required background color. **OR** b. To select a color, click  .

Field	Description
Font color	To set a font color for the text on the login screen: a. Enter the hex code of the required font color. **OR** b. To select a color, click  .

Field descriptions for Banner image section

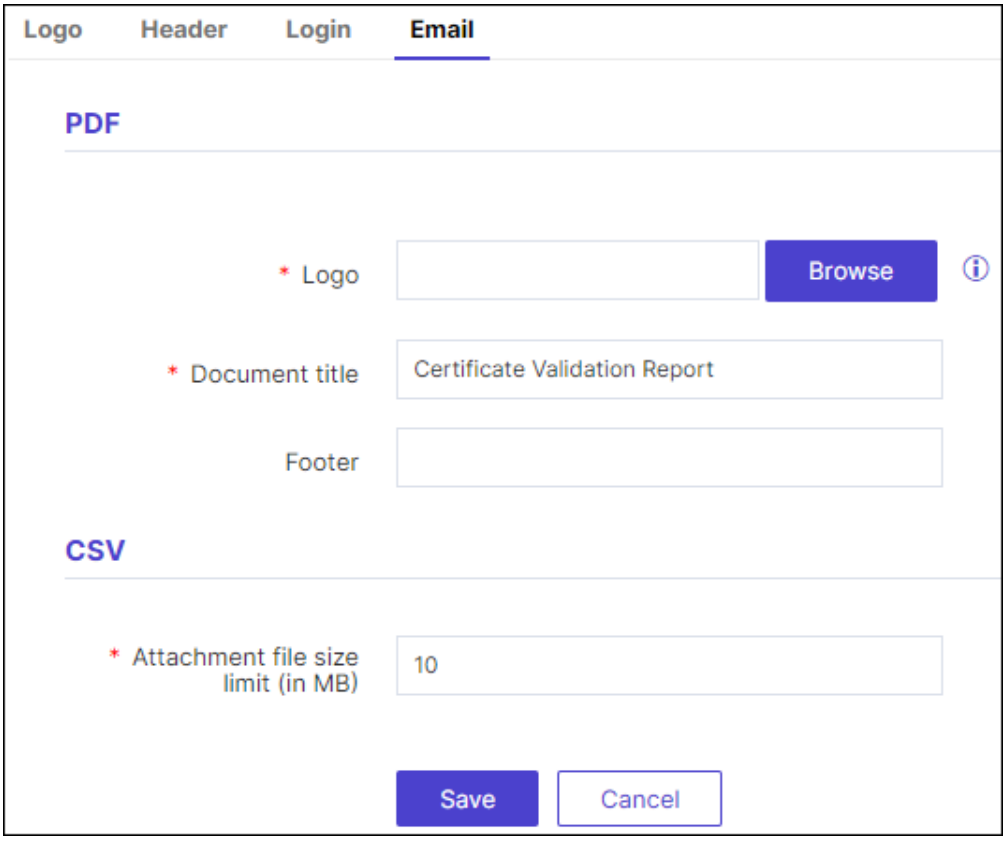
Field	Description
Enable banner image in login screen	To display a banner image on the login screen, turn on this toggle.
Upload image*	**Note:** This field is enabled only when the **Enable banner image in login screen** is turned on. To upload a banner image: a. Click  . b. From Windows Explorer, navigate to the location of the image, select the image, and click **Open**. **Note:** • Image formats allowed for upload: **.jpg**, **.jpeg**, and **.png** • Recommended image resolution: 500 X 500 (width X height) • Image size: < 5 MB c. In the **Confirmation Message** dialog box, click **Yes**.

2. In the **Preview** section, view a preview of your customization for the login screen.
3. To apply the changes, click **Save**.

Customizing the Email

To customize the cosmetics of how email are represented:

1. On the **Settings :: Theme** page, click the **Email** tab and enter the **PDF** section details:



Field descriptions for PDF section

Field	Description
***Logo**	To upload a logo image for the attachment: a. Click **Browse**. b. Navigate to the location of the image, select the image, and click **Open**. **Note:** The image size must be less than 50 KB.
***Document title**	Name to be assigned to the PDF when it is downloaded.
Footer	Footer content to be added to the PDF.
**: Mandatory fields*	

2. In the **CSV** section, enter the **Attachment file size limit (in MB)**.

Note: This is a mandatory field.

3. To apply the changes configured above, click **Save**.
4. For Email Template section, click here.

• Email Template

Email Template

Email template involves customizing the design and content to align with specific communication needs, ensuring a consistent and professional appearance for outgoing emails.

In the **Email Template** section, follow these steps to create a new email template:

1. Click **+ Create new**.
   The **Email Template Config** page is displayed.
2. Enter the **Email Template Config** section details:

Field descriptions for Email Template section

Field	Description
***Name**	Provide a unique name for the email template.
Description	Explain or provide information about the email template.
Upload logo	To choose the logo. a. Click **Browse**. b. From Windows Explorer, navigate to the location of the logo image, select the image, and click **Open**. **Note:** • Image formats allowed for upload: **.png** and **.svg** • Maximum image resolution allowed: 865 X 185 (width X height) • Image size: < 5 MB • Recommended image dimensions: 175 X 37 (width X height).

Field	Description
Upload banner	To choose the banner. a. Click **Browse**. b. From Windows Explorer, navigate to the location of the logo image, select the image, and click **Open**. **Note:** • Upload an image in the **.png / .svg / .jpeg / .jpg** format only • The maximum resolution of the image should be 700 x 200 (width x height) • The size of the image must be less than 5 MB • Recommended image size is 700 x 200 (width x height).
Body	Add the body content before or after the "[[BodyContent]]" and do not remove the "[[BodyContent]]" string. The content before and after the body content can remain the same, while the content added within the string is dynamic and can be adjusted based on the requirements.
Signature	Add signature content in the email, serving as a verification mark for authenticity.
Footer Message	Add the Footer Message content to the email.
**: Mandatory fields*	

3. In the **Preview** section, view a preview of your customization for the email template.
4. Click **Create**.
   The **Email Template** will be generated and displayed in the Templates section.

What to do next:

- **Edit** an email template by hovering over it, click **(Edit)** icon, making the necessary changes, and then click **Update**.
- **Clone** an email template.by hovering over it, click **(Clone)** icon, making all the necessary changes, and then click **Create**.
- **Delete** an email template.by hovering over it, click **(Delete)** icon and then click **Delete**.

Glossary

Definitions of common terms used in guide

Term	Definition
HSM	An HSM (Hardware Security Module) is a piece of hardware and associated software or firmware that usually resides in a PC or server and provides at least the minimal cryptographic functions. These functions include (but are not limited to) encryption, decryption, key generation, and hashing.
LDAP	The Lightweight Directory Access Protocol (LDAP) is an authentication protocol to validate a user's credentials, entered in an application, against the credentials stored in the Active Directory database.
PAM	Privileged Access Management (PAM) is the practice of managing users/ devices/applications that have elevated access to an organization's most confidential and critical resources.
RADIUS	The Remote Authentication Dial-In User Service (RADIUS) protocol is a networking protocol that provides centralized authentication, authorization, and accounting management.
RBAC	Role and Resource-Based Access Control (RBAC) is a method of restricting AppViewX functions, network resources that can be managed and monitored in AppViewX based on the roles of individual users within an enterprise.
Resource	All the devices and objects that are configured within AppViewX are termed as Resources. Resources can be assigned to a user group. Users within a user group will inherit resources assigned to that group. User groups can be assigned more than a resource.
Role	A set of permissions to execute specific tasks in the application is termed as Roles in AppViewX. Roles can be assigned only to a user group. Users within user groups will inherit role permissions assigned to that group. User groups can be assigned more than one role.
SAML	The SecurityAssertion Markup Language (SAML) protocol is used for authenticating and authorizing user identity for Single Sign On (SSO) services.
TACAS	The Terminal Access Controller Access Control System (TACACS) authentication is used to validate users requesting remote access.

Definitions of common terms used in guide (continued)

Term	Definition
User	A user is an individual who has access to AppViewX using a unique username and password maintained internally or by an external enterprise server such as Active Directories (AD).
User Group	user group is a set of individual users assigned with the same roles and resources. You can associate one or more roles and resources to a user group. Users within that user group are granted the role and resource permissions.

Chapter 2: Platform API Guide

The AppViewX Platform is a module that lets you enable general configuration settings such as authentication, authorization, and integration of external services like log forwarding, HSM integration, SMTP configuration, and so on. These general configuration settings are applicable to all AppViewX subsystems such as ADC, CERT+, Security+, Visual Workflow, and so on.

Overview

The AppViewX Platform is a module that lets you enable general configuration settings such as authentication, authorization, and integration of external services like log forwarding, HSM integration, SMTP configuration, and so on. These general configuration settings are applicable to all AppViewX subsystems such as ADC, CERT+, Security+, Visual Workflow, and so on.

An API enables users to programmatically transfer data in and out of the AppViewX subsystems. With access to RESTful AppViewX APIs, you can leverage the raw potential of AppViewX. It provides a powerful way to channel the data into native business applications. This document comprises of module-wise APIs used in the AppViewX Platform.

Restful HTTPS Requests

HTTP GET

GET requests, retrieve resource representation/information only and not to modify it.

HTTP POST

POST APIs create new subordinate resources. For example, a file is subordinate to a directory containing it or a row is subordinate to a database table. In terms of REST, POST methods are used to create a new resource into the collection of resources.

HTTP PUT

PUT APIs are used to update existing resources (if a resource does not exist then API may decide whether to create a new resource or not).

HTTP DELETE

DELETE APIs are used to delete resources (identified by the Request-URI).

Description of Server Responses

HTTP Code	Description	Response Message
200	OK	The request was successful (some API calls may return 201 instead).
400	Bad Request	The request is not understood or required parameters are missing.
401	Unauthorized	Authentication failed or the user doesn't have permissions for the requested operation.
403	Forbidden	Access denied.
404	Not Found	Resource not found.
429	Too many requests	The number of requests to the service has crossed the threshold.
503	Service unavailable	The client cannot communicate with the service.
504	Gateway timeout	The given request has exceeded the expected time.

This guide explains how to use the AppViewX API to perform different functions. It includes descriptions, pointers to code samples, and request/response formats.

URI Scheme

- **Host :** {url}
- **BasePath :** /avxapi

- **Schemes :** HTTPS
- **URL :** https://{url}/avxapi

Types of Accounts in AppViewX

There are two types of accounts in AppViewX:

- **User Accounts**: These are used by actual users.
- **Service Accounts**: These are used by system services such as web servers, automation tools, and so on.

AppViewX recommends using a Service Account for accessing APIs from automation tools. Service Accounts are supported with oAuth standard for a more secure and standard way of accessing APIs.

Note: AppViewX supports both User Account and Service Account for accessing APIs.

Accessing API with User Account

For accessing APIs with a user account, you need to get the session ID by providing a username and password in the login API. This session ID can then be used for accessing other APIs.

Note: You can also use the username and password in all API calls instead of the sessionId. However, this is not recommended.

Retrieve session ID using login API

This API used to retrieve the session ID using the login API for secure authentication and access to system resources.

Before you begin

- Make sure you have valid login credentials (Username and Password) for accessing the system.
- You cannot use OAuth credentials (Client ID and Client Secret) for login.
- To access the APIs using the service token, use the API with the Service Account.

Request Structure

Endpoint	`/login`
Type	`POST`
Sample URL	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/login?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type	application/json
Request timeout period	15 minutes

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

	Description
username *Header*	(Mandatory) Use login name of the user. **Type:** String **Example:** "admin"
password *Header*	(Mandatory) Password for the username. **Type:** String **Example:** "AppViewX@123"
otp *Header*	(Mandatory only if MFA is enabled) If MFA is enabled, enter the OTP received on your registered email ID in the header. Multifactor authentication (MFA) is a security mechanism that requires users to provide two or more verification factors to gain access to a resource If MFA is enabled, and you try to login with only the username and password, you will get the following error upon execution of the API: **MFA is enabled. We have sent an OTP to your email ID: aaa********r@appviewx.com**. In this case, ensure that the OTP is included in the header and try logging in again. **Type:** String **Example:** "OTP : **609700**"
Content-Type *Header*	(Mandatory) The parameter should be set to `application/json` to specify the nature of the data in the payload. **Type:** String **Example:** "application/json"
gwsource *Query*	(Mandatory) Source from which the request is triggered. The values can be: • web • external

Input Parameters (continued)

	Description
	Type: String

Response Structure

- **Status Code:** 200 Ok
- **Message:** Login Successful
- **Headers:**
  - **Content-Type:** application/json

Response Parameters

Name	Description
response	The response contains the attributes needed to retrieve the session ID.
message	Success message or failure description in case of error.
appStatusCode	Application specific status code for the response. Will be non-null for failure response.
tags	More info in case of failure response.

Name	Description
status	Indicates the overall status of the response. The values can be: • SUCCESS • FAILURE
appStatusCode	An application-specific status code, if applicable.
statusDescription	Description of the status, if available.
sessionId	Unique identifier for the session.
lockDownPeriod	Number of login attempts remaining.
termsAccepted	
passwordExpiryMsg	
emailId	

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	NA	Login successful
400 Bad request	ACCT_AUTH_001	Username or password cannot be null or empty.
401 Unauthorized	ACC_AUTH_022	Login failed. Invalid credentials.
401 Unauthorized	ACC_AUTH_006	Login failed. Invalid credentials.

Sample Request/Response

Use Case

Log in to the application with a username and password.

Request URL

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/login?gwsource=external
```

Request Payload

```
{}
```

Sample Response


```
{
    "response": {
        "status": "SUCCESS",
        "appStatusCode": null,
        "statusDescription": null,
        "sessionId": "avx~~c73a4f56-f4ab-4cdf-aadf-6d90bf406077",
        "authCode": null,
        "lockDownPeriod": 15,
        "emailId": null,
        "termsAccepted": true,
        "passwordExpiryMsg": ""
    },
    "message": "Login successful.",
    "appStatusCode": null,
    "tags": null,
    "headers": null
}
```

Using Session ID for further API calls

The sessionID retrieved using the login API can be used in the header for making further API calls.

Before you begin

- Session ID is obtained from the login API.
- Ensure that the session ID is valid and has not expired.

Request Structure

Endpoint:	`/role`
Type:	`POST`
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/role?&gwsource=external` To understand the elements of the sample URL, click here.
Headers:	
Content-Type:	application/json

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Use session ID retrieved from login API, if username and password are not provided. **Type:** *String* **Example:** "sessionId": "ce7f1a14-2bf9-4e4a-89a8-bc780a255813"
gwsource *Query*	(Mandatory) Source from which the request is triggered. The values can be: • web • external **Type:** *String*
Payload *String*	(Mandatory) Input data for request body in application/json format. For payload details, see **Payload** section.

Payload

Name	Description
name *String*	(Mandatory) Name of the role to be added. **Example:** "role_1"
description *String*	(Optional) Description of the role to be added. **Example:** "Adding a new role"

Response Structure

- **Status Code:** 201 Created
- **Message:** Role added successfully
- **Headers:**
  - **Content-Type:** application/json

Response Parameters

Name	Description
response	Contains the response attributes for role added successfully.
message	Success message or failure description in case of error.
appStatusCode	Application specific status code for the response. Will be non-null for failure response.
tags	More info in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
201 Created	null	Role added successfully.
409 Conflict	ACCT_RO_002	Role name already exists
400 Bad Request	VALIDATION_ERROR_0004	'name' should have at least '2' characters, Mandatory Field 'name' is missing or empty.
400 Bad Request	ACCT_RO_015	Role name invalid.

Sample Request/Response

Use Case

Using the session ID acquired from the login API to execute subsequent API calls, specifically for adding a role API.

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/role?gwsource=external
```

Request Payload

```
{
"payload": {
 "name":"role_01",
 "description":"Adding a new role"
}
}
```

Sample Response

```
{
"response": "Role added successfully",
"message": "Role added successfully",
"appStatusCode": null,
"tags": null,
"headers": null
}
```

Accessing API with Service Account

For accessing APIs with a service account, you need to get the Access Token by providing Client ID and Client Secret in get-service-token API. This Access Token can then be used for accessing other APIs.

Note: Access Token Validity is 30 minutes by default and it can be configured in **Settings** > **Authentication** > **oAuth Settings**.

- Retrieve Access Token using get-service-token API
- Using Access Token in the header for further API calls

Retrieve Access Token using get-service-token API

The API provides a streamlined process for retrieving service tokens related to account management tasks.

Before you begin

- Make sure you have valid login credentials for accessing the system.

Request Structure

Endpoint:	/acctmgmt-get-service-token
Type:	POST
Sample URL:	https://<IP/HostName/TenantName>:<GWPORT>/avxapi/acctmgmt-get-service-token?gwsource=external To understand the elements of the sample URL, click here.
Headers:	
Content-Type:	application/json
Authentication:	Yes
Request timeout period	15 minutes

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

	Description
Authorization *Header*	(Mandatory) Please form a string in this format <Client ID>:<Client Secret> and do base64 encoding. Then prepend a key 'Basic' before the encoded value. Final value should be "Basic <EncodedValue>". **Type:** *String* **Example:** "admin"
Content-Type *Header*	(Mandatory) The parameter should be set to `application/json` to specify the nature of the data in the payload. **Type:** *String* **Example:** "application/json"
grant_type *Payload*	(Mandatory) Payload Type should be "Form". The value of the param should be "Client_Credentials". **Type:** *Text*

Response Structure

- **Status Code:** 200 Ok
- **Message:** Successful
- **Headers:**
  - **Content-Type:** application/json

Response Parameters

Name	Description
response	The response contains the attributes needed to retrieve the access token.
message	Success message or failure description in case of error.
appStatusCode	Application specific status code for the response. Will be non-null for failure response.
tags	More info in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	NA	Successful
400 Bad request	ACCT_SA_003	Service account is invalid/not found::[Service account not found in the database]
400 Bad request	OAUTH_CLNT_015	Client Password is incorrect::[Invalid Client credential]
400 Bad request	ACCT_SA_001	Invalid Request::[Invalid client Id or secret]
500 Internal Server Error	avx-common-011	Error while processing.

Sample Request/Response

Use Case

Retrieve Access Token.

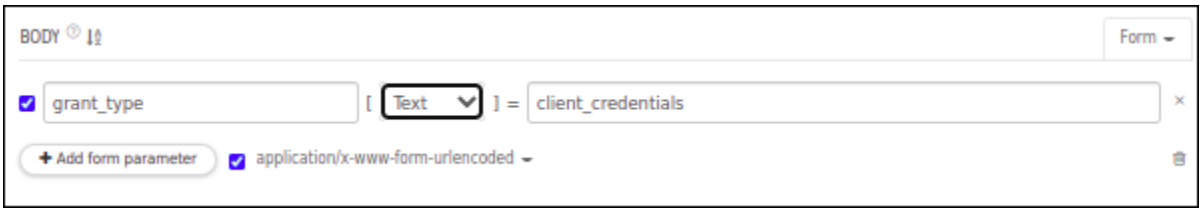
Request URL

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/acctmgmt-get-service-token?gwsource=external
```

Content-Type: application/x-www-form-urlencoded

Authorization: Basic
NTIxYzNhZDItZWE0ZS00NDdiLWE1MWItOTYyMWJiN2VhMTI2OjU1QVUjTk84JSpaaGd2TmZhWVVtdHZYMGRrRWhvZ

Request Payload



Sample Response

```
{
"response":
 "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJwbGF0Zm9ybSIsImF1ZCI6ImF2eCIsImNsaWVudElkIjoiOTcwNzRlNDEtOGFmOS00NTZkLTlhNjQtZjBj
 NGJiOTA4MDQ4IiwiaXNzIjoiYXZ4IiwiZXhwIjoxNjUwMzY5MzY3LCJncmFudCB0eXBlIjoiY2xpZW50X2NyZWRlbnRpYWxzIn0.HZnkuUEjXIeqJWqpqiNWFHqIDI7
 GYf4cWx6VwbjGD_0",
"message": null,
```

```
"appStatusCode": null,
"tags":{},
"headers": null
}
```


Using Access Token in the header for further API calls

The access token retrieved using the get-service-token API can be used in the header for making further API calls.

Before you begin

- Access Token is obtained from the get-service-token API.
- Ensure that the Access Token is valid and has not expired.

Request Structure

Endpoint:	/resource
Type:	POST
Sample URL:	https://<IP/HostName/TenantName>:<GWPORT>/avxapi/resource?gwsource=external To understand the elements of the sample URL, click here.
Headers:	
Content-Type:	application/json

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.

- **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

  The tenant name will be included in the endpoint URL for a SaaS deployment.

- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

Name	Description
Token *Header*	(Mandatory) Use token retrieved from login API. **Type:** *String* **Example:** eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJwbGF0Zm9ybSIsImF1ZCI6ImF2eCIsImNsaWVudElkIjoiOTcwNzRlNDEtOGFmOS00NTZkLTlhNjQtZjBjNGJiOTA4MDQ4IiwiaXNzIjoiYXZ4IiwiZXhwIjoxNjUwMzY5MzY3LCJncmFudCB0eXBlIjoiY2xpZW50X2NyZWRlbnRpYWxzIn0.HZnkuUEjXIeqJWqpqiNWFHqIDI7GYf4cWx 6VwbjGD_0
gwsource *Query*	(Mandatory) Source from which the request is triggered. The values can be: • web • external **Type:** *String*
Payload *String*	(Mandatory) Input data for request body in application/json format. For payload details, see **Payload** section.

Payload

Name	Description
name *String*	(Mandatory) Name of the resource to create. Name cannot be duplicated. **Example:** "resource_1"
description *String*	(Optional) Description of the resource. **Example:** "This is a sample resource."

Response Structure

- **Status Code:** 201 Created
- **Message:** Resource added successfully
- **Headers:**
  - **Content-Type:** application/json

Response Parameters

Name	Description
response	Contains the response attributes for resource added successfully.
message	Success message or failure description in case of error.
appStatusCode	Application specific status code for the response. Will be non-null for failure response.
tags	More info in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
201 Created	null	Resource added successfully
409 Conflict	RBAC_RE_005	Resource with the given name already exists
400 Bad Request	VALIDATION_ERROR_0004	'name' should have at least '2' characters, Mandatory Field 'name' is missing or empty
400 Bad Request	VALIDATION_ERROR_0004	Invalid "name".

HTTP Code	appStatusCode	Response Message
401 Unauthorized	AVX_GW_012	Unauthorized access, reason - Invalid Token
407 Proxy Authentication Required	AVX_GW_011	Session validation failed, reason - Session information is missing.

Sample Request/Response

Use Case

Add a resource using API with Access Token.

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/resource?gwsource=external
```

Request Payload

```
{
 "payload": {
 "name": "resource_1",
 "description": "This is a sample resource."
 }
 }
```

Sample Response

```
{
 "response": "Resource added successfully",
 "message": "Resource added successfully",
 "appStatusCode": null,
 "tags": null,
 "headers": null
 }
```

Commons

- Add a Resource
- Add Service Account
- Search for a Resource

Add a Resource

This API is used to create a new resource. A resource is a logical entity to group one or more ACL managed entities.

Before you begin

- Session ID is obtained from the login API.
- Ensure that the session ID is valid and has not expired.
- Make sure you have valid login credentials for accessing the system.

Request Structure

Endpoint:	/resource
Type:	POST
Sample URL:	https://<IP/HostName/TenantName>:<GWPORT>/avxapi/resource?gwsource=external

To understand the elements of the sample URL, click here.
Headers:
Content-Type: application/json

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

Name	Description
sessionId (or) Token *Header*	(Mandatory) Use either Session Id or Token received after login. **Type:** *String* **Example:** "sessionId": "ce7f1a14-2bf9-4e4a-89a8-bc780a255813"
username	(Mandatory) Use login name of the user.

Input Parameters (continued)

Name	Description
Header	**Type:** *String* **Example:** "admin"
Password *Header*	(Mandatory) Password for the username. **Type:** *String* **Example:** "AppViewX@123"
gwkey *Query*	(Optional) Tenant Key. Needed only in case of multi-tenant installation. **Type:** *String* **Example:** "f000ca01"
gwsource *Query*	(Mandatory) Source from which the request is triggered. The values can be: • web • external **Type:** *String*
Payload *String*	(Mandatory) Input data for request body in application/json format. For payload details, see **Payload** section.

Payload

Name	Description
name *String*	(Mandatory) Name of the resource to create. Name cannot be duplicated. **Example:** "resource_1"
description *String*	(Optional) Description of the resource. **Example:** "This is a sample resource."

Response Structure

- **Status Code:** 201 Created
- **Message:** Resource added successfully
- **Headers:**
  - **Content-Type:** application/json

Response Parameters

Name	Description
response	Contains the response attributes for resource added successfully.
message	Success message or failure description in case of error.
appStatusCode	Application specific status code for the response. Will be non-null for failure response.
tags	More info in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
201 Created	null	Resource added successfully
409 Conflict	RBAC_RE_005	Resource with the given name already exists
400 Bad Request	VALIDATION_ERROR_0004	'name' should have at least '2' characters, Mandatory Field 'name' is missing or empty
400 Bad Request	VALIDATION_ERROR_0004	Invalid "name".
401 Unauthorized	AVX_GW_012	Unauthorized access, reason - Invalid Token
407 Proxy Authentication Required	AVX_GW_011	Session validation failed, reason - Session information is missing.

Sample Request/Response

Use Case

Add a new resource with the name resource_1.

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/resource?gwsource=external
```

Request Payload

```
{
 "payload": {
 "name": "resource_1",
 "description": "This is a sample resource."
 }
 }
```

Sample Response

```
{
 "response": "Resource added successfully",
 "message": "Resource added successfully",
 "appStatusCode": null,
 "tags": null,
 "headers": null
 }
```

Add Service Account

This API is used to create a new service account.

Before you begin

- Session ID is obtained from the login API.
- Ensure that the session ID is valid and has not expired.
- Make sure you have valid login credentials for accessing the system.

Request Structure

Endpoint:	/acctmgmt-add-service-account
Type:	POST
Sample URL:	https://<IP/HostName/TenantName>:<GWPORT>/avxapi/acctmgmt-add-service-account?gwsource=external To understand the elements of the sample URL, click here.

Headers:	
Content-Type:	application/json
Authentication:	Yes
Request timeout period	15 minutes

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

Name	Description
sessionId (or) Token	(Mandatory) Use either Session Id or Token received after login.
Header	**Type:** *String*

Input Parameters (continued)

Name	Description
	Example: "sessionId": "ce7f1a14-2bf9-4e4a-89a8-bc780a255813"
gwsource *Query*	(Mandatory) Source from which the request is triggered. The values can be: • web • external **Type:** *String*
Payload *String*	(Mandatory) Input data for request body in application/json format. For payload details, see **Payload** section.

Payload

Name	Description
loginName *String*	(Mandatory) Unique names used as the service account name for authentication. Duplication is not allowed. **Example:** "internal90"
email *String*	(Mandatory) Email Address. **Example:** "internaldemo188@appviewx.com"
description *String*	(Optional) Description of the service account. **Example:** "description"

Response Structure

- **Status Code:** 200 OK
- **Message:** Success
- **Headers:**
  - **Content-Type:** application/json

Response Parameters

Name	Description
response	Contains the response attributes for service account added success.
message	Success message or failure description in case of error.
appStatusCode	Application specific status code for the response. Will be non-null for failure response.
tags	More info in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	null	Success
409 Conflict	ACCT_SA_008	Operation failed. Unable to add new entity. Entity already exists
400 Bad Request	ACCT_US_015	Mandatory Field 'email' is missing or empty.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials.
407 Proxy Authentication Required	AVX_GW_011	Session validation failed, reason - Session information is missing.

Sample Request/Response

Use Case

To add a Service account.

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/acctmgmt-add-service-account?gwsource=external
```

Request Payload

```
{
"payload": {
"loginName":"internal90",
"email": "internaldemo188@appviewx.com",
```

```
"description":"description"
}
}
```

Sample Response

```
{
    "response": "Success",
    "message": null,
    "appStatusCode": null,
    "tags": null,
    "headers": null
}
```

Search for a Resource

This API is used to search for a resource based on input filter condition. A resource is a logical entity to group one or more ACL managed entities. The response could be one or more resource(s) matching the input.

Before you begin

- Session ID is obtained from the login API.
- Ensure that the session ID is valid and has not expired.
- Make sure you have valid filter value for search.

Request Structure

Endpoint:	/resource-search
Type:	POST
Sample URL:	https://<IP/HostName/TenantName>:<GWPORT>/avxapi/resource-search?gwsource=external To understand the elements of the sample URL, click here.
Headers:	
Content-Type:	application/json

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

Name	Description
sessionId (or) Token	(Mandatory) Use either Session Id or Token received after login.
Header	**Type:** *String*
	Example: "sessionId": "ce7f1a14-2bf9-4e4a-89a8-bc780a255813"
Token	(Mandatory) Access token received after login.
Query	**Type:** *String*
	Example: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJwbGF0Zm9ybSIsImF1ZCI6ImF2eCIsImNsaWVudElkIjoiOTcwNzRlNDEtOGFmOS00NTZkLTlhNjQtZjBjNGJiOTA4MDQ4IiwiaXNzIjoiYXZ4IiwiZXhwIjoxNjUwMzY5MzY3LCJncm

Input Parameters (continued)

Name	Description
	FudCB0eXBlIjoiY2xpZW50X2NyZWRlbnRpYWxzIn0.HZnkuUEjXIeqJWqpqiNWFHqI DI7GYf4cWx6VwbjGD_0
gwsource *Query*	(Mandatory) Source from which the request is triggered. The values can be: • web • external **Type:** *String*
Payload *String*	(Mandatory) Input data for request body in application/json format. For payload details, see **Payload** section.

Payload

Name	Description
filterValue *String*	(Optional) Input filter string value to filter the resources. **Example:** "resource_1"
sortColumn *String*	(Optional) Column by which the output has to be sorted. **Example:** "name"
startIndex *Integer*	(Optional) Start index to show in output in case if there are more than one matching records. **Example:** "1"
maxSize *Integer*	(Optional) The number of records to return in a response. maxSize is starting from the start index. **Example:** "3"
sortOrder *String*	(Optional) The order to sort. Possible values are asc and desc. **Example:** "asc"

Response Structure

- **Status Code:** 200 OK
- **Message:** Matching results found for the given input.
- **Headers:**
  - **Content-Type:** application/json

Response Parameters

Name	Description
response	Contains the response attributes for search of resource successfully.
message	Success message or failure description in case of error.
appStatusCode	Application specific status code for the response. Will be non-null for failure response.
tags	More info in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	null	Matching results found for the given input.
404 Not Found	DG_009	No matching records found
401 Unauthorized	AVX_GW_012	Unauthorized access, reason - Invalid Token
400 Bad Request	DG_006	Invalid sort Column.

Sample Request/Response

Use Case

Search a resource with the name Role_admin.

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/resource-search?gwsource=external
```

Request Payload

```
{
 "payload": {
```

```
"startIndex" : 1,
"maxSize" : 3,
"sortOrder":"asc",
"sortColumn" : "name",
"filterValue" : "resource_1"
}
}
```


Sample Response


```
{
"response": {
"data": [
{
"name": "Role_admin",
"description": "Super access will have the permissions to access all the resources in AppViewX.",
"state": "A",
"_id": " Role_admin ",
"_keywords": null
}
],
"totalRecords": 1,
"obtainedRecords": 1,
"obtainedRecordRange": {
"start": 1,
"end": 1
}
},
"message": "Matching results found for the given input.",
"appStatusCode": null,
"tags": null,
"headers": null
}
```


Note: The state of a resource indicates if the resource is active or not. ‘A’ stands for active.

Get Resources for User Group

This API is used to fetch all the resources for a given user group.

Before you begin

- Session ID is obtained from the login API.
- Ensure that the session ID is valid and has not expired.
- Make sure you have valid User Group name.

Request Structure

Endpoint:	/usergroup-getResources
Type:	POST
Sample URL:	https://<IP/HostName/TenantName>:<GWPORT>/avxapi/usergroup-getResources?gwsource=external To understand the elements of the sample URL, click here.
Headers:	
Content-Type:	application/json

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

Name	Description
sessionId (or) Token *Header*	(Mandatory) Use either Session Id or Token received after login. **Type:** *String* **Example:** "sessionId": "ce7f1a14-2bf9-4e4a-89a8-bc780a255813"
gwsource *Query*	(Mandatory) Source from which the request is triggered. The values can be: • web • external **Type:** *String*
Payload *String*	(Mandatory) Input data for request body in application/json format. For payload details, see **Payload** section.

Payload

Name	Description
Name *String*	(Mandatory) Name of the user group. **Example:** "admin usergroup"
startIndex *Integer*	(Optional) Start index to show in output in case if there are more than one matching records. **Example:** "1"

Payload (continued)

Name	Description
maxSize *Integer*	(Optional) The number of records to return in a response. maxSize is starting from the start index. **Example:** "0"

Response Structure

- **Status Code:** 200 OK
- **Message:** Matching results found for the given input.
- **Headers:**
  - **Content-Type:** application/json

Response Parameters

Name	Description
response	Contains the response attributes for resource of user group.
message	Success message or failure description in case of error.
appStatusCode	Application specific status code for the response. Will be non-null for failure response.
tags	More info in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	null	Matching results found for the given input.
404 Not Found	DG_009	No matching records found.
400 Bad Request	RBAC_RE_021	Mandatory field 'name' is missing or empty
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials.

Sample Request/Response

Use Case

Get all resources under the user group usergroup_1.

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/usergroup-getResources?gwsource=external
```

Request Payload

```
{
 "payload": {
 "startIndex": 1,
 "maxSize": 0,
 "name": "usergroup_1"
 }
 }
```

Sample Response

```
{
 "response":{
 "data":[
 {"name": " resource_0", "description": "Resource for usergroup_0", "state": "A",…},
 {"name": "resource_1", "description": " Resource for usergroup_1", "state": "A",…},
 {"name": " resource_2", "description": “Resource for usergroup_1”, "state": "A", ,…},
 {"name": " resource_3", "description": "Resource for usergroup_1", "state": "A",…}
 ],
 "totalRecords": 4,
 "obtainedRecords": 4,
 "obtainedRecordRange":{
 "start": 1,
 "end": 4
 }
 },
 "message": "Matching results found for the given input.",
 "appStatusCode": null,
 "tags": null,
 "headers": null
 }
```

Note: The state of a resource indicates if the resource is active or not. ‘A’ stands for active.

Delete a Resource

This API is used to delete a resource.

Before you begin

- Ensure that the session ID is valid and has not expired.
- Make sure you have valid resource name to be deleted.

Request Structure

Endpoint:	`/resource`
Type:	`DELETE`
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/resource?gwsource=External&resourceName=resource_1` To understand the elements of the sample URL, click here.
Headers:	
Content-Type:	application/json

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

Name	Description
sessionId (or) Token *Header*	(Mandatory) Use either Session Id or Token received after login. **Type:** *String* **Example:** "sessionId": "ce7f1a14-2bf9-4e4a-89a8-bc780a255813"
gwsource *Query*	(Mandatory) Source from which the request is triggered. The values can be: • web • external **Type:** *String*
resourceName *Query*	(Mandatory) Name of the resource to be deleted. **Type:** *String* **Example:** "resource_1"

Response Structure

- **Status Code:** 200 OK
- **Message:** Resource deleted successfully.
- **Headers:**
  - **Content-Type:** application/json

Response Parameters

Name	Description
response	Contains the response attributes for resource deleted successfully.
message	Success message or failure description in case of error.
appStatusCode	Application specific status code for the response. Will be non-null for failure response.
tags	More info in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	null	Resource deleted successfully.
404 Not Found	RBAC_RE_005	Resouce Name doesnot exist.
403 Forbidden	RBAC_RE_020	Current user(s) aclIdentifier/resource cannot be deleted.
400 Bad request	RBAC_RE_001	ResourceName Cannot be Empty.

Sample Request/Response

Use Case

Delete a resource with name resource_1.

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/resource?resourceName=resource_1;gwsource=external
```

Request Payload

```
NA
```

Sample Response

```
{
"response": "Resource deleted successfully",
"message": "Resource deleted successfully",
"appStatusCode": null,
"tags": null,
"headers": null
}
```

Search for a Role

This API is used to search for a role based on the input filter condition. A role is a logical entity to group one or more Access Control Functions. The response could be one or more resource(s) matching the input.

Before you begin

- Session ID is obtained from the login API.
- Ensure that the session ID is valid and has not expired.
- Make sure you have valid filter value for search.

Request Structure

Endpoint:	`/role-search`
Type:	`POST`
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/role-search?gwsource=external` To understand the elements of the sample URL, click here.
Headers:	
Content-Type:	application/json

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

Name	Description
sessionId (or) Token *Header*	(Mandatory) Use either Session Id or Token received after login. **Type:** *String* **Example:** "sessionId": "ce7f1a14-2bf9-4e4a-89a8-bc780a255813"
gwsource *Query*	(Mandatory) Source from which the request is triggered. The values can be: • web • external **Type:** *String*
Payload *String*	(Mandatory) Input data for request body in application/json format. For payload details, see **Payload** section.

Payload

Name	Description
filterValue *String*	(Optional) Input filter string value to filter the role. **Example:** "admin"
sortColumn *String*	(Optional) Column by which the output has to be sorted. **Example:** "name"
startIndex	(Optional) Start index to show in output in case if there are more than one matching records.

Payload (continued)

Name	Description
Integer	**Example:** "1"
maxSize *Integer*	(Optional) The number of records to return in a response. maxSize is starting from the start index. **Example:** "2"
sortOrder *String*	(Optional) The order to sort. Possible values are asc and desc. **Example:** "asc"

Response Structure

- **Status Code:** 200 OK
- **Message:** Matching results found for the given input.
- **Headers:**
  - **Content-Type:** application/json

Response Parameters

Name	Description
response	Contains the response attributes for search of role successfully.
message	Success message or failure description in case of error.
appStatusCode	Application specific status code for the response. Will be non-null for failure response.
tags	More info in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	null	Matching results found for the given input.
404 Not Found	DG_009	No matching records found.
400 Bad Request	DG_006	Invalid sort Column.

HTTP Code	appStatusCode	Response Message
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials.

Sample Request/Response

Use Case

Search a role with the name Role_admin.

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/role-search?gwsource=external
```

Request Payload

```
{
 "payload": {
 "startIndex" : 1,
 "maxSize" : 2,
 "sortColumn" : "name",
 "sortOrder":"asc",
 "filterValue" : "admin"
 }
 }
```

Sample Response

```
{
 "response": {
 "data": [
 {
 "name": "admin",
 "description": "admin",
 "permissions": [
 "certificate:connectorActions:secureConnector",
 "certificate:settings:casettings:custom_ca",
 "certificate:settings:appsettings:view",
 "adc:dashboard:deviceheatmap:modifysettings",
 "certificate:client:adminaccess",
 "adc:deviceGroup:delete"
 ],
```

```
"state": "A",
"accessControlObjects": null,
"_id": "admin",
"_keywords": null
}
],
"totalRecords": 1,
"obtainedRecords": 1,
"obtainedRecordRange": {
"start": 1,
"end": 1
}
},
"message": "Matching results found for the given input.",
"appStatusCode": null,
"tags": null,
"headers": null
}
```


Note: The state of a role indicates if the role is active or not. ‘A’ stands for active.

Add a Role

This API is used to add a new role to the system.

Before you begin

- Session ID is obtained from the login API.
- Ensure that the session ID is valid and has not expired.

Request Structure

Endpoint:	/role
Type:	POST
Sample URL:	https://<IP/HostName/TenantName>:<GWPORT>/avxapi/role?gwkey=f000ca01&gwsource=external To understand the elements of the sample URL, click here.

Headers:	
Content-Type:	application/json

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Use session ID retrieved from login API, if username and password are not provided. **Type:** *String* **Example:** "sessionId": "ce7f1a14-2bf9-4e4a-89a8-bc780a255813"

Input Parameters (continued)

Name	Description
gwsource *Query*	(Mandatory) Source from which the request is triggered. The values can be: • web • external **Type:** *String*
Payload *String*	(Mandatory) Input data for request body in application/json format. For payload details, see **Payload** section.

Payload

Name	Description
name *String*	(Mandatory) Name of the role to be added. **Example:** "role_1"
description *String*	(Optional) Description of the role to be added. **Example:** "Adding a new role"

Response Structure

- **Status Code:** 201 Created
- **Message:** Role added successfully
- **Headers:**
  - **Content-Type:** application/json

Response Parameters

Name	Description
response	Contains the response attributes for role added successfully.
message	Success message or failure description in case of error.
appStatusCode	Application specific status code for the response. Will be non-null for failure response.

Response Parameters (continued)

Name	Description
tags	More info in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
201 Created	null	Role added successfully
409 Conflict	ACCT_RO_002	Role name already exists
400 Bad Request	VALIDATION_ERROR_0004	'name' should have at least '2' characters, Mandatory Field 'name' is missing or empty.
400 Bad Request	ACCT_RO_015	Role name invalid

Sample Request/Response

Use Case

Add a role with a valid role name.

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/role?gwsource=external
```

Request Payload

```
{
"payload": {
 "name":"role_01",
 "description":"Adding a new role"
}
}
```

Sample Response

```
{
"response": "Role added successfully",
"message": "Role added successfully",
"appStatusCode": null,
"tags": null,
```

```
"headers": null
}
```

Get Role Information

This API is used to retrive the role information.

Before you begin

- Ensure that the session ID is valid and has not expired.
- Make sure you have valid role name to get its information.

Request Structure

Endpoint:	`/role`
Type:	`GET`
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/role?roleName=role_1;gwsource=external` To understand the elements of the sample URL, click here.
Headers:	
Content-Type:	application/json

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

Name	Description
sessionId (or) Token *Header*	(Mandatory) Use either Session Id or Token received after login. **Type:** *String* **Example:** "sessionId": "ce7f1a14-2bf9-4e4a-89a8-bc780a255813"
gwsource *Query*	(Mandatory) Source from which the request is triggered. The values can be: • web • external **Type:** *String*
roleName *Query*	(Mandatory) Name of the role. **Type:** *String* **Example:** "role_1"

Response Structure

- **Status Code:** 200 OK
- **Message:** Role Information Retrieved Successfully.
- **Headers:**
  - **Content-Type:** application/json

Response Parameters

Name	Description
response	Contains the response attributes for role information retrieved successfully.
message	Success message or failure description in case of error.
appStatusCode	Application specific status code for the response. Will be non-null for failure response.
tags	More info in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	null	Role Information Retrieved Successfully.
404 Not Found	ACCT_RO_001	Role(s) not found.
400 Bad request	ACCT_RO_015	Mandatory field 'roleName' is missing or empty

Sample Request/Response

Use Case

Get the information about the role **role_1**.

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/role?roleName=role_1;gwsource=external
```

Request Payload

```
NA
```

Sample Response

```
{
 "response": {
 "name": "role_1",
 "description": "role_1 details",
 "permissions": [
 "permission_1"
 ],
 "state": "A",
 "_id": "log",
```

```
"_keywords": [
"role used to test role functions.",
"log",
"Enabled"
]
},
"message": "Role Information Retrieved Successfully",
"appStatusCode": null,
"tags": null
}
```


Delete a Role

This API is used to delete a role.

Before you begin

- Ensure that the session ID is valid and has not expired.
- Make sure you have valid role name to be deleted.

Request Structure

Endpoint:	`/role`
Type:	`DELETE`
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/role?gwsource=External&roleName=role_01` To understand the elements of the sample URL, click here.
Headers:	
Content-Type:	application/json

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.

- **HostName**: A human-readable label assigned to a device (host) on a network

  The hostname will be included in the endpoint URL for an on-prem deployment.

- **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

  The tenant name will be included in the endpoint URL for a SaaS deployment.

- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

Name	Description
sessionId (or) Token *Header*	(Mandatory) Use either Session Id or Token received after login. **Type:** *String* **Example:** "sessionId": "ce7f1a14-2bf9-4e4a-89a8-bc780a255813"
gwsource *Query*	(Mandatory) Source from which the request is triggered. The values can be: • web • external **Type:** *String*
roleName *Query*	(Mandatory) Name of the role to delete. **Type:** *String* **Example:** "role_01"

Response Structure

- **Status Code:** 200 OK
- **Message:** Role deleted successfully.
- **Headers:**
  - **Content-Type:** application/json

Response Parameters

Name	Description
response	Contains the response attributes for role deleted successfully.
message	Success message or failure description in case of error.
appStatusCode	Application specific status code for the response. Will be non-null for failure response.
tags	More info in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	null	Role deleted successfully.
404 Not Found	ACCT_RO_001	RoleName doesnot exist.
409 Forbidden	NA	Role(s) which have active user(s) cannot be deleted.
409 Conflict	ACCT_RO_016	Administrative role cannot be deleted
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials.
400 Bad Request	ACCT_RO_015	Mandatory field 'roleName' is missing or empty.
400 Bad Request	ACCT_RO_032	Pre-shipped role(s) are not eligible for updation/deletion

Sample Request/Response

Use Case

Delete a role with name role_01.

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/role?gwsource=External&roleName=role_01
```

Request Payload

```
NA
```

Sample Response

```
{
 "response": "Role deleted successfully",
 "message": "Role deleted successfully",
 "appStatusCode": null,
 "tags": null,
 "headers": null
 }
```

Clone a Role

This API is used to clone a role.

Before you begin

- Ensure that the session ID is valid and has not expired.
- Make sure you have valid role name to be cloned.

Request Structure

Endpoint:	/role-clone
Type:	POST
Sample URL:	https://<IP/HostName/TenantName>:<GWPORT>/avxapi/role-clone?gwsource=external To understand the elements of the sample URL, click here.
Headers:	
Content-Type:	application/json

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

Name	Description
sessionId (or) Token *Header*	(Mandatory) Use either Session Id or Token received after login. **Type:** *String* **Example:** "sessionId": "ce7f1a14-2bf9-4e4a-89a8-bc780a255813"
gwsource *Query*	(Mandatory) Source from which the request is triggered. The values can be: • web • external **Type:** *String*

Input Parameters (continued)

Name	Description
Payload *String*	(Mandatory) Input data for request body in application/json format. For payload details, see **Payload** section.

Payload

Name	Description
existingName *payload*	(Mandatory) Name of the role to be cloned. **Type:** *String* **Example:** "role_1"
newName *payload*	(Mandatory) Name of the cloned new role. **Type:** *String* **Example:** "clonerole_1"
description *payload*	(Optional) Description of the cloned role. **Type:** *String* **Example:** "Clone test role"

Response Structure

- **Status Code:** 200 OK
- **Message:** Clone role successful.
- **Headers:**
  - **Content-Type:** application/json

Response Parameters

Name	Description
response	Contains the response attributes for role cloned successfully.
message	Success message or failure description in case of error.

Response Parameters (continued)

Name	Description
appStatusCode	Application specific status code for the response. Will be non-null for failure response.
tags	More info in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	null	Clone role successful.
404 Not Found	ACCT_RO_001	Role Name to be cloned not found
400 Bad request	VALIDATION_ERROR_0004	Mandatory Field 'existingName' is missing or empty, Mandatory Field 'newName' is missing or empty
400 Bad request	VALIDATION_ERROR_0004	Mandatory Field 'existingName' is missing or empty, 'existingName' should have at least '2' characters
400 Bad request	VALIDATION_ERROR_0004	'newName' should have at least '2' characters, Mandatory Field 'newName' is missing or empty
400 Bad request	VALIDATION_ERROR_0004	'newName' cannot exceed '64' characters
400 Bad request	ACCT_RO_026	Invalid Description
409 Conflict	ACCT_RO_002	ClonedRole Name already exists for the given RoleName

Sample Request/Response

Use Case

Clone a role role_1 to create a new cloned role named clonerole_1.

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/role-clone?gwsource=external
```

Request Payload

```
{
 "payload": {
 "existingName": "role_1",
 "newName": "clonerole_1",
```

```
"description": "clone test role."
}
}
```

Sample Response

```
{
"response": "Clone role successful",
"message": "Clone role successful",
"appStatusCode": null,
"tags": null,
"headers": null
}
```

Share Dashboard to User Group

This API is used to share an existing dashboard to one or more existing usergroups. The sharing can be restricted to read-only or as a read-write.

Before you begin

- Session ID is obtained from the login API.
- Ensure that you have the necessary payload details.

Request Structure

Endpoint:	`/dashboard-share-usergroupdetails-update`
Type:	`PUT`
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/dashboard-share-usergroupdetails-update?name=Dashboard1&gwsource=WEB` To understand the elements of the sample URL, click here.
Headers:	
Content-Type:	application/json

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

Name	Description
sessionId (or) Token *Header*	(Mandatory) Use either Session Id or Token received after login. **Type:** *String* **Example:** "sessionId": "ce7f1a14-2bf9-4e4a-89a8-bc780a255813"
gwsource *Query*	(Mandatory) Source from which the request is triggered. The values can be: • web • external **Type:** *String*
name	(Mandatory) Name of the dashboard to be shared.

Input Parameters (continued)

Name	Description
Query	**Type:** *String* **Example:** "Dashboard1"
Payload *String*	(Mandatory) Input data for request body in application/json format. For payload details, see **Payload** section.

Payload

Name	Description
readUserGroup *String*	(Optional) Name of the user group that need to have only read access to the dashboard. **Example:** "UG1"
readWriteUserGroup *String*	(Optional) Name of the user group that need to have read-write access to the dashboard. **Example:** "UG2"

Response Structure

- **Status Code:** 200 OK
- **Message:** Success
- **Headers:**
  - **Content-Type:** application/json

Response Parameters

Name	Description
response	Contains the response attributes for share dashboard to user group successfully.
message	Success message or failure description in case of error.
appStatusCode	Application specific status code for the response. Will be non-null for failure response.

Response Parameters (continued)

Name	Description
tags	More info in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	null	Success
404 Not Found	ADC_DASH_0045	Dashboard not available for given name.
400 Bad Request	ADC_DASH_0051	Invalid dashboard name.
403 Forbidden	ADC_DASH_0048	Permission not available for dashboard.

Sample Request/Response

Use Case

Share a dashboard named Dashboard1 in read mode to the usergroup and in read/write mode to the usergroup.

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/dashboard-share-usergroupdetails-update?name=Dashboard1&gwsource=WEB
```

Request Payload

```
{
"payload": {
"readUserGroups": [
"UG1"
],
"readWriteUserGroups": ["UG2"]
}
}
```

Sample Response

```
{
"response": "Success",
"message": null,
"appStatusCode": null,
```

```
"tags": null,
"headers": null
}
```

Add a User Group

This API is used to add a new user group to the system.

Before you begin

- Session ID is obtained from the login API.
- Ensure that the session ID is valid and has not expired.

Request Structure

Endpoint:	/usergroup
Type:	POST
Sample URL:	https://<IP/HostName/TenantName>:<GWPORT>/avxapi/usergroup?gwsource=external To understand the elements of the sample URL, click here.
Headers:	
Content-Type:	application/json

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.

- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

Name	Description
sessionId (or) Token *Header*	(Mandatory) Use either Session Id or Token received after login. **Type:** *String* **Example:** "sessionId": "ce7f1a14-2bf9-4e4a-89a8-bc780a255813"
gwsource *Query*	(Mandatory) Source from which the request is triggered. The values can be: • web • external **Type:** *String*
Payload *String*	(Mandatory) Input data for request body in application/json format. For payload details, see **Payload** section.

Payload

Name	Description
name *String*	(Mandatory) Name of the user group. **Example:** "usergroup_1"
description *String*	(Optional) Description of the user group. **Example:** "Adding user group"

Response Structure

- **Status Code:** 201 Created
- **Message:** Usergroup added successfully
- **Headers:**
  - **Content-Type:** application/json

Response Parameters

Name	Description
response	Contains the response attributes for user group added successfully.
message	Success message or failure description in case of error.
appStatusCode	Application specific status code for the response. Will be non-null for failure response.
tags	More info in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
201 Created	null	Usergroup added successfully
409 Conflict	RBAC_US_023	Usergroup already exists.
400 Bad Request	ACCT_USERGROUP_001	Mandatory field 'userGroupName' is missing or empty.

Sample Request/Response

Use Case

Add a user group with a valid name.

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/usergroup?gwsource=external
```

Request Payload

```
{
 "payload": {
 "name": "usergroup_1",
 "description": "Adding user group"
```

```
}
}
```

Sample Response

```
{
"response": " Usergroup added successfully",
"message": " Usergroup added successfully",
"appStatusCode": null,
"tags": null,
"headers": null
}
```

Associate Permissions to Role

This API is used to assign/un-assign ACF permissions to a role.

Before you begin

- Session ID is obtained from the login API.
- Ensure that the session ID is valid and has not expired.

Request Structure

Endpoint:	/role-updatePermission
Type:	PUT
Sample URL:	https://<IP/HostName/TenantName>:<GWPORT>/avxapi/role-updatePermission?gwsource=external To understand the elements of the sample URL, click here.
Headers:	
Content-Type:	application/json

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

Name	Description
sessionId (or) Token *Header*	(Mandatory) Use either Session Id or Token received after login. **Type:** *String* **Example:** "sessionId": "ce7f1a14-2bf9-4e4a-89a8-bc780a255813"
gwsource *Query*	(Mandatory) Source from which the request is triggered. The values can be: **Type:** *String* • web • external

Input Parameters (continued)

Name	Description
Payload *String*	(Mandatory) Input data for request body in application/json format. For payload details, see **Payload** section.

Payload

Name	Description
roleName *String*	(Mandatory) Name of the role. **Example:** "role_1"
assignPermissionList *Array*	(Optional) ACF permissions to be assigned to the role. Refer to the list of possible permissions list for details. **Example:** "["general:accounts:resource:clone", "general:accounts:resource:delete"]"
unassignPermissionList *Array*	(Optional) ACF permissions to be unassigned from the role. Refer to the list of possible permissions list for details. **Example:** "["general:accounts:resource:delete"]"

Note: Even if the assignPermissionList and unassignPermissionList contain invalid ACF permission text that cannot be processed, the API would still go-ahead to assign/un-assign any functions in wither list that can be processed.

Response Structure

- **Status Code:** 202 Accepted
- **Message:** ACF assignment initiated for the given role.
- **Headers:**
  - **Content-Type:** application/json

Response Parameters

Name	Description
response	Contains the response attributes for ACF assignment initiated for the given role.
message	Success message or failure description in case of error.
appStatusCode	Application specific status code for the response. Will be non-null for failure response.
tags	More info in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	null	ACF assignment initiated for the given role.
400 Bad Request	ACCT_RO_015	Mandatory field 'roleName' is missing or empty.
404 Not Found	ACCT_RO_001	Role(s) not found.

Sample Request/Response

Use Case

Assign and unassign few ACF permissions to/from the role “role_1”.

