appviewX

Platform User Guide

Version: 2021.1.0

Copyright AppViewX, Inc.

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
1.0	Initial Release of AppViewX_v2021.1.0 Platform.	September 2021

About the Documentation

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.

Audience

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

Text Conventions

The following text conventions are used in this document:

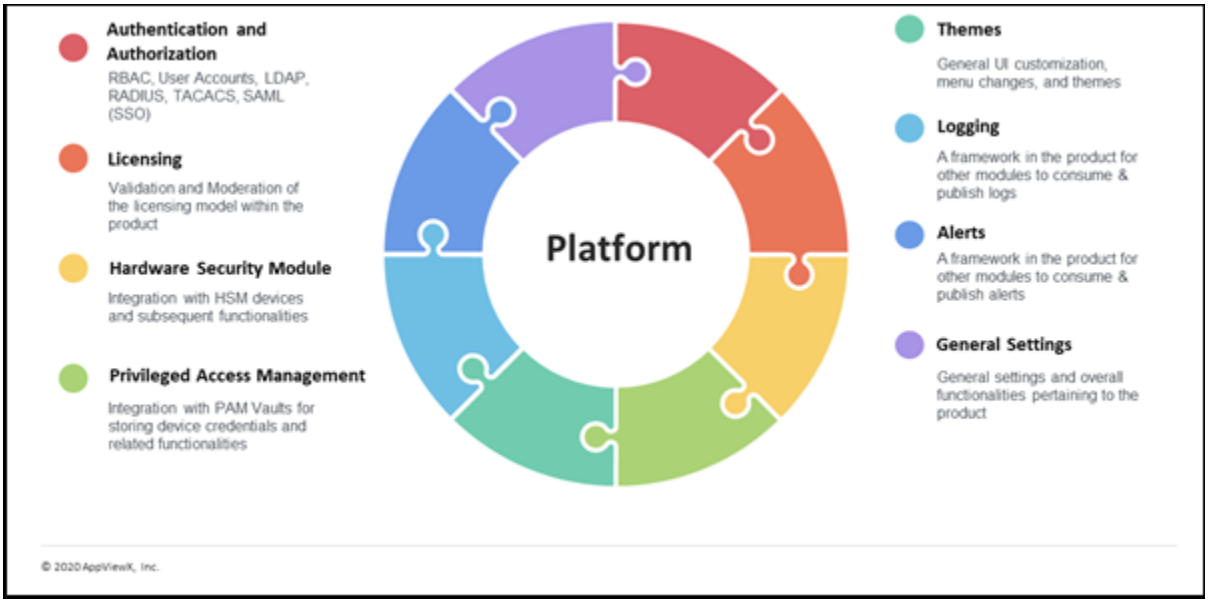
Convention	Description
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in the text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`codeblock`	Indicates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

Chapter 1: 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:



Chapter 2: Configuring Authentication Settings

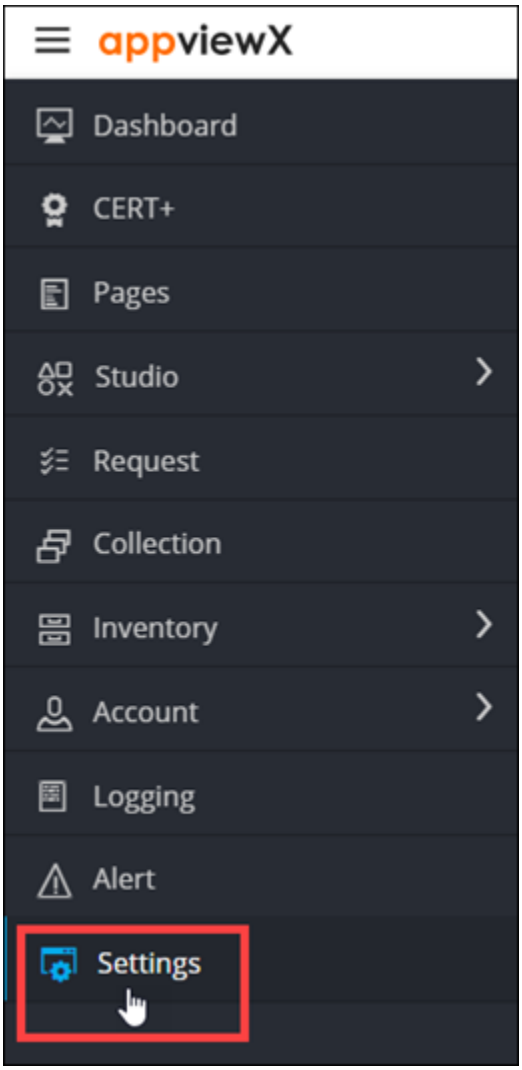
Configuring the LDAP Authentication

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.

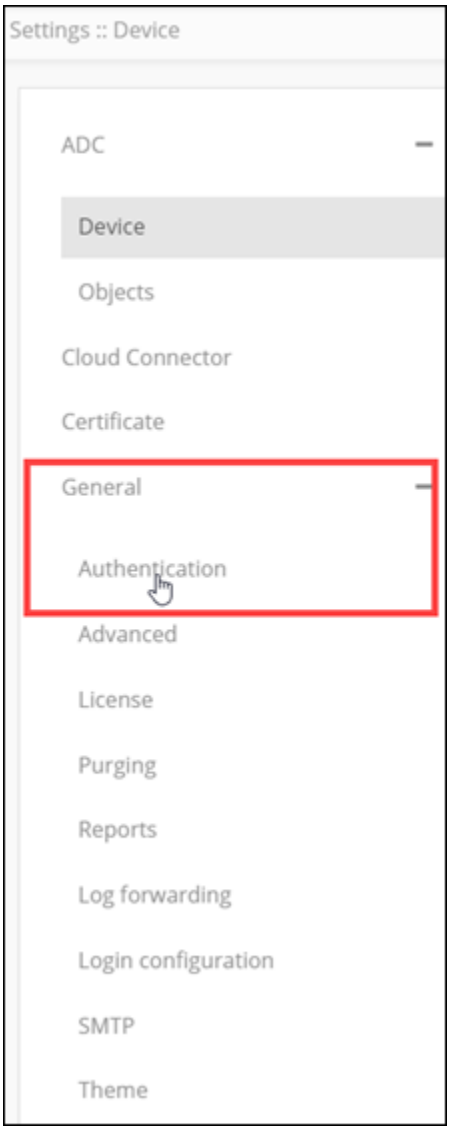
AppViewX integrates with the Active Directory and Open LDAP for authentication of external users. It also enables configuring multiple servers in the event that users belong to multiple domains.

To configure the LDAP authentication:

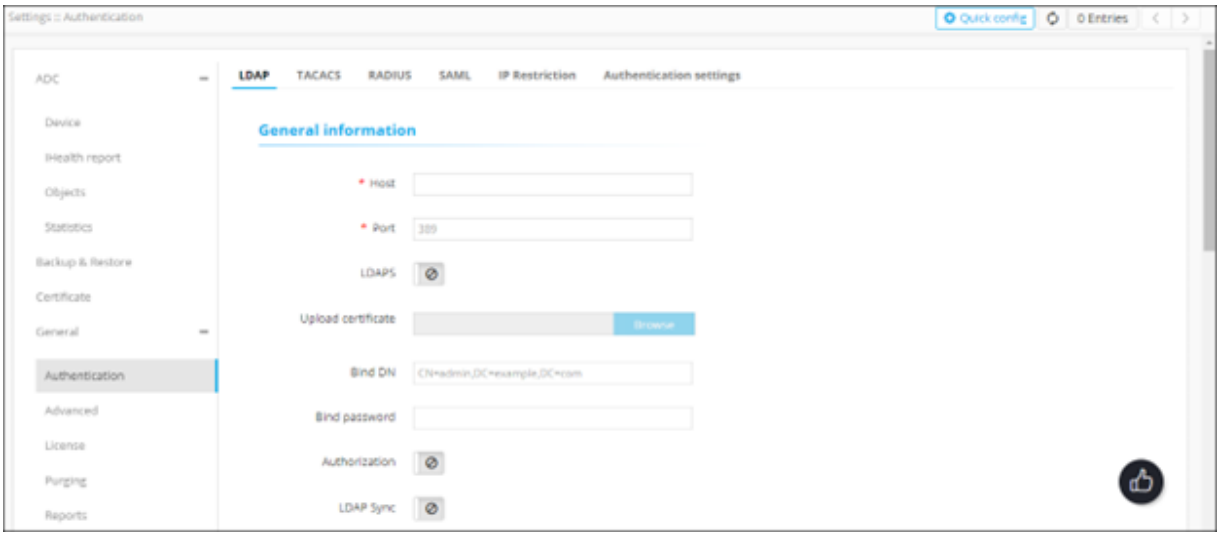
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Authentication**.



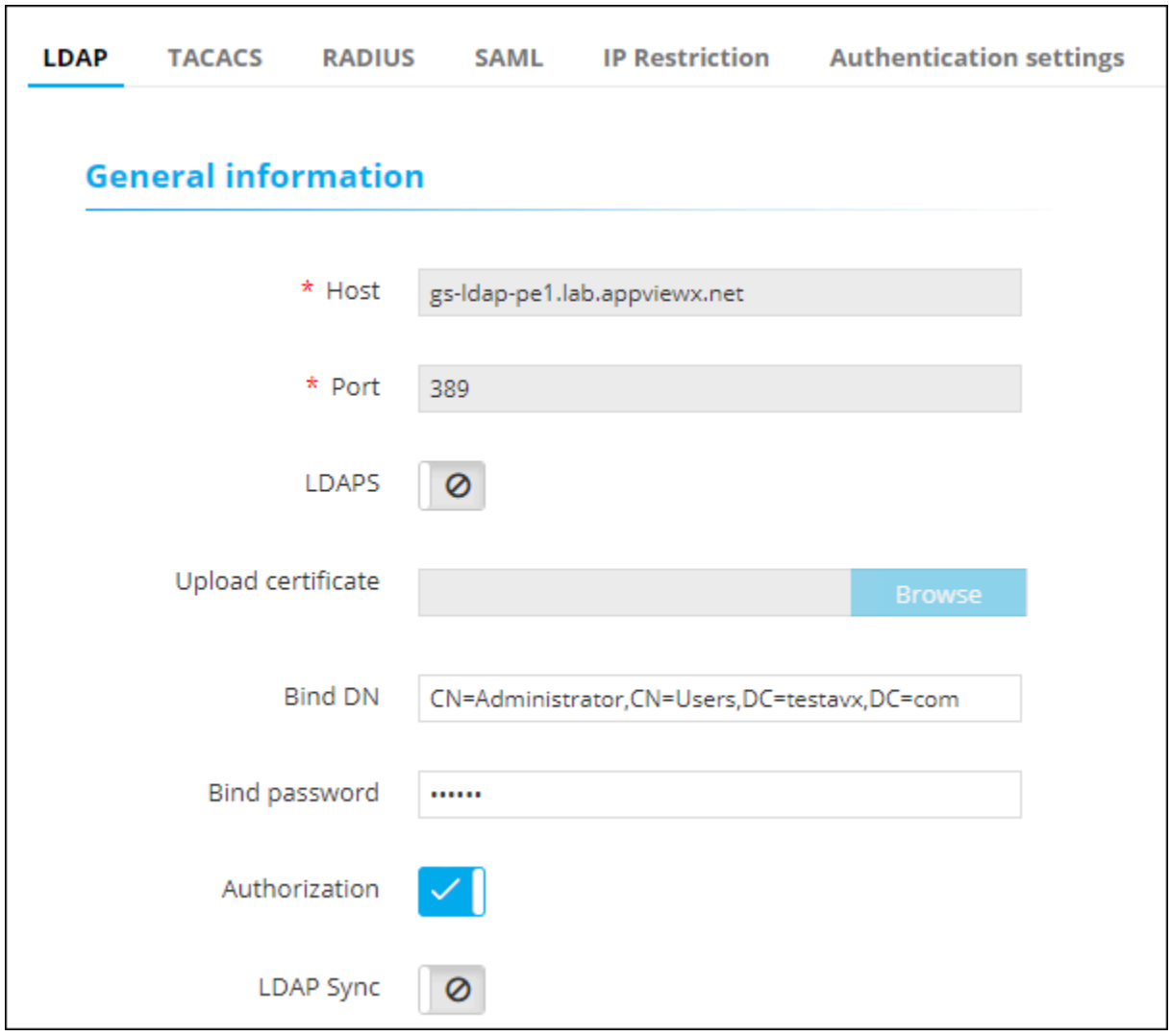
The **Settings :: Authentication** page is displayed, with the **LDAP** tab open by default.



5. To configure the LDAP settings, in the **General Information** section, enter the following details (sample values are shown in the image below the table):

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. 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.

Field	Description
	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.
All * marked fields are mandatory.	



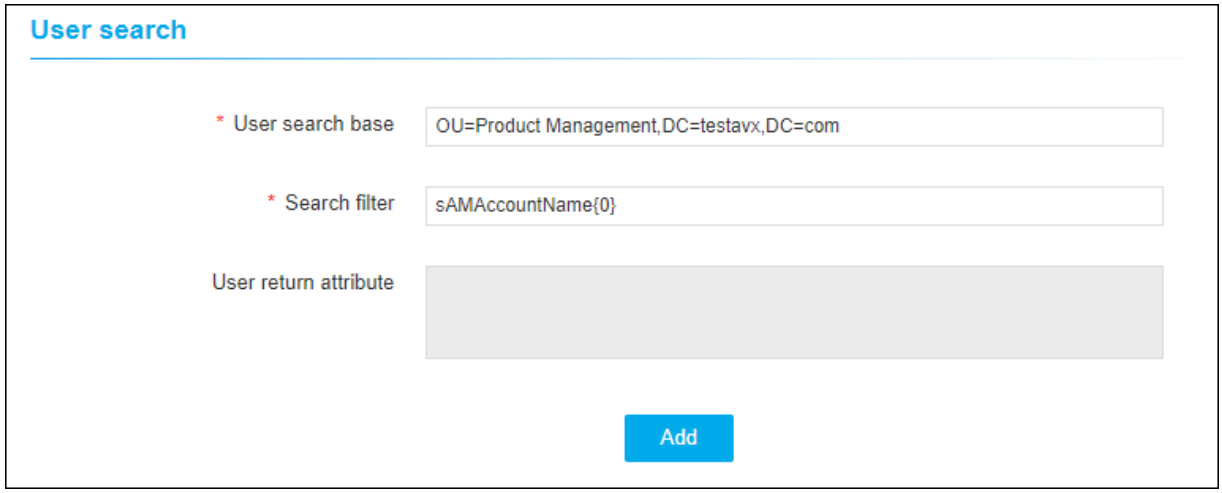
6. After entering the above connection details, to test if the host is reachable and the port is valid for establishing an LDAP/LDAPS connection, click **Test Connection**.

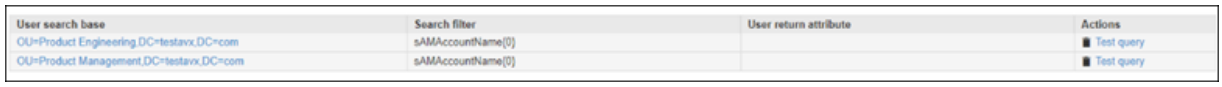
> **Note:** You can test the connection of LDAPS only when you save all of the configuration details. Bind DN and Bind password details cannot be validated through a test connection.

7. 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 below the table):

Field	Description
***User search base**	Base directory where the user is present.

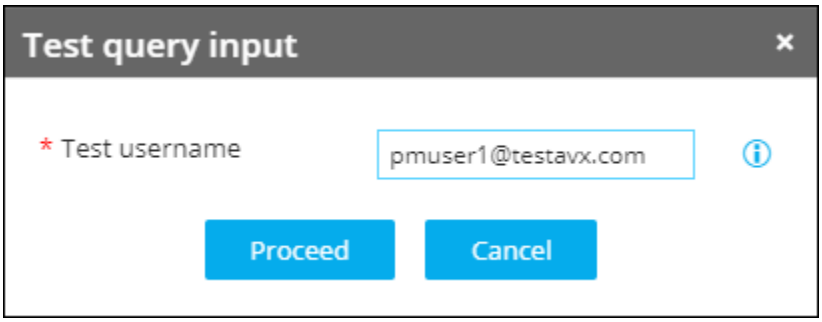
Field	Description
***Search filter**	Criteria for searching for the user from the search base.
User return attribute	User information to be retrieved from the search base. **Note:** This field is enabled only when the **Authorization** toggle (in the **General Information** section) is turned on. **Note:**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



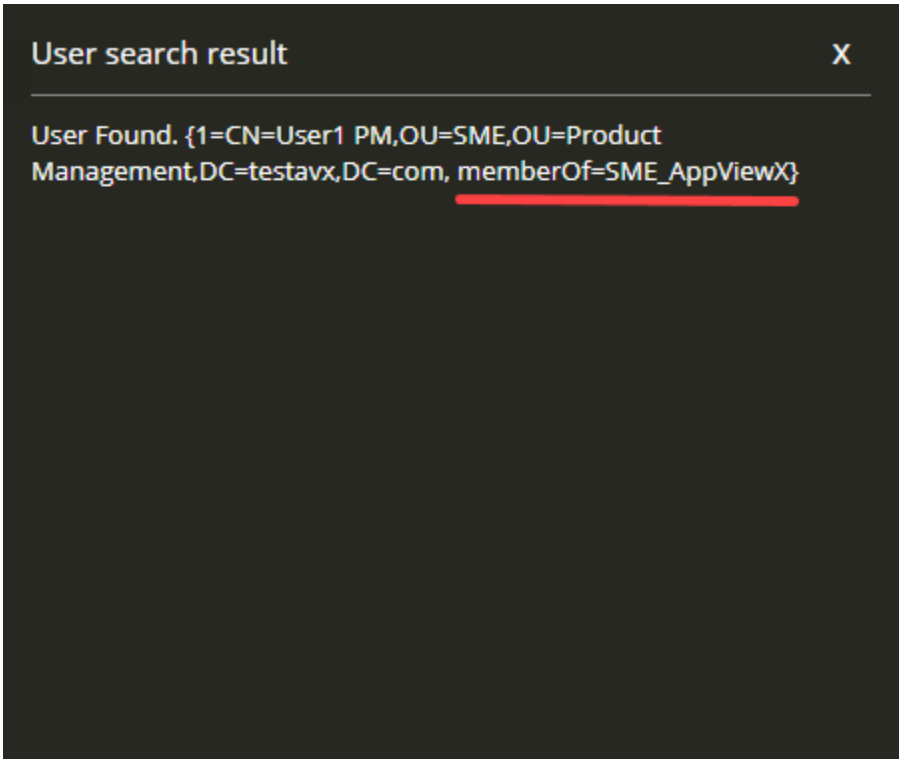


Note: You can now add multiple OUs in User search so that it checks multiple OUs to validate a user's presence in the Active Directory.

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



The output is displayed as shown in the image below:



10. 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	Description
***Group search base**	Base directory where the user group is present.
***Search filter**	Criteria to search the user group from the search base.

Field	Description
Group return attribute	User group information to be retrieved from the search base.
All * marked fields are mandatory.	

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.

11. 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.
12. To save the LDAP settings, click **Save** or to reconfigure the settings, click **Reset**.
    The LDAP authentication settings thus configured are saved and displayed in the table shown at the end of this screen:

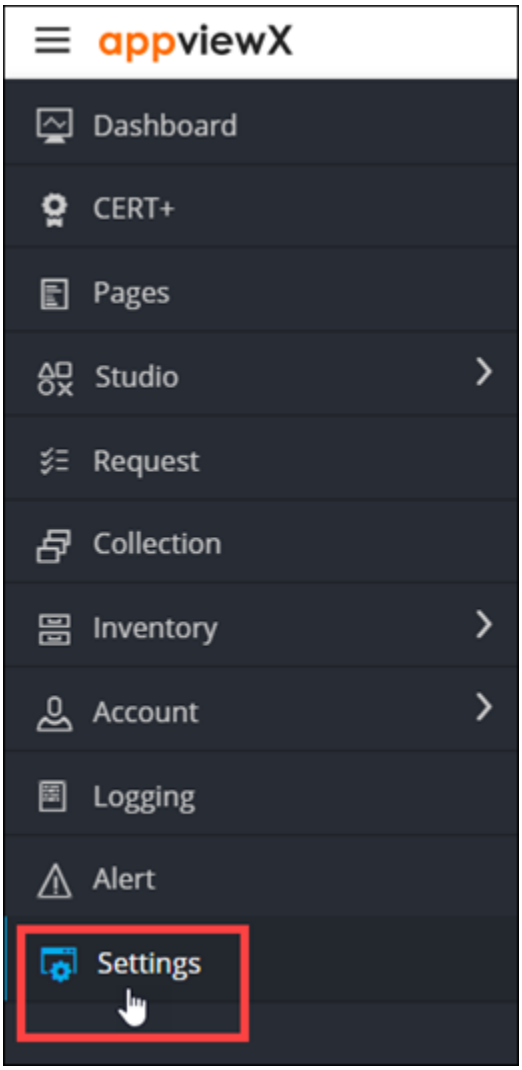
Note: In the case of multiple LDAP servers, to define/update the order in which the servers will be authenticated, drag and drop the entries in this table.

Configuring the TACACS Authentication

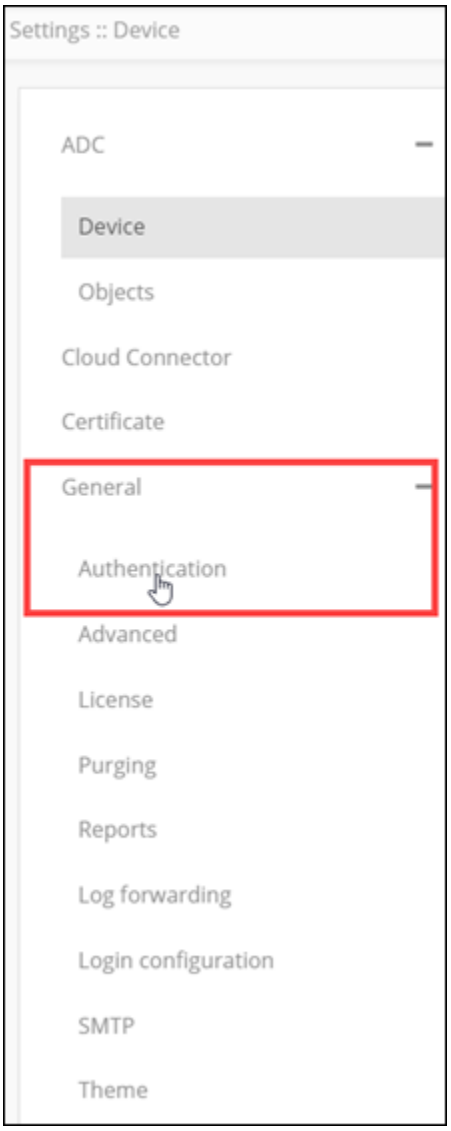
he Terminal Access Controller Access Control System (TACACS) authentication is used to validate users requesting remote access. AppViewX integrates with TACACS for authentication of external users.

To configure the TACACS authentication:

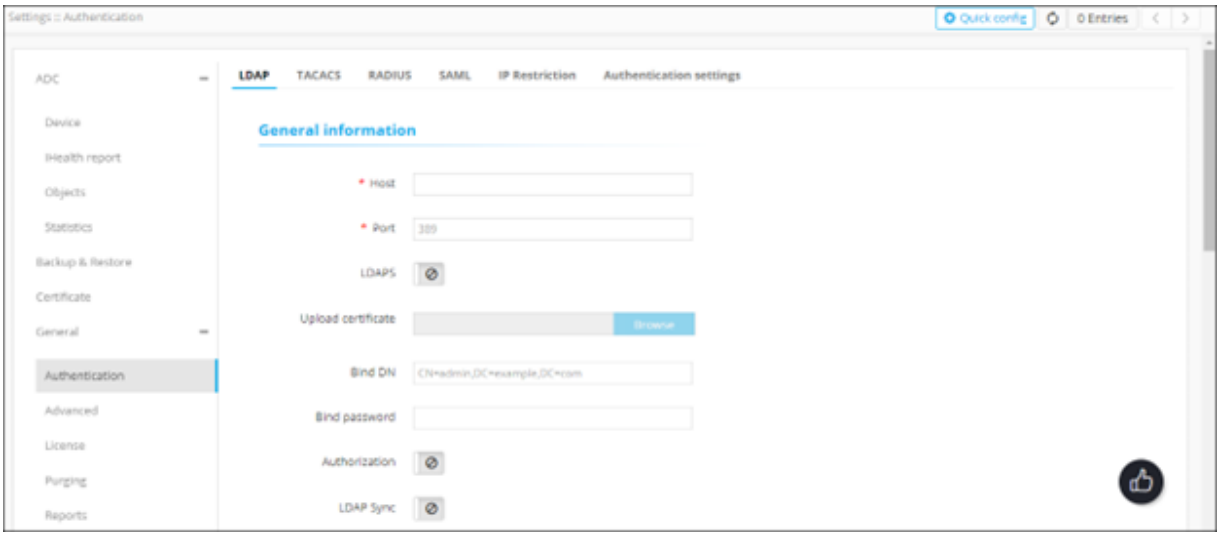
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Settings**.



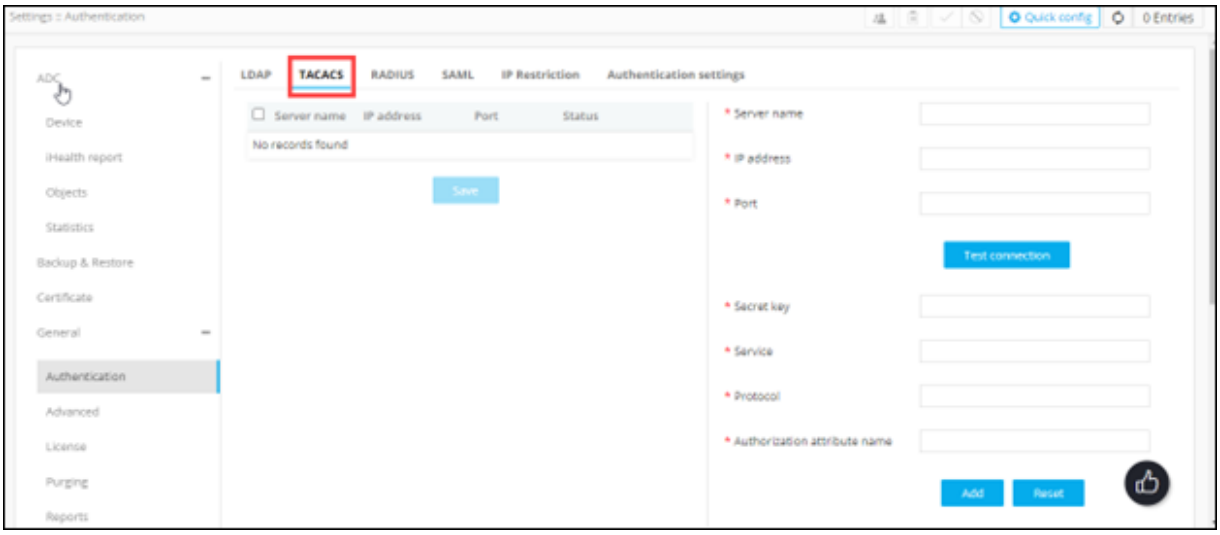
3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Authentication**.



The **Settings :: Authentication** page is displayed, with the **LDAP** tab open by default.



5. To configure the **TACACS** authentication settings, on the **Settings :: Authentication** page, click the **TACACS** tab.



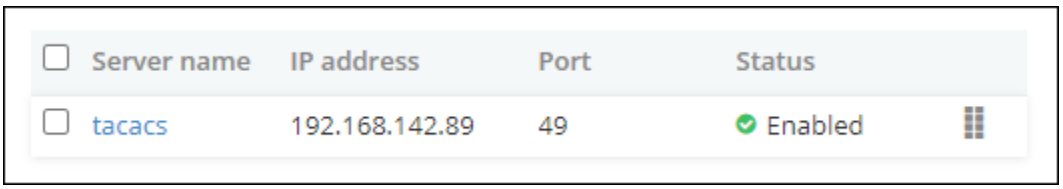
6. Enter the following details (sample values are shown in the image below the table):

Field	Description
***Server name**	Name of the TACACS server.
***IP address**	IP address of the TACACS server.
***Port**	Port number of the TACACS server.
All * marked fields are mandatory.	

7. To test the connectivity between AppViewX and the IP address mentioned above, click **Test connection**.
8. Enter the following details (sample values are shown in the image below the table):

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.
All * marked fields are mandatory.	

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



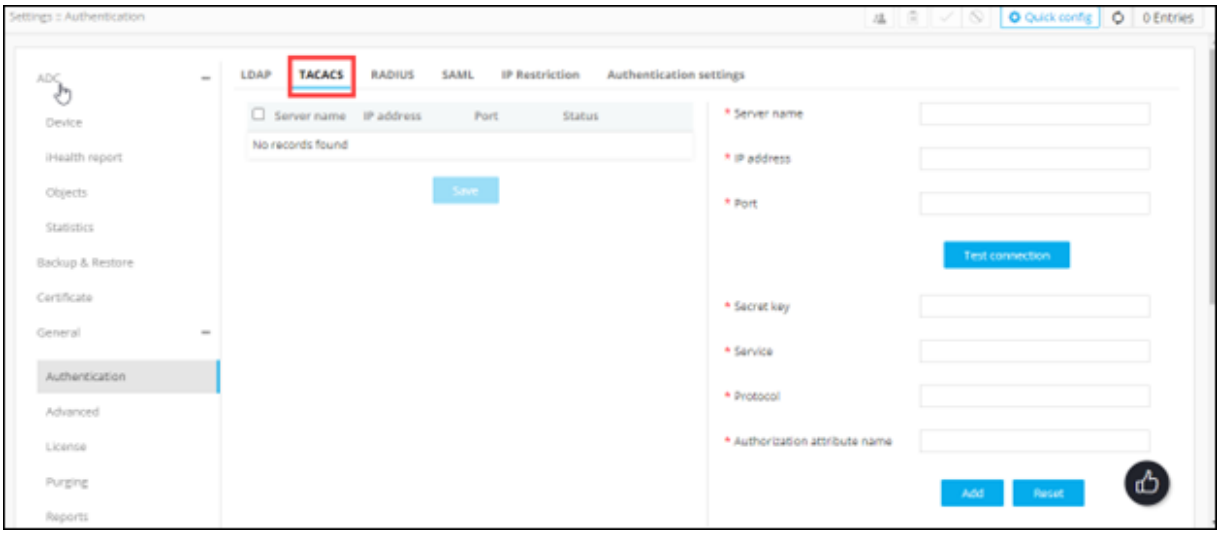
Note: In the case of multiple TACACS servers, to define/update the order in which the servers will be authenticated, drag and drop the entries in this table.

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

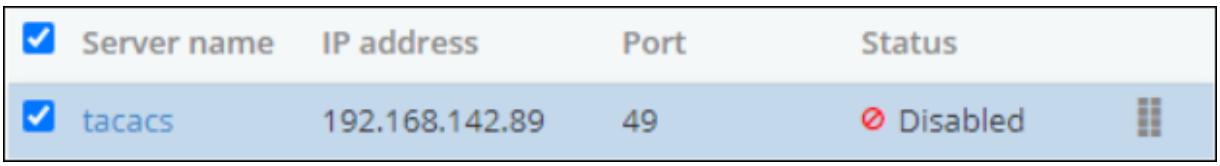
Enabling a TACACS Server for Authentication

To enable a TACAS server for authentication:

1. Navigate to the **Settings :: Authentication** page.
2. To configure the TACACS authentication settings, on the **Settings :: Authentication** page, click the **TACACS** tab.



3. 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.



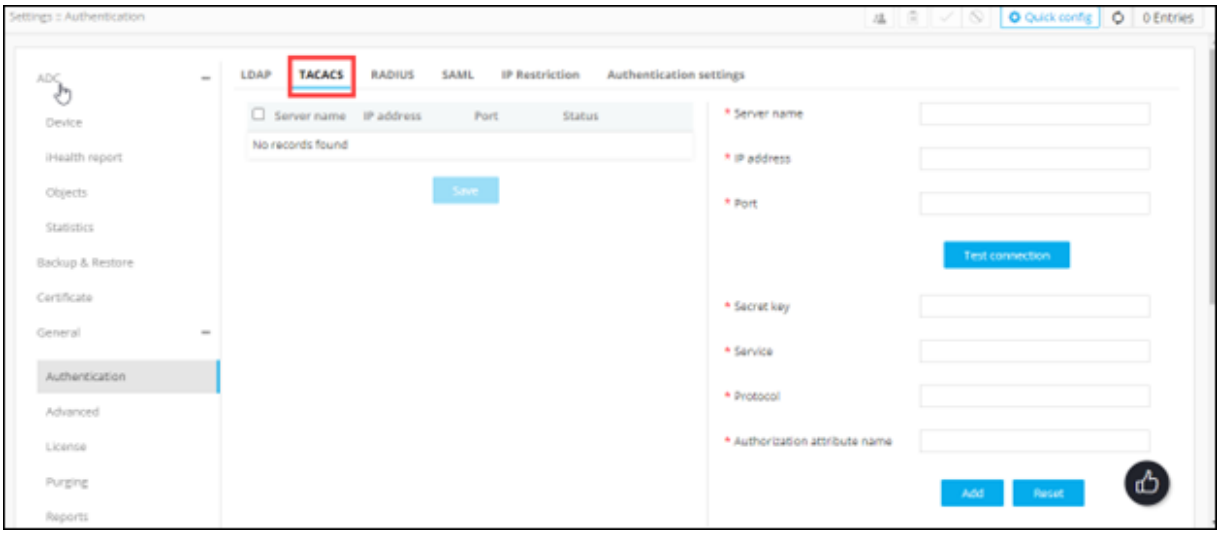
4. From the top-right corner of the page, click 

.
5. In the **Confirmation message** dialog box, click **Proceed**.

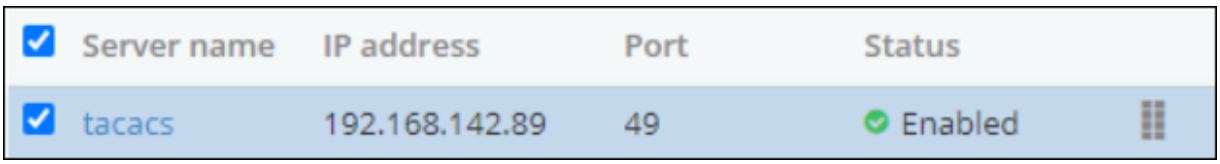
Disabling a TACACS Server for Authentication

To disable a TACAS server for authentication:

1. Navigate to the **Settings :: Authentication** page.
2. To configure the TACACS authentication settings, on the **Settings :: Authentication** page, click the **TACACS** tab.



3. 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.



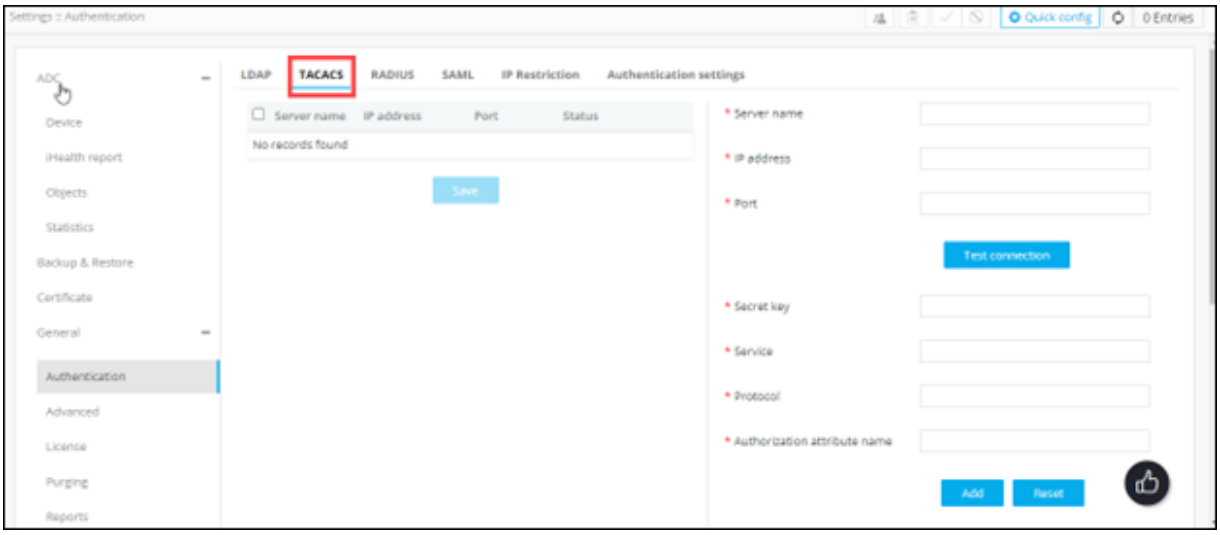
4. From the top-right corner of the page, click 

.
5. In the **Confirmation message** dialog box, click **Proceed**.

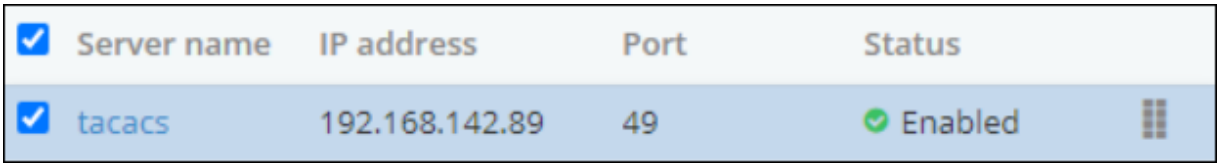
Deleting a TACACS Server

To delete a TACAS server :

1. Navigate to the **Settings :: Authentication** page.
2. To configure the TACACS authentication settings, on the **Settings :: Authentication** page, click the **TACACS** tab.



3. 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.



4. From the top-right corner of the page, click 

.
5. In the **Confirmation message** dialog box, click **Proceed**.

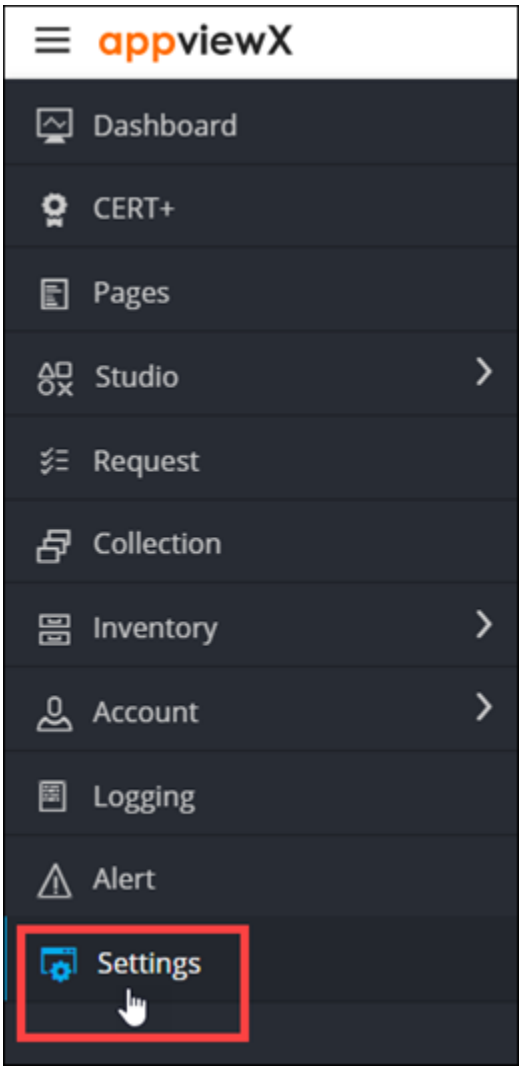
Configuring the RADIUS Configuration

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

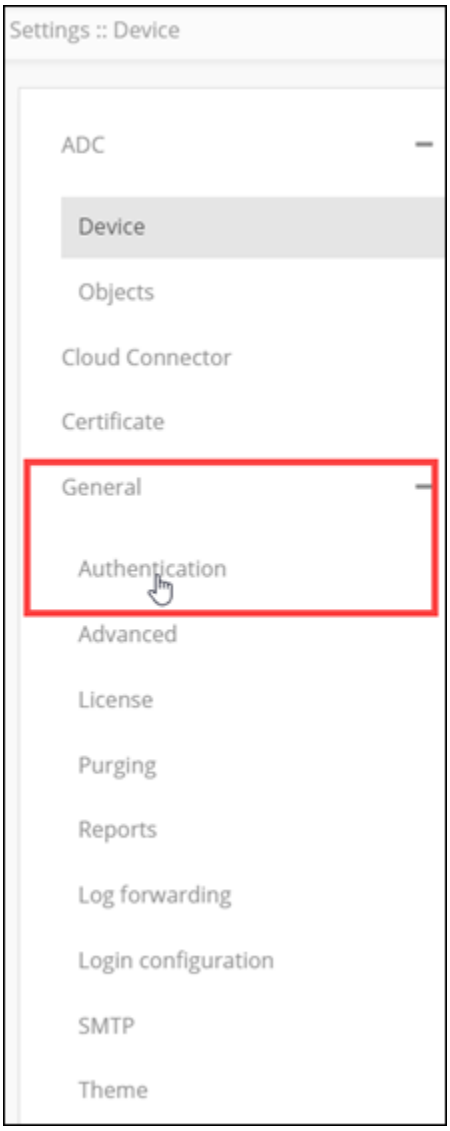
AppViewX integrates with RADIUS for authentication of external users.

To configure the RADIUS authentication:

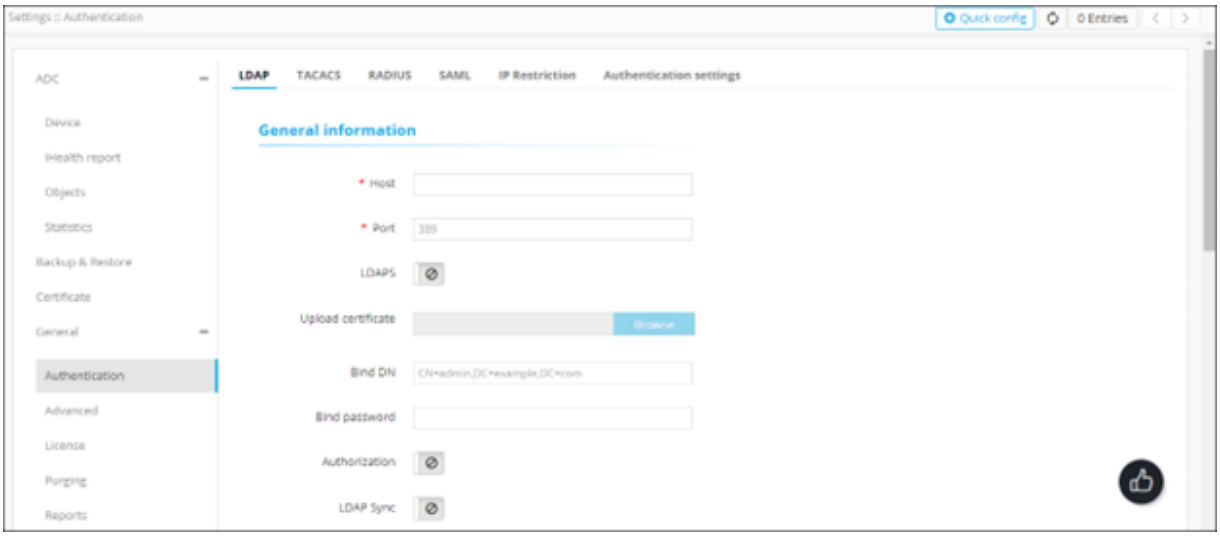
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Settings**.



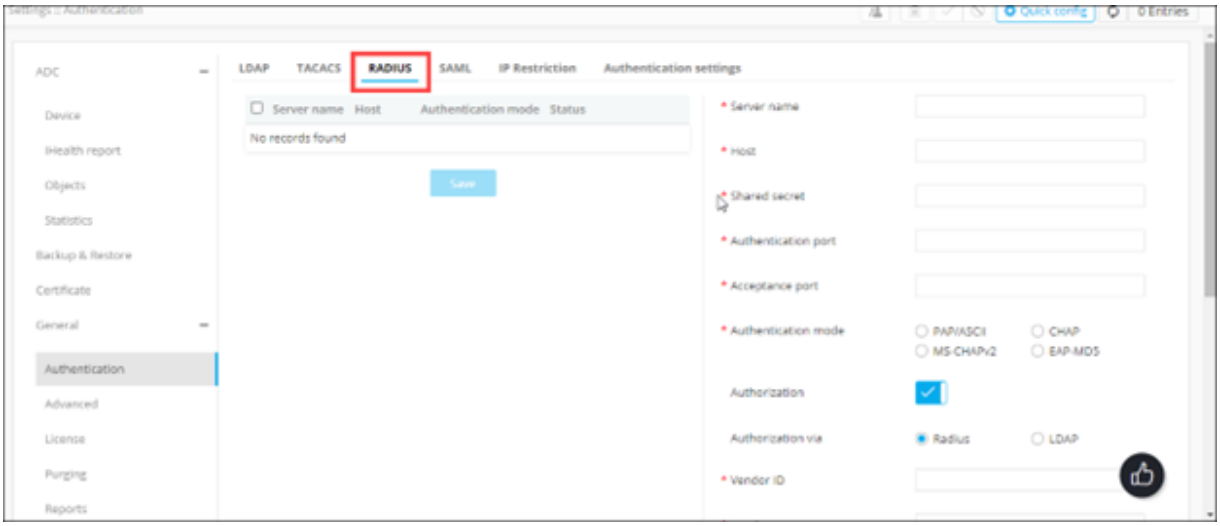
3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Authentication**.



The **Settings :: Authentication** page is displayed, with the **LDAP** tab open by default.