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/role-updatePermission?gwsource=external
```

Request Payload

```
{
 "payload": {
 "roleName": "role_1",
 "assignPermissionList": [
 "general:accounts:resource:clone",
 "general:accounts:resource:delete"
 ],
 "unassignPermissionList": [
 "general:accounts:resource:delete"
 ]
```

```
}
}
```

Sample Response

```
{
"response": "ACF assignment initiated for the given role",
"message": "ACF assignment initiated for the given role",
"appStatusCode": null,
"tags": null,
"headers": null
}
```

Search User Group

This API is used to search / get the details about a user group. The user group can be filtered by the given input.

Before you begin

- Session ID is obtained from the login API.
- Ensure that the session ID is valid and has not expired.
- Make sure you have valid filter value for search.

Request Structure

Endpoint:	`/usergroup-search`
Type:	`POST`
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/usergroup-search?gwsource=external` To understand the elements of the sample URL, click here.
Headers:	
Content-Type:	application/json

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

Name	Description
sessionId (or) Token *Header*	(Mandatory) Use either Session Id or Token received after login. **Type:** *String* **Example:** "sessionId": "ce7f1a14-2bf9-4e4a-89a8-bc780a255813"
gwsource *Query*	(Mandatory) Source from which the request is triggered. The values can be: **Type:** *String* • web • external

Input Parameters (continued)

Name	Description
Payload *String*	(Mandatory) Input data for request body in application/json format. For payload details, see **Payload** section.

Payload

Name	Description
filterValue *String*	(Mandatory) Input filter string value to filter the user group. **Example:** "admin usergroup""
sortColumn *String*	(Optional) Column by which the output has to be sorted. **Example:** "name"
startIndex *Integer*	(Optional) Start index to show in output in case if there are more than one matching records. **Example:** "1"
maxSize *Integer*	(Optional) The number of records to return in a response. maxSize is starting from the start index. **Example:** "2"
sortOrder *String*	(Optional) The order to sort. Possible values are asc and desc. **Example:** "asc"

Response Structure

- **Status Code:** 200 OK
- **Message:** Matching results found for the given input.
- **Headers:**
  - **Content-Type:** application/json

Response Parameters

Name	Description
response	Contains the response attributes for search of user group successfully.
message	Success message or failure description in case of error.
appStatusCode	Application specific status code for the response. Will be non-null for failure response.
tags	More info in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	null	Matching results found for the given input.
404 Not Found	DG_009	No matching records found::[No matching records are found in the AppViewX database for your query. Check your query parameters.]
400 Bad Request	DG_006	Invalid sort Column
400 Bad Request	avx-common-028	Invalid/ Incorrect payload
400 Bad Request	DG_007	Invalid sort order

Sample Request/Response

Use Case

Get the details about a user group with the name usergroup_1.

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/usergroup-search?gwsource=external
```

Request Payload

```
{
 "payload": {
 "startIndex" : 1,
 "maxSize" :1,
```

```
"sortColumn" : "name",
"sortOrder":"asc",
"filterValue" : "admin usergroup"
}
}
```

Sample Response

```
{
"response":{
"data":[
{
"name": "super access",
"description": "Super access will have the permissions to access all the resources in AppViewX.",
"state": "A",
"_id": "super access",
"_keywords":[
"super access",
"Super access will have the permissions to access all the resources in AppViewX.",
"Enabled"
]
}
],
"totalRecords": 1,
"obtainedRecords": 1,
"obtainedRecordRange":{
"start": 1,
"end": 1
}
},
"message": "Matching results found for the given input.",
"appStatusCode": null,
"tags": null,
"headers": null
}
```

Delete a User Group

This API is used to delete a user group.

Before you begin

- Ensure that the session ID is valid and has not expired.
- Make sure you have valid user group name to be deleted.

Request Structure

Endpoint:	`/userGroup`
Type:	`DELETE`
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/userGroup?userGroupName=group_1;gwsource=external` To understand the elements of the sample URL, click here.
Headers:	
Content-Type:	application/json

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL

- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

Name	Description
sessionId (or) Token *Header*	(Mandatory) Use either Session Id or Token received after login. **Type:** *String* **Example:** "sessionId": "ce7f1a14-2bf9-4e4a-89a8-bc780a255813"
gwsource *Query*	(Mandatory) Source from which the request is triggered. The values can be: • web • external **Type:** *String*
userGroupName *Query*	(Mandatory) Name of the user group to be deleted. **Type:** *String* **Example:** "group_1"

Response Structure

- **Status Code:** 200 OK
- **Message:** UserGroup deleted successfully.
- **Headers:**
  - **Content-Type:** application/json

Response Parameters

Name	Description
response	Contains the response attributes for user group deleted successfully.
message	Success message or failure description in case of error.
appStatusCode	Application specific status code for the response. Will be non-null for failure response.

Response Parameters (continued)

Name	Description
tags	More info in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	null	UserGroup deleted successfully.
404 Not Found	ACCT_USERGROUP_030	UserGroup doesnot exist.
403 Forbidden	AVX_GW_005	User does not have access to the targeted API
400 Bad request	RBAC_US_019	Usergroup(s) which have active user(s) cannot be deleted
405 Method Not Allowed	RBAC_US_015	Admin usergroup cannot be deleted

Sample Request/Response

Use Case

Add a user group with the name group_1.

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/userGroup?userGroupName= group_1;gwsource=external
```

Request Payload

```
NA
```

Sample Response

```
{
"response": "UserGroup deleted successfully",
"message": "UserGroup deleted successfully",
"appStatusCode": null,
"tags": null,
"headers": null
}
```

Associate User Group with Resources

This API is used to associate one or more resources to a user group.

Before you begin

- Session ID is obtained from the login API.
- Ensure that the session ID is valid and has not expired.

Request Structure

Endpoint:	`/usergroup-updateResource`
Type:	`POST`
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/usergroup-updateResource?gwsource=web` To understand the elements of the sample URL, click here.
Headers:	
Content-Type:	application/json

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

Name	Description
sessionId (or) Token *Header*	(Mandatory) Use either Session Id or Token received after login. **Type:** *String* **Example:** "sessionId": "ce7f1a14-2bf9-4e4a-89a8-bc780a255813"
gwsource *Query*	(Mandatory) Source from which the request is triggered. The values can be: • web • external **Type:** *String*
Payload *String*	(Mandatory) Input data for request body in application/json format. For payload details, see **Payload** section.

Payload

Name	Description
filterValue *String*	(Mandatory) Value to filter the name. **Example:** "internal90"
assignPermissionList *Array*	(Optional) ACF permissions to be assigned to the role. **Example:** "resource_2"
unassignPermissionList *Array*	(Optional) ACF permissions to be unassigned from the role. **Example:** "resource_1"

Response Structure

- **Status Code:** 200 OK
- **Message:** Successfully associated user group - resource
- **Headers:**
  - **Content-Type:** application/json

Response Parameters

Name	Description
response	Contains the response attributes for getting details about a user group.
message	Success message or failure description in case of error.
appStatusCode	Application specific status code for the response. Will be non-null for failure response.
tags	More info in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	null	Successfully associated user group - resource
400 Bad Request	ACCT_USERGROUP_001	Mandatory field 'userGroupName' is missing or empty
404 Not Found	ACCT_USERGROUP_027	UserGroup not found.

Sample Request/Response

Use Case

Get the details about a user group with the name usergroup_1.

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/usergroup-updateResource?gwsource=external
```

Request Payload

```
{
 "payload": {
 "name": "testgroup",
 "assignList" : [
```

```
"resource_2"
],
"unassignList": [
"resource_1"
]
}
}
```


Sample Response


```
{
"response": "Updating usergroup with resource(s) successful",
"message": "Updating usergroup with resource(s) successful",
"appStatusCode": null,
"tags": null,
"headers": null
}
```


Add a User

This API is used to create a new user.

Before you begin

- Session ID is obtained from the login API.
- Ensure that the session ID is valid and has not expired.

Request Structure

Endpoint:	/user
Type:	POST
Sample URL:	https://<IP/HostName/TenantName>:<GWPORT>/avxapi/user?gwsource=external To understand the elements of the sample URL, click here.
Headers:	
Content-Type:	application/json

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

Name	Description
sessionId (or) Token *Header*	(Mandatory) Use either Session Id or Token received after login. **Type:** *String* **Example:** "sessionId": "ce7f1a14-2bf9-4e4a-89a8-bc780a255813"
gwsource *Query*	(Mandatory) Source from which the request is triggered. The values can be: • web • external **Type:** *String*

Input Parameters (continued)

Name	Description
Payload *String*	(Mandatory) Input data for request body in application/json format. For payload details, see **Payload** section.

Payload

Name	Description
loginName *String*	(Mandatory) Unique names used as the username for authentication. Duplication is not allowed. **Example:** "appviewx"
password *String*	(Mandatory) A password that can be used to authenticate. **Note:** Not relevant if 'isExternalAuth' is set to Y. **Example:** "QWRtaW5AMTIz"
confirmPassword *String*	(Mandatory) Reconfirm the given password. **Note:** Not relevant if 'isExternalAuth' is set to Y. **Example:** "QWRtaW5AMTIz"
isExternalAuth *String*	(Mandatory) Specify if the user is from an external authentication system like LDAP, Radius, etc. Possible values are 'Y' for yes and 'N' for No. **Example:** "N"
comment *String*	(Optional) Comment for the user. **Example:** "This is a test user"
preferredContactMode *String*	(Mandatory) Preferred contact mode. Possible values are 'E' for email. **Example:** "E"
email	(Mandatory) Email address.

Payload (continued)

Name	Description
String	**Example:** "appviewx@app.com"

Response Structure

- **Status Code:** 201 Created
- **Message:** User added successfully.
- **Headers:**
  - **Content-Type:** application/json

Response Parameters

Name	Description
response	Contains the response attributes for user added successfully.
message	Success message or failure description in case of error.
appStatusCode	Application specific status code for the response. Will be non-null for failure response.
tags	More info in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
201 Created	null	User added successfully.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials.
409 Conflict	ACCT_US_042	User name already exist.
400 Bad Request	ACCT_US_015	Mandatory field 'loginName' is missing or empty.

Sample Request/Response

Use Case

Add a new internal user with login name **appviewx**.

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/user?gwsource=external
```

Request Payload

```
{
 "payload": {
 "loginName": "appviewx",
 "password":"QWRtaW5AMTIz",
 "confirmPassword": "QWRtaW5AMTIz",
 "isExternalAuth" : "N",
 "comment": "This is a test user",
 "preferredContactMode": "E",
 "email": "appviewx@app.com"
 }
 }
```

Sample Response

```
{
 "response": "User added successfully",
 "message": "User added successfully",
 "appStatusCode": null,
 "tags": null,
 "headers": null
 }
```

Associate Roles to a User Group

This API is used to associate or disassociate one or more roles to a user group.

Before you begin

- Session ID is obtained from the login API.
- Ensure that the session ID is valid and has not expired.

Request Structure

Endpoint:	/usergroup-updateRoles
Type:	PUT

Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/usergroup-updateRoles?gwsource=web` To understand the elements of the sample URL, click here.
Headers:	
Content-Type:	application/json

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

Name	Description
sessionId (or) Token	(Mandatory) Use either Session Id or Token received after login.
Header	**Type:** *String*

Input Parameters (continued)

Name	Description
	Example: "sessionId": "ce7f1a14-2bf9-4e4a-89a8-bc780a255813"
gwsource *Query*	(Mandatory) Source from which the request is triggered. The values can be: • web • external **Type:** *String*
Payload *String*	(Mandatory) Input data for request body in application/json format. For payload details, see **Payload** section.

Payload

Name	Description
assignRoles *Array*	(Optional) An array of role names to assign. **Example:** ["R1"]
unassignRoles *Array*	(Optional) An array of role names to unassign. **Example:** "[ ]"
name *String*	(Mandatory) Name of the user-group for consideration. **Example:** "UG1"

Note: Even if the assignRoles and unassignRoles contain invalid role names that cannot be processed, the API would still go-ahead to assign/unassign any role in the list that can be successfully processed.

Response Structure

- **Status Code:** 200 OK
- **Message:** Successfully updated usergroup - role association.

- **Headers:**
  - **Content-Type:** application/json

Response Parameters

Name	Description
response	Contains the response attributes for assign role to user group.
message	Success message or failure description in case of error.
appStatusCode	Application specific status code for the response. Will be non-null for failure response.
tags	More info in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	null	Successfully updated usergroup - role association.
400 Bad Request	ACCT_USERGROUP_001	Mandatory field 'userGroupName' is missing or empty
400 Bad Request	ACCT_USERGROUP_044	Assign/Unassign Role list cannot be empty
404 Not Found	ACCT_USERGROUP_027	UserGroup not found.

Sample Request/Response

Use Case

role_1, role_2, and role_3 are existing in the application. role_1 and role_2 have to be assigned to the user group *appviewx_usergroup* and role_3 has to be unassigned.

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/usergroup-updateRoles?gwsource=external
```

Request Payload

```
{
 "payload" : {
 "name": "admin usergroup",
 "assignRoles": ["R1"],
```

```
"unassignRoles": []
}
}
```

Sample Response

```
{
    "response": "Successfully updated usergroup - role association. ",
    "message": "Successfully updated usergroup - role association. ",
    "appStatusCode": null,
    "tags": null,
    "headers": null
}
```

Associate User Groups to a User

This API is used to associate or disassociate one or more user groups to a user.

Before you begin

- Session ID is obtained from the login API.
- Ensure that the session ID is valid and has not expired.

Request Structure

Endpoint:	`/user-updateUsergroups`
Type:	`PUT`
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/user-updateUsergroups?gwsource=web` To understand the elements of the sample URL, click here.
Headers:	
Content-Type:	application/json

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

Name	Description
sessionId (or) Token *Header*	(Mandatory) Use either Session Id or Token received after login. **Type:** *String* **Example:** "sessionId": "ce7f1a14-2bf9-4e4a-89a8-bc780a255813"
gwsource *Query*	(Mandatory) Source from which the request is triggered. The values can be: • web • external **Type:** *String*

Input Parameters (continued)

Name	Description
Payload *String*	(Mandatory) Input data for request body in application/json format. For payload details, see **Payload** section.

Payload

Name	Description
loginName *String*	(Mandatory) Login name of the user. **Example:** "internal90"
assignUserGroups *Array*	(Optional) An array of user group names to assign. **Example:** "usergroup_1", "usergroup_2"
unassignedUserGroup *Array*	(Optional) An array of user group names to unassign. **Example:** "usergroup_3"

Note: Even if the assignUserGroups and unAssignUserGroups contain invalid user group names that cannot be processed, the API would still go-ahead to assign/un-assign any user group in the list that can be successfully processed.

Response Structure

- **Status Code:** 200 OK
- **Message:** Successfully modified user-usergroup association.
- **Headers:**
  - **Content-Type:** application/json

Response Parameters

Name	Description
response	Contains the response attributes for assigning user group to a user.
message	Success message or failure description in case of error.

Response Parameters (continued)

Name	Description
appStatusCode	Application specific status code for the response. Will be non-null for failure response.
tags	More info in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	null	Successfully modified user-usergroup association.
400 Bad Request	ACCT_US_015	Mandatory Field 'loginName' is missing or empty
400 Bad Request	ACCT_US_56	Assign/Unassign Usergroup list cannot be empty for User

Sample Request/Response

Use Case

"usergroup_1, usergroup_2, and usergroup_3 are existing in the application. usergroup_1 and usergroup_2 have to be assigned to the user with loginname user_1 and usergroup_3 has to be unassigned"

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/user-updateUsergroups?gwsource=external
```

Request Payload

```
{
 "payload": {
 "loginName": "appviewx",
 "assignUserGroups": [
 "usergroup_1",
 "usergroup_2"
 ],
 "unassignUserGroups": [
 "usergroup_3"
 ]
```

```
}
}
```

Sample Response

```
{
 "response": "Successfully modified user-user group association",
 "message": " Successfully modified user-user group association ",
 "appStatusCode": null,
 "tags": null,
 "headers": null
}
```

Search for a user

This API is used to search for a user using filter conditions.

Before you begin

- Session ID is obtained from the login API.
- Ensure that the session ID is valid and has not expired.
- Make sure you have valid filter value for search.

Request Structure

Endpoint:	`/user-search`
Type:	`POST`
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/user-search?gwsource=external` To understand the elements of the sample URL, click here.
Headers:	
Content-Type:	application/json

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

Name	Description
sessionId (or) Token *Header*	(Mandatory) Use either Session Id or Token received after login. **Type:** *String* **Example:** "sessionId": "ce7f1a14-2bf9-4e4a-89a8-bc780a255813"
gwsource *Query*	(Mandatory) Source from which the request is triggered. The values can be: **Type:** *String* • web • external

Input Parameters (continued)

Name	Description
Payload *String*	(Mandatory) Input data for request body in application/json format. For payload details, see **Payload** section.

Payload

Name	Description
filterValue *String*	(Mandatory) Input filter string value to filter the user. **Example:** "appviewx_user1"
sortColumn *String*	(Optional) Column by which the output has to be sorted. **Example:** "loginName"
startIndex *Integer*	(Optional) Start index to show in output in case if there are more than one matching records. **Example:** "1"
maxSize *Integer*	(Optional) The number of records to return in a response. maxSize is starting from the start index. **Example:** "2"
sortOrder *String*	(Optional) The order to sort. Possible values are asc and desc. **Example:** "asc"

Response Structure

- **Status Code:** 200 OK
- **Message:** Matching results found for the given input.
- **Headers:**
  - **Content-Type:** application/json

Response Parameters

Name	Description
response	Contains the response attributes for search of user successfully.
message	Success message or failure description in case of error.
appStatusCode	Application specific status code for the response. Will be non-null for failure response.
tags	More info in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	null	Matching results found for the given input.
404 Not Found	DG_009	No matching records found.
400 Bad Request	DG_006	Invalid sort Column.

Sample Request/Response

Use Case

Search for use with name appviewx_user1.

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/user-search?gwsource=external
```

Request Payload

```
{
"payload": {
"startIndex" : 1,
"maxSize" : 2,
"sortColumn" : "loginName",
"sortOrder" :"asc",
"filterValue" : "appviewx_user1"
}
}
```

Sample Response

```
{
"response": {
"data": [
{
"loginName": "appviewx_user1",
"firstName": "Appviewx",
"lastName": "user1",
"comment": Appviewx login user,
"email": "",
"mobile": "",
"preferredContactMode": "",
"isExternalAuth": "N",
"state": "A",
"roles": null,
"swImages": null,
"authenticationMode": "Internal",
"available": "Active",
"lastLogIn": "Online",
"sessionIds": null,
"aclIdentifiers": null,
"tenantId": null,
"availableIncorrectAttempt": 10,
"lastLoginTimestamp": 1585669200198,
"adUserGroups": null,
"sso": false,
"date": "2020-04-13 12:05:09",
"_id": "5d258291d7f495bb31691fc4",
"userGroups": null,
"_keywords": null,
"isSSO": false
}
],
"totalRecords": 1,
"obtainedRecords": 1,
"obtainedRecordRange": {
"start": 1,
"end": 1
```



```
}

},

"message": "Matching results found for the given input.",

"appStatusCode": null,

"tags": null,

"headers": null

}
```


Assign User group to Service Account

This API is used to create a new resource. A resource is a logical entity to group one or more ACL managed entities.

Before you begin

- Session ID is obtained from the login API.
- Ensure that the session ID is valid and has not expired.

Request Structure

Endpoint:	`/platform-assign-usergroup-to-service-account`
Type:	`PUT`
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/platform-assign-usergroup-to-service-account?gwsource=web` To understand the elements of the sample URL, click here.
Headers:	
Content-Type:	application/json

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.

- **HostName**: A human-readable label assigned to a device (host) on a network

  The hostname will be included in the endpoint URL for an on-prem deployment.

- **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

  The tenant name will be included in the endpoint URL for a SaaS deployment.

- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

Name	Description
sessionId (or) Token *Header*	(Mandatory) Use either Session Id or Token received after login. **Type:** *String* **Example:** "sessionId": "ce7f1a14-2bf9-4e4a-89a8-bc780a255813"
gwsource *Query*	(Mandatory) Source from which the request is triggered. The values can be: • web • external **Type:** *String*
Payload *String*	(Mandatory) Input data for request body in application/json format. For payload details, see **Payload** section.

Payload

Name	Description
loginName *String*	(Mandatory) Unique names used as the service account name for authentication. Duplication is not allowed. **Example:** "internal90"
assignedUserGroup *Array*	(Optional) Mention the array of user groups to be assigned. **Example:** "admin usergroup" **Type:** *String*
unassignedUserGroup *Array*	(Optional) Mention the array of user groups to be unassigned. **Example:** "[ ]"

Response Structure

- **Status Code:** 200 OK
- **Message:** Success
- **Headers:**
  - **Content-Type:** application/json

Response Parameters

Name	Description
response	Contains the response attributes for create a new resource.
message	Success message or failure description in case of error.
appStatusCode	Application specific status code for the response. Will be non-null for failure response.
tags	More info in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
201 OK	null	Success

HTTP Code	appStatusCode	Response Message
400 Bad Request	ACCT_SA_003	Service account is invalid/not found.
404 Not Found	ACCT_USERGROUP_027	UserGroup not found.

Sample Request/Response

Use Case

To assign/unassign user groups to service account.

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/platform-assign-usergroup-to-service-account?gwsource=web
```

Request Payload

```
{
"payload": {
"loginName": "internal90",
"assignedUserGroup": [
"admin usergroup"
],
"unassignedUserGroup": [
]
}
}
```

Sample Response