5. To configure the RADIUS authentication settings, on the **Settings:: Authentication** page, click the **RADIUS** tab.

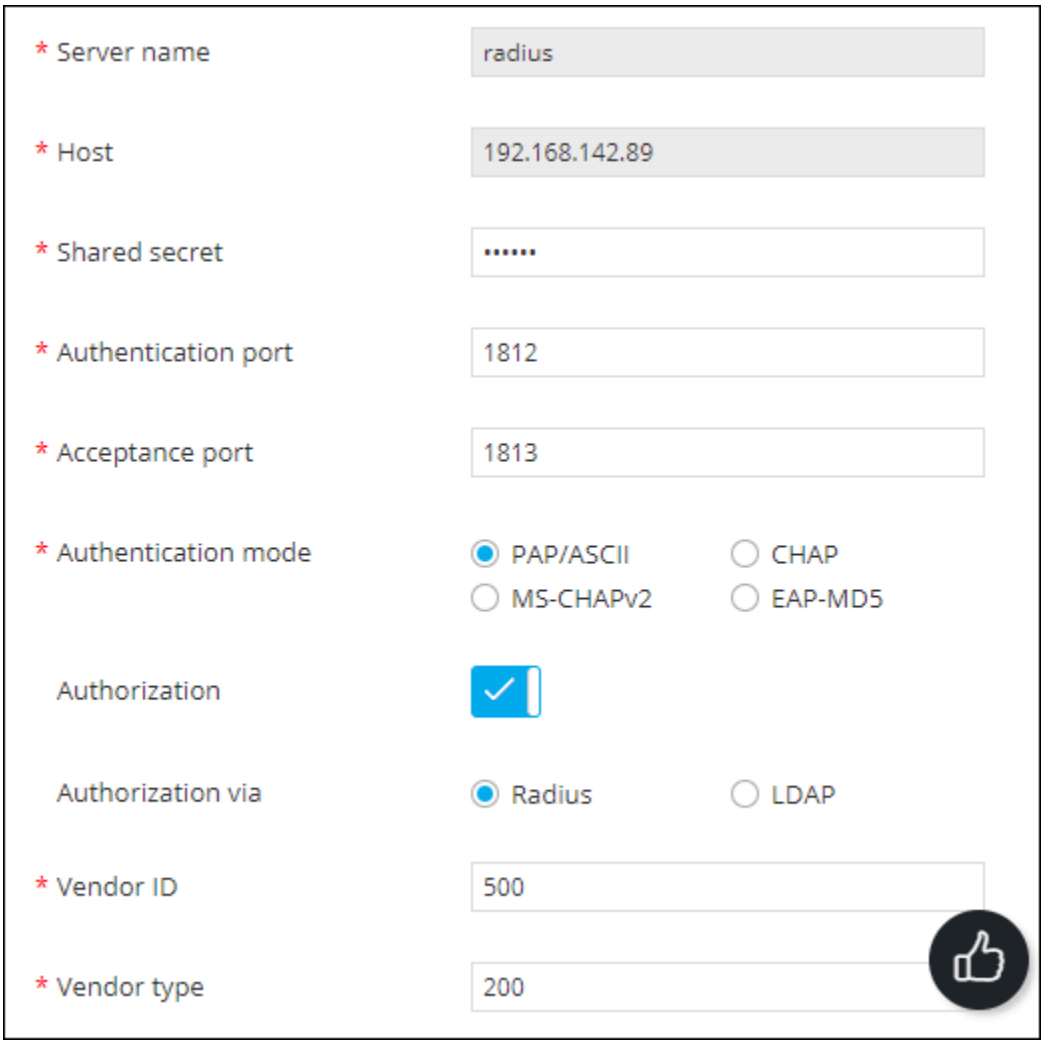


6. Enter the following details (sample values are shown in the image below the table):

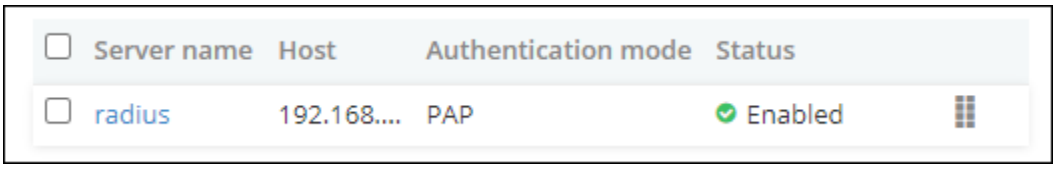
Field	Description
***Server name**	Name of the RADIUS server.
***Host**	The IP address of the RADIUS server.
***Shared secret**	A unique key for authentication between the AppViewX server and the RADIUS server.
***Authentication port**	Port number that AppViewX will use for authentication.

Field	Description
	Note: The default authentication port number is 1812. Please check with your sysadmin 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 sysadmin 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.
All * marked fields are mandatory.	



7. 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 shown in the left half of the screen:



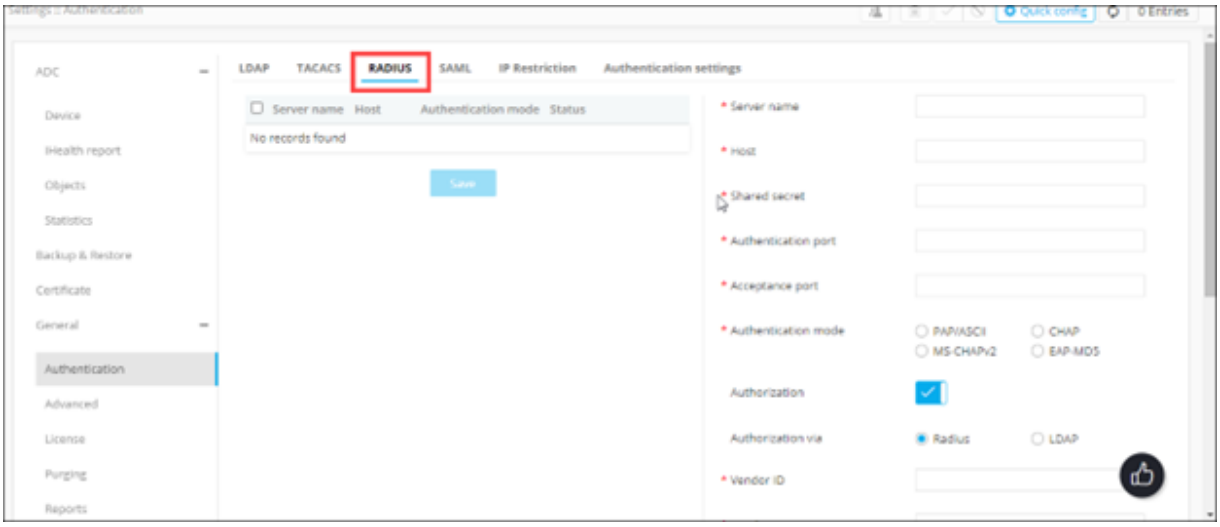
Note: In the case of multiple RADIUS servers, to define/update the order in which the servers will be authenticated, drag and drop the entries in this table.

- 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. Navigate to the **Settings:: Authentication** page.
2. To configure the RADIUS authentication settings, on the **Settings:: Authentication** page, click **RADIUS** tab.



3. 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.

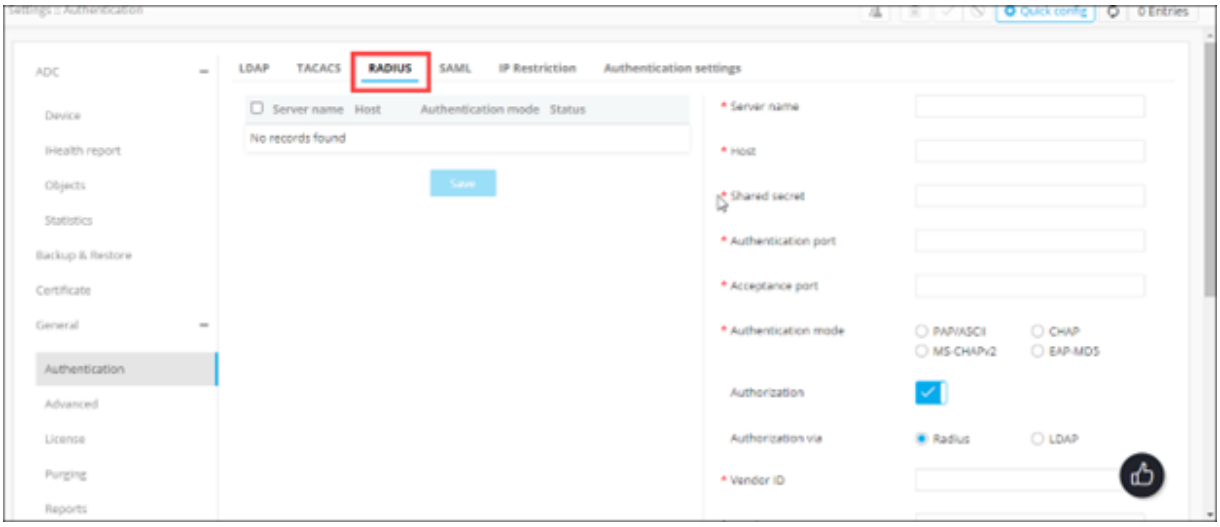
4. From the top-right corner of the page, click 

5. In the **Confirmation** message dialog box, click **Proceed**.

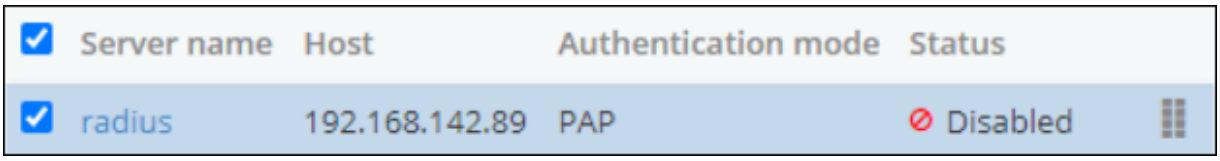
Disabling a RADIUS Server for Authentication

To disable a RADIUS server for authentication:

1. Navigate to the **Settings:: Authentication** page.
2. To configure the RADIUS authentication settings, on the **Settings:: Authentication** page, click the **RADIUS** tab.



3. 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.



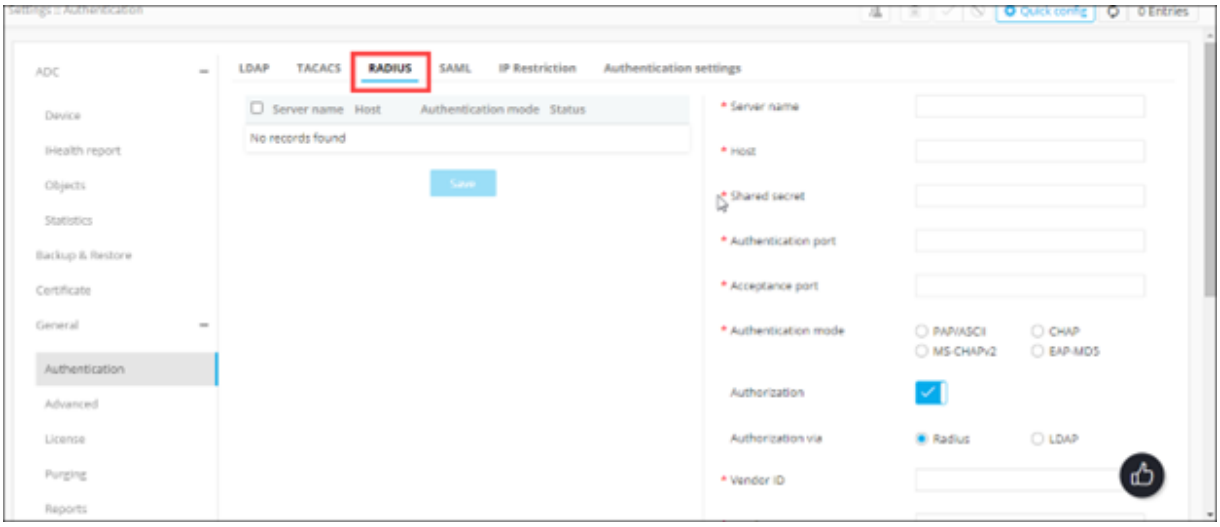
4. From the top-right corner of the page, click 

5. In the **Confirmation** message dialog box, click **Proceed**.

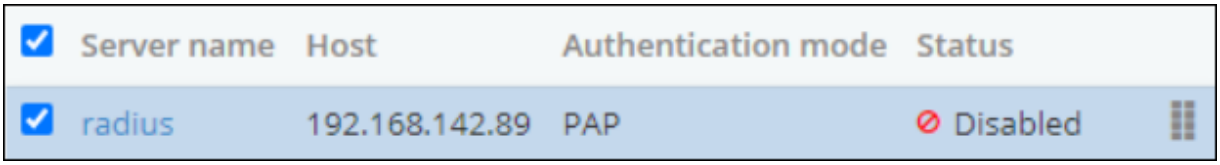
Deleting a RADIUS Server

To delete a RADIUS server:

1. Navigate to the **Settings:: Authentication** page.
2. To configure the RADIUS authentication settings, on the **Settings:: Authentication** page, click **RADIUS** tab.



3. 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.



4. From the top-right corner of the page, click 

.
5. In the **Confirmation** message dialog box, click **Proceed**.

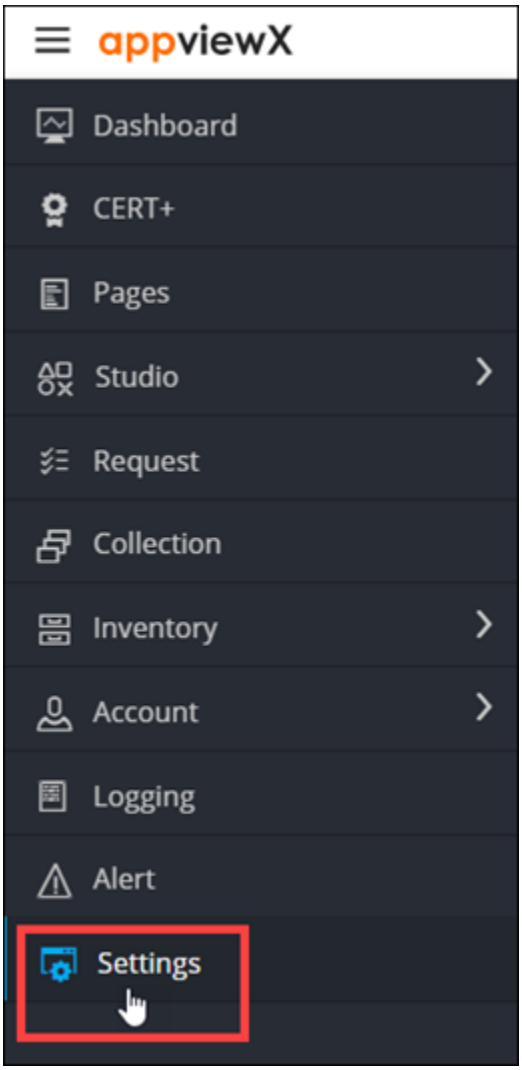
Configuring Single Sign On Settings with AppViewX

The Security Assertion Markup Language (SAML) protocol is used for authenticating and authorizing user identity for Single Sign On (SSO) services.

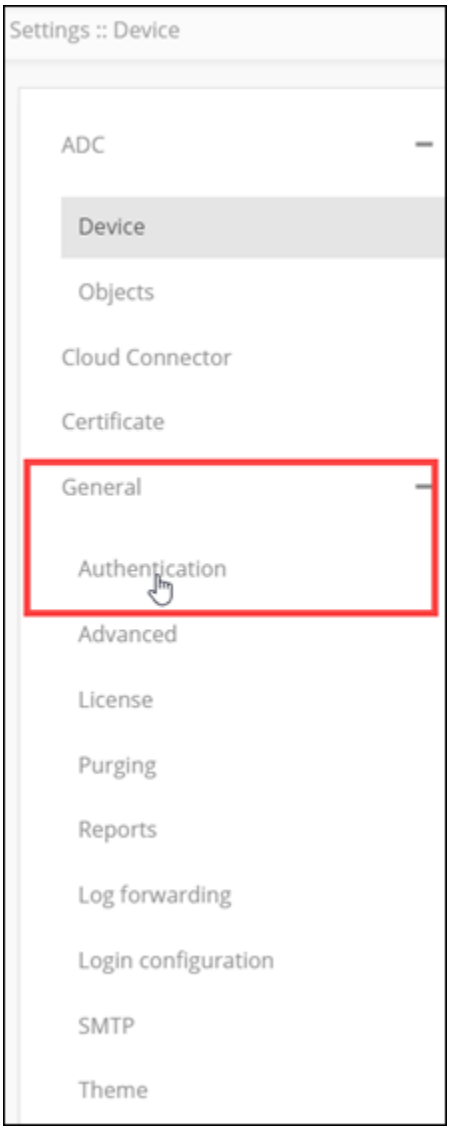
AppViewX integrates with SAML 2.0 for authenticating external users when Single Sign On is enabled. In this case, the Identity Provider (IdP) is used for user authentication and authorization.

To configure single sign on settings with AppViewX:

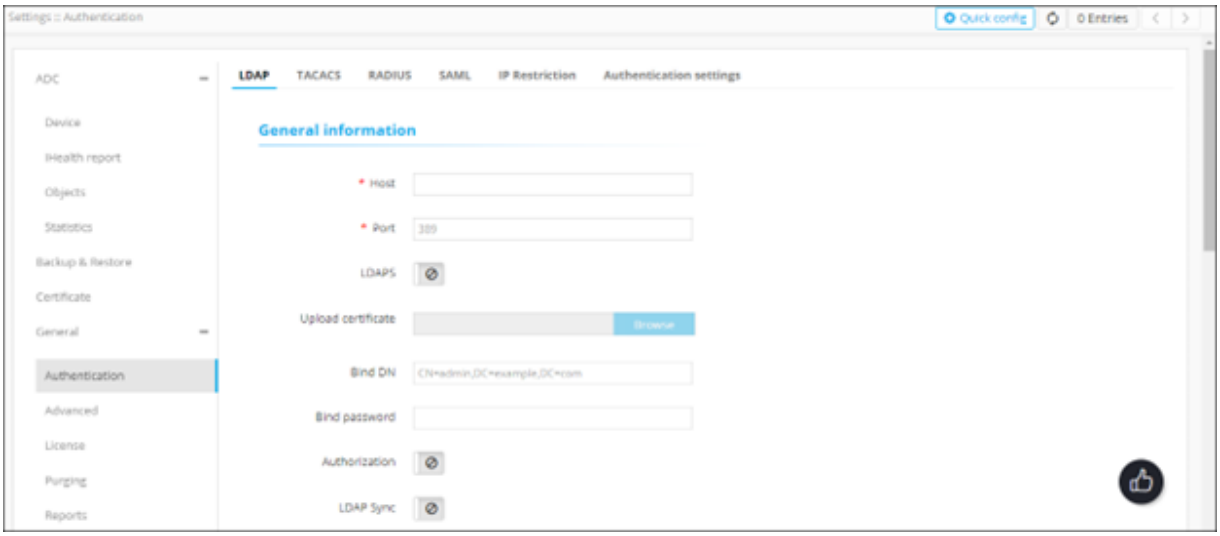
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Settings**.



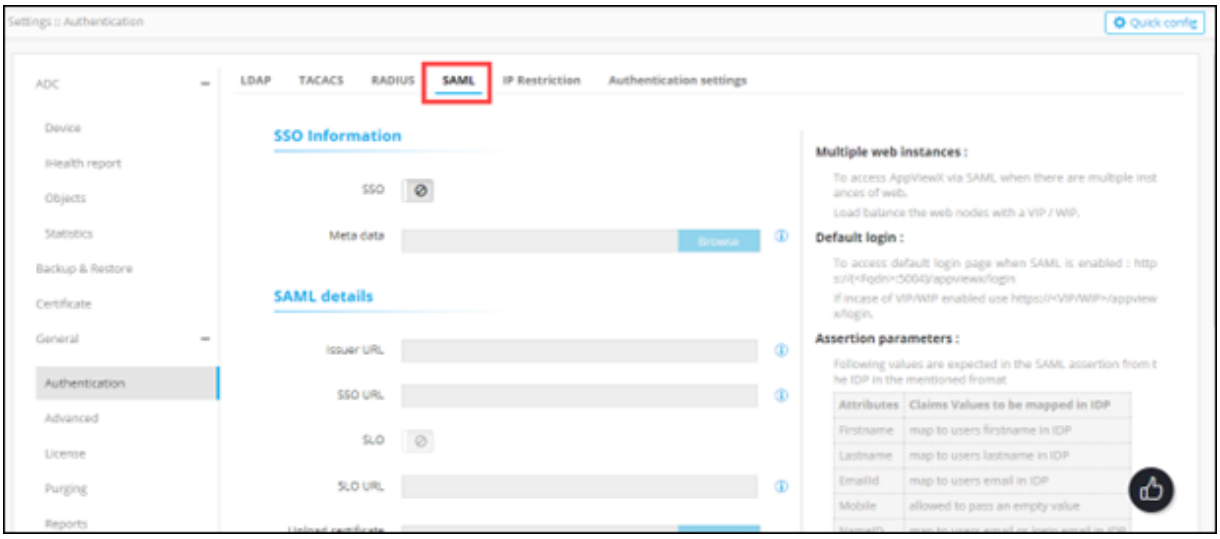
3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Authentication**.



The **Settings :: Authentication** page is displayed, with the **LDAP** tab open by default.



5. To configure the SAML authentication settings, on the **Settings :: Authentication** page, click the **SAML** tab.



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

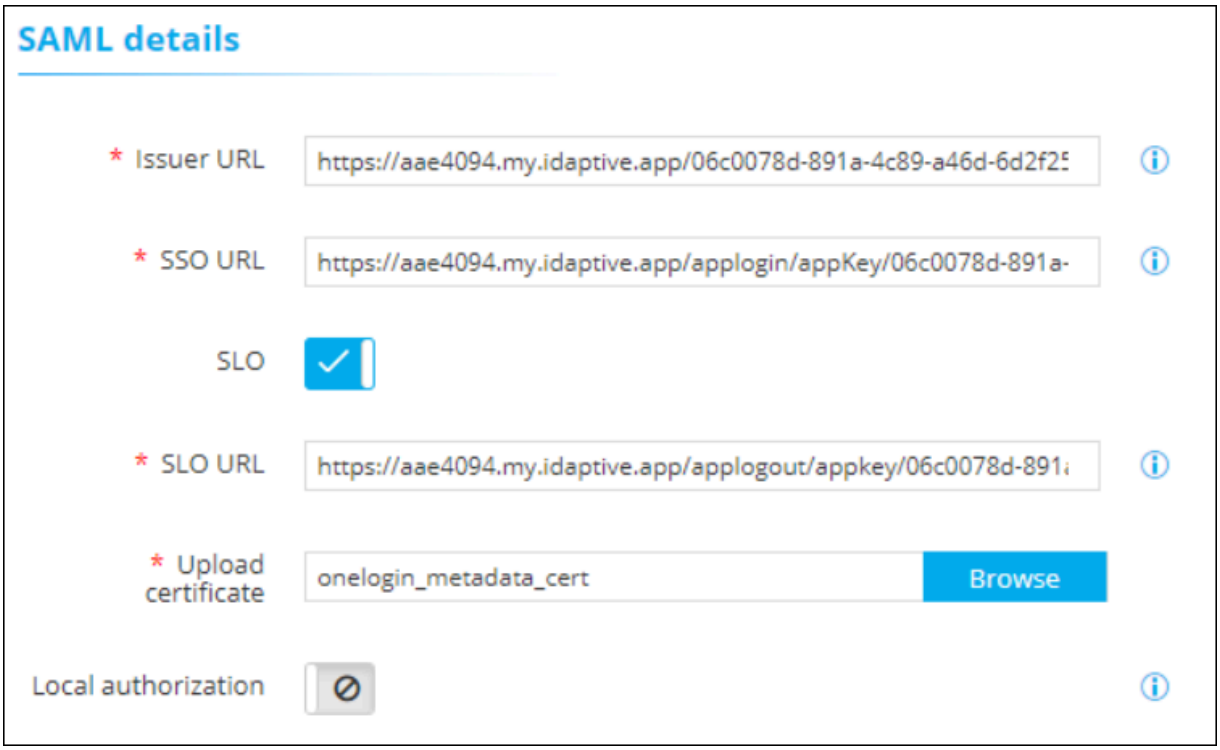
Field	Description
SSO	To use SAML authentication for Single Sign On, turn on the **SSO** toggle. The **Config Information** section is displayed with the field information auto-populated as shown below:

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.

7. If the IdP is not able to pass the roles/user group as a part of of the SAML assertion and requires AppViewX to perform the authorization, in the **SAML details** section, to enable local authorization, enter the following details (sample values are shown in the image below the table):

Field	Description
***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.

Field	Description
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. **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.
All * marked fields are mandatory.	



8. To save the SAML authentication settings, click **Save** or to cancel the authentication settings, click **Cancel**.

- Integrating SAML (Vendor-specific)
- ADFS Integration
- Forgerock Integration
- Idaptive Integration
- Okta Integration
- OneLogin Integration

Integrating SAML (Vendor-specific)

To read vendor-specific steps for SAML integration, click the vendor name from the following list:

- ADFS
- Forgerock
- Idaptive
- Okta
- OneLogin

ADFS Integration

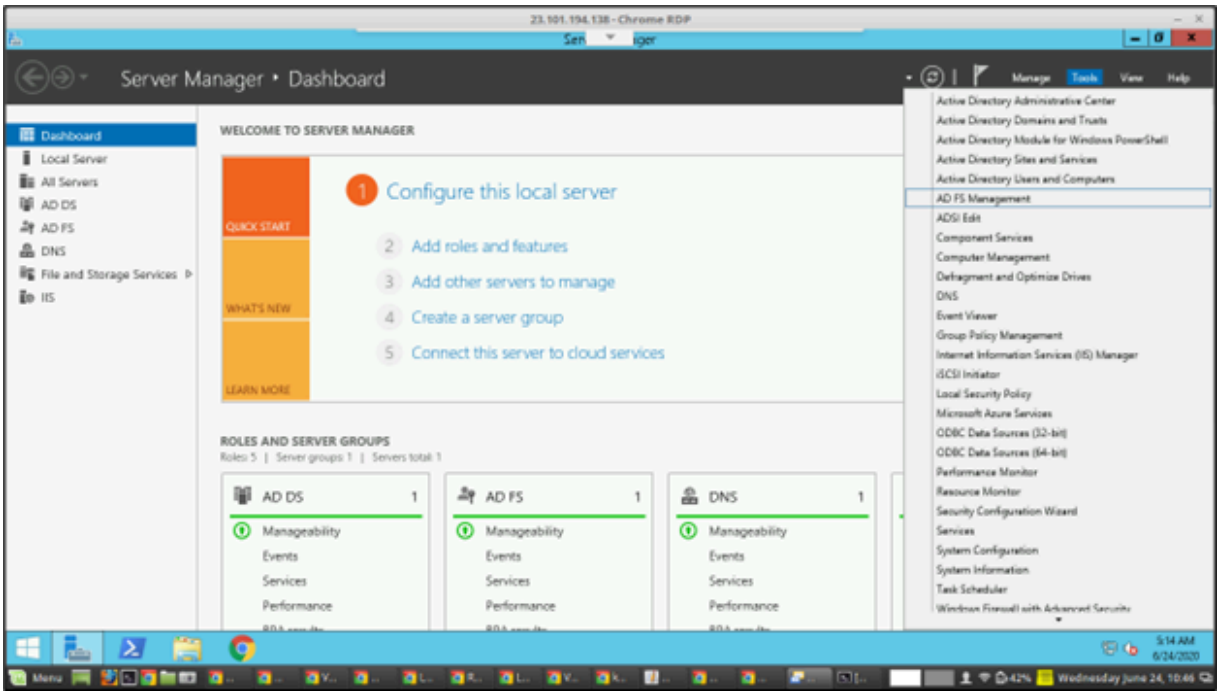
The below steps are performed at the IdP end. The navigation and screenshots might differ based on the version of the IdP. (This is just an example configuration)

Prerequisite

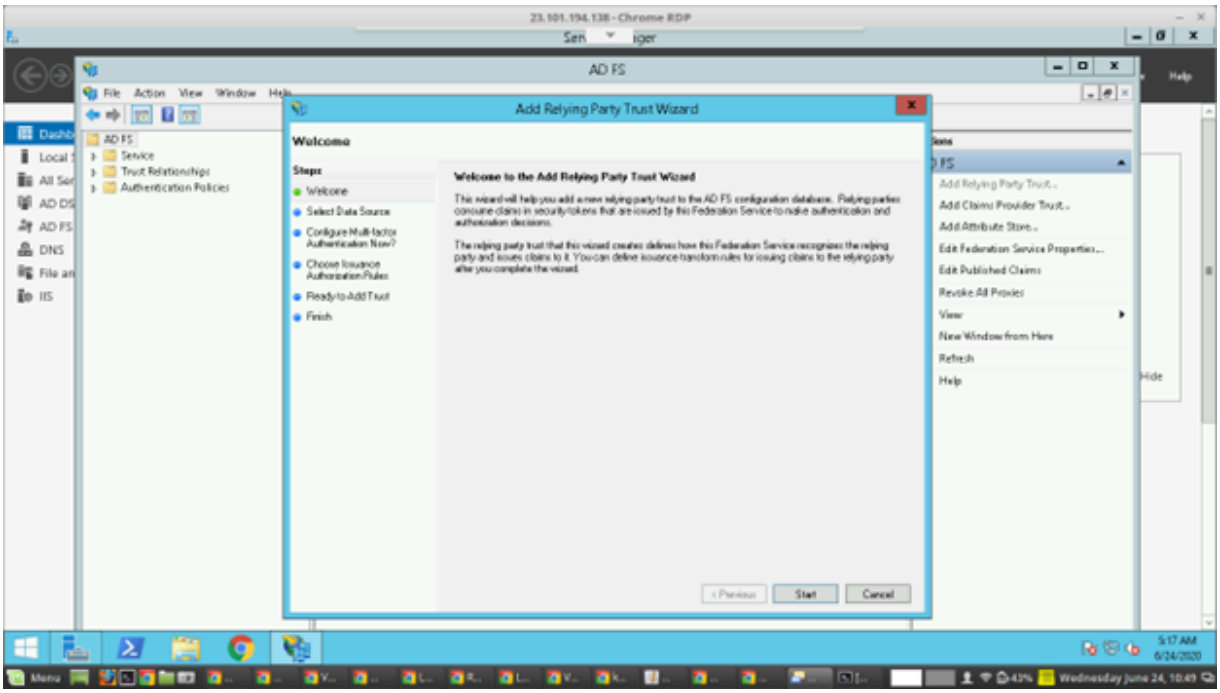
To enable ADFS based single sign-on, the ADFS service should be installed and configured with the respective Active Directory Domain.

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

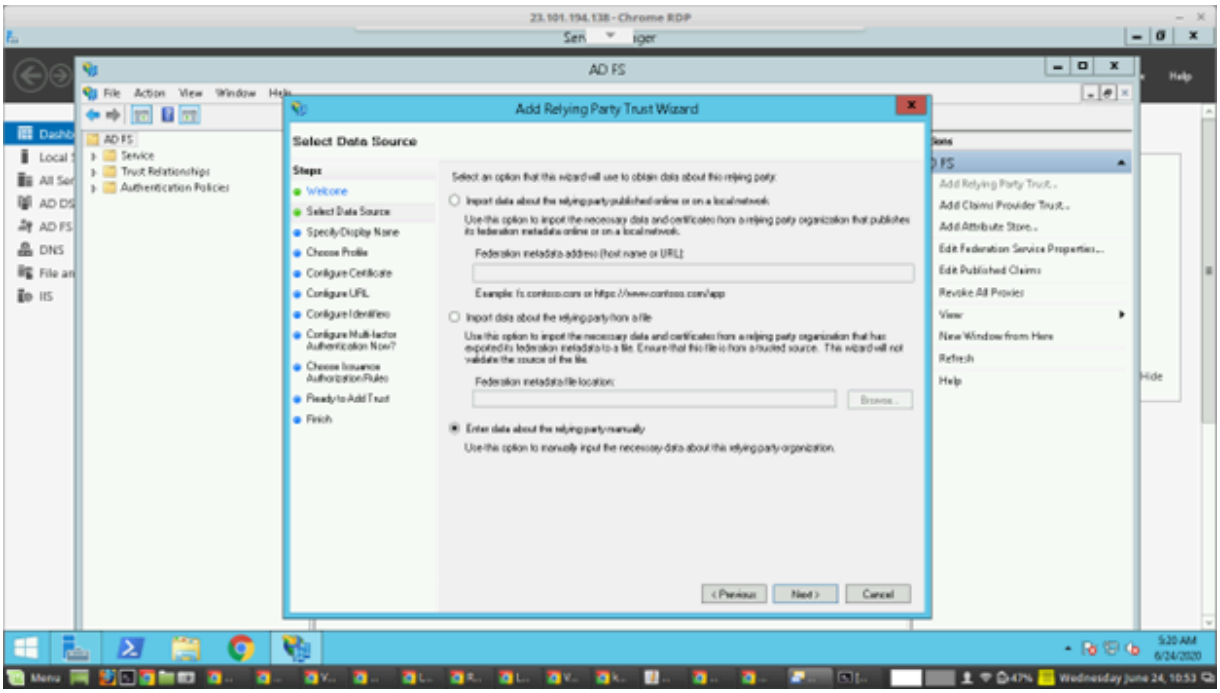
1. Navigate to **Server Manager** > **Tools** > **AD FS Management**.



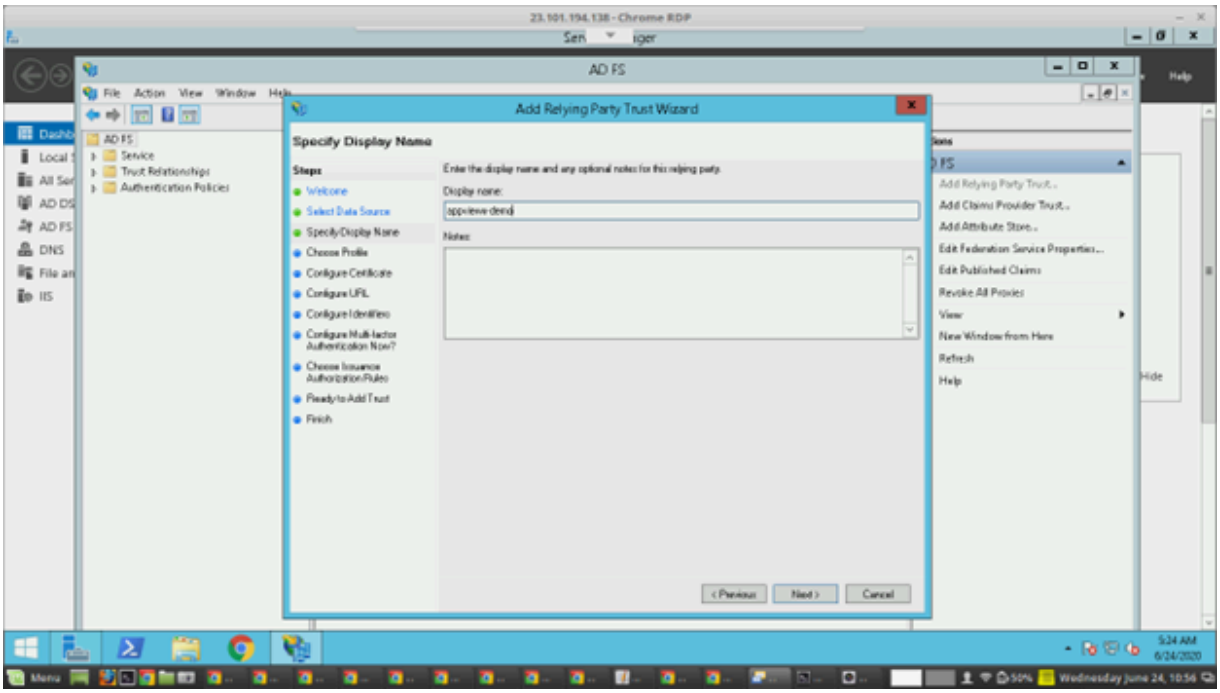
2. In the **AD FS** window, under **Actions** select **Add Relying Party Trust**.



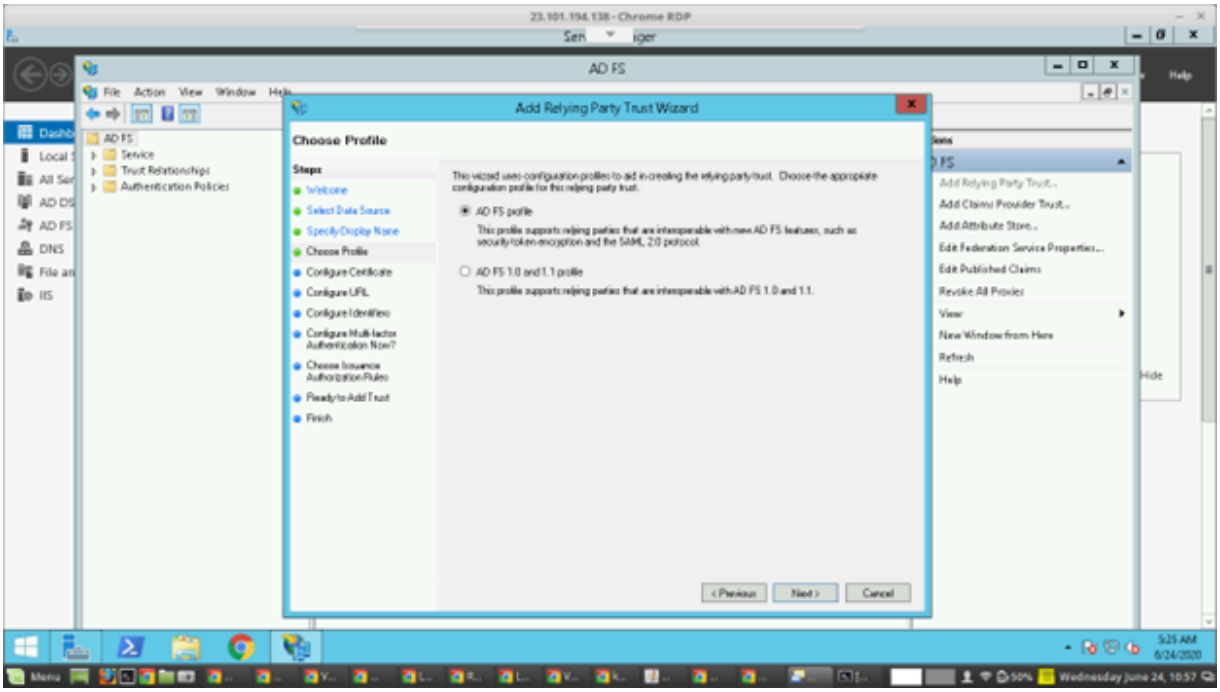
3. Start the **Add Relying Party Trust wizard**.
4. Under the **Select Data Source** section, select the **Enter data about the relying party manually** option and click **Next**.



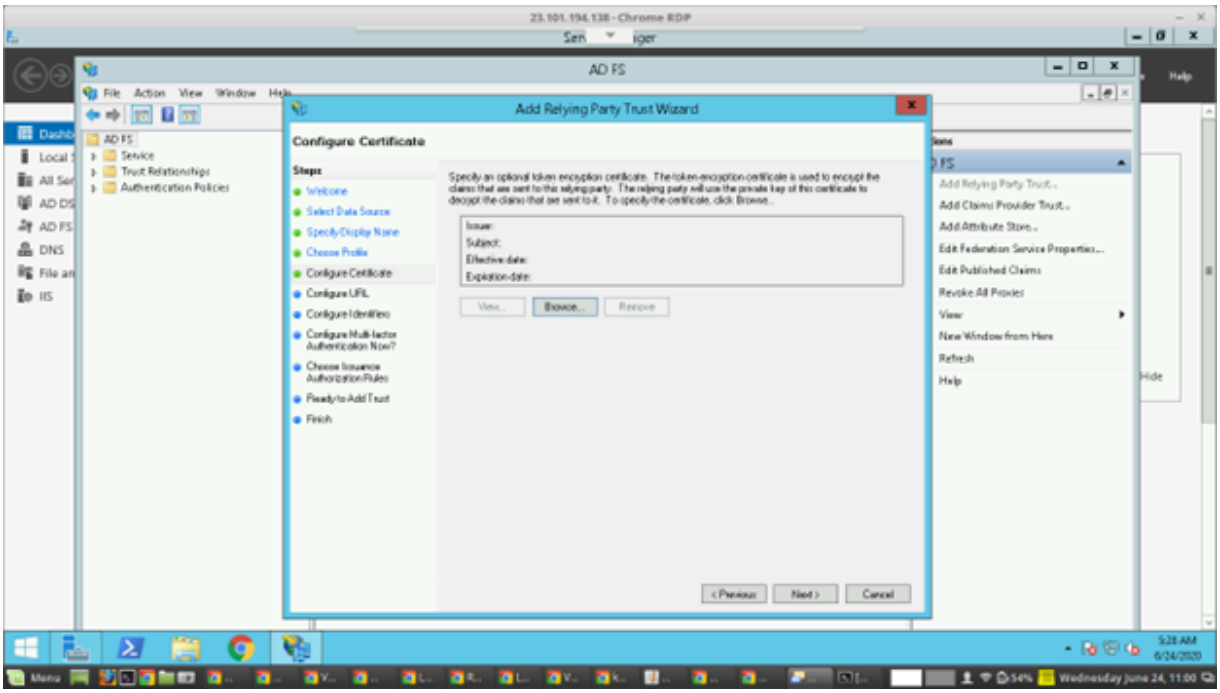
5. Enter a **Display Name** and click **Next**.



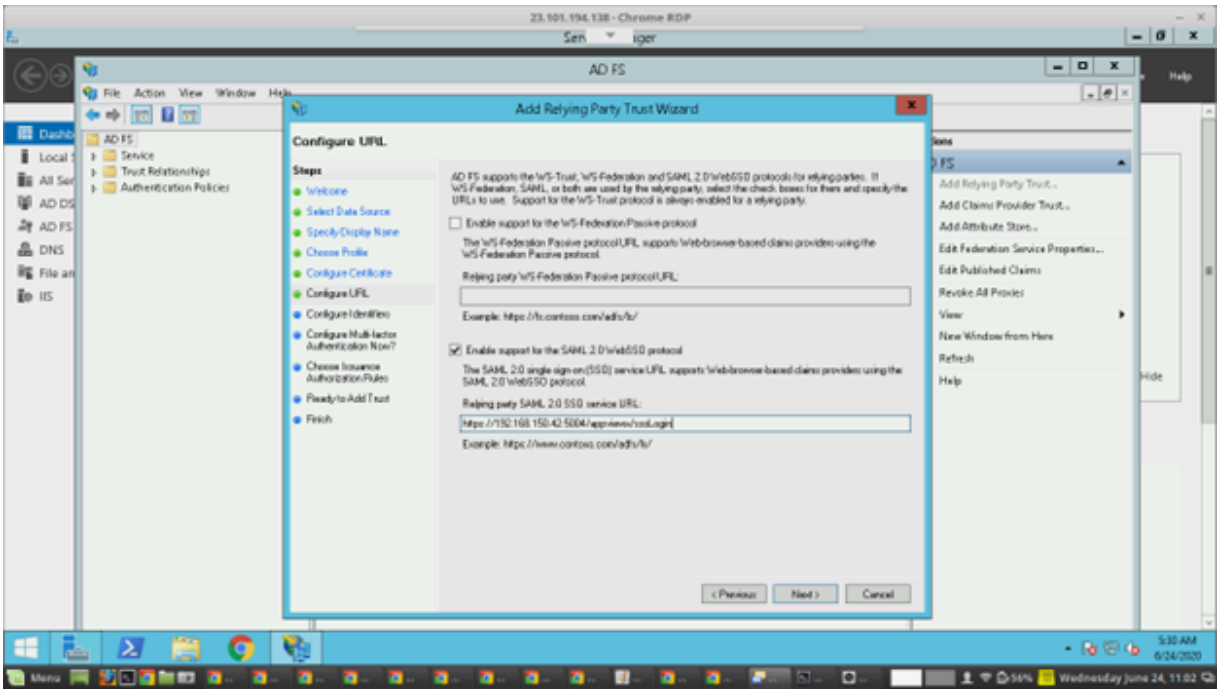
6. Under the **Choose Profile** section, select the **AD FS profile**option and click **Next**.



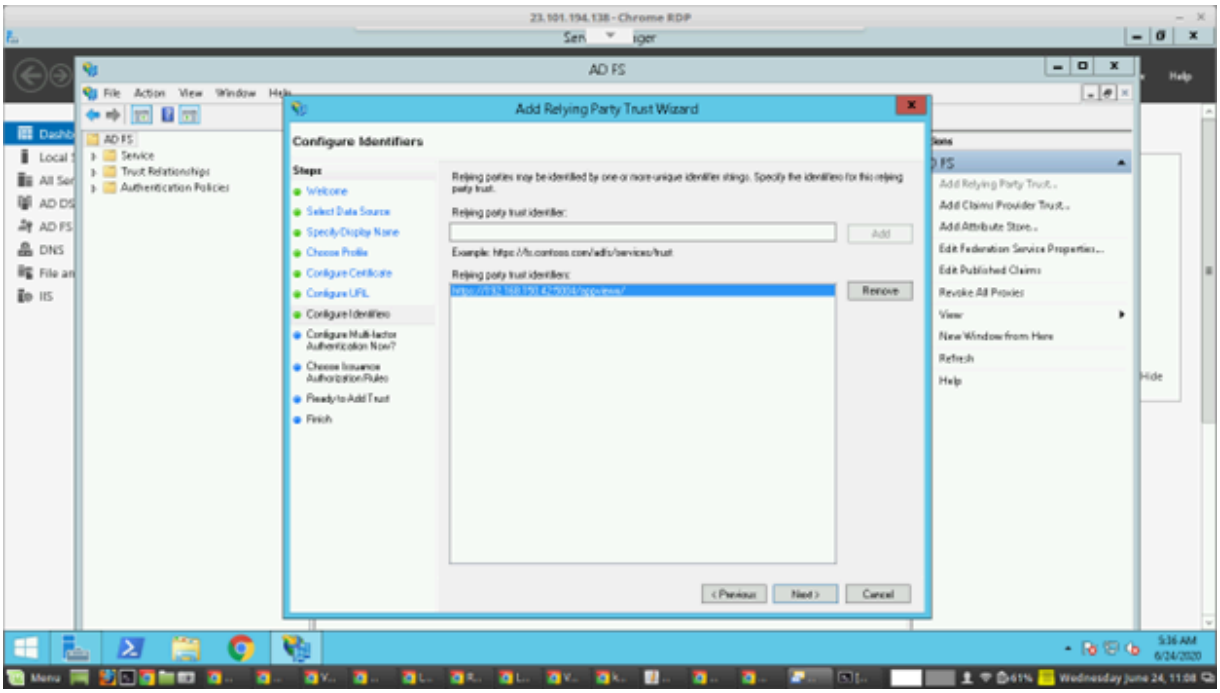
7. Add a new token encryption certificate if needed or leave it with the default setting and click **Next**.