```
{
"response": "success",
"message": null,
"appStatusCode": null,
"tags": null,
"headers": null
}
```

Glossary

This section describes common terms used in this guide.

Acronyms and Abbreviations

Term/Abbreviation	Expansion
ACL	Access Control List
API	Application Programming Interface
HSM	Hardware Security Module
HTTPS	Hypertext Transfer Protocol Secure
SMTP	Simple Mail Transfer Protocol
URI	Uniform Resource Indicator
URL	Uniform Resource Locator

Chapter 3: Reporting User Guide

This guide describes AppViewX's Build Your Own Report (BYOR) tool and provides step by step instructions on creating customized reports using preexisting hooks and query builder, sharing and scheduling reports, performing actions on reports (pin, share, clone, delete), associating workflows to reports and more.

Module Overview

AppViewX's Build Your Own Report (BYOR) report builder is a low-code reporting and product usage analytics tool that empowers non-technical users to build best-in-class reports and eliminates dependence on development teams. AppViewX's Reporting platform showcases interactive dashboards that display compelling report data, thereby assisting in smarter decision making.

With AppViewX's BYOR you can:

- **Explore pre-shipped reports:** Application Delivery, Security, Certificate, and Automation.
- **Build your own reports (BYOR):** Build customizable reports using Low Code report builder.
- **Access multiple data sources:** Query explorer, REST API, Script.

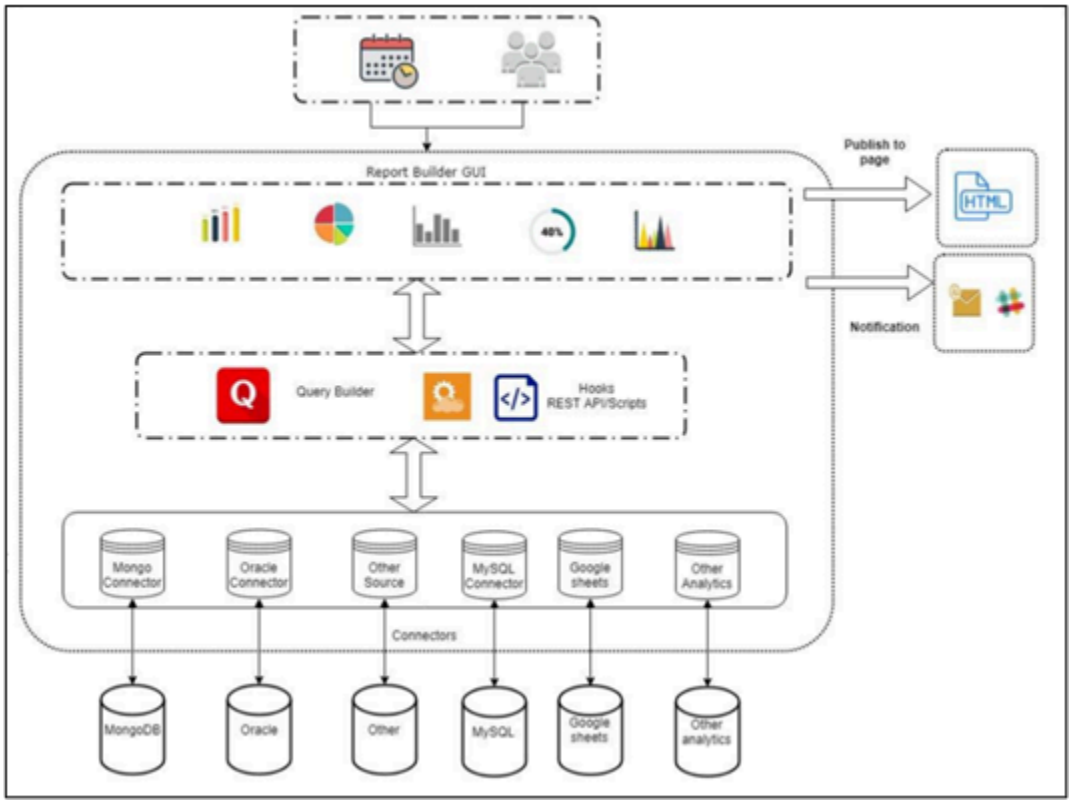
- **WYSIWYG:** What you see is what you get, preview reports as you build them.
- **Configure chart drilldowns:** Add detailed levels of data to your reports.
- **Visualize your data:** Pin reports to a self-service dashboard for quick access and insights.
- **Schedule reports:** Schedule and share reports as email attachments (PDF, xls, csv).
- **Build actionable reports:** Integrate with workflows for actionable reports and auto remediation.
- **Connect to your data:** Study data quickly and easily through product & feature usage report metrics.
- **Reduce turnaround time:** Increased efficiency with automation of the reporting process.

Prerequisites

Web Browser Requirement

Browsers	Version
Internet Explorer	v11.0.9600.18817 or later
Firefox	118.0.1 (64-bit) or later
Google Chrome	117.0.5938.134 (Official Build) (64-bit) or later

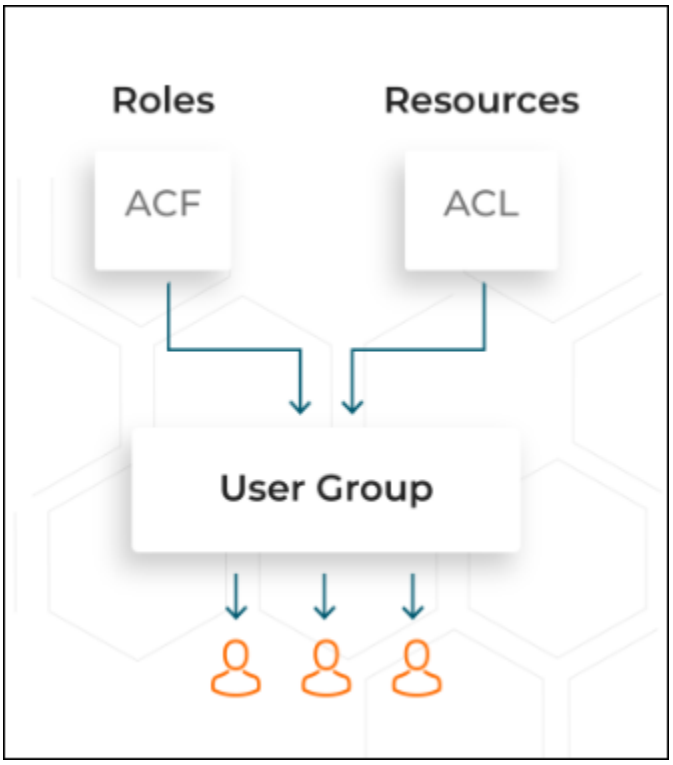
Reference Architecture



The plug-in as part of the above architecture is **avx-commons**.

Configuring Role Based Access Control

AppViewX offers comprehensive support for Role and Resource-Based Access Control (RBAC). RBAC is a method of restricting AppViewX functions, network resources that can be managed and monitored in AppViewX based on the roles of individual users within an enterprise. It allows you to integrate with the existing identity stores such as Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) to enforce authorization policies. Roles and Resources can be customized to suit any organizational structure and user requirements.



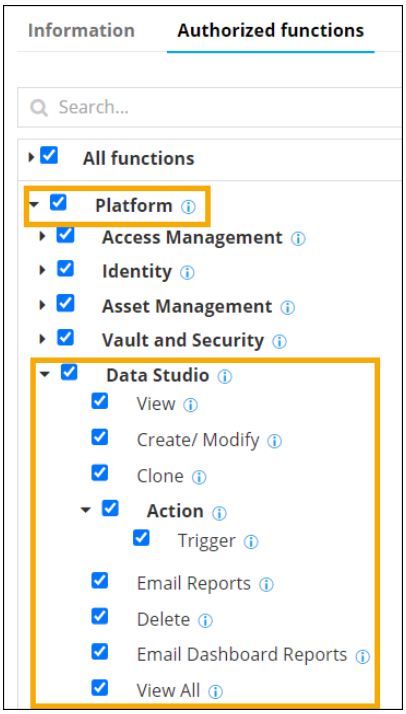
RBAC lets employees have access rights only to the AppViewX functions and network resources they need to do their jobs and prevents them from accessing information that doesn't pertain to them.

To get an overview of the actions that can be permitted or restricted in the Reports module:

New Menu	Old Menu
In the **Platform** module, from the left pane, under **IDENTITY**, select **Role**. The **Role** page is displayed, with all the roles listed with their **Name**, **Description**, and **Status**.	From the main menu, select **Account** > **Role**. The **Role** page is displayed, with all the roles listed with their **Name**, **Description**, and **Status**.

Note: For more information on how to switch between menus, click here.

1. On the **Role** page, select any role from the list of roles, for example **admin**.
2. To see the list of permissions that can be defined for this role, under the **Authorized Functions** tab, click ▸ to expand **Platform** and then expand **Data Studio**. A selected checkbox indicates that the corresponding action has been authorized in the Reports module.



The following table describes the various actions that can be authorized or restricted in the **Reports** module:

Action	Description
View	Provision to allow or restrict a user to view detailed information on the reports created by the logged in user.
Create/Modify	Provision to allow or restrict a user to create or modify a report.
Clone	Provision to allow or restrict a user to clone existing report(s).
Action > Trigger	Provision to allow or restrict a user to execute reports across AppViewX.
Email Reports	Provision to allow or restrict user access to email reports in My Reports, Store, Widget in PDF format and manage scheduling.
Delete	Provision to allow or restrict a user to delete existing report(s).
Email Dashboard Reports	Provision to allow or restrict a user to email entire dashboards in a PDF format.
View All	Provision to allow or restrict a user to view detailed information on existing reports created for all users.

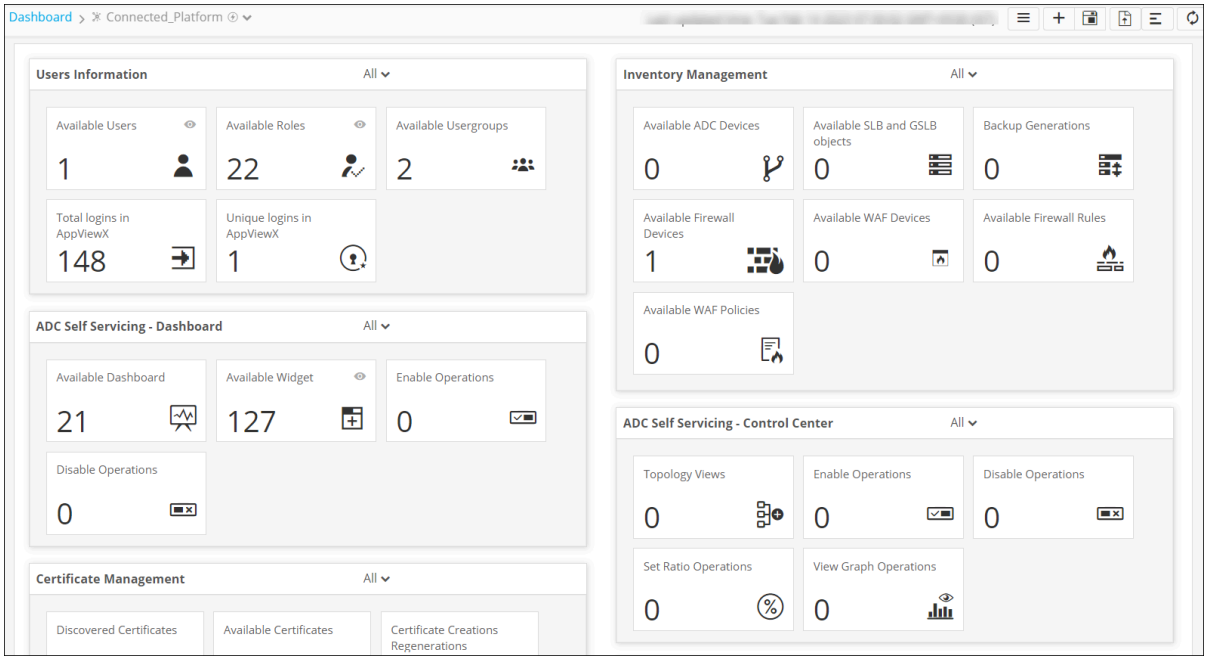
Note: If you are using the old menu, under the **Authorized Functions** tab, expand **Studio** > **Reports**.

3. Once the required permissions have been assigned, click **Save**.

Getting Started with Dashboards

Dashboards allow you to manage, monitor, and interpret all configured applications and their objects. Widgets on the dashboard display reports that provide consolidated statistics of all accessible certificates, devices, and objects by extracting data from the respective inventories and recording the key value indicators.

- **Legacy dashboards:** These are hard-coded dashboards displaying predefined widgets to serve specific use cases. Widgets and reports on these dashboards cannot be modified or downloaded. For example: **Connected Platform**.



The following table describes the options available on this dashboard:

Options	Description
Dashboard name	Displays the name of the current dashboard.

Options	Description
	Allows you to navigate to the Dashboard inventory.

Options	Description
	Allows you to create a dashboard/widget.

Options	Description
	Allows you to save the dashboard.

Options	Description
	Allows you to align the widgets on the dashboard.

Options	Description
	Refreshes the dashboard.

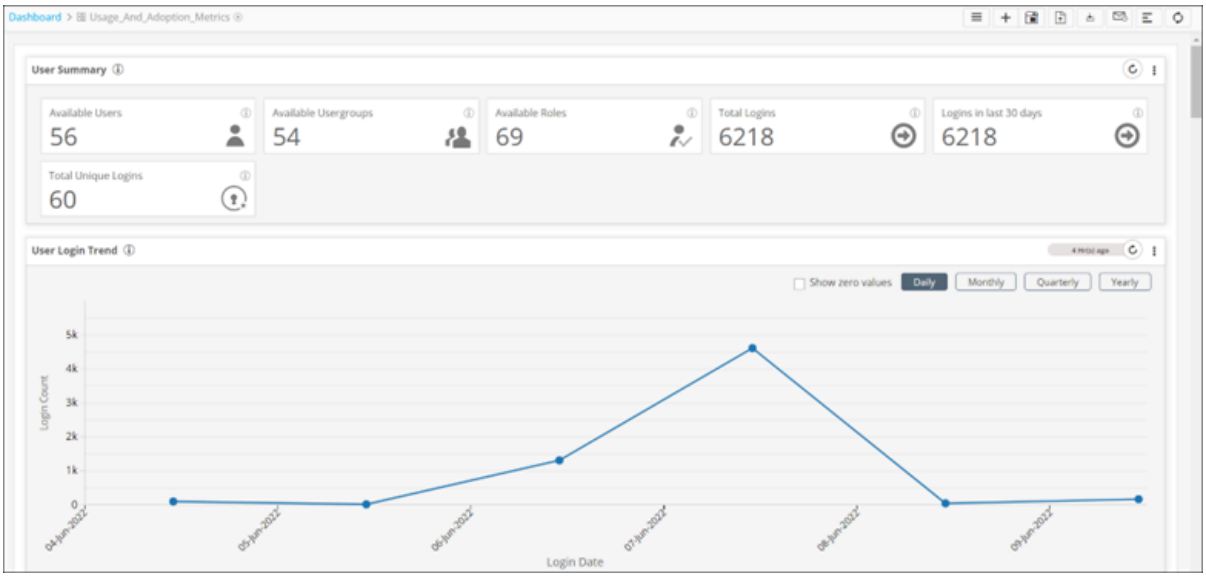
- **Custom dashboards:** These dashboards display reports and widgets created and pinned by the user. Widgets and reports on these dashboards can be added, removed, or modified as necessary and can also be shared among multiple roles. These dashboards can also be downloaded to your laptop. For example: Usage and Adoption Metrics, License Usage, and so on.

- Usage and Adoption Metrics Dashboard
- Accessing the Dashboard Inventory
- Building a Custom Dashboard
- Pinning Reports to a Dashboard
- Downloading a Dashboard

Usage and Adoption Metrics Dashboard

Product Usage and Metrics is a useful tool for understanding the interactions between the customer and your product/service. It helps capture day to day information on how the product or service is being used by customers. Moreover, it can help capture the duration, frequency, feature usage, activity logs. Analyzing this data empowers you to provide an improved customer experience.

The **Usage and Adoption Metrics** dashboard displays predefined widgets to provide the AppViewX metric usage reports and up-to-the-minute reports. It contains the status and statistics of devices and certificates managed within the AppViewX platform. It displays reports related to user summary, logins, user activity, asset inventory and more.

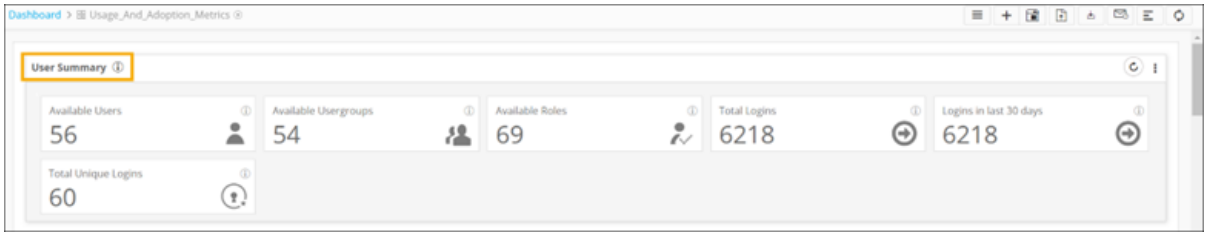


The following table describes the options available on this dashboard:

Options	Description
Dashboard name	Displays the name of the current dashboard.
	Allows you to navigate to the Dashboard inventory.
	Allows you to create a dashboard/widget.
	Allows you to save the dashboard.
	Allows you to export the dashboard.
	Allows you to download the dashboard to your laptop.
	Allows you to schedule and email reports from the dashboard.
	Allows you to align the widgets on the dashboard.
	Refreshes the dashboard.

Following are the various reports and metrics that are available on this dashboard:

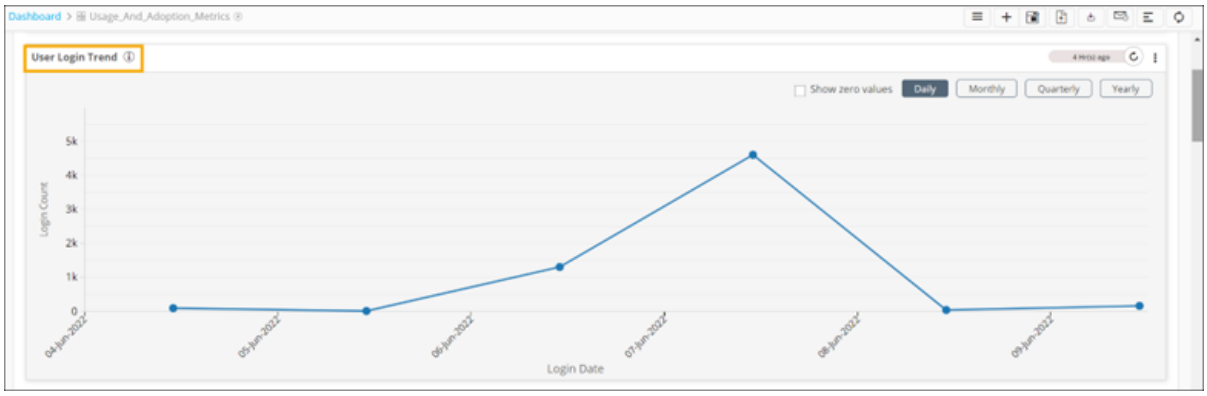
- The **User Summary** report gives a snapshot of user login, summary, and trends.



The following table describes the metrics displayed in this widget:

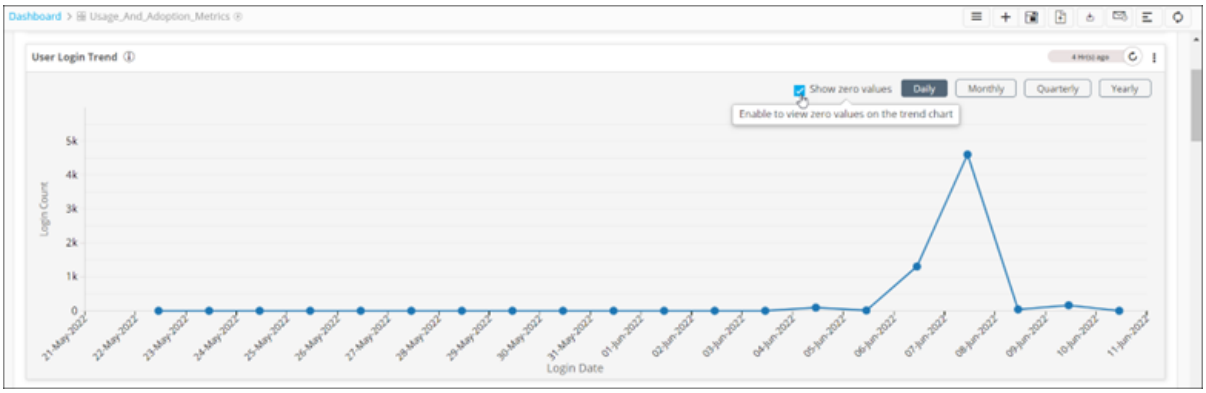
Metric	Description
Available Users	This metric displays available users in AppViewX.
Available User Groups	This metric displays available user groups in AppViewX.
Available Roles	This metric displays the available roles in AppViewX.
Total Logins	This metric displays the total number of logins in AppViewX.
Logins in last 30 days	This metric displays the number of logins in the last 30 days.
Total Unique Logins	This metric displays the total unique logins from different IDs.

- The **User Login Trend** report displays the date-wise count of logins in AppViewX.



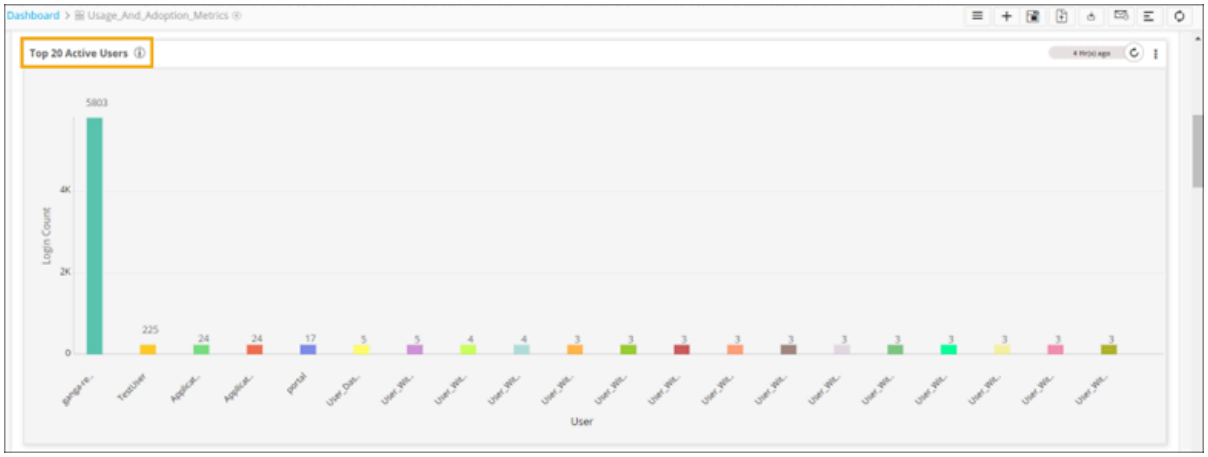
Note: The default selection is set to **Daily**.

- To display dates on which there were zero logins into AppviewX, select the **Show zero values** checkbox.

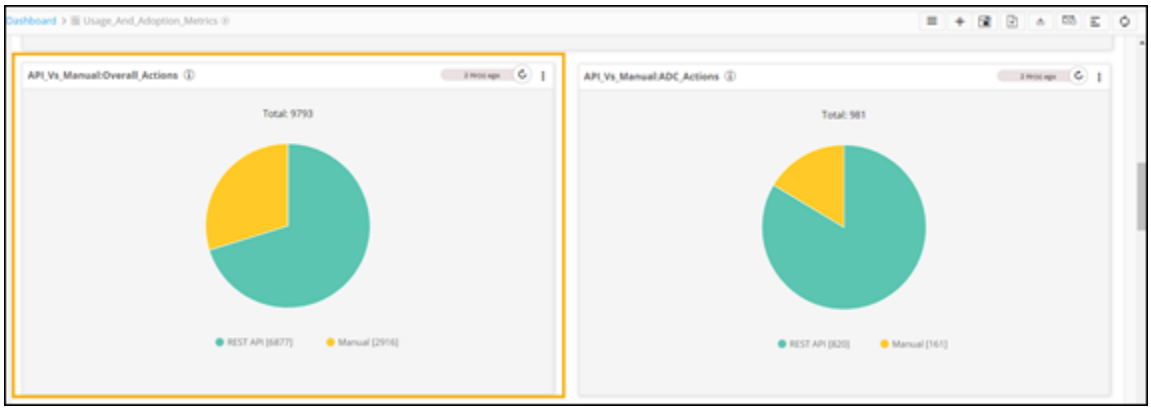


- Select **Monthly**, **Quarterly**, and **Yearly** options to get data based on the respective timelines.

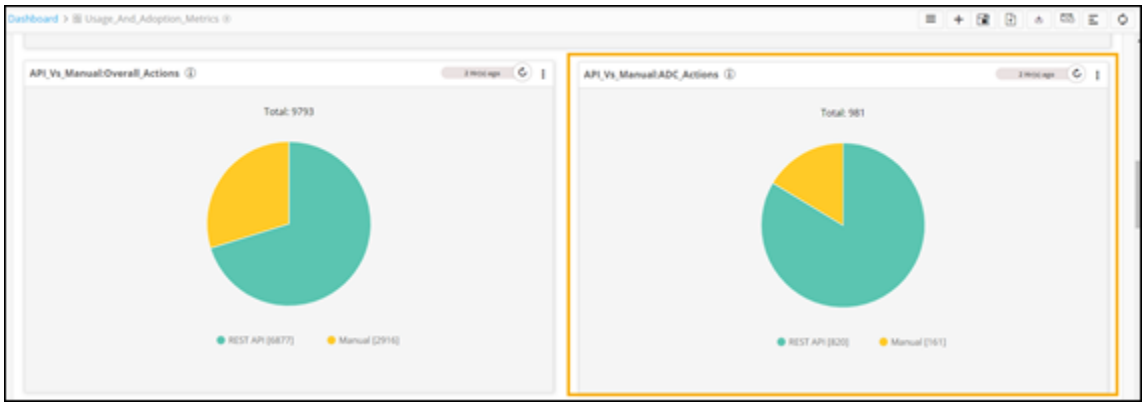
- The **Top 20 Active Users** chart displays the top 20 active users by login count.



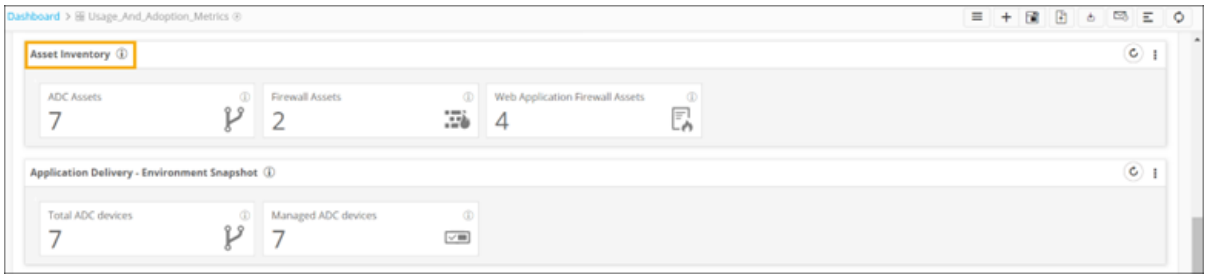
- The **API_vs_Manual:Overall_Actions** pie chart shows the list of actions triggered either manually or via API.



- The **API_vs_Manual:ADC_Actions** pie chart shows the list of ADC actions triggered either manually or via API.



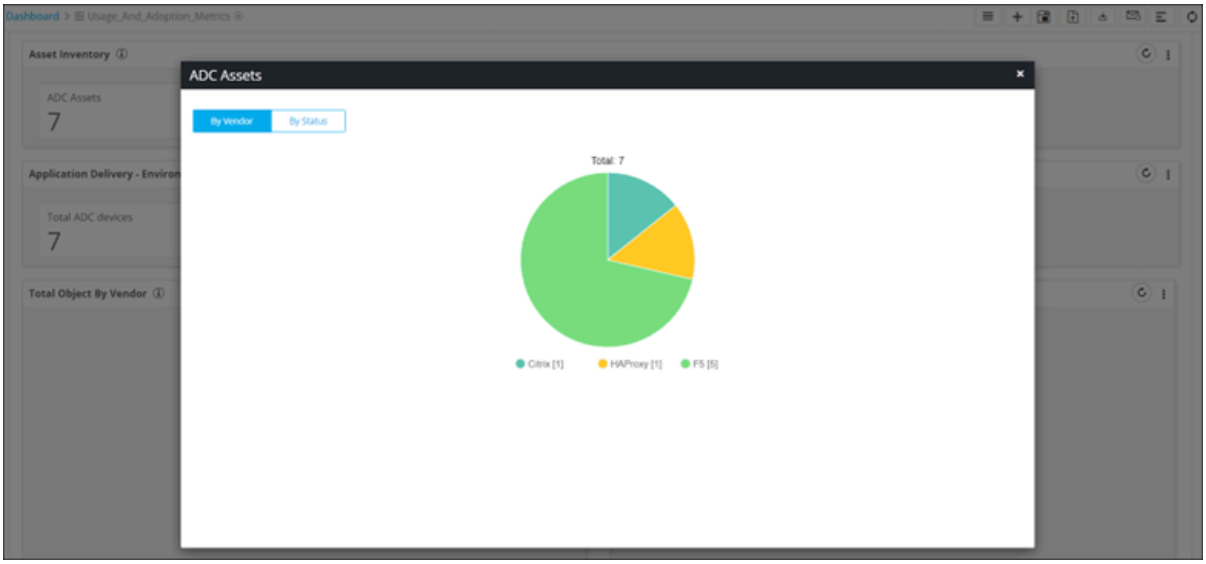
- The **Asset Inventory** widget displays the inventory of different types of assets such as ADC, firewall, and WAF.



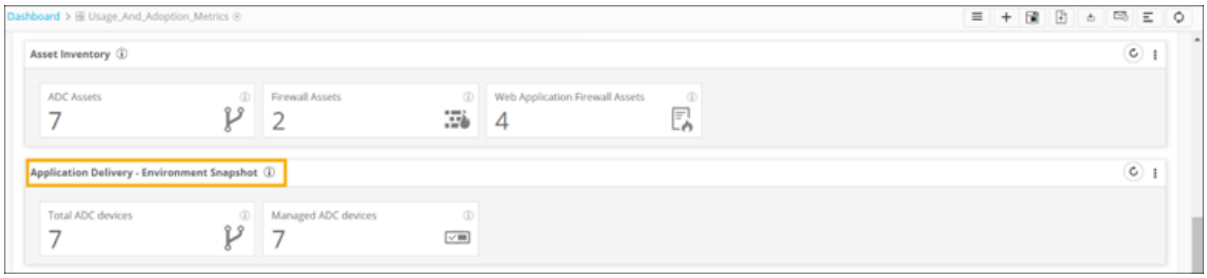
The following table describes the metrics displayed on this widget:

Metric	Description
ADC Assets	This metric displays the total count of all available ADC devices.
Firewall Assets	This metric displays the total count of all available Firewall devices.
Web Application Firewall Assets	This metric displays the total count of all available WAF devices.

- To drill down a chart to display more levels of information, click any metric.



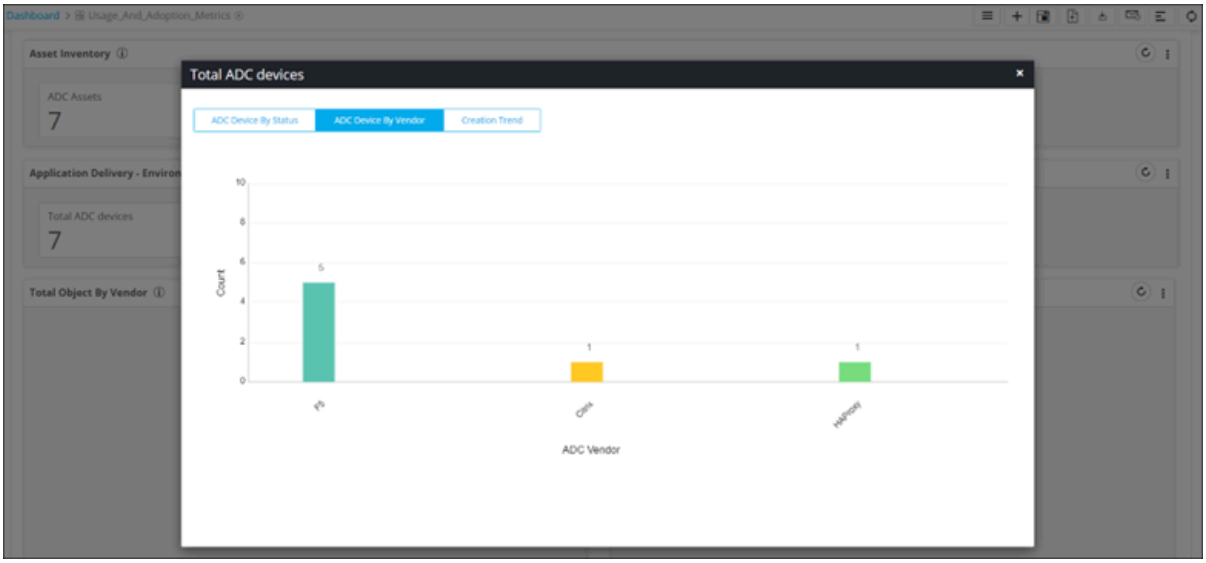
- The **Application Delivery - Environment Snapshot** widget displays a snapshot of application delivery. Each metric displays the total count of respective devices.



The following table describes the metrics displayed on this widget:

Metric	Description
Total ADC devices	This metric displays the total count of all available ADC devices.
Total Application Service Objects	This metric displays the total application service objects.
Managed ADC devices	This metric displays all the managed ADC devices.

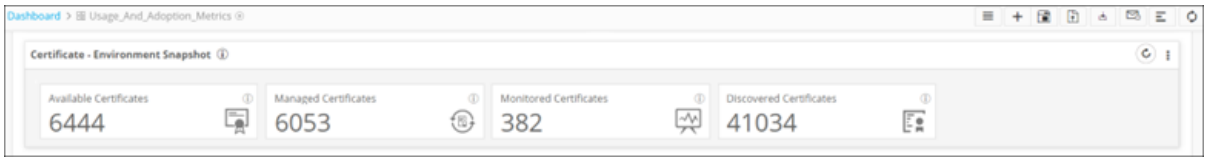
- To drill down a chart to display more levels of information, click any metric.



- The **Total Object by Vendor** pie chart displays the count of all ADC objects by vendor.

- The **Application Service Actions** pie chart shows a snapshot of application services performed.

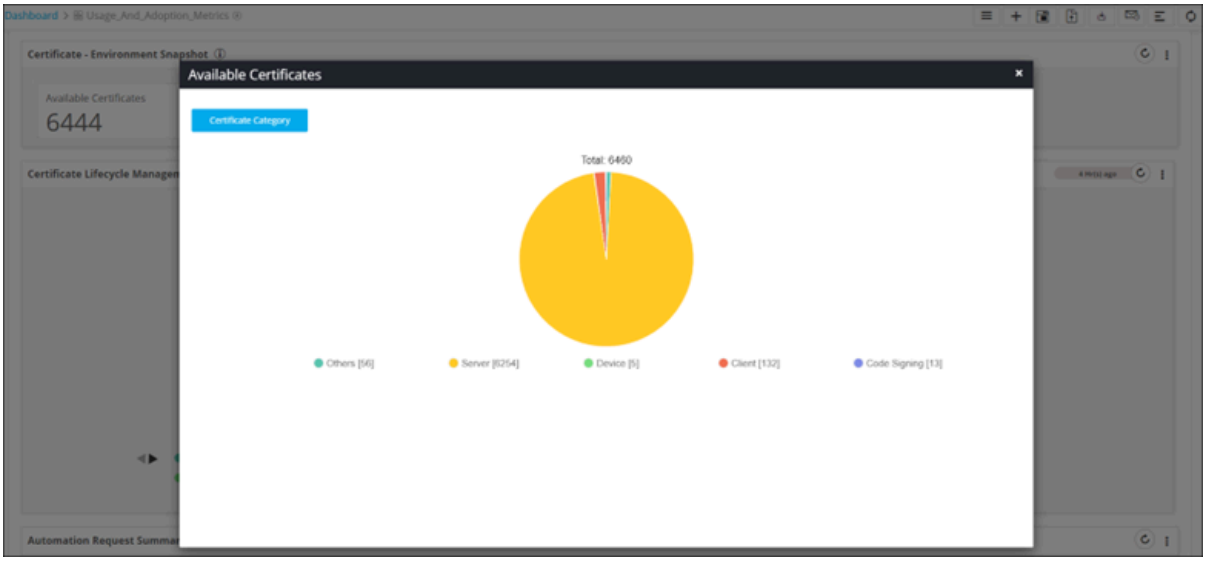
- The **Certificate - Environment Snapshot** widget displays a snapshot of managed and monitored certificates.



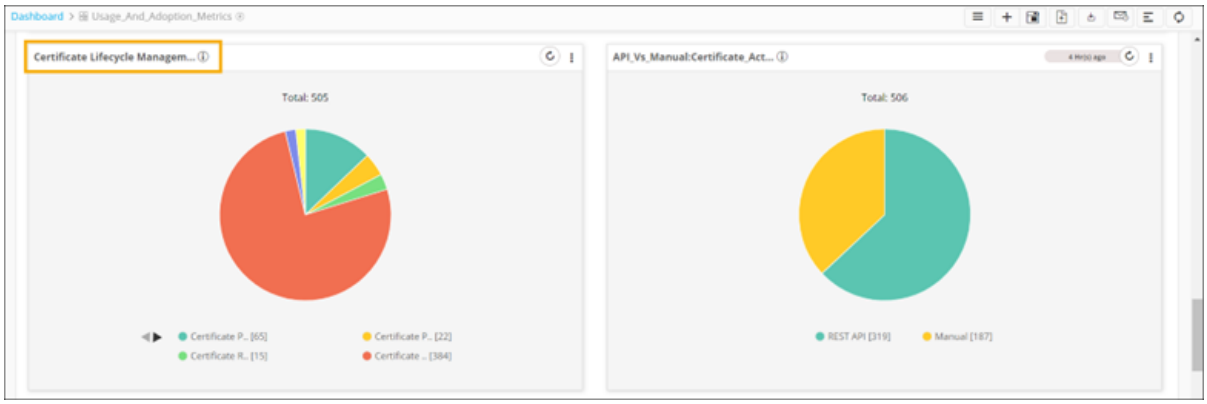
The following table describes the metrics displayed on this widget:

Metric	Description
Available Certificates	This metric displays the total count of all available certificates.
Managed Certificates	This metric displays the total count of all managed certificates.
Discovered Certificates	This metric displays the total count of all discovered certificates.

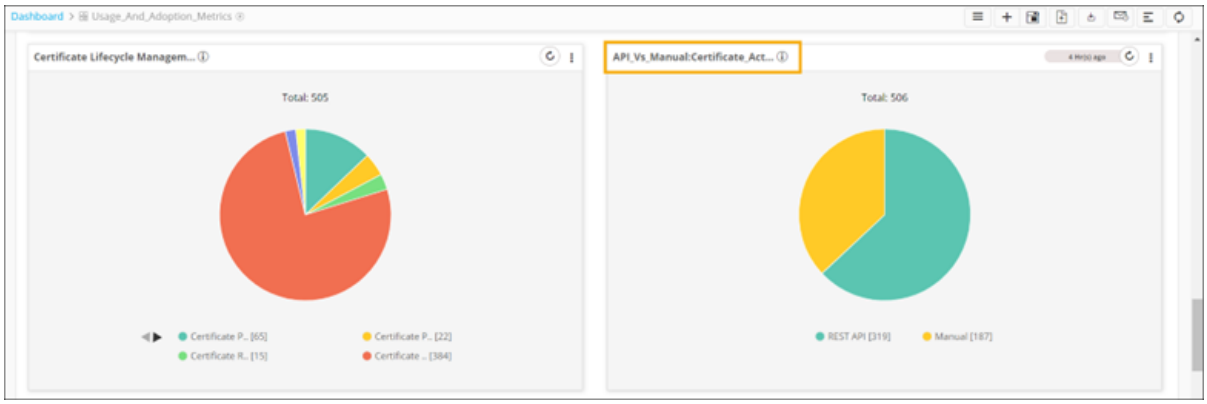
- To drill down a chart to display more levels of information, click any metric.



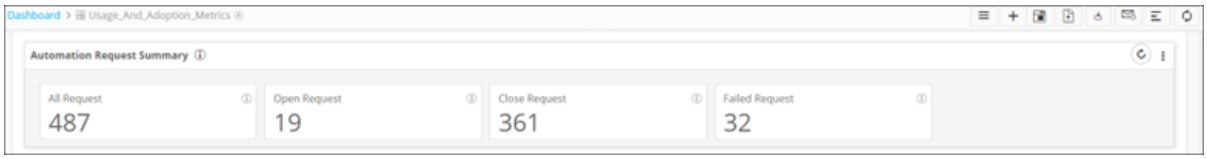
- The **Certificate Lifecycle Management** pie chart displays a snapshot of certificate actions performed, such as certificate push, certificate rollback, certificate push and bind and so on.



- The **API_vs_Manual:Certificate_Actions** pie chart shows a list of certificate actions triggered either manually or via API.



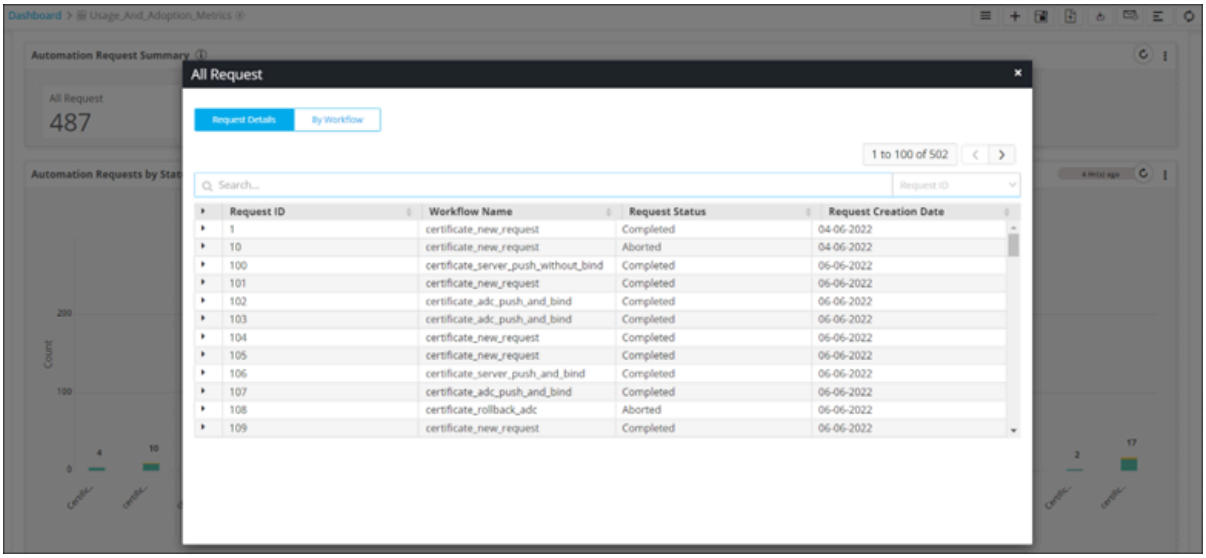
- The **Automation Request Summary** widget displays a snapshot of automation request status and trend.



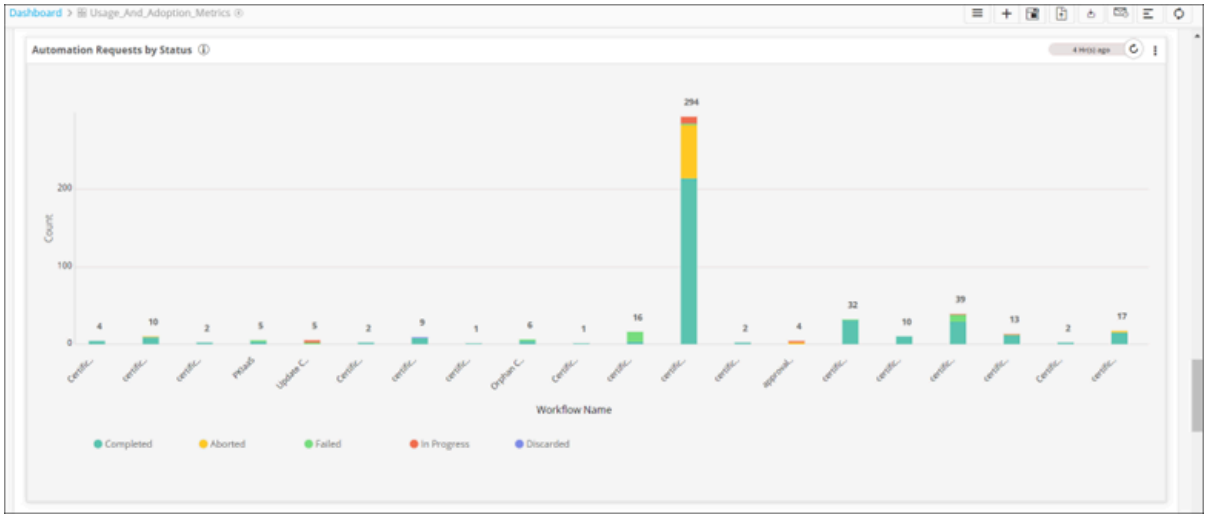
The following table describes the metrics displayed in this widget:

Metric	Description
All Request	This metric displays the count of total workflow automation requests.
Open Request	This metric displays the count of open workflow automation requests.
Close Request	This metric displays the count of closed workflow automation requests.
Failed Request	This metric displays the count of failed workflow automation requests.

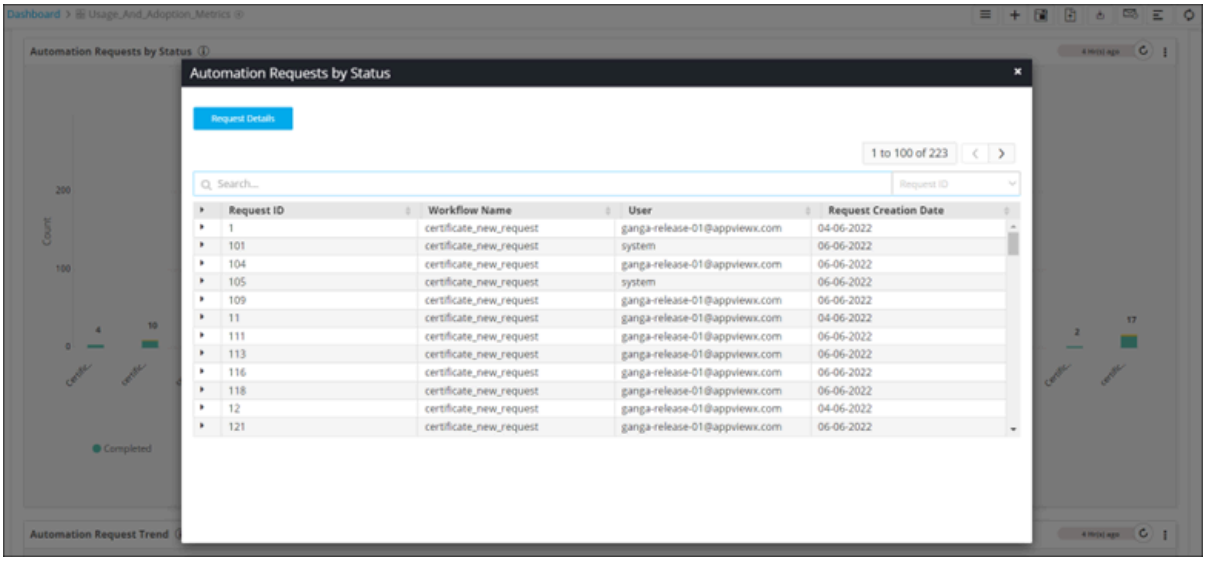
- To drill down a chart to display more levels of information, click any metric.



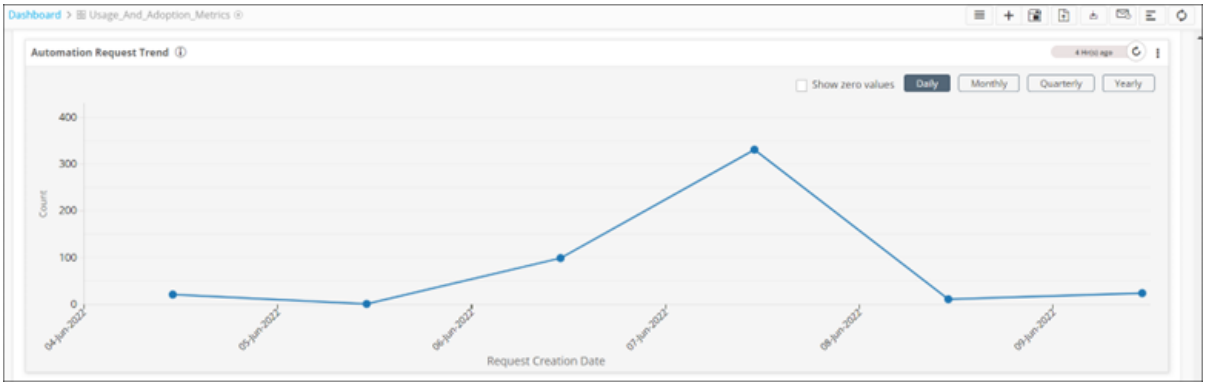
- The **Automation Request by Status** stacked bar graph displays the request status by workflow.



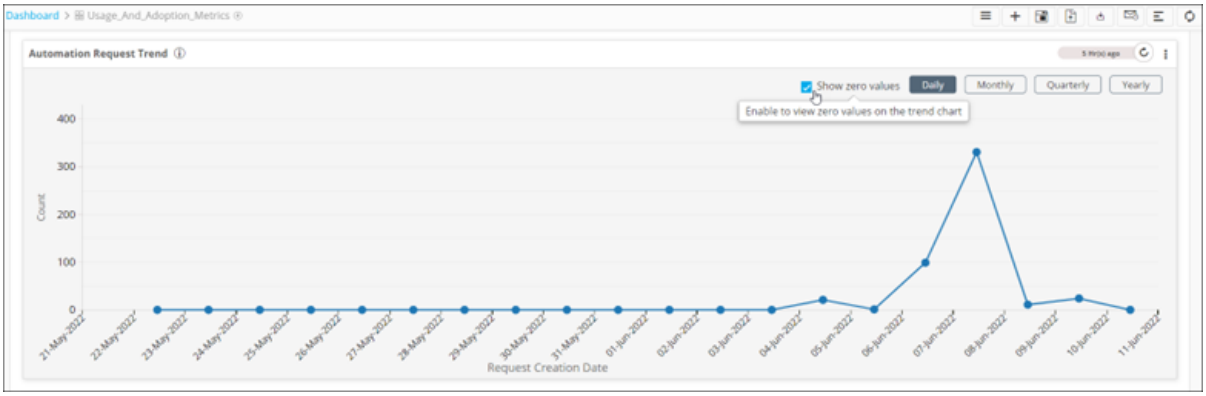
- To drill down a chart to display more levels of information, click any metric.



- The **Automation Request Trend** line chart displays the trend of all automation requests.

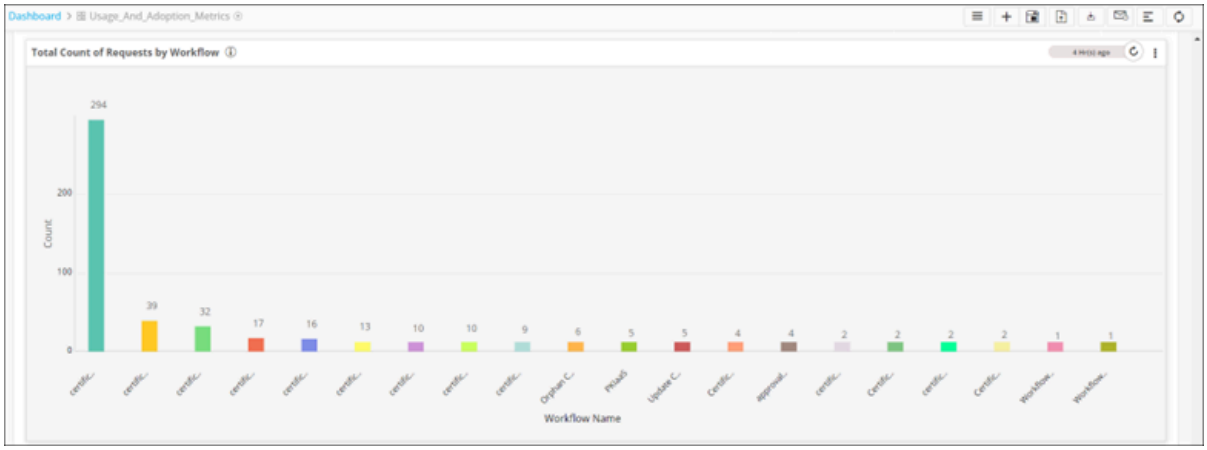


- To display dates on which there were zero logins into AppviewX, select the **Show zero values** checkbox.

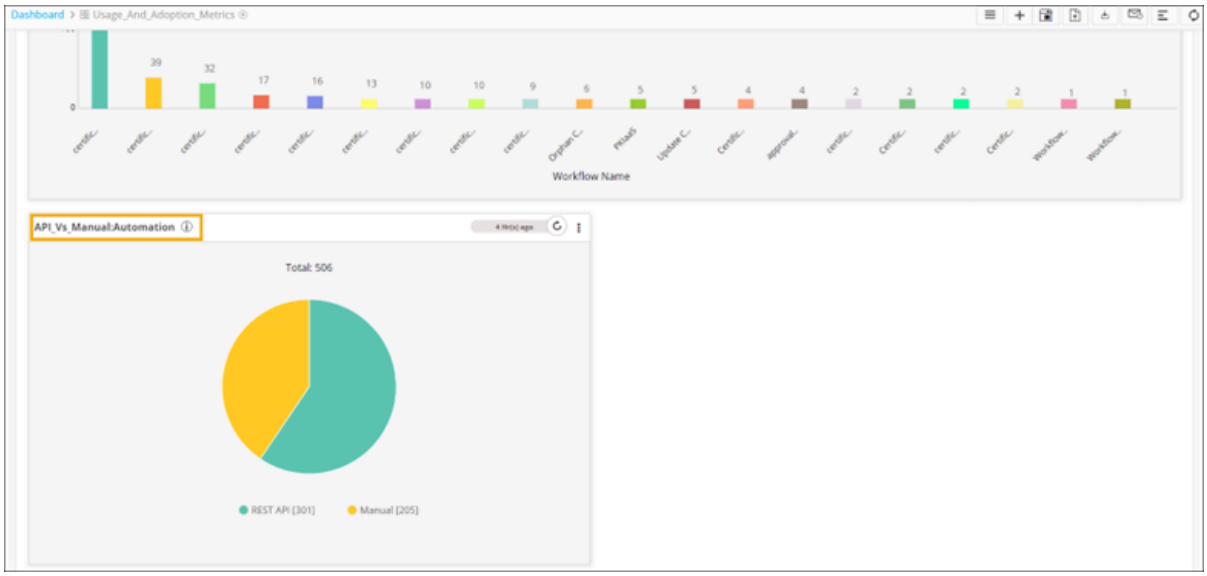


- To get data based on the respective timelines, click **Monthly**, **Quarterly**, and **Yearly** buttons.

- The **Total Count of Requests by Workflow** bar graph displays the total count of requests by workflow.



- The **API_vs_Manual:Automation** pie chart displays a list of automation requests triggered either manually or via API.



Accessing the Dashboard Inventory

New Menu	Old Menu
In the **ADC+** or **CERT+** module, from the left pane, click **Dashboards**. The default dashboard is displayed.	From the main menu, select **Dashboards**. The default dashboard is displayed.

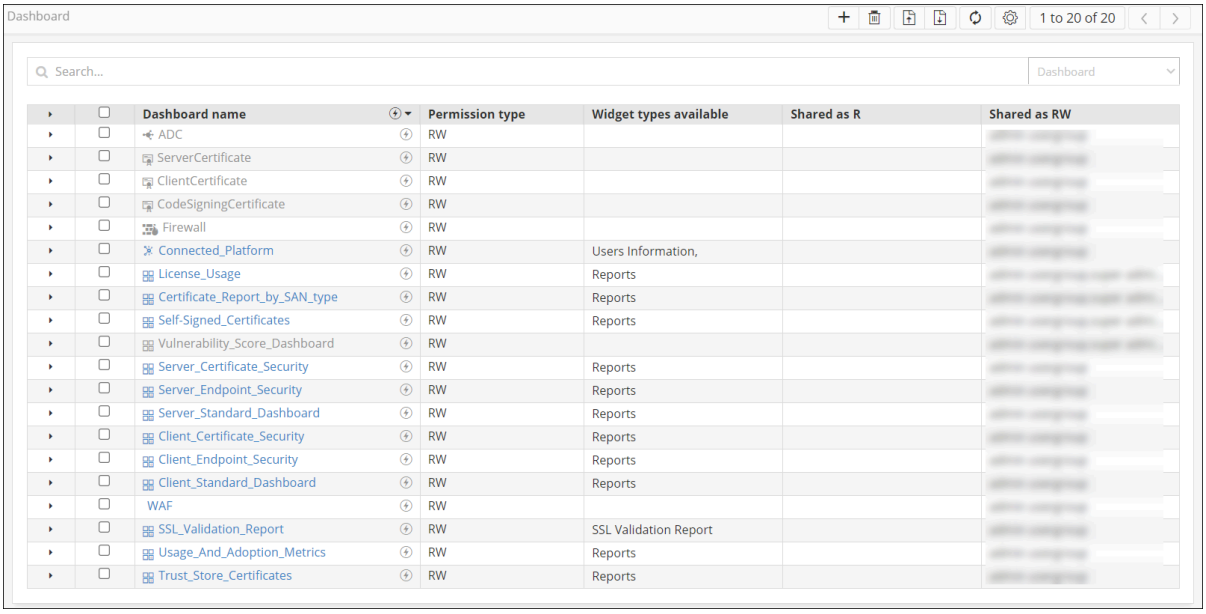
New Menu	Old Menu

Note: For more information on how to switch between menus, click here.

From the top left corner of the screen, click **Dashboard**.

Tip: You can also click ☰ from the command bar on the top right to navigate to the **Dashboard** inventory page.

The dashboard inventory is displayed.



The following table describes the various options available on the **Dashboard** inventory page:

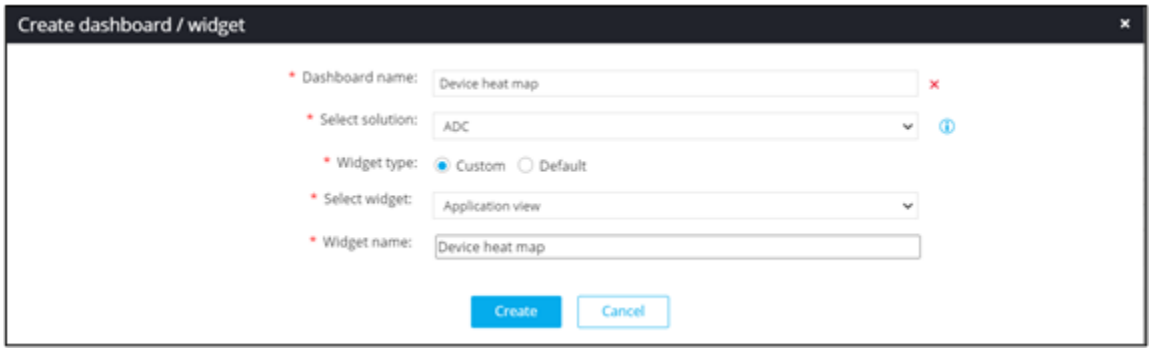
Options	Description
Search bar	Searches for the given keyword(s) in the field and shows a list of results that match the searched keyword(s).
⚡	Allows you to assign the dashboard as the default dashboard that is displayed when the user logs in.
+	Allows users to create a new dashboard.

Options	Description
	Allows users to delete a dashboard from the list.
	Allows users to export a dashboard from the list.
	Allows users to import a file to create a dashboard.
	Refreshes the page by clicking on the refresh button.
	Allows users to auto-sort the dashboards alphabetically.

Building a Custom Dashboard

You can build a custom dashboard to display a specific set of reports.

1. On the Dashboard inventory page, from the top right corner of the screen, click **(Add)** icon in the command bar.
   The **Create dashboard / widget** pop-up window is displayed.
2. Enter or select the required field information.



The following table describes the field description to create a custom dashboard:

Field	Description
***Dashboard name**	Enter the name of the dashboard.
***Select solution**	ADC is the default selection. You can add widgets belonging to multiple solutions to this dashboard.

Field	Description
***Widget type**	Select the type of widget as: • **Custom**: Choose this option to build a customized widget. • **Default**: Choose this option to select the default widget.
***Select widget**	Select an required widget from the customized widgets in the dropdown.
***Widget name**	Enter the name of the widget.
Note: The asterisk (*) symbol indicates mandatory fields.	

3. Click **Create**.
   A new dashboard is created. You can now pin reports and widgets to this dashboard as per your requirement.

Pinning Reports to a Dashboard

You can pin customized reports to an existing dashboard or a new dashboard. A maximum of 20 reports can be pinned to a dashboard. Pinning a report to the dashboard allows users to visualize different reports in the same place.

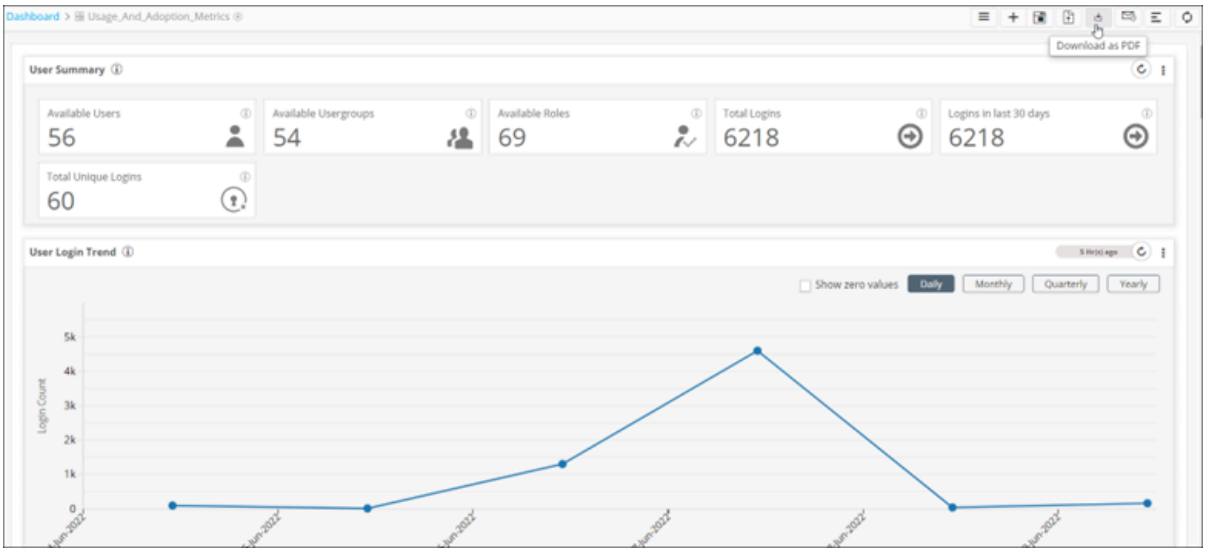
Note: For more information on how to pin a report to the dashboard, click here.

Downloading a Dashboard

You can also download an entire dashboard as a PDF to your device.

Note: You can only download Custom dashboards and not Legacy dashboards.

1. On the Dashboard inventory page, click on a dashboard name.
   The selected dashboard is displayed on the screen.
2. To download the dashboard as a PDF file, from the command bar on the top right corner of the screen, click **(Download)** icon.



The dashboard is downloaded to your device as a PDF.

3. To view the dashboard in PDF format, click on the downloaded file.

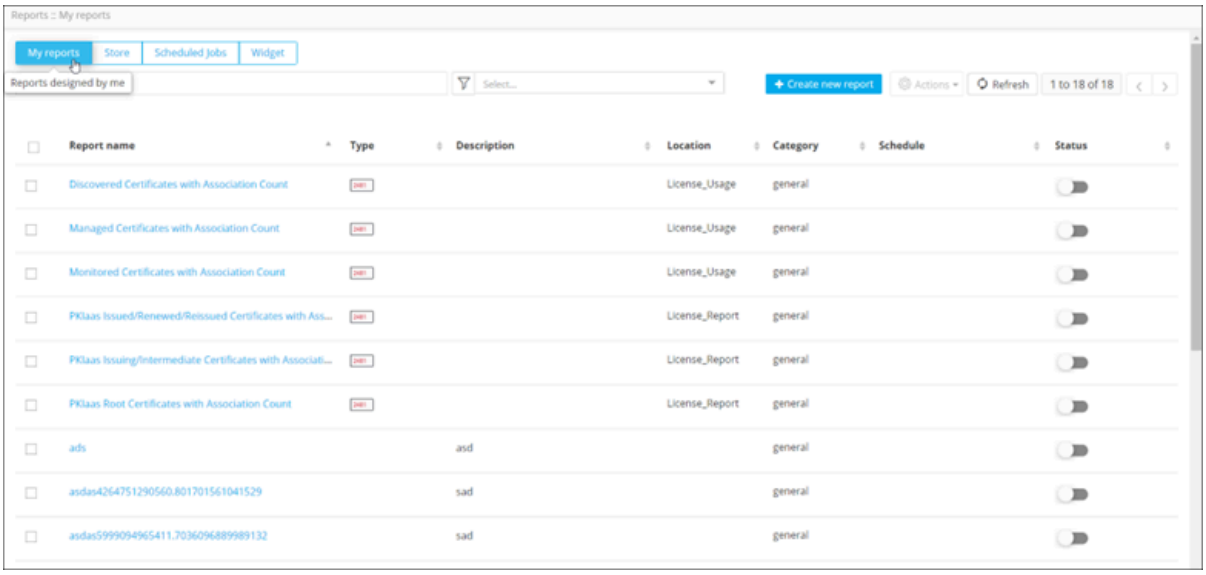
Accessing the Reports Module

New Menu	Old Menu
In the **Platform** module, from the left pane, under **DATA STUDIO**, select **Reports**. The **Reports :: My Reports** page is displayed.	From the main menu, select **Studio** > **Reports**. The **Reports :: My Reports** page is displayed.
Note: For more information on how to switch between menus, click here.	

- My Reports
- Store
- Scheduled jobs
- Widget

My Reports

The **Reports :: My reports** page shows the list of all reports created by users.



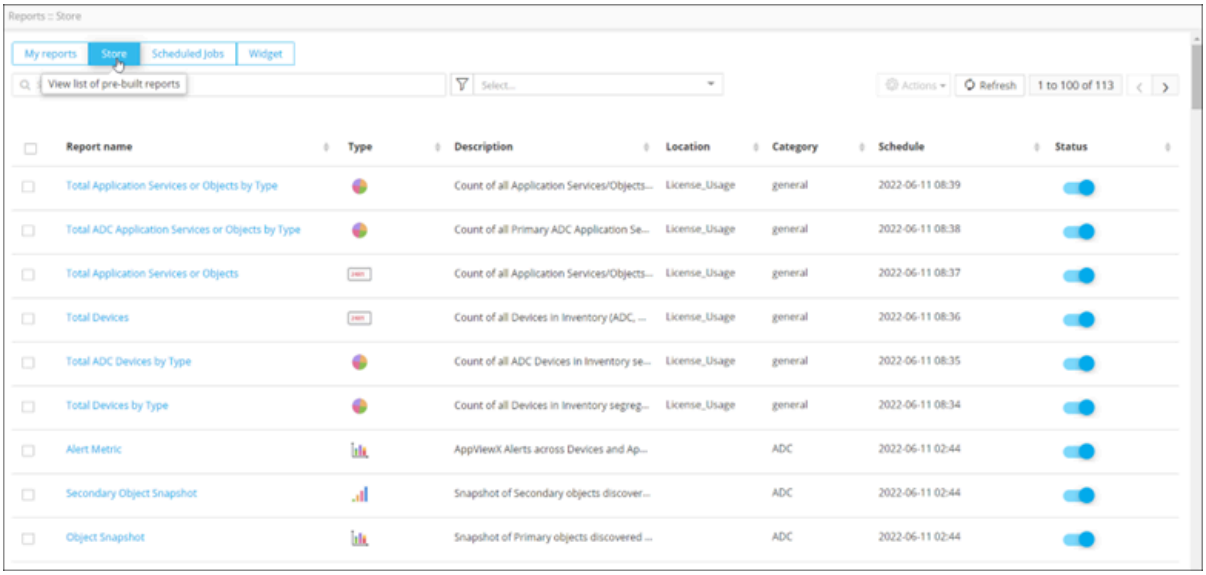
The following table describes the options available on the **My reports** page:

Options	Description
Search bar	Searches for the given keyword(s) in the field and produces results featuring the searched keyword(s).
	Allows you to filter reports according to different categories, such as ADC, Certificate and so on.
Create new report	Allows you to create a new custom report.
Actions	Allows you to perform actions (pin, share, clone, delete) on the reports. **Note:** This option is enabled only when a report(s) is selected.
Refresh	Refreshes the page.
Report name	Displays the names of the reports in alphabetical order (A to Z and Z to A).
Type	Displays reports according to the type - pie, donut, bar, stacked bar, grid, line metric.
Description	Displays a brief description of the report.
Location	Displays the location of the report on the dashboard.

Options	Description
Category	Displays the category of the report - • **General**: This is a default category. • **Certificate**: This relates to Certificate reports specifically. • **ADC**: This relates specifically to ADC reports.
Schedule	Displays the date and time of a scheduled report.
Status	Displays whether a report has been enabled or is disabled.

Store

The **Reports :: Store** page shows a list of ready-to-use reports made available to users.



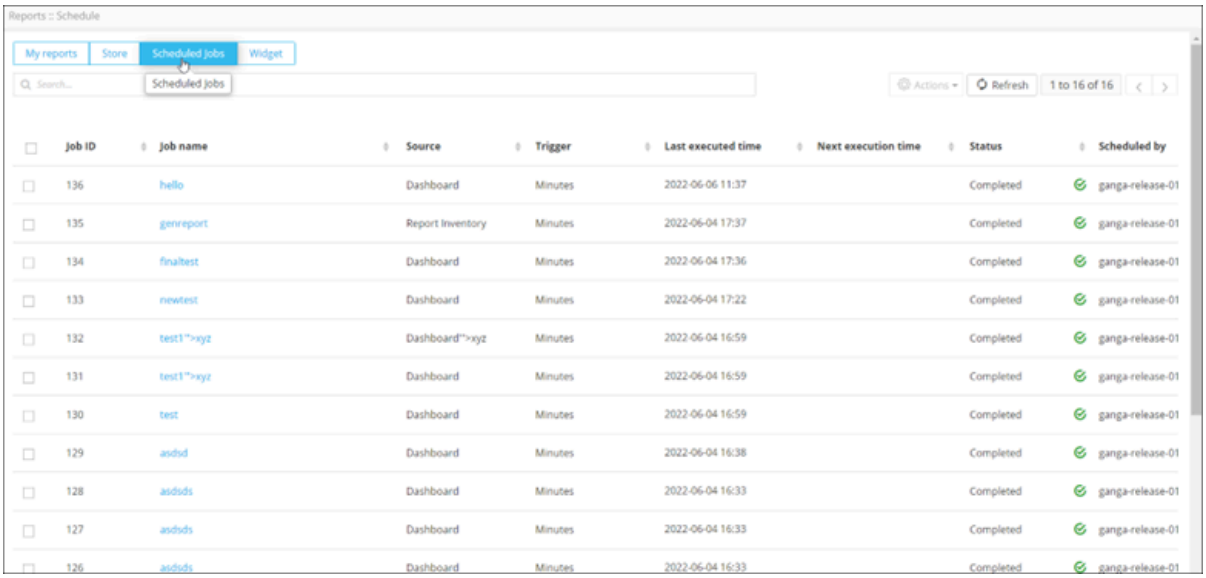
The following table describes the options available under the **Store** page:

Options	Description
Search bar	Searches for the given keyword(s) in the field and produces results featuring the searched keyword(s).
	Allows you to filter reports according to different categories.
Actions	Allows you to perform actions (pin, share, clone) on the reports.

Options	Description
	Note: This option is enabled only when a report(s) is selected. **Note:** You cannot delete reports available in the Store.
Refresh	Refreshes the page.
Report name	Displays the names of the reports in alphabetical order (A to Z and Z to A).
Type	Displays reports according to the type - pie, donut, bar, stacked bar, grid, line metric.
Description	Displays a brief description of the report.
Location	Displays the location of the report on the dashboard.
Category	Displays the category of the report - • **General**: This is a default category. • **Certificate**: This relates to Certificate reports specifically. • **ADC**: This relates to ADC reports specifically.
Schedule	Displays the date and time of a scheduled report.
Status	Displays whether a report has been enabled or is disabled.

Scheduled jobs

The **Reports :: Schedule** page lists all the scheduled jobs or the emails that have been scheduled by a user to trigger at pre-set time intervals.



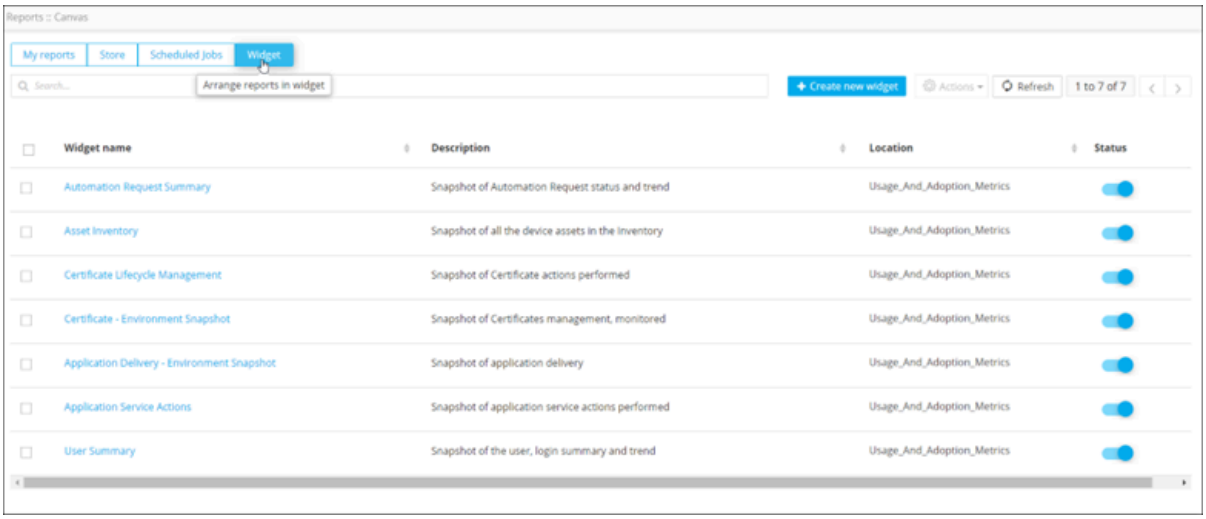
The following table describes the options available under the **Scheduled Jobs** tab:

Options	Description
Search bar	Searches for the given keyword(s) in the field and produces results featuring the searched keyword(s).
Refresh	Refreshes the page.
Job ID	Displays the Job ID.
Job name	Displays the Job name.
Source	Displays the source of the scheduled job.
Trigger	Displays the frequency at which the job is scheduled to be triggered.
Last executed time	Displays the time when the job was last executed.
Next execution time	Displays the time when the job will be executed next.
Status	Displays the status (pause/resume) of the job. You can click on the green arrow to change the status.
Scheduled by	Displays the name of the user who scheduled the job.

Note: For more information on scheduling reports, click here.

Widget

A widget allows you to arrange data in a visually striking display. Only metric charts can be used to create widgets. The **Reports :: Canvas** page shows the list of pre-built widgets available for the user.



This table describes the options available under the **Widget** page:

Options	Description
Search bar	Searches for the given keyword(s) in the field and produces results featuring the searched keyword(s).
Create new widget	Allows you to create a new widget.
Actions	Allows you to perform actions (pin, clone, delete, share) on the widgets. **Note:** This option is enabled only when a widget(s) is selected.
Refresh	Refreshes the page.
Widget name	Displays the names of the widget.
Description	Displays a brief description of the widget.
Location	Displays the location of the widget on the dashboard.
Status	Displays whether a widget has been enabled or is disabled. **Note:** You can enable or disable a widget by turning the toggle on or off.

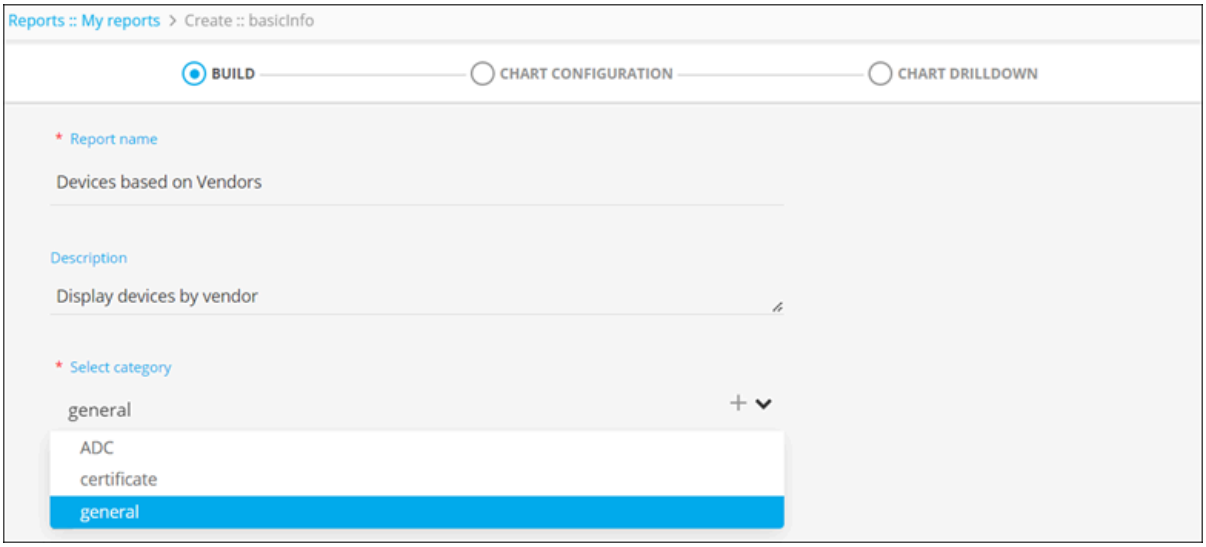
Creating a Report/BYOR

There are three steps involved in creating a report using AppViewX's report builder tool.

- Build
- Chart Configuration
- Chart Drilldown.

Build

1. To create a customized report, on the **Reports :: My Reports** page, click **Create New Report**.
2. On the **Reports :: My reports > Create :: basicinfo** page, under the **BUILD** section, enter or select the required field information.



The following table describes the field information in this section:

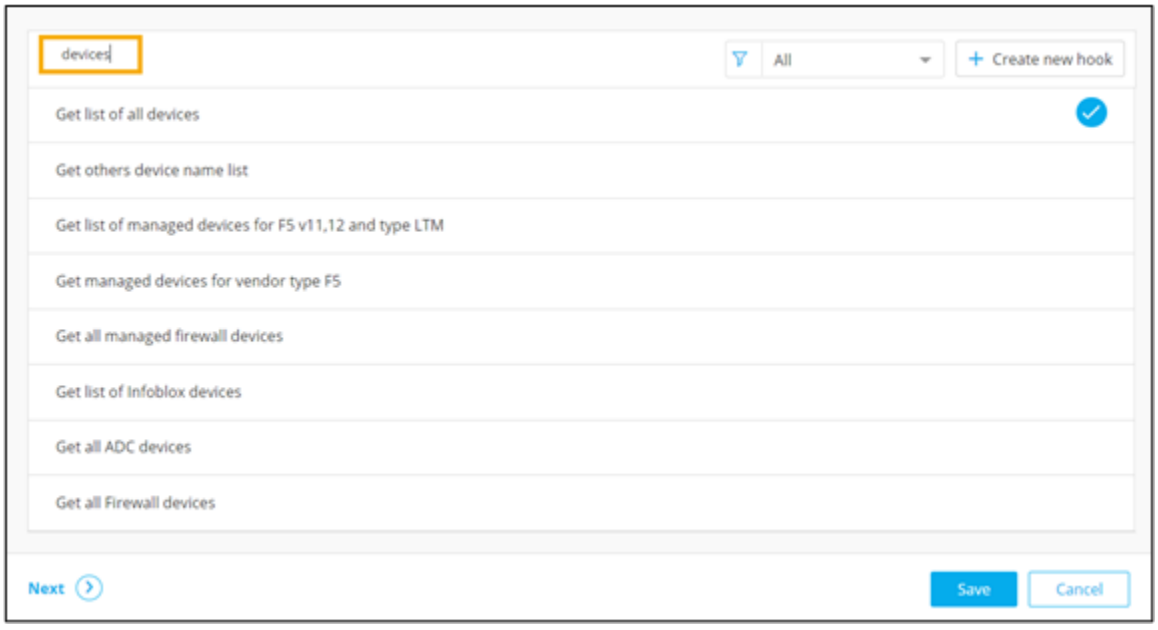
Field	Description
***Report name**	Enter a valid report name. For example: **Devices based on vendors**.
Description	Enter a valid description of the report.

Field	Description
	For example: **Display devices by vendor**.
***Select category**	Select category from the options available in the drop down menu or click + to add a new category. • **Certificate** - Select category as certificate for creating certificate related reports specifically. • **ADC** - Select category as ADC for building ADC related reports specifically. • **General** - Select category as general for all reports.
Note: The asterisk (*) symbol indicates mandatory fields.	

3. To query certificates based on role permissions, select the **ACL Restricted** check box.

Note: Check this box specifically for creating certificate related reports.

4. To query report data, either select a preexisting hook or click **Create new Hook**.



Note: For more information on creating hooks, click here.

5. To save this basic information on the report, click **Save**.

6. To go to the next stage of report building, click **Next**.
   The CHART CONFIGURATION section is displayed.

Chart Configuration

The chart configuration page lists seven types of chart options that can be selected for creating reports. These options are:

- Pie Chart
- Donut
- Bar
- Stacked Bar
- Grid
- Line
- Metric.

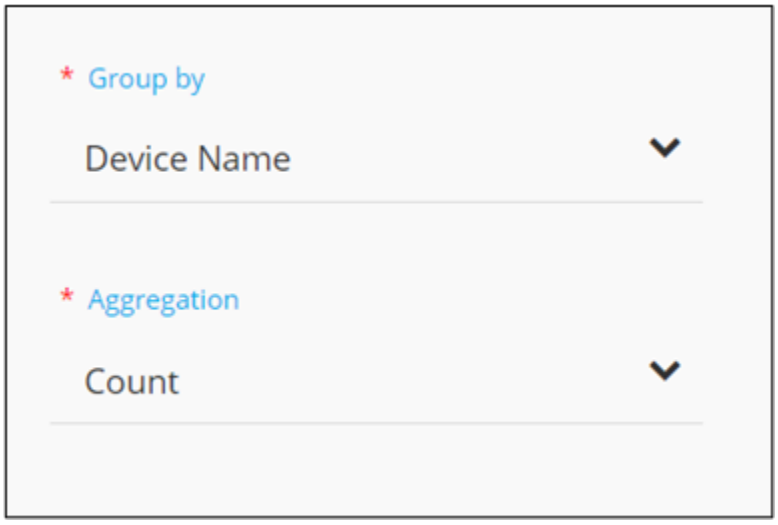
- How to Design a Custom Pie Chart
- How to Design a Custom Donut Chart
- How to Design a Custom Bar Chart
- How to Design a Custom Stacked Bar Chart
- How to Design a Custom Grid Chart
- How to Design a Custom Line Chart
- How to Design a Custom Metric Chart

How to Design a Custom Pie Chart

Creating a report using a pie chart allows you to display multiple classes of data and their proportions. It helps to summarize a large data set visually. It is easy to understand and requires minimal explanation.

To design a custom pie chart:

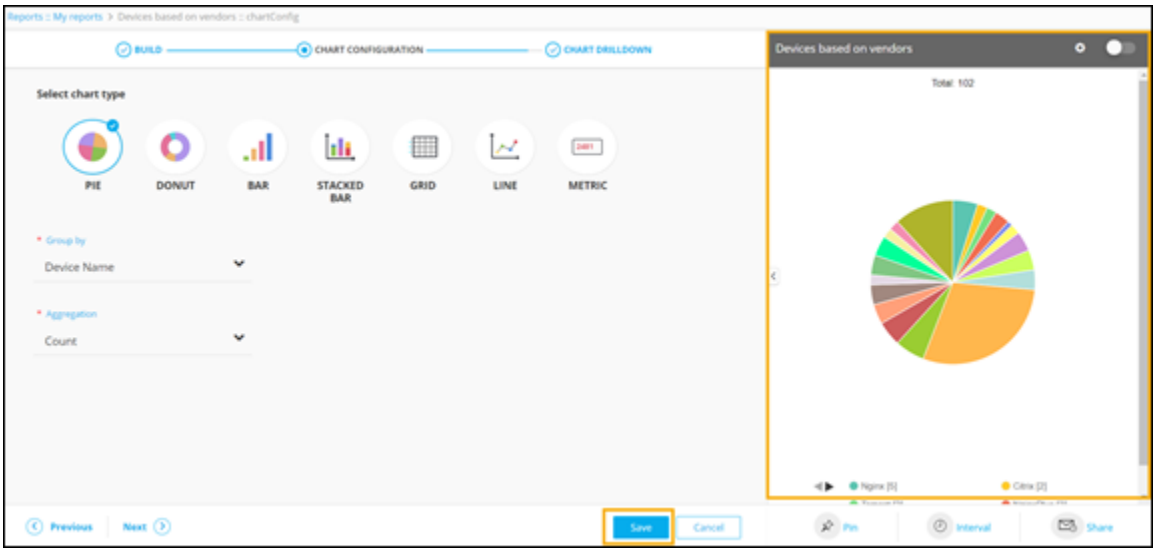
1. Build a report.
2. Under the **CHART CONFIGURATION** section, **Select chart type** as **PIE**.
3. Enter or select the required field information.



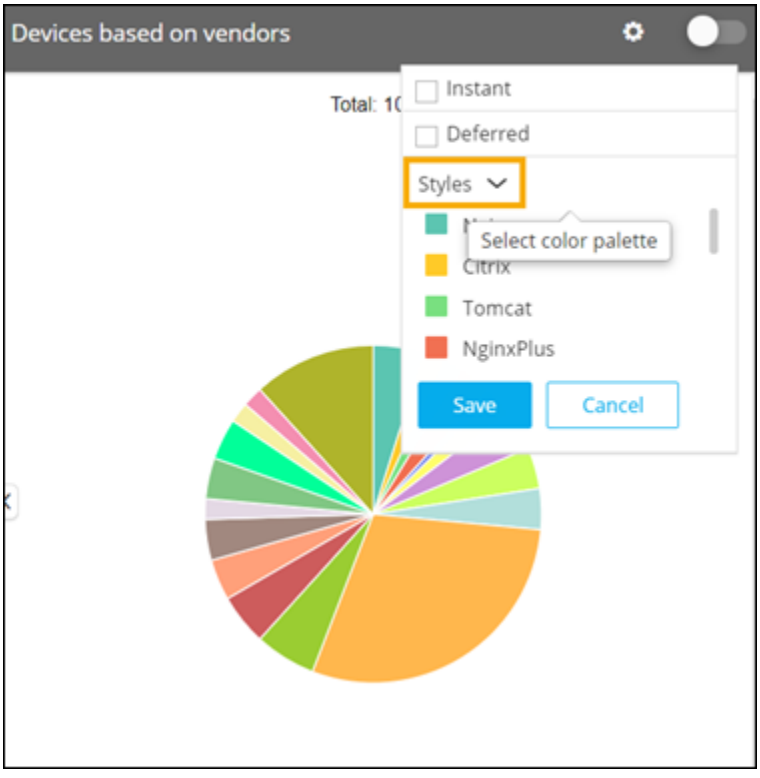
The following table describes the field information in this section:

Field	Description
***Group by**	Select a value from the dropdown menu on the basis of which report data will be grouped. For example: **Device Name**.
***Aggregation**	Select the calculation to be done on the report data for the dropdown. The following options are available: • **Average**: Calculates the average value of a given set of data. • **Sum**: Calculates the sum of all values in a given set of data. • **Count**: Calculates the total number of items in a given numeric field. • **Maximum**: Displays the maximum value in a given set of data. • **Minimum**: Displays the minimum value in a given set of data.
Note: The asterisk (*) symbol indicates mandatory fields.	

4. Click **Save**.
   A preview of the pie chart is generated on the right side of the screen.



5. To select the data loading pattern, in the chart's preview window, click  **(Settings)** icon.
   The following options are displayed:
   - **Instant**: This option allows you to enable live data loading and see changes in data immediately. This can be used in the case of small databases.
   - **Deferred**: This option allows you to enable lazy data loading and is useful in the case of larger databases. The default time interval for this is set at 30 minutes.
6. To change the style/font color of their pie chart, click **Styles**.



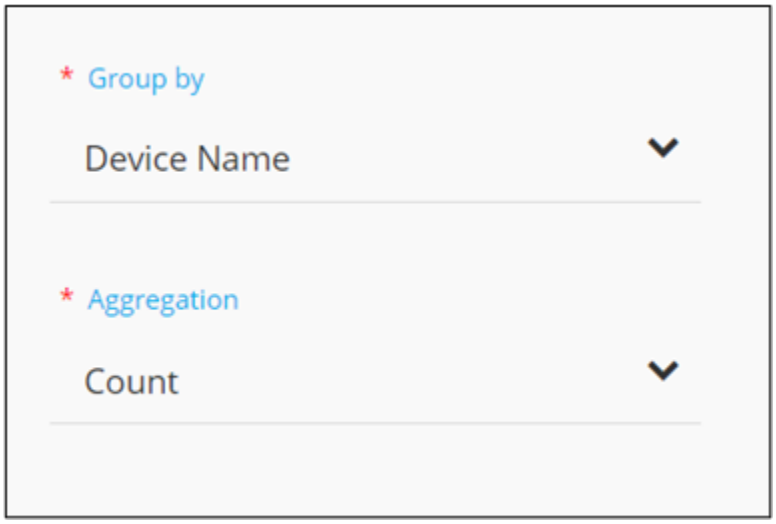
7. To enable the report, turn on the toggle. Only enabled reports are visible on the dashboard to which they are pinned.
8. Click **Next**.
   The CHART DRILLDOWN section is displayed.

How to Design a Custom Donut Chart

A donut chart, similar to a pie chart, allows you to compare between categories and visualize part to whole relationships. A donut chart has the added advantage of having a blank space in the middle where extra information can be supplemented.

To design a custom donut chart:

1. Build a report.
2. Under the **CHART CONFIGURATION** section, select the **DONUT** chart.
3. Enter or select the required field information .



The following table describes the field information in this section:

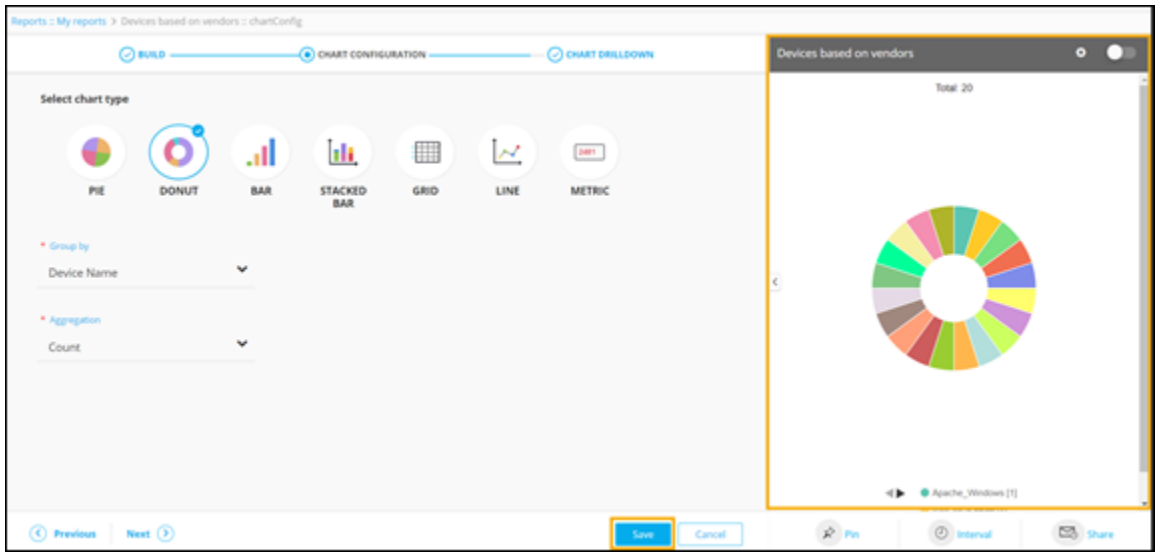
Field	Description
***Group by**	Select a value from the dropdown menu on the basis of which report data will be grouped. For example: **Device Name**.
***Aggregation**	Select the calculation to be done on the report data for the dropdown. The following options are available: • **Average**: Calculates the average value of a given set of data. • **Sum**: Calculates the sum of all values in a given set of data.

Field	Description
	• **Count**: Calculates the total number of items in a given numeric field. • **Maximum**: Displays the maximum value in a given set of data. • **Minimum**: Displays the minimum value in a given set of data.

Note: The asterisk (*) symbol indicates mandatory fields.

4. Click **Save**.

   A preview of the donut is generated on the right side of the screen.



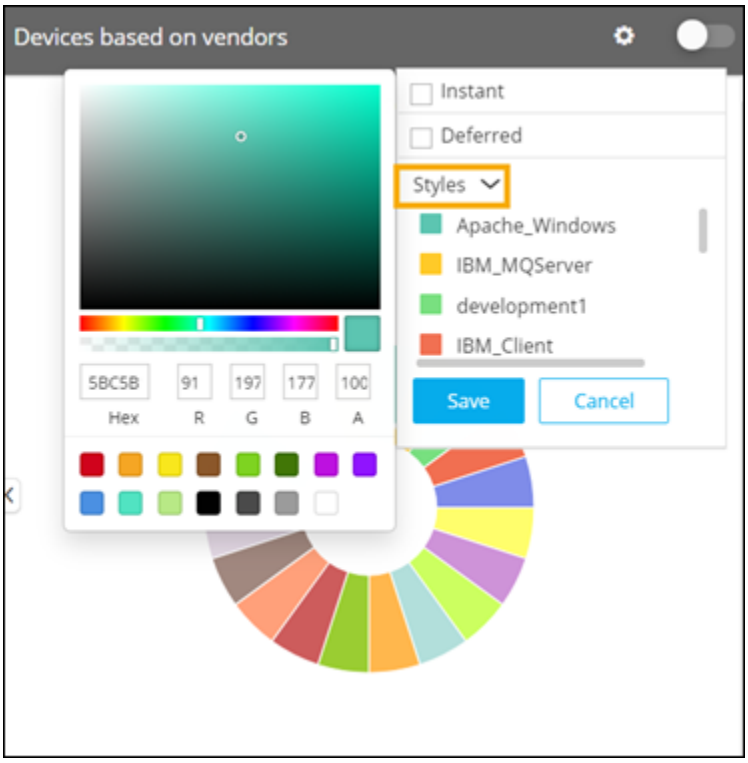
5. To select the data loading pattern, in the chart's preview window, click **(Settings)** icon.

   The following options are displayed:

   • **Instant**: This option allows you to enable live data loading and see changes in data immediately. This can be used in the case of small databases.

   • **Deferred**: This option allows you to enable lazy data loading and is useful in the case of larger databases. The default time interval for this is set at 30 minutes.

6. To change the style/font color of the donut, click **Styles**.



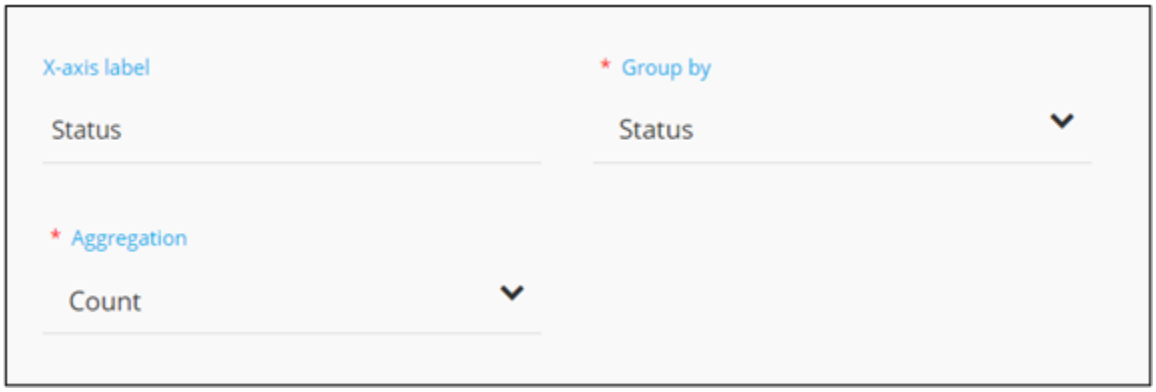
7. To enable the report, turn on the toggle. Only enabled reports are visible on the dashboard to which they are pinned.
8. Click **Next**.
   The CHART DRILLDOWN section is displayed.

How to Design a Custom Bar Chart

A bar chart allows you to compare data across different categories. It is especially useful for measuring changes in data over longer periods of time or measuring larger changes in data.

To design a custom bar Chart:

1. Build a report.
2. Under the **CHART CONFIGURATION** section, select the **BAR** chart.
3. Enter or select the required field information.

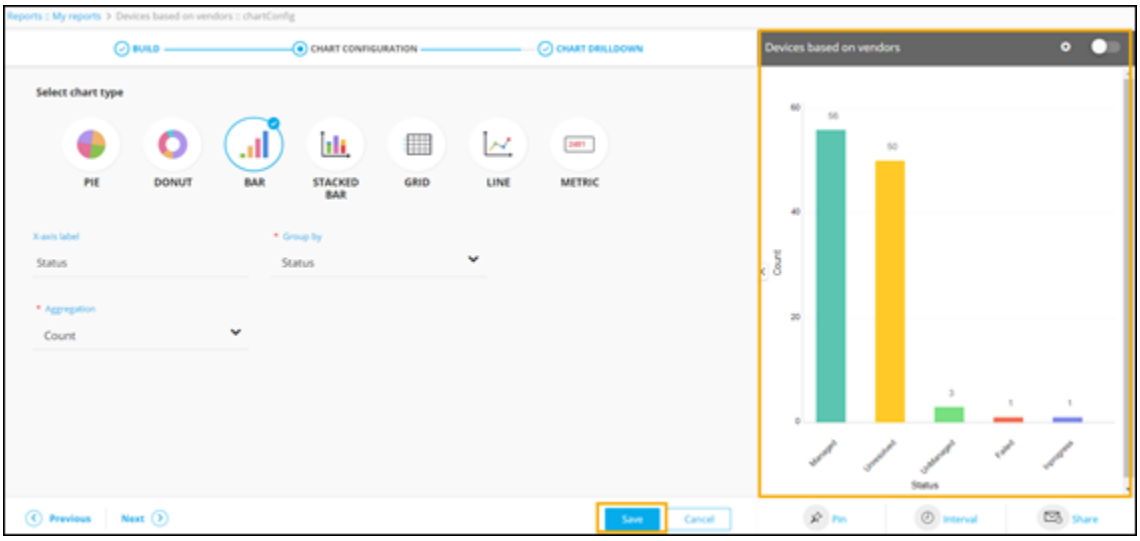


The following table describes the field information in this section:

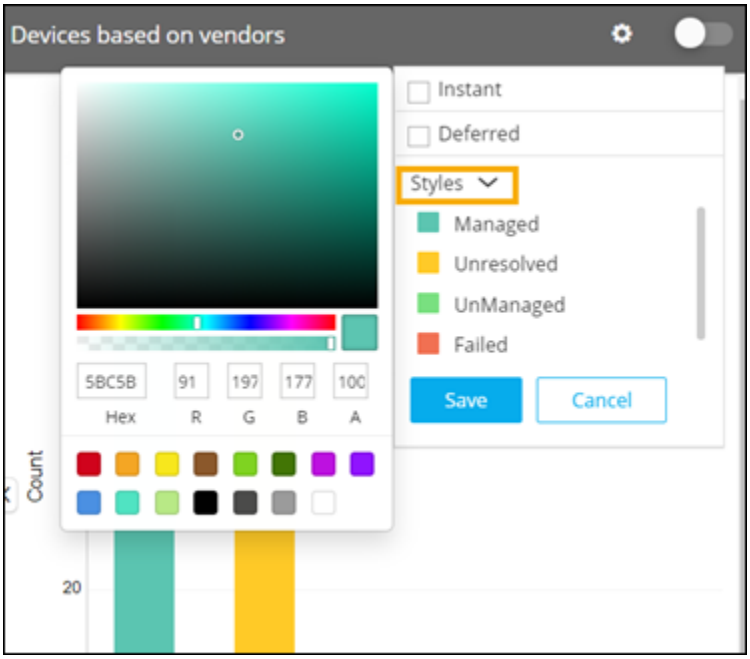
Field	Description
X-axis label	Enter the criteria for the X-axis label. For example: **Status**.
***Group by**	Select a value from the drop down menu on the basis of which data will be grouped. For example: **Status**. This will generate a report that shows the status of devices as managed, unmanaged and so on.
***Aggregation**	Select the calculation to be done on the report data for the dropdown. The following options are available: • **Average**: Calculates the average value of a given set of data. • **Sum**: Calculates the sum of all values in a given set of data. • **Count**: Calculates the total number of items in a given numeric field. • **Maximum**: Displays the maximum value in a given set of data. • **Minimum**: Displays the minimum value in a given set of data.
Note: The asterisk (*) symbol indicates mandatory fields.	

4. Click **Save**.

   A preview of the bar chart is generated on the right side of the screen.



5. To select the data loading pattern, in the chart's preview window, click **(Settings)** icon.
   The following options are displayed:
   - **Instant**: This option allows you to enable live data loading and see changes in data immediately. This can be used in the case of small databases.
   - **Deferred**: This option allows you to enable lazy data loading and is useful in the case of larger databases. The default time interval for this is set at 30 minutes.
6. To change the style/font color of the bar chart, in the chart's preview window, click **Styles**.



7. To enable the report, turn on the toggle. Only enabled reports are visible on the dashboard to which they are pinned.

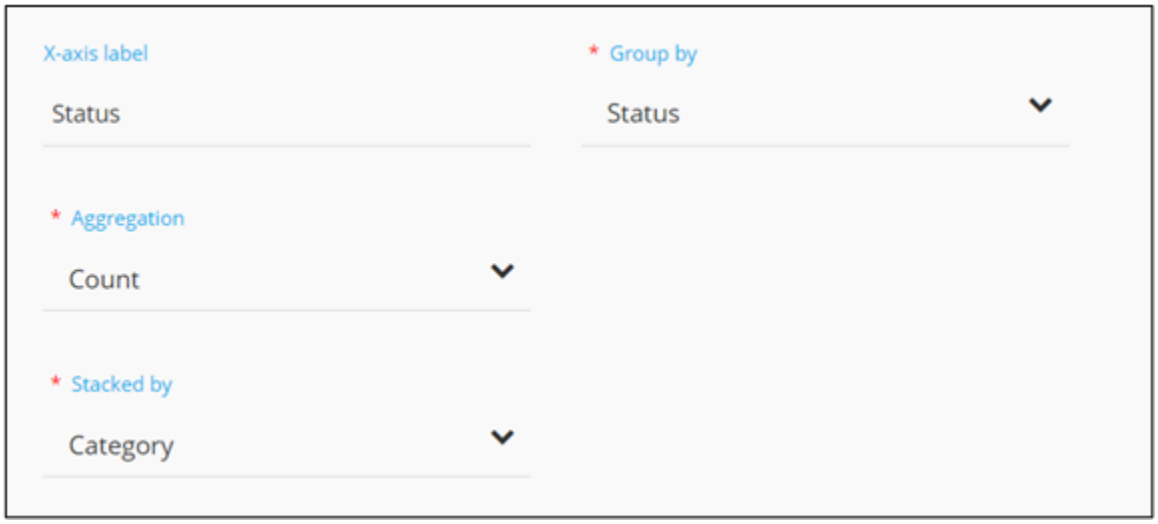
8. Click **Next**.
   The CHART DRILLDOWN section is displayed.

How to Design a Custom Stacked Bar Chart

A stacked bar chart is useful for comparing data across several categories as well as analysing the relation between sub-categories. In a stacked bar, each bar is divided into segments which represent different categories within that single bar category.

To design a custom stacked bar chart:

1. Build a report.
2. Under the **CHART CONFIGURATION** section, select the **STACKED BAR** chart.
3. Enter or select the required field information.

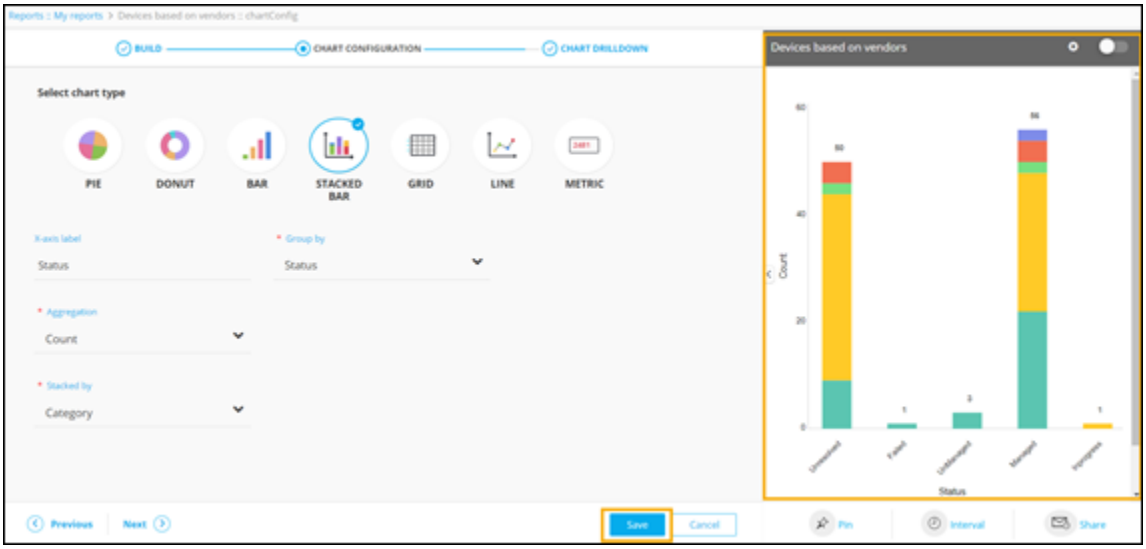


The following table describes the field information in this section:

Field	Description
X-axis label	Enter the criteria for the X-axis label. For example: **Status**.
***Group by**	Select a value from the drop down menu on the basis of which report data will be grouped. For example: **Status**.
***Aggregation**	Select the calculation to be done on the report data for the dropdown. The following options are available: • **Average**: Calculates the average value of a given set of data. • **Sum**: Calculates the sum of all values in a given set of data.

Field	Description
	• **Count**: Calculates the total number of items in a given numeric field. • **Maximum**: Displays the maximum value in a given set of data. • **Minimum**: Displays the minimum value in a given set of data.
***Stacked by**	Select the parameter from the drop down menu on the basis of which the data will be stacked in the chart. For example: **Category** of device.
Note: The asterisk (*) symbol indicates mandatory fields.	

4. Click **Save**.
   A preview of the stacked bar chart is generated on the right side of the screen.



5. To select the data loading pattern, in the chart's preview window, click **(Settings)** icon.
   The following options are displayed:
   - **Instant**: This option allows you to enable live data loading and see changes in data immediately. This can be used in the case of small databases.
   - **Deferred**: This option allows you to enable lazy data loading and is useful in the case of larger databases. The default time interval for this is set at 30 minutes.
6. To change the style/font color of the stacked bar chart, click **Styles**.

7. To enable the report, turn on the toggle. Only enabled reports are visible on the dashboard to which they are pinned.
8. Click **Next**.
   The CHART DRILLDOWN section is displayed.

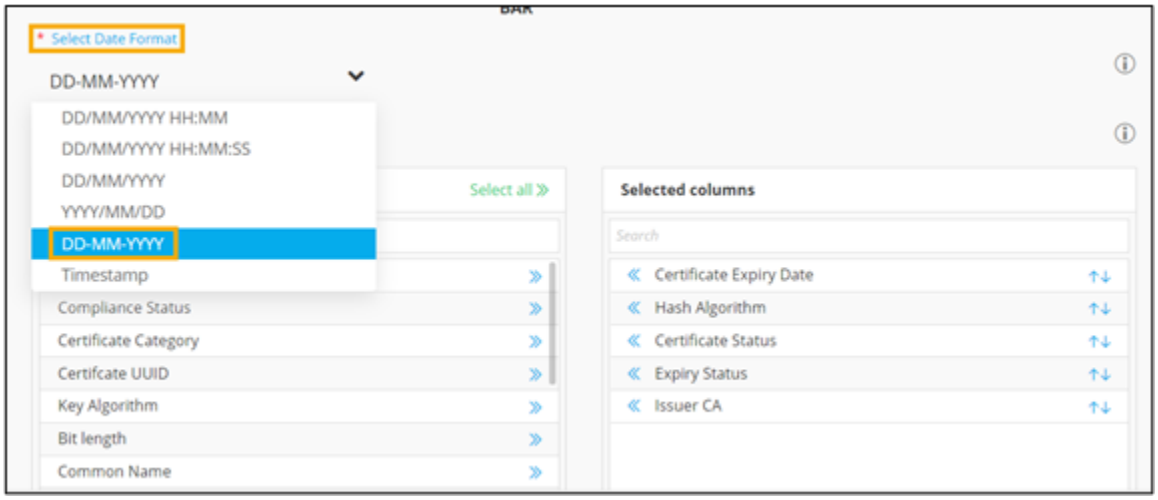
How to Design a Custom Grid Chart

A grid is a tabular representation of data with each row displaying specific information pertaining to selected fields in the columns.

- The grid chart supports server side search functionality.
- It also supports server side sorting, where you can sort the report data in ascending or descending order.
- Grid chart also has provision for downloading high volumes of data in Excel or CSV formats.
- Date formats are customizable for grid charts as per user needs. You can select the specific date format from the dropdown.

To design a custom grid chart:

1. Build a report.
2. Under the **CHART CONFIGURATION** section, select the **GRID** chart.
3. **Select Date Format** from the dropdown.

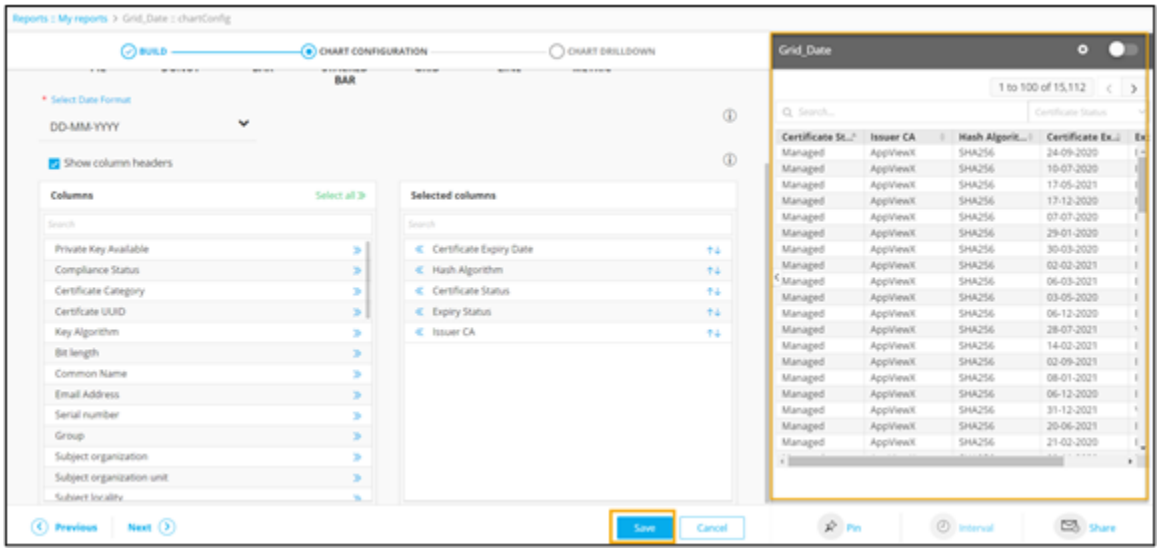