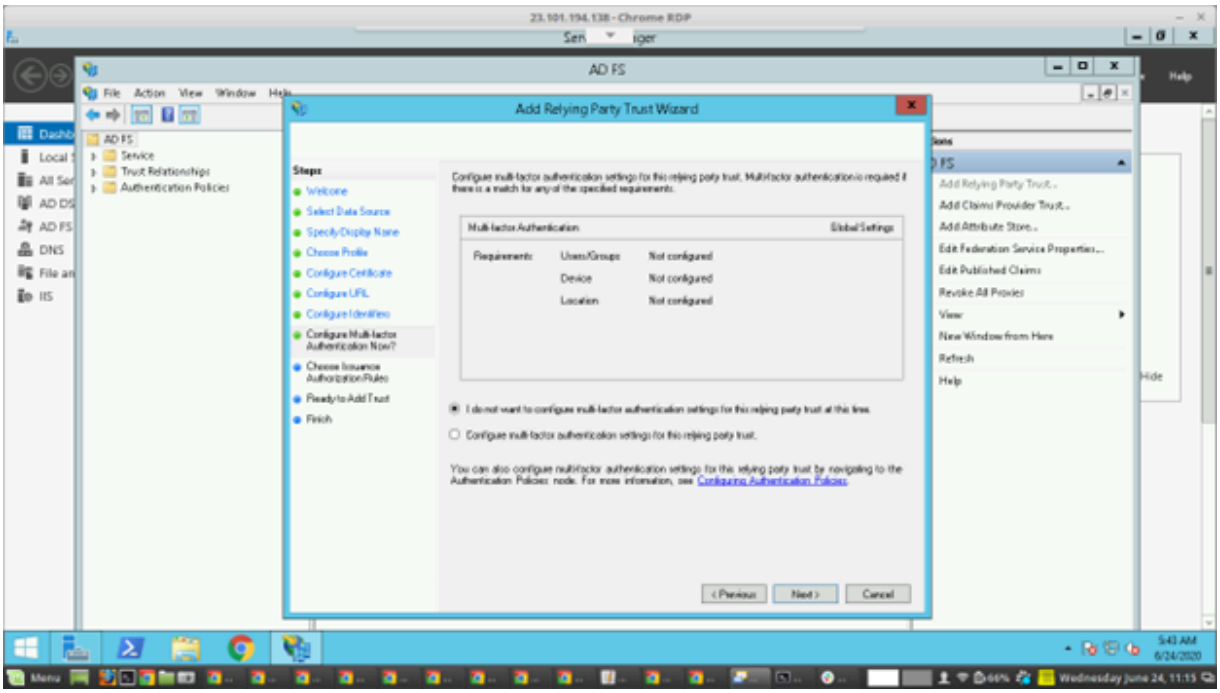
8. Under the **Configure URL** section, select the **Enable support for SAML 2.0 WebSSO protocol** option and enter the AppViewX Service URL which was copied in the previous step of Enabling SSO in AppViewX and click **Next**.



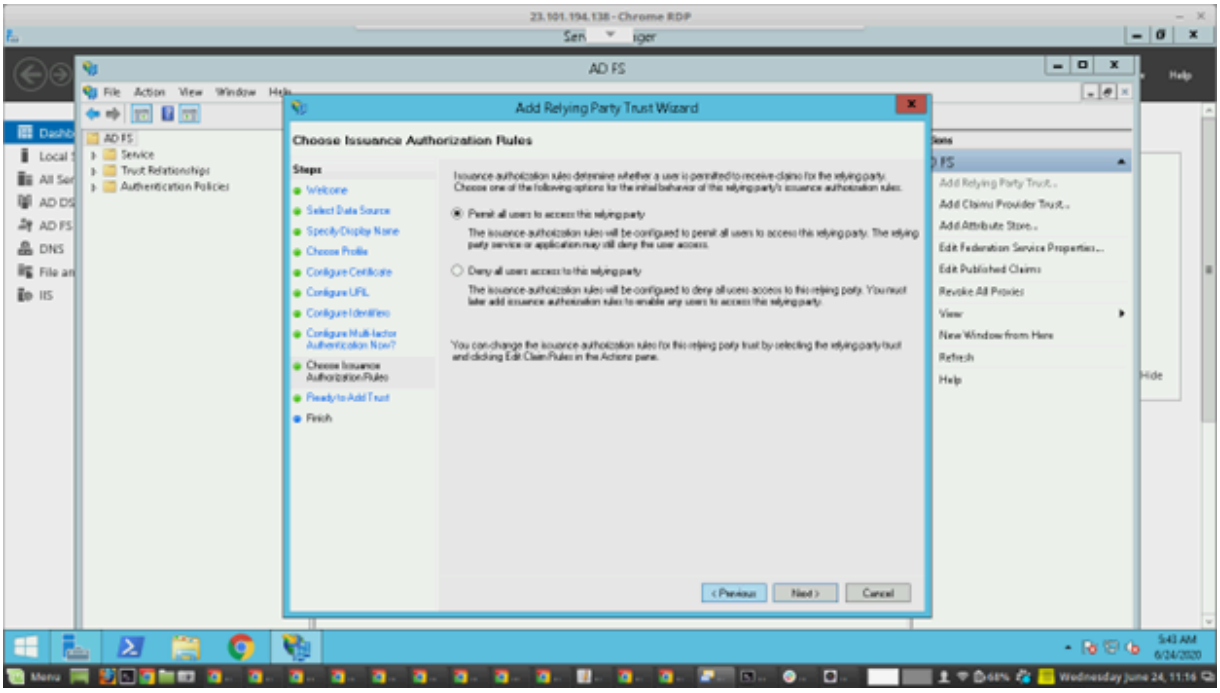
9. Under the **Configure Identifiers** section. enter the **AppViewX Entity ID** which was copied in the previous step of Enabling SSO in AppViewX and click **Add**.



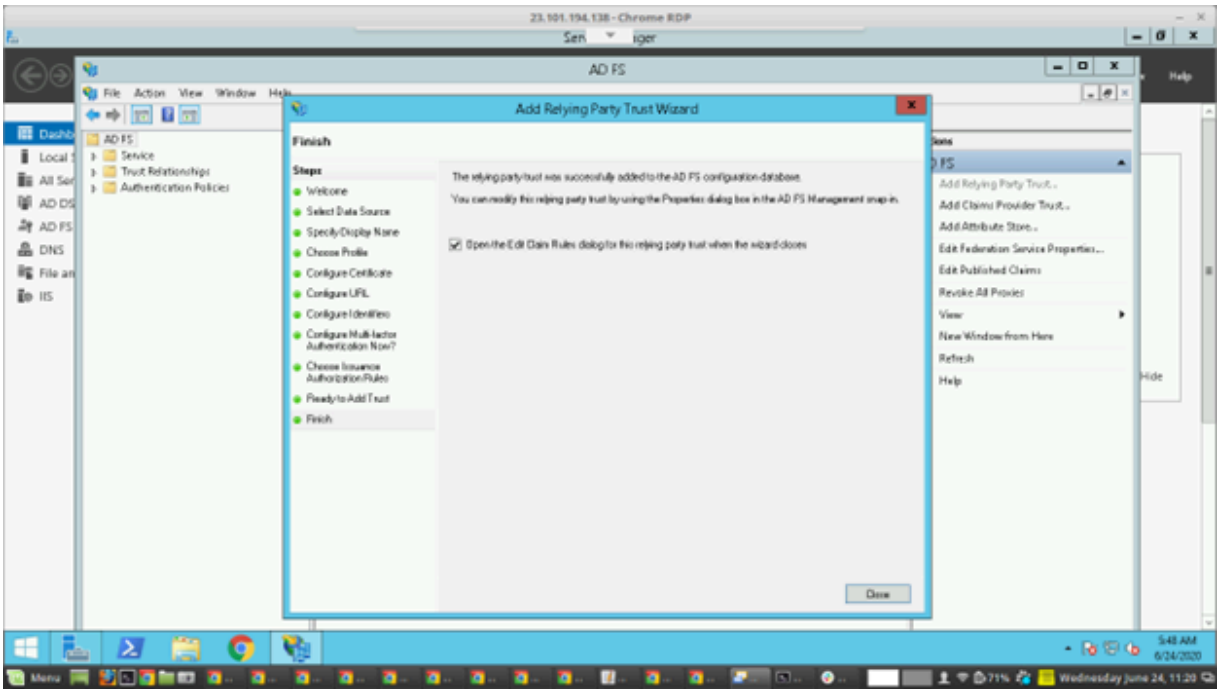
10. Click **Next**.
11. Under the **Choose Multi-factor Authentication** section, select the **I do not want to configure multi-factor authentication settings at this time** option. If the organization has a multi-factor authentication setting, enable it and click **Next**.



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



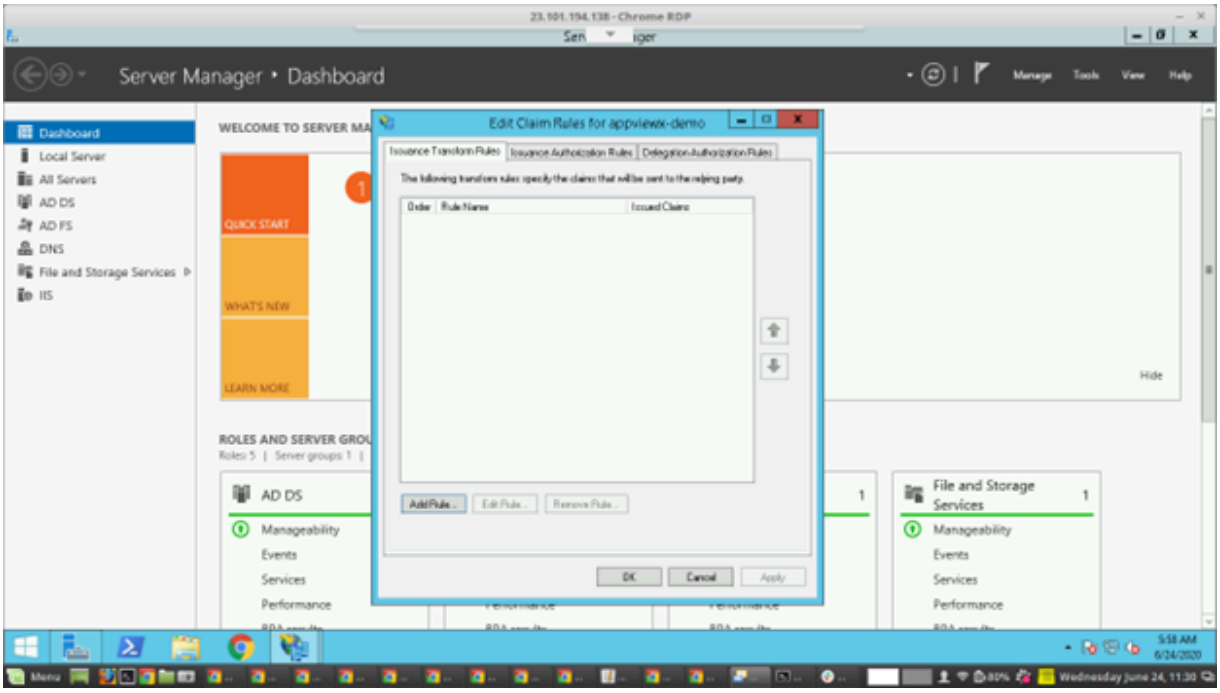
13. Under the **Ready to Add Trust** section, review the configuration done in the wizard and click **Next**.
14. Under the **Finish** section, select the **Open the Edit Claims** checkbox and click **Close**.



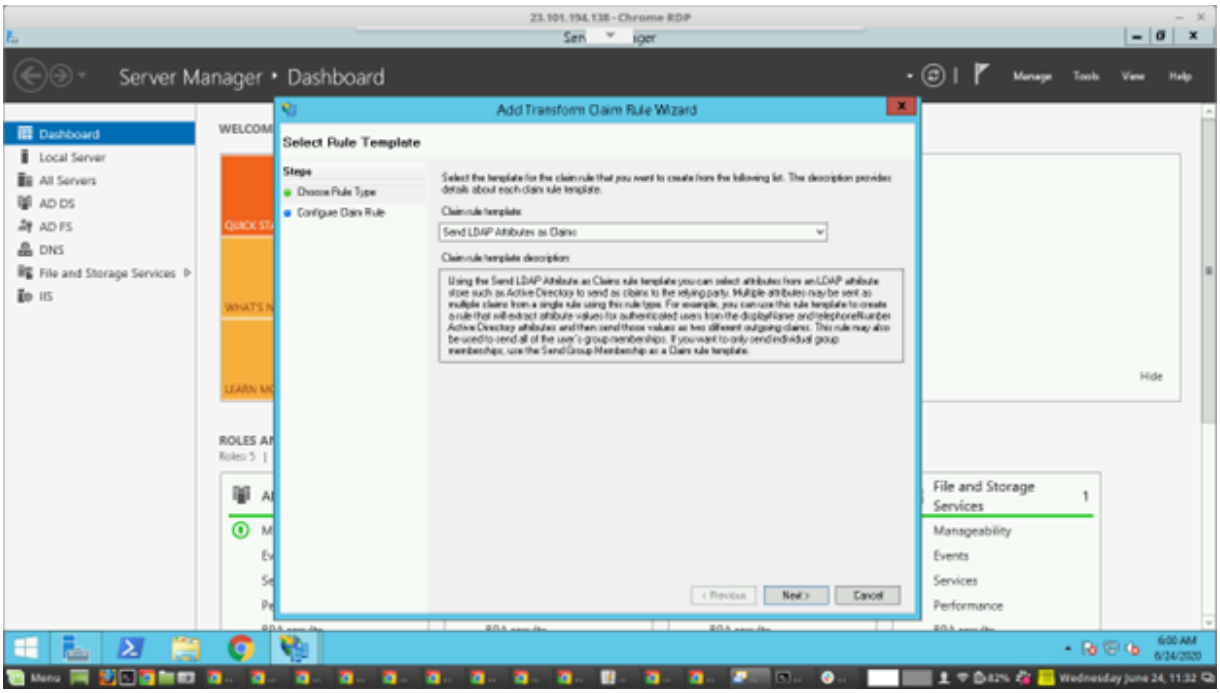
Add Claim Rules

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**.

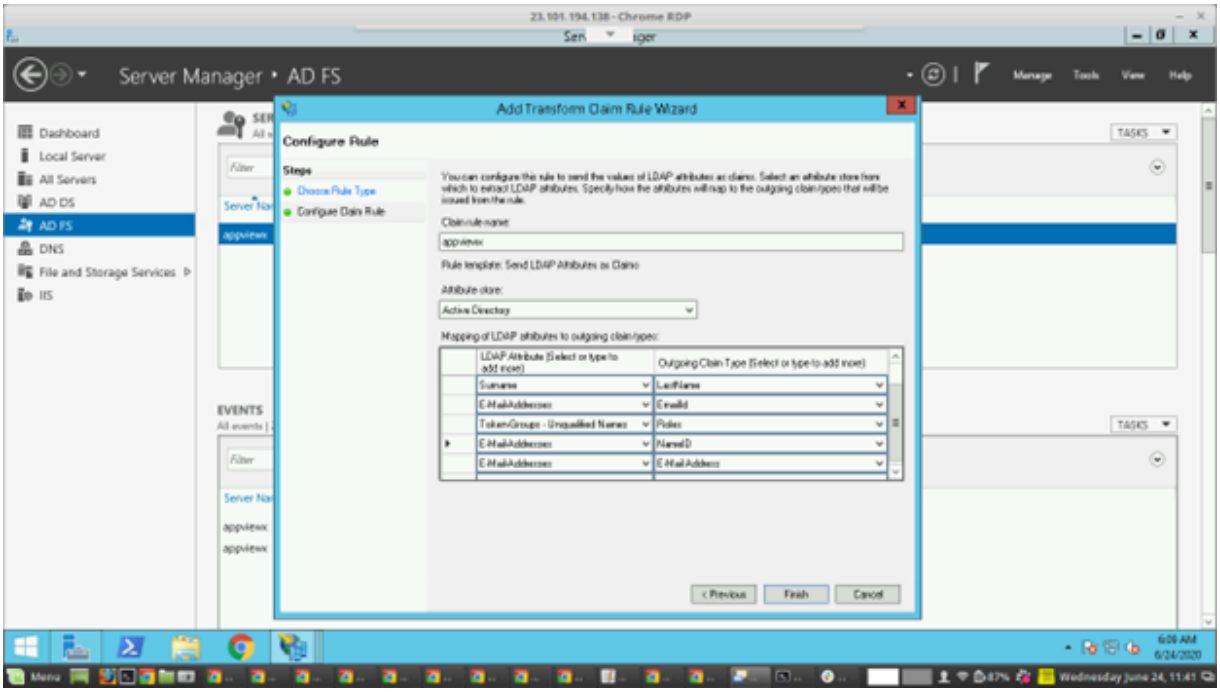


3. Enter a **Rule name** and select the **Attribute store** as **Active Directory**.

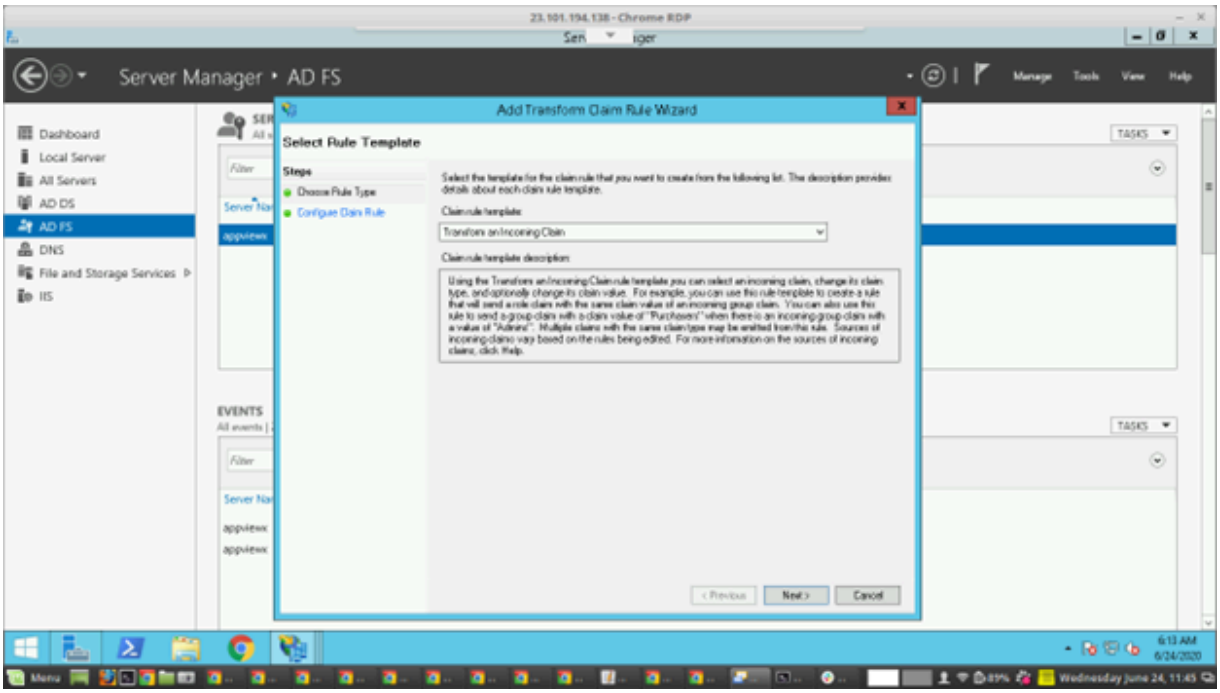
4. Enter the claim types as below and click **Finish**.

   Display-Name > FirstName, Surname > LastName, E-Mail-address > EmailId, Token-Groups-Unqualified Names > Roles, E-Mail-address > NameID, E-Mail-address > E-Mail-address.

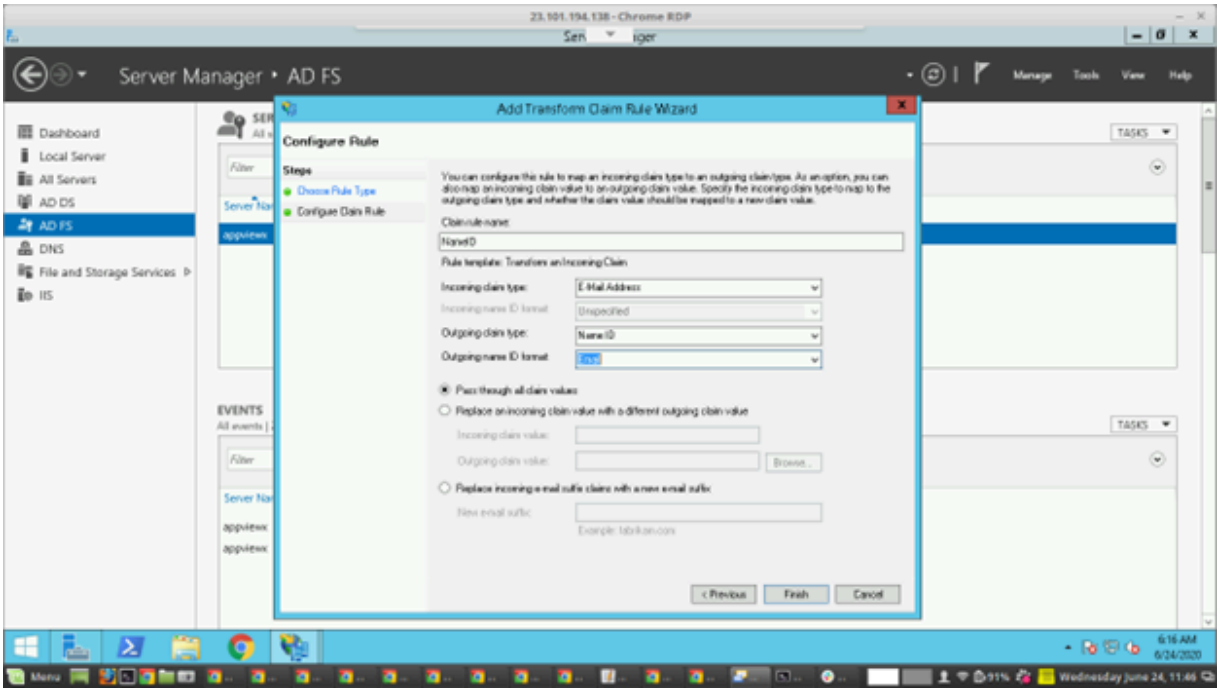
5. Create another rule to transform the incoming claim by clicking **Add Rule** > **Rule Template** (Transform an Incoming Claim) and click **Next**.



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 click **Finish**.

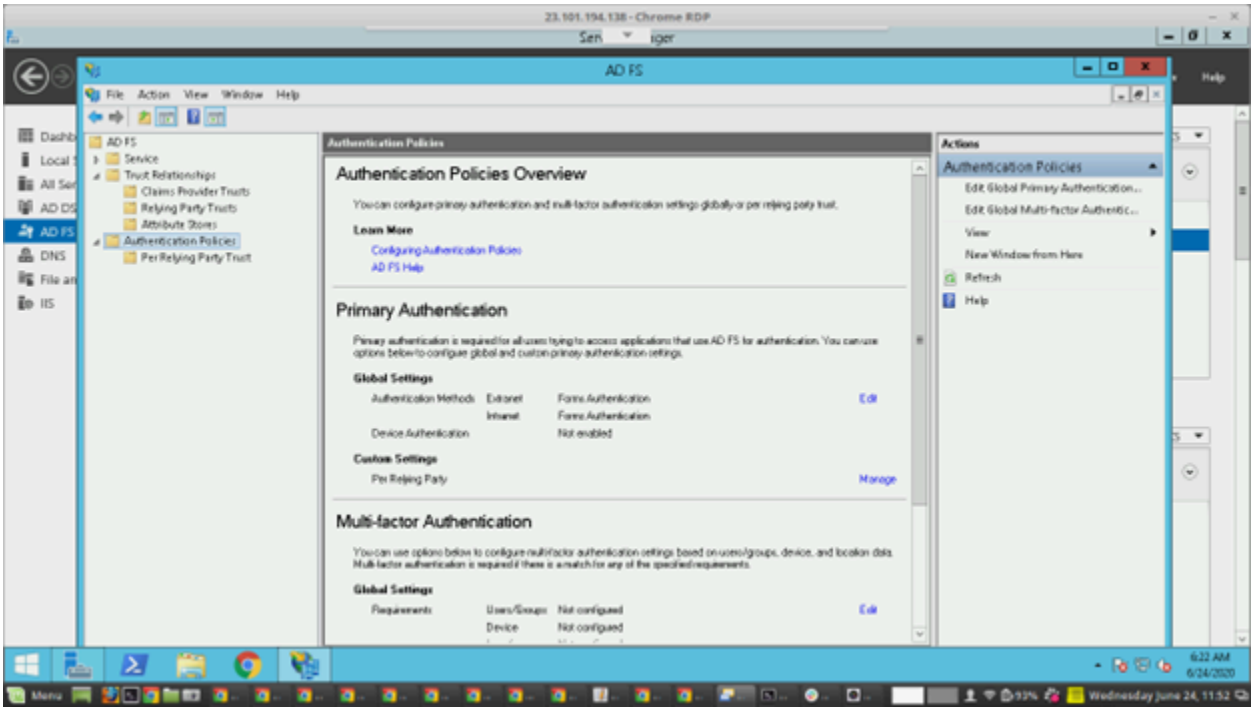


7. In the **Edit Claims** pane, click **Apply** and **OK**.



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:

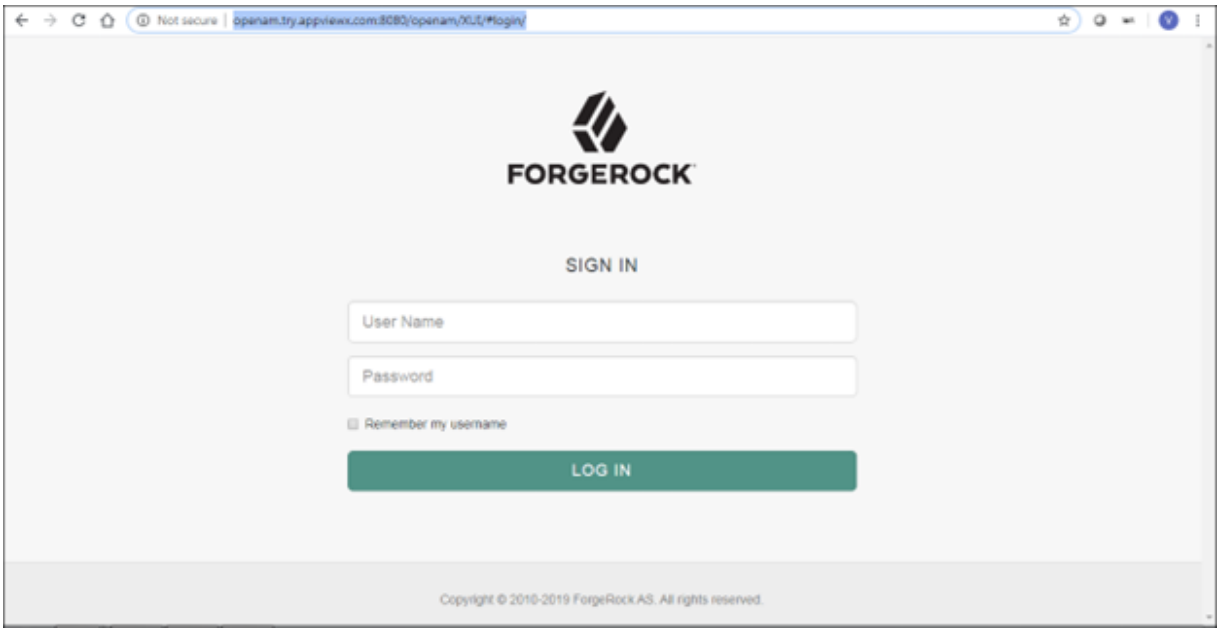
https://appviewx.westus.cloudapp.azure.com/federationmetadata/2007-06/federationmetadata.xml

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.

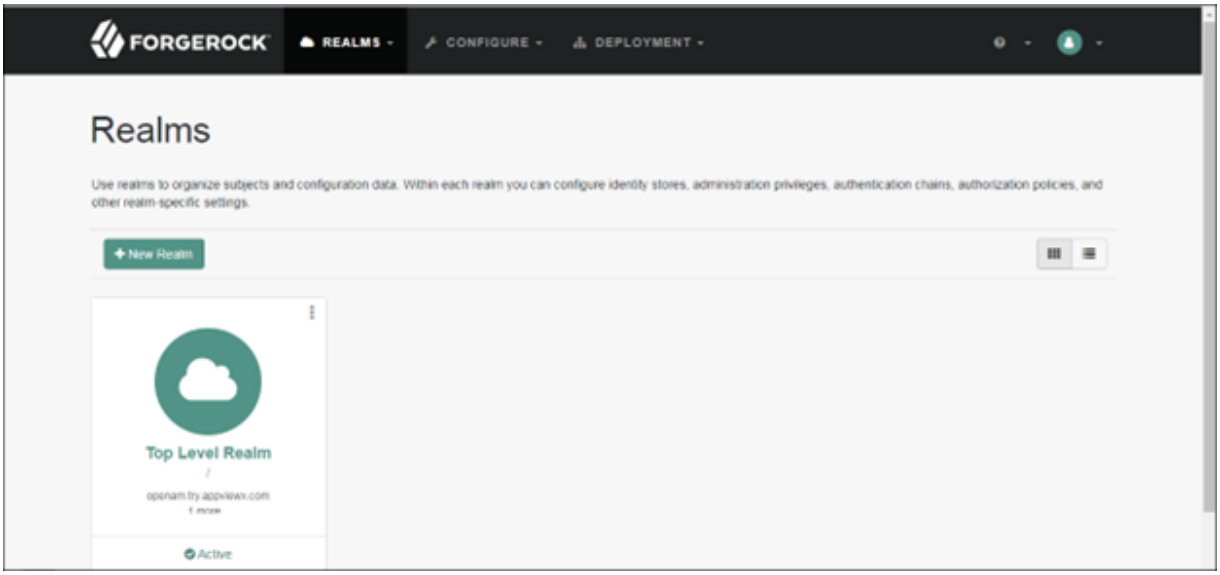
Sample IDP initiated URL: https://appviewx.westus.cloudapp.azure.com/adfs/ls/idpinitiatedsignon

Forgerock Integration

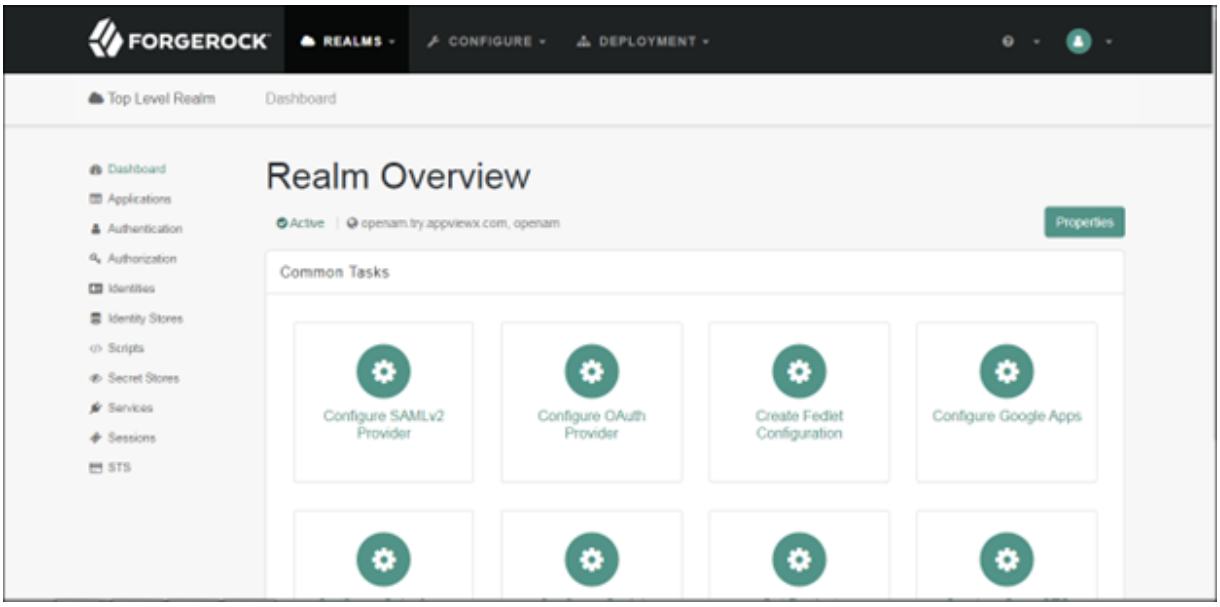
1. Login to the Forgerock IDP intense / console.



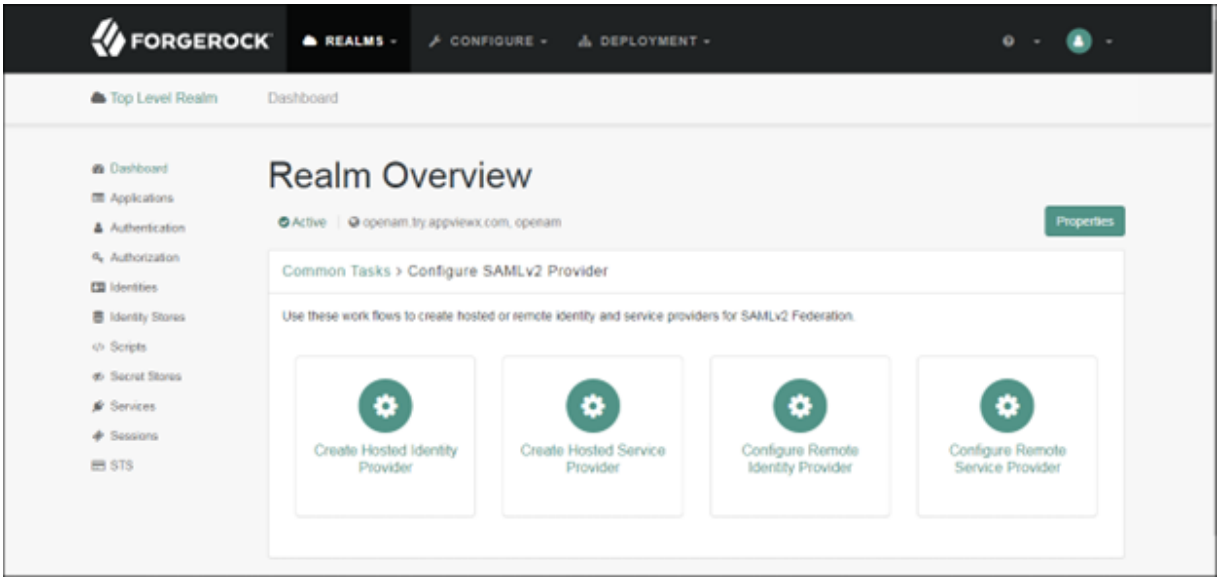
2. Select the respective Realm.



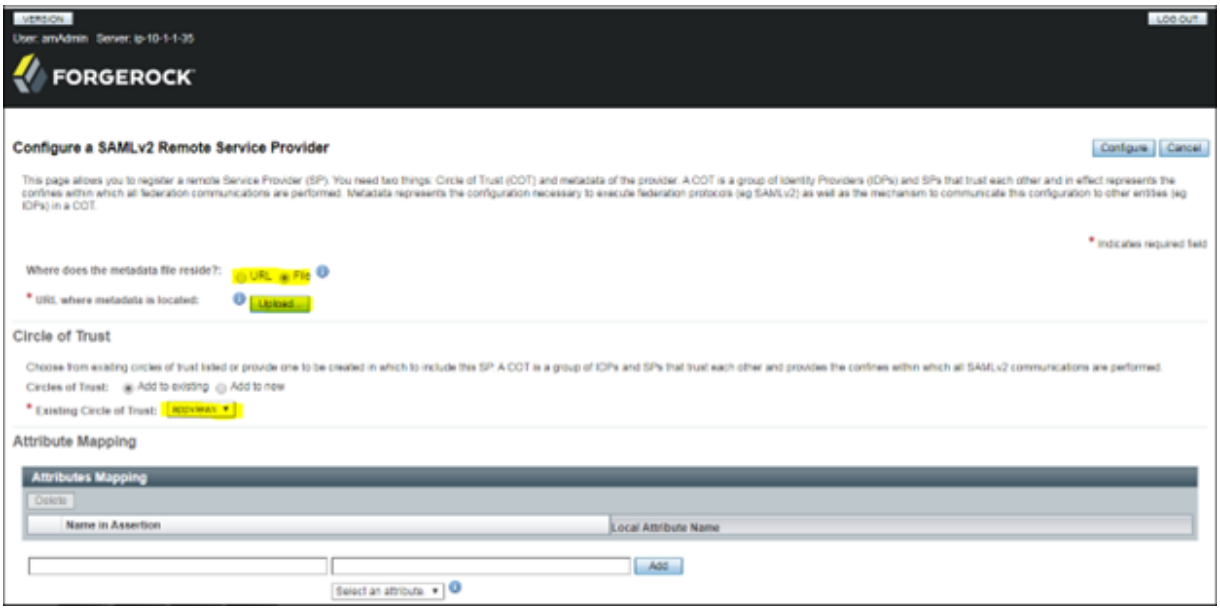
3. Under **Common Tasks**, select **Configure SAML v2 provider**.



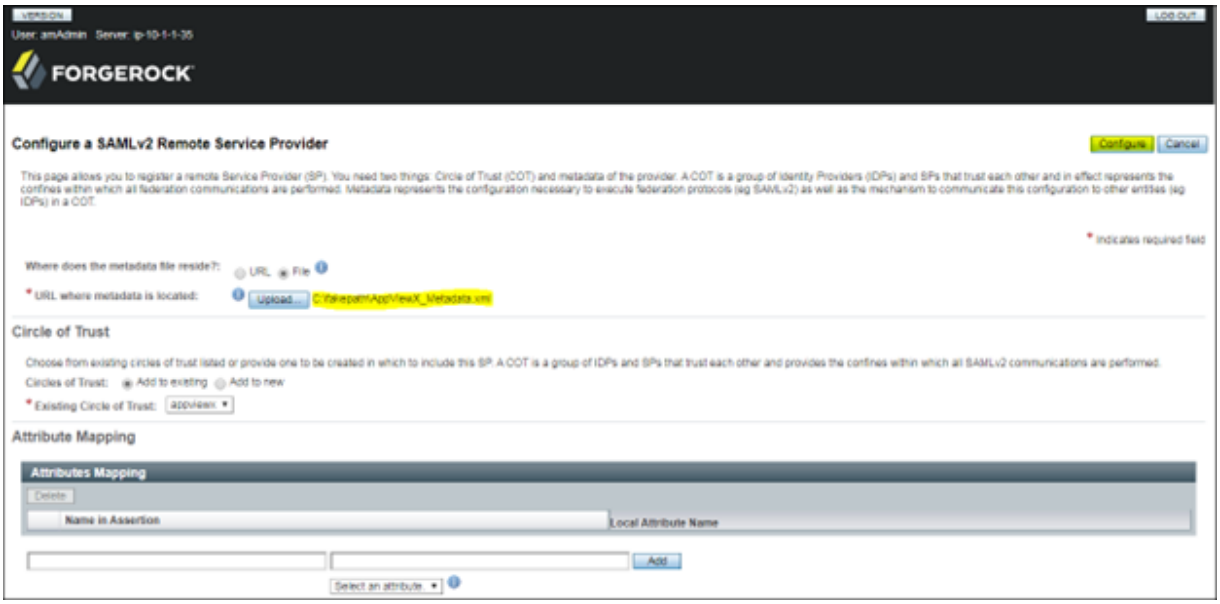
4. For Configuring AppViewX configuration, select **Configure Remote Service Provider**.



5. For metadata upload, select the **File** option and select/create the circle of trust for mapping AppViewX to the IDP and click **Upload**.

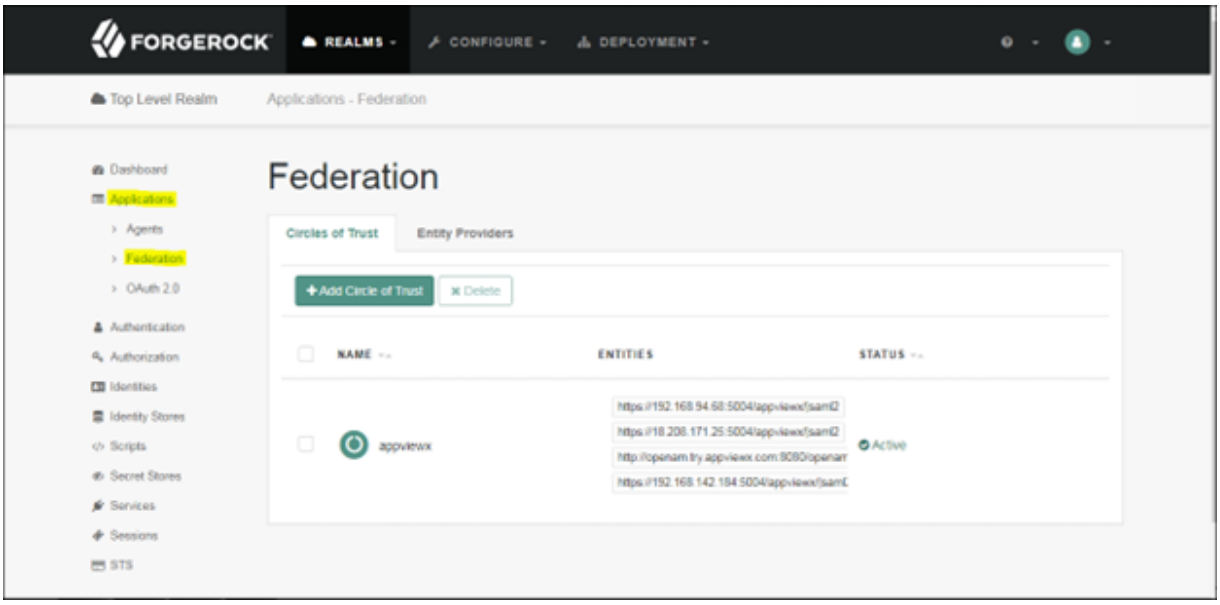


6. Upload the AppViewX metadata which was downloaded earlier and click **Configure** to save the settings.

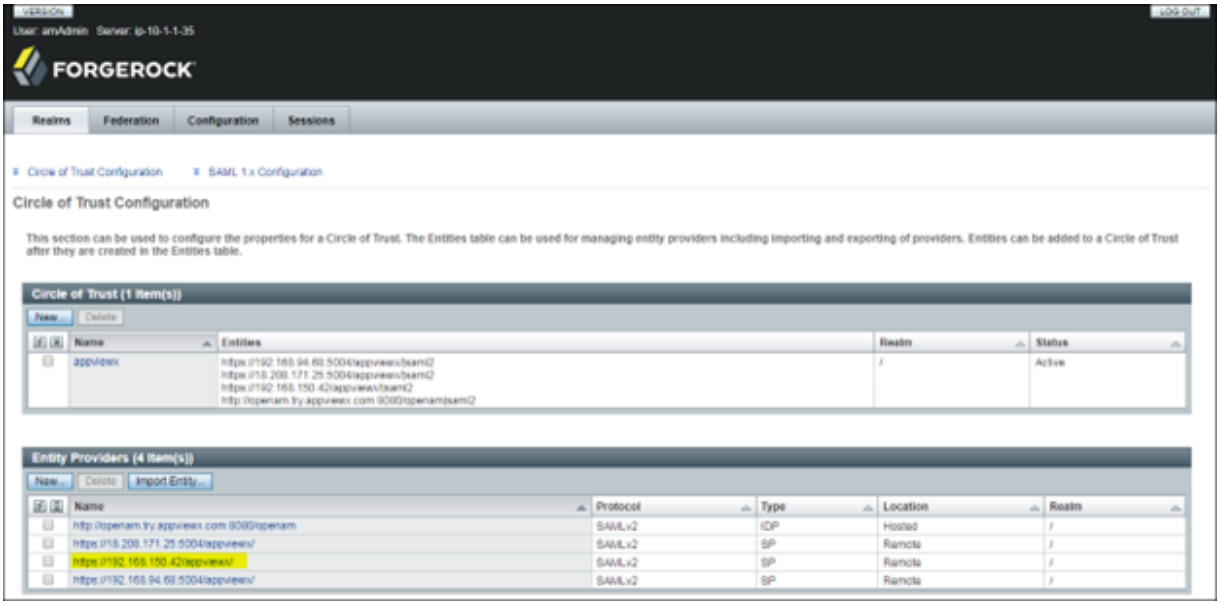


The page will redirect to the common tasks under the specific realm.