4. To configure the column headers to be displayed within the grid, click  .

> **Tip:** To arrange the order in which **Selected columns** are displayed in the grid, click  .

5. Click **Save**.

   A preview of the grid chart is generated on the right side of the screen.



6. To select the data loading pattern, click  **(Settings)** icon.

   The following options are displayed:

- **Instant**: This option allows you to enable live data loading and see changes in data immediately. This can be used in the case of small databases.
- **Deferred**: This option allows you to enable lazy data loading and is useful in the case of larger databases. The default time interval for this is set at 30 minutes.

7. To enable the report, turn on the toggle. Only enabled reports are visible on the dashboard to which they are pinned.

> **Note:** Color code mapping is not applicable to the grid chart.

8. Click **Next**.
   The CHART DRILLDOWN section is displayed.

How to Design a Custom Line Chart

Line charts are a simple and quick way of tracking changes over a period of time. They are a better choice for tracking changes over a short period of time. A line chart can also be used to compare changes for multiple groups over the same period of time.

To design a custom line chart:

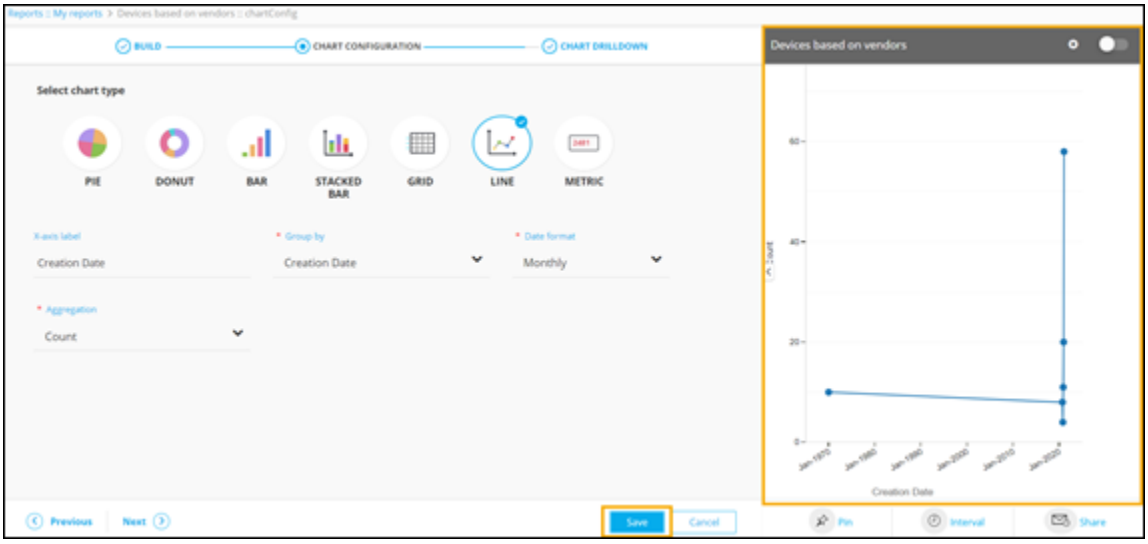
1. Build a report.
2. Under the **CHART CONFIGURATION** section, select the **LINE** chart.
3. Enter or select the required field information.

The following table describes the field information in this section:

Field	Description
X-axis label	Enter the criteria for the X-axis label. For example: **Creation Date**.
***Group by**	Select a value from the dropdown on the basis of which report data will be grouped. For example: **Creation Date**.

Field	Description
***Date format**	Select a valid date format from the dropdown menu. For example: **Monthly**.
***Aggregation**	Select the calculation to be done on the report data for the dropdown. The following options are available: • **Average**: Calculates the average value of a given set of data. • **Sum**: Calculates the sum of all values in a given set of data. • **Count**: Calculates the total number of items in a given numeric field. • **Maximum**: Displays the maximum value in a given set of data. • **Minimum**: Displays the minimum value in a given set of data.
Note: The asterisk (*) symbol indicates mandatory fields.	

4. Click **Save**.
   A preview of the line chart is generated on the right side of the screen.



5. To select the data loading pattern, in the chart's preview window, click **(Settings)** icon.
   The following options are displayed:
   • **Instant**: This option allows you to enable live data loading and see changes in data immediately. This can be used in the case of small databases.
   • **Deferred**: This option allows you to enable lazy data loading and is useful in the case of larger databases. The default time interval for this is set at 30 minutes.
6. To enable the report, turn on the toggle. Only enabled reports are visible on the dashboard to which they are pinned.

Note: Color code mapping is not applicable to the line chart.

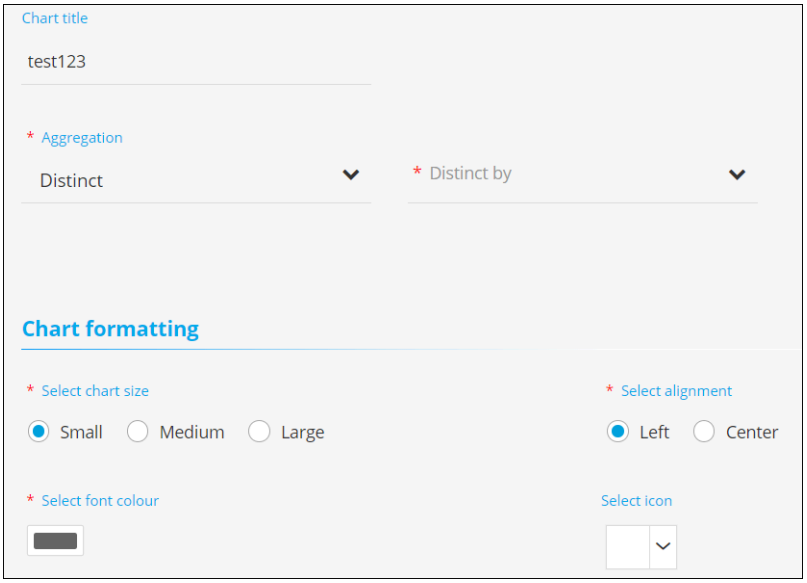
7. Click **Next**.
   The CHART DRILLDOWN section is displayed.

How to Design a Custom Metric Chart

A metric chart displays specific information about a process and its functioning. It allows you to highlight a metric on the dashboard, giving instant information about the data and helps in tracking progress.

To design a custom metric chart:

1. Build a report.
2. Under the **CHART CONFIGURATION** section, select the **METRIC** chart.
3. Enter or select the required field information.



The following table describes the field information in this section:

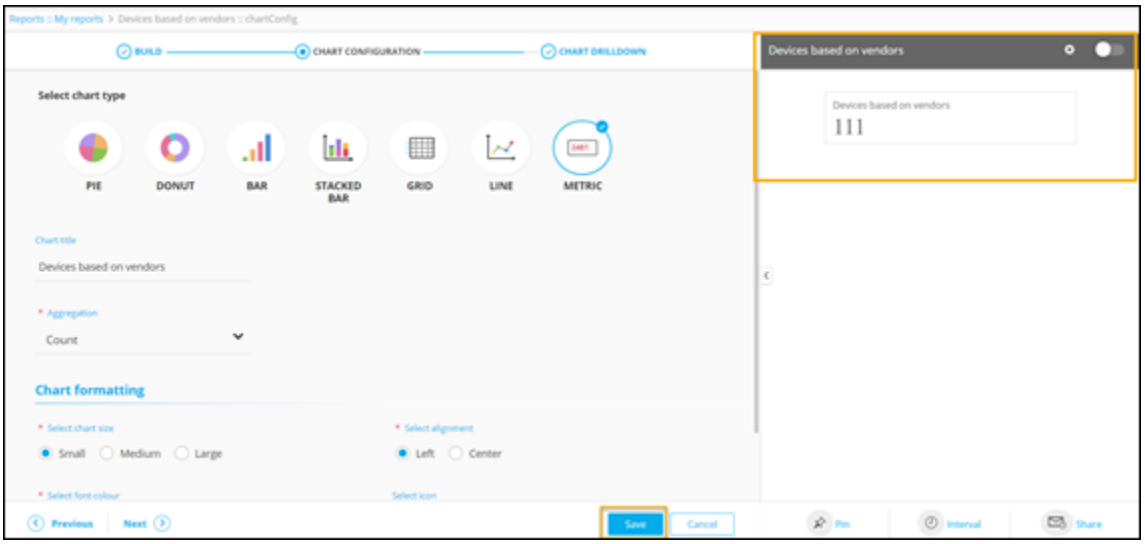
Field	Description
Chart Title	Enter the chart title. For example: **Devices based on vendors**.

Field	Description
***Aggregation**	Select the calculation to be done on the report data for the dropdown. The following options are available: • **Average**: Calculates the average value of a given set of data. • **Sum**: Calculates the sum of all values in a given set of data. • **Count**: Calculates the total number of items in a given numeric field. • **Maximum**: Displays the maximum value in a given set of data. • **Minimum**: Displays the minimum value in a given set of data. • **Distinct**: Displays the number of distinct or unique values as specified in the **Distinct by** field.
***Select chart size**	Select the metric size. For example, Small.
***Select alignment**	Select the placement of the metric on the screen. For example: **Left**.
***Select font color**	Select the color of the font on the metric.
Select icon	Select an icon for the metric chart from the dropdown menu.

Note: The asterisk (*) symbol indicates mandatory fields.

4. Click **Save**.

   A preview of the metric chart is generated on the right side of the screen.



5. To select the data loading pattern, in the chart's preview window, click **(Settings)** icon.

   The following options are displayed:

- **Instant**: This option allows you to enable live data loading and see changes in data immediately. This can be used in the case of small databases.
- **Deferred**: This option allows you to enable lazy data loading and is useful in the case of larger databases. The default time interval for this is set at 30 minutes.

6. To enable the report, turn on the toggle. Only enabled reports are visible on the dashboard to which they are pinned.

> **Note:** Color code mapping is not applicable to the metric chart.

7. Click **Next**.
   The CHART DRILLDOWN section is displayed.

Chart Drilldown

This section of the report builder allows you to make reporting more interactive and engaging by supplementing additional details within a chart. Adding a drilldown to your report helps in visualizing specific data pertaining to information displayed in the chart with a single click of the mouse. Drilldown also lightens the load on the server by presenting only a single layer of data at a time, which also significantly enhances the reporting performance.

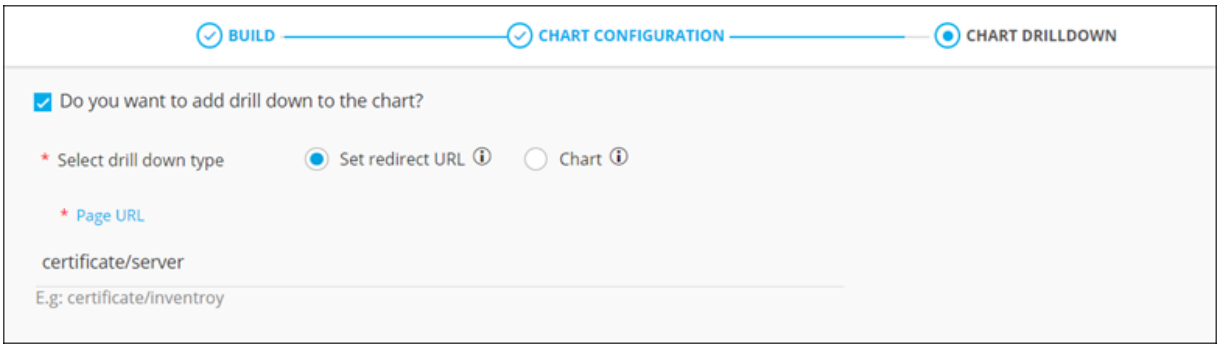
- How to Set a Redirect URL
- How to Add a Drilldown Chart

How to Set a Redirect URL

You can enter a URL to redirect to any webpage or another existing report (within AppViewX pages) directly from the chart .

To add a redirect URL to your report:

1. Build a report.
2. Design a custom chart.
3. Under the **CHART DRILLDOWN** section, enter or select the required field information.



The following table describes the field information required in this section:

Field	Description
Do you want to add a drill down to the chart?	To add a drilldown to the chart, select this checkbox.
***Select drill down type**	Select **Set redirect URL**.
***Page URL**	Enter a valid URL.

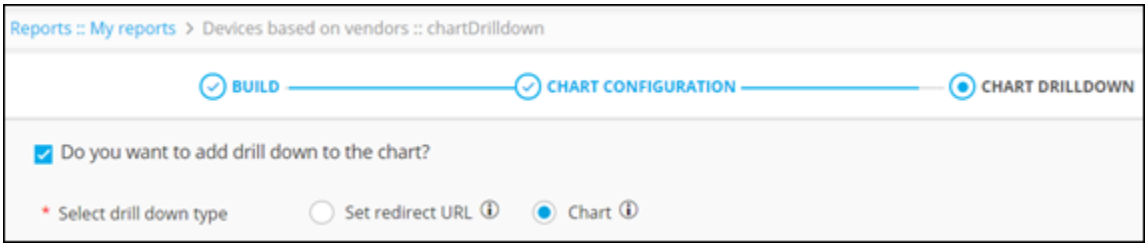
Note: The asterisk (*) symbol indicates mandatory fields.

4. Click **Save & Enable**.

How to Add a Drilldown Chart

You can add up to five levels of drilldown charts to a report.

1. Under the **CHART DRILLDOWN** section, enter or select the required field information.



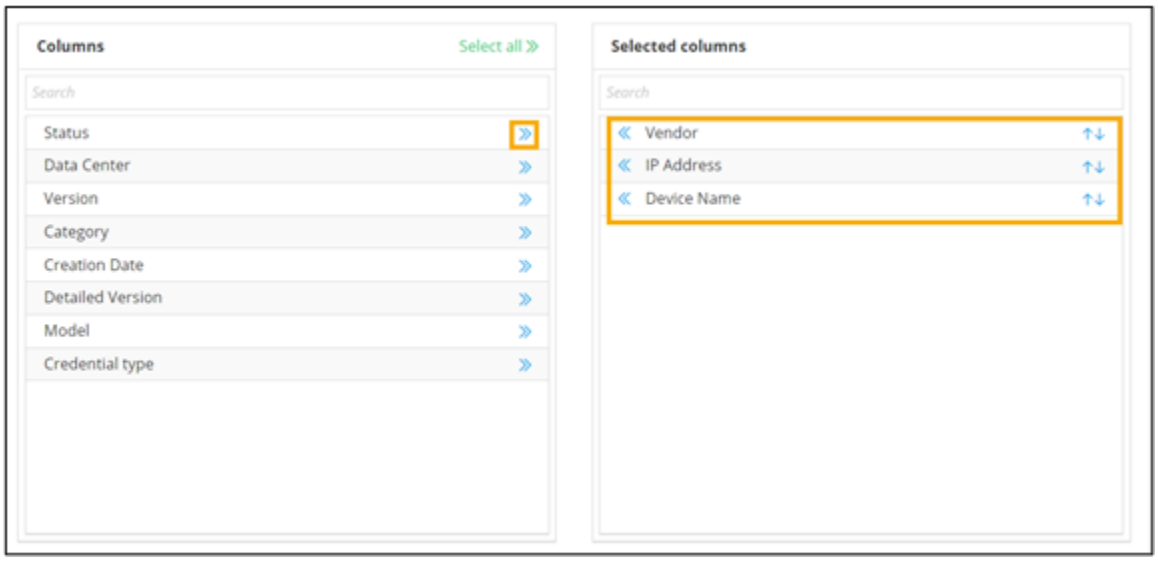
The following table describes the field information required in this section:

Field	Description
Do you want to add a drill down to the chart?	Check this box to add a drilldown to the chart.
***Select drill down type**	Select **Chart** as the drilldown type.

Note: The asterisk (*) symbol indicates mandatory fields.

2. Select the **GRID** chart. and enter a suitable **Chart title**.

3. To configure the column headers to be displayed within the grid, click .
   Selected columns are displayed on the right side.



Note: To remove a column, click .

4. To enable the chart, click **Save & Enable**.
5. To get more information on the devices in the drilldown, click on any of the bars on the bar chart.

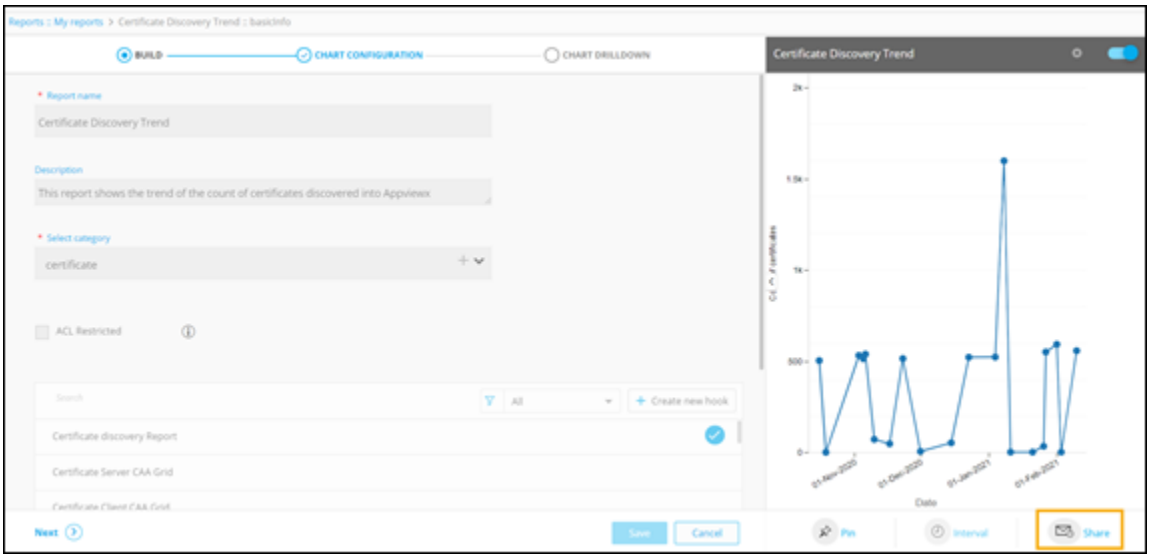
Sharing your Reports

Once a report is generated, it can be emailed either as inline content or as a PDF attachment. You can also schedule reports to be generated on a recurring basis.

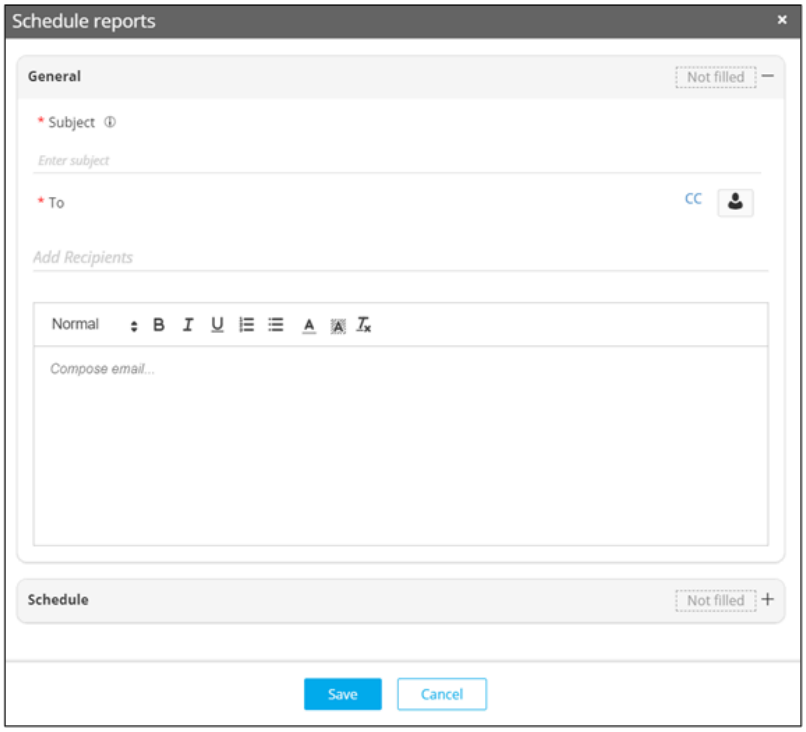
- How to Email reports as PDF
- How to Schedule reports

How to Email reports as PDF

1. Under the **BUILD** section, from the bottom right corner of the screen, click **Share**.



A pop-up window to **Schedule reports** is displayed.



2. In the **Schedule reports** window, under the **General** section, enter or select the required field information.

   The following table describes all the fields in the **General** section:

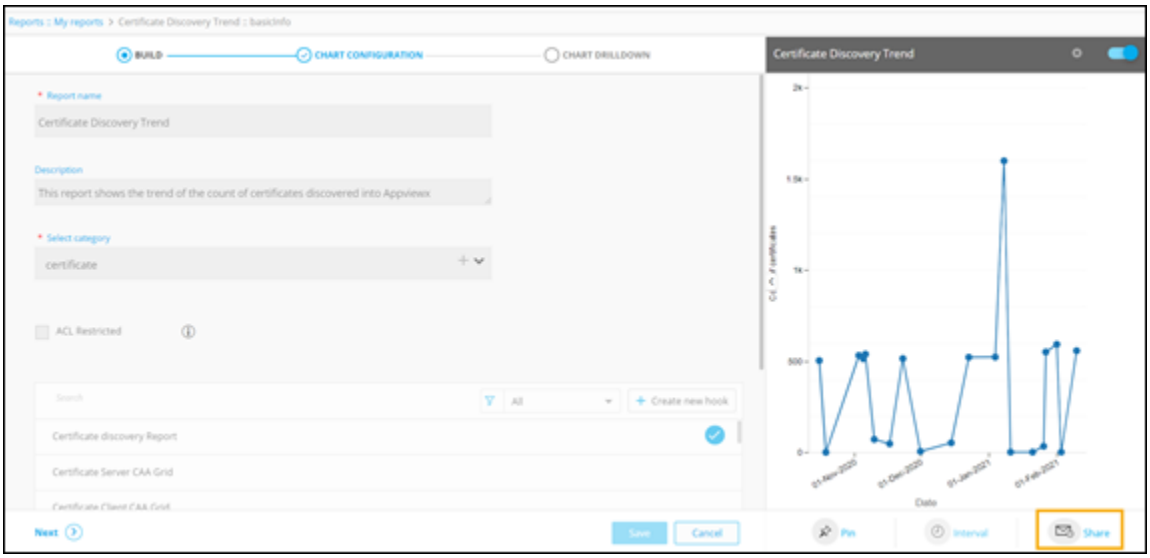
Field	Description
***Subject**	Enter a subject for the email which will also be populated under **Scheduled Jobs** on the **Reports :: Schedule** page.
***To**	Enter the names of the recipients of the email. Two options are available here: • Add single/multiple email addresses. • Add user groups(s).
Email body/text	Compose the email.

Note: The asterisk (*) symbol indicates mandatory fields.

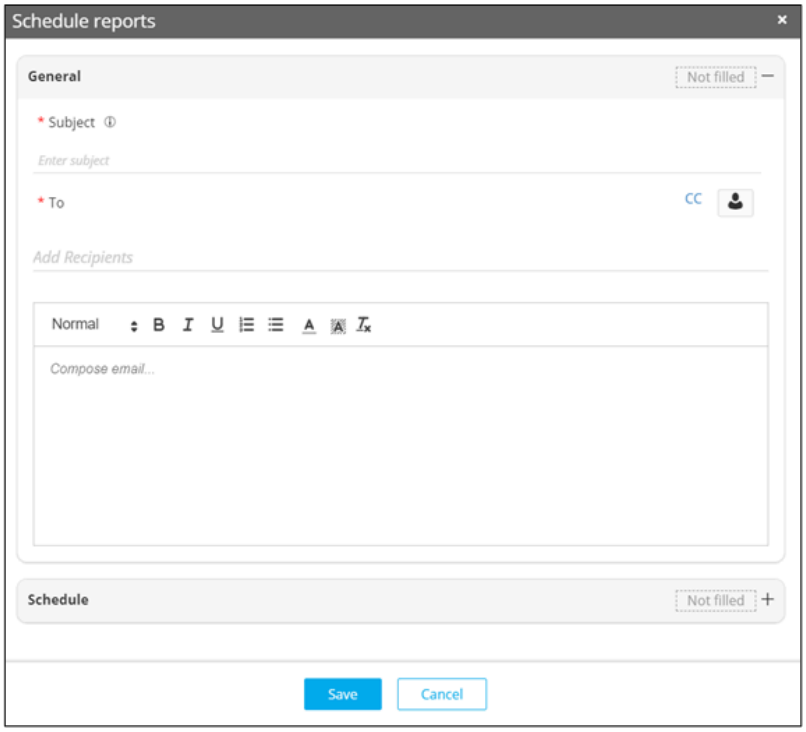
How to Schedule reports

Reports can be scheduled to be generated on a recurring basis.

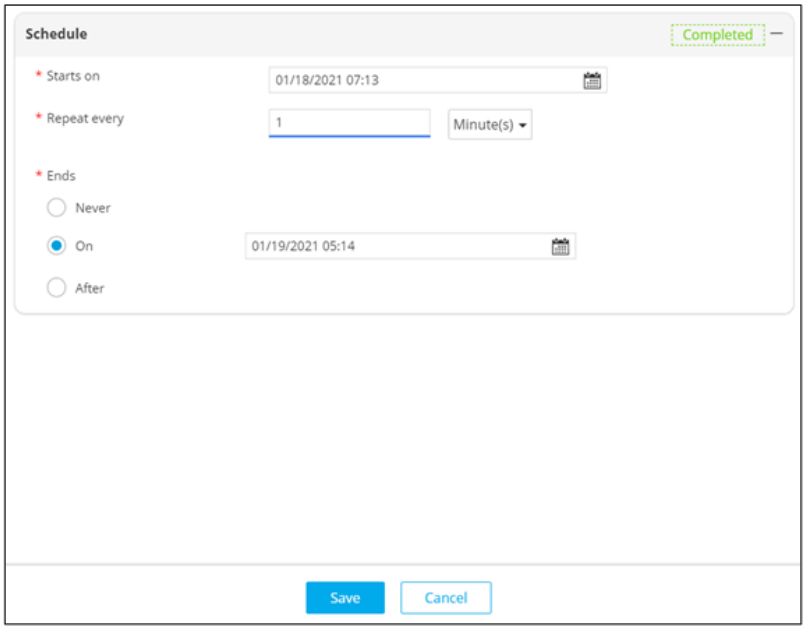
1. Under the **BUILD** section, from the bottom right corner of the screen, click **Share**.



A pop-up window to **Schedule reports** is displayed.



2. In the **Schedule reports** window, under the **Schedule** section, enter or select the required field information.



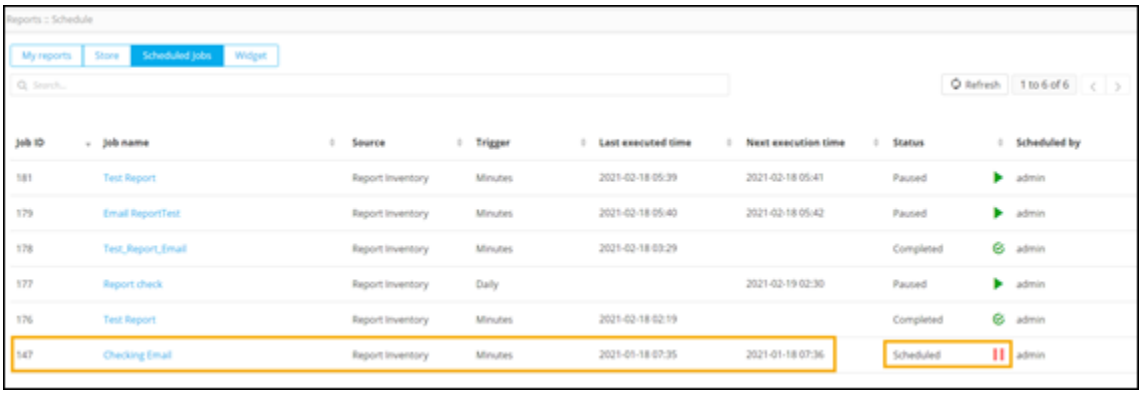
The following table describes the fields in the **Schedule** section:

Field	Description
***Starts on**	Select the date on which report is to be scheduled.
***Repeat every**	Select the numeric value and the frequency of recurrence as minutes, hours, days, weeks, months, or years.
***Ends**	Select when the report should stop recurring. The options available are: • **Never** • **On** a specific date. • **After** a set number of occurrences.

Note: The asterisk (*) symbol indicates mandatory fields.

3. Click **Save**.

   The scheduled report will be displayed on the **Reports :: Schedule** page.



4. To disable/pause the scheduled job, click **(Pause)** icon.
5. To resume the scheduled job, click **(Resume)** icon.

Hooks

A hook is a mechanism used to query and retrieve data from different sources such as database, device, or external vendors, and leverage them as part of the report building process.

The mode of query can be one of the following:

- Query Explorer (GUI based)
- Script (Python)
- REST API.

Using Preexisting Hooks to Build Reports

You can build customized reports by using preexisting hooks from the **Hooks Inventory**.

Note: For more information on the **Hooks Inventory**, refer to the Automation User Guide.

Example 1

The report builder can be used to build a report to get a list of devices based on vendors using a preexisting hook.

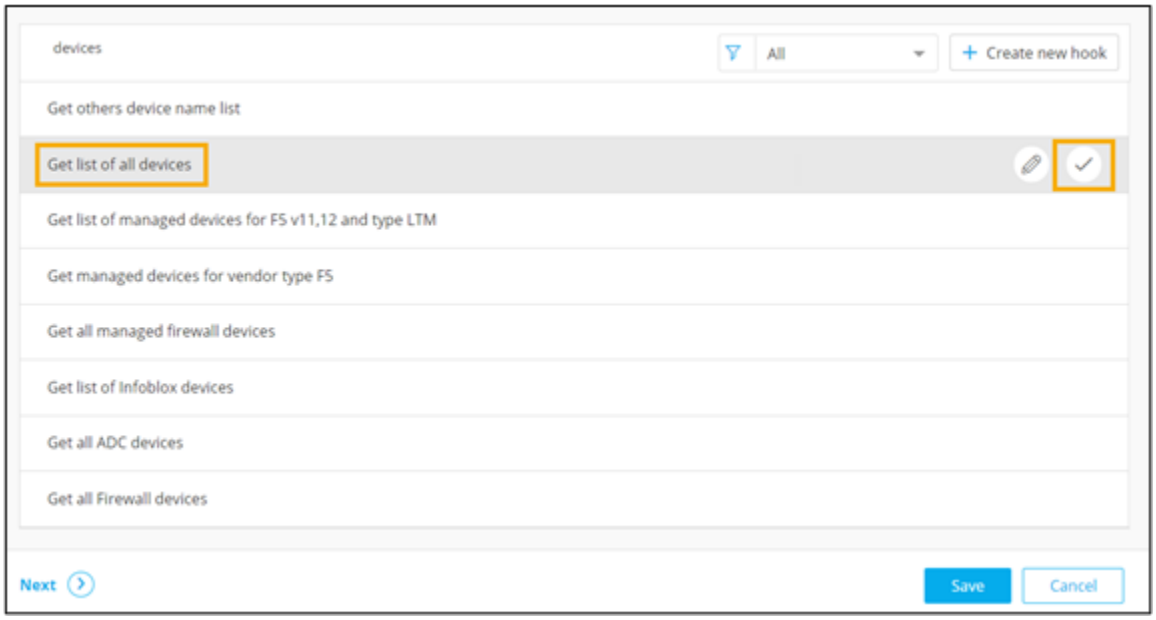
1. On the Reports :: My Reports page, click **Create new report**.
2. On the **Reports :: My reports > Create :: basicinfo** page that is displayed, under the **BUILD** section, enter or select the required field information.

The following table describes the various fields in this section:

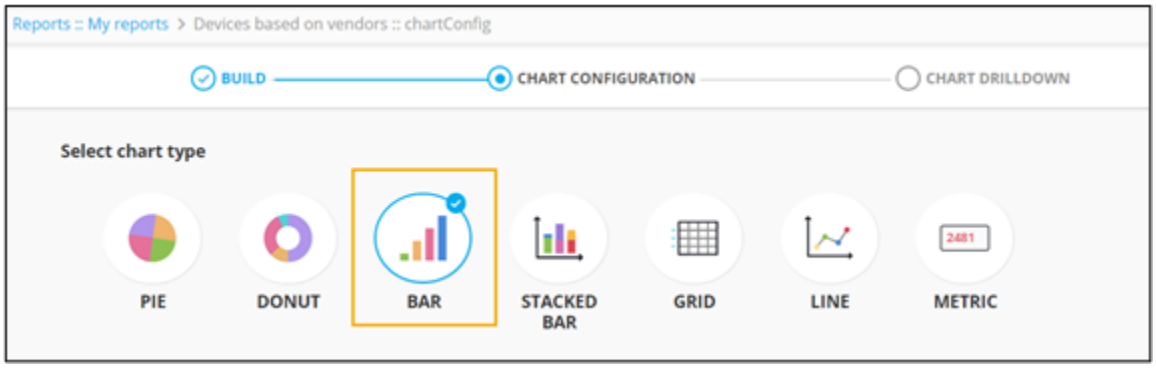
Field	Description
***Report name**	Enter a valid report name. For example: **Devices based on vendors**.
Description	Enter a valid description. For example: **Devices based on the vendor names**.
***Select category**	Select the category as **general** from the dropdown list.

Note: The asterisk (*) symbol indicates mandatory fields.

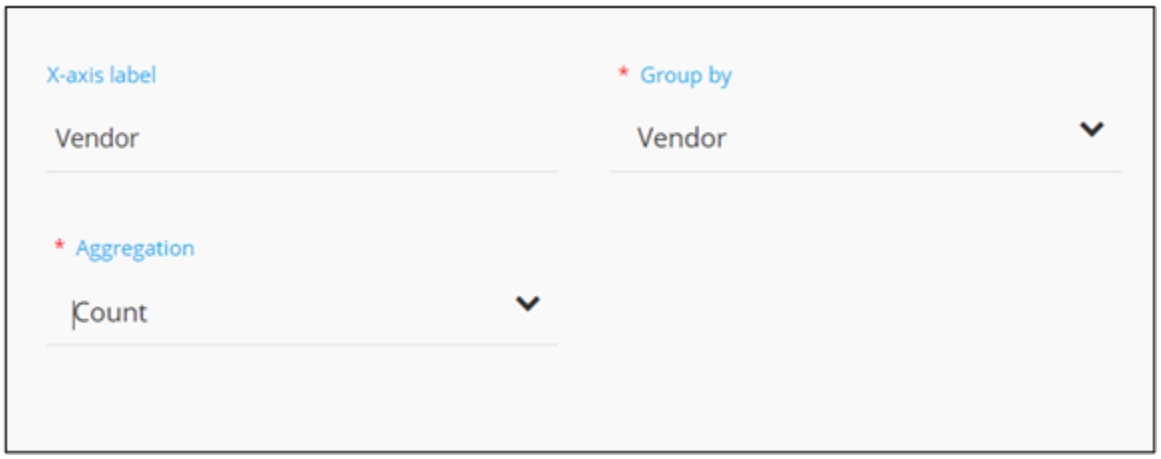
3. Search for the required hook from the pre-existing inventory.
4. To select the hook, click .



5. Click **Next**.
6. Under the **CHART CONFIGURATION** section, that is displayed, select the **BAR** chart.



7. Enter or select the required field information.

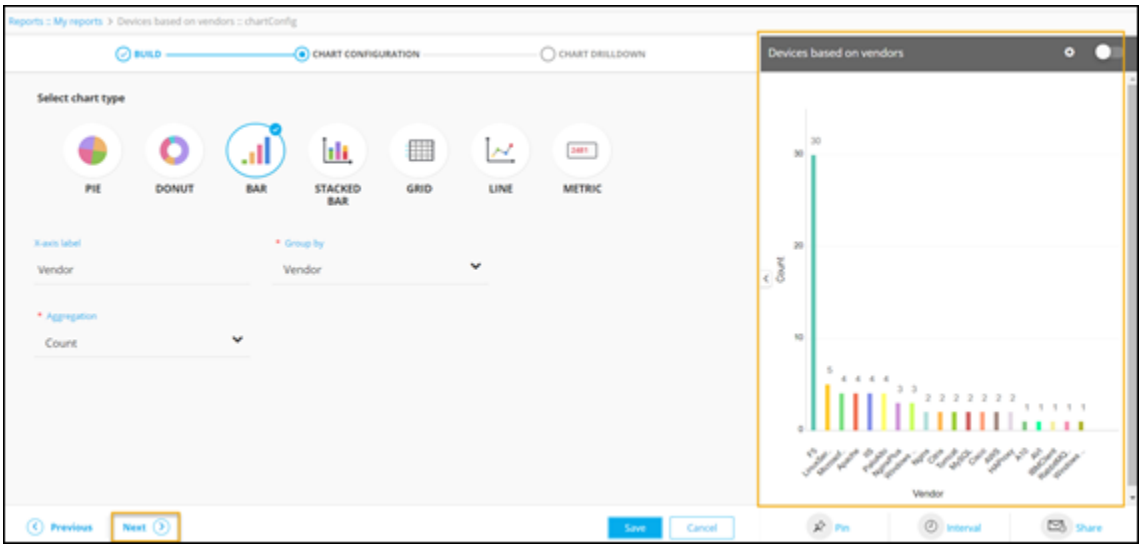


The following table describes the various fields in this section:

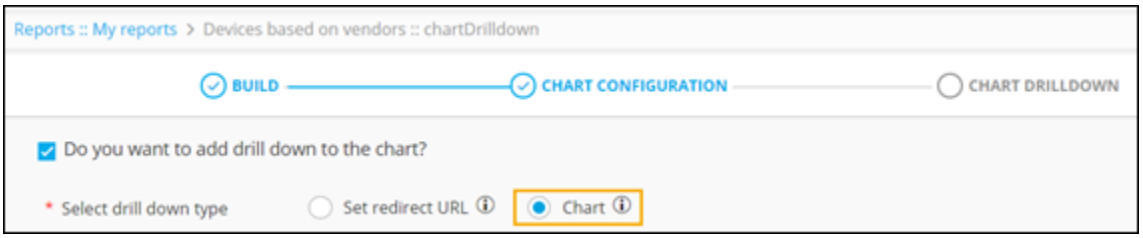
Field	Description
X-axis label	Enter criteria for the X-axis label. For example: **Vendor**.
***Group by**	Select a value from the drop down menu on the basis of which report data will be grouped. For example: **Vendor**.
***Aggregation**	Select the calculation to be done on the report data for the dropdown. For example, count to get the number of devices by name. The following options are available: • **Average**: Calculates the average value of a given set of data. • **Sum**: Calculates the sum of all values in a given set of data. • **Count**: Calculates the total number of items in a given numeric field. • **Maximum**: Displays the maximum value in a given set of data. • **Minimum**: Displays the minimum value in a given set of data.
 **Note:** The asterisk (*) symbol indicates mandatory fields.	

8. To save chart configuration, click **Next**.

   A preview of the bar chart is displayed on the right side of the screen.

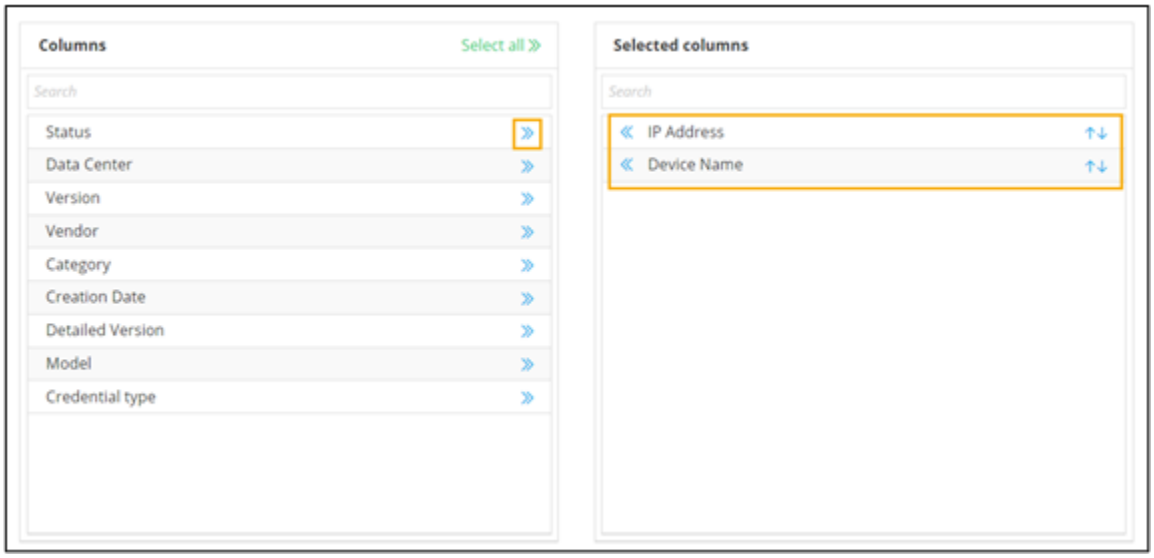


9. To add a drill down to the chart, under the **CHART DRILLDOWN** section that is displayed, select the **Do you want to add drill down to the chart?** check box.
10. Select the type of drill down as **Chart**.

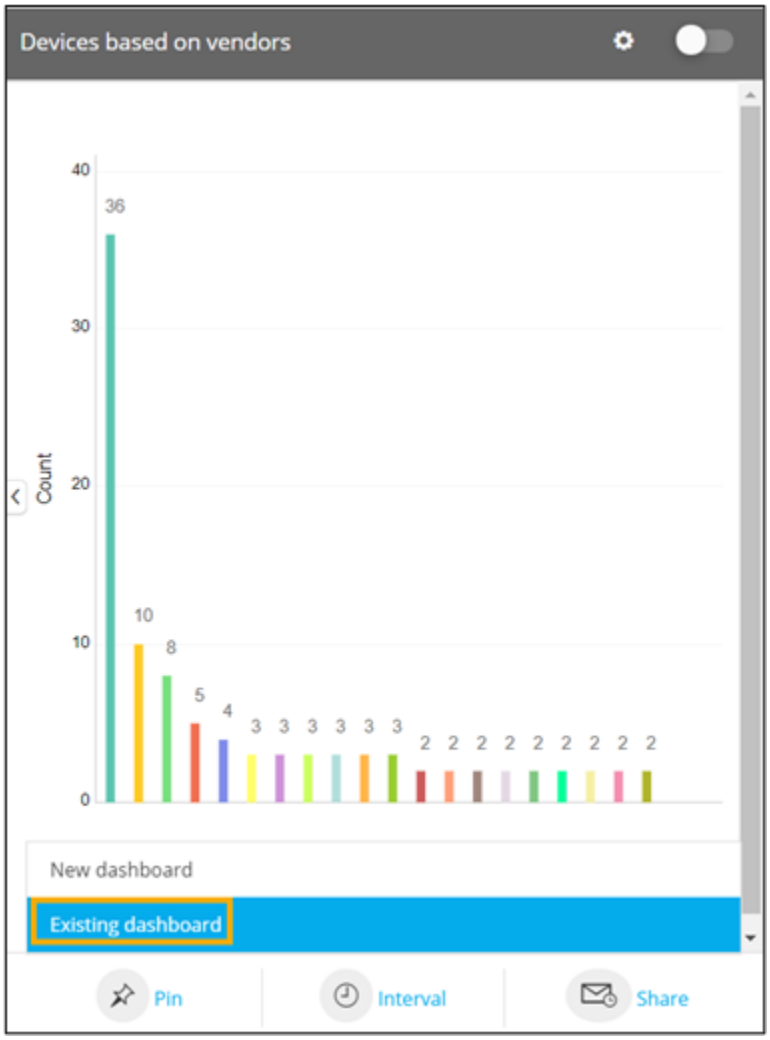


11. Select chart type as **GRID** and enter the **Chart title**.

12. To configure the column headers to be displayed within the grid, click  .
Selected columns are displayed on the right side.

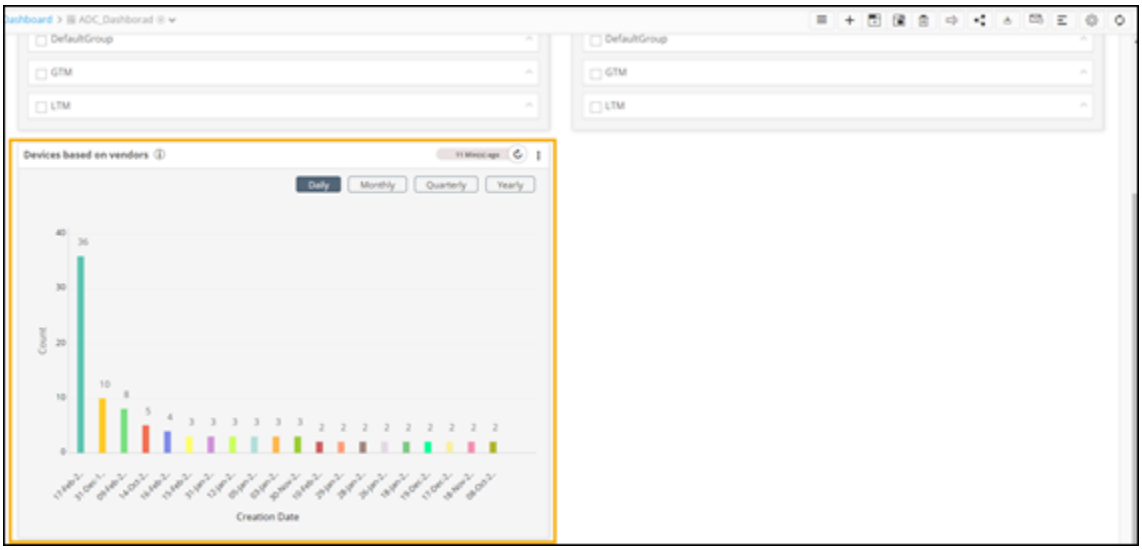


13. To pin the report to a dashboard, under the chart preview, click **Pin**.
14. To pin the report to a dashboard already available in the Dashboard inventory, select **Existing dashboard** from the options.

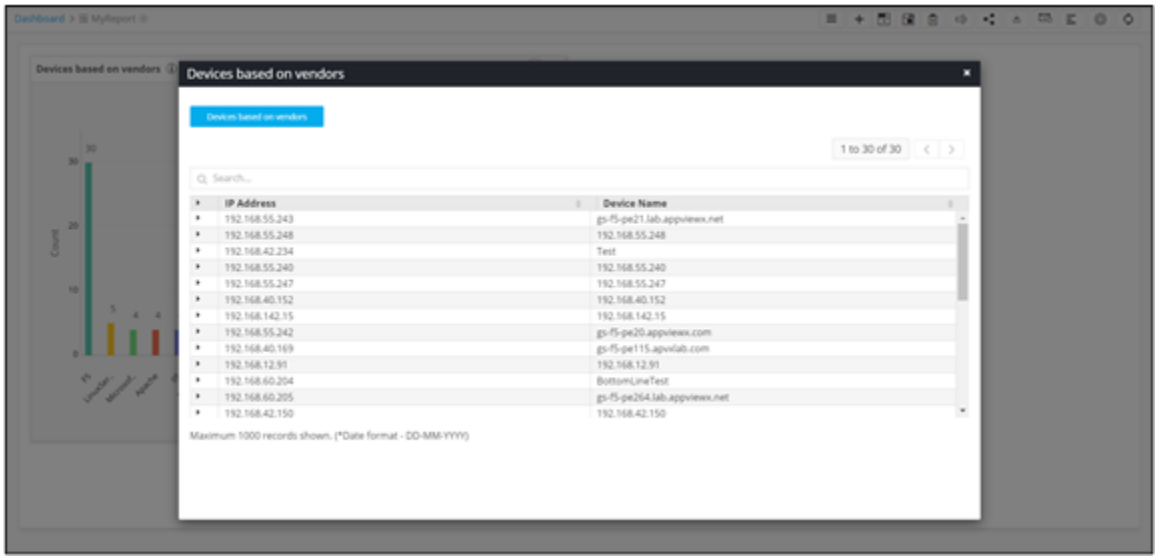


15. Select a dashboard from the list and click **Save**.
16. To enable the report, click **Save & Enable**.
17. To view this report on the dashboard, select this dashboard on the Dashboard inventory page.

    The **Devices based on vendors** report can be seen on the selected dashboard.



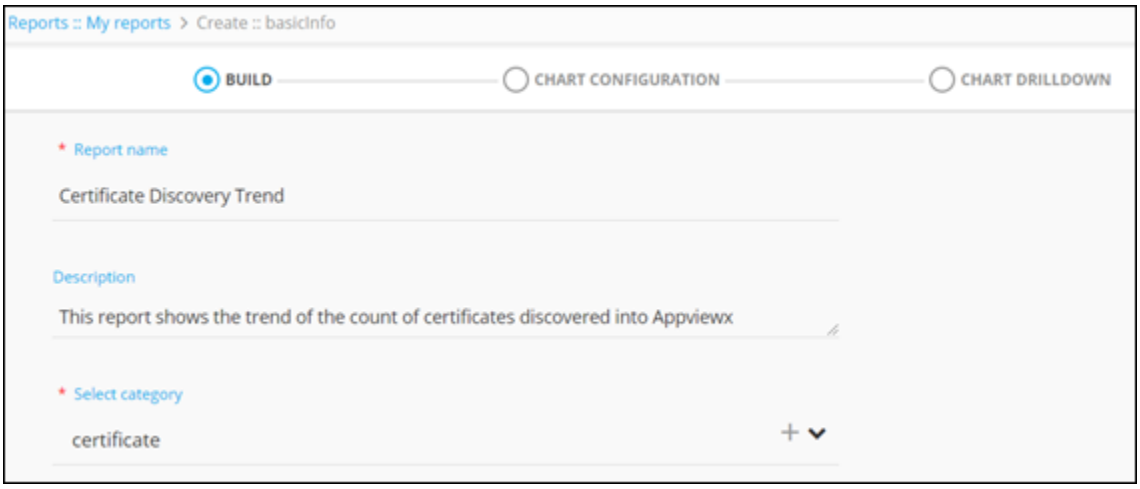
18. To display specific data on each of the vendors, click on any of the bars for the chart drilldown.



Example 2

To create a report for getting the **Certificate Discovery Trend** for all certificate types using a preexisting hook:

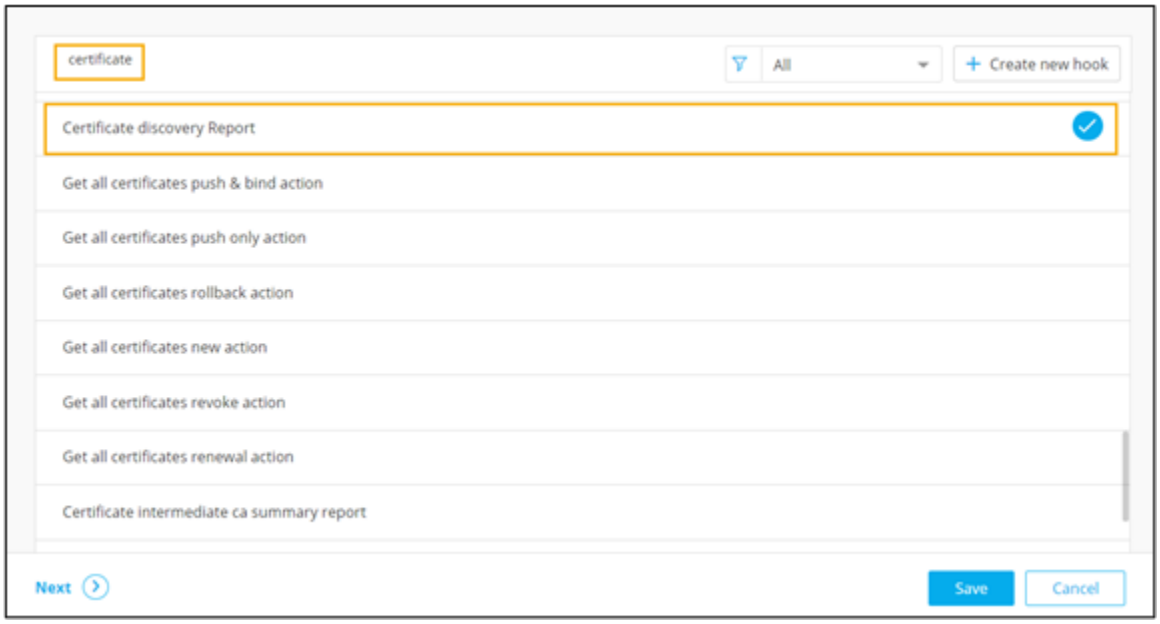
1. On the Reports :: My Reports page, click **Create new report**.
2. On the **Reports :: My reports > Create :: basicinfo** page that is displayed, under the **BUILD** section, enter or select the required field information.



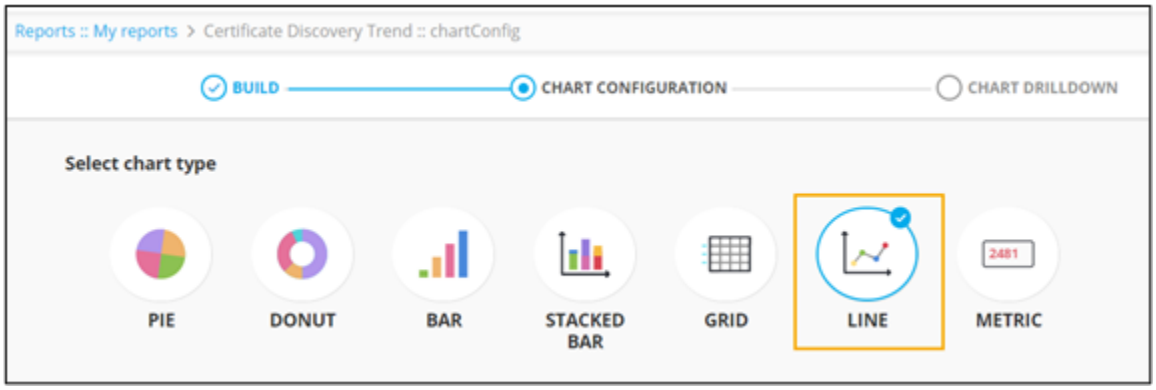
The following table describes the various fields in this section:

Field	Description
***Report name**	Enter a valid report name. For example: **Certificate Discovery Trend**.
Description	Enter a valid description. For example: **This report shows the trend of the count of certificates discovered into Appviewx.**
***Select category**	Select the category as **certificate** from the dropdown list.
Note: The asterisk (*) symbol indicates mandatory fields.	

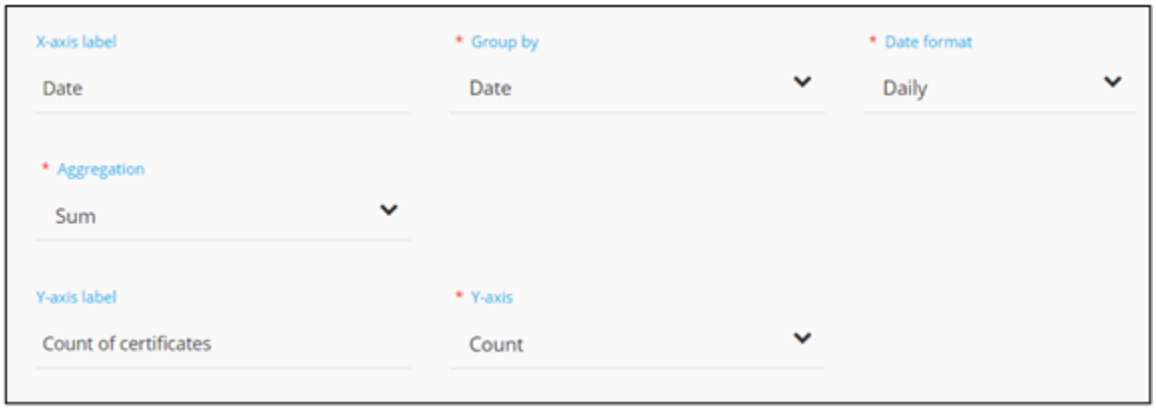
3. Search for the required hook from the pre-existing inventory.
4. To select the hook, click .



5. Click **Next**.
6. Under the **CHART CONFIGURATION** section that is displayed, select the **LINE** chart.



7. Enter or select the required field information.



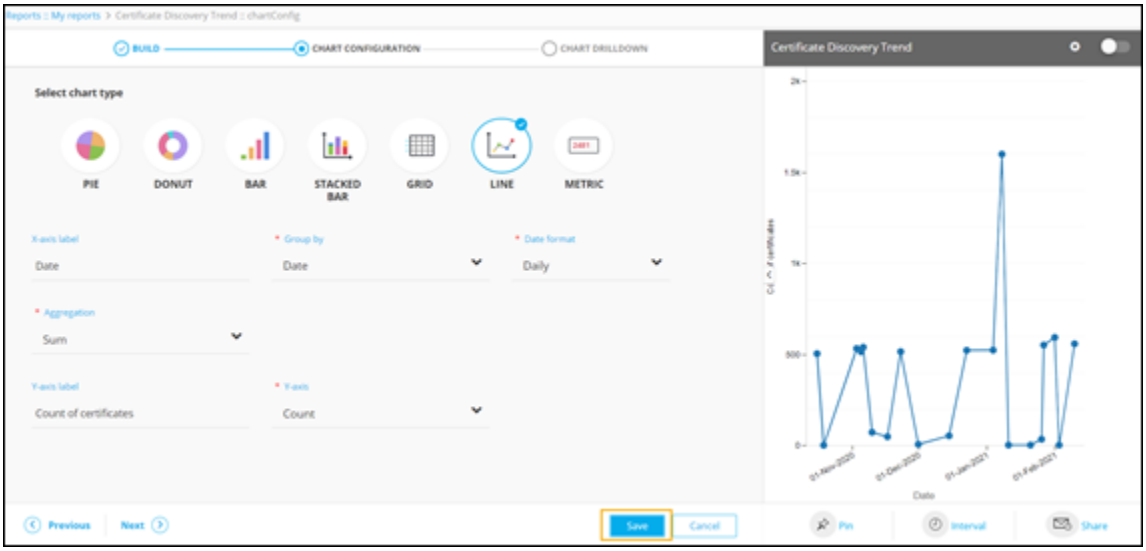
The following table describes the various fields in this section:

Field	Description
X-axis label	Enter the criteria for the X-axis label. For example: **Date**.
***Group by**	Enter the value on which data will be grouped. For example: **Date**.
***Date format**	Select a valid date format from the dropdown. For example: **Daily**.
***Aggregation**	Select the calculation to be done on the report data for the dropdown. For example, count to get the number of devices by name. The following options are available: • **Average**: Calculates the average value of a given set of data. • **Sum**: Calculates the sum of all values in a given set of data. • **Count**: Calculates the total number of items in a given numeric field. • **Maximum**: Displays the maximum value in a given set of data. • **Minimum**: Displays the minimum value in a given set of data.
Y-axis label	Enter the criteria for the Y-axis label. For example: **Count of certificates**.
***Y-axis**	Select a value from the dropdown. For example: **Count**.

Note: The asterisk (*) symbol indicates mandatory fields.

8. To save chart configuration details, click **Save**.

A preview of the line chart is displayed on the right side of the screen.



Using Query Explorer to build Reports

AppViewX's Report builder has an enhanced, intuitive **Query Explorer**. The GUI-based query explorer maps all major database collections in AppViewX and helps you build your own customized reports. Over 40 out of the box (OOB) queries are pre-shipped to the end-user. It also comes with advanced conditional operators to build complex queries.

Each query filter has a set of predefined fields associated with it. Query actions will differ according to the data in the query fields. The query builder also comes equipped with an auto-suggestion feature that aids you in selecting appropriate values from the suggested entries.

Query explorer also exhibits improved performance with query optimization by supporting four million to 50 million records. Its performance optimized search inventory enables higher volumes of data to be balanced and reduces load time.

Conditional Operators

Query Explorer has ten conditional operators that allow users to build complex queries. All of these operators support dynamic values. The dynamic values can be passed at runtime by using payload to perform queries.

The conditional operators are categorized based on field types: String, Integer, Date, and Boolean Variable.

Field Type: String

When you choose the field type as **String**, the values for the conditional operators are auto-populated from the database. The following conditional operators are available when you choose the field type as **String**:

- **Is** - This operator is used if the query is for a particular value.

  For example, Status is Managed.

The report will display data specific to this query and show the list of devices only with **Managed** status.

- **Is not** - This operator generates results where the condition is not matched.

  For example, Vendor is not Citrix.

  The report will display data that matches all criteria except the one that is selected and show the list of devices of all vendors except Citrix.

- **Is one of** - This operator allows multiple values to be selected and matches all conditions.For example, Category is one of Server, Firewall, WAF.

  The report will display data where all the three conditions are matched and show a list of devices that belong to the three selected categories.

- **Is not one of** - This operator allows multiple values to be selected and gives results where the conditions are not matched.

  For example, Category is not one of ADC, Firewall.

  The report will display data that matches all criteria except the ones that are selected and show a list of all devices except ADC and Firewall.

- **Exists** - A boolean operator is provided for narrowing down the search parameters so that the result is either True or False.

The report will display data after confirming if the selected field is available in the database (True) or not (False).

- **Regex** - Regular expression (Regex) is a sequence of characters defining a search pattern specifying a set of strings for a particular purpose.

  For example, Device name regex .*

The period (.) means match any character and the asterisk (*) means any number of times. So .* means match anything and the report will display all the device names.

- **Starts with** - This operator allows users to enter the first three letters/numbers of the search criteria.

The report will display results matching hash algorithms that start with ‘SHA’.

- **Ends with** - This operator allows users to enter the last three letters/numbers of the search criteria.

The report will display results matching hash algorithms that end with ‘256’.

- **Contains** - This operator allows users to enter some values for the search criteria and generates results that contain those values.

The report will display results with hash algorithms that contain the value ‘256’.

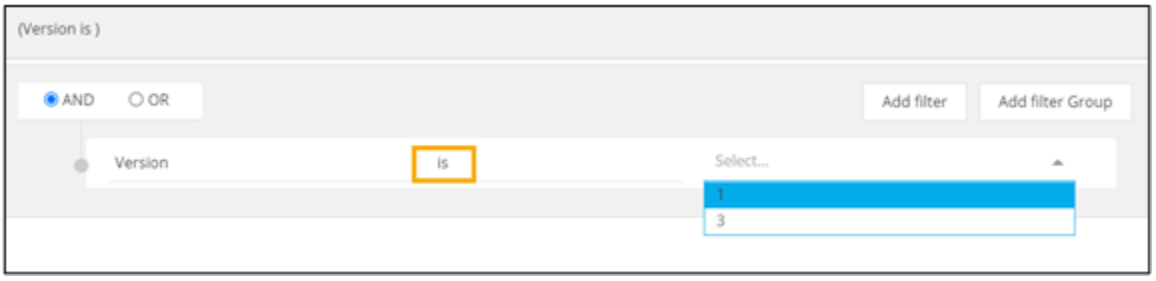
- **Does not contain** - This operator allows users to enter some values for the search criteria and generates results that do not contain those values.

The report will display results with hash algorithms that do not contain the value ‘256’.

Field Type: Integer

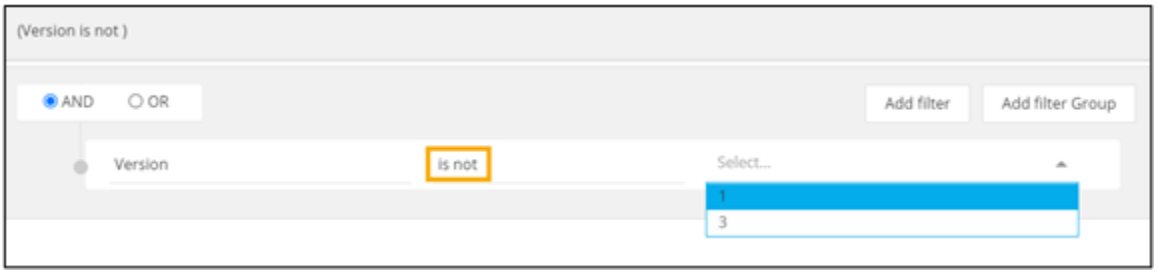
When you choose the field type as Integer, the values for the conditional operator are auto-populated from the database. The following conditional operators are available when you choose the field type as Integer:

- **Is**: This operator is used if the query is for a particular value. For example, version is 1.



The report generated will display data specific to this query and show the certificates with Version equal to 1.

- **Is not**: This operator generates results if the condition is not matched. For example, version is not 1.



The report generated will display data that matches all criteria except the one that is selected and show certificates with Version not equal to 1.

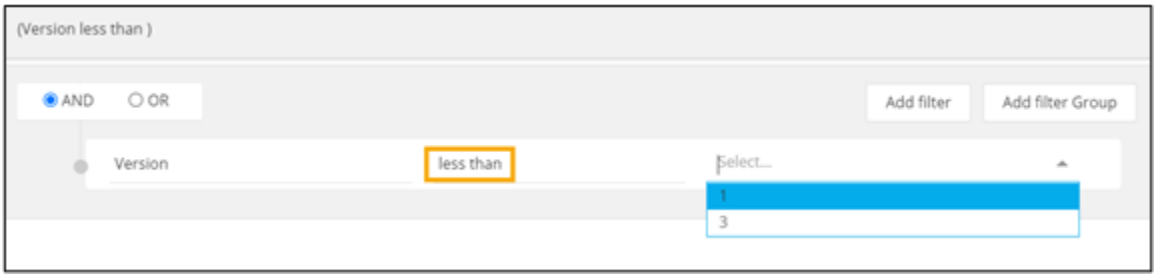
- **Exists**: A boolean operator is provided for narrowing down the search parameters so that the result is either True or False.

The report will display data after confirming if the selected field is available in the database or not. If the field is available, the result is True. If the field is not available, the result is False.

- **Greater than**: This operator is used to display records that match values greater than the selected value. For example, Version greater than 1.

The report generated will display certificates with version greater than 1.

- **Less than**: This operator is used to display records that match values less than the selected value. For example, Version less than 1.



The report generated will display certificates with version less than 1.

- **Greater than or is**: This operator is used to display records that match values greater than or equal to the selected value. For example, Version greater than or is 1.

The report generated will display certificates with version greater than or equal to 1.

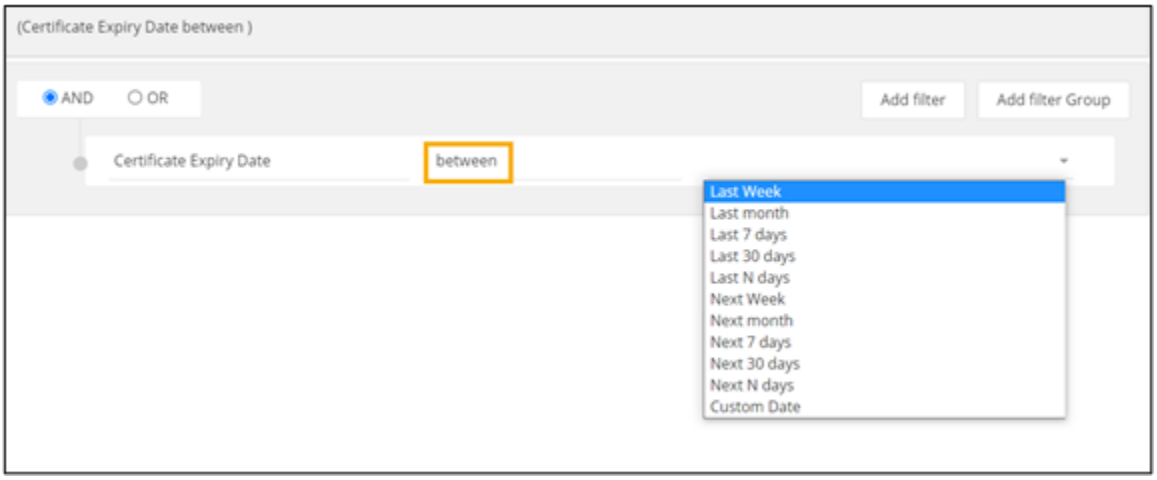
- **Less than or is**: This operator is used to display records that match values less than or equal to the selected value. For example, Version less than or is 1.

The report generated will display certificates with version less than or equal to 1.

Field Type: Date

When you choose the field type as Date, the values for the conditional operators are predefined and need to be selected from the dropdown list. The following conditional operators are available when you choose the field type as Date:

- **Between** - This operator allows users to select the duration for which reports will be generated.



The following table describes the date values supported by the **between** operator:

Date Type	Description	Example
Last Week	Returns records within the previous selected time period, starting with the beginning of that time frame.	For example, a filter run on July 27, 2021 will return any records with a date range of July 18 to July 24, 2021.
Last Month		For example, a filter run on July 27, 2021 will return any records with a date range of 1 June to 30 June 2021.
Last 7 days		For example, a filter run on July 27, 2021 will return any records with a date range of July 21 to July 27, 2021.
Last 30 days		For example, a filter run on July 27, 2021 will return any records with a date range of 27 June to 26 July, 2021.
Last N days		For example, a filter run on July 27, 2021 will return any records with a date range of Nth day to July 27, 2021.
Next Week	Returns records within the next selected time period, including records with values up to the end of that time frame.	For example, a filter run on July 27, 2021 will return any records with a date range of August 1 to August 7, 2021.

Date Type	Description	Example
Next Month		For example, a filter run on July 27, 2021 will return any records with a date range of August 1 to August 31, 2021.
Next 7 days		For example, a filter run on July 27, 2021 will return any records with a date range of July 27 to August 2, 2021.
Next 30 days		For example, on July 27, 2021 will return any records with a date range of July 27 to August 30, 2021.
Next N days		For example, a filter run on July 27, 2021 will return any records with a date range of July 27, 2021 to the Nth day.
Custom Date	Returns records within the defined custom date.	

- **On** - This operator allows users to select a specific day for which the records will be generated.

The following table describes the date values supported by the **On** operator:

Date Type	Description	Example
Today	Returns records for the selected time period, including records with values up to the end of that time frame.	For example, a **Certificate Expiry Date** filter run on July 27, 2021 will return records for certificates expiring on July 27, 2021.

Date Type	Description	Example
Yesterday		For example, a **Certificate Expiry Date** filter run on July 27, 2021 will return records for certificates expiring on July 26, 2021.
Custom Date	Returns records within the defined custom date.	For example, a **Certificate Expiry Date** filter run on a custom date, say August 1, will return records for certificates expiring on August 1, 2021.

- **Not on** - This operator allows users to select the time period for which the records should not be generated.

The following table describes the date values supported by the **not on** operator:

Date Type	Description	Example
Today	Returns records for the time period other than the selected time period, including records with values up to the end of that time frame.	For example, a **Certificate Expiry Date** filter run on July 27, 2021 will return records for certificates not expiring on July 27, 2021.
Yesterday		For example, a **Certificate Expiry Date** filter run on July 27, 2021 will return records for certificates not expiring on July 26, 2021.
Custom Date	Returns records for the time period other than the defined custom date.	For example, a **Certificate Expiry Date** filter run on a custom date, say August 1, will return records for certificates not expiring on August 1, 2021.

- **After** - This operator allows users to generate records of dates after the selected time period.

The following table describes the date values supported by the **after** operator:

Date Type	Description	Example
Today	Returns records for the selected time period, including records with values up to the end of that time frame.	For example, a **Certificate Expiry Date** filter run on July 27, 2021 will return records for certificates expiring after July 27, 2021.
Yesterday		For example, a **Certificate Expiry Date** filter run on July 27, 2021 will return records for certificates expiring after July 26, 2021.
Custom Date	Returns records within the defined custom date.	For example, a **Certificate Expiry Date** filter run on a custom date, say August 1, will return records for certificates expiring after August 1, 2021.

- **Before** - This operator allows users to generate records before the selected time period.

The following table describes the date values supported by the **before** operator:

Date Type	Description	Example
Today	Returns records for the selected time period, including records with values up to the end of that time frame.	For example, a **Certificate Expiry Date** filter run on July 27, 2021 will return records for certificates expiring before July 27, 2021.

Date Type	Description	Example
Yesterday		For example, a **Certificate Expiry Date** filter run on July 27, 2021 will return records for certificates expiring before July 26, 2021.
Custom Date	Returns records within the defined custom date.	For example, a **Certificate Expiry Date** filter run on a custom date, say August 1, will return records for certificates expiring before August 1, 2021.

- **At or after** - This operator allows users to generate records at or after the selected time period.

The following table describes the date values supported by the on operator:

Date Type	Description	Example
Today	Returns records for the selected time period, including records with values up to the end of that time frame.	For example, a **Certificate Expiry Date** filter run on July 27, 2021 will return records for certificates expiring at or after July 27, 2021.
Yesterday		For example, a **Certificate Expiry Date** filter run on July 27, 2021 will return records for certificates expiring at or after July 26, 2021.
Custom Date	Returns records within the defined custom date.	For example, a **Certificate Expiry Date** filter run on a custom date, say August 1, will return records for certificates expiring at or after August 1, 2021.

- **At or before** - This operator allows users to generate records at or before the selected time period.

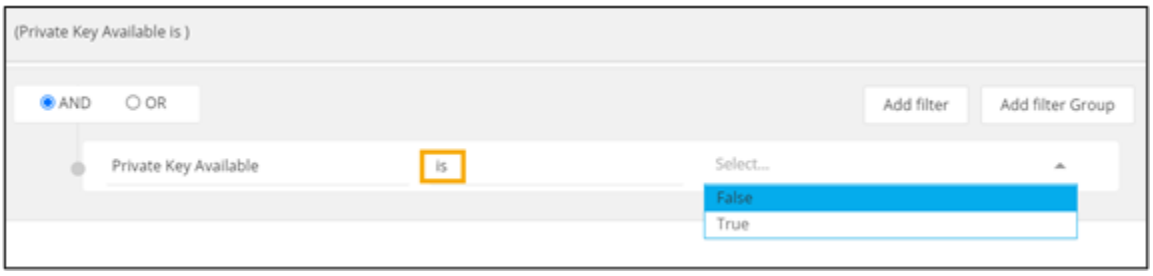
The following table describes the date values supported by the on operator:

Date Type	Description	Example
Today	Returns records for the selected time period, including records with values up to the end of that time frame.	For example, a **Certificate Expiry Date** filter run on July 27, 2021 will return records for certificates expiring at or before July 27, 2021.
Yesterday		For example, a **Certificate Expiry Date** filter run on July 27, 2021 will return records for certificates expiring at or before July 26, 2021.
Custom Date	Returns records within the defined custom date.	For example, a **Certificate Expiry Date** filter run on a custom date, say August 1, will return records for certificates expiring at or before August 1, 2021.

Field Type: Boolean Variable

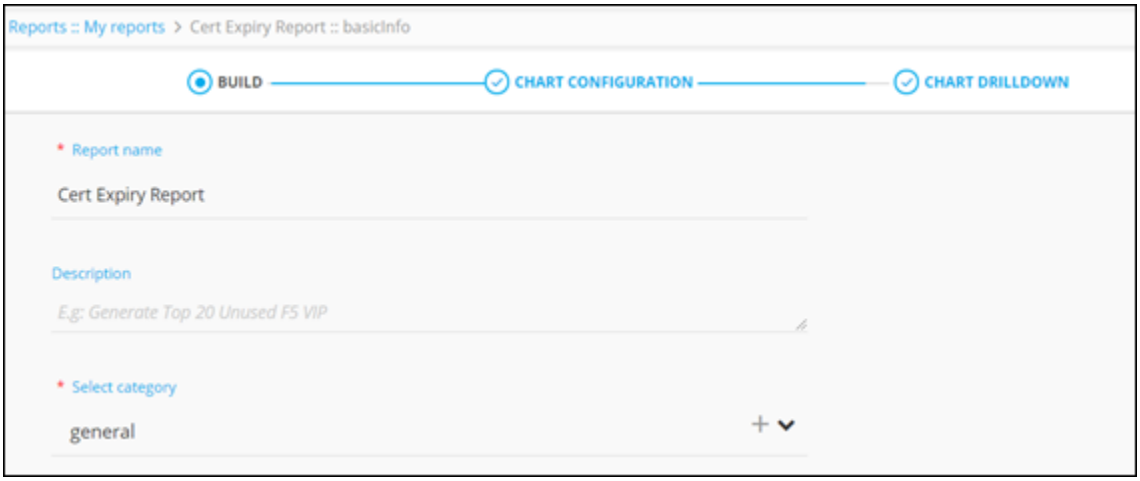
When you choose the field type as **Boolean**, the values for the conditional operator are either **true** or **false**. The conditional operator available when choosing the field type as Boolean is:

- **Is** - The report will display data after confirming if the selected field is available in the database (**True**) or not (**False**).



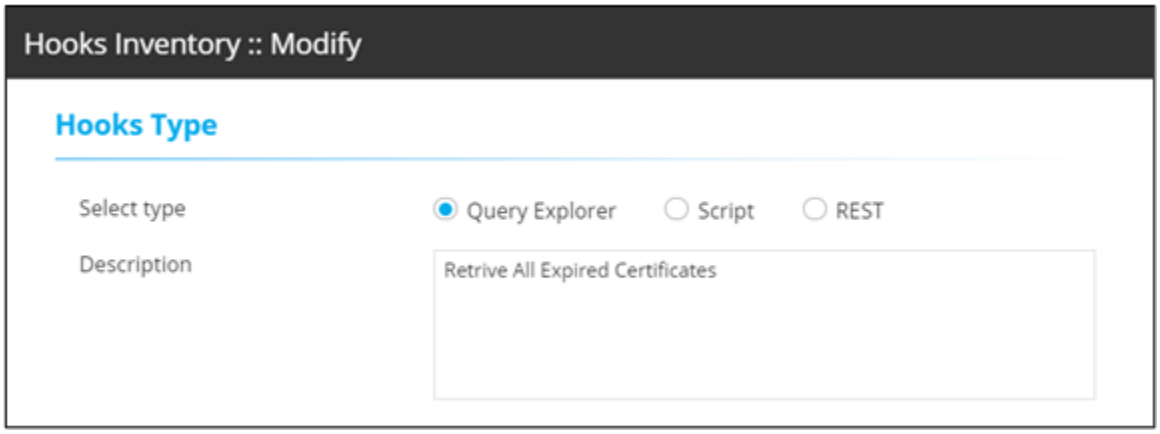
Create a CERT Expiry Report using Query Explorer

1. On the Reports :: My Reports page, click **Create new Report**.
2. Under the **BUILD** section, enter or select the basic information on the report.



3. To modify a hook, hover your mouse over a hook from the pre-populated list and click  .

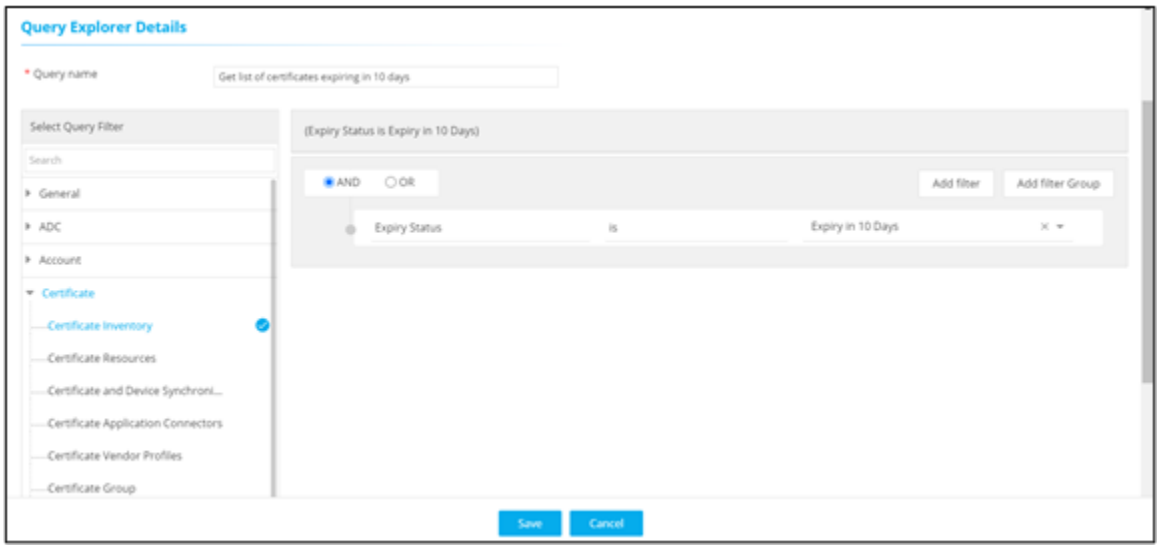
4. In the **Hooks Inventory::Modify** pop-up window that is displayed, under **Hooks Type**, enter or select the required field information.



This table describes the field information in this section:

Field	Description
Select type	Select hook type as **Query Explorer**.
Description	Enter a description of the hook.

5. In the **Query Explorer Details** section, enter or select the required field information.



The following table describes the various fields in this section:

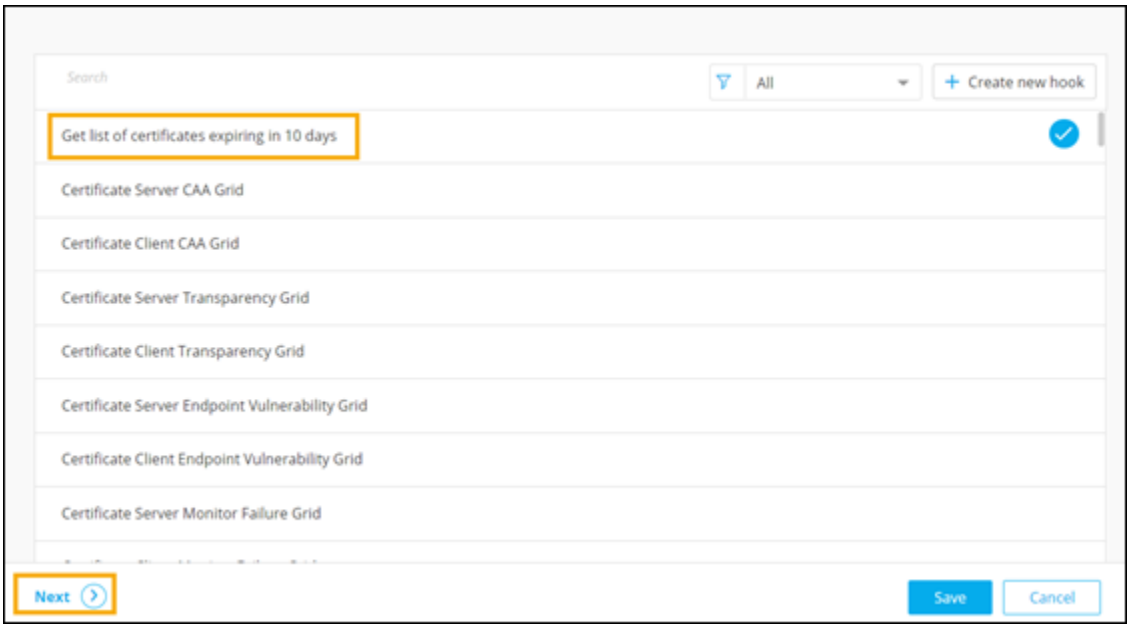
Field	Description
***Query name**	Enter a valid Query name. For example: **Get list of certificates expiring in 10 days**.

Field	Description
Select Query Filter	Select an appropriate query filter. For example:**Certificate Inventory** under **Certificate**, since this report is to get data on certificates.
Add filter	Add a filter and select appropriate fields from the predefined values. For example: **Expiry status is Expiry in 10 days**.
AND/OR	Select the appropriate conditional parameters depending on the type of output required in the report. **AND**: Report will reflect data satisfying all the filter conditions. **OR**: Report will reflect data satisfying either of the filter conditions.
Note: The asterisk (*) symbol indicates mandatory fields.	

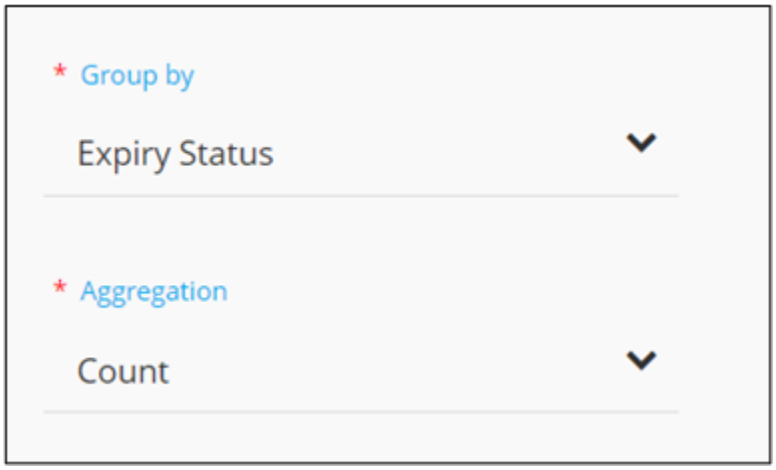
Note:

- Users can add more filters and apply conditional operators to generate different kinds of data in their reports. For example, add another filter to get data on **Compliance Status** of the certificates that are expiring in 10 days.
- Set the conditional parameter to **AND** to generate a report that satisfies both the defined conditions and display certificates that are both compliant and are expiring in 10 days. Setting the conditional parameter to **OR** will generate a report that reflects data satisfying either of the two defined conditions.

6. To create this new hook, click **Save**.
7. To save the basic information, click **Next**.
   The new hook is displayed in the list of hooks.

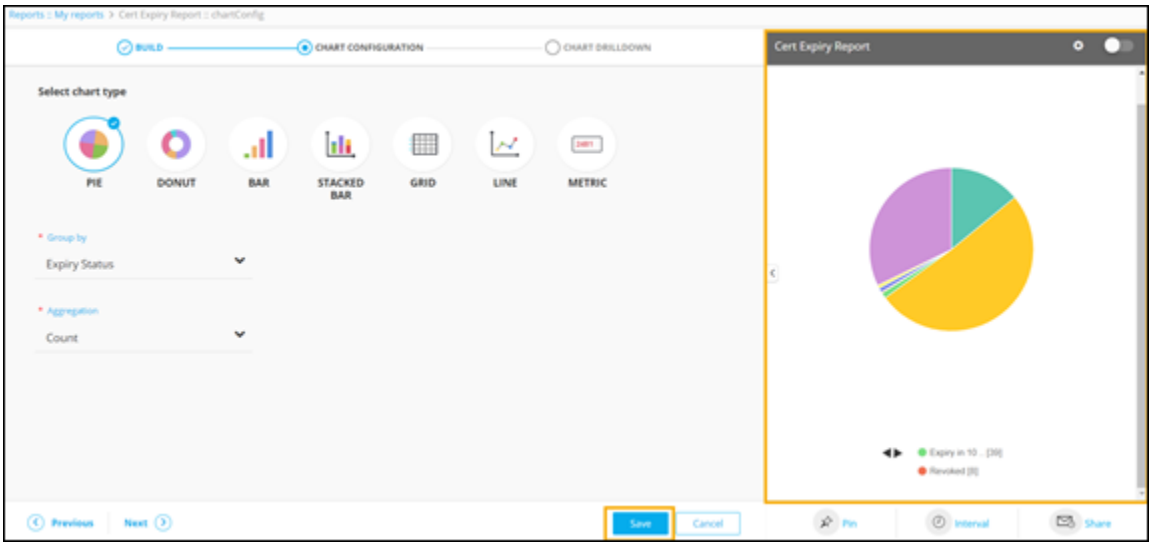


8. Under the **CHART CONFIGURATION** section, select the **PIE** chart.
9. Select the appropriate values for the various fields.

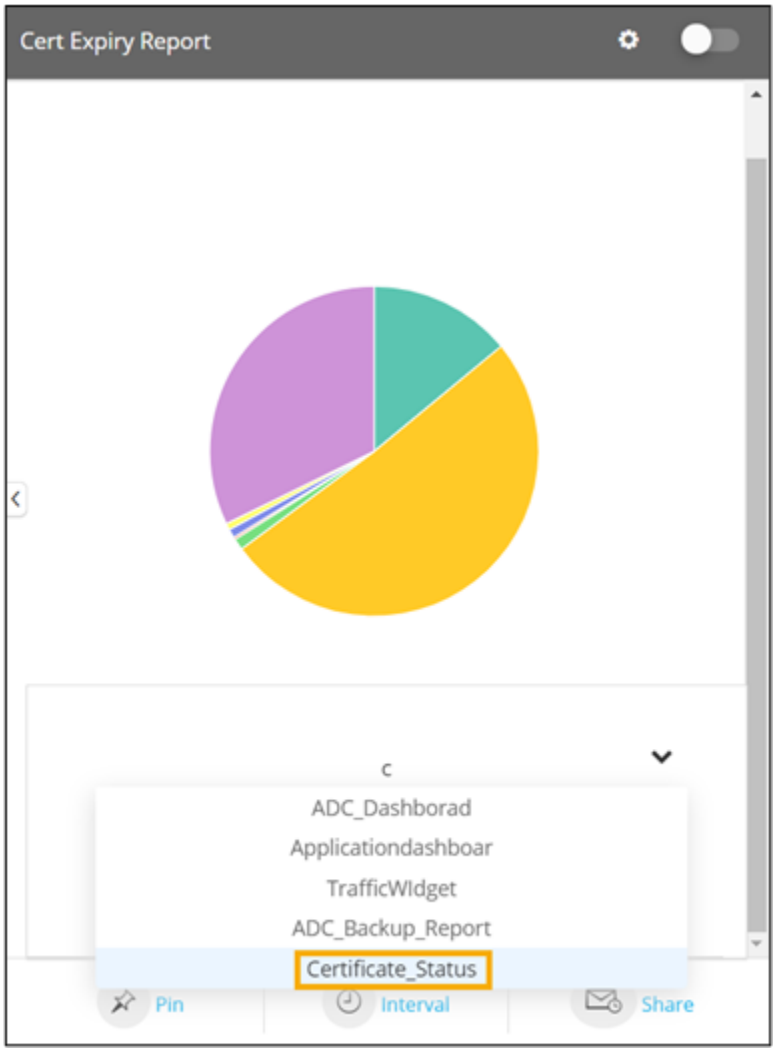


10. Click **Save**.

    A preview of the pie chart is displayed on the right side of the screen.

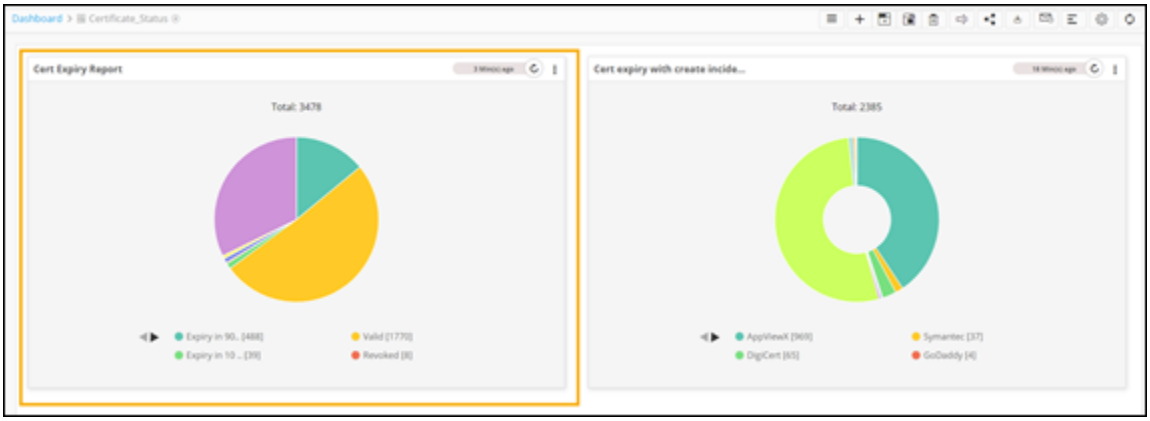


11. To pin the report to the dashboard, under the chart preview, click **Pin**.
12. From the options displayed, select **Existing dashboard**.
13. From the list of available dashboards, select the required dashboard and click **Save**.



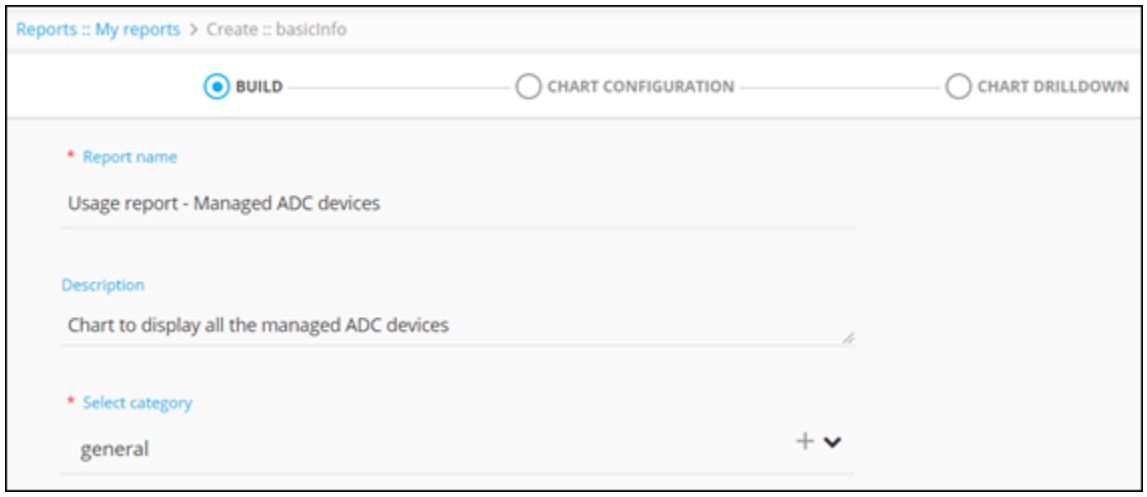
14. To pin this report to the new dashboard, click **Save**.
15. To enable the report, turn on the toggle.
16. To view this report on the dashboard, search for the dashboard in the dashboard inventory.

    The **Cert Expiry Report** can be seen on the dashboard.



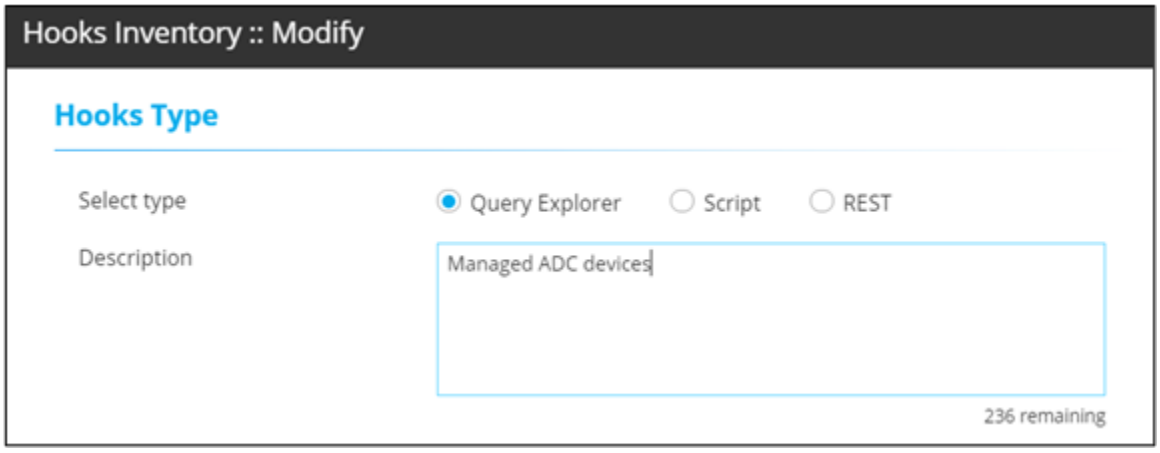
Create an ADC Usage Report using Query Explorer

1. On the Reports :: My Reports page, click **Create new Report**.
2. Under the **BUILD** section, enter or select the basic information on the report.



3. To modify the hook, select a hook from the pre-populated list and click .

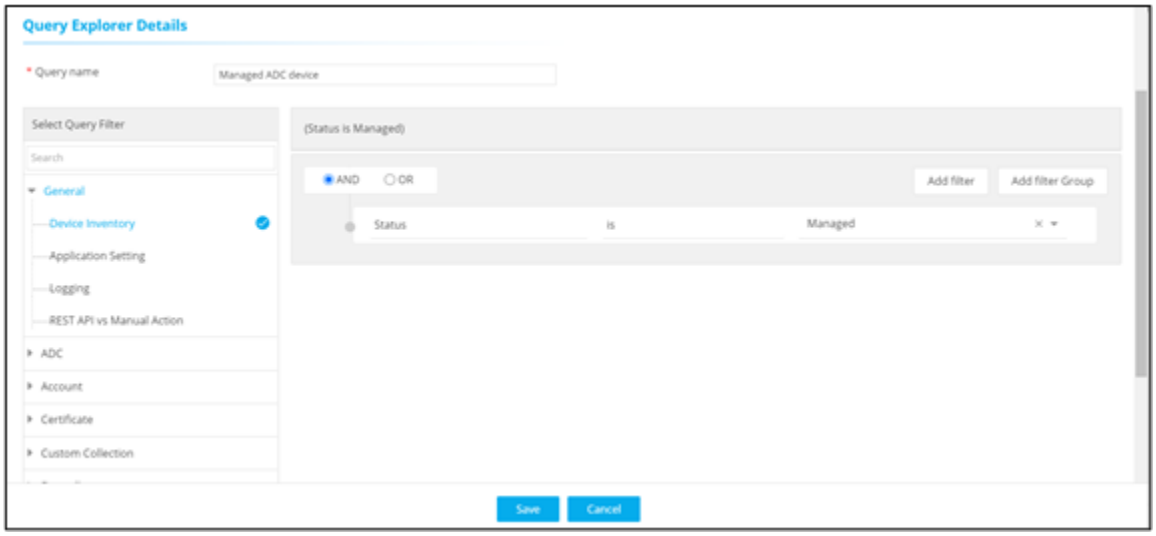
4. In the **Hooks Inventory::Modify** pop-up window that is displayed, under **Hooks Type**, enter or select the field information.



This table describes the field information in this section:

Field	Description
Select type	Select hook type as **Query Explorer**.