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



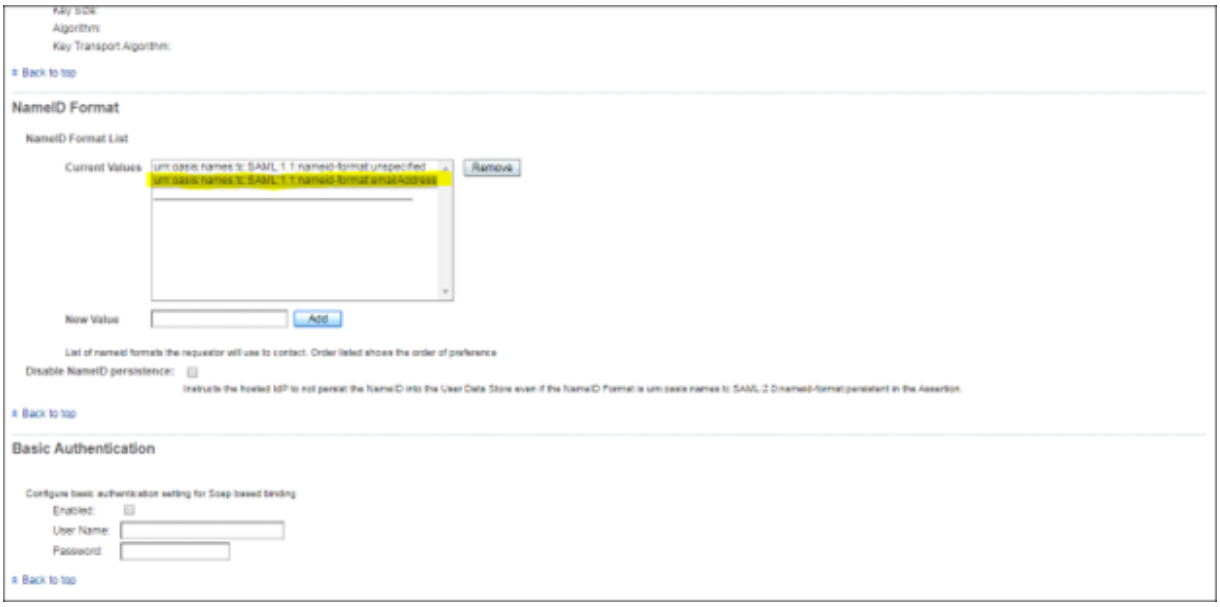
8. Select the entity providers tab.



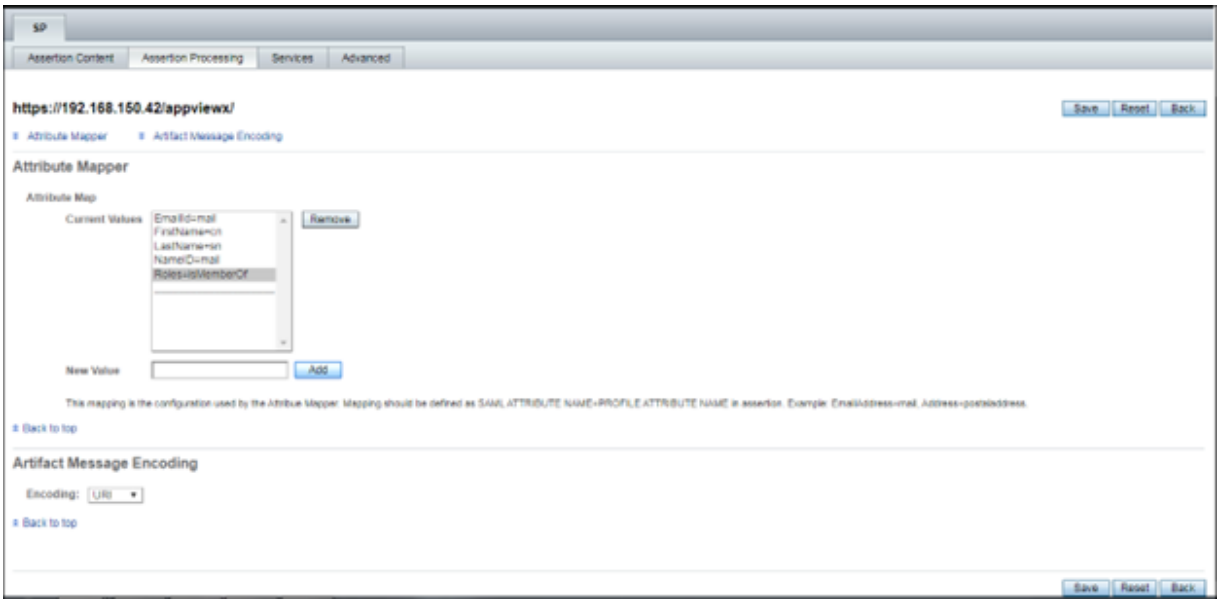
This will redirect to the Federation tab with the list of Service providers and IDP configuration.

9. Select the respective Entity ID to navigate to the settings of the respective entity configuration.
10. On the **Assertion Content** tab, add the following in the NameID Format and click **Save** on the top right.

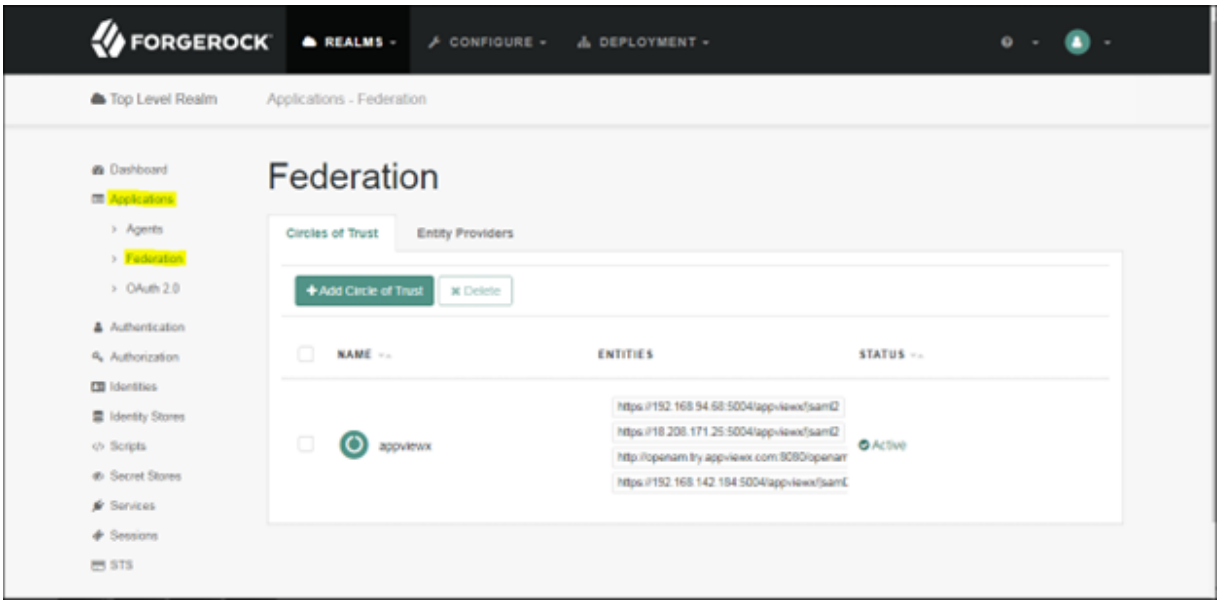
    urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress



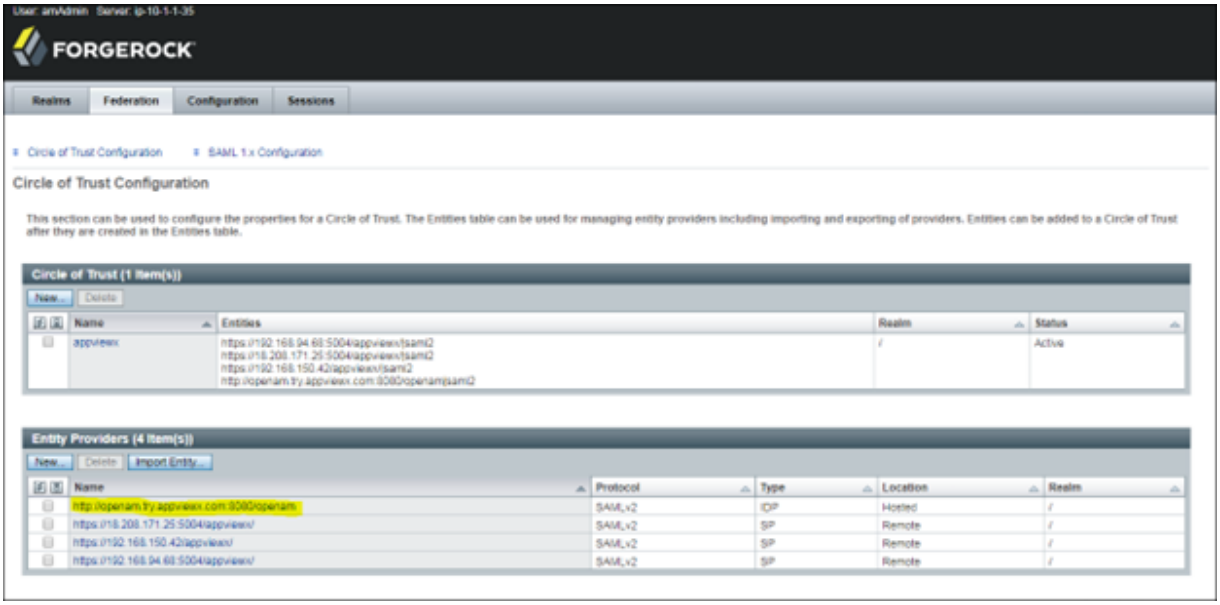
11. On the **Assertion Processing** tab, add the below assertion parameter which has to be passed as a part of the SAML assertion and click **Save**.
    EmailId=mail ; FirstName=cn ; LastName=sn ; NameID=mail ; Roles=isMemberOfAuthentication.



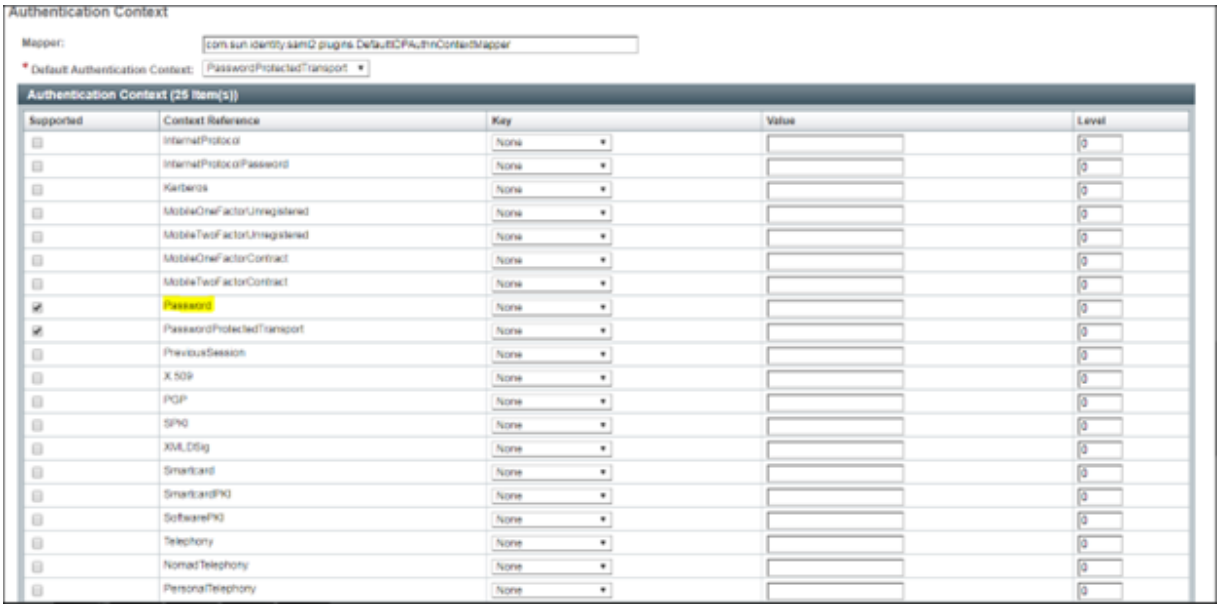
12. Modify IDP configuration to accept a password-based Authentication Context.
13. Navigate to **Applications** > **Federation** and select Entity Provider TAB.



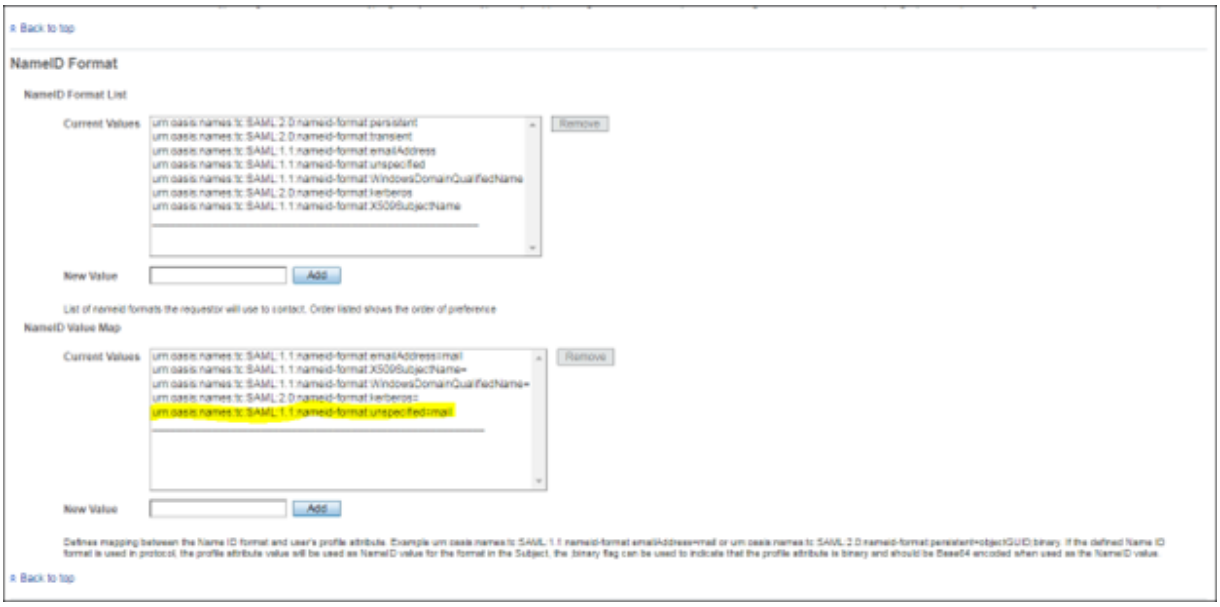
14. Under the **Federation** tab, select the IDP config under **Entity Providers**.



15. Under the **Authentication Context** section, check the Password-based context.



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

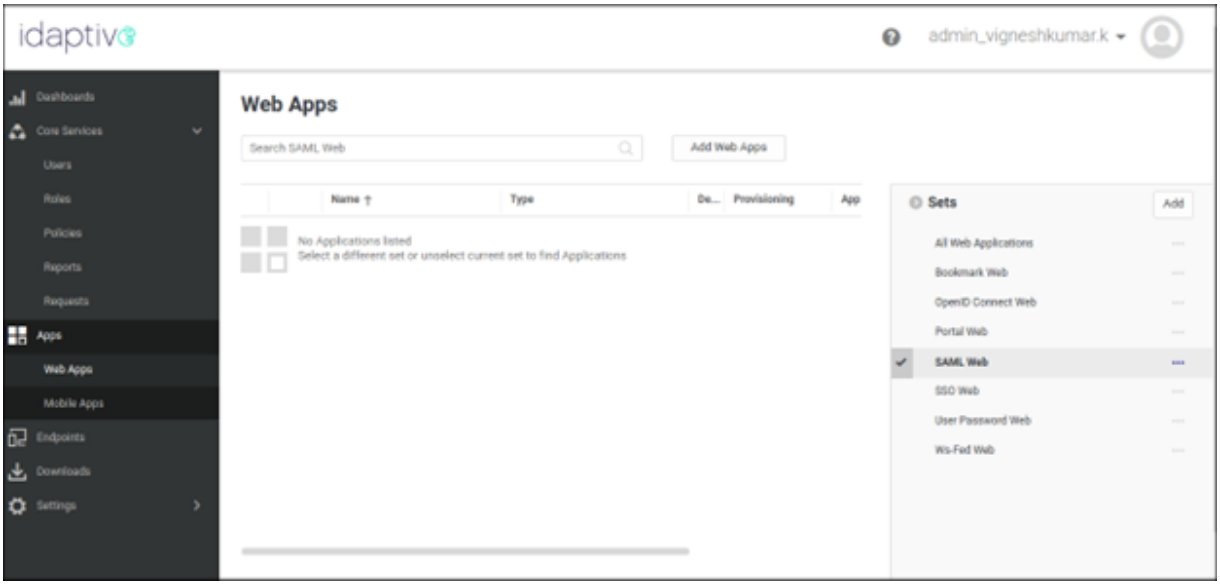


17. Now access AppViewX with the SSO authentication with Forgerock.
18. Export IDP metadata and upload it in AppViewX SSO settings. To export metadata using the IDP URL and save it as an XML file. **Sample URL:**http://openam.try.appviewx.com:8080/openam/saml2/jsp/exportmetadata.jsp?entityid=http://openam.try.appviewx.com:8080/openam

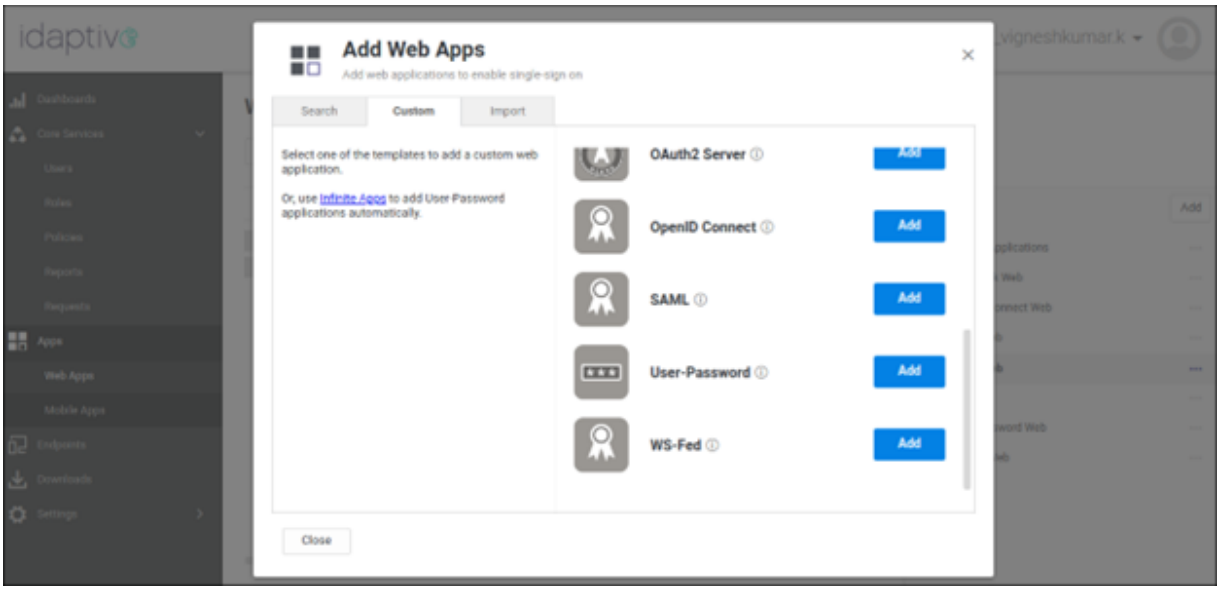
Note: Role name passed in as a part of the SAML assertion should be configured in appviewx on the Accounts > UserGroup and assign a role for accessing the application. For an IDP initiated SSO the following structure like URL should be used. **Sample IDP initiated URL:** http://openam.try.appviewx.com:8080/openam/idpssoinit?metaAlias=/idp&spEntityID=https://192.168.x.x:31443/appviewx/

Idaptive Integration

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

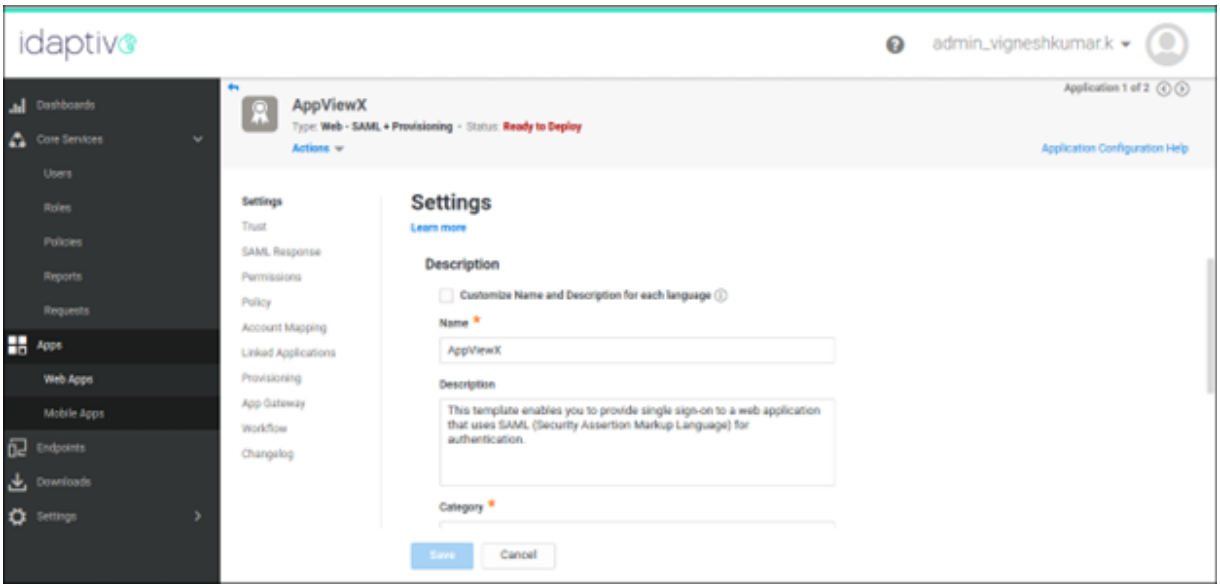


4. Click **Add Web Apps**.
5. In the **Add Web Apps** window, under the **Custom** tab, click **Add** for **SAML**.

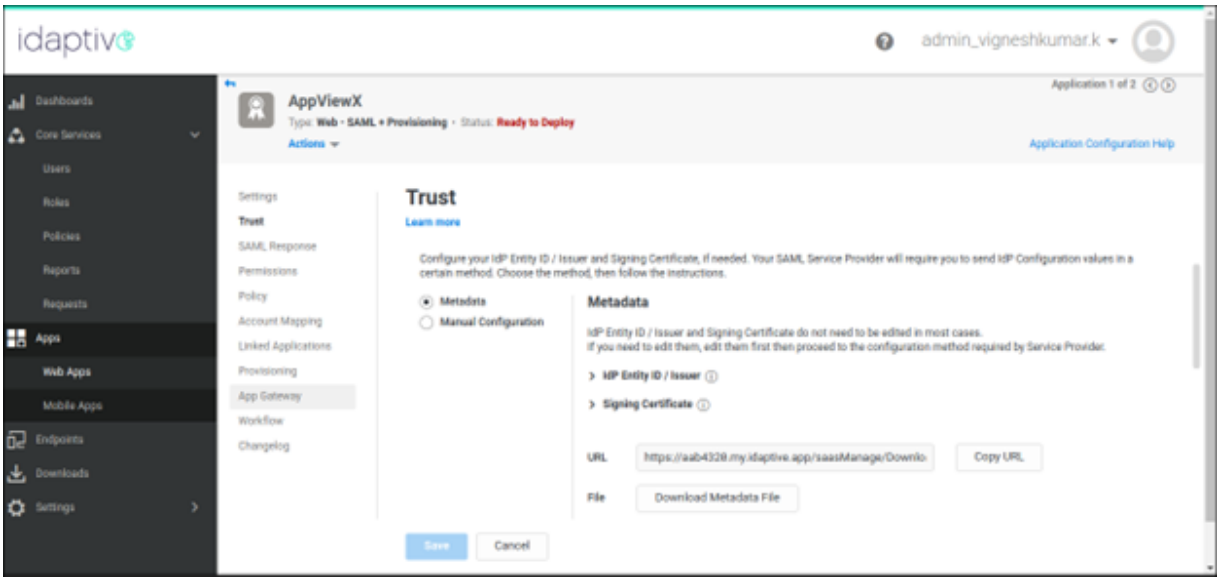


SAML app is added to the Web Apps Inventory.

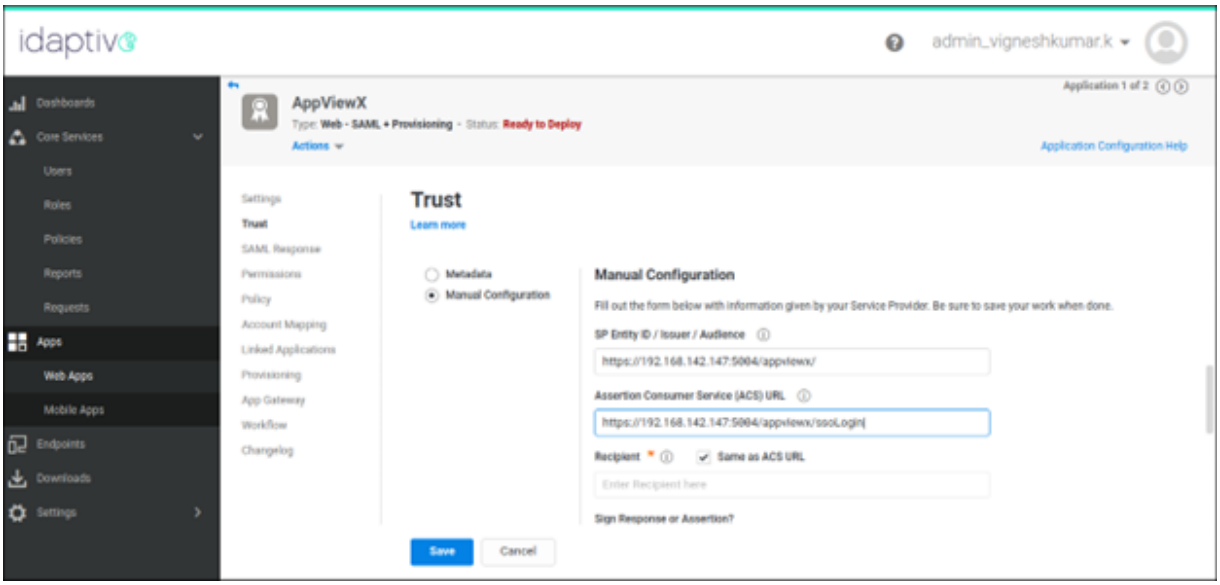
6. Select the SAML app in the Web Apps Inventory and proceed with the configuration.
7. In the **Settings** tab, enter the name for the app as **AppViewX** and save the configuration.



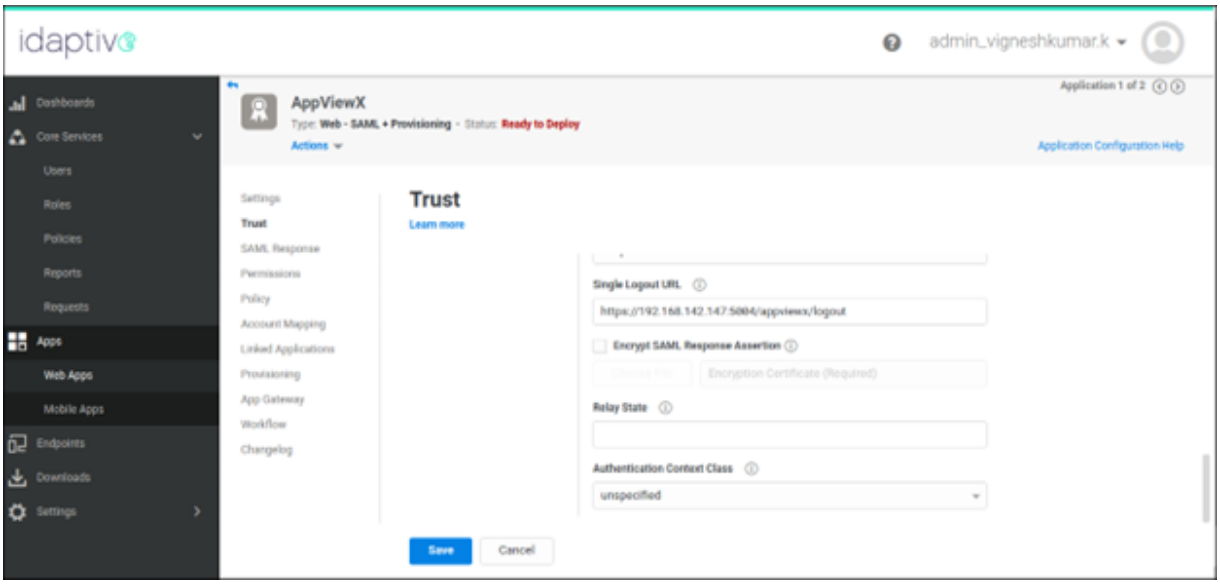
8. In the **Trust** tab, click **Download Metadata File**.



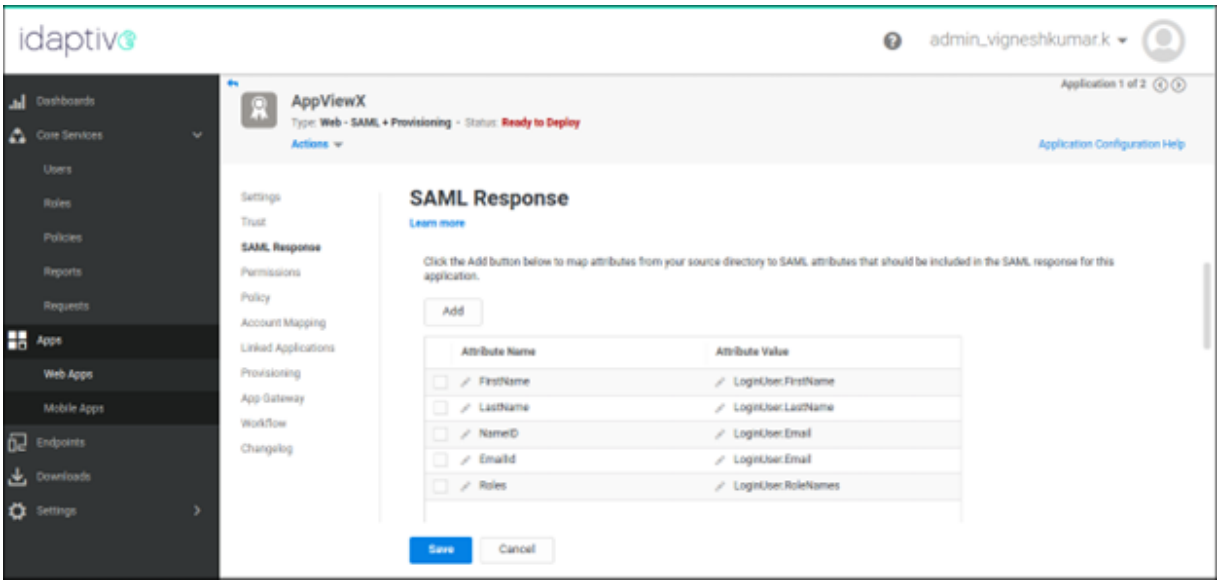
9. Select the **Manual Configuration** option.
10. Copy and paste the Entity ID URL from AppViewX on the SP Entity ID field in Idaptive portal and the Service URL from AppViewX on the ACS URL field in the Idaptive portal.



11. Check if the Recipient checkbox is the same compared to the ACS URL. Leave the rest of the settings to default. Configure the Single Logout URL field with the value copied from the SLO URL in AppViewX. **Save** the config.



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 / Security Groups).



13. Click **Save**.
14. Assign the application to the respective Role and the Role to the respective Users. Once done configure the same Role in AppViewX in the **Account** > **User Group** module and assign respective AppViewX Role permission to the User Group.
15. Now access AppViewX with the help of External login using SAML.

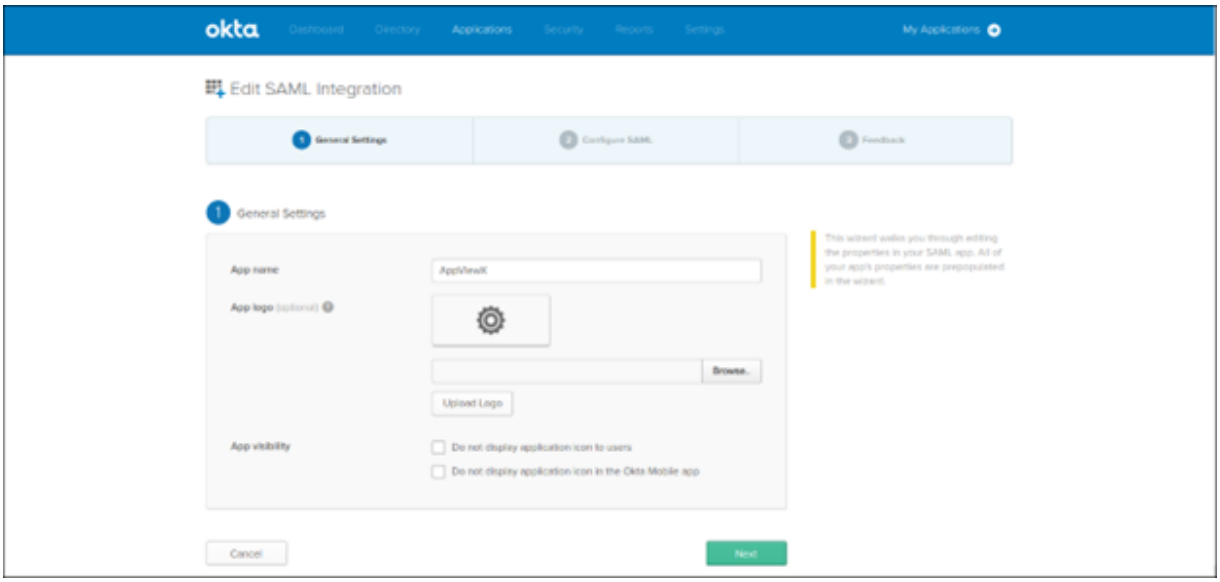
Okta Integration

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)

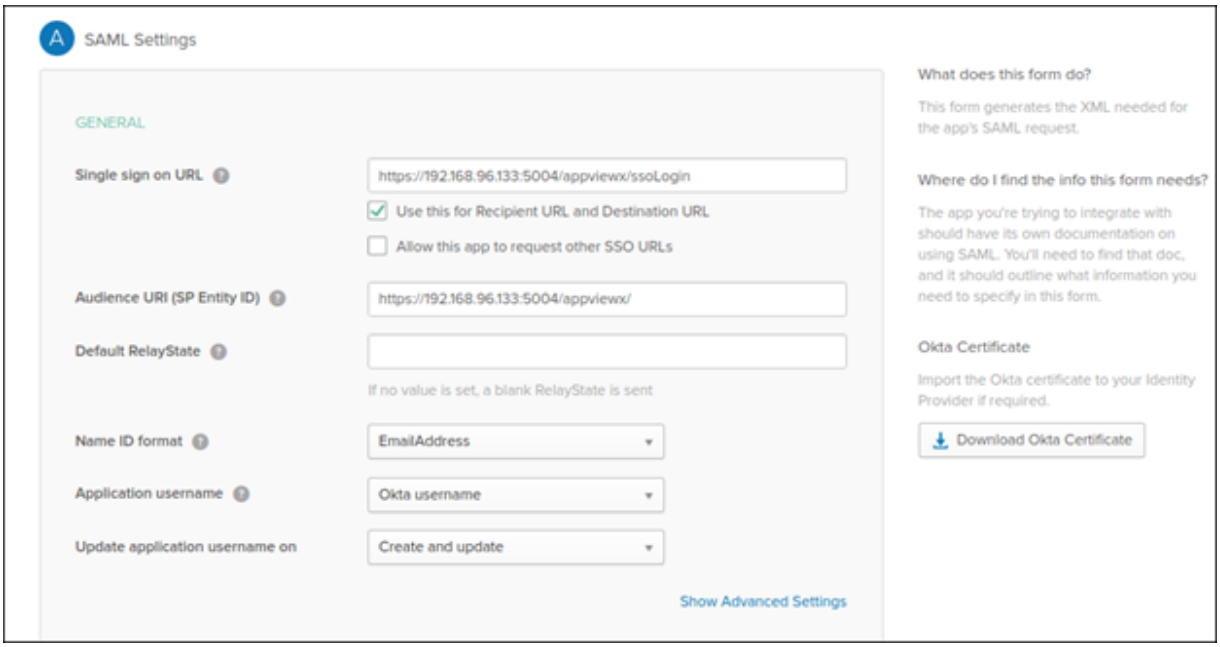
Complete the following steps to begin the IDP configuration:

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.

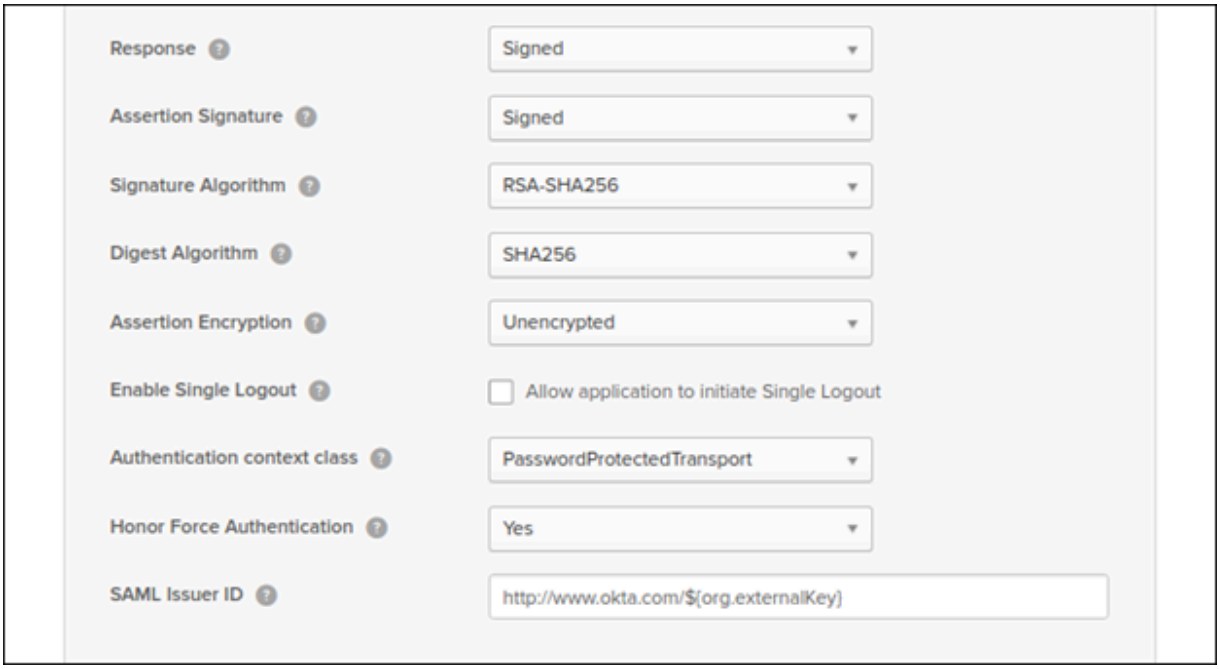
1. Create an application.



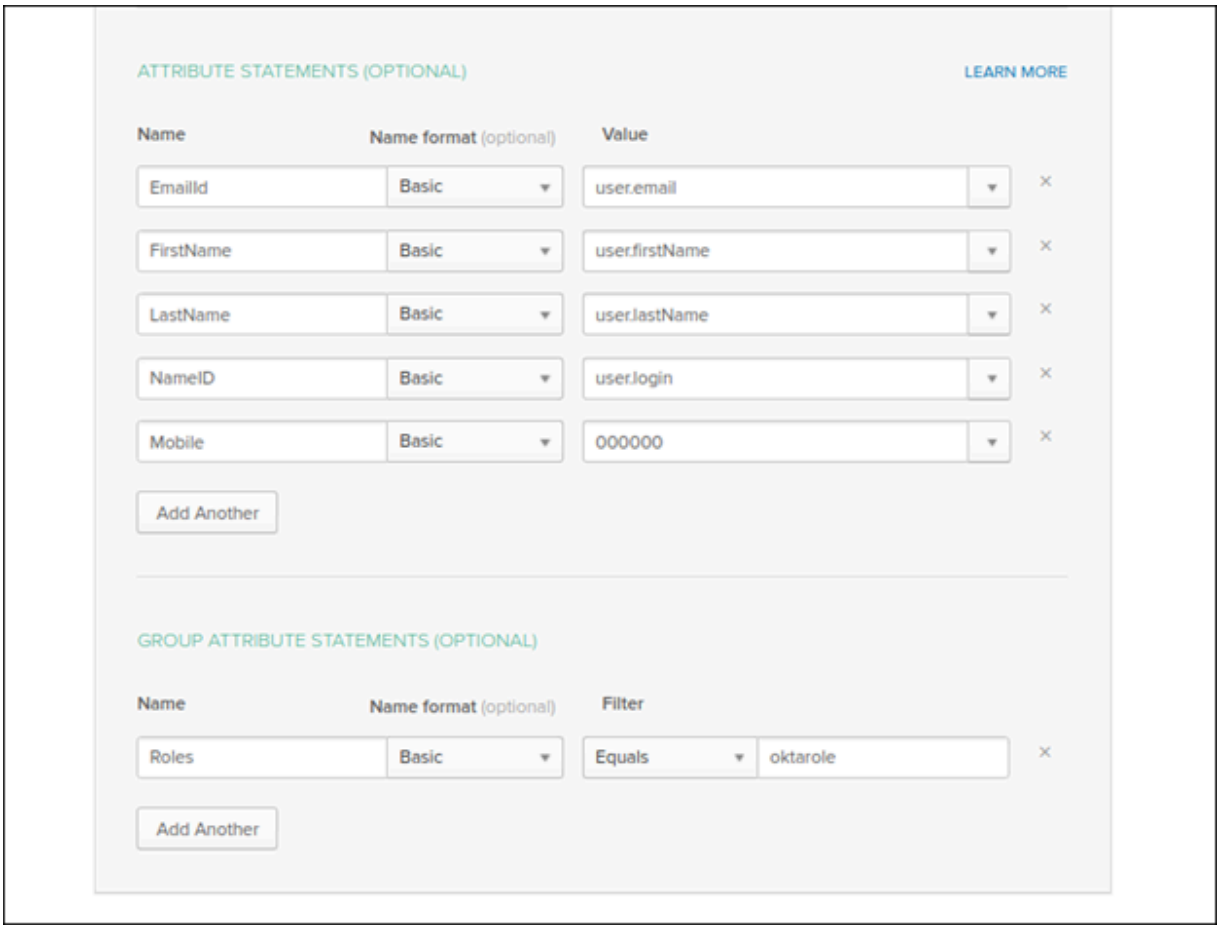
2. Configure service provider details.



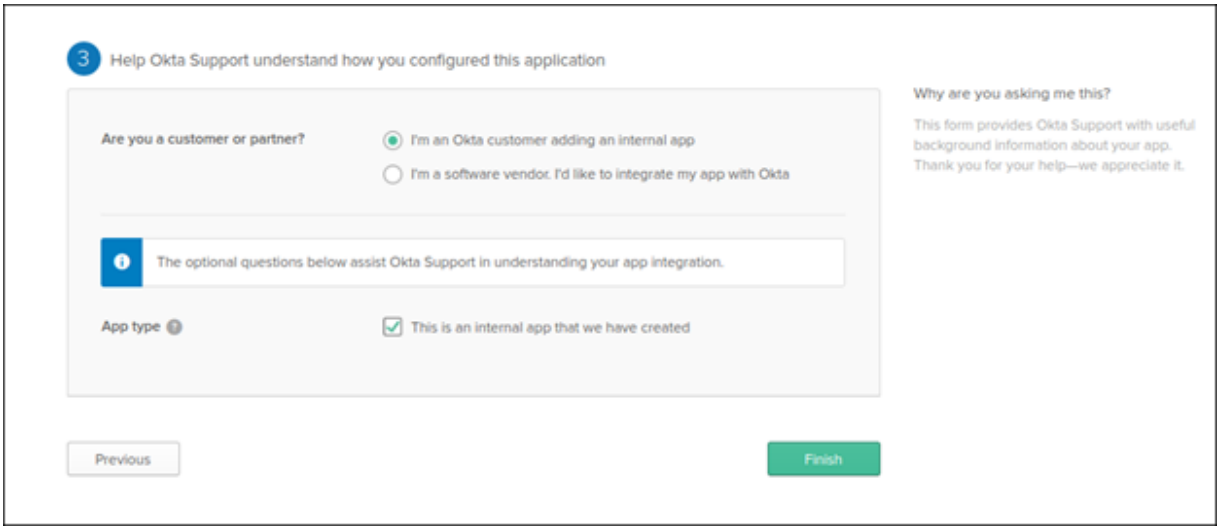
3. Show Advanced Settings screen.