Description	Enter a description of the hook.

5. In the **Query Explorer Details** section, enter or select the field information.



The following table describes the various fields in this section:

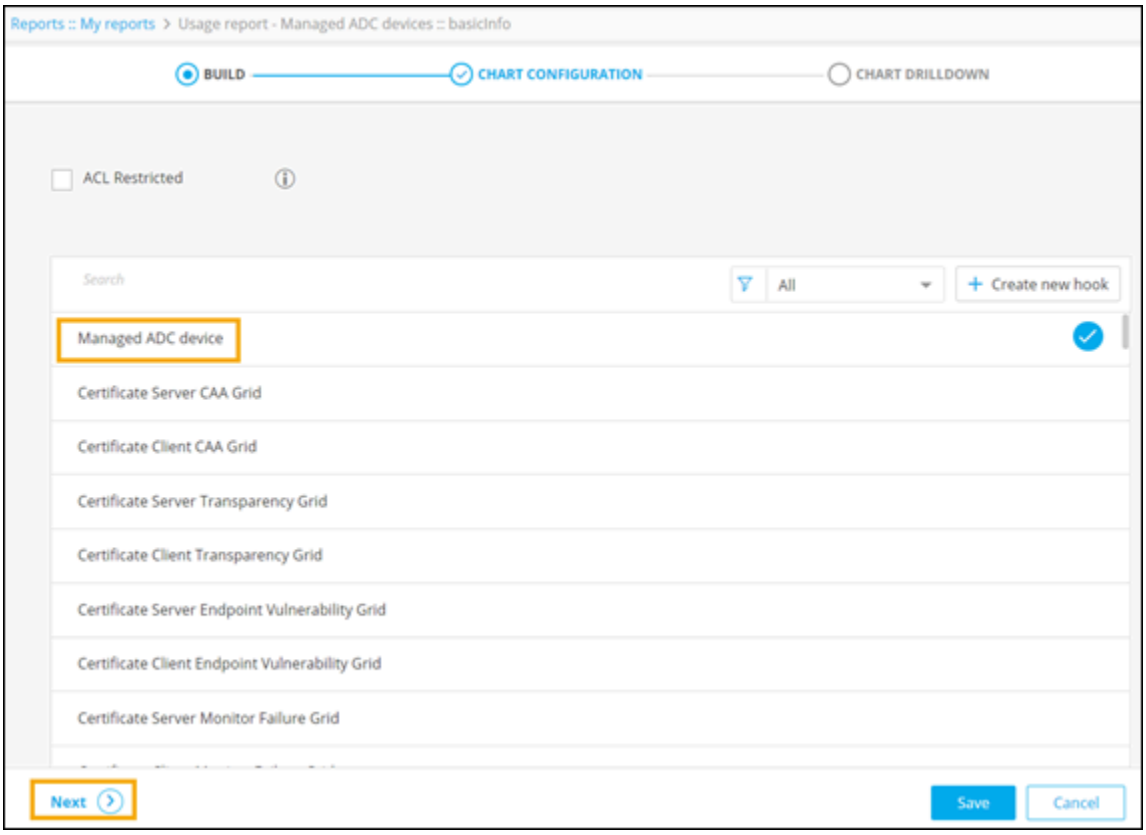
Field	Description
Query name	Enter a valid Query name. For example: **Managed ADC devices**.

Field	Description
Select Query Filter	Select an appropriate query filter. For example: **Device Inventory** under **General**, since this report is to get data on devices.
Add filter	Select appropriate fields from the pre-defined values. For example: **Status is Managed**.
AND/OR	Select the appropriate conditional parameters depending on the type of output required in the report. **AND**: Report will reflect data satisfying all the filter conditions. **OR**: Report will reflect data satisfying either of the filter conditions.

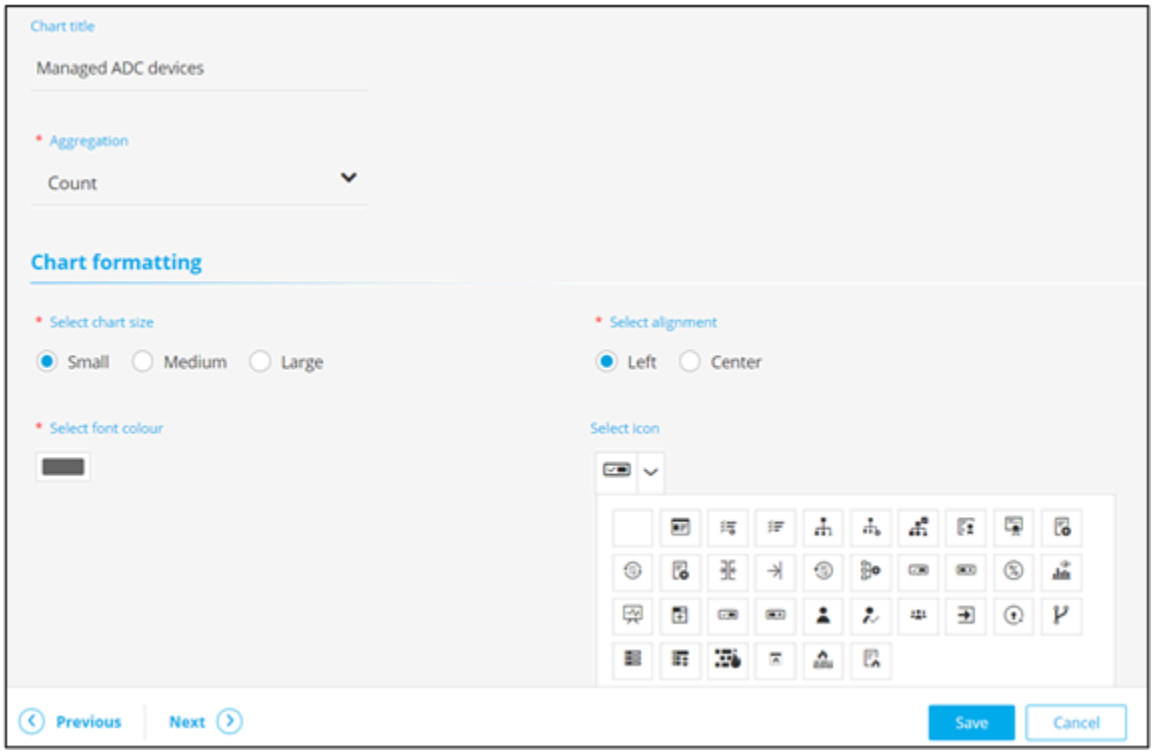
Note:

- Users can add more filters and apply conditional operators to generate different kinds of data in their reports. For example, adding another filter to get data on credential type of the ADC devices that are managed.
- Set the conditional parameter to **AND** to generate a report that satisfies both the conditions and display devices that are both managed and required manual credentials entry. Setting it to **OR** will generate a report that reflects data satisfying either of these two defined conditions.

6. To create this new hook, click **Save**.
   The new hook can be seen in the list of hooks.

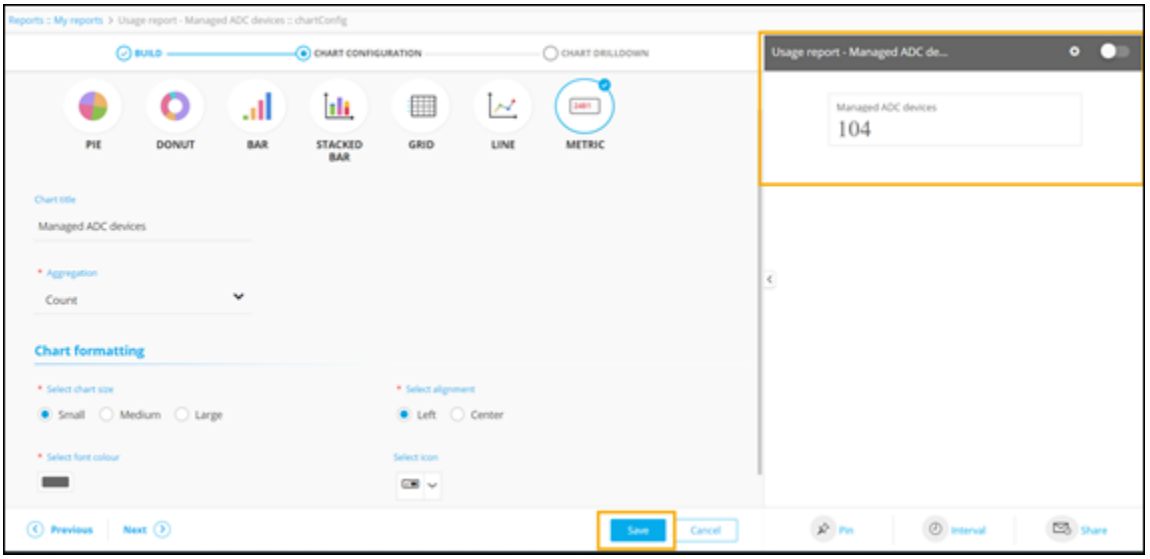


7. To save the basic information, click **Next**.
8. Under the **CHART CONFIGURATION** section that is displayed, select the chart type as **METRIC**.
9. Enter or select the required field information as shown here.



10. Click **Save**.

    A preview of the metric is displayed on the right side of the screen.



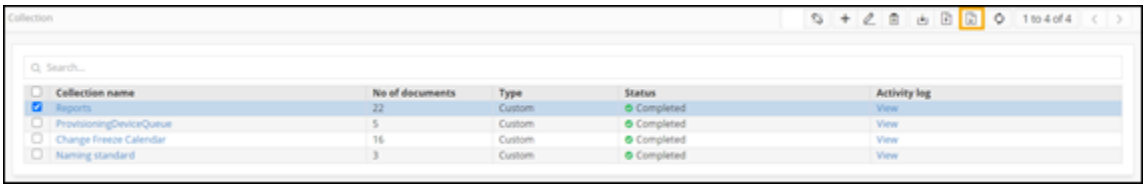
Importing Custom Data in Query Explorer

You can import data and upload it into the **Collection** module of the AppViewX platform and enable it to build custom queries to create reports.

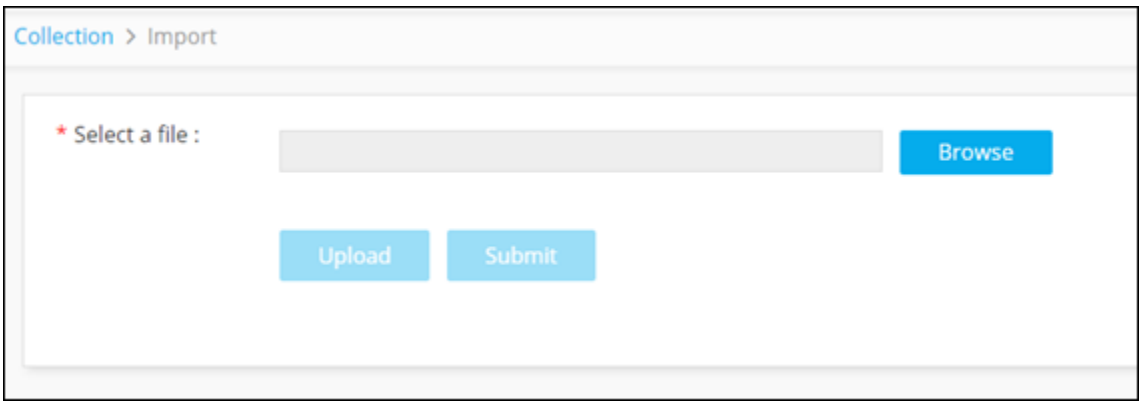
To import a collection into the Query Explorer:

New Menu	Old Menu
1. From the main navigation menu, select **Automation**. 2. In the **Automation** module, from the left menu, under **WORKFLOW**, click **Collection**. The **Collection** page is displayed.	From the main navigation menu, select **Collection**. The **Collection** page is displayed.
Note: For more information on how to switch between menus, click here.	

1. To import a collection, on the **Collection** page, from the command bar on top right corner, click .

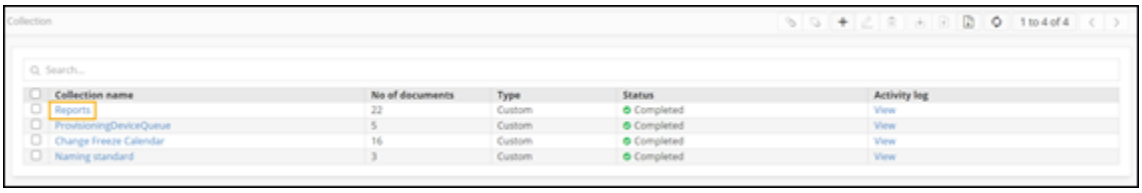


2. To select a file to be uploaded to the **Collection** module, click **Browse**.



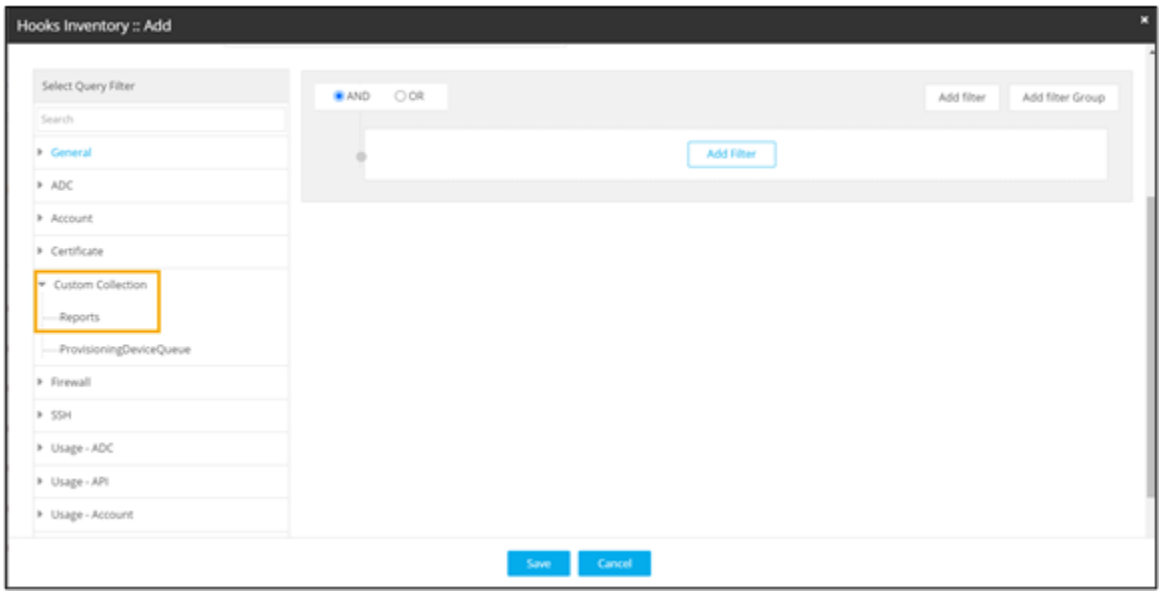
3. Select the required file and click **Upload**.
4. Select the collection and click **Submit**.

   The newly created collection can be seen on the **Collection** page under **Collection Name**.



5. To enable the collection to build a custom query, select the collection and from the command bar click  .
6. On the Reports :: My Reports page, click **Create new report**.
7. Under the **BUILD** section, click **Create new hook**.

   The newly created collection is displayed in the **Hooks Inventory::Add** pop-up window in the **Custom Collection** category.



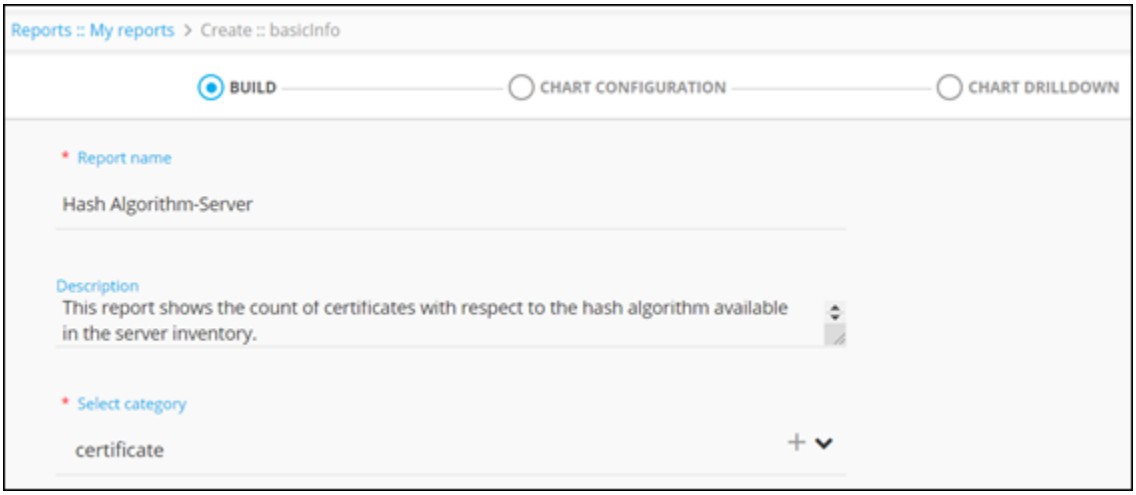
Using Scripts to build Reports

The report builder allows you to create reports using preexisting and custom scripts. You can add your own custom code to generate reports that meet your requirements.

- Example 1
- Example 2

Example 1

1. On the Reports :: My Reports page, click **Create new report**.
2. Under the **BUILD** section, enter or select the field information.

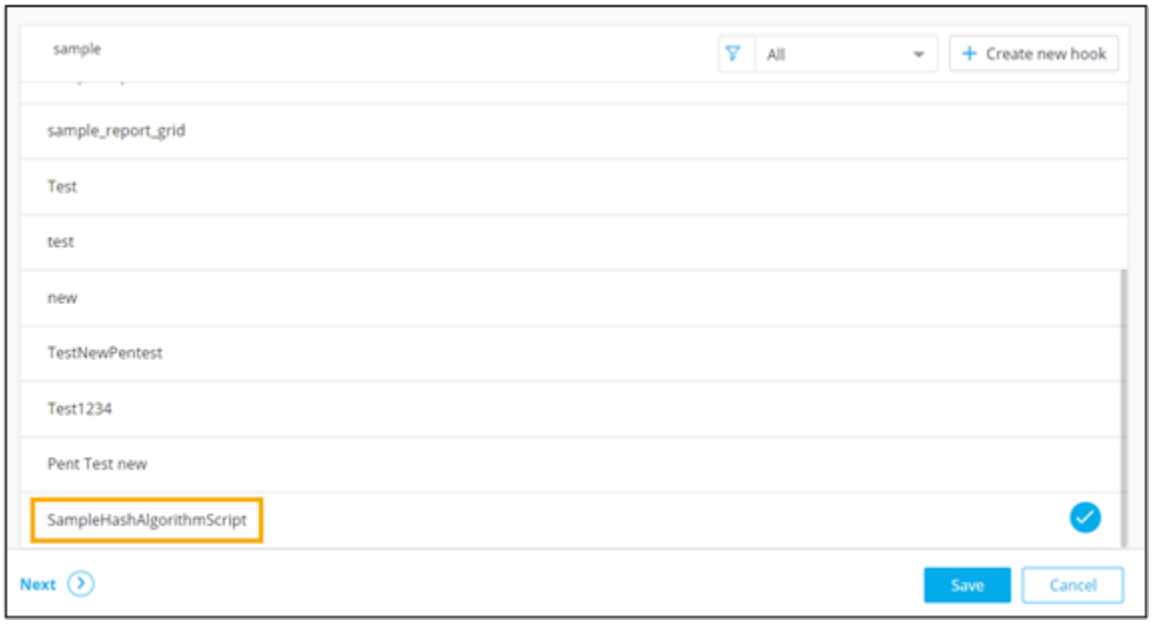


This table describes the field information under this section:

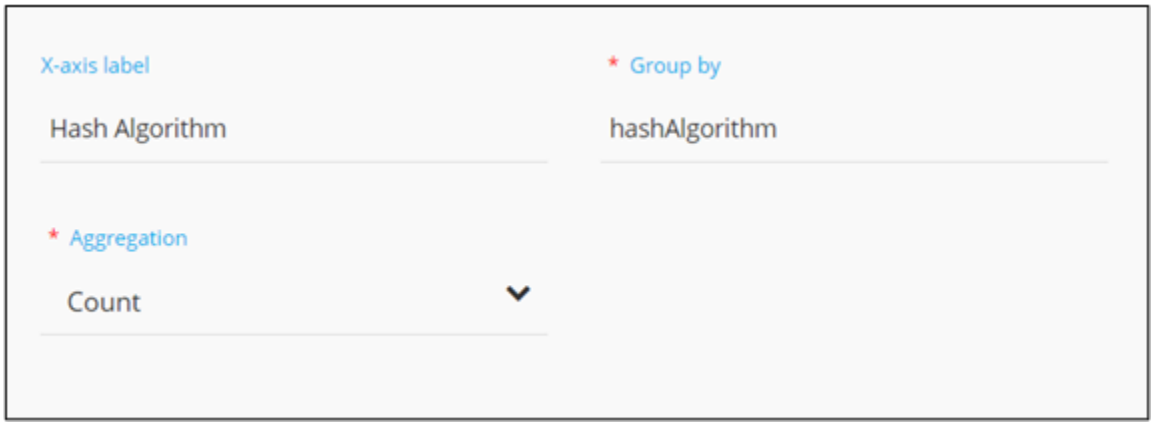
Field	Description
***Report name**	Enter a valid report name. For example, **Hash Algorithm-Server**.
Description	Enter a description of the report. For example: **This report shows the count of certificates with respect to the hash algorithm available in the server inventory.**
***Select category**	Select category as **certificate**.

Note: The asterisk (*) symbol indicates mandatory fields.

3. Select the **ACL restricted** check box.
4. Select a sample script from the list of available hooks.



5. To save your selections, click **Next**.
6. Under the **CHART CONFIGURATION** section, select the **BAR** chart.
7. Enter or select the required field information.



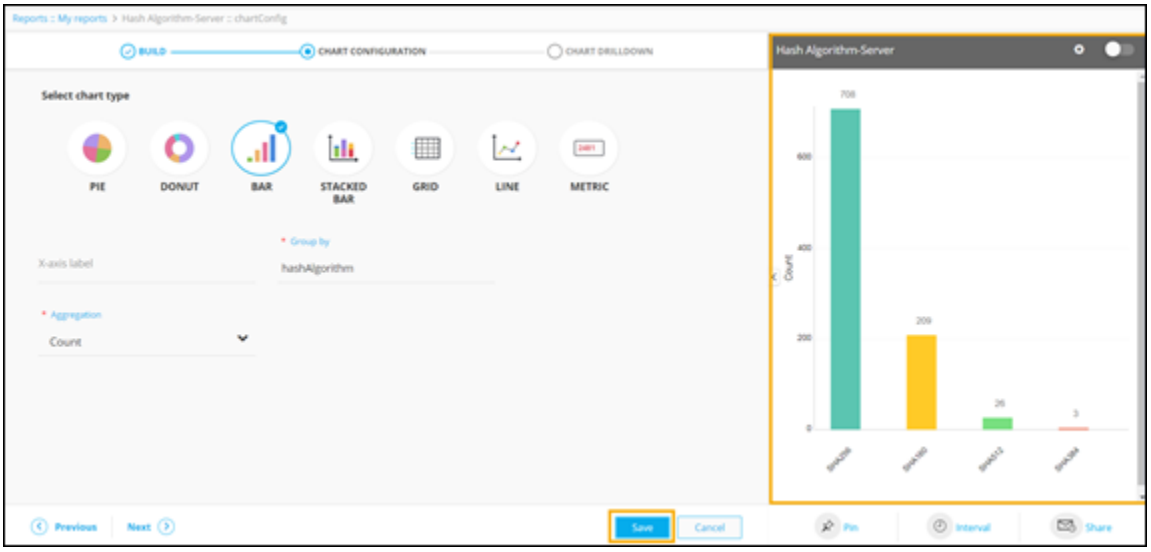
This table describes the field information under this section:

Field	Description
X-axis label	Enter the criteria for the X-axis label. For example, Hash algorithm.
***Group by**	Select a value from the dropdown menu on the basis of which report data will be grouped.

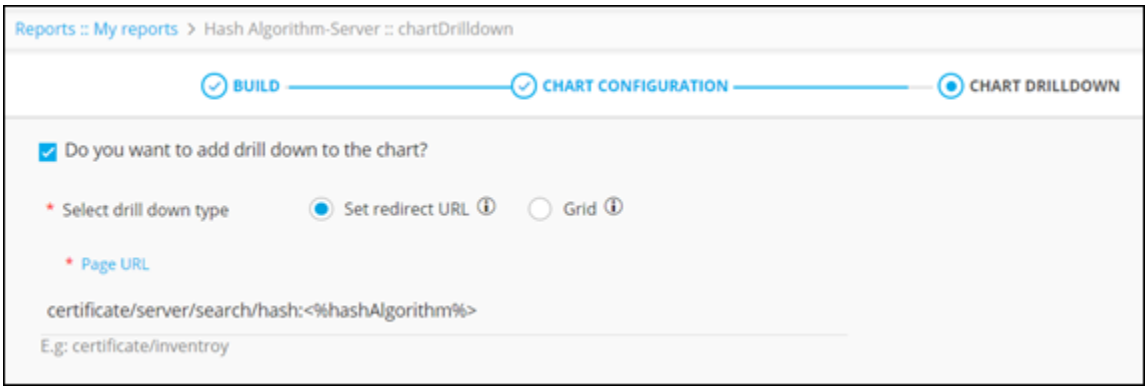
Field	Description
	For example, hashAlgorithm.
***Aggregation**	Select the calculation to be done on the report data for the dropdown. The following options are available: • **Average**: Calculates the average value of a given set of data. • **Sum**: Calculates the sum of all values in a given set of data. • **Count**: Calculates the total number of items in a given numeric field. • **Maximum**: Displays the maximum value in a given set of data. • **Minimum**: Displays the minimum value in a given set of data.
	Note: The asterisk (*) symbol indicates mandatory fields.

8. Click **Save**.

   A preview of the bar chart is displayed on the right side of the screen.



9. To add drill down to the report, click **Next**.
10. Under the **CHART DRILLDOWN** section, enter or select the required field information.



The following table describes the field information on this page:

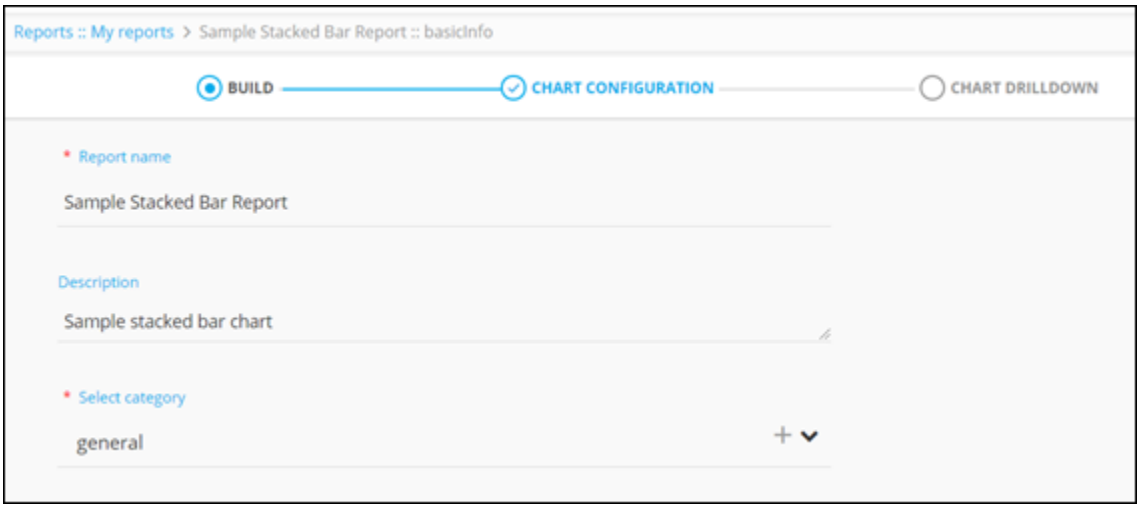
Field	Description
***Select drill down type**	Select drill down type as redirect URL.
***Page URL**	Enter a valid URL.

Note: The asterisk (*) symbol indicates mandatory fields.

11. To enable drill down, click **Save & Enable**.
    You will be redirected to the drill down URL, click on any of the bars on the bar chart.

Example 2

1. On the Reports :: My Reports page, click **Create new report**.
2. Under the **BUILD** section, enter or select the required field information.



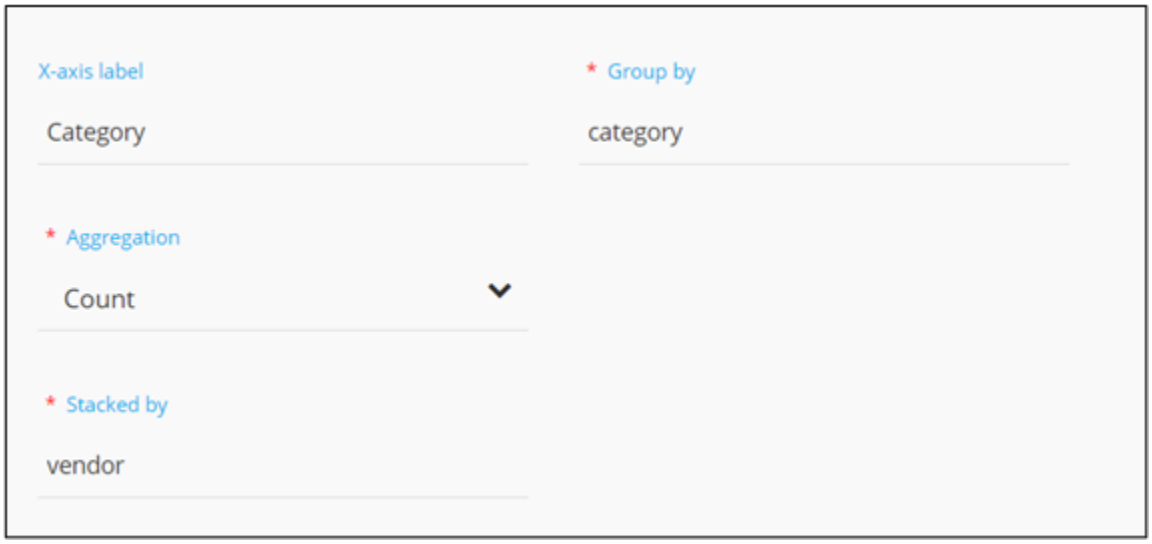
This table describes the field information in this section:

Field	Description
***Report name**	Enter a valid report name.
Description	Enter a valid description of the report.
***Select category**	Select category as general.

Note: The asterisk (*) symbol indicates mandatory fields.

3. Select the required hook from the list and click .

4. Click **Next**.
5. Under the **CHART CONFIGURATION** section, select the **STACKED BAR** chart.
6. Enter or select the field information on this page.



This table describes the fields in this section:

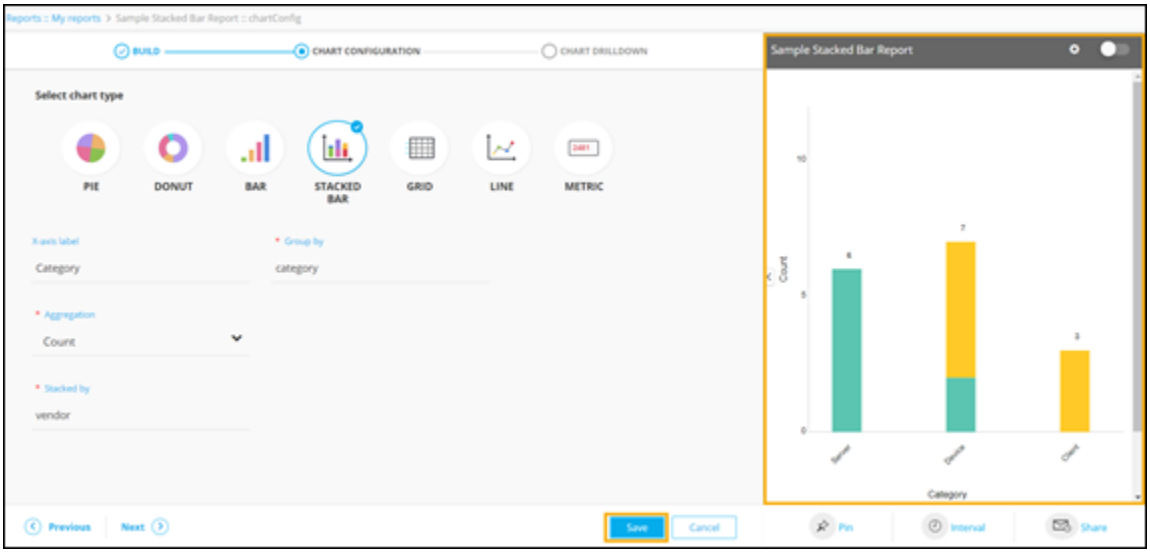
Field	Description
X-axis label	Enter the criteria for the X-axis label.
***Group by**	Enter the criteria on the basis of which report data will be grouped.

Field	Description
	For example, **category**.
***Aggregation**	Select the calculation to be done on the report data for the dropdown. The following options are available: • **Average**: Calculates the average value of a given set of data. • **Sum**: Calculates the sum of all values in a given set of data. • **Count**: Calculates the total number of items in a given numeric field. • **Maximum**: Displays the maximum value in a given set of data. • **Minimum**: Displays the minimum value in a given set of data.
***Stacked by**	Enter the criteria on the basis of which report data will be stacked. For example, **vendor**.

Note: The asterisk (*) symbol indicates mandatory fields.

7. Click **Save**.

   A preview of the stacked bar chart is displayed on the right side of the screen.



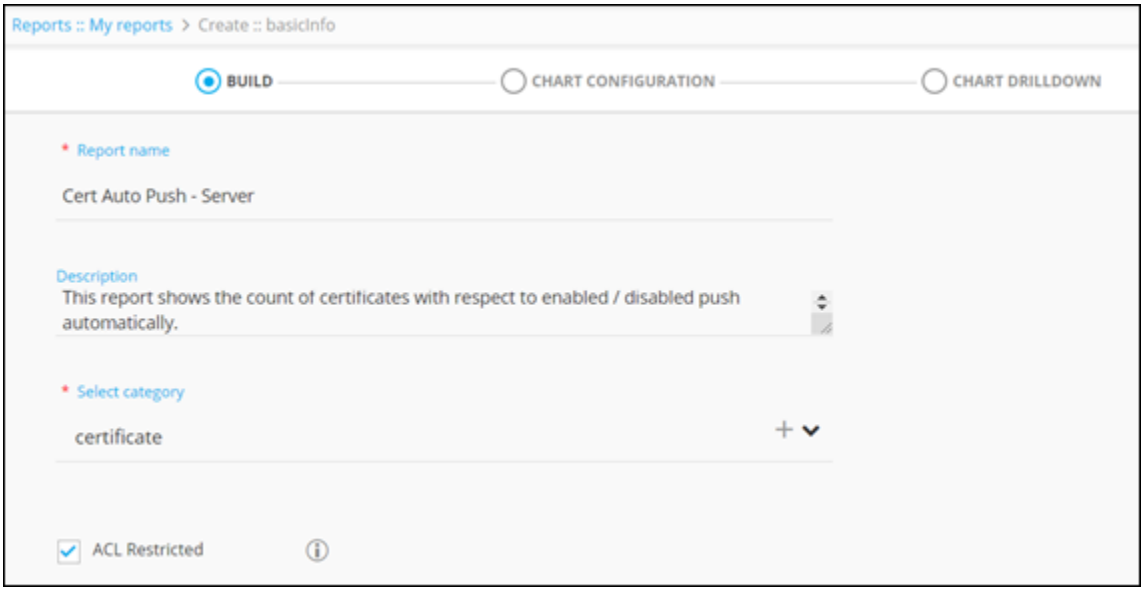
Using REST API to build Reports

You can also use the report builder to create reports using preexisting or custom APIs. You can integrate your internal APIs into this platform to generate customized reports.

- Creating a Report using Sample REST API

Creating a Report using Sample REST API

1. On the Reports :: My Reports page, click **Create new report**.
2. Under the **BUILD** section, enter or select the required field information.



This table describes the field information under this section:

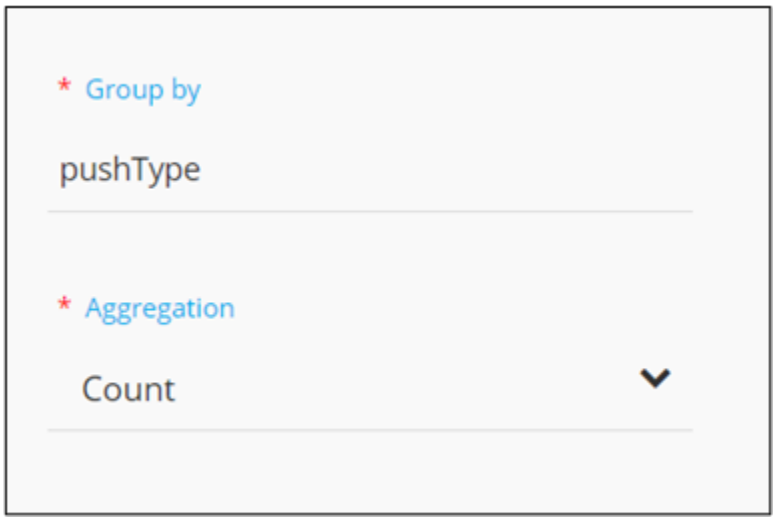
Field	Description
***Report name**	Enter a valid report name. For example, **Cert Auto Push server**.
Description	Enter a valid description for the report. For example: **This report shows the count of certificates with respect to enabled / disabled push automatically.**
***Select category**	Select category as certificate.

Field	Description
ACL restricted	Select this checkbox to query certificates based on role permission.

Note: The asterisk (*) symbol indicates mandatory fields.

3. Select a sample API hook from the list of preexisting hooks.

4. Click **Next**.
5. Under the **CHART CONFIGURATION** section, select the **PIE** chart.
6. Enter or select the required field information.

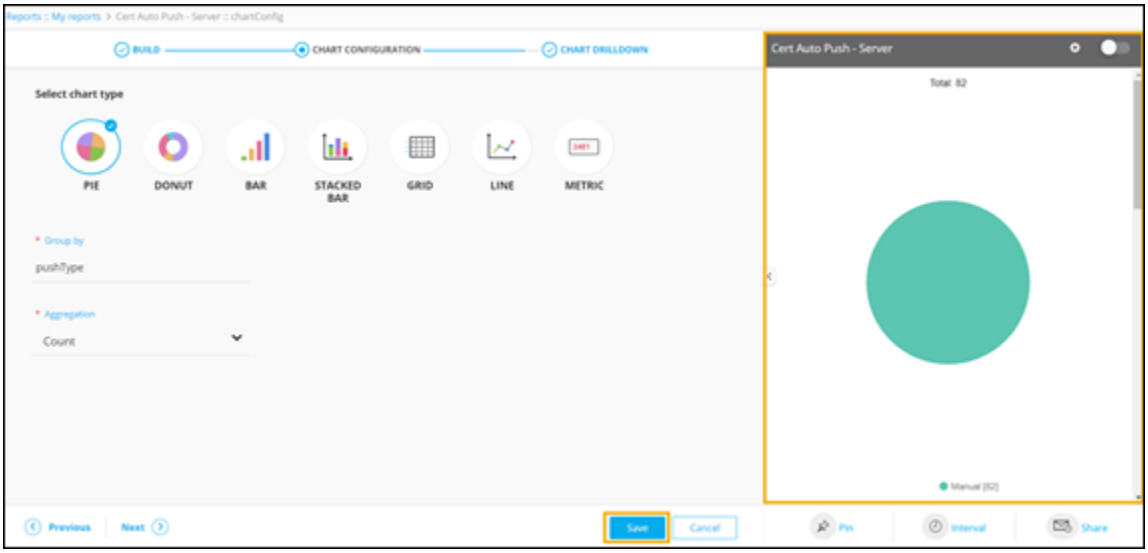


The following table describes the field information in this section:

Field	Description
***Group by**	Enter the criteria on the basis of which report data will be grouped. For example: **pushType**.
***Aggregation**	Select the calculation to be done on the report data for the dropdown. The following options are available: • **Average**: Calculates the average value of a given set of data. • **Sum**: Calculates the sum of all values in a given set of data. • **Count**: Calculates the total number of items in a given numeric field. • **Maximum**: Displays the maximum value in a given set of data. • **Minimum**: Displays the minimum value in a given set of data.
Note: The asterisk (*) symbol indicates mandatory fields.	

7. Click **Save**.

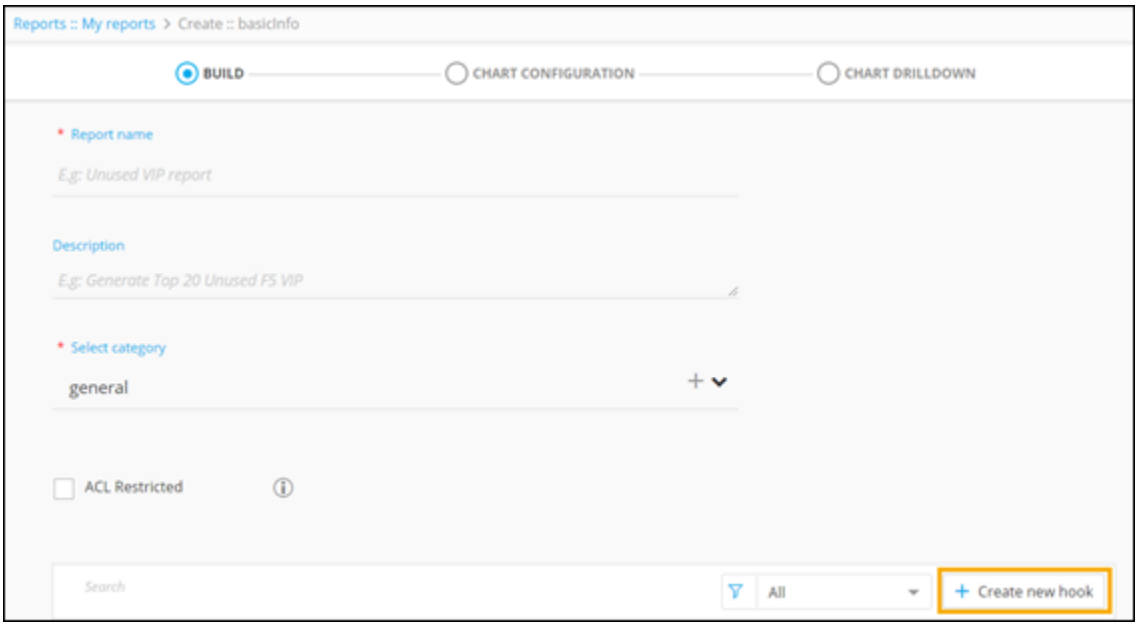
   A preview of the pie chart is generated on the right side of the screen.



Creating a New Hook

To create a new hook for generating reports based on a specific category:

1. On the Reports :: My Reports page, click **Create new report**.
2. Under the **BUILD** section, click **Create new hook**.



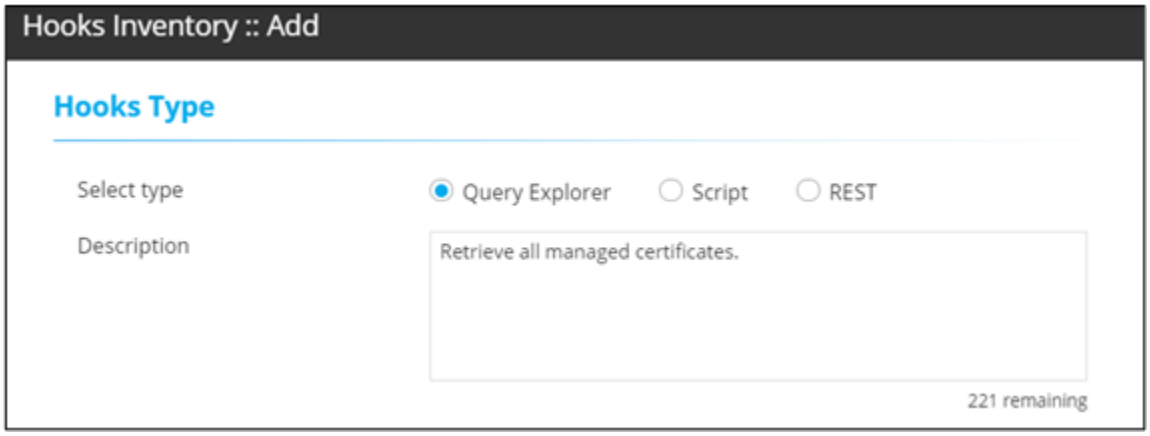
The **Hooks Inventory :: Add** window pops up. You can add/create a new hook according to your specific requirements.

- Creating a Query Explorer Hook
- Creating a Script Hook
- Creating a REST API Hook

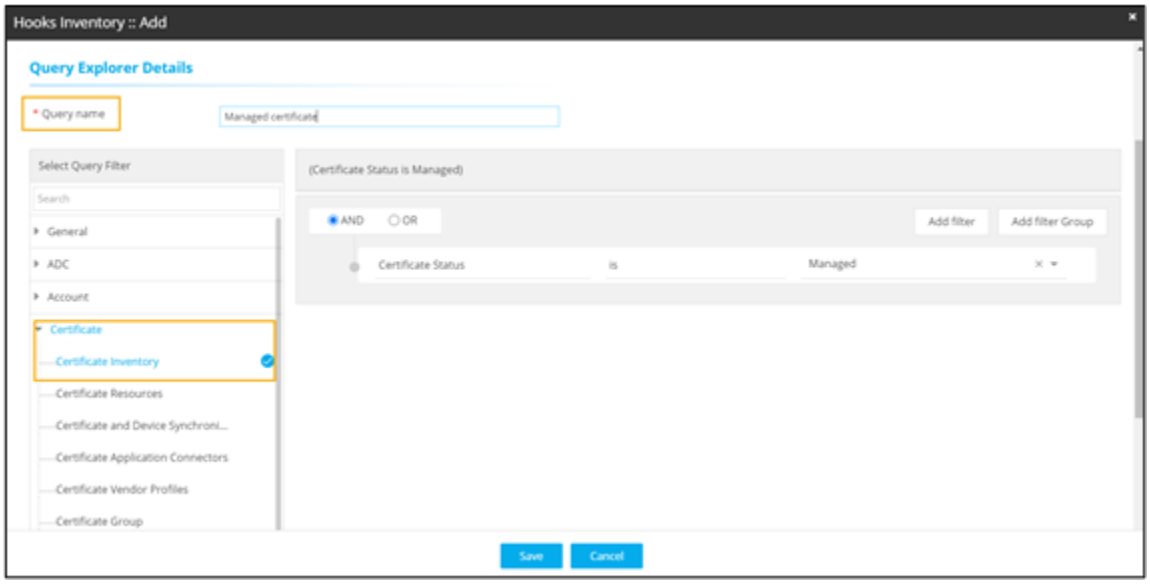
Creating a Query Explorer Hook

To create a hook based on Query Explorer:

1. In the **Hooks Inventory :: Add** window, under **Hooks Type**, select the **Query Explorer** option.
2. Add a description for the selected hook.



3. Under the **Query Explorer Details**section, enter or select the required field information.



The following table describes the various fields in the **Query Explorer Details** section:

Field	Description
***Query name**	Enter a valid query name. For example: **Managed certificates**.
Select Query Filter	Select an appropriate query filter from the pre-populated list of filters. For example:**Certificate Inventory** under **Certificate section**.

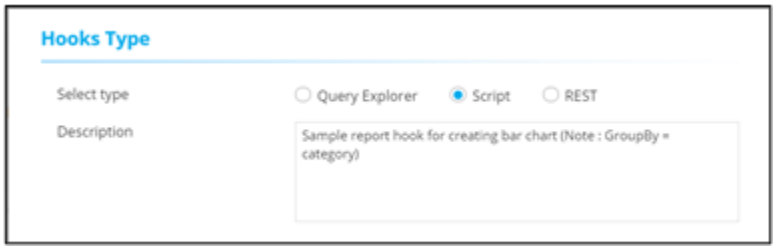
Field	Description
Add Filter	Add a filter and select appropriate fields from the predefined values. For example: **Certificate Status is Managed**.
AND/OR	Select the appropriate conditional parameters depending on the type of output required in the report. **AND**: Report will reflect data satisfying all the filter conditions. **OR**: Report will reflect data satisfying either of the filter conditions.
Note: The asterisk (*) symbol indicates mandatory fields.	

4. To add this new hook to the Hooks Inventory, click **Save**.

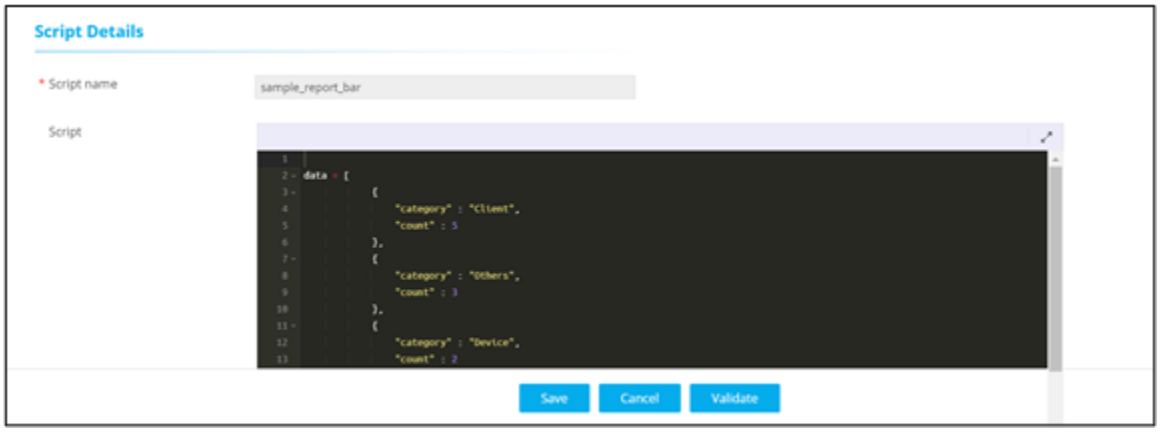
Creating a Script Hook

To create a hook based on Script:

1. In the **Hooks Inventory :: Add** window, under **Hooks Type**, select the **Script** option.
2. Add a description for the selected hook.



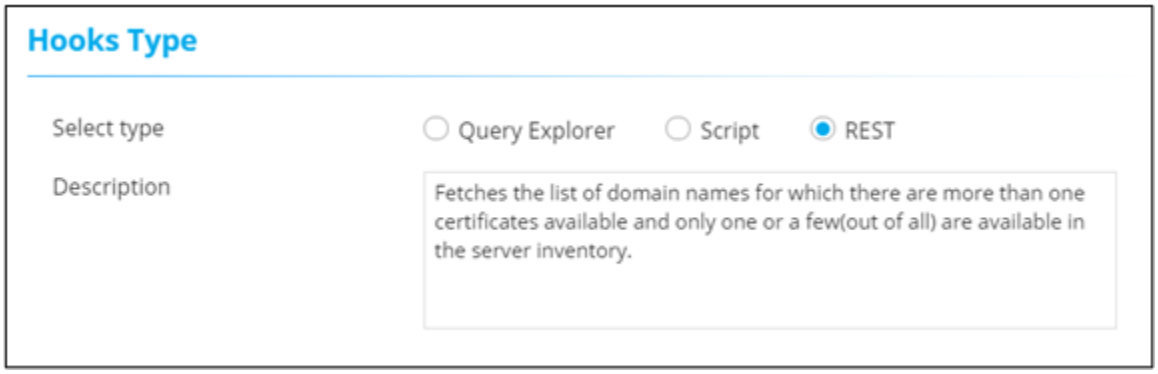
3. Under the **Script Details** section, enter a valid script name and define the script logic .



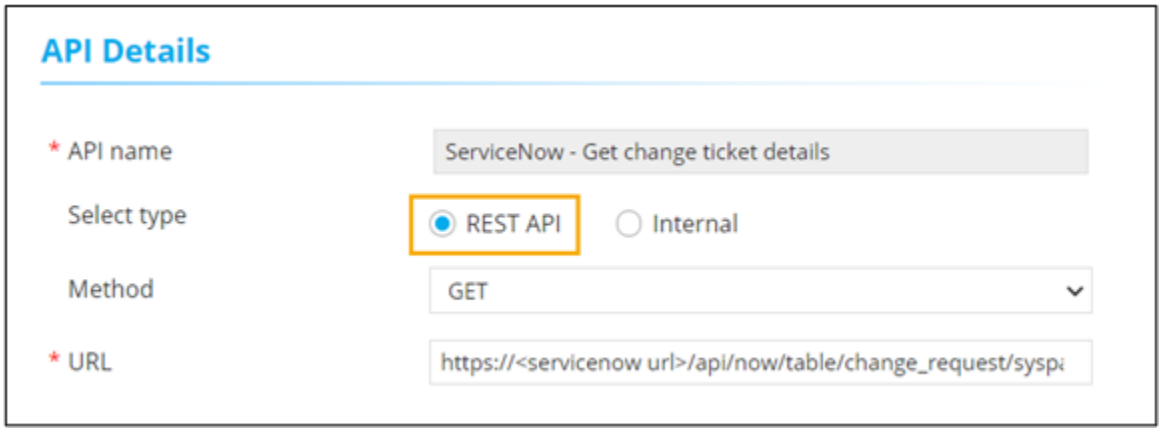
4. To add this new hook to the Hooks Inventory, click **Save**.

Creating a REST API Hook

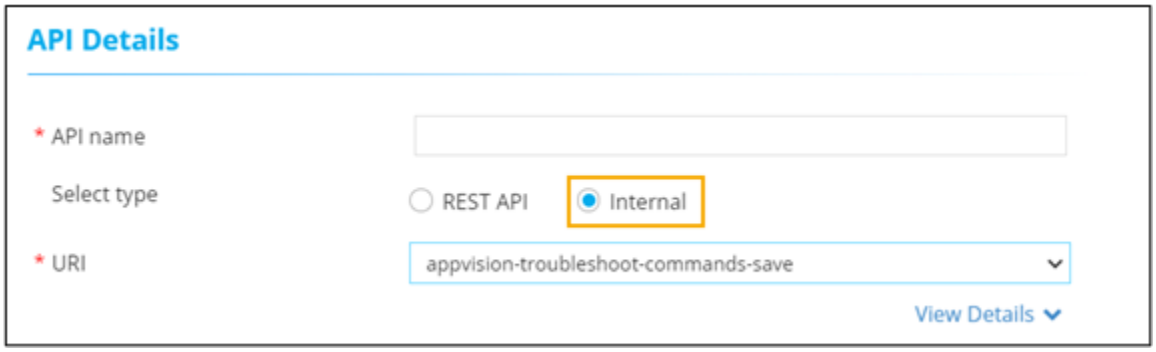
1. In the **Hooks Inventory :: Add** window, under **Hooks Type**, select the **REST** option.
2. Enter a description for the selected hook.



3. Under **API Details**, enter or select the field information.
   - **Using REST API**



◦ **Using Internal API**



The following table describes field description in this section:

Field	Description
API name	Enter a valid name for the API.
Select type	You can select between REST API and Internal. • **REST API**: Use this to select external API and enter the URL. • **Internal**: Use this to select an internal API and select a URI (Uniform Resources Identifier) from the dropdown menu.
Path params	Parameters that are used to identify a specific resource(s).
Query params	Parameters that are used to filter resources.

Note: The asterisk (*) symbol indicates mandatory fields.

4. Under **Request Body**, enter the payload and response mapping details.

The following table describes field description in this section:

Field	Description
Payload	Payload is the actual data that needs to be passed for the API.
Response mapping	Mapping an integration response from the backend.

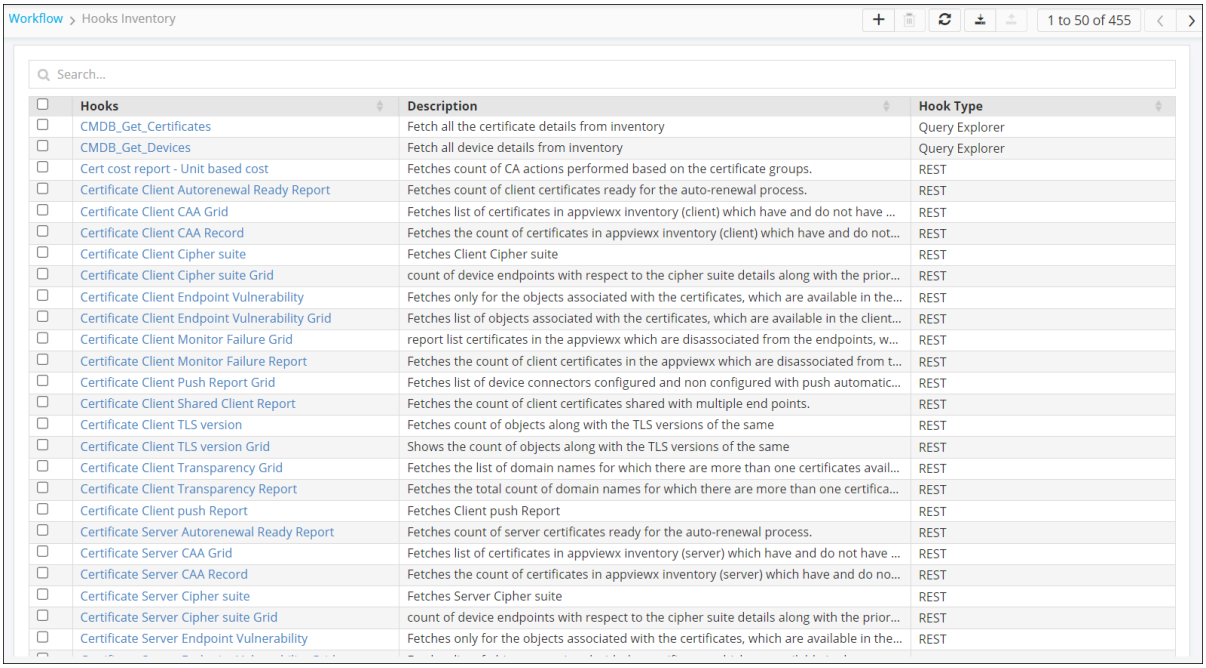
5. To add this new hook to the Hooks Inventory, click **Save**.

Reusing Hooks

The **Hooks Inventory** lists all the hooks that are available to you for building reports. Any new hook created will be added to the **Hooks Inventory** and can be reused for creating reports.

To create and reuse hooks:

1. Go to the **Hooks Inventory** in the **Automation** module.

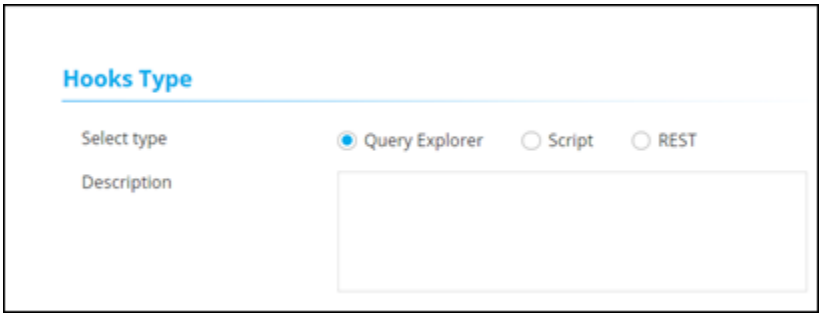


Note: For more information on the Hooks Inventory, refer to the Automation User Guide

2. To add a new hook, from the command bar at the top right corner of the screen, click +.

   The **Workflow > Hooks Inventory > Add** page is displayed.

3. Under the **Hooks Type** section, enter or select the required field information.

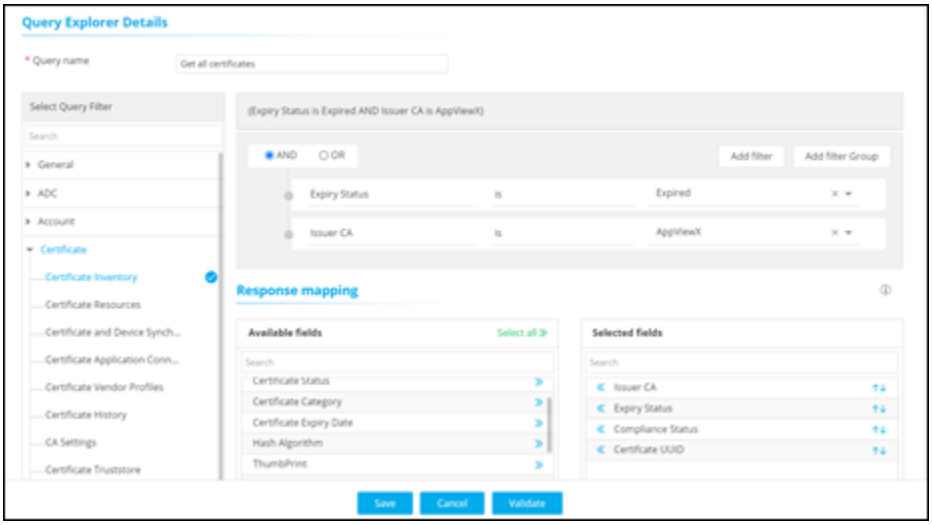


This table describes the field information in this section:

Field	Description
Select Type	Select hook type as **Query Explorer**.
Description	Enter a valid description.

Field	Description
	For example: **Retrieve all certificates that have been managed or monitored.**

4. Under the **Query Explorer Details** section, enter or select the required field information.



This table describes the various fields in this section:

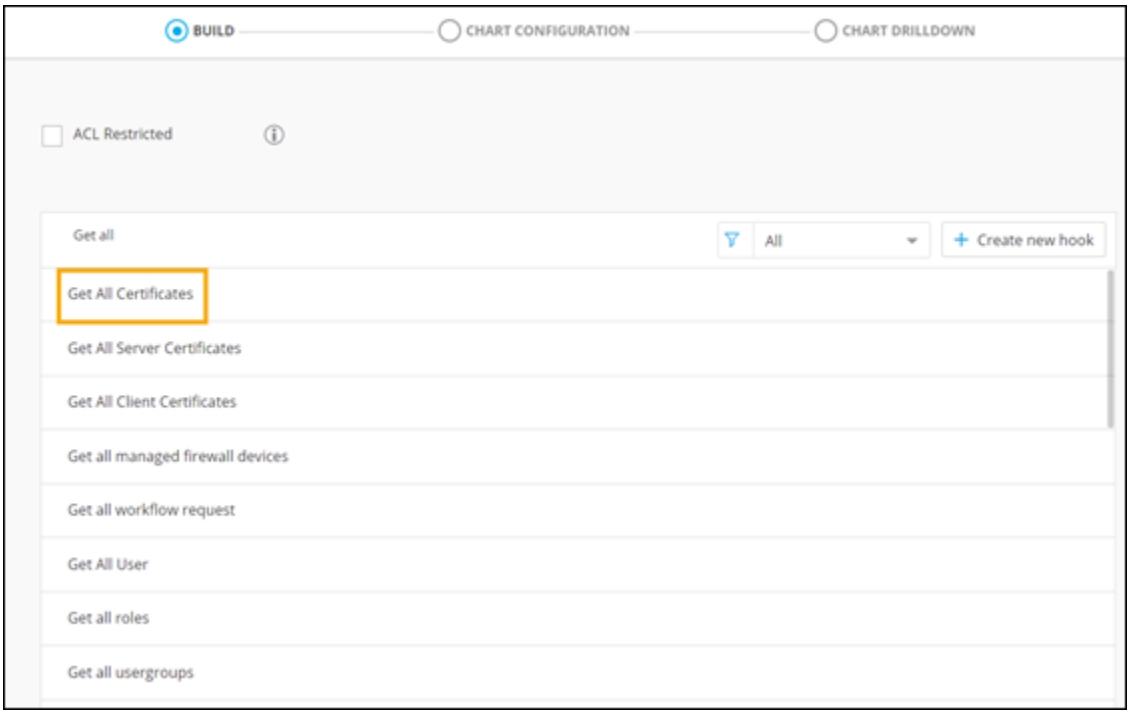
Field	Description
Query name	Enter a valid query name. For example: **Get all certificates**.
Select Query Filter	Select an appropriate query filter from the collection of hooks. For example: **Certificate Inventory** under the **Certificate section.**
Add filter	Add a filter(s) and select appropriate fields from the predefined values. For example: **Expiry Status is Expired and Issuer CA is AppViewX.**
AND/OR	Select the appropriate conditional parameters depending on the type of output required in the report. **AND**: Report will reflect data satisfying all the filter conditions. **OR**: Report will reflect data satisfying either of the filter conditions.

Field	Description
Response Mapping	Select the fields from the available list to map the integration response. For example: Select **Issuer CA, Expiry Status, Certificate Status, Certificate UUID.** Selected fields appear on the right side.

Note: The asterisk (*) symbol indicates mandatory fields.

5. To add this hook to the **Hooks Inventory**, click **Save**.
6. On the Reports :: My Reports page, click **Create new report**.

   The new hook is added to the list of hooks.



Report Widgets

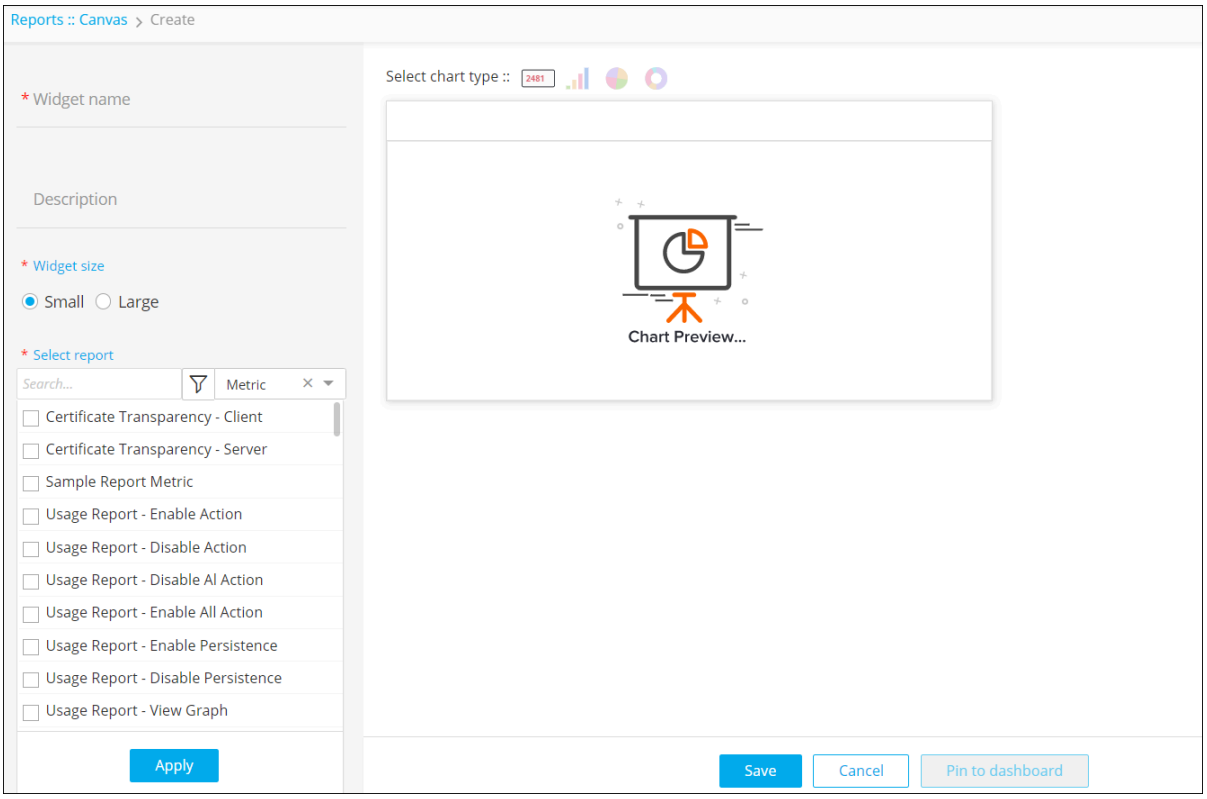
You can create customized widgets, pin them to a dashboard, and also download report widgets to your device using the Report builder.

How to Create a Widget

Creating a User Summary Widget

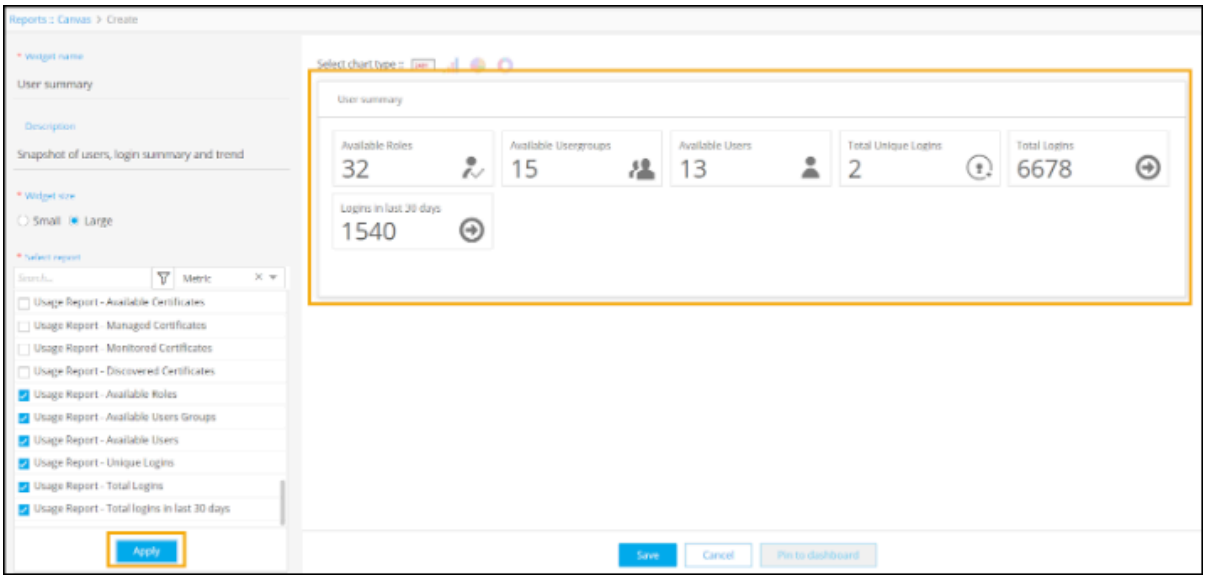
To create a **User Summary** widget that displays the information on user groups, roles, and login summary:

1. On the Reports :: Canvas page, click **Create new widget**.
2. On the **Reports::Canvas > Create** page, enter a **Widget name** (mandatory field) and **Description** (optional field).

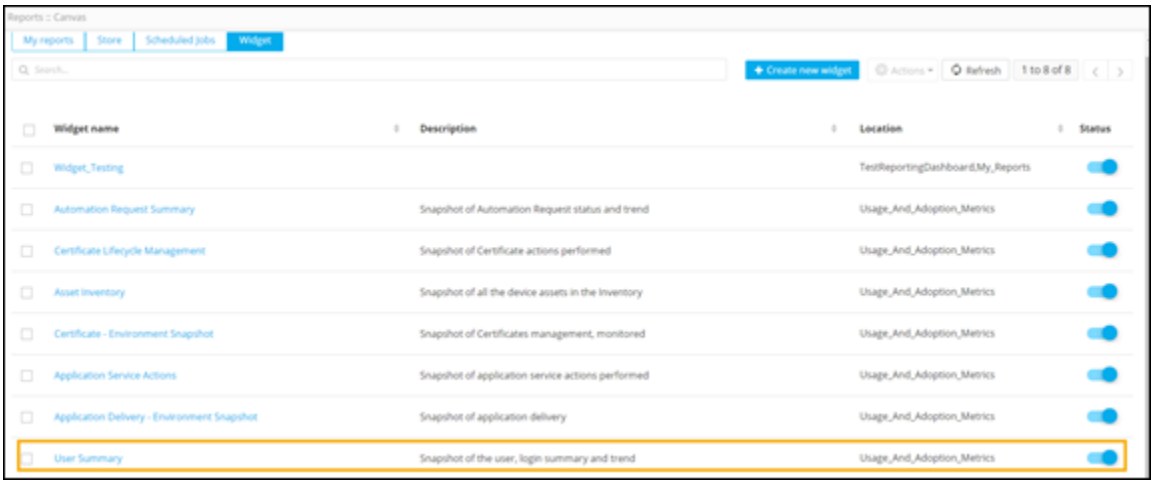


3. Select the **Widget size** as **Small** or **Large**.
4. Select the report(s) to be displayed on the widget from the list of metric reports available.

5. To see a preview of the widget, click **Apply**.
   The preview is displayed on the right side of the page.



6. Click **Save**.
7. To enable the widget, turn on the **Status** toggle.
   The **User Summary** widget is displayed on the **Reports :: Canvas**page.

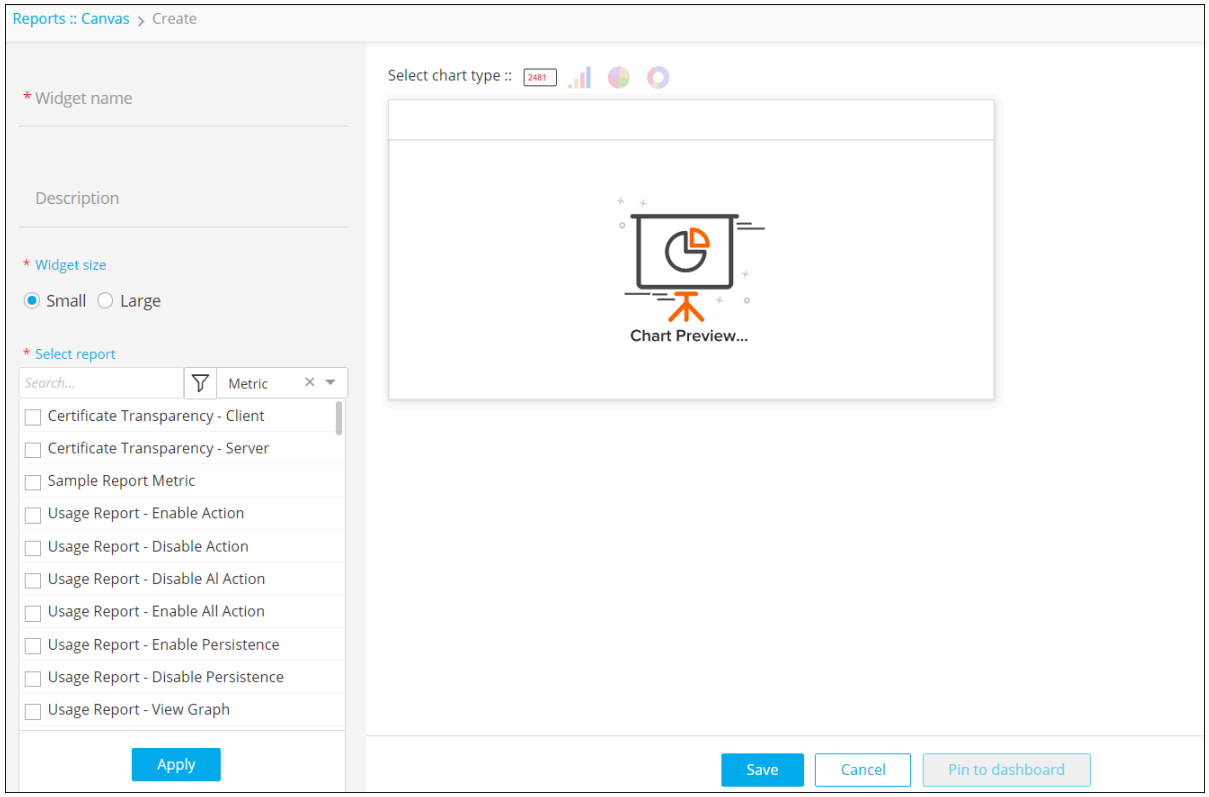


Important: Only enabled widgets are available on the **Reports :: Canvas** page.

Creating a Certificate Lifecycle Management Widget

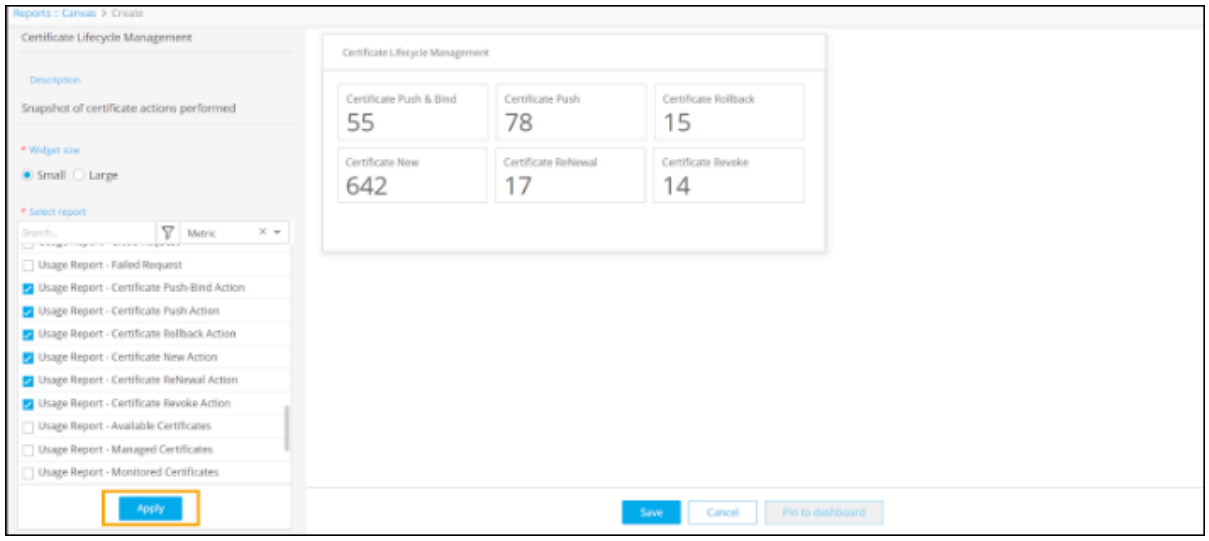
To create a **Certificate Lifecycle Management** widget that displays a snapshot of certificate actions performed:

1. On the Reports :: Canvas page, click **Create new widget**.
2. On the **Reports::Canvas > Create** page, enter a **Widget name** (mandatory field) and **Description** (optional field).

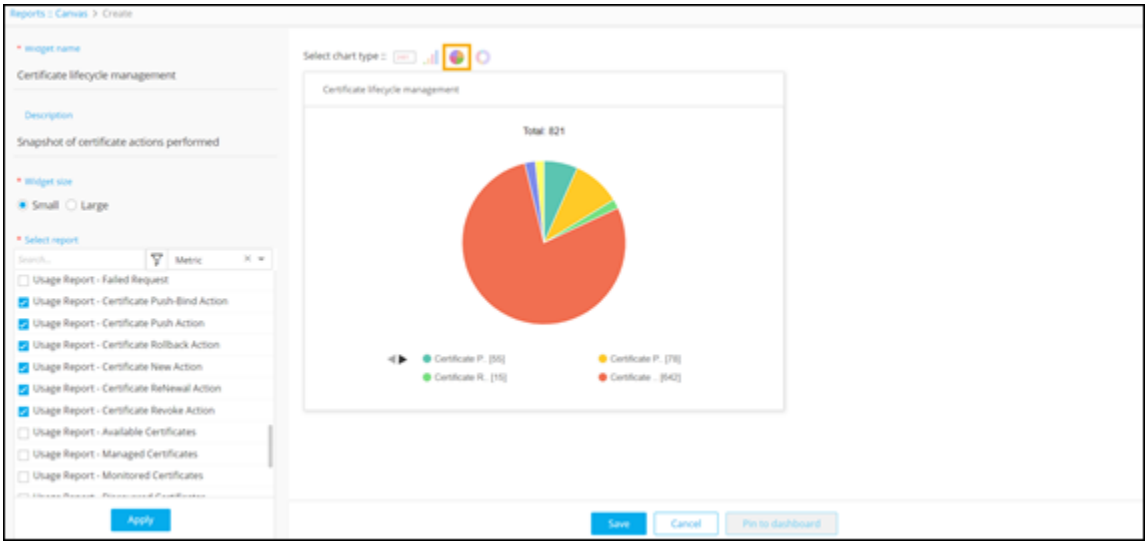


3. Select the **Widget size** as **Small** or **Large**.
4. Select the report(s) to be displayed on the widget from the list of metric reports available.
5. To see a preview of the widget, click **Apply**.

   The preview is displayed on the right side of the page.



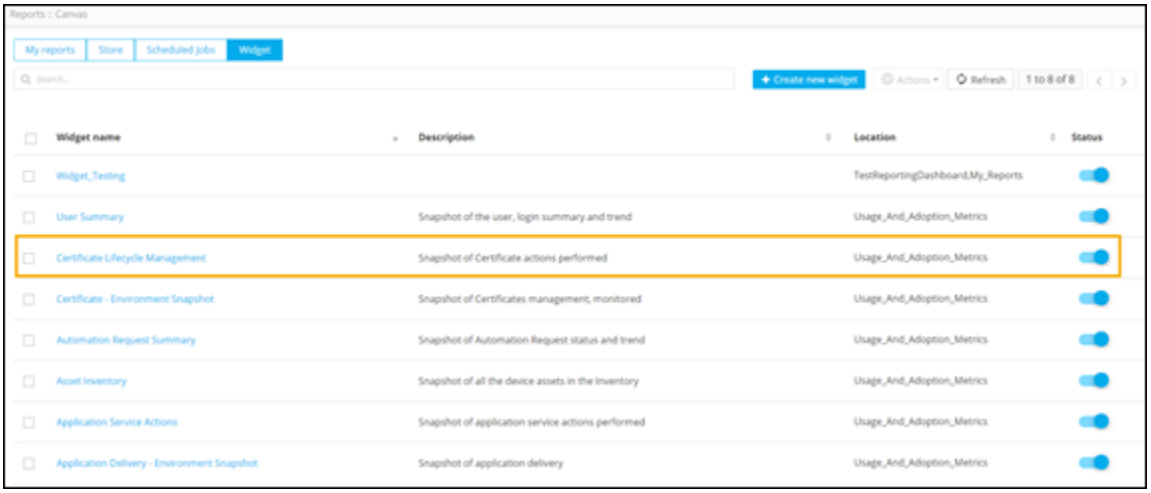
6. To view this widget as a pie chart, from the options available on top of the widget, click  .



Note: You can choose between four chart types: metric, bar, pie, and donut.

7. To save this widget, click **Save**.
8. To enable the widget, turn on the **Status** toggle.

   The **Certificate Lifecycle Management** widget is displayed on the **Reports :: Canvas** page.



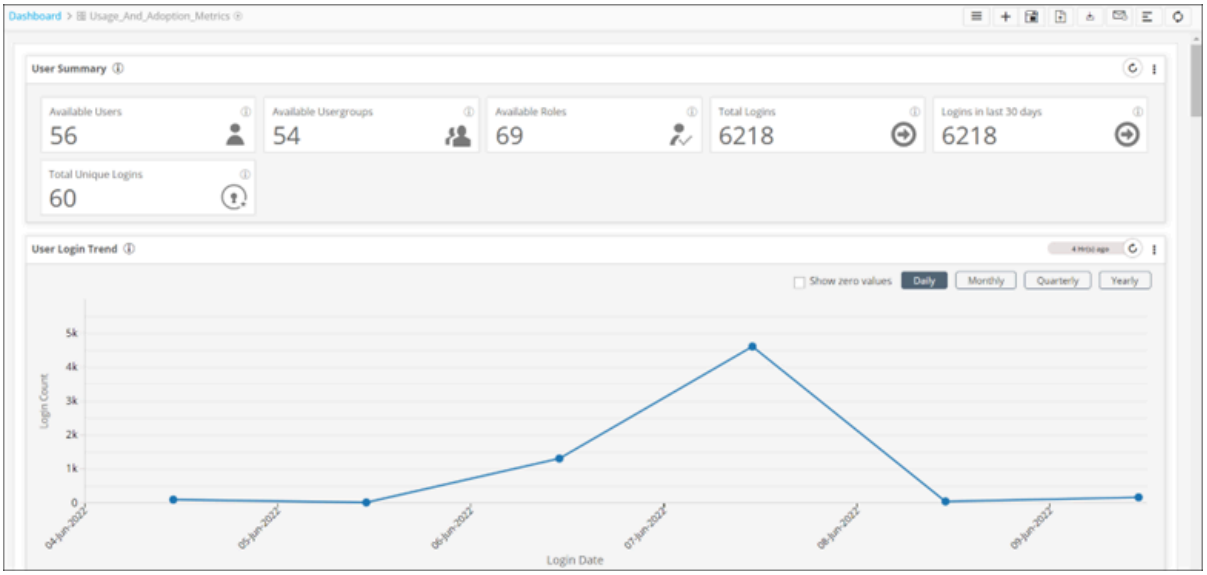
Important: Only enabled widgets are available on the **Reports :: Canvas** page.

Downloading Report Widgets

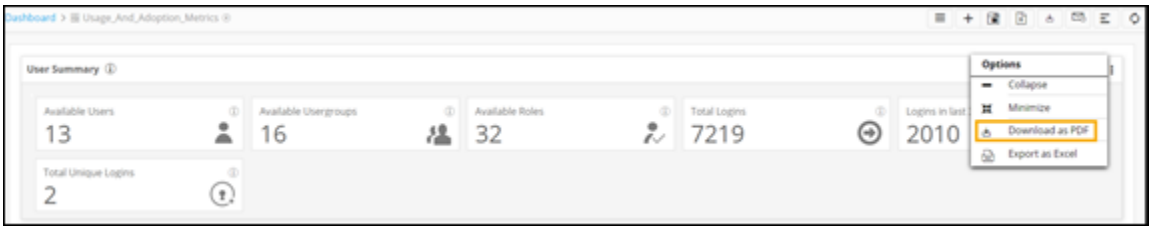
Report widgets can also be downloaded to your device as a PDF or CSV file.

To download the widget as PDF:

1. From the **Dashboard** inventory page, select the **Usage_And_Adoption_Metrics** dashboard.
   This dashboard displays all the widgets pinned to this dashboard.



2. To download a widget, from the top right corner of the widget, click ⋮.
3. From the options displayed, select **Download as PDF**.



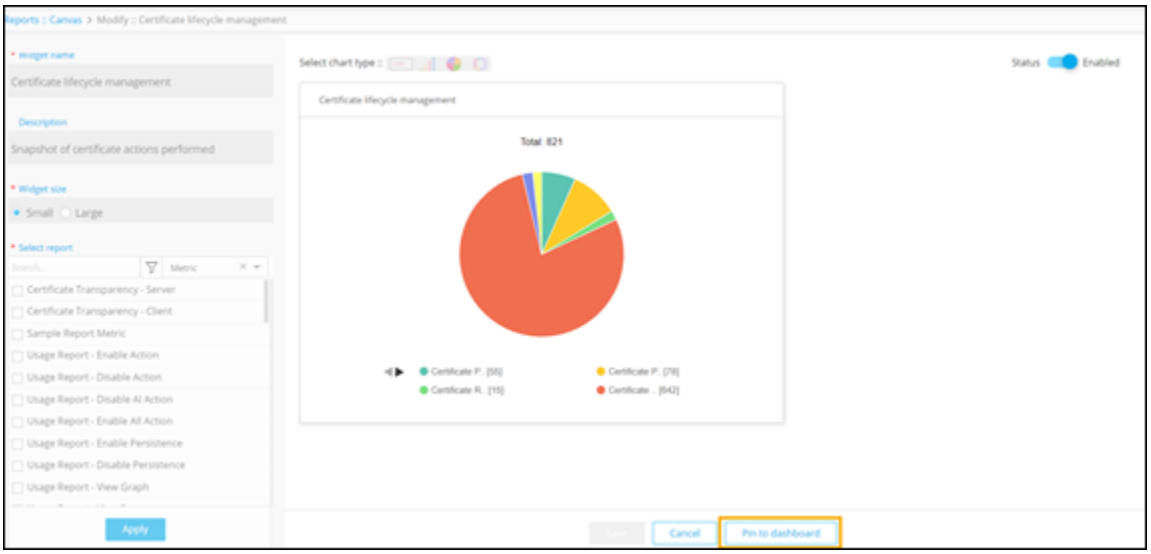
   The widget is downloaded to your machine as a PDF file.

Pinning a Widget to a Dashboard

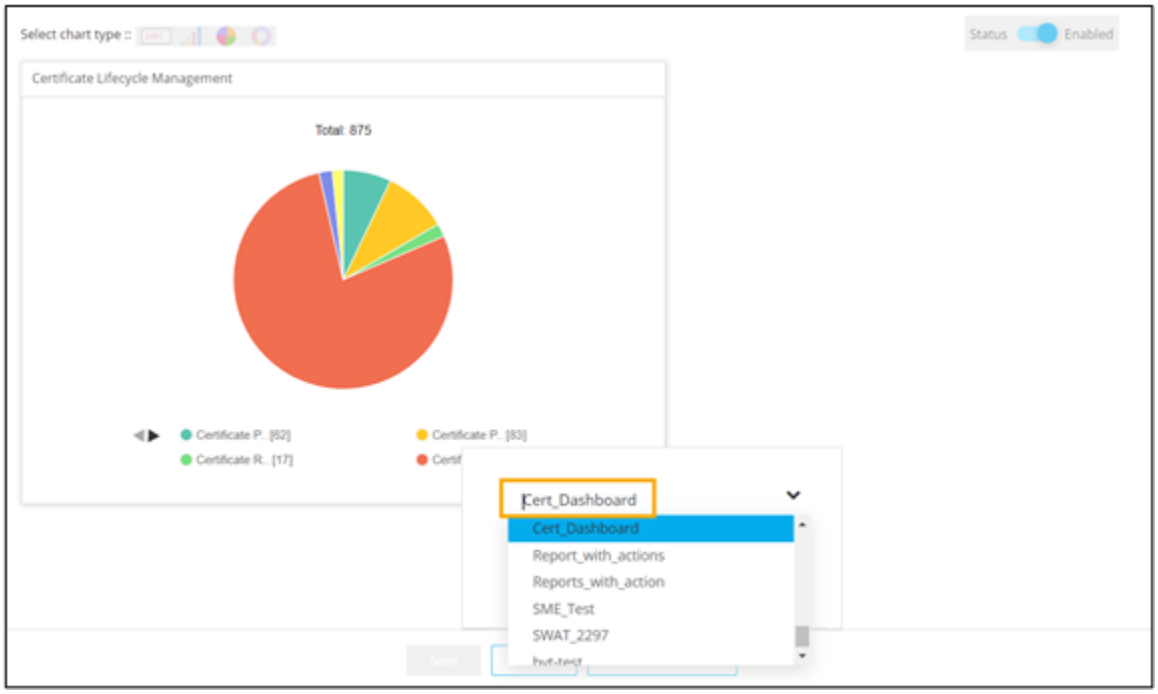
Once a widget has been created and saved, it can be pinned to a dashboard.

To pin a widget to a dashboard:

1. On the Report :: Canvas page, click on the widget to be pinned.
2. Click **Pin to dashboard**.

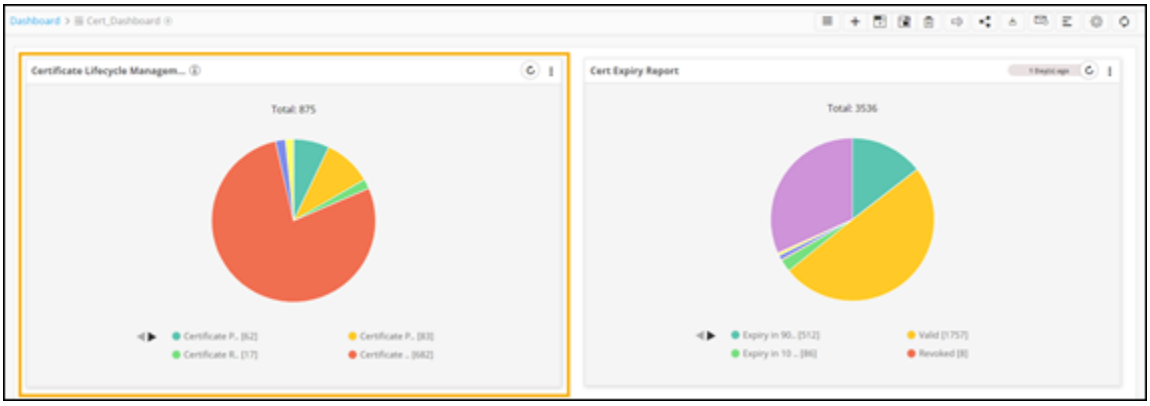


3. To pin the widget to an existing dashboard, click **Existing dashboard**.
4. Select a dashboard from the list of dashboards displayed in the dropdown.



5. To pin the widget to the selected dashboard, click **Save**.
6. On the Dashboard inventory page, click on the dashboard to which this widget was pinned.

The widget is displayed on the dashboard.



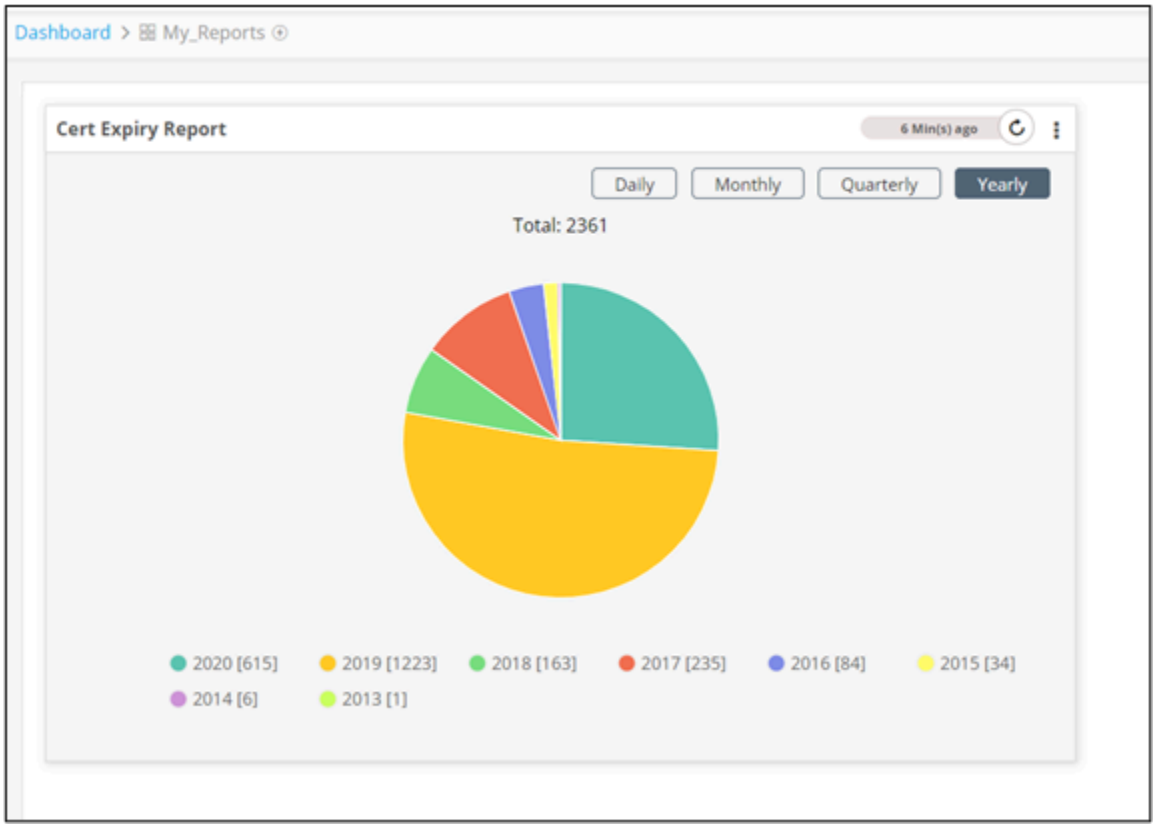
Downloading Reports

Once a report has been generated and pinned to a dashboard it can be downloaded in multiple formats (.pdf, .csv, and .xls).

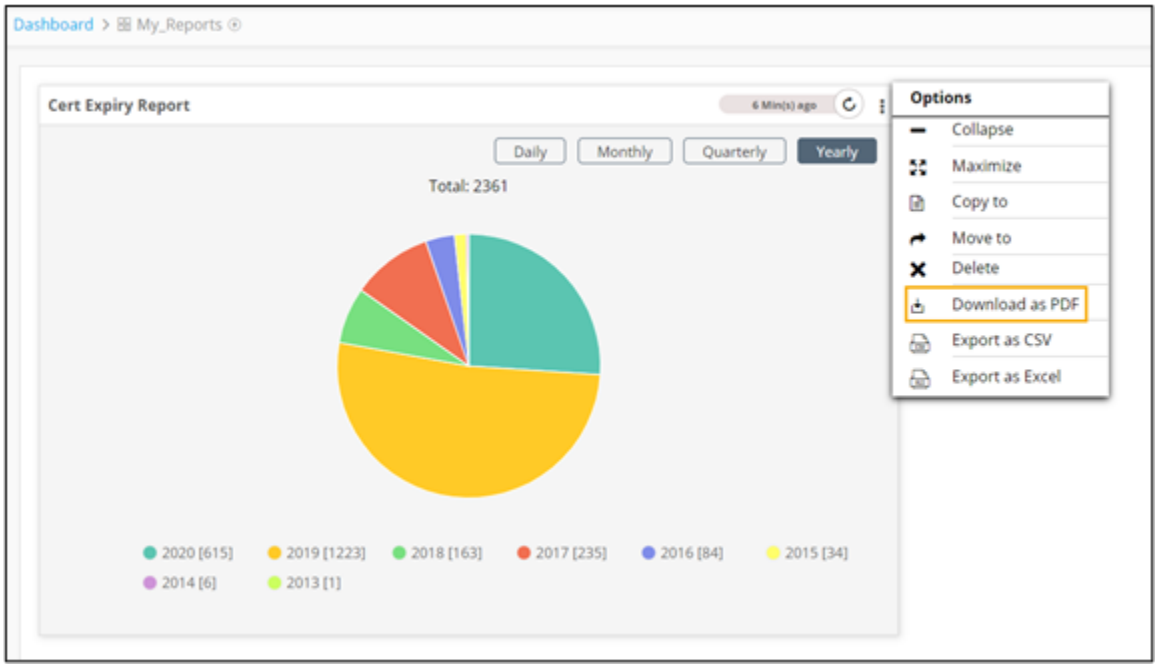
- Downloading a Report in the PDF Format
- Downloading a Report in the CSV Format
- Downloading a Report as an Excel sheet
- Downloading Drilldown Reports

Downloading a Report in the PDF Format

1. From the Dashboard inventory page, select the dashboard on which the report that you want to download has been pinned.
   The pinned report can be seen on the dashboard.



2. To download the report to your device as a PDF file, from the top right corner of the report, click ⋮.
3. From the **Options** dropdown menu, select **Download as PDF**.

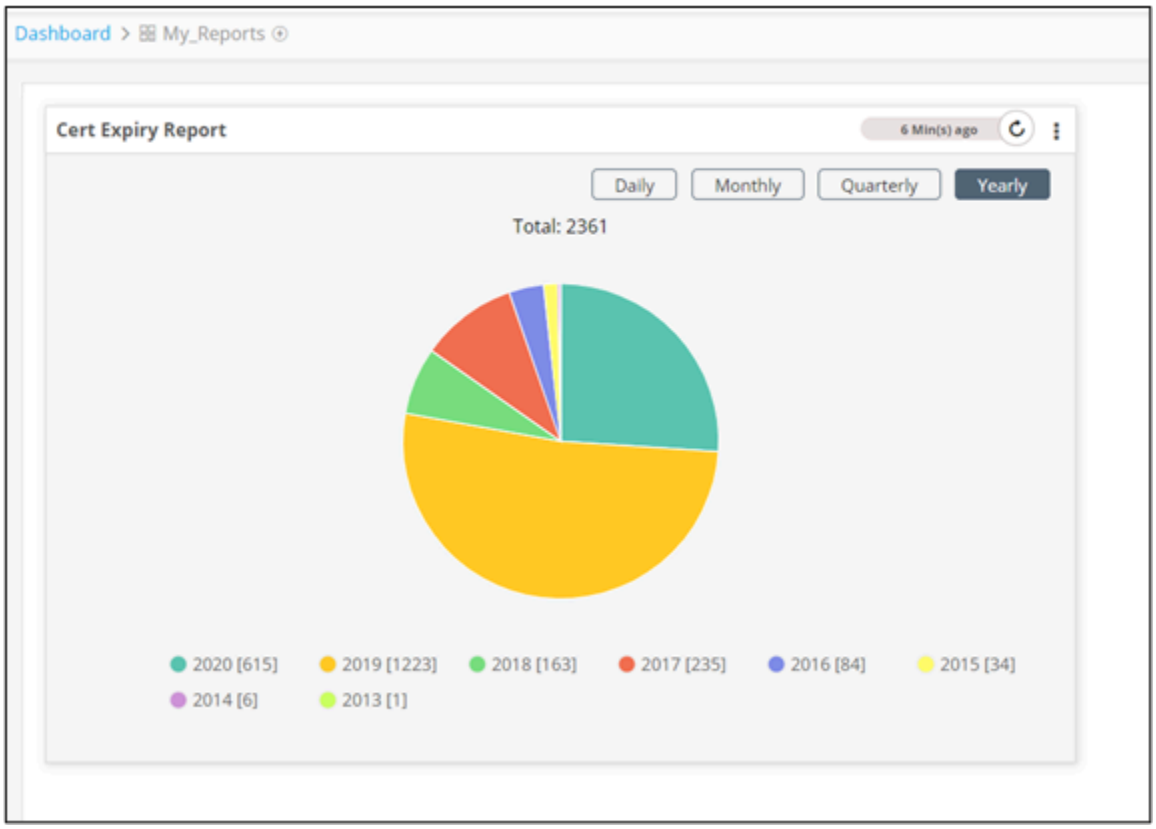


The report will be downloaded to your machine as a PDF file.

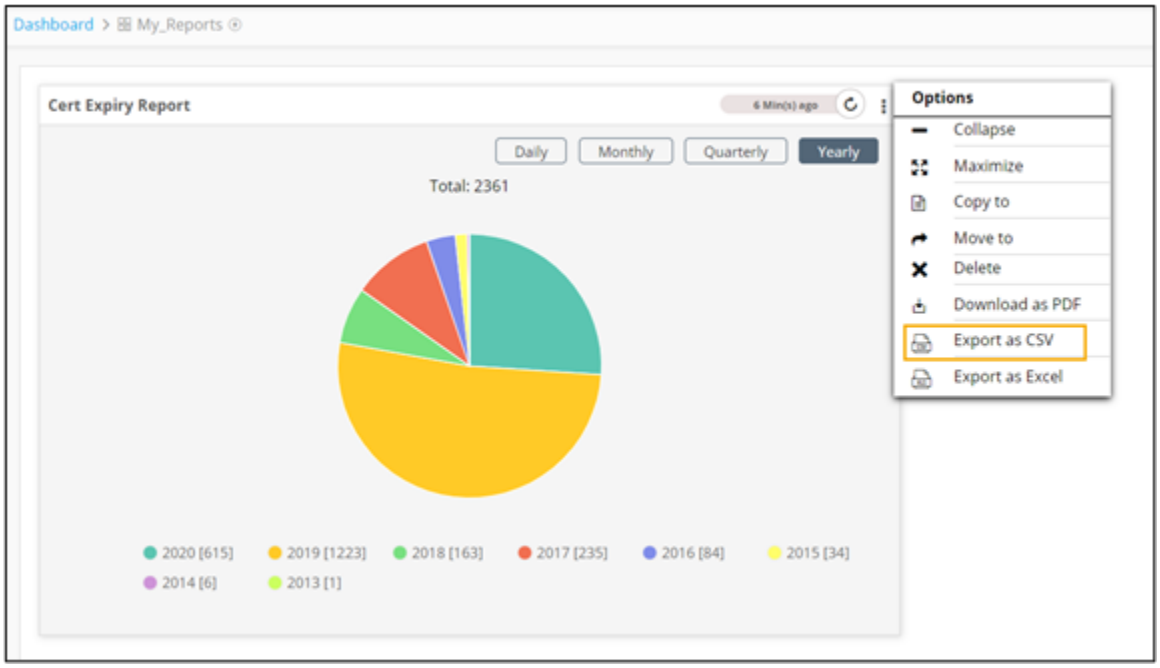
Note: In the case of **Grid** reports, the PDF download only supports up to 1000 rows.

Downloading a Report in the CSV Format

1. From the Dashboard inventory page, select the dashboard on which the report that you want to download has been pinned.
   The pinned report can be seen on the dashboard.



2. To download the report to your device as a PDF file, from the top right corner of the report, click ⋮.
3. From the **Options** dropdown menu, select **Export as CSV**.

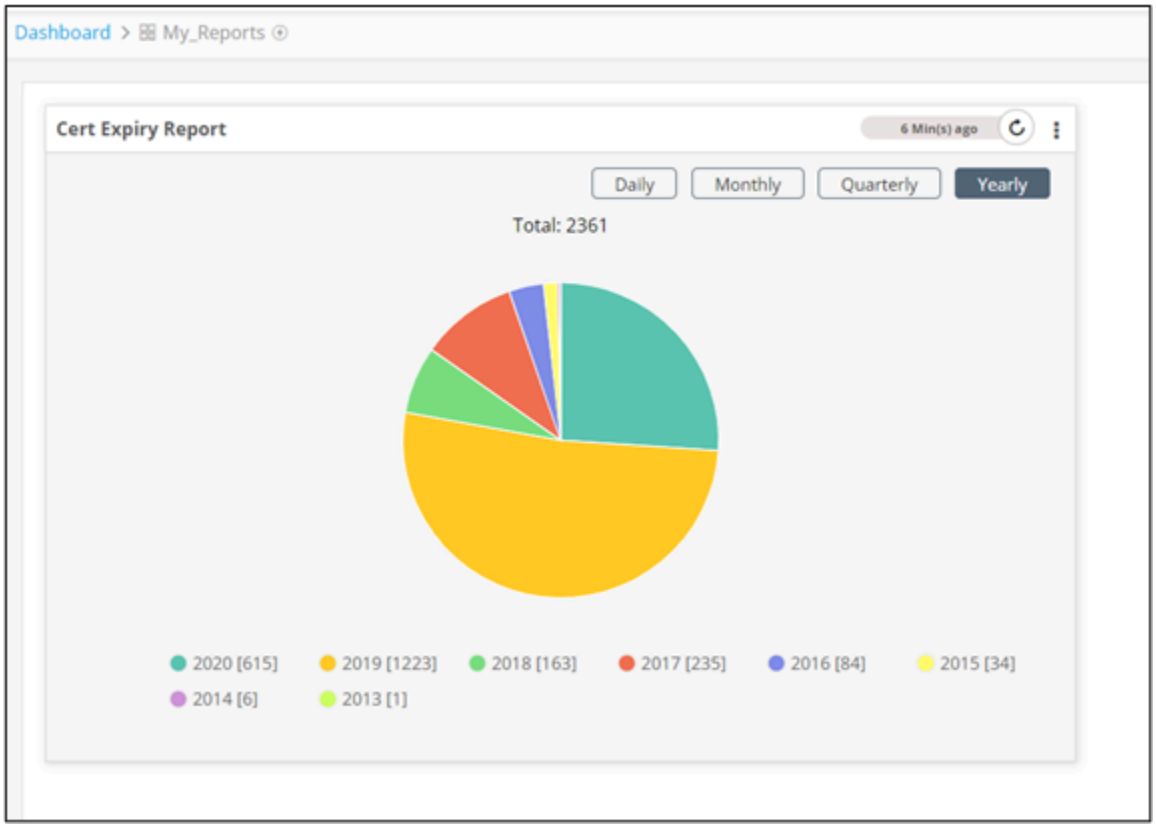


The report will be downloaded to your machine as a .csv file.

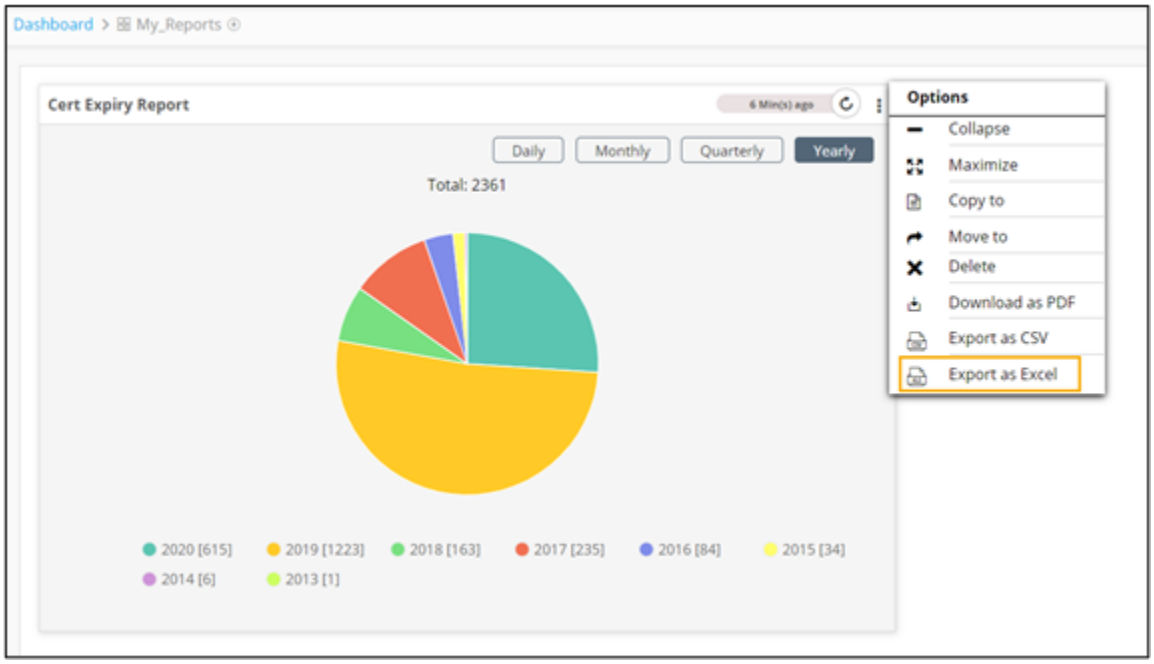
Note: In the case of **Grid** reports, the .csv file only supports up to 1,00,000 rows.

Downloading a Report as an Excel sheet

1. From the Dashboard inventory page, select the dashboard on which the report that you want to download has been pinned.
   The pinned report can be seen on the dashboard.



2. To download the report to your device as a PDF file, from the top right corner of the report, click ⋮.
3. From the **Options** dropdown menu, select **Export as Excel**.



The report will be downloaded to your machine as a .xls file.

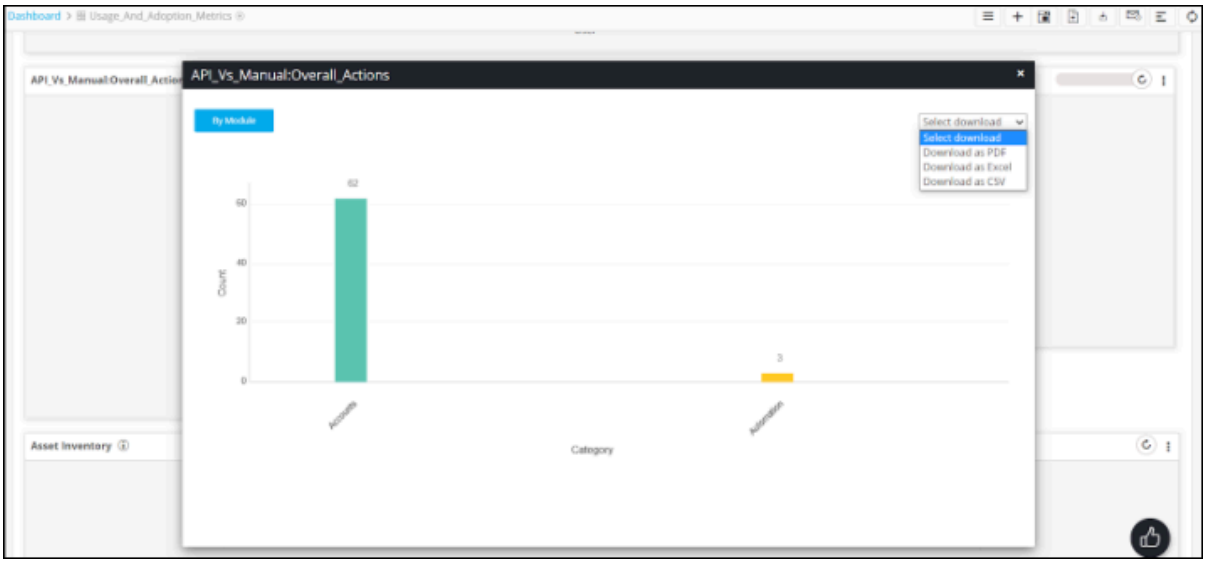
Note: In the case of **Grid** reports, the .xls file only supports up to 1,00,000 rows.

Downloading Drilldown Reports

You can download the drilldown reports from the OOB reports available on the Store page or any custom reports in the following formats:

- PDF
- Excel
- CSV.

1. Go to the Dashboard inventory page.
2. Select a report that has a drilldown report and open it.
3. In the drilldown report window, expand the **Select download** dropdown menu.



4. Select the download format from the options available.
   The report is downloaded to your machine in the format selected.

Performing Actions on Reports

- Pinning Reports
- Cloning Reports

- Sharing Reports
- Deleting Reports

Pinning Reports

You can pin reports to a dashboard from the Reports :: My Reports page. A maximum of 20 reports can be pinned to a dashboard. Pinning a report to the dashboard allows you to visualize different reports in the same place.

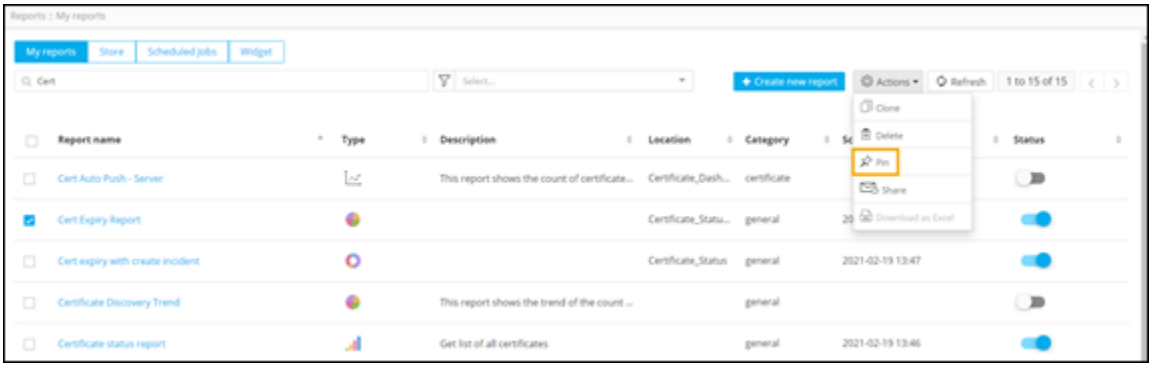
Note: Only reports that are enabled are visible on the dashboard to which they are pinned.

To pin a report to dashboard:

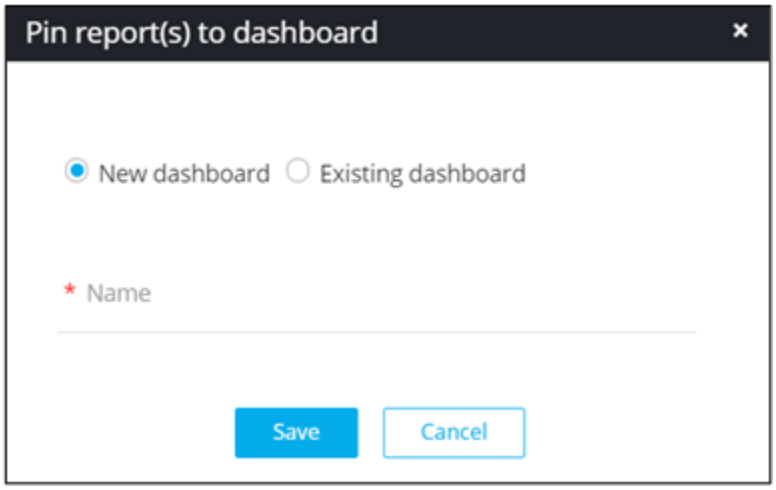
1. On the Reports :: My Reports page, select the report to be pinned.

   Note: Ensure that the selected report is enabled. You can enable a report by turning on the toggle under the **Status** column.

2. From the command bar on the top right, click **Actions**.
3. From the list of available actions, select **Pin**.



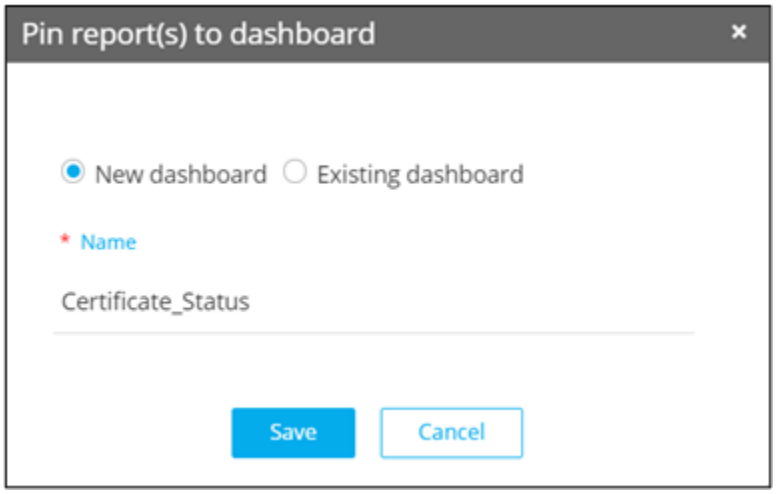
4. In the **Pin report(s) to dashboard** window that is displayed, select if the report is to be pinned to a new or existing dashboard.



- Pinning Reports to a New Dashboard
- Pinning Reports to an Existing dashboard

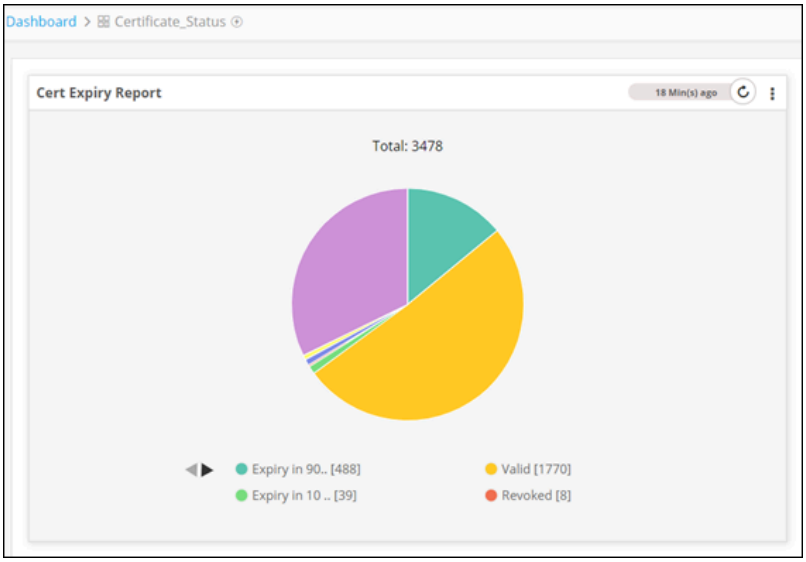
Pinning Reports to a New Dashboard

1. In the **Pin report(s) to dashboard** window, enter a **Name** for the dashboard.



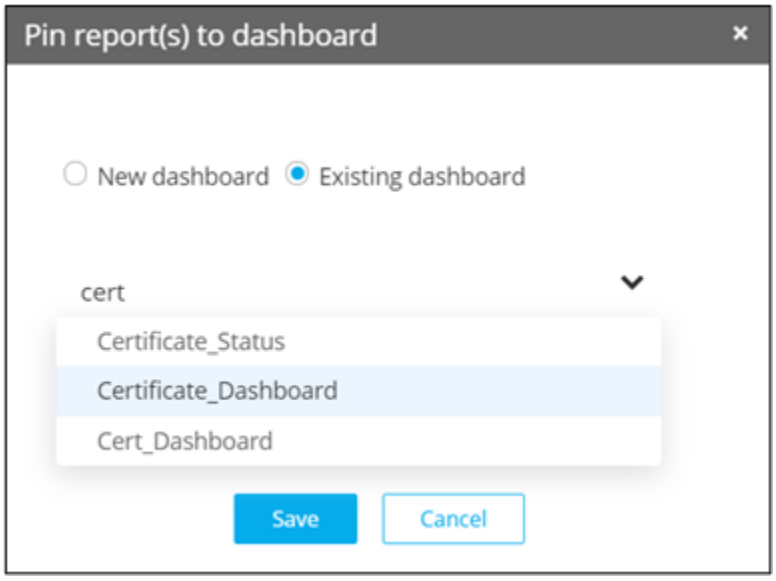
2. To pin the report to the new dashboard, click **Save**.
   The new dashboard is listed on the Dashboard Inventory page.
3. To view the pinned report, click on the dashboard.

The report is displayed on the dashboard.



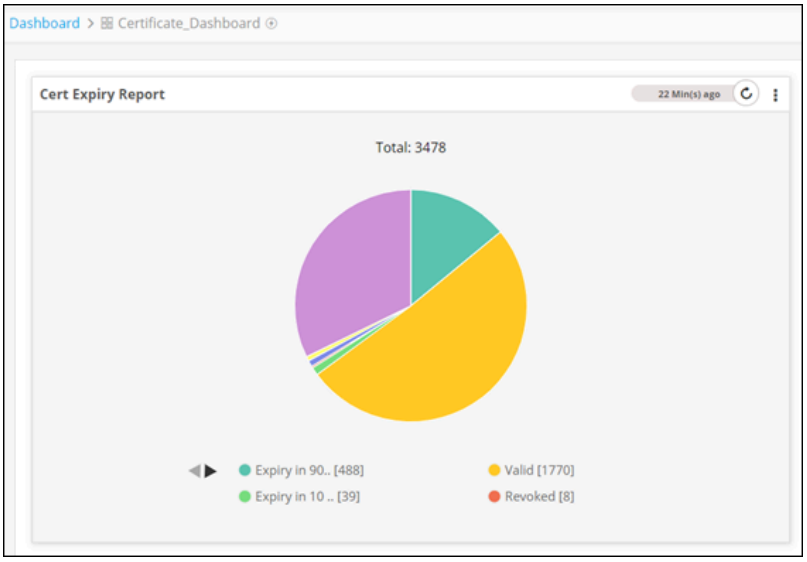
Pinning Reports to an Existing dashboard

1. In the **Pin report(s) to dashboard** window, select the dashboard from the options available in the dropdown.



2. To pin the report to the selected dashboard, click **Save**.

The report is displayed on the selected dashboard.

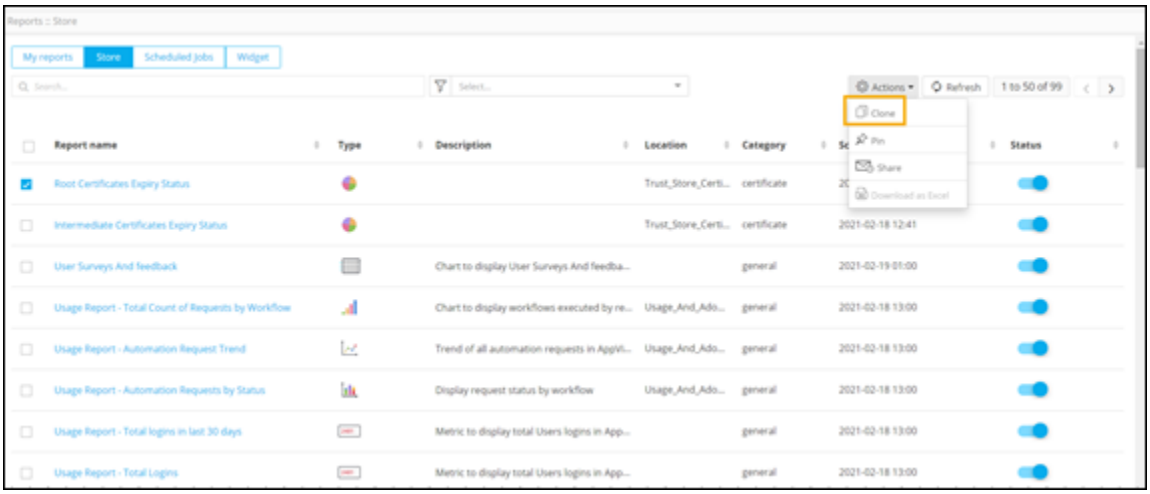


Cloning Reports

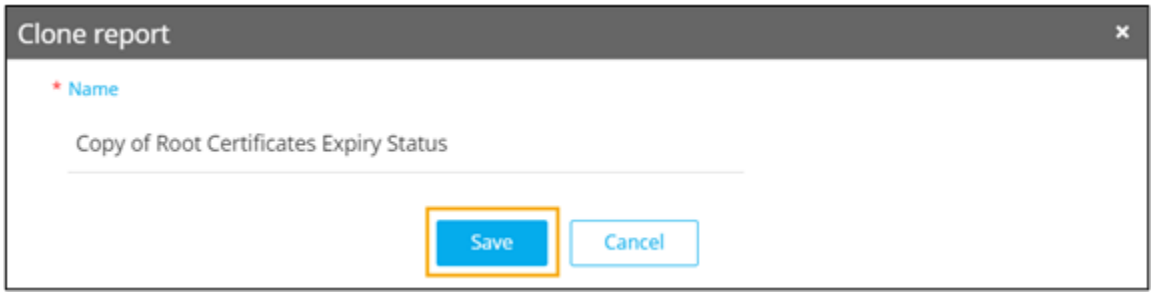
AppViewX's report builder allows you to clone a report. You can clone a report to make modifications, display additional data, and create additional levels of drilldown if not available in the previous report. Instead of creating a second report from scratch, you can clone an existing report and make the necessary changes.

To clone a report:

1. From the Reports :: Store page, select the report to be cloned.
2. From the command bar, click **Actions**.
3. From the list of available actions, select **Clone**.



4. In the **Clone report** pop-up window, change the name of the report (if required) and click **Save**.



The cloned report is added to the Reports :: My reports page.

Sharing Reports

Once a report is generated, it can be emailed either as inline content or as a PDF attachment to other users or user groups.

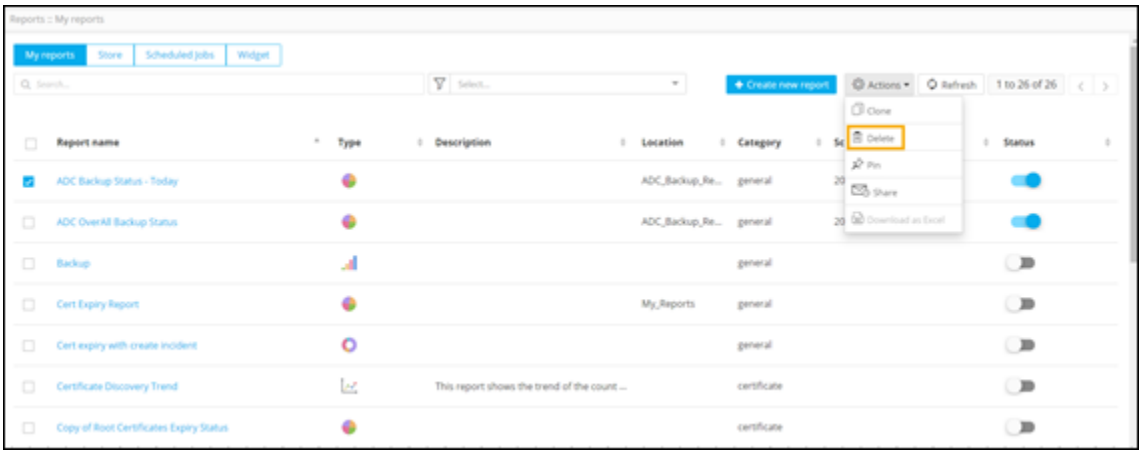
Note: For more information on sharing reports, click here.

Deleting Reports

AppViewX's report builder also allows you to delete reports.

To delete a report:

1. On the Reports :: My Reports page, select the report to be deleted.
2. From the command bar, click **Actions**.
3. From the list of available actions, select **Delete**.



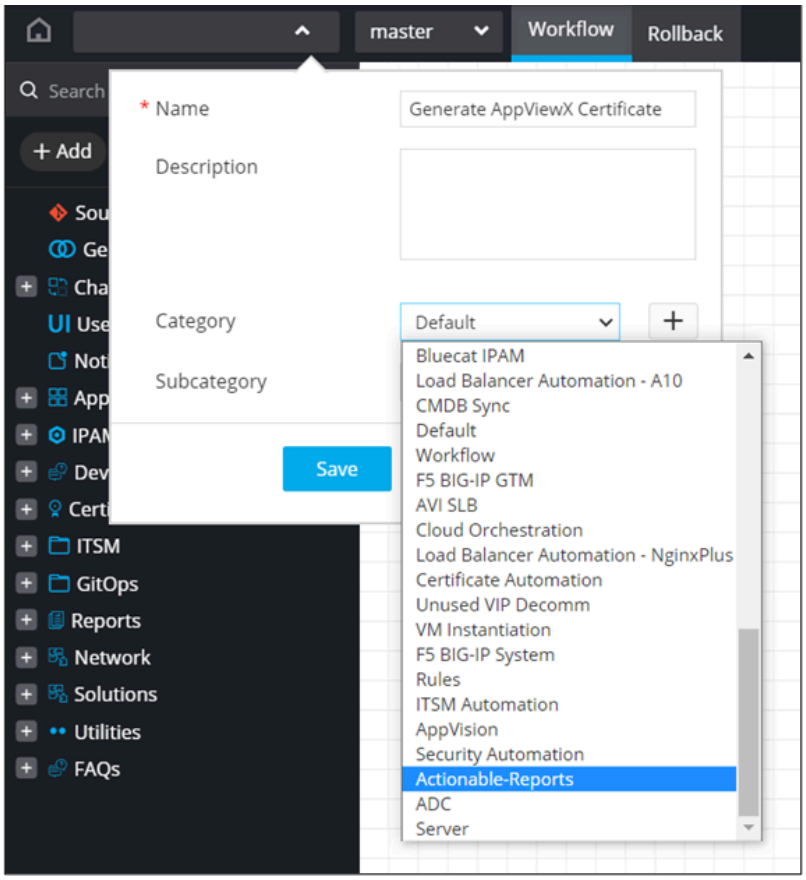
4. To delete the selected report, click **Yes** in the **Confirm delete** pop-up window.

BYOR with Actionable Workflow

You can build customized reports, pin them to the dashboard, and assign one or more closed loop workflows for quick actions. These workflows can be triggered at specific time intervals to gather data and integrate it into the reports. Assigning a workflow to your reports aids in elimination of redundant tasks, reduces processing time, improves efficiency, and gives greater visibility.

To assign an actionable workflow to your report:

1. Go to the **Workflow** page in the **Automation** module.
2. To create a new workflow, click **Create New**.
3. Enter or select the field information.

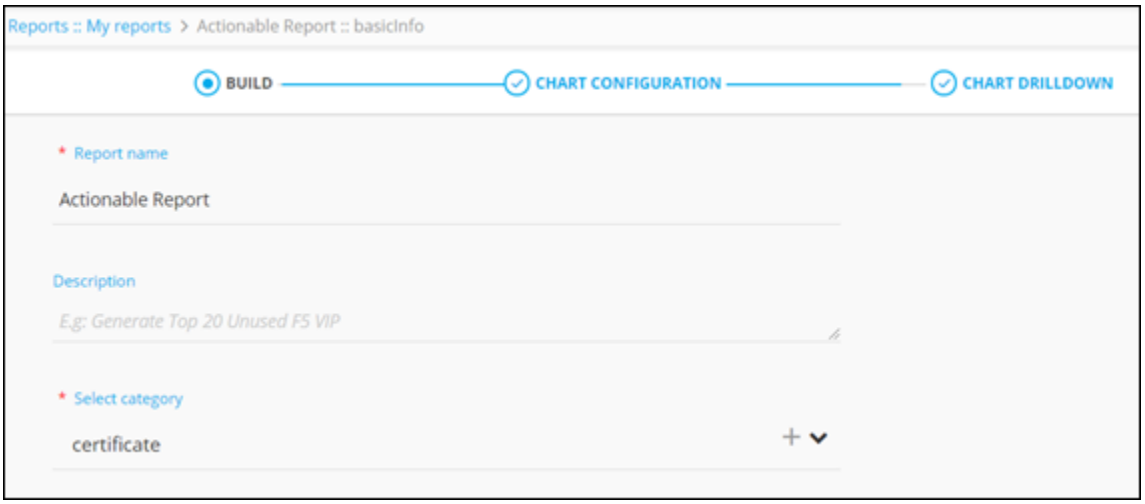


The following table describes the various fields in this section:

Field	Description
***Name**	Enter a valid name for the workflow. For example: **Generate AppViewX Certificate.**
Description	Enter a description for the workflow.
Category	Select the category as **Actionable-Reports** from the dropdown list.
Subcategory	The subcategory is set to **default**.

Note: The asterisk (*) symbol indicates mandatory fields.

4. Drag and drop the relevant workflow tasks and enable the workflow.
5. Go to the Reports :: My Reports page and click **Create new report**.
6. Under the **BUILD** section, enter or select the field information.

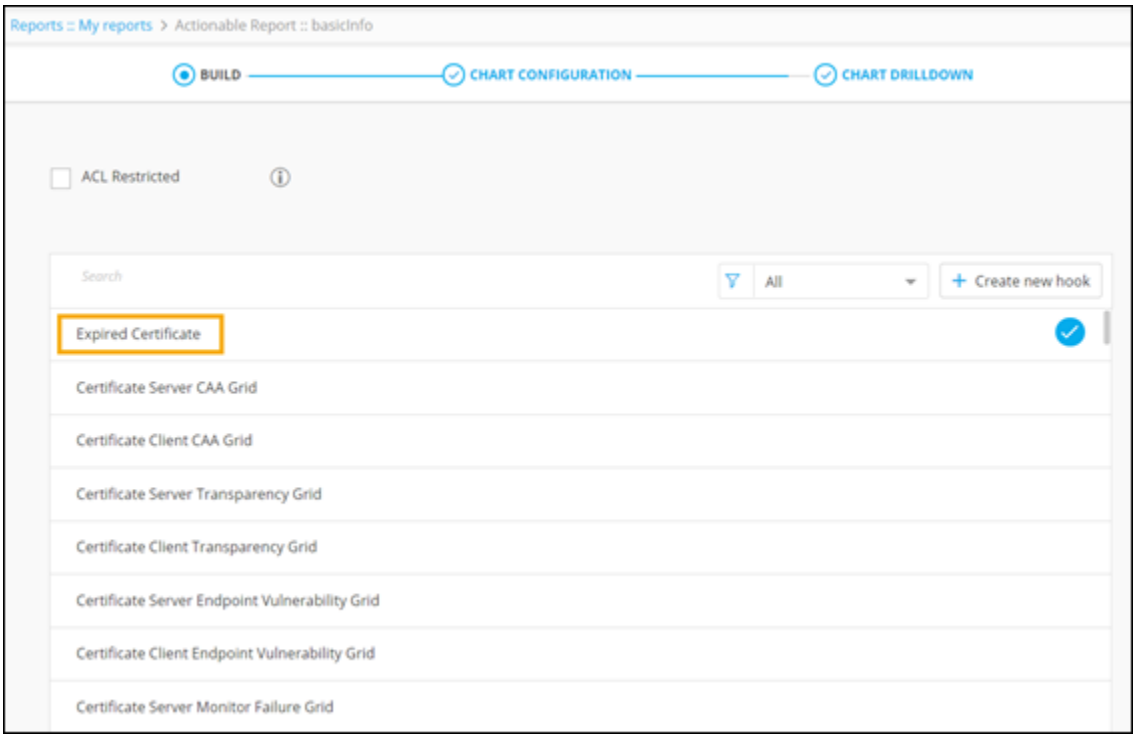


The following table describes the fields under this section:

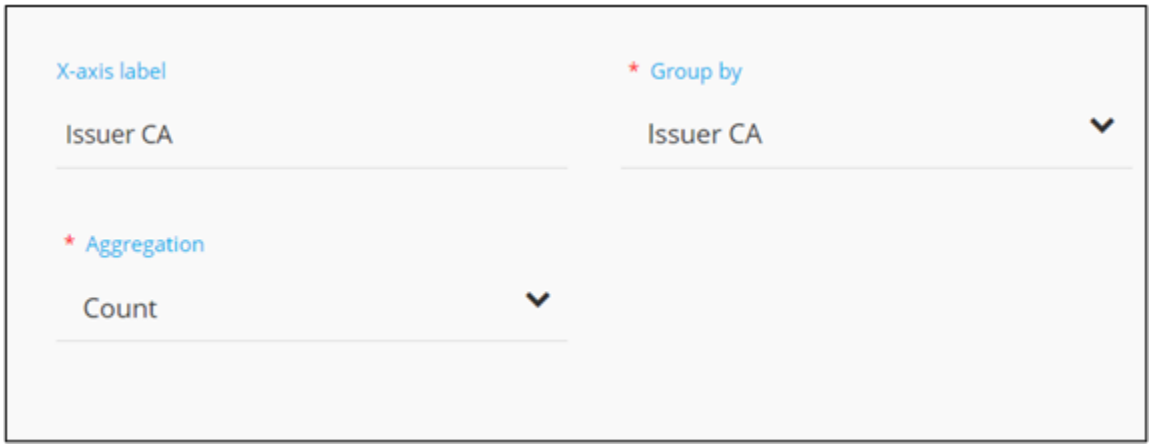
Field	Description
***Report name**	Enter a valid report name. For example: **Actionable Report.**
Description	Enter a description of the report.
***Select category**	Select the category as **certificate** from the dropdown.

Note: The asterisk (*) symbol indicates mandatory fields.

7. Select the hook from the list and click **Next**.



8. Under the **CHART CONFIGURATION** section, select the chart type as **BAR**.
9. Select the field information for creating the chart.



This table describes the field information in this section:

Field	Description
X-axis label	Enter the criteria for the X-axis label. For example: **Issuer CA.**
***Group by**	Select a value from the dropdown list on the basis of which report data will be grouped. For example: **Issuer CA.**

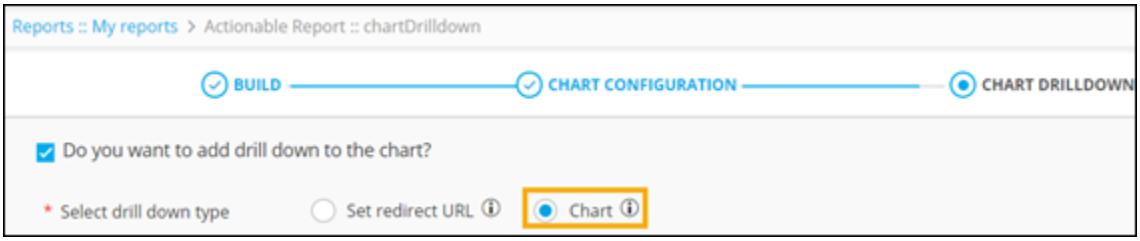
Field	Description
***Aggregation**	Select the calculation to be done on the report data for the dropdown. The following options are available: • **Average**: Calculates the average value of a given set of data. • **Sum**: Calculates the sum of all values in a given set of data. • **Count**: Calculates the total number of items in a given numeric field. • **Maximum**: Displays the maximum value in a given set of data. • **Minimum**: Displays the minimum value in a given set of data.

Note: The asterisk (*) symbol indicates mandatory fields.

10. Click **Save**.

    A preview of the chart is generated on the right side of the screen.

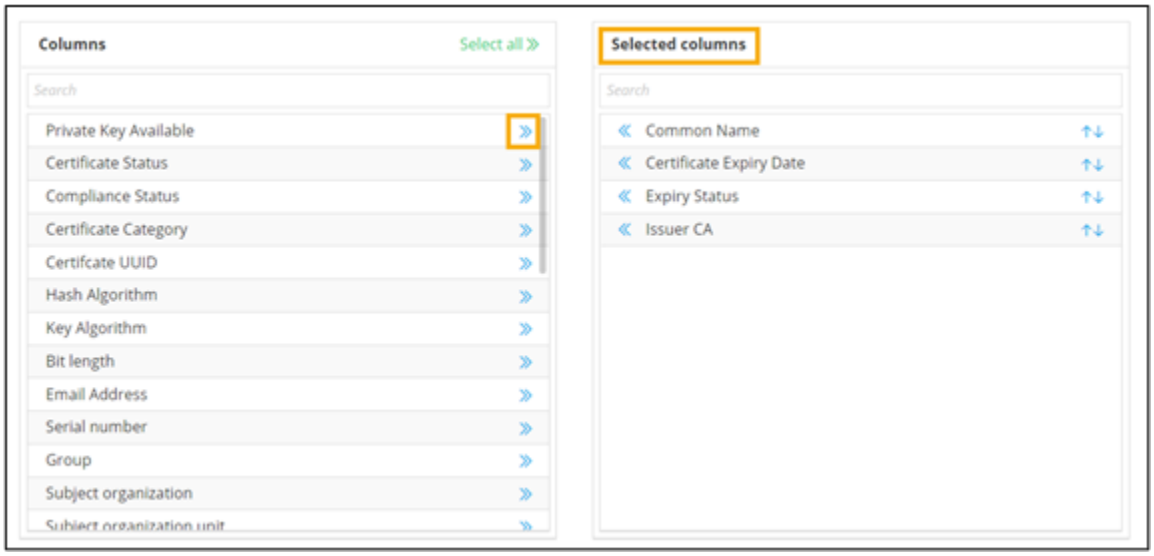
11. To add **Chart Drilldown**, click **Next**.
12. Select drilldown type as **Chart**.



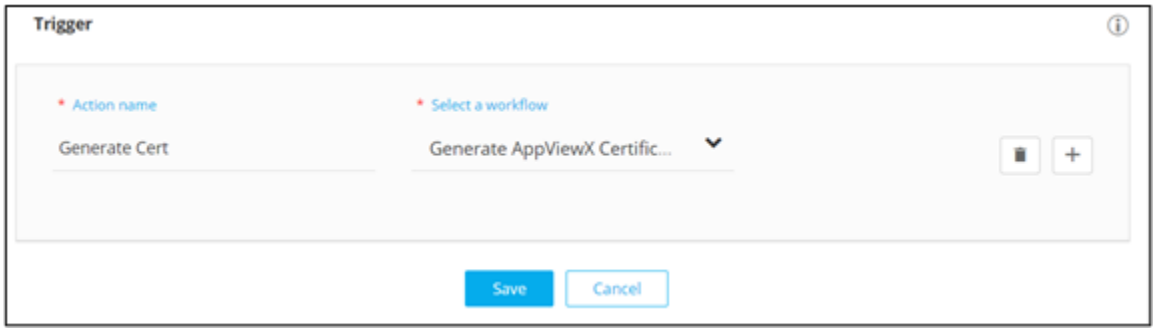
13. Select the chart type as **GRID** and enter the **Chart title** as **Generate Certificate**.

14. To configure the column headers to be displayed within the grid, click  .

    Selected columns are displayed on the right.



15. Enter or select the field information to associate a workflow with the report.



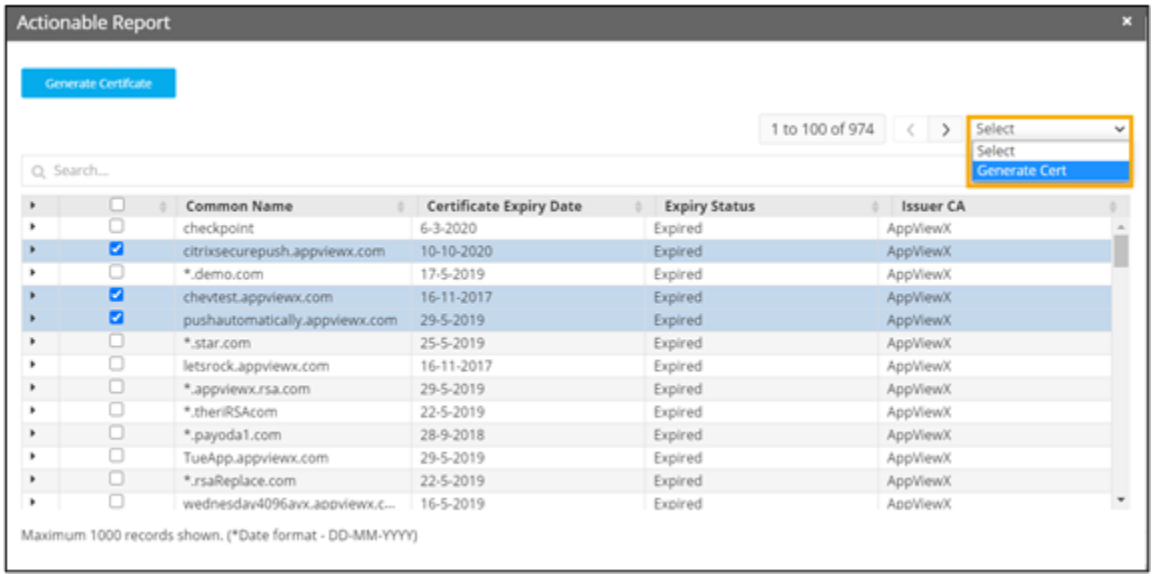
This table describes the field information in this section:

Field	Description
***Action name**	Enter a valid action name. For example: **Generate Cert**.

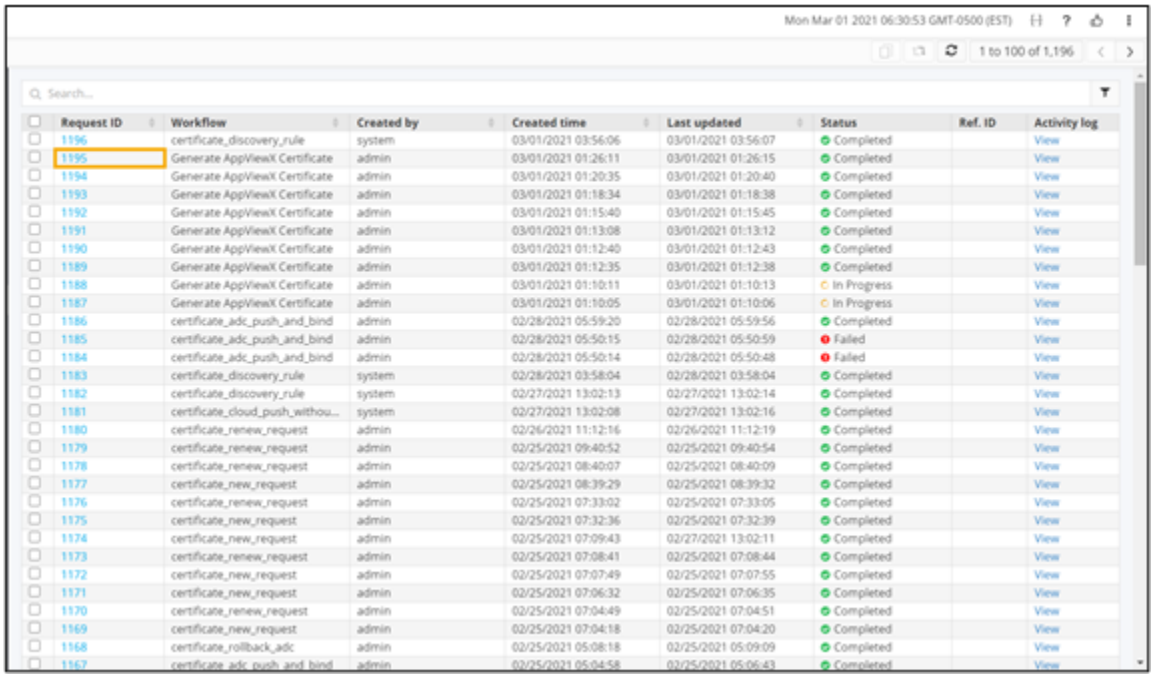
Field	Description
***Select a workflow**	Select the workflow that was created (Generate AppViewX Certificate) from the dropdown menu.

Note: The asterisk (*) symbol indicates mandatory fields.

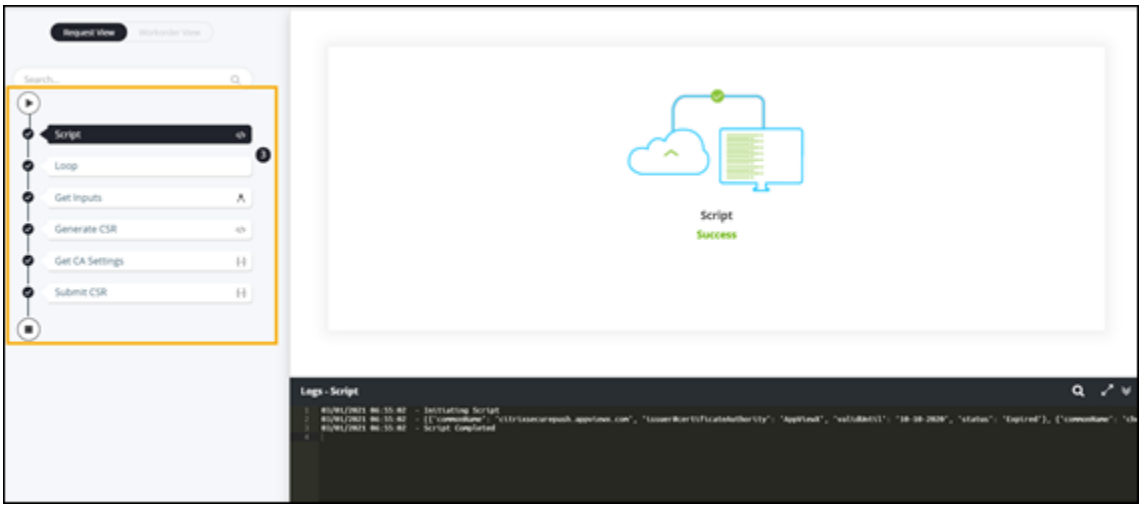
16. To enable the workflow, click **Save & Enable**.
17. To display the chart drilldown, click any of the bars in the graph.
18. Select the **Common Name** for the actionable workflow.
19. To trigger the workflow, select the workflow from the dropdown menu.



20. On the **Request :: All** page, select the workflow **Request ID**.



A stage-wise view of the workflow is displayed.



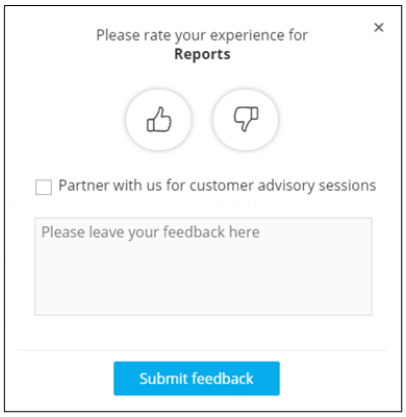
21. To view the payload that was passed for the actionable workflow, click **Script**.
22. To see successful completion of the workflow, click **Submit CSR**.

User Feedback and Survey Reports

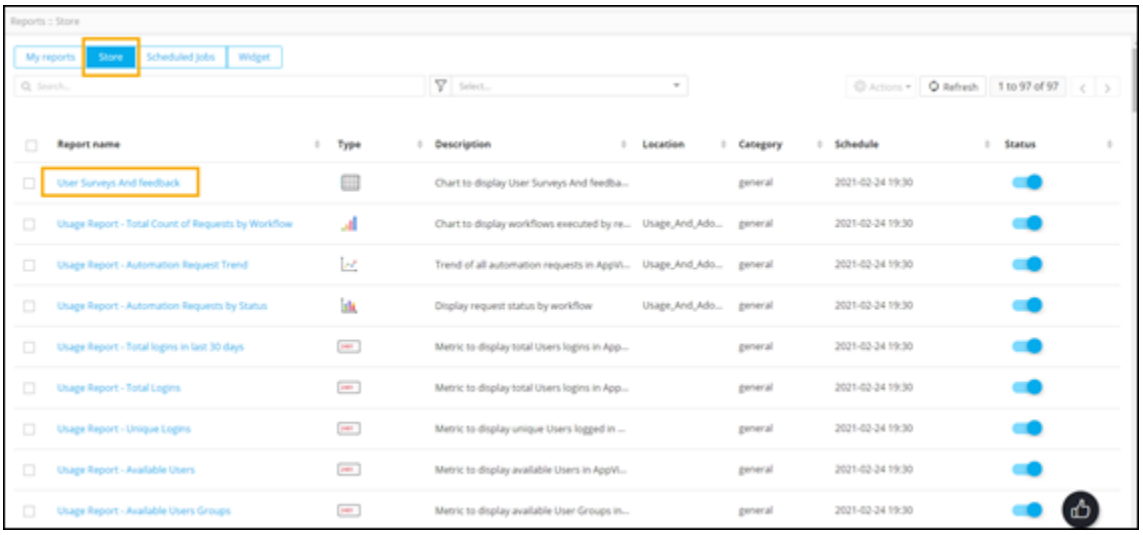
AppViewX hosts a user feedback feature on its report building platform, where users can rate their experience with the report builder and also submit a descriptive comment on the tool. This feedback can then be used to create reports to track customer experience.

Submitting a Feedback

1. Log into AppViewX.
2. From the top right corner of the screen, click **(Profile)** icon.
3. From the menu displayed, click **Feedback**.
4. Enter your feedback comments, and then click **Submit feedback**.



The **User Surveys and feedback** report on the **Store** page gives detailed information on user feedback.

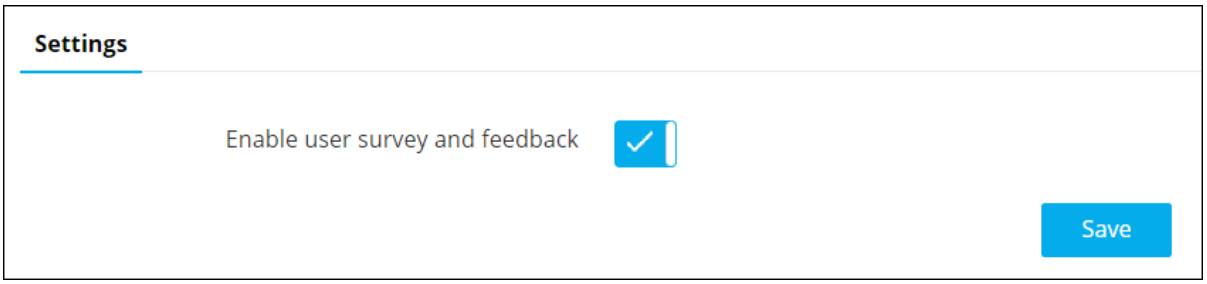


Enabling/Disabling the Feedback Option

To enable or disable the feedback option:

New Menu	Old Menu
1. Navigate to the **Platform** module. 2. From the left menu, under **SYSTEM ADMINISTRATION**, click **User Survey**. The **Settings :: Reports** page is displayed.	1. From the main menu, select **Settings**. 2. On the **Settings** page, under **General**, select **Reports**. The **Settings :: Reports** page is displayed.
Note: For more information on how to switch between menus, click here.	

1. To enable feedback, on the **Settings :: Reports** page, turn on the toggle.



2. To disable feedback, turn off the toggle.
3. Click **Save**.

Best Practices

Listed here are some best practices that will help you build visually engaging, insightful and effective reports:

- **Identifying target audience and their requirements**

  Before you even start building reports, it is important to know who the target audience or end user is. Meeting with them to know about their specific requirements is crucial to build comprehensive reports that display complete and accurate information.

- **Choosing the right chart**

  The right chart or graph can help you display your data most efficiently and effectively. Pie charts can be used for fewer data points, while bar graphs can be used to show comparison among categories.

Line charts, on the other hand, are most useful for showing changes over a period of time. Choosing the wrong chart can create confusion and the data might even be interpreted incorrectly. The Reports module offers seven different chart types to choose from.

- **Highlighting key areas**

  Using colors to highlight key areas is a powerful way to guide the end users to important data. However, the choice of colors is crucial and overuse of colors in your reports may be distracting. The **Reports** module offers color code mapping for pie charts, donut charts, bar charts, and stacked bar charts.

- **Grouping related metrics together on Dashboard**

  It is important to group related metrics together to help the end user quickly make connections between the data on a dashboard. The **Reports** module has a provision for moving widgets around on the dashboard so that you can keep related widgets/reports in one place.

- **Adding interactive elements**

  Using the **Chart Drilldown** feature in the **Reports** module is a great way to ensure that your reports are interactive. Displaying high level data first and allowing the user to drill down for further details keeps the user engaged.

- **Keeping it simple**

  Last, but not least, keep your reports simple. Do not clutter it with too much information and avoid using too many colors. Prioritize readability by making them visually appealing and easy to understand.

Troubleshooting

Following are the common issues you may face when working with the **Reports** module:

Issue	Cause	Solution
There is something wrong with my Scheduled Job.	**Avx_platform_report_generator** plugin is disabled.	Check plugin status and enable it.
Report pinned to dashboard shows error message.	Report is not enabled.	Enable the report on My Reports page.
I am not able to edit a report in the **Store**.	Prebuilt reports in the **Store** cannot be edited .	Clone the report and customize it as per your need.

Issue	Cause	Solution
Schedule time elapsed error while defining the interval.	Time entered is the same as the current time.	Enter a time which is 1-2 minutes later than the current time.

In case of any other issues with the **Reports** module, users can access the following logs for further investigation:

- avx-subsystems log
- avx-commons log.