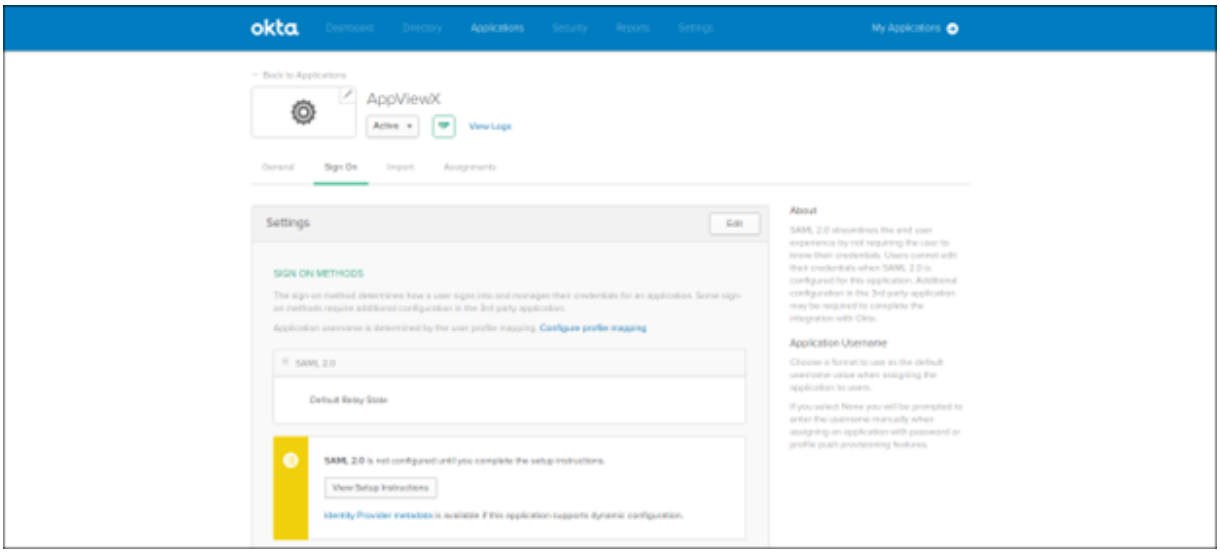
4. Configure the User Attributes to be passed during the SAML assertion.



5. Finish the IDP configuration.

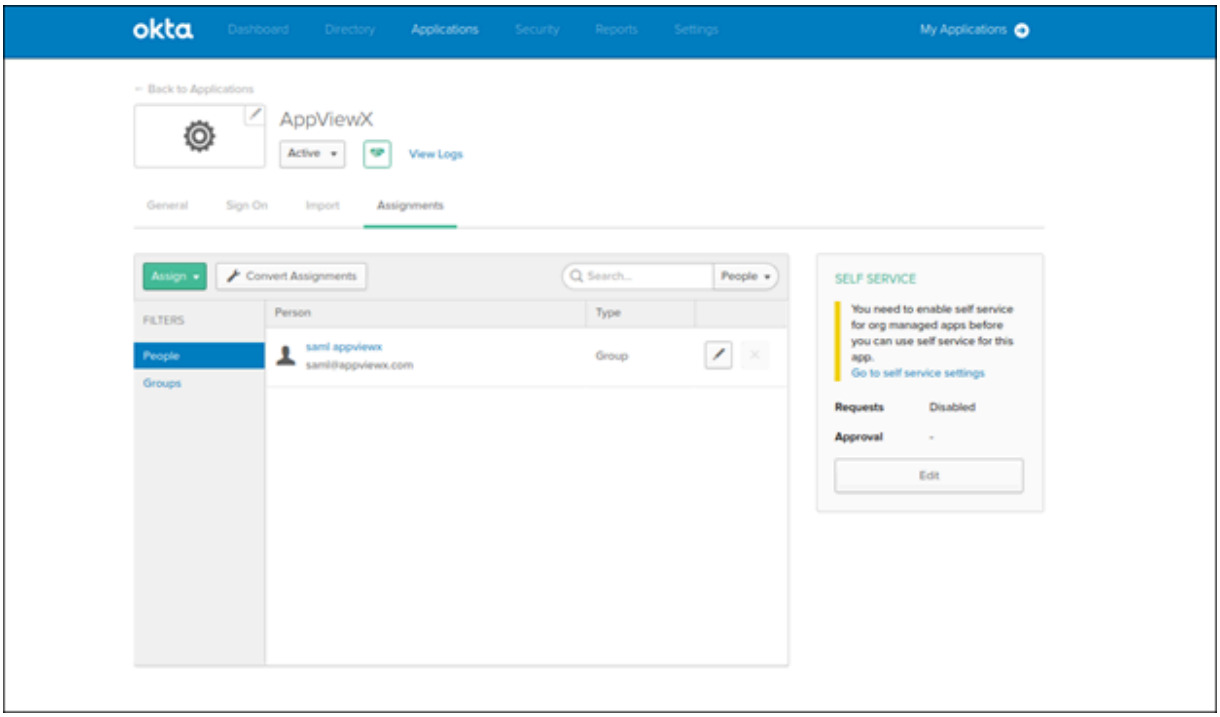


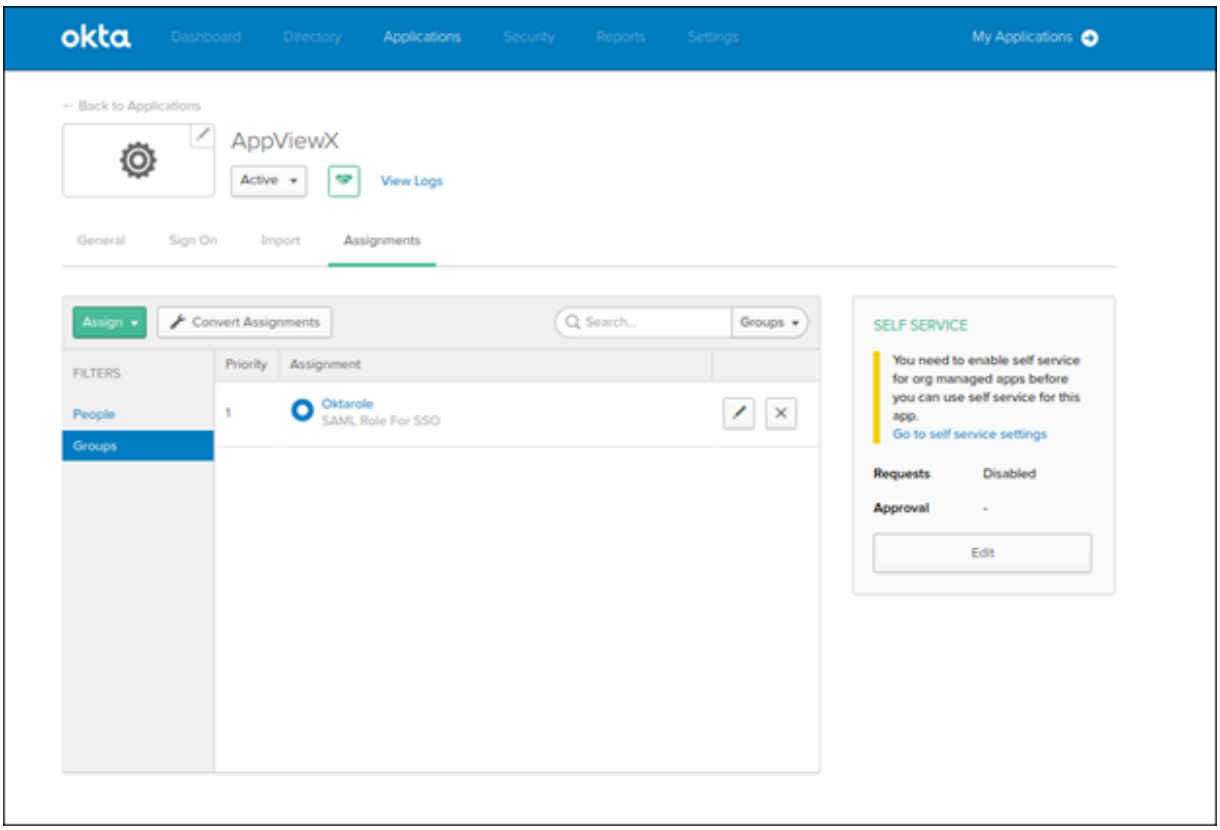
6. Click the View Setup Instructions in the Sign On tab.



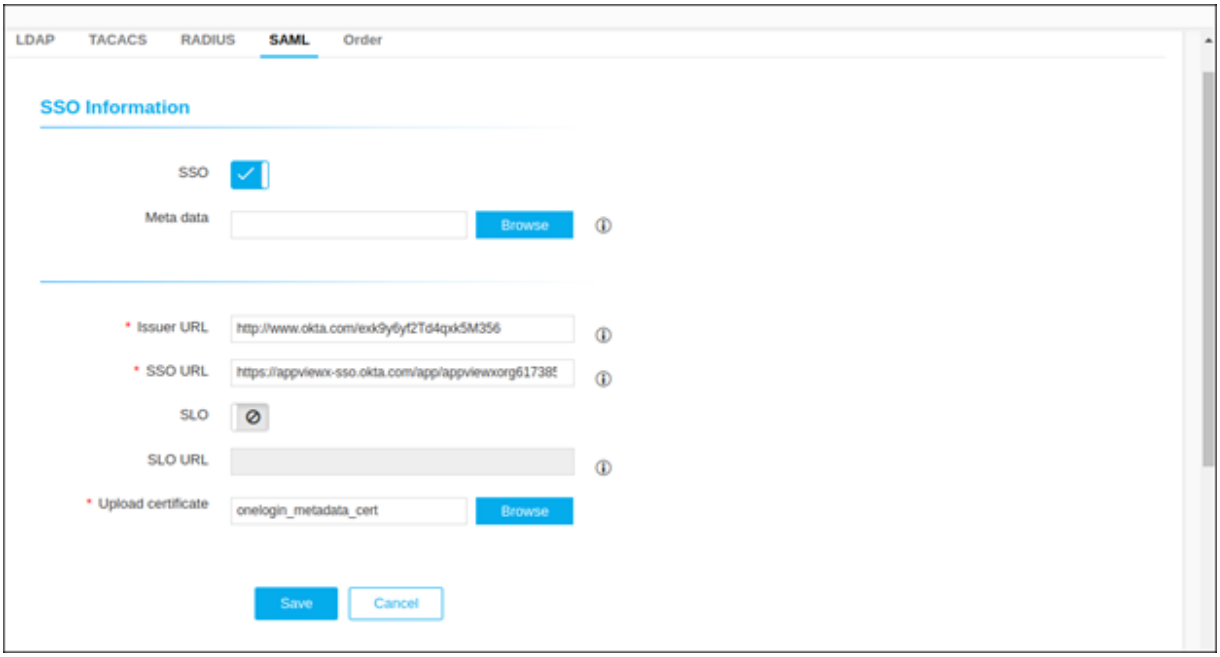
7. Copy and paste the content from the Optional section and save it as an XML file.

8. Map the application to a User/User Group.





9. Browse and upload the IDP metadata to AppViewX. Then, click Save.

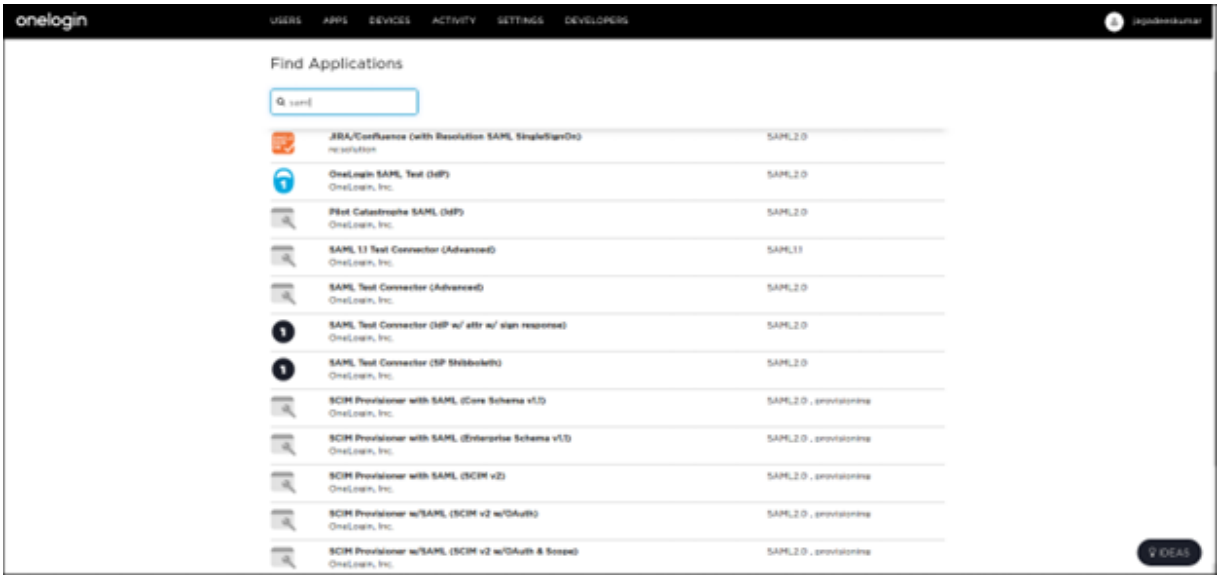


OneLogin Integration

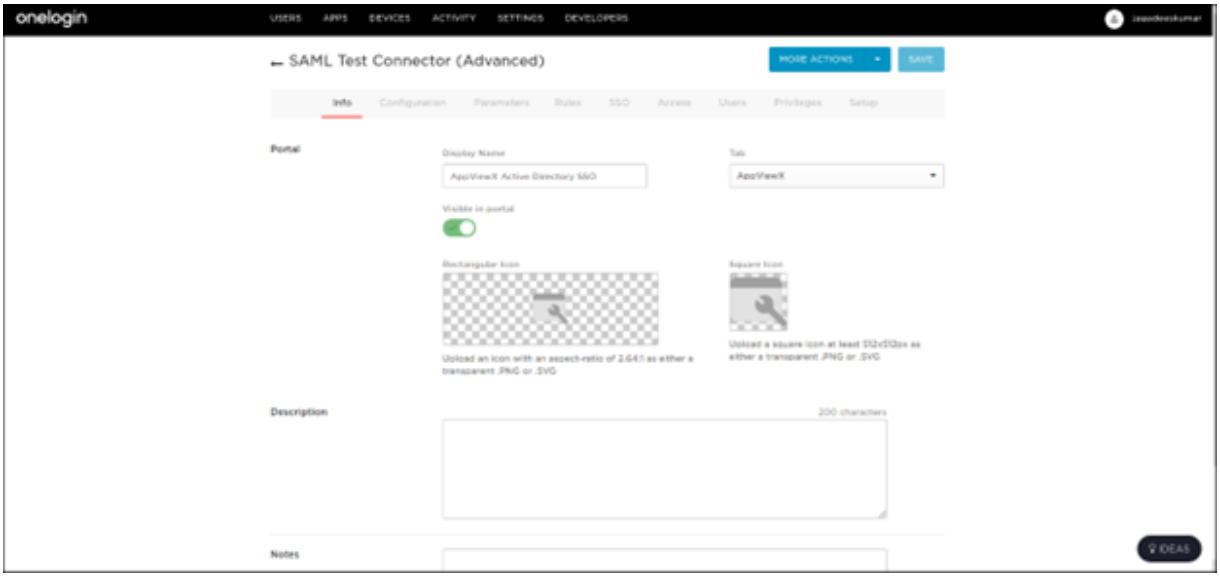
The below steps are performed at the IdP end. The navigation and screenshots might differ based on the version of the IdP. (This is just an example configuration)

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

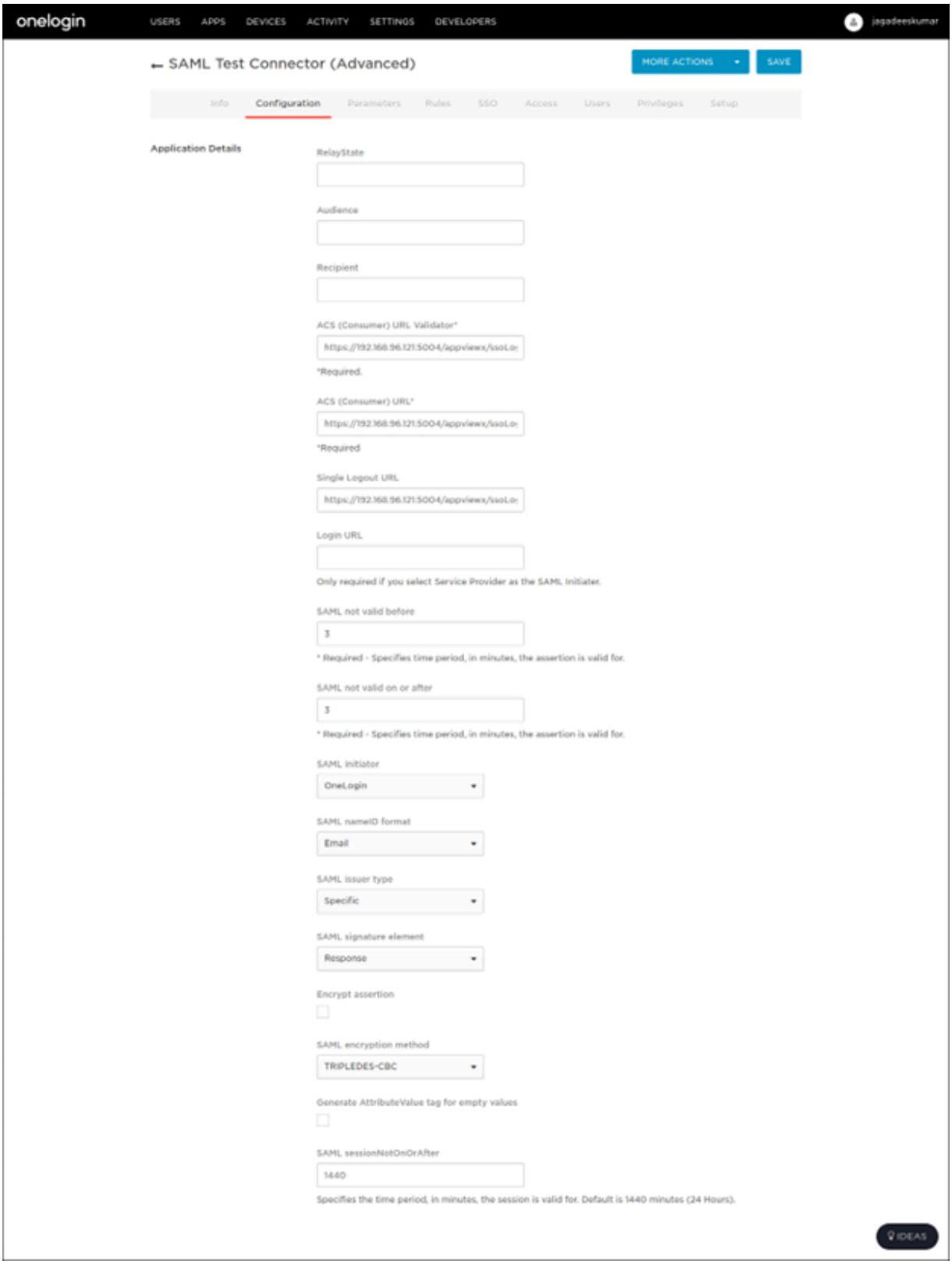
1. Create a new application. Click Add application and search for SAML Test Connector.



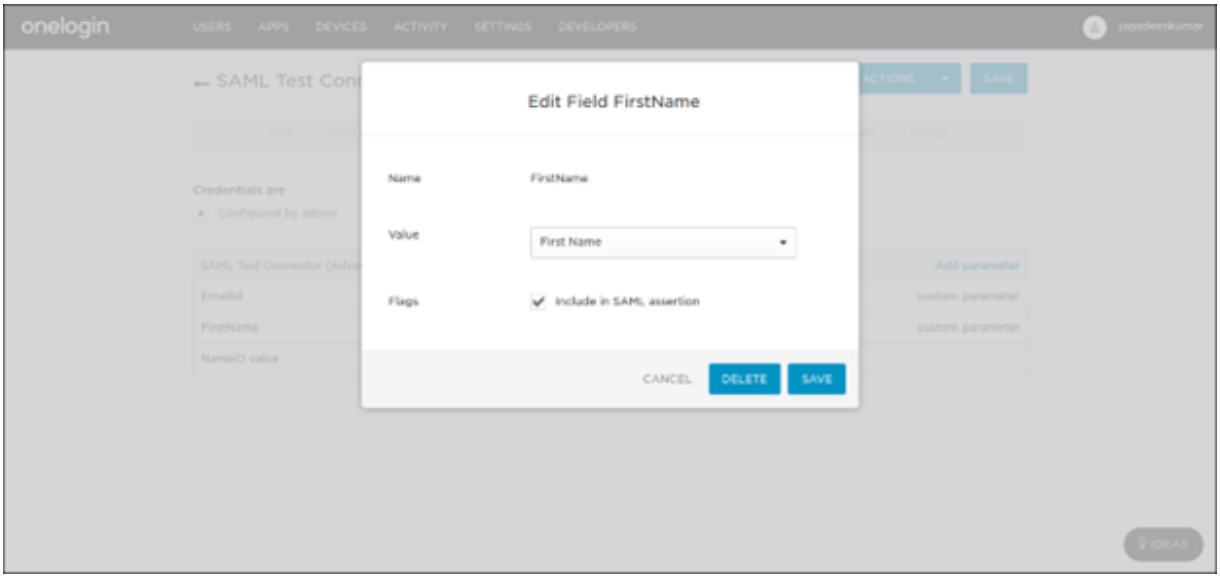
2. Provide the application name and application details of AppViewX on the information page.



3. **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.

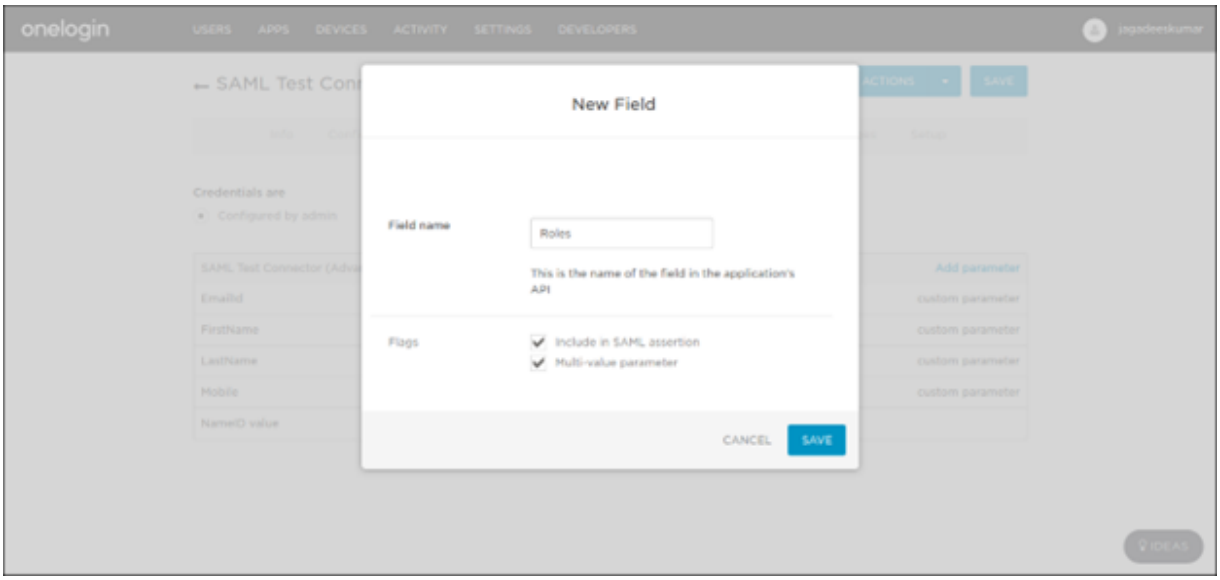


4. **Parameters to be sent to AppViewX:**The following parameters are samples that have been sent to AppViewX. Create a parameter called FirstName which sends the user's first name to AppViewX in the SAML Assertion.

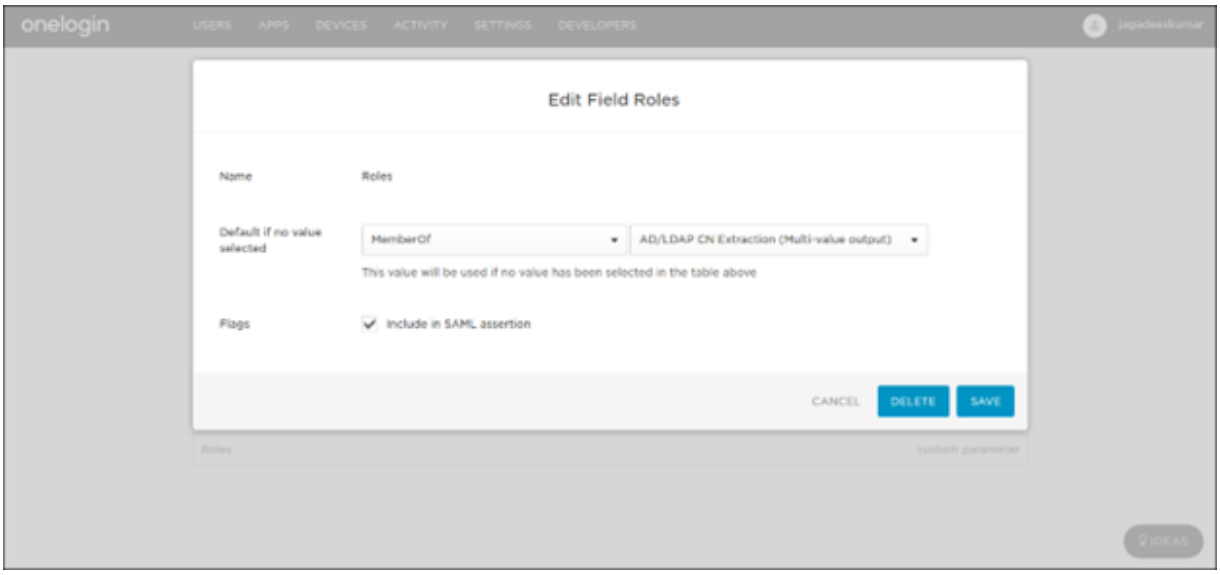


Include the flag in SAML Assertion for all the added parameters.

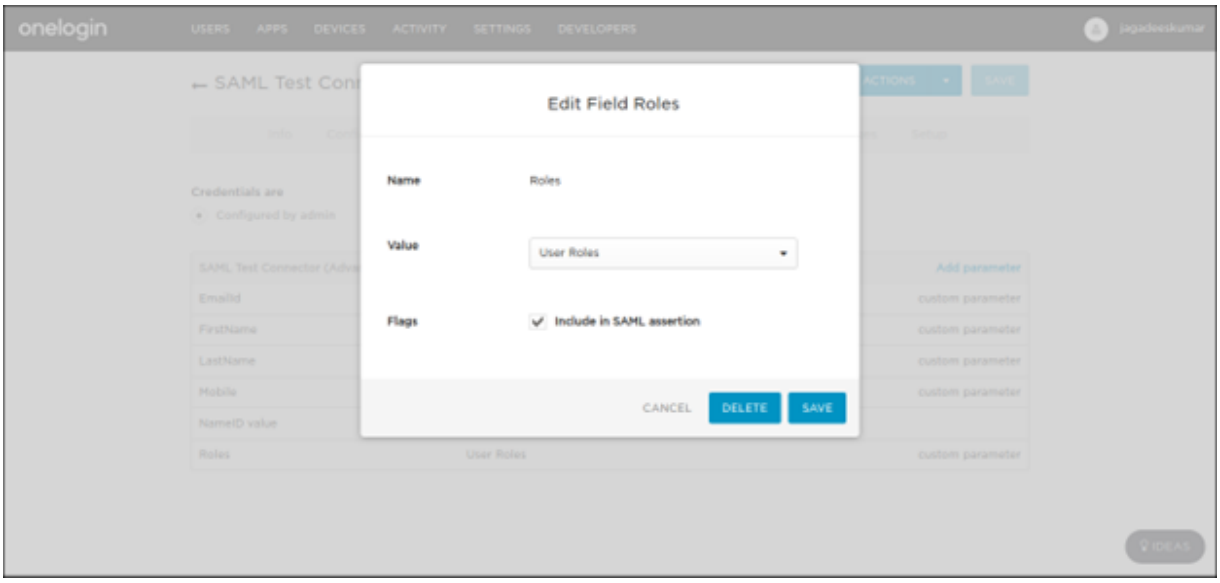
5. **Sending User Groups to AppViewX:** To send User Groups to AppViewX from OneLogin through SAML Assertion, the following configuration has to be performed. OneLogin should be integrated with the Active Directory. Provide the field name as Roles and enable the Flags SAML assertion and multi-value parameter.



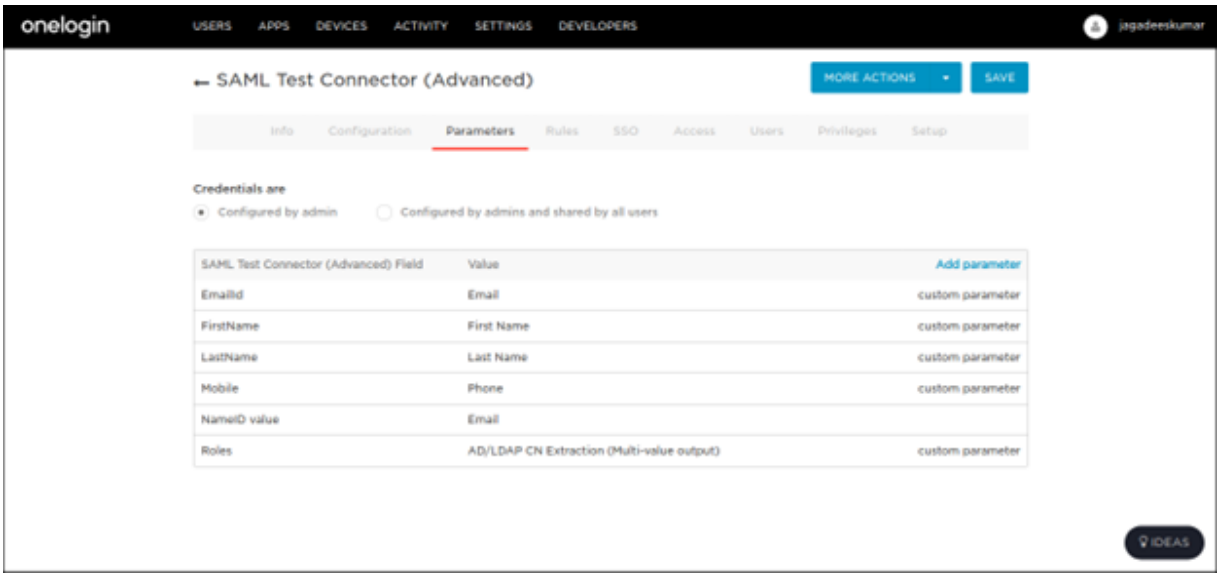
6. To pass the respective user's MemberOf attribute as Role, provide the field name as MemberOf and select the AD/LDAP CN Extractor.



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



7. **Other parameters that have to be passed:** The following parameters have to be passed to AppViewX through the SAML assertion.



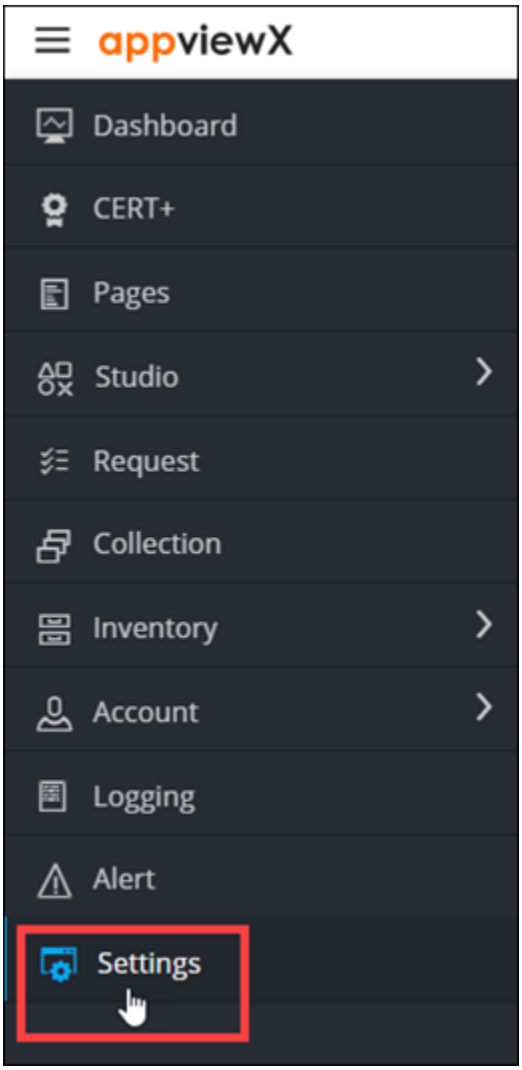
8. **Assign application to User and Role:** Once the federation metadata is downloaded, click Save. Create the UserGroup under Roles in the Administration section. The created application is then assigned to the user group and the synced users will be added to it.

Configuring the IP Restrictions

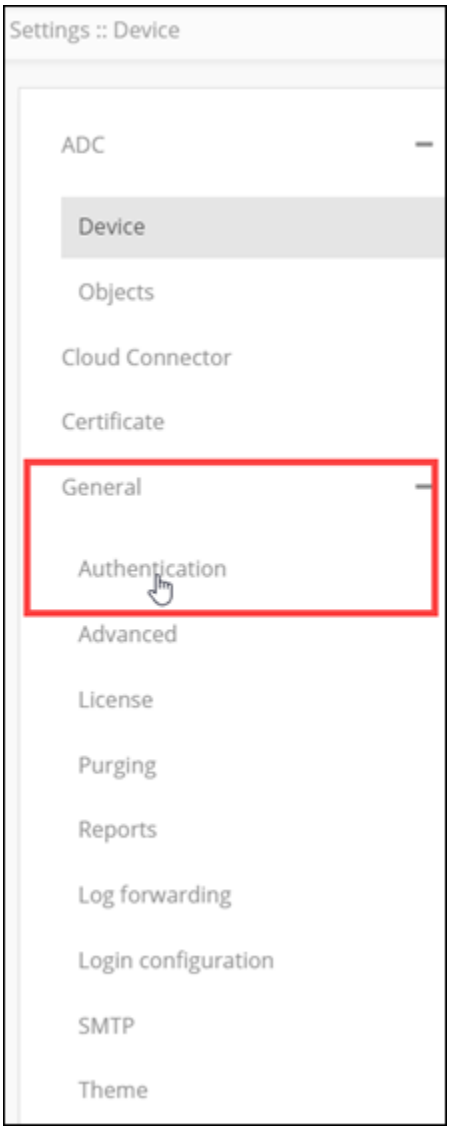
For enhanced security and if the administrator wants to whitelist specific IP addresses for user login, AppViewX lets you configure IP restrictions to allow access from whitelisted IP addresses/subnet ranges.

To configure IP restrictions:

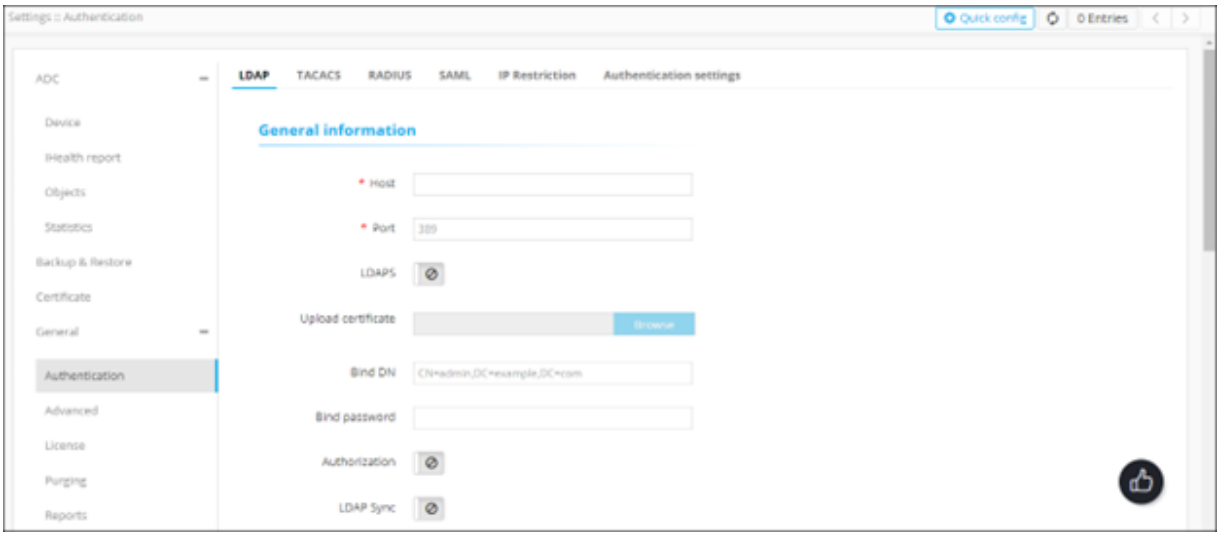
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Settings**.



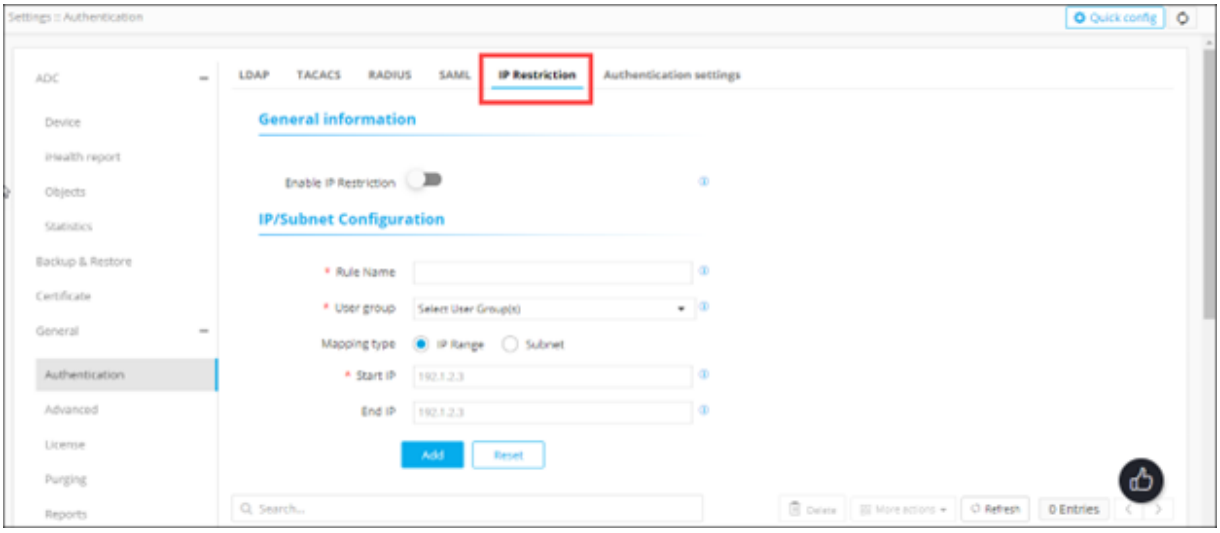
3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Authentication**.



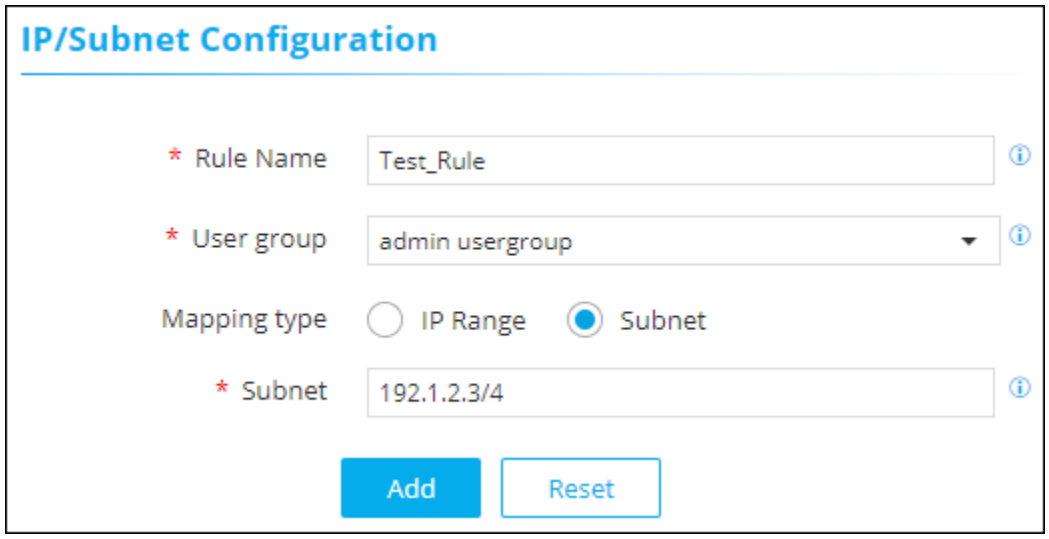
The **Settings :: Authentication** page is displayed, with the **LDAP** tab open by default.



5. To configure the IP restrictions, on the **Settings :: Authentication** page, click the **IP Restriction** tab.



6. In the **General Information** section, turn on the **Enable IP Restriction** toggle.
7. In the **IP/Subnet Configuration** section, enter the required field information.

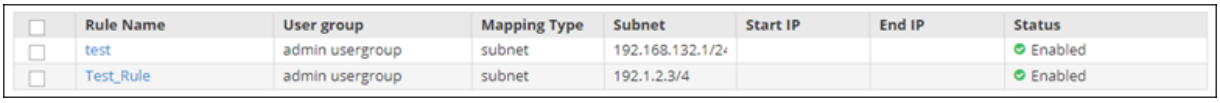


The following table describes the field information in this section:

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. **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.

Field	Description
	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**.

8. 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.



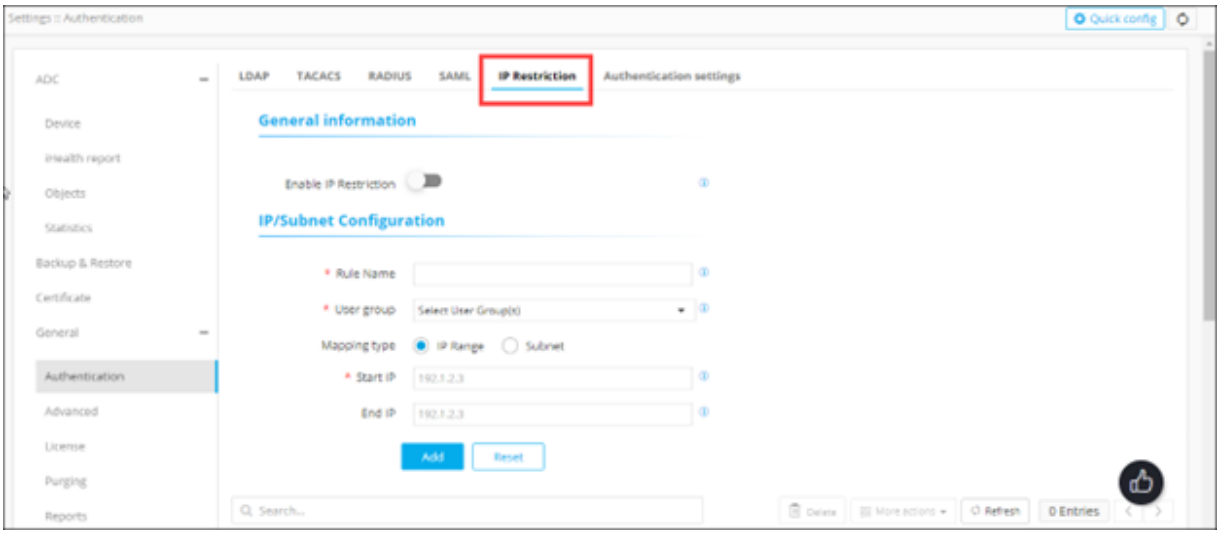
Rule Name	User group	Mapping Type	Subnet	Start IP	End IP	Status
test	admin usergroup	subnet	192.168.132.1/24			Enabled
Test_Rule	admin usergroup	subnet	192.1.2.3/4			Enabled

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

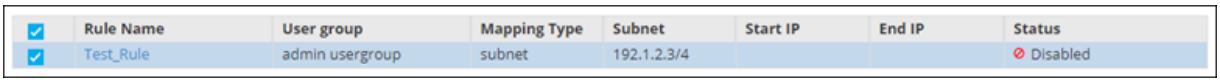
Enabling a IP Restriction Rule

To enable a IP restrictions rule:

1. Navigate to the **Settings :: Authentication** page.
2. To configure the IP restrictions, on the **Settings :: Authentication** page, click the **IP Restriction** tab.

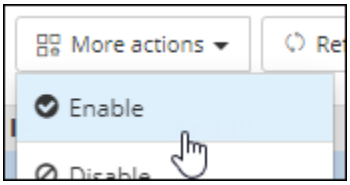


3. From the table at the end of the page, for the IP restrictions rule you want to enable, select the check box corresponding to that rule.



	Rule Name	User group	Mapping Type	Subnet	Start IP	End IP	Status
☑	Test_Rule	admin usergroup	subnet	192.1.2.3/4			Disabled

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

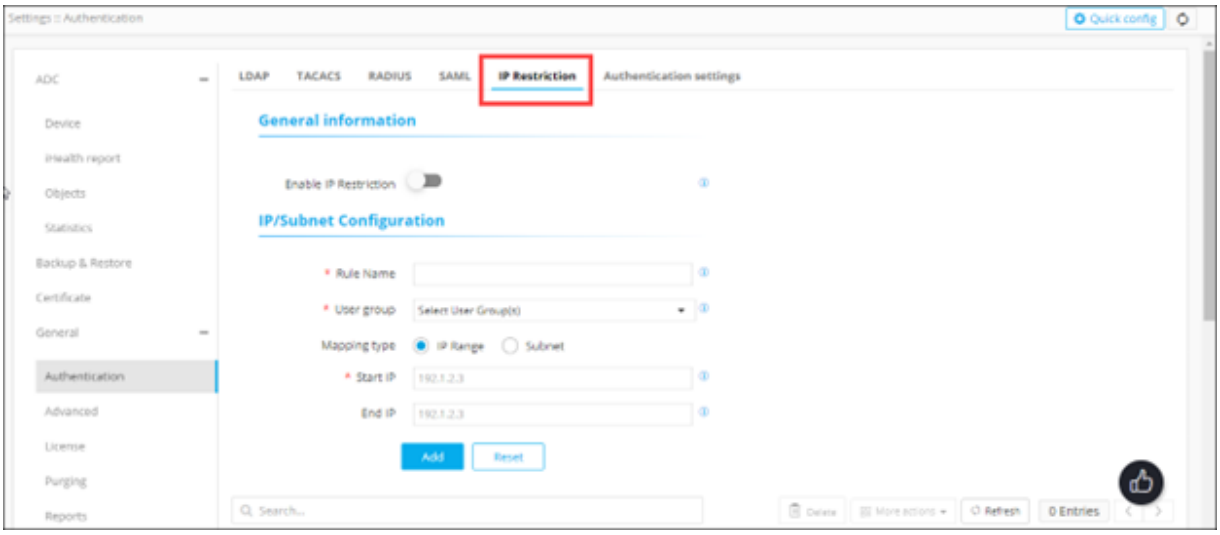


5. In the **Enable** dialog box, click **Yes**.

Disabling an IP Restriction Rule

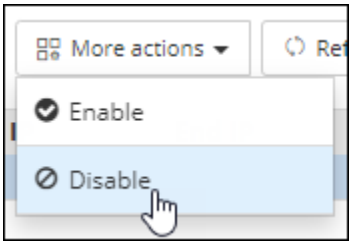
To disable a IP restrictions rule:

1. Navigate to the **Settings :: Authentication** page.
2. To configure the IP restrictions, on the **Settings :: Authentication** page, click the **IP Restriction** tab.



3. 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.

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

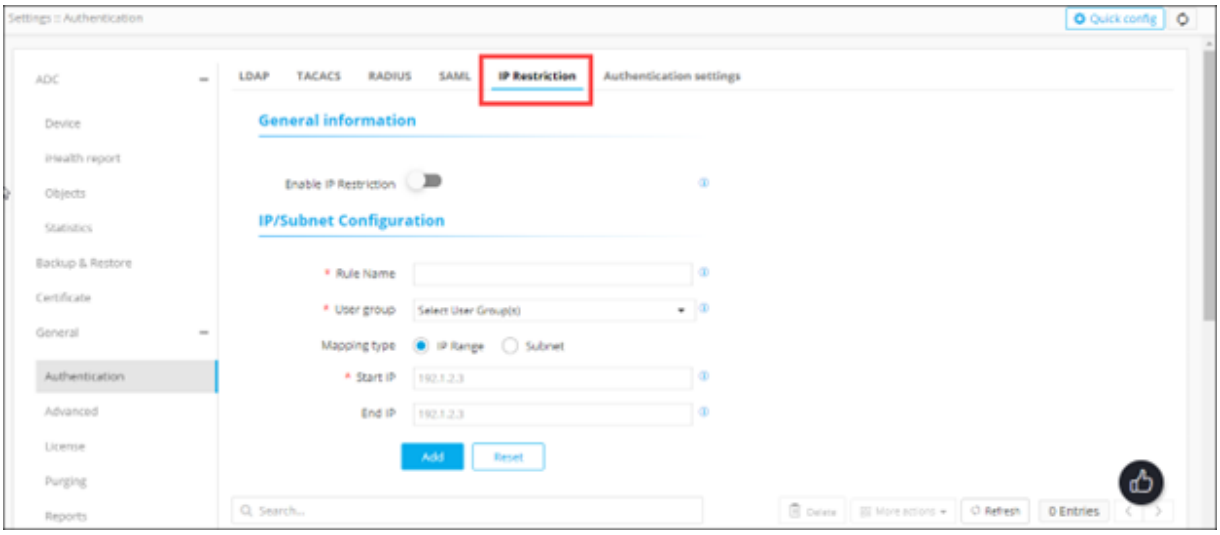


5. In the **Disable** dialog box, click **Yes**.
   The selected rule is disabled.

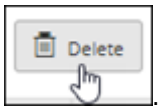
Deleting an IP Restriction Rule

To delete an IP restrictions rule:

1. Navigate to the **Settings :: Authentication** page.
2. To configure the IP restrictions, on the **Settings :: Authentication** page, click the **IP Restriction** tab.



3. 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.

4. Click 

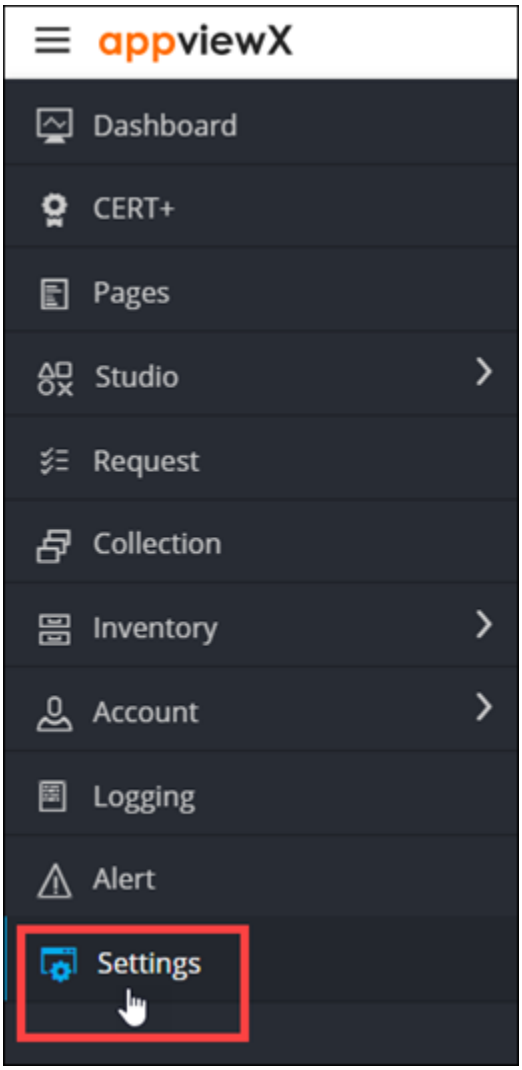
.
5. In the **Confirmation** dialog box, click **Yes**.
   The selected rule is deleted.

Configuring Authentication Settings

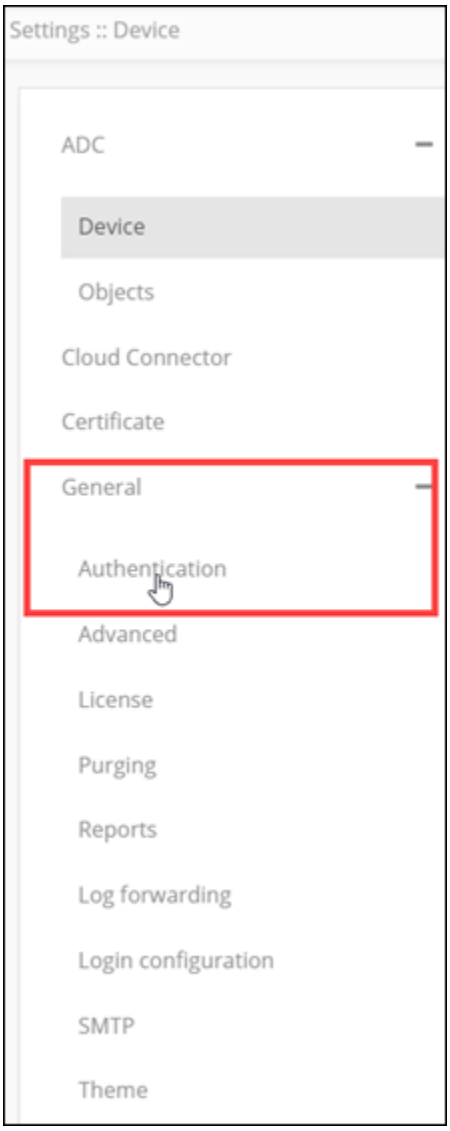
In addition to configuring authentication settings, AppViewX also lets you enable birthright provisioning for new users, configure the order in which user credentials are authenticated, enable/disable an authentication check, and other user and node settings.

To configure the authentication settings:

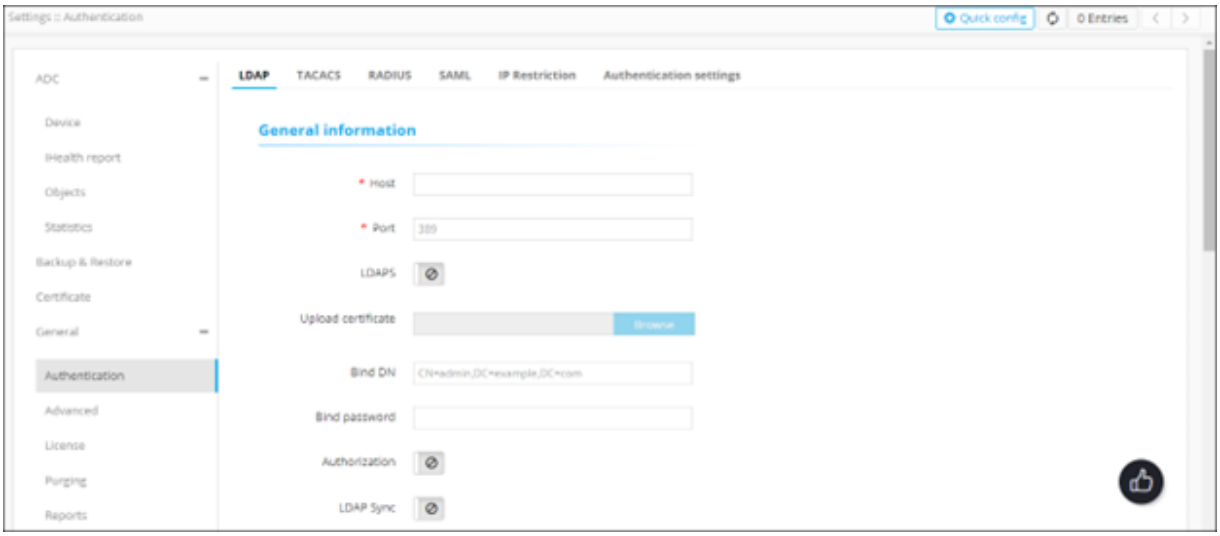
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Settings**.



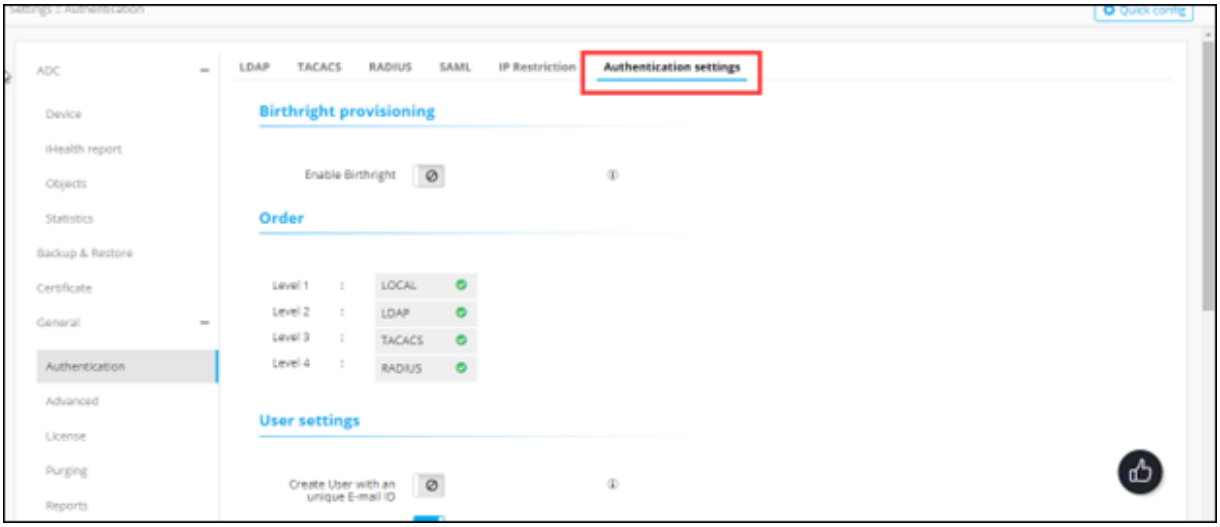
3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Authentication**.



The **Settings :: Authentication** page is displayed, with the **LDAP** tab open by default.

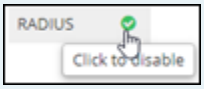


5. On the **Settings :: Authentication** page, click the **Authentication settings** tab.



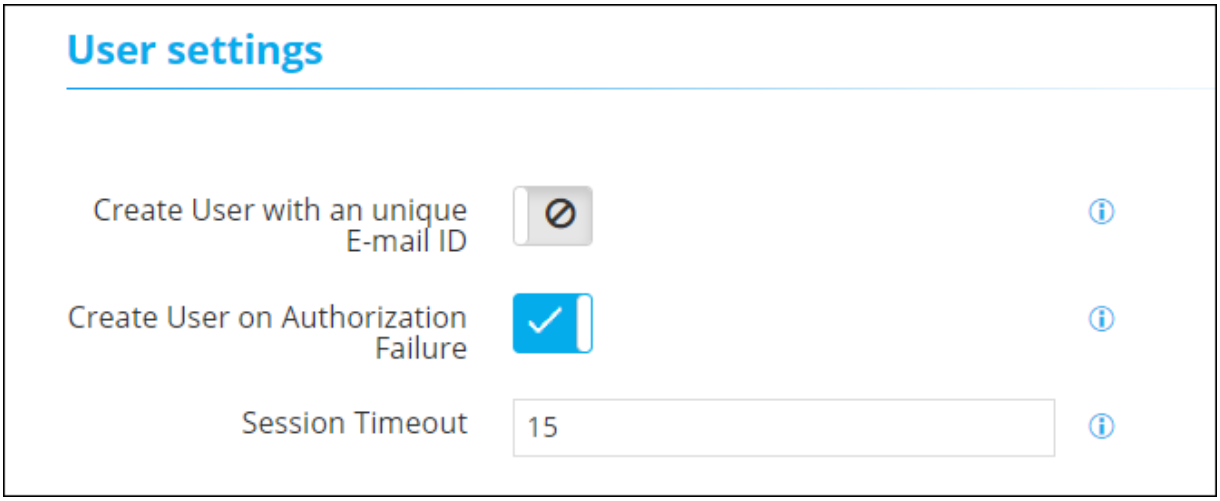
6. To enable **Birthright provisioning** for new users who log into the system with a predefined set of permissions (associated with the user group), turn on the **Enable Birthright** toggle.
   To do this, the admin should select the user group (Assigned with the defined permissions), which will act as a default user group for all the users logging in to AppViewX. Fore more details, refer to the content on creating a role and associating it with a user group.
7. 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.

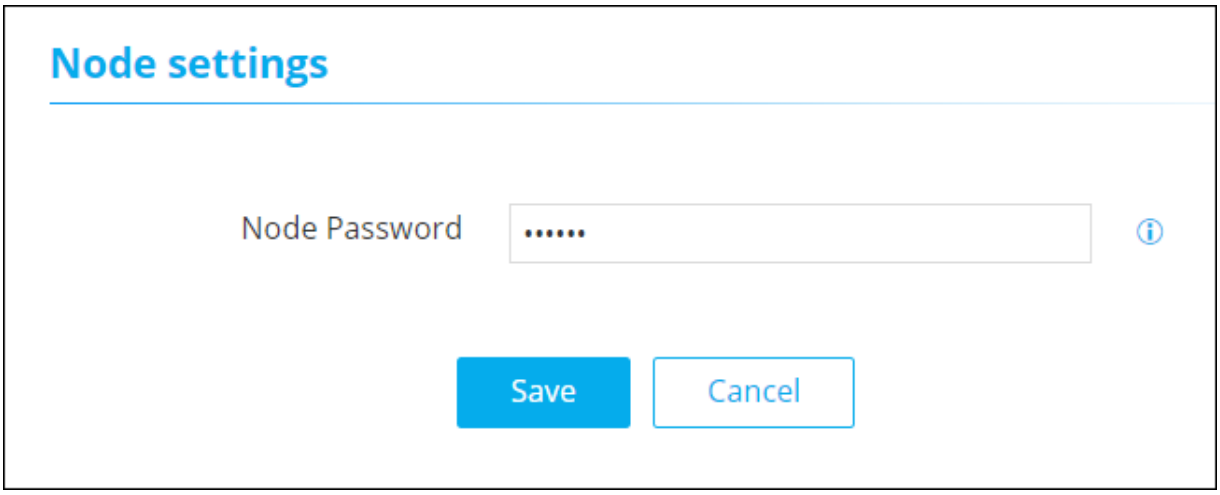
8. In the **User settings** section, enter the required field information.



The following table describes the field information in this section:

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.

9. 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.

10. Click **Save**.

Chapter 3: Configuring Role and Resource-Based Access Control

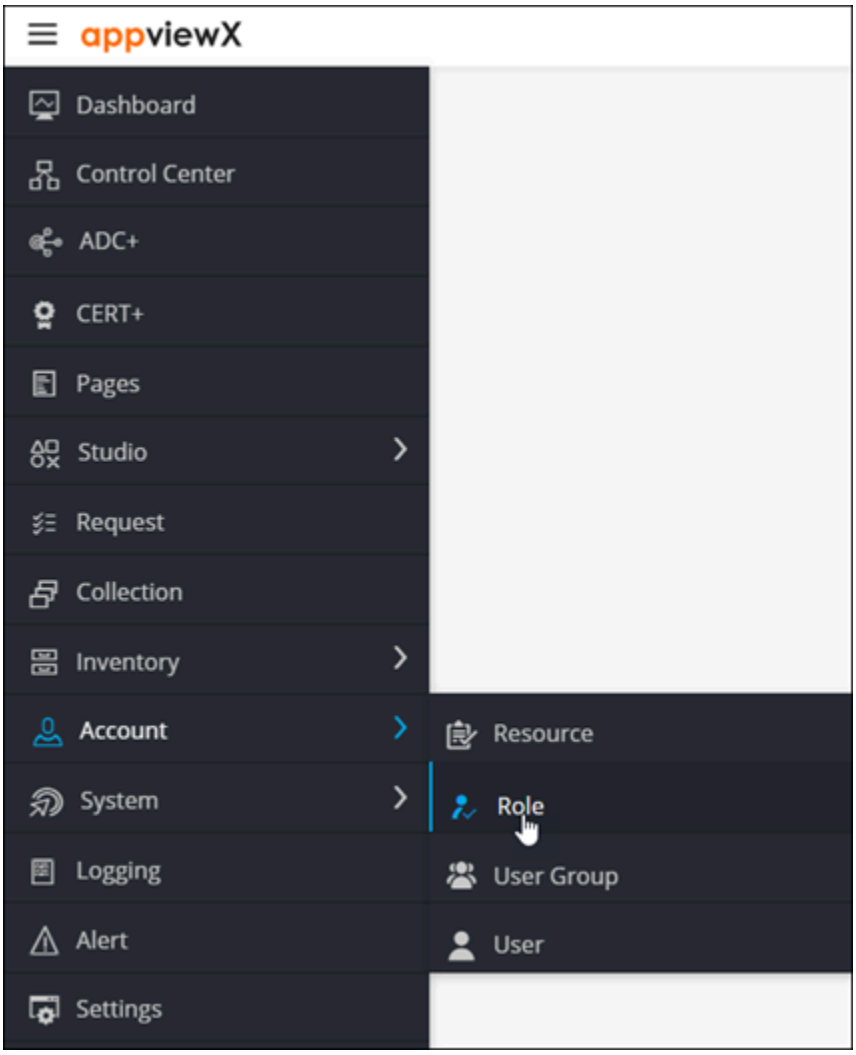
Managing Roles

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.

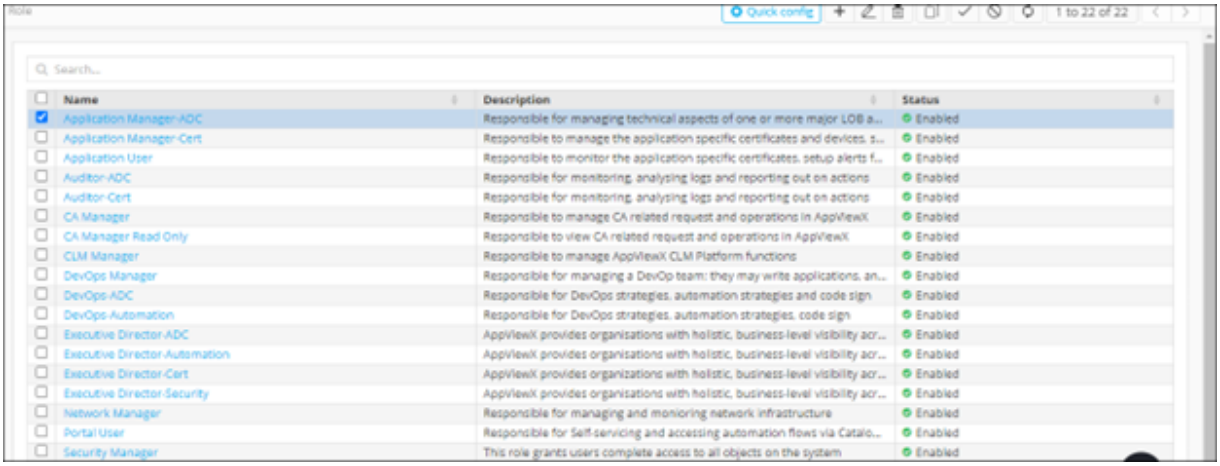
Creating a Role

To create a role:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, select **Account** > **Role**.



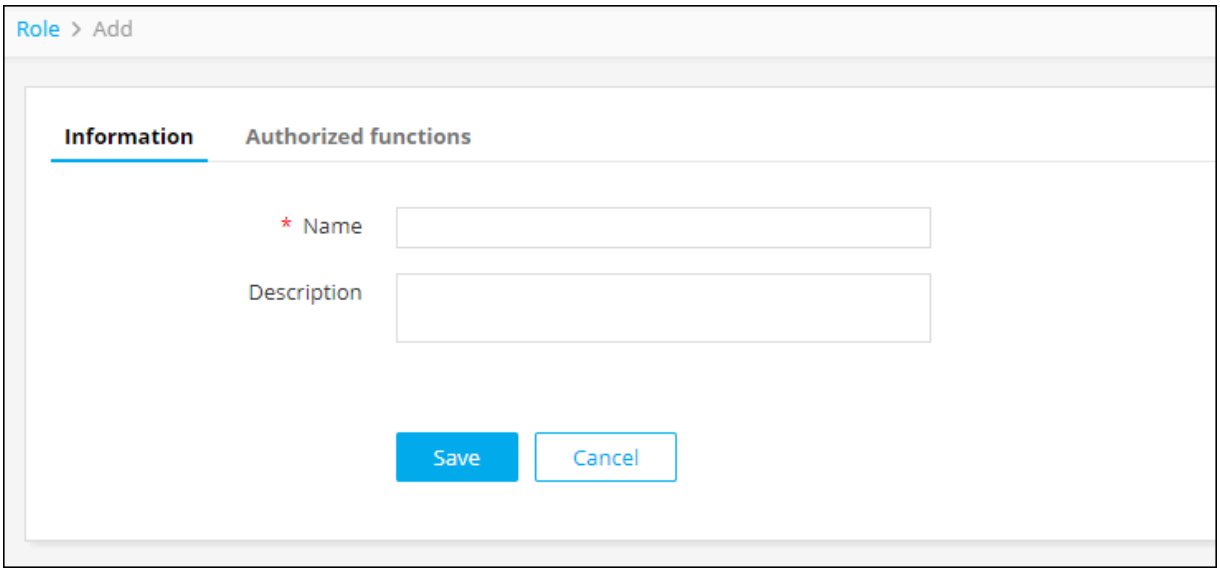
The **Role** page is displayed.



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

.

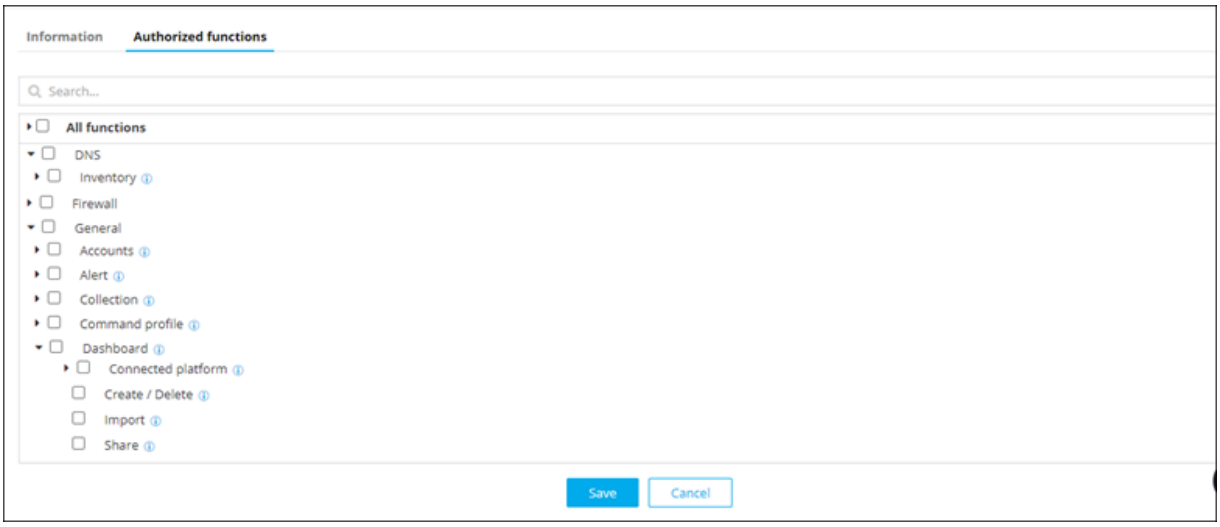
   The **Add** page is displayed.



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

Field	Description
***Name**	Name of the role.
Description	Role/features/functionalities associated with the role.
All * marked fields are mandatory.	

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

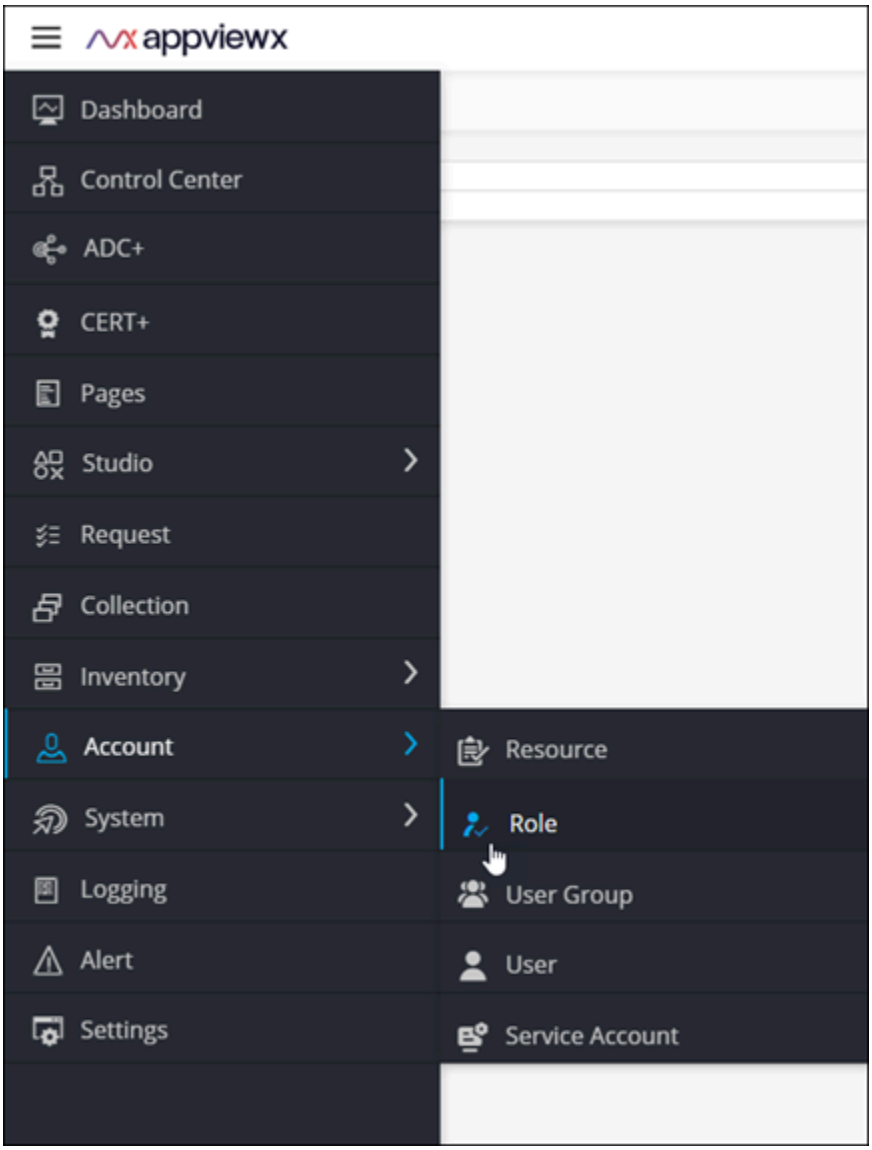


8. Click **Save**.
   Details of the new role are displayed in the list on the **Role** page.

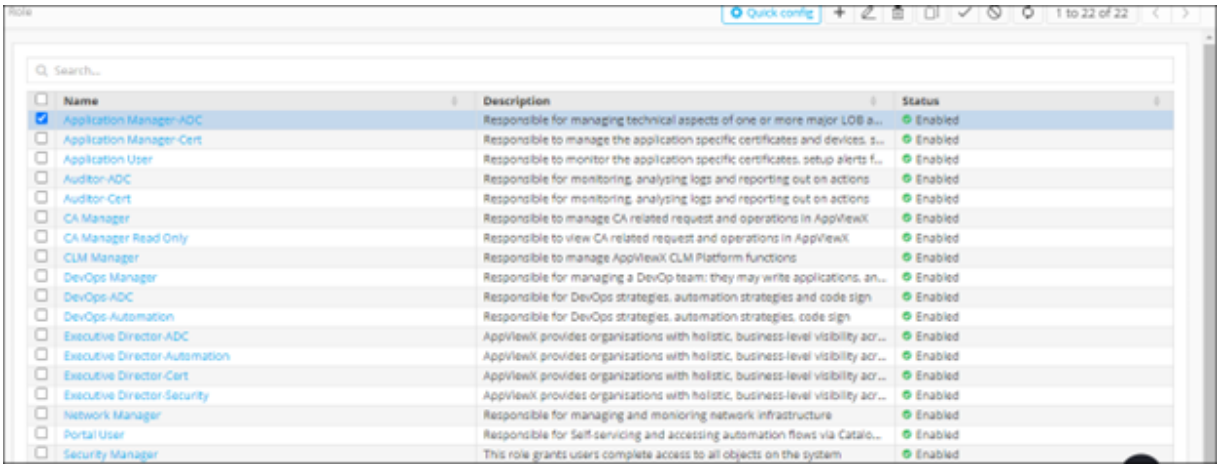
Modifying a Role

To modify a role:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the icon.
2. From the menu displayed, click **Account** > **Role**.

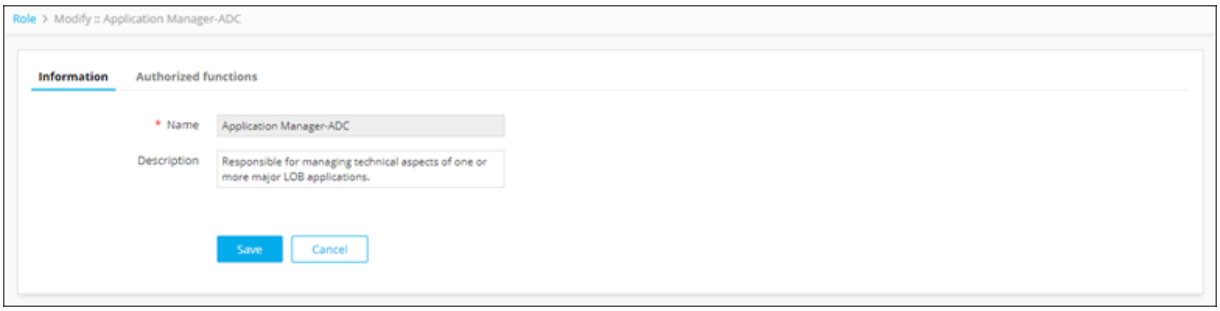


The **Role** page is displayed.



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

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

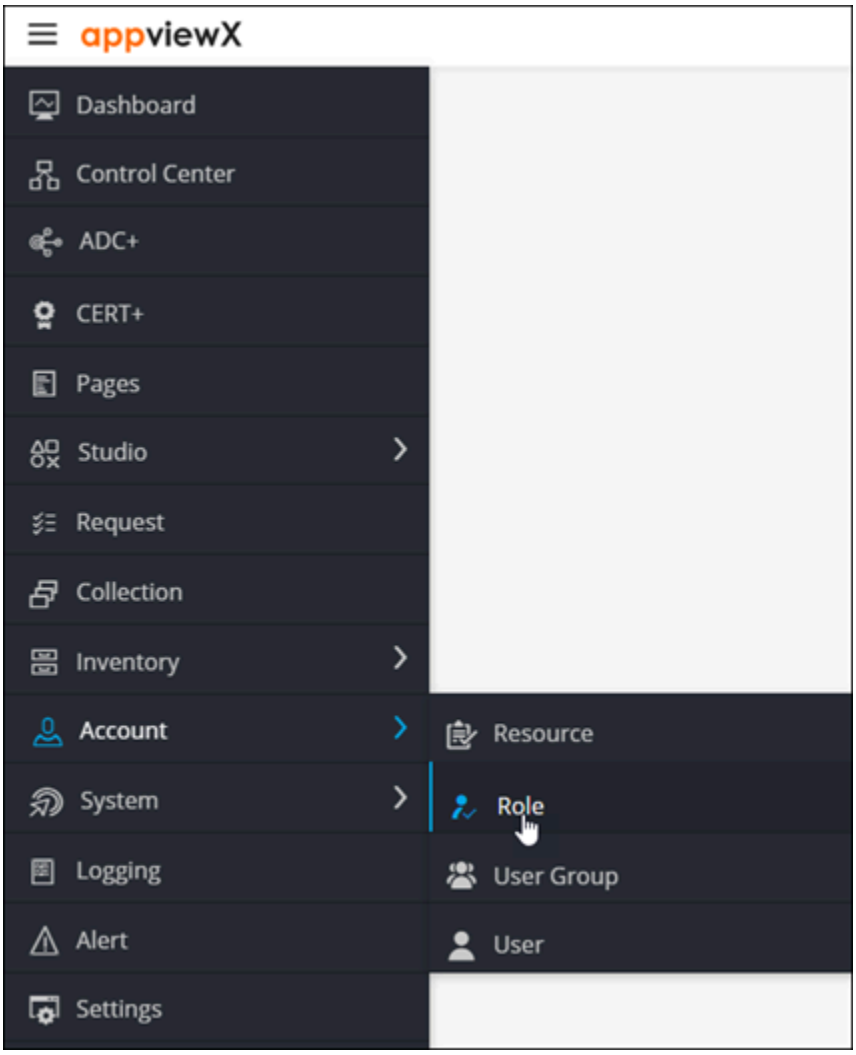


6. Click **Save**.
   The selected role is modified.

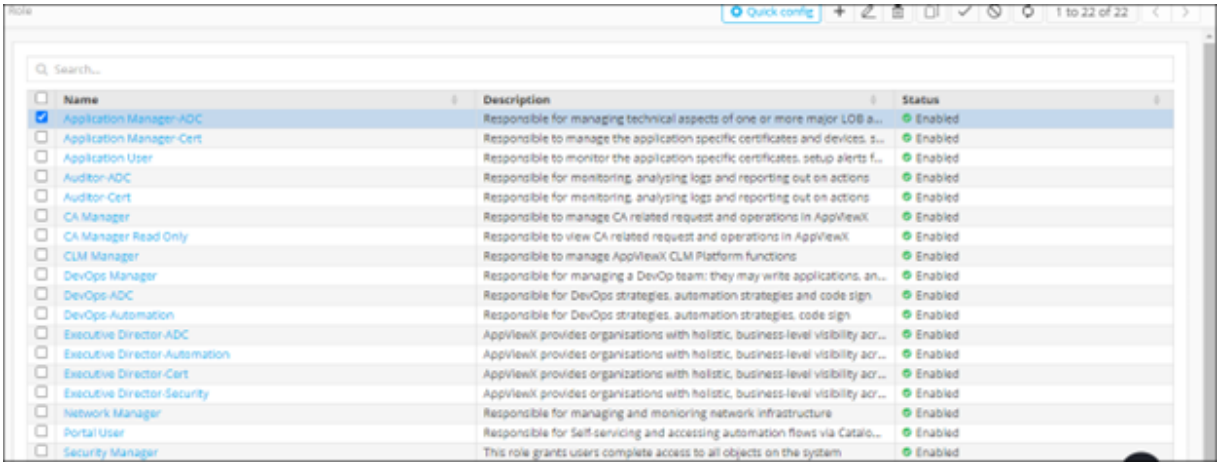
Enabling a Role

To enable a role:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the icon.
2. From the menu displayed, click **Account** > **Role**.



The **Role** page is displayed.



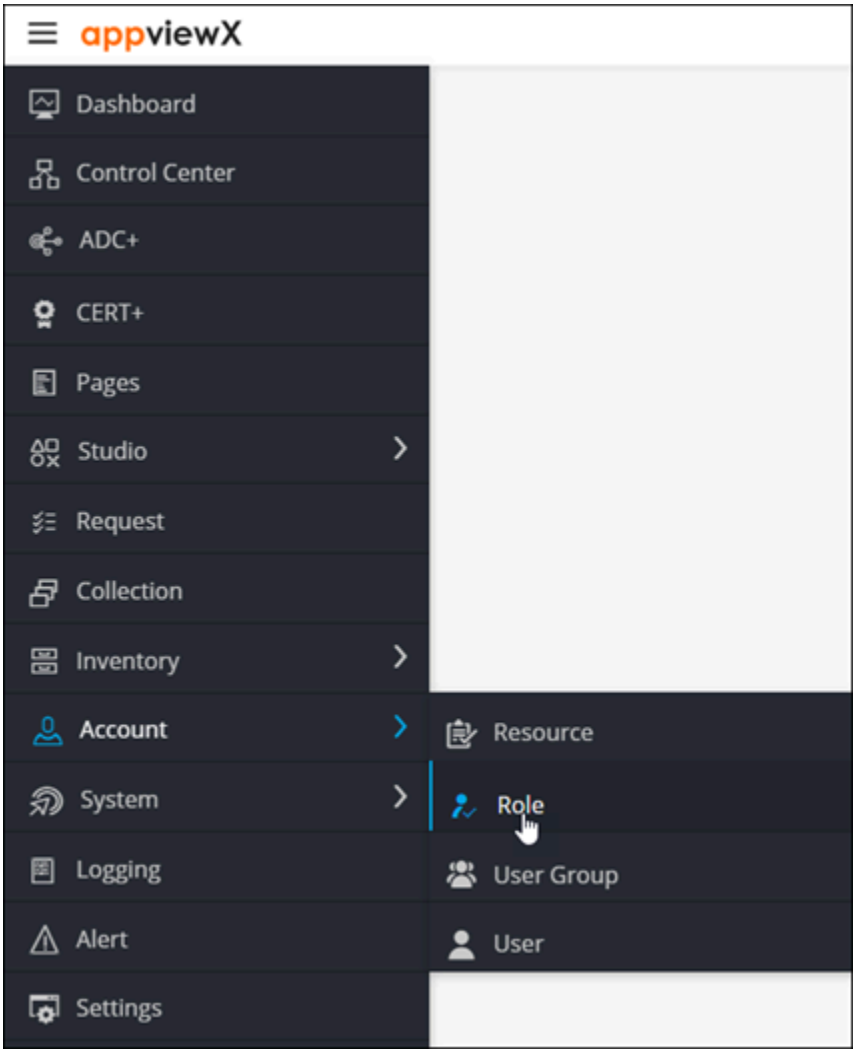
3. For the (disabled) role you want to enable, select the corresponding check box.
4. From the top right corner of the screen, click 

.
5. In the **Confirmation** dialog box, click **Yes**.
   The selected role is enabled.

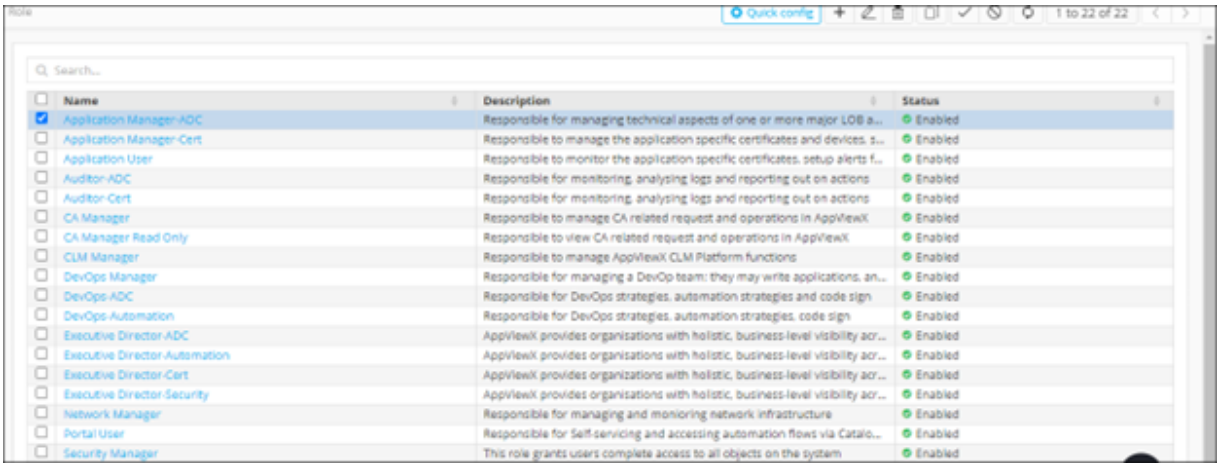
Disabling a Role

To disable a role:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Account** > **Role**.



The **Role** page is displayed.



3. For the (enabled) role you want to disable, select the corresponding check box.
4. From the top right corner of the screen, click 

.
5. In the **Confirmation** dialog box, click **Yes**.

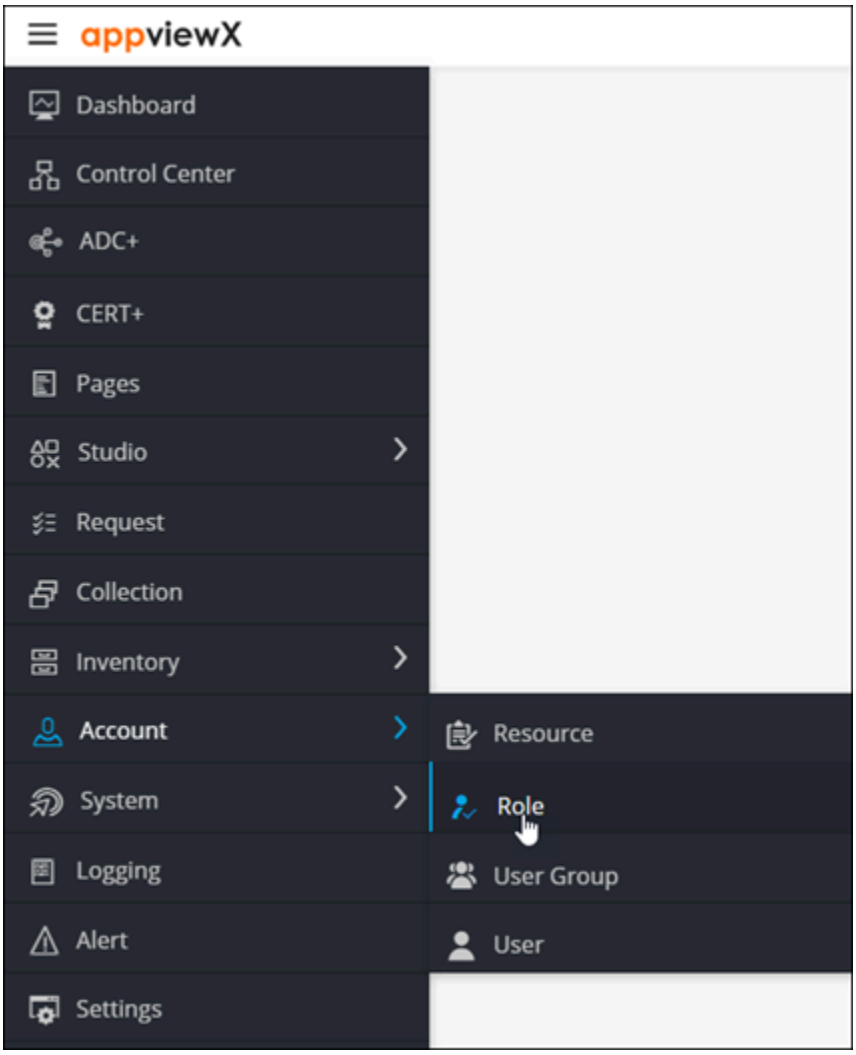
   The selected role is disabled.

Cloning a Role

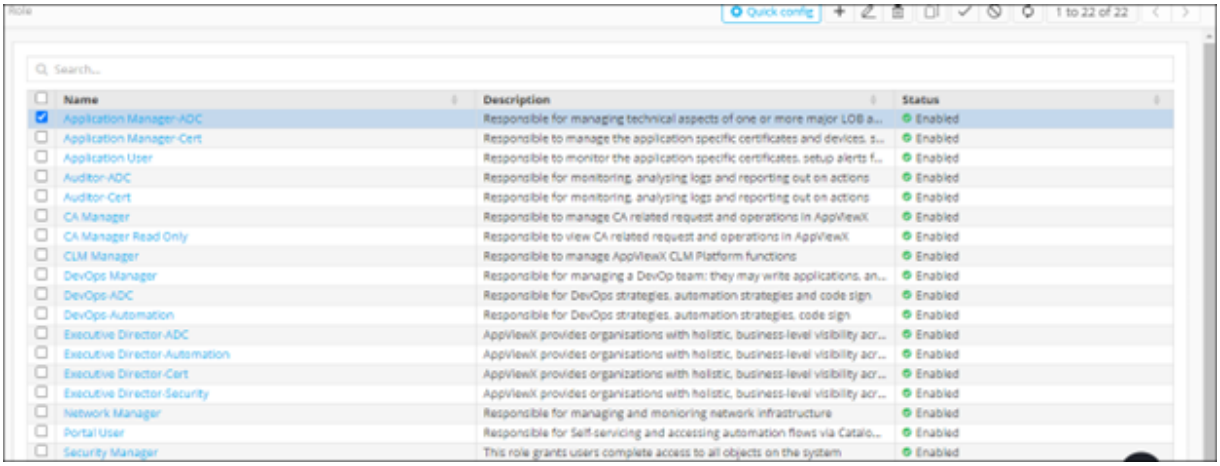
Cloning lets you create a copy of an existing role with a different name. You can modify the permissions and tasks that can be performed while cloning a role.

To clone a role:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the icon.
2. From the menu displayed, click **Account** > **Role**.

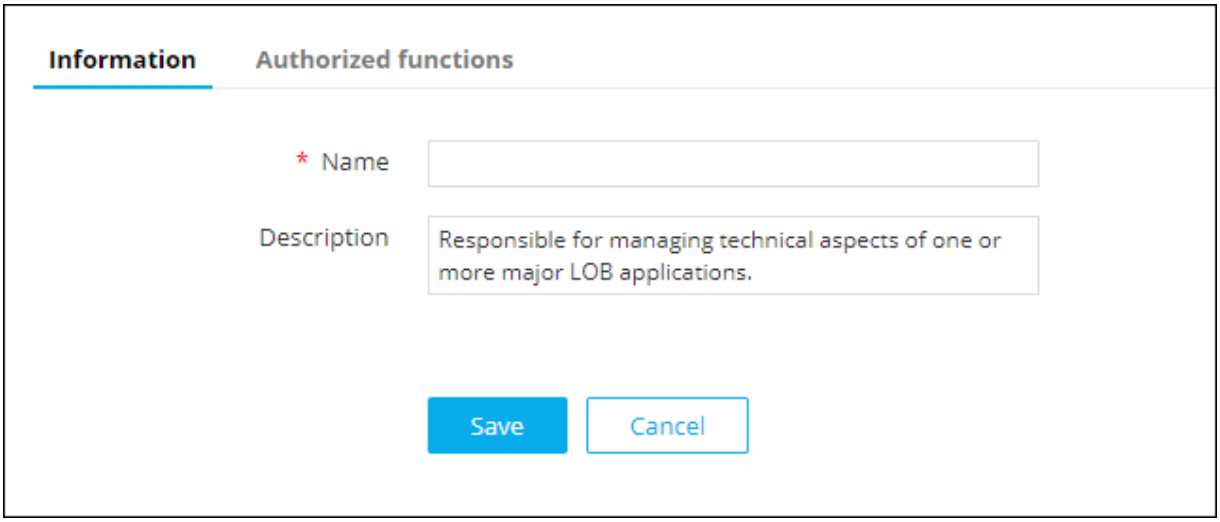


The **Role** page is displayed.



3. For the role you want to clone, select the corresponding check box.
4. From the top right corner of the screen, click 

.
5. In the **Information** section, enter a new **Name** for the role.



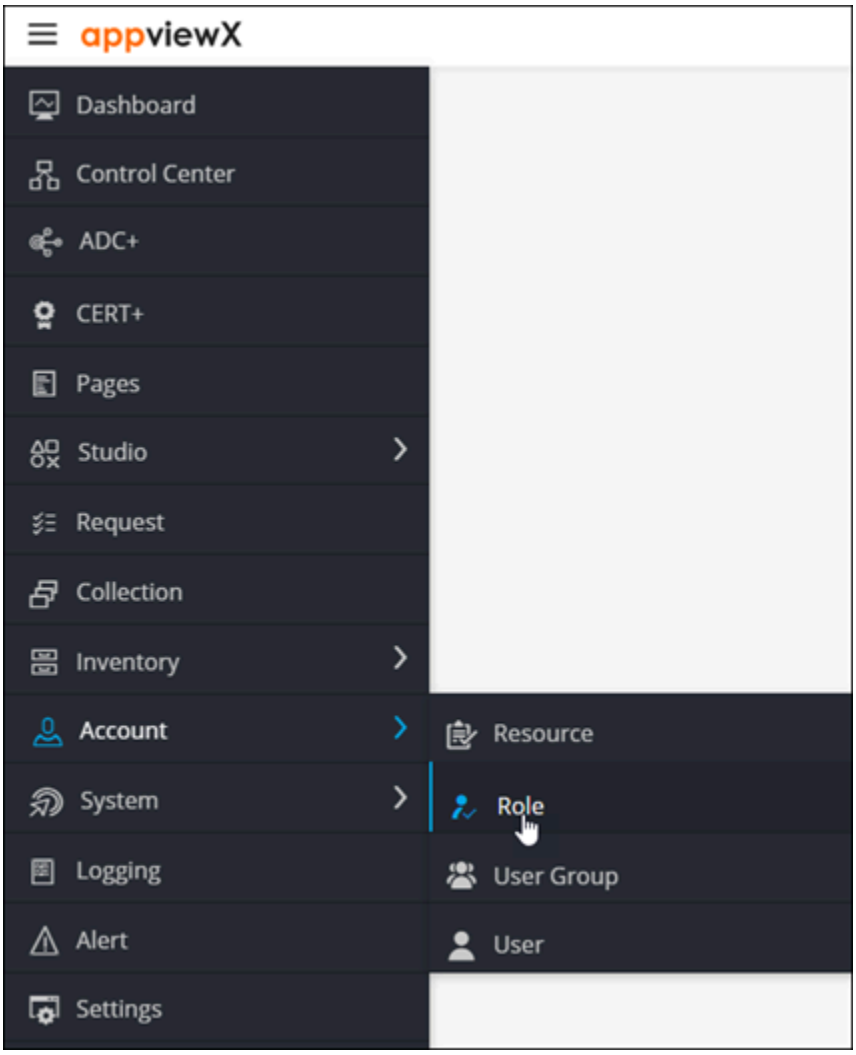
6. Click **Save**.
   The selected role is cloned.

Deleting a Role

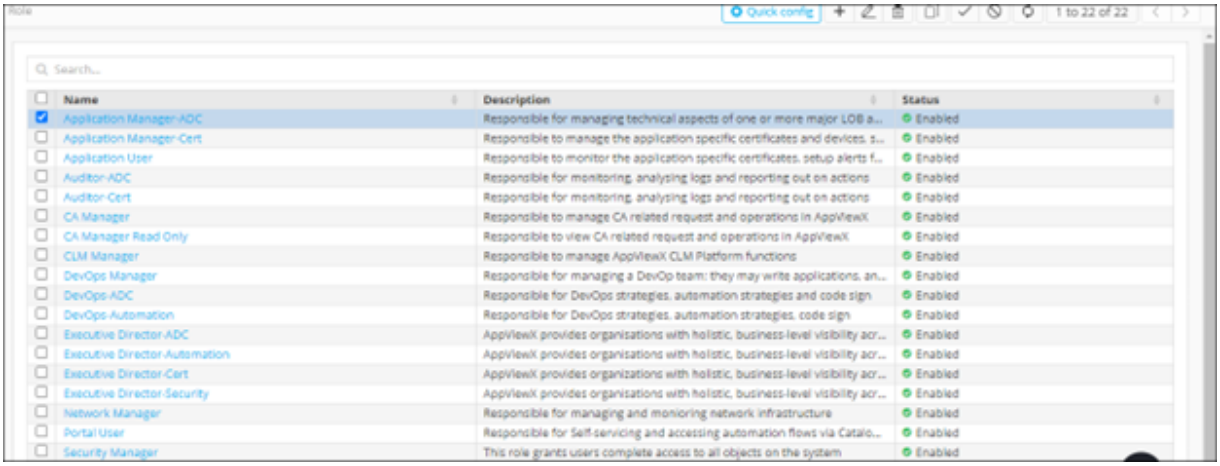
Note: A role that has active users belonging to it cannot be deleted.

To delete a role:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, select **Account** > **Role**.



3. The **Role** page is displayed.



4. For the record you want to delete, select the corresponding check box.
5. From the top right corner of the screen, click 

.
6. In the **Confirmation** dialog box, click **Yes**.
   The selected role is deleted.

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.

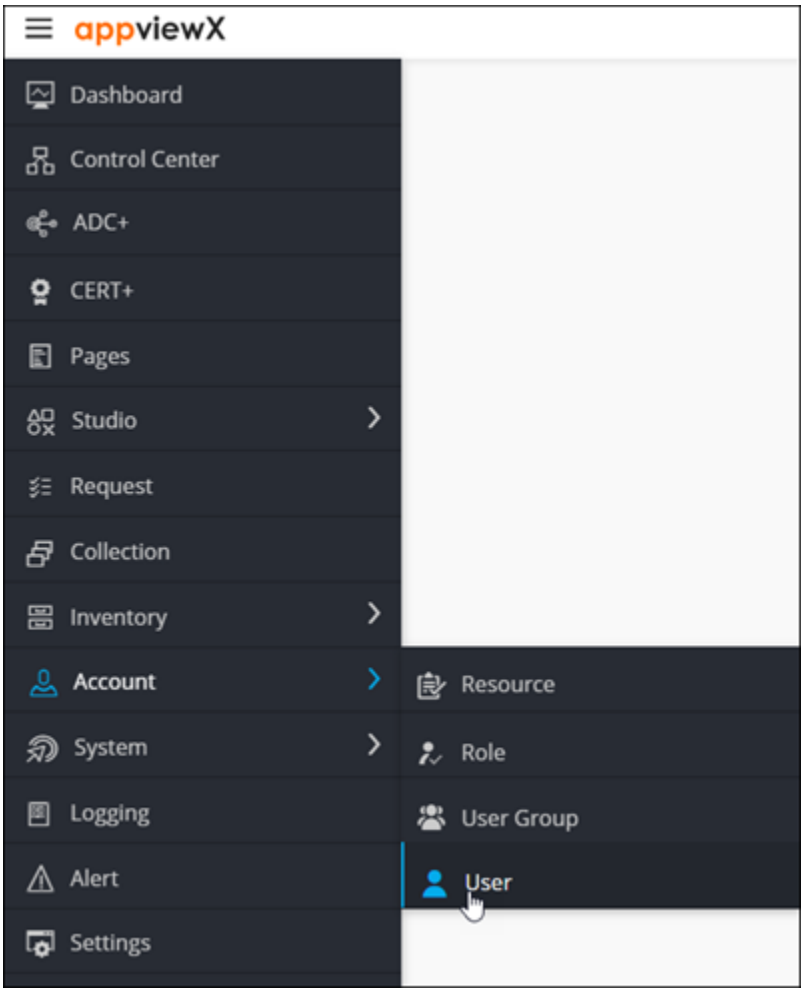
Note: You must add a user to the user group as the roles and resources cannot be directly associated with the user.

- Creating a User
- Modifying a User
- Importing a User
- Enabling a User
- Disabling a User
- Deleting a User

Creating a User

To create a user:

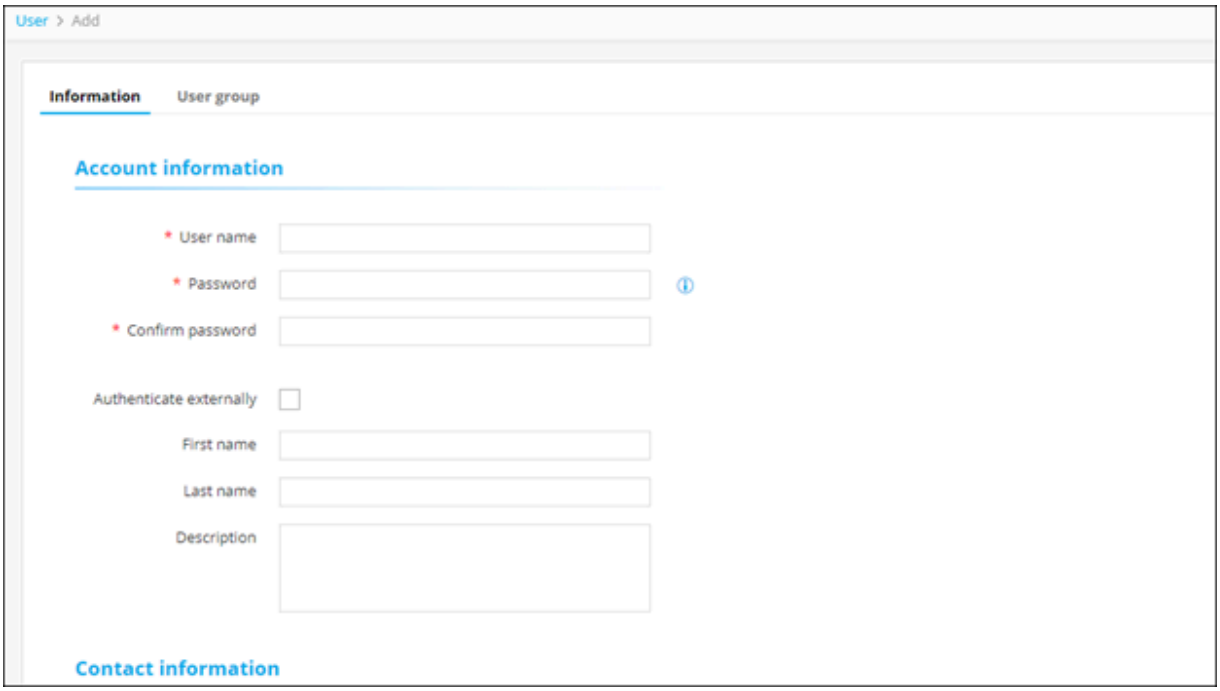
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Account** > **User**.



The **User** page is displayed.

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

.
4. The **Add** page is displayed, with the **Information** tab open by default.



5. In the **Account Information** section, enter the following details:

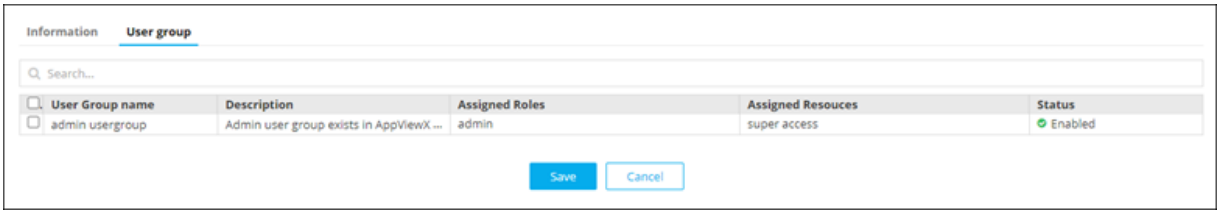
Field	Description
***User name**	Enter the user name for the new user.
***Password**	Enter the password for the new user. **Note:** The new password should have: • At least one uppercase, lowercase, and numeric character • At least one special character (~!@#$^&*_-+=|()) • 6 to 24 characters **Note:** 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.

Field	Description
	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.
All * marked fields are mandatory.	

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

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.
All * marked fields are mandatory.	

7. Click **Save**.
8. The user should be assigned or mapped to a user group to be able to log into AppViewX and access the product. To add the user to a group, click the **User group** tab.

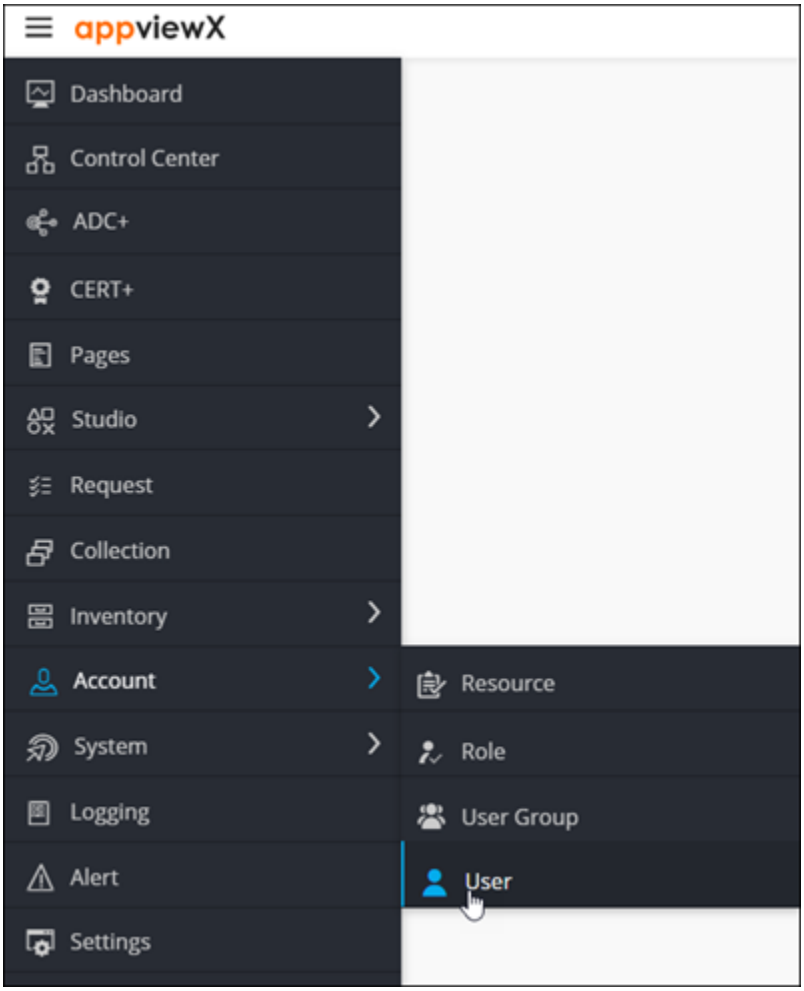


9. To add the user to a group, select the check box for that user group.
10. Click **Save**.

Modifying a User

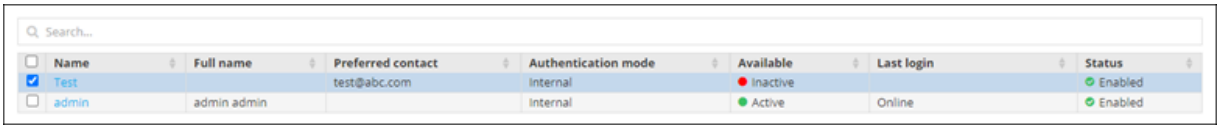
To modify a user:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Account** > **User**.



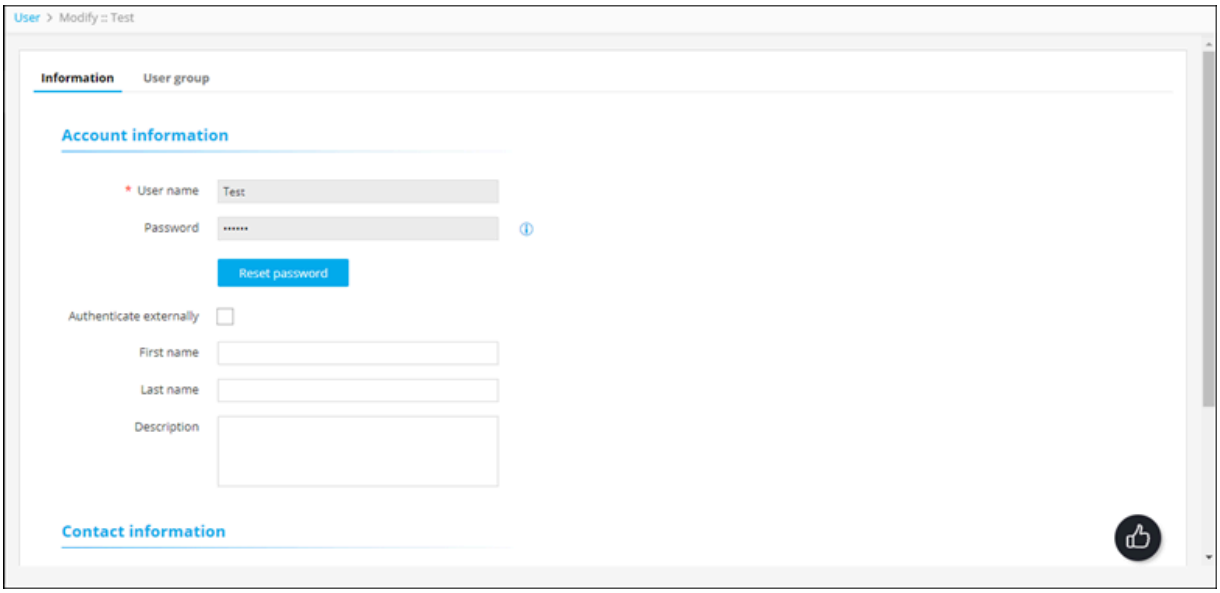
The **User** page is displayed.

3. From the **User** page, select the check box against the user you want to modify.



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

.
5. The **Modify** page is displayed, with the **Information** tab open by default.



6. In the **Account Information** section, update the required details:

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:

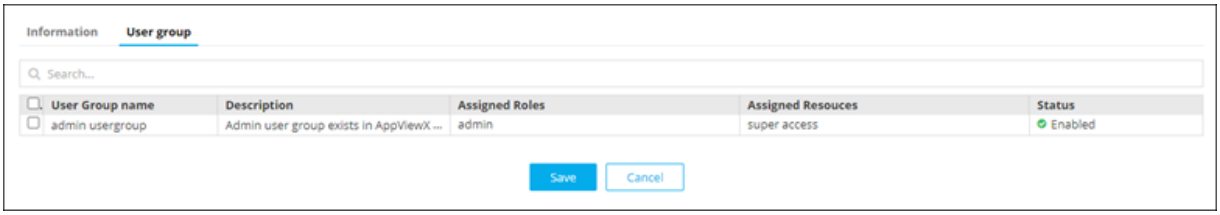
Field	Description
	• At least one uppercase, lowercase, and numeric character • At least one special character (~!@#$^&*_-+=|()) • 6 to 24 characters **Note:** The new password should not contain: • The user name • The same character more than three times consecutively • Blank spaces
***Confirm Password**	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.
All * marked fields are mandatory.	

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

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.

Field	Description
	Note: This field is mandatory only if the preferred mode of contact is Phone number.
All * marked fields are mandatory.	

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

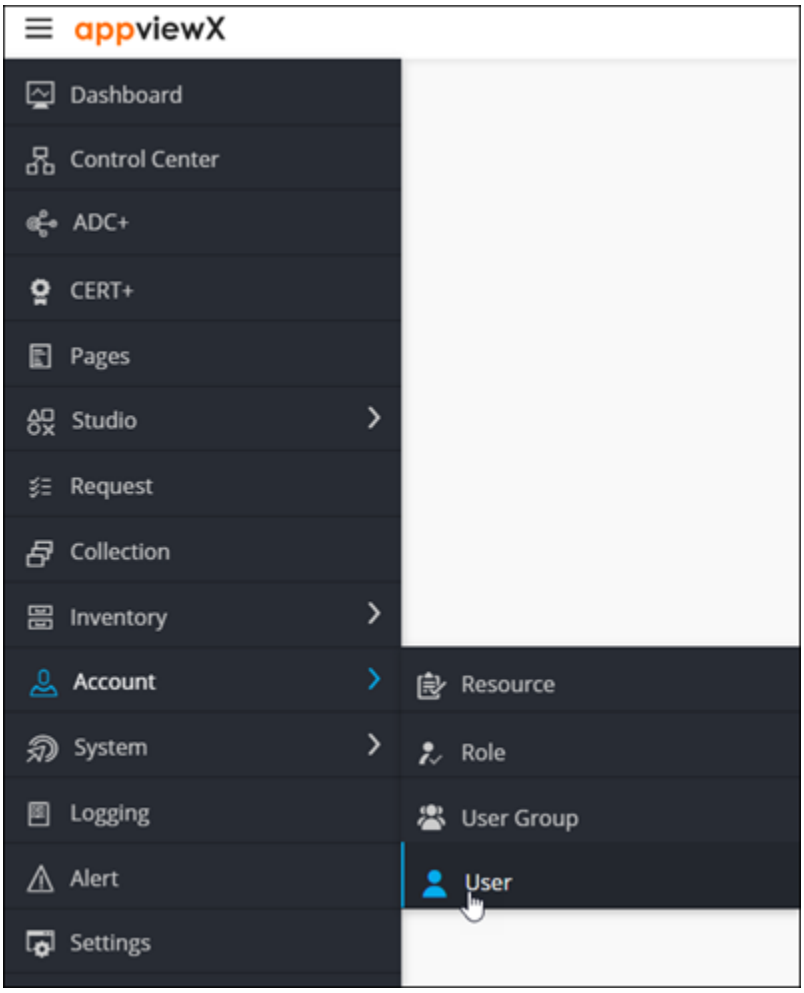


10. To add the user to a group, select the check box for that user group.
11. Click **Save**.

Importing a User

To import users into AppViewX:

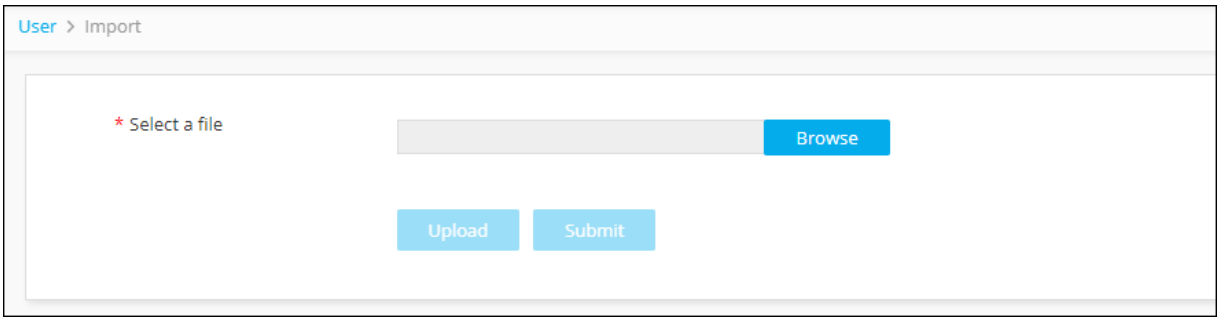
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Account** > **User**.



The **User** page is displayed.

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

.
4. The **Import** screen is displayed.



5. Click **Browse** and 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.

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

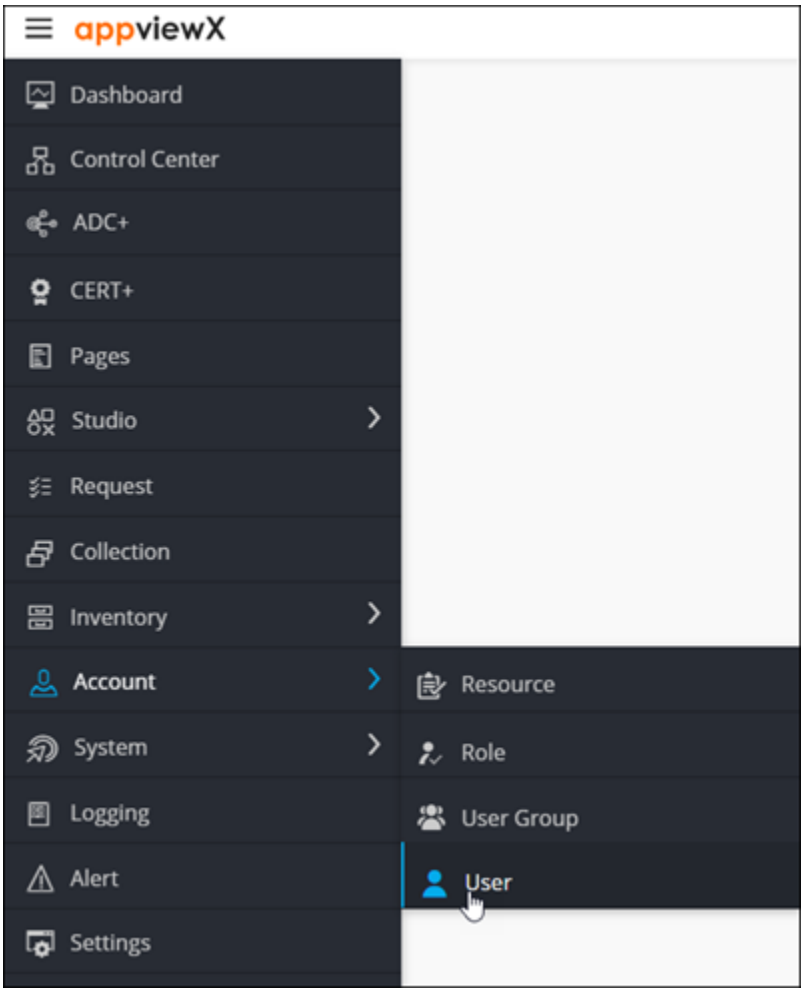
> **Note:** The user details displayed at this point are only for review; the user details have not been imported yet.

7. 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.
8. Click **Submit**.

Enabling a User

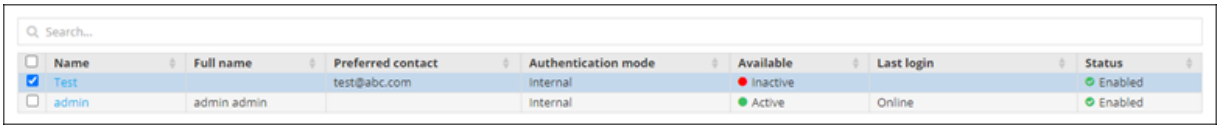
To enable a user:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the icon.
2. From the menu displayed, click **Account** > **User**.



The **User** page is displayed.

3. From the **User** page, select the check box against the user you want to enable.



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

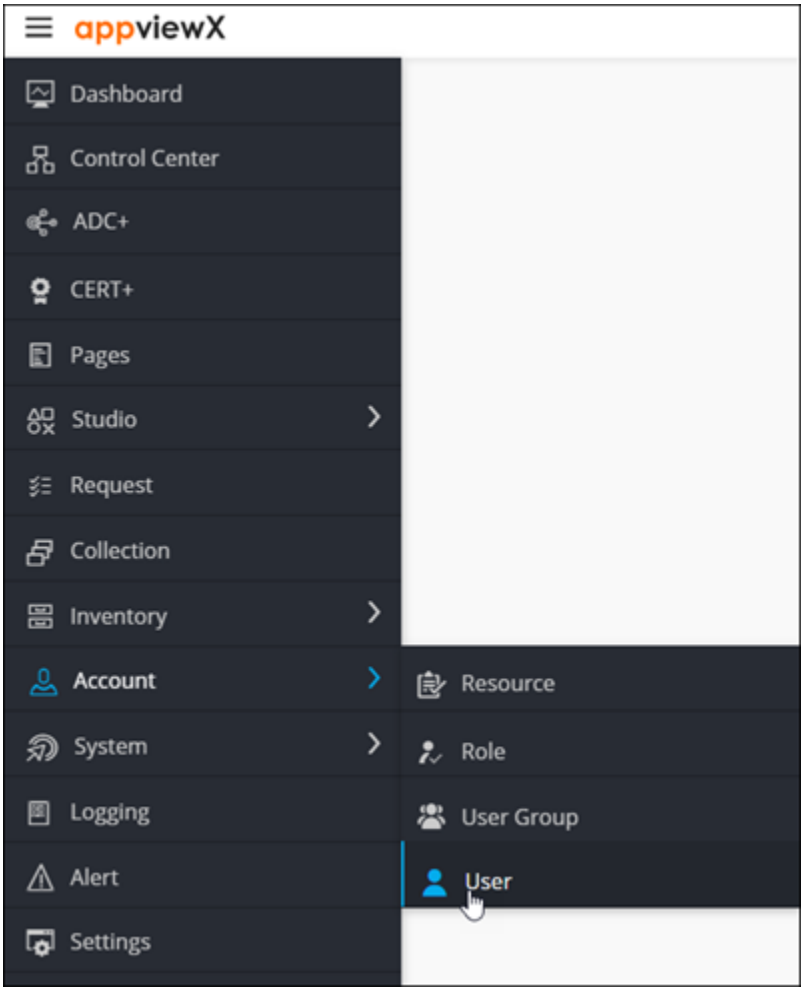
.

5. In the **Confirmation** dialog box, click **Yes**.
   The selected user is enabled.

Disabling a User

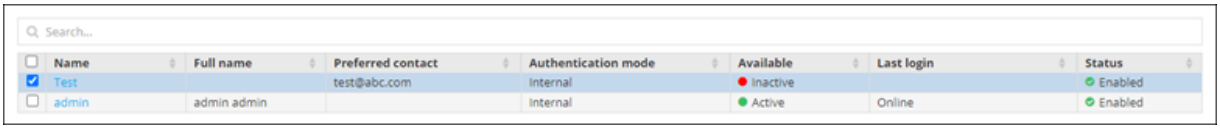
To disable a user:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Account** > **User**.



   The **User** page is displayed.

3. From the **User** page, select the check box against the user you want to disable.



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

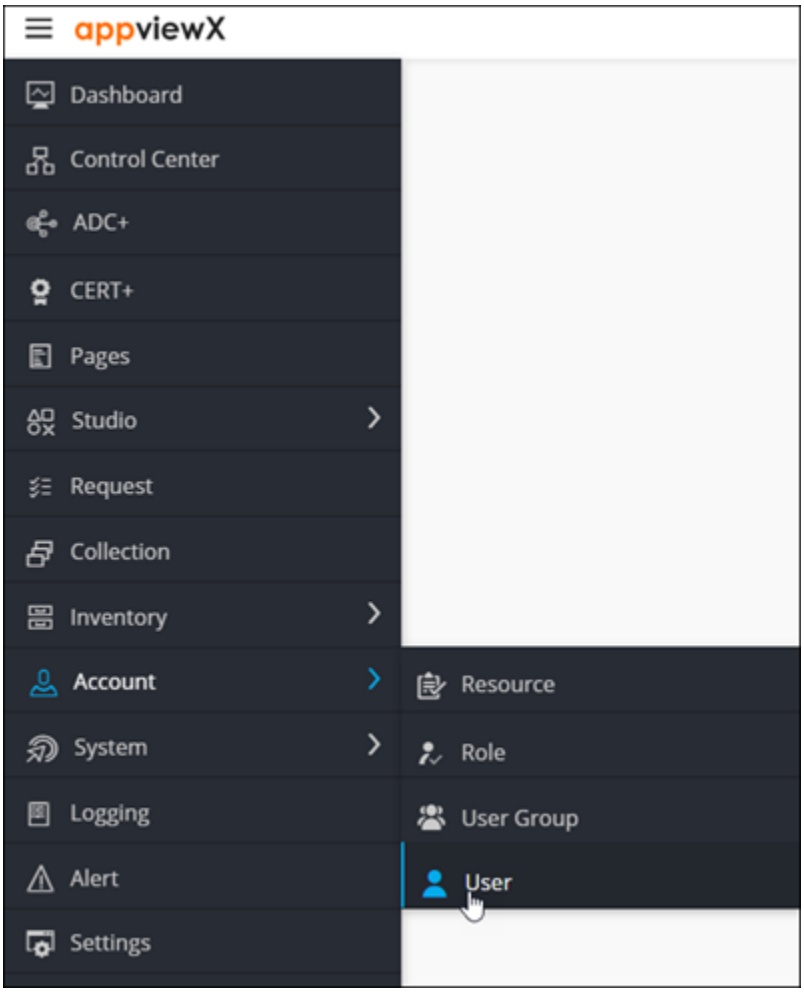
.
5. In the **Confirmation** dialog box, click **Yes**.

   The selected user is disabled.

Deleting a User

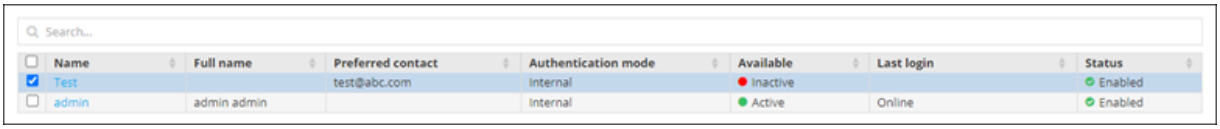
To delete a user:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Account** > **User**.



The **User** page is displayed.

3. From the **User** page, select the check box against the user you want to delete.



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

.

5. In the **Confirmation** dialog box, click **Yes**.
   The selected user is deleted.

Managing User Groups

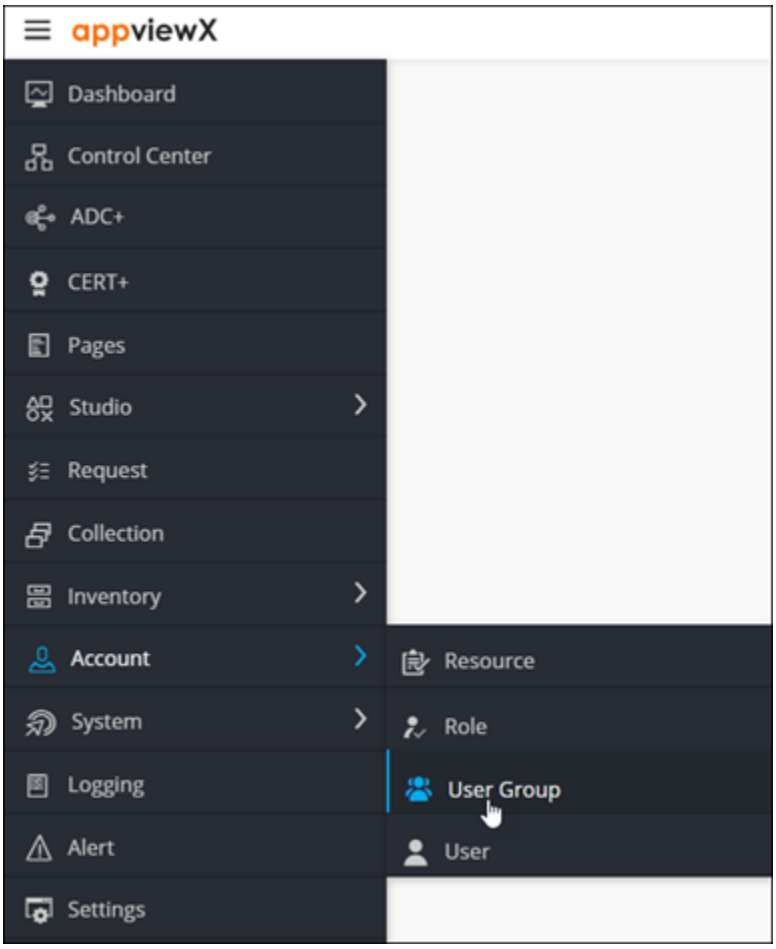
A user group is a set of individual users assigned with the same roles and resources. You can associate one or more roles and resources to a user group. Users within that user group are granted the role and resource permissions.

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

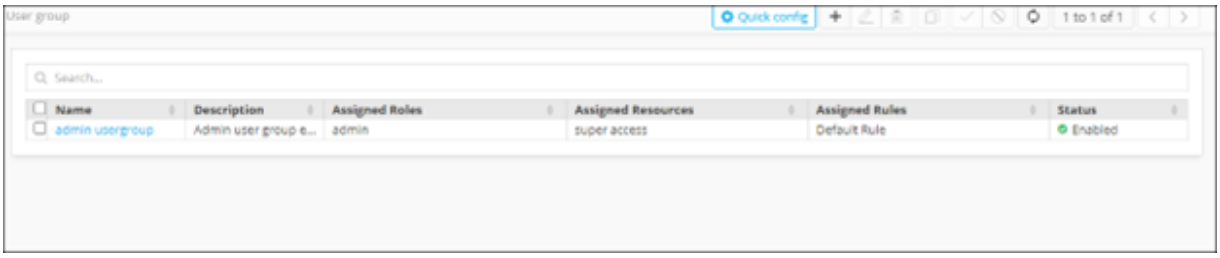
Creating a User Group

To create a user group:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the icon.
2. From the menu displayed, select **Account** > **User Group**.



The **User Group** page is displayed.



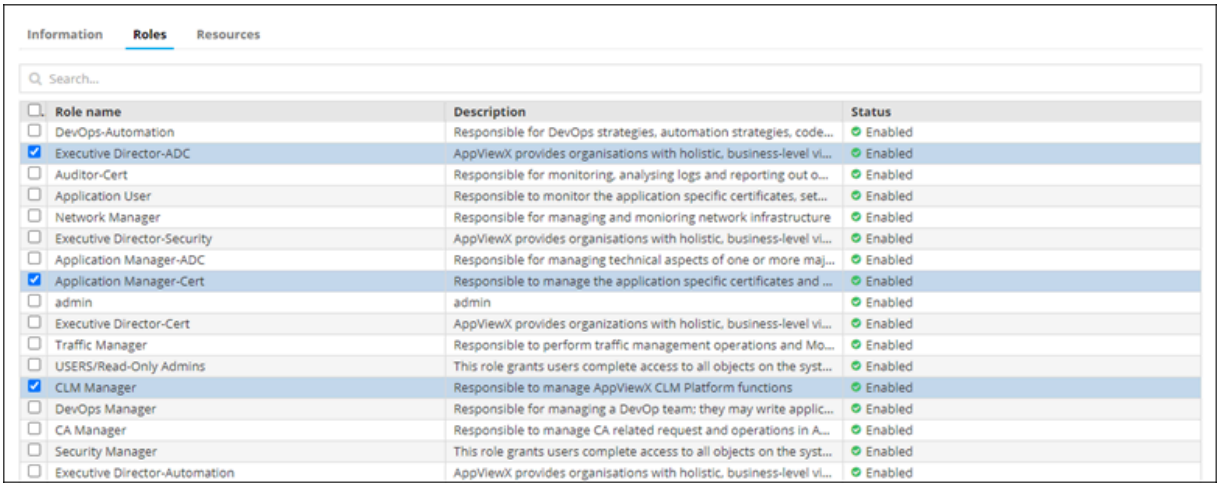
3. From the top right corner of the screen, click 

.
4. The **Add** page is displayed, with the **Information** tab open by default.

5. Enter the following details:

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).
All * marked fields are mandatory.	

6. Click **Save**.
7. 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,

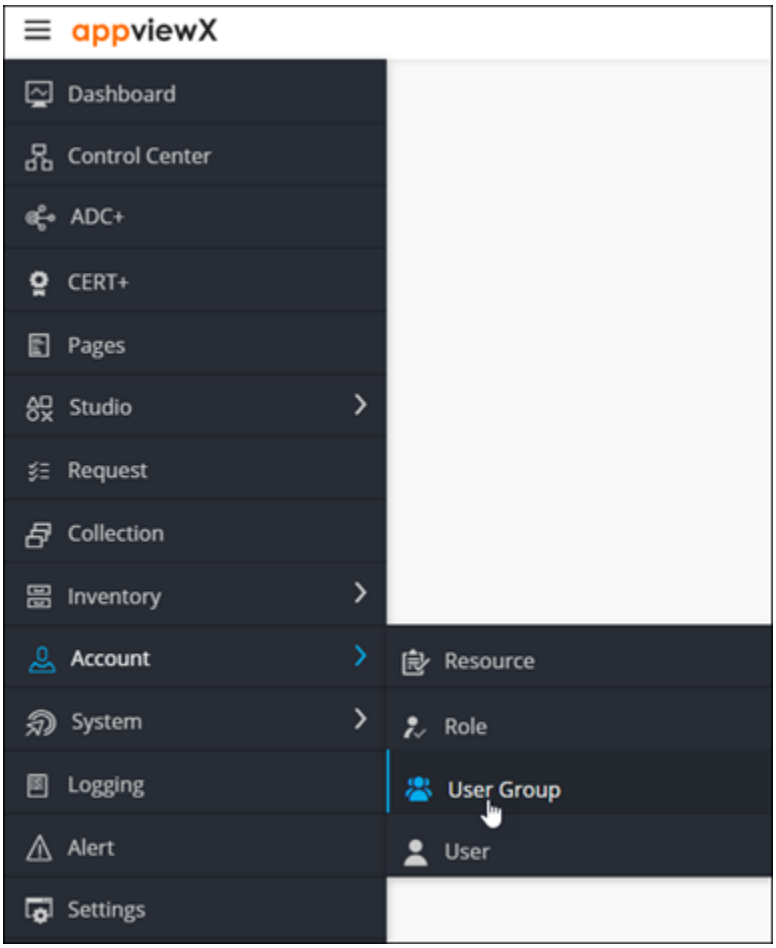
the higher-level access permissions (Read/Write) take precedence and the user has Read/Write access.

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.

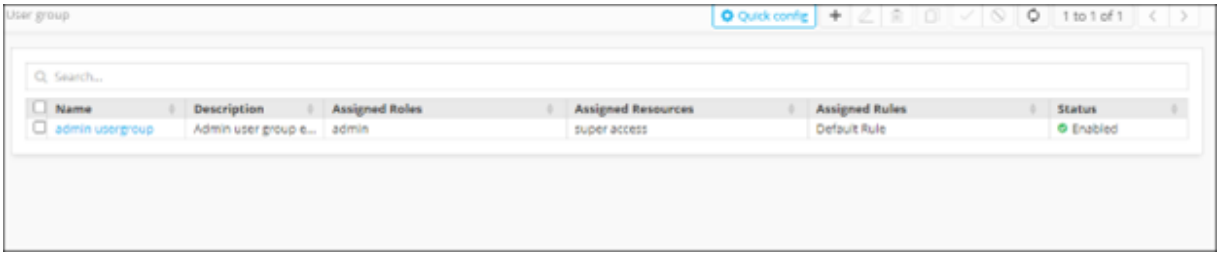
Cloning a User Group

To clone a user group:

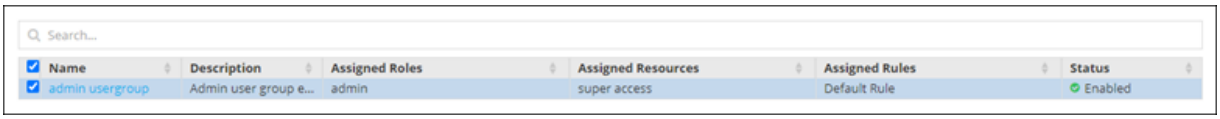
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, select **Account** > **User Group**.



The **User Group** page is displayed.



3. From the **User Group** page, select the user group you want to clone.



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

.
5. The **Cloning** page is displayed, with the **Information** tab open by default.

6. Update the required details:

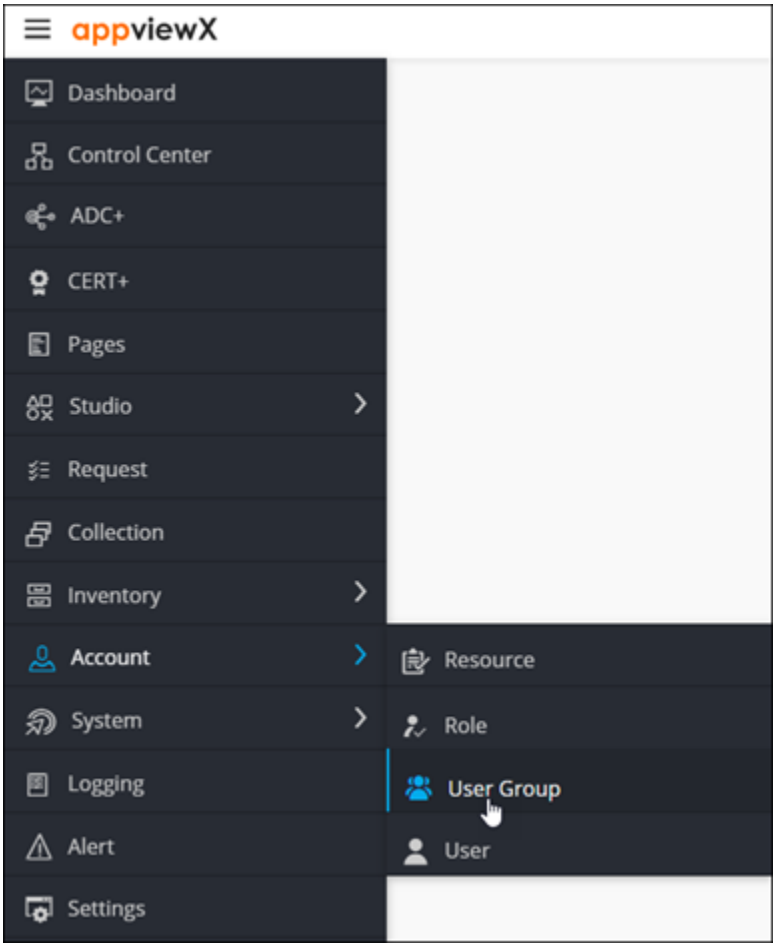
Field	Description
***Name**	User group name.
Description	Brief description of the group (which makes it easy for the administrators to decide if a user should be assigned to this group or not).
All * marked fields are mandatory.	

7. Click **Save**.

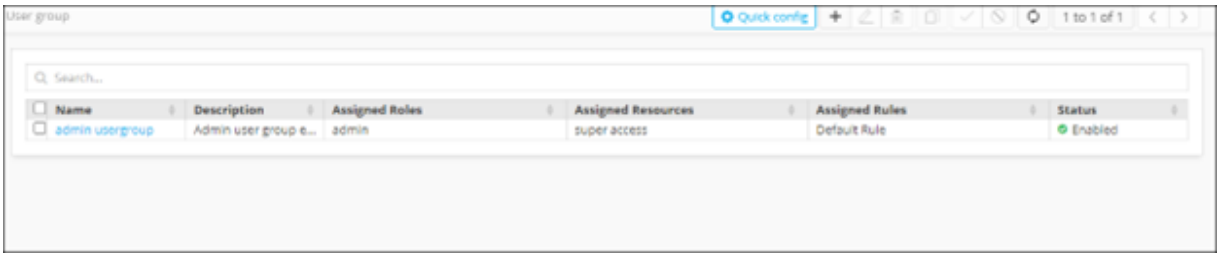
Modifying a User Group

To create a user group:

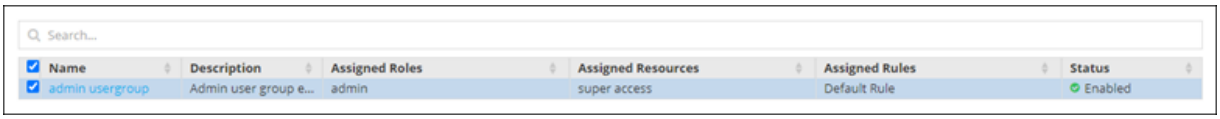
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, select **Account** > **User Group**.



The **User Group** page is displayed.



3. From the **User Group** page, select the user group you want to modify.



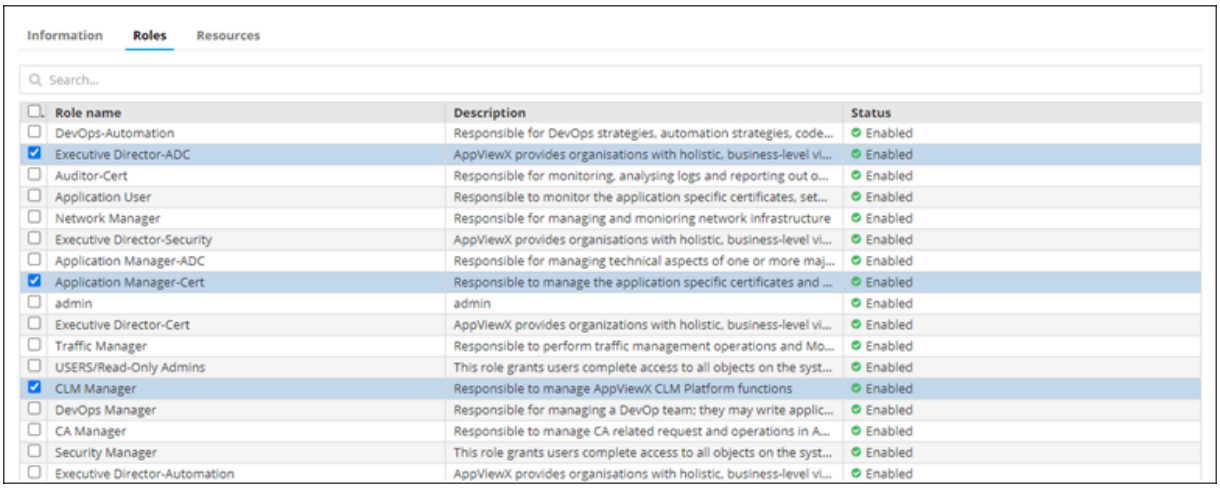
4. From the top right corner of the screen, click 

.
5. The **Modify** page is displayed, with the **Information** tab open by default.

6. Update the required details:

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).
All * marked fields are mandatory.	

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

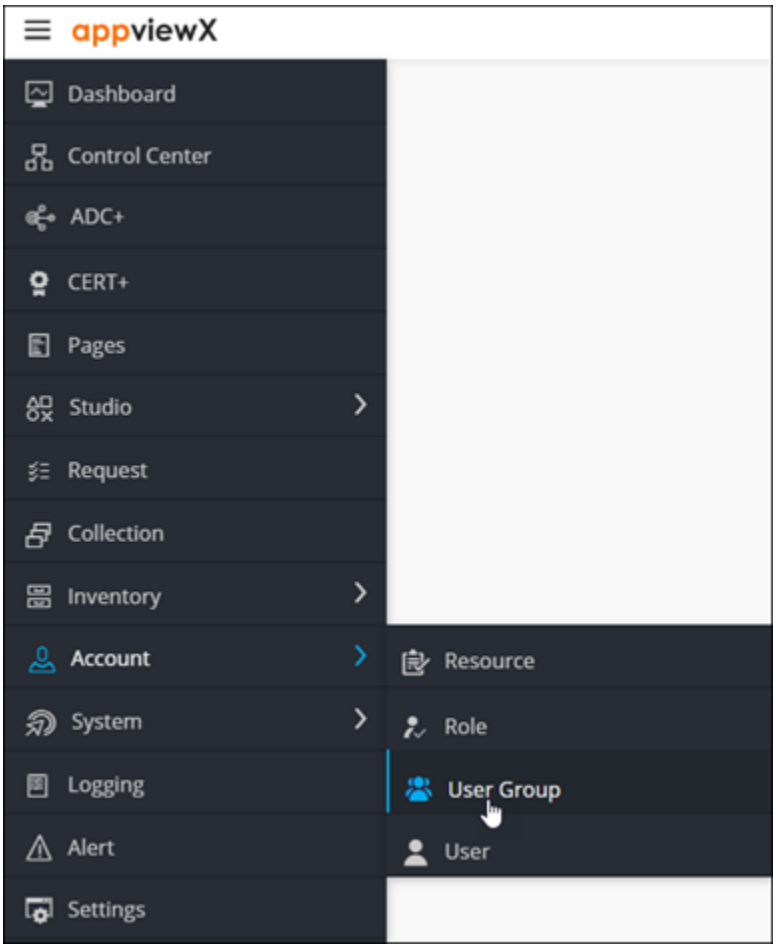


.

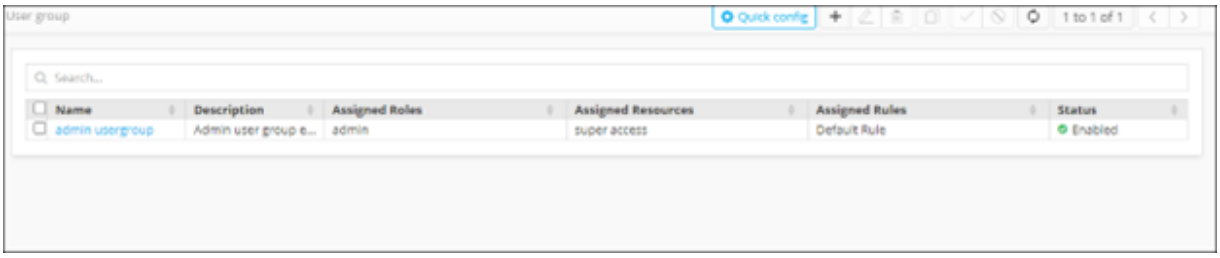
Enabling a User Group

To enable a user group:

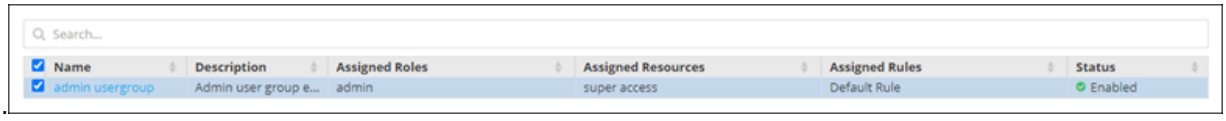
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, select **Account** > **User Group**.



The **User Group** page is displayed.



3. From the **User Group** page, select the user group you want to enable.



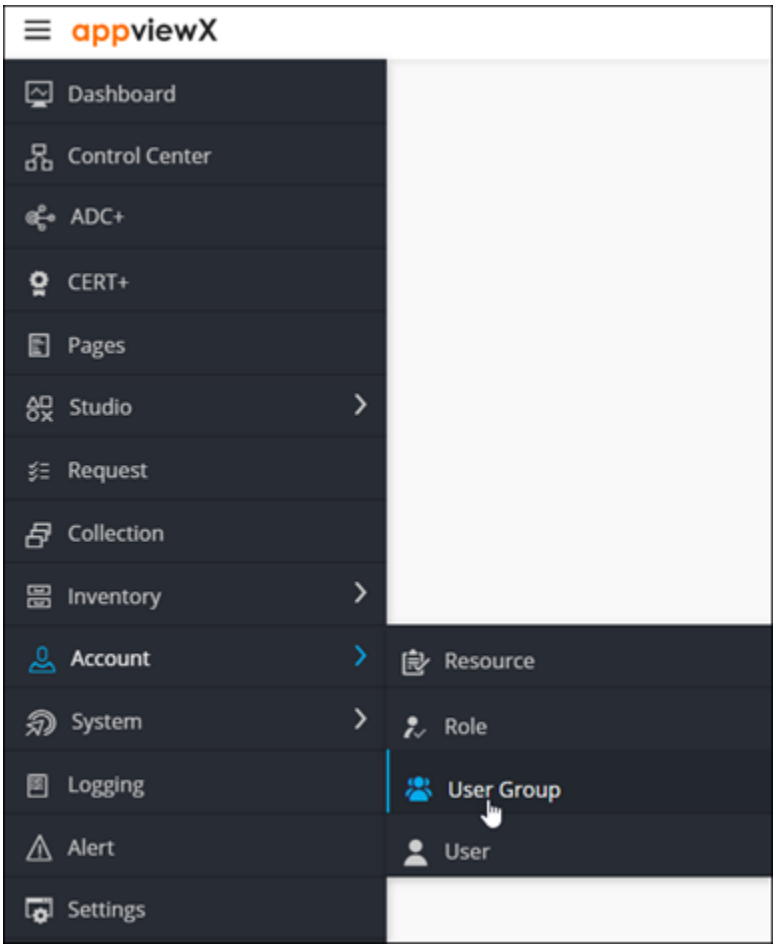
4. From the top right corner of the screen, click 

.
5. In the **Confirmation** dialog box, click **Yes**.

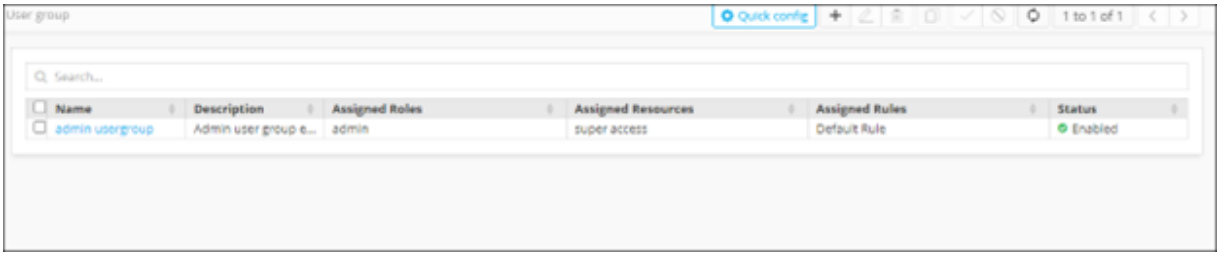
Disabling a User Group

To disable a user group:

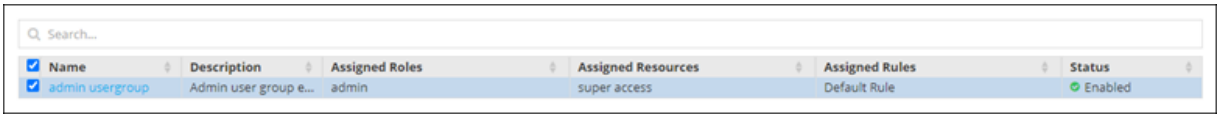
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, select **Account** > **User Group**.



The **User Group** page is displayed.



3. From the **User Group** page, select the user group you want to disable.



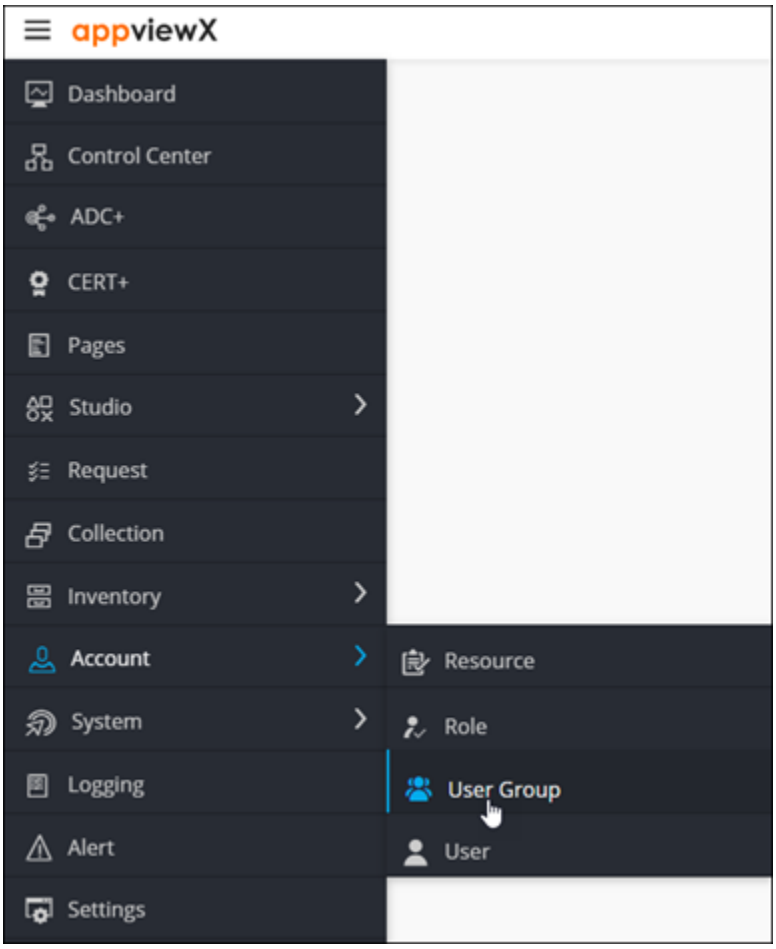
4. From the top right corner of the screen, click 

.
5. In the **Confirmation** dialog box, click **Yes**.

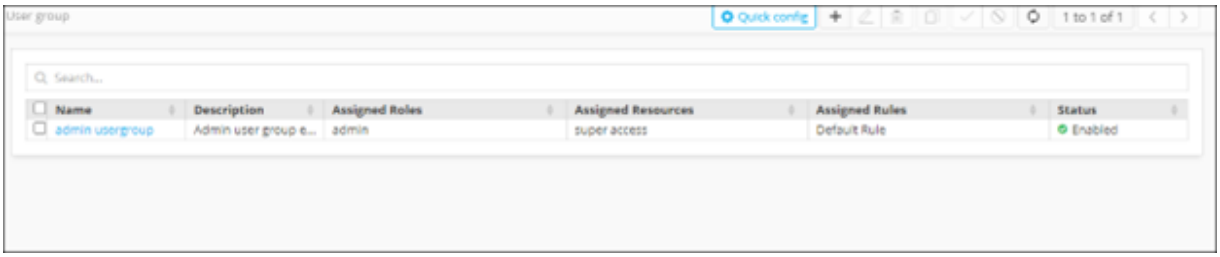
Deleting a User Group

To delete a user group:

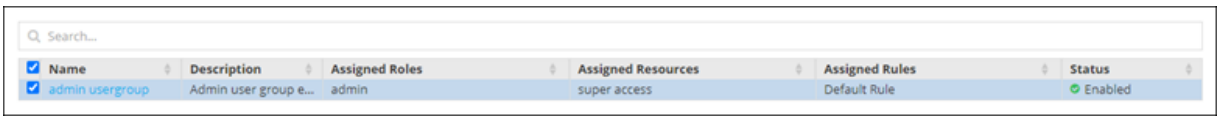
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, select **Account** > **User Group**.



The **User Group** page is displayed.



3. From the **User Group** page, select the user group you want to delete.



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

.
5. In the **Confirmation** dialog box, click **Yes**.

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 the Quick Config Option

Quick Config wizard flow can be accessed in the following ways:

- Navigate to **Menu** > **Settings** > **General** > **Authentication** > **Quick Config**.
- Navigate to **Menu** > **Account** > **User group** > **Quick Config**.
- Navigate to **Account** > **Role** > **Quick Config**.
- Navigate to **Account** > **Resource** > **Quick Config**.

Once you access the Quick Config options using any of the above methods, the Authentication stage opens in a wizard flow with the LDAP sub-tab displayed by default. On the same screen as part of wizard flow, user groups, roles, and resources stages are displayed at the top. Click on the respective stage for configuration.

- Authentication
- Resource

- Role
- User Group

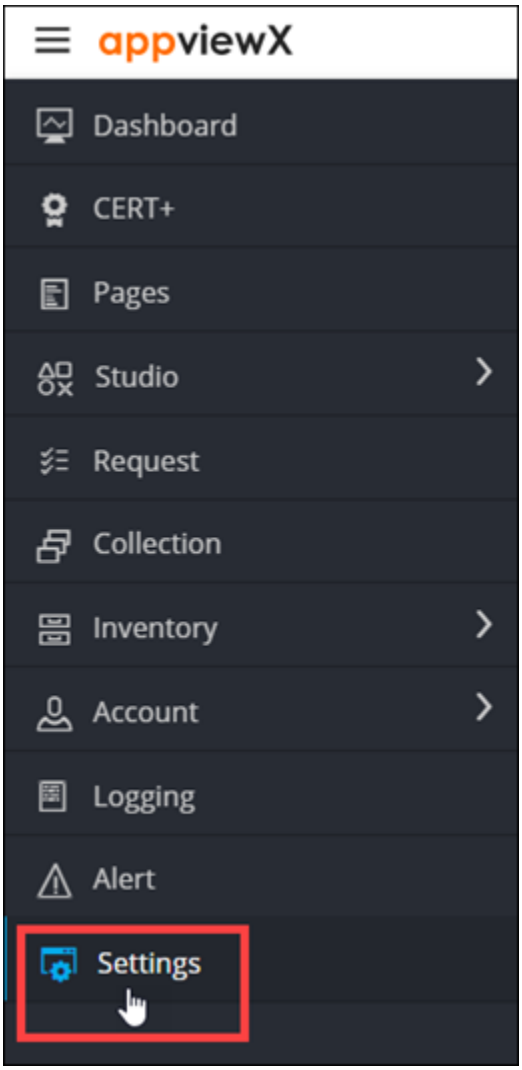
Authentication

- 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

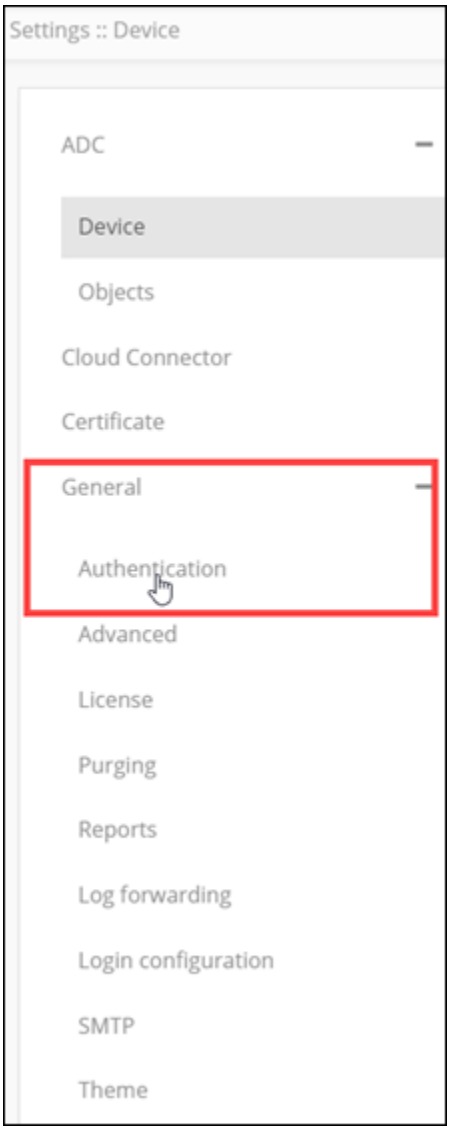
Configure the Role-Based Access Control for LDAP

To configure the RBAC settings for LDAP:

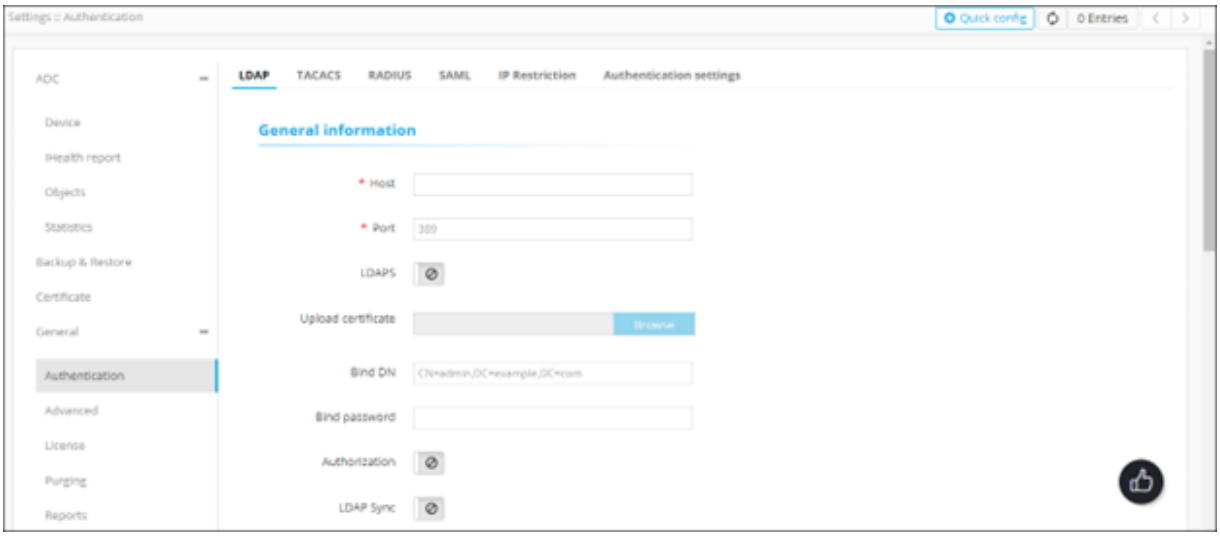
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



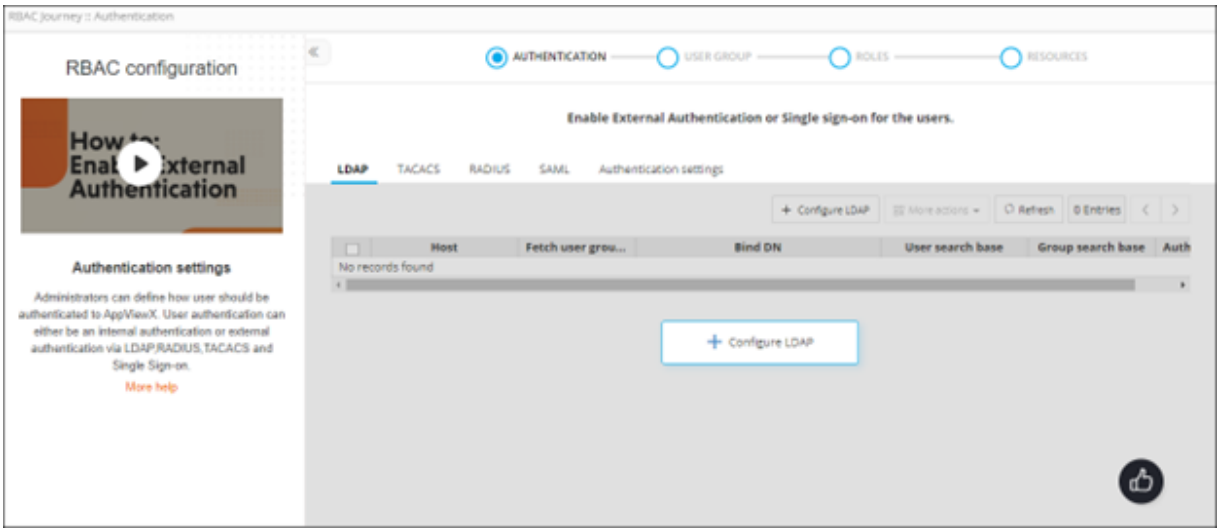
3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Authentication**.



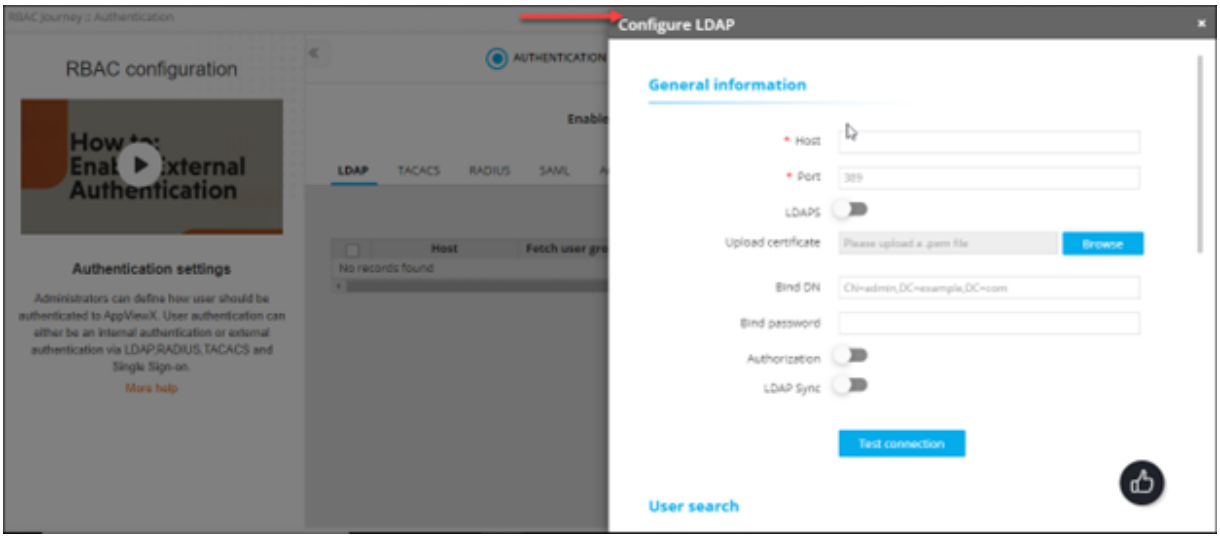
The **Settings :: Authentication** page is displayed, with the **LDAP** tab open by default.



5. From the top-right corner of the screen, click **Quick Config**. The **RBAC Journey :: Authentication** page is displayed.



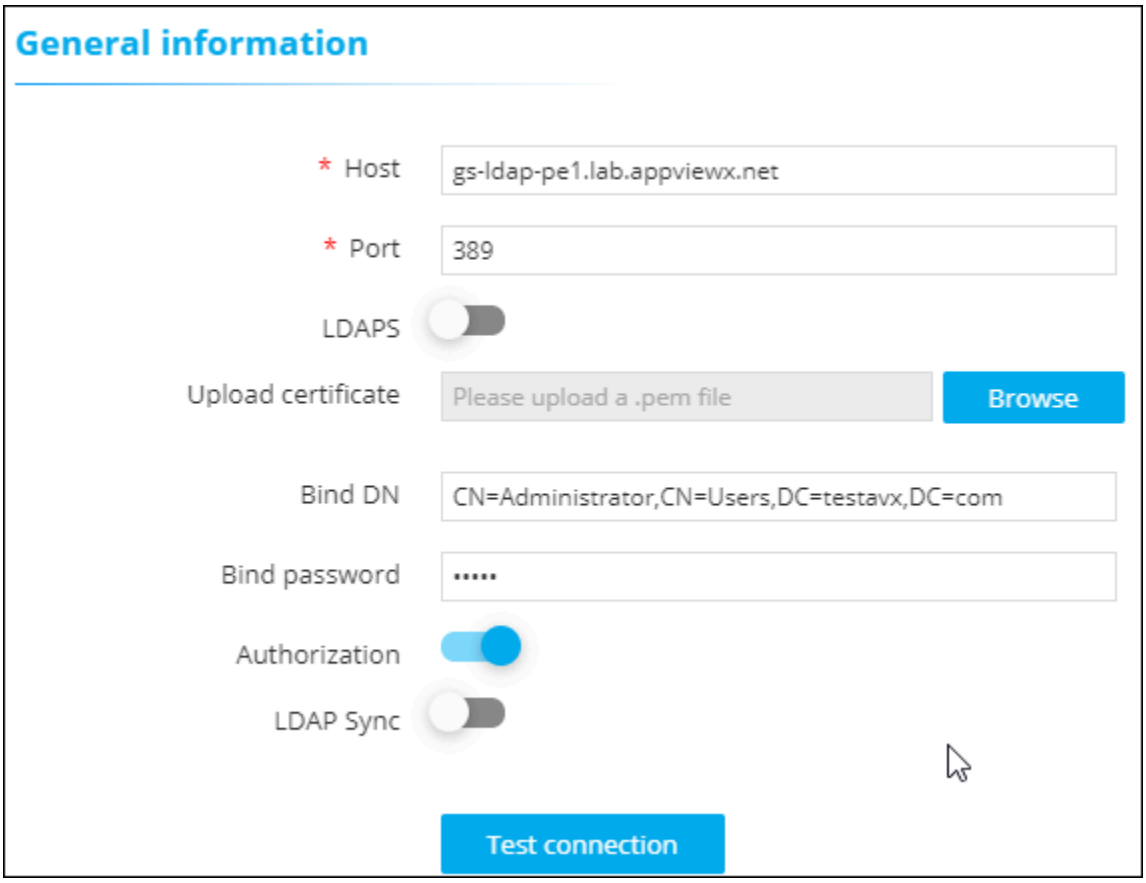
6. On the **RBAC Journey :: Authentication** page, click **Configure LDAP**.
   The **Configure LDAP** action pane is displayed.



7. In the **General Information** section, enter the following details (sample values are shown in the image below the table):

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.

Field	Description
	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.
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.
All * marked fields are mandatory.	



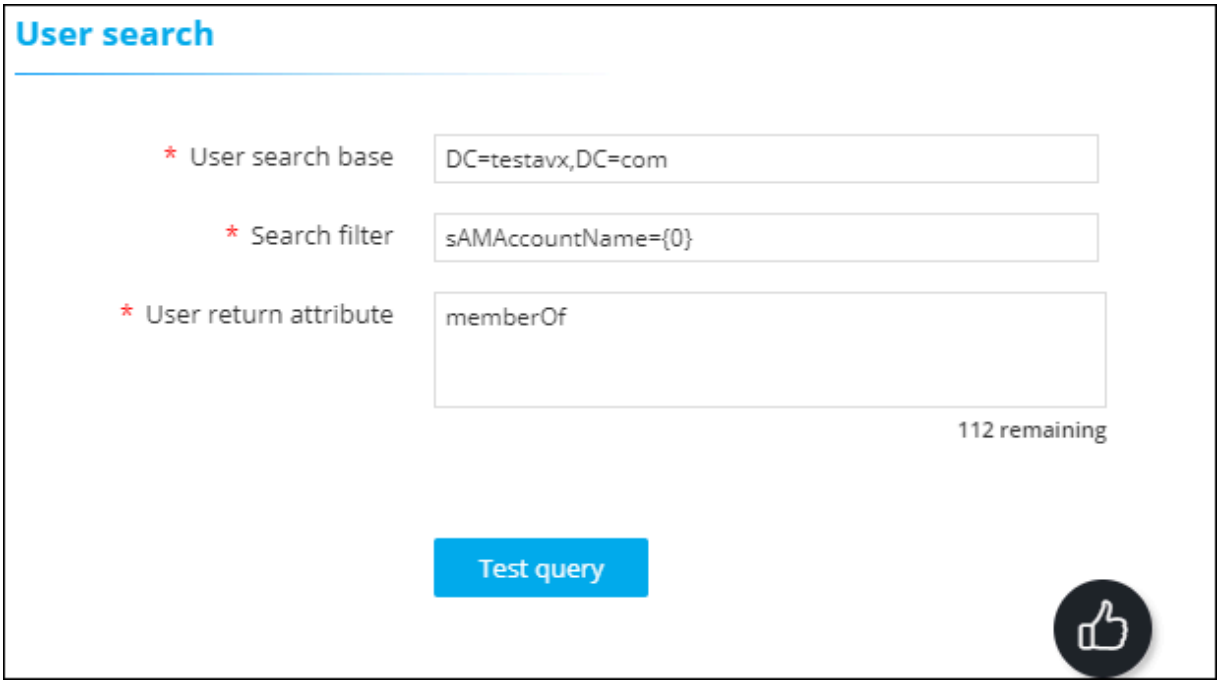
8. After entering the above connection details, to test if the host is reachable and the port is valid for establishing an LDAP/LDAPS connection, click **Test Connection**.

> **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.

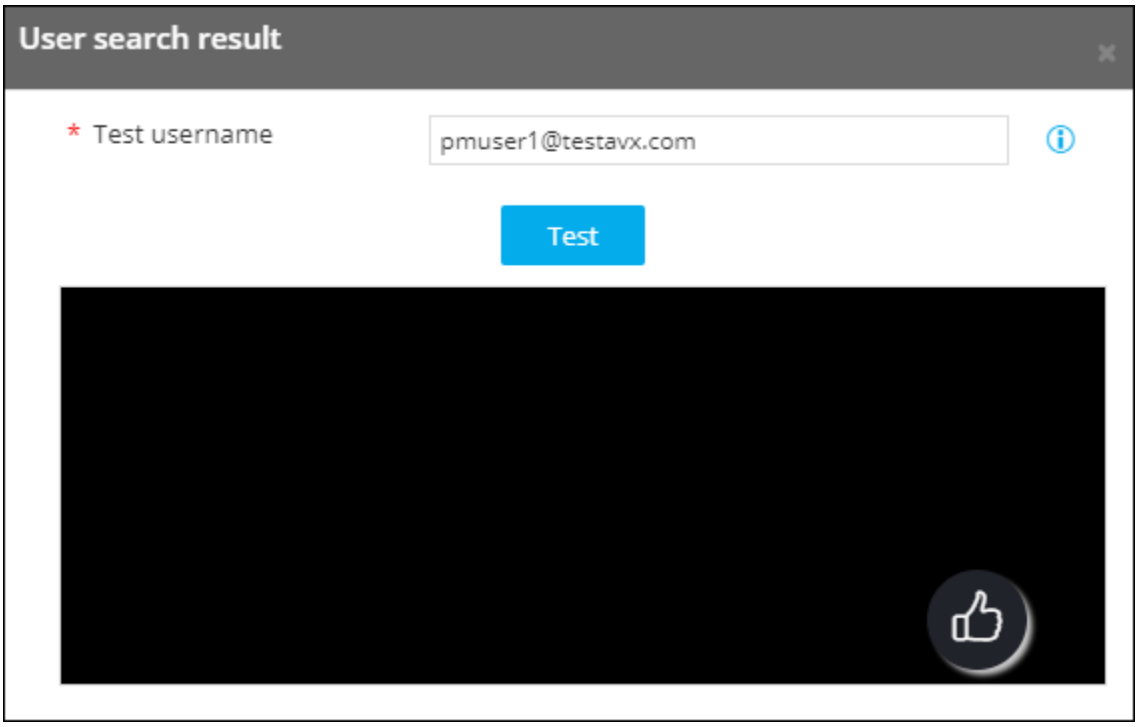
9. The **User Search** section collects information to validate a user's presence in the Active Directory. In the **User Search** section, enter the following details(sample values are shown in the image below the table):

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.

Field	Description
	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.
All * marked fields are mandatory.	



10. After entering the above details, to test if the user is present in the Active Directory, click **Test query**.
11. 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.

12. 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	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.

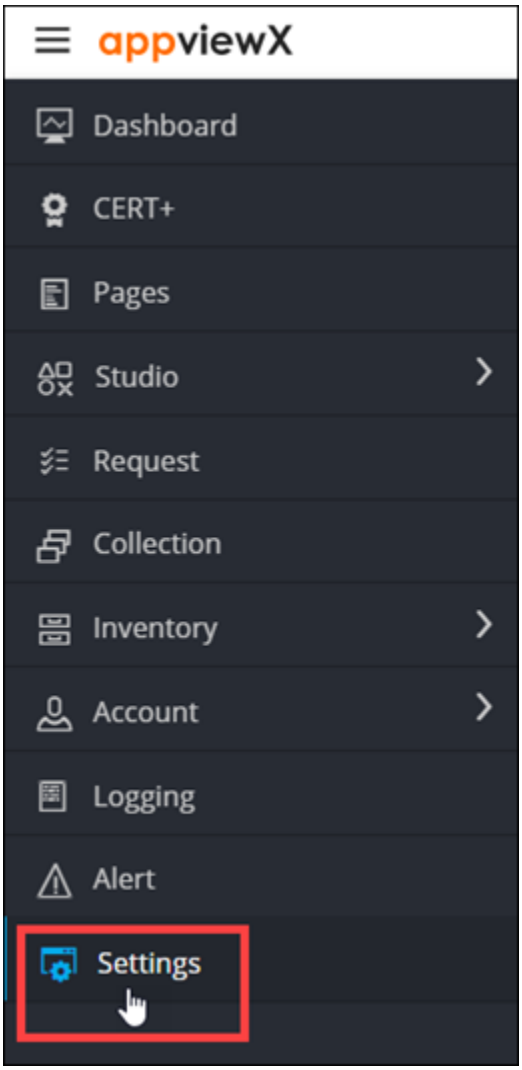
Note: Group search can be performed only if the customer's LDAP is of type Open LDAP. Microsoft Active Directory does not need group search configuration. For Open LDAP, group search needs to be configured mandatorily. The User return attribute in the User search section does not return the group membership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

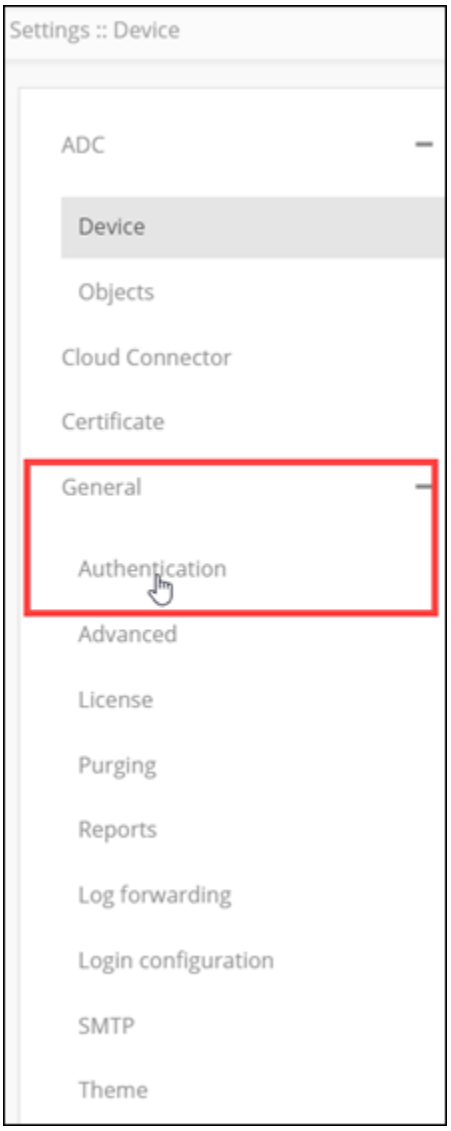
Deleting a LDAP Configuration

To delete a LDAP configuration:

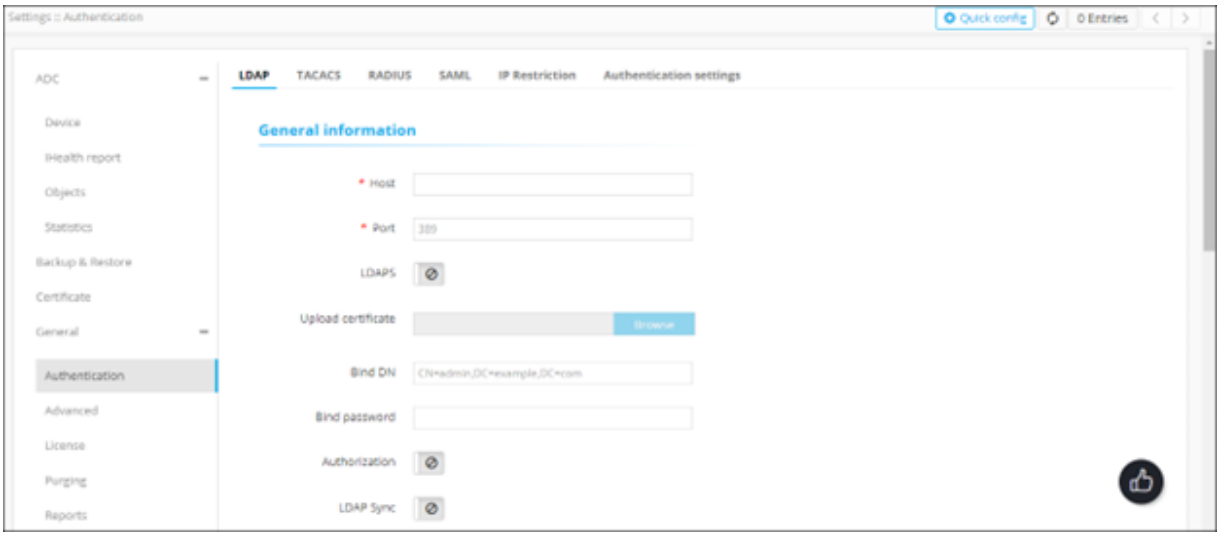
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the icon.
2. From the menu displayed, click **Settings**.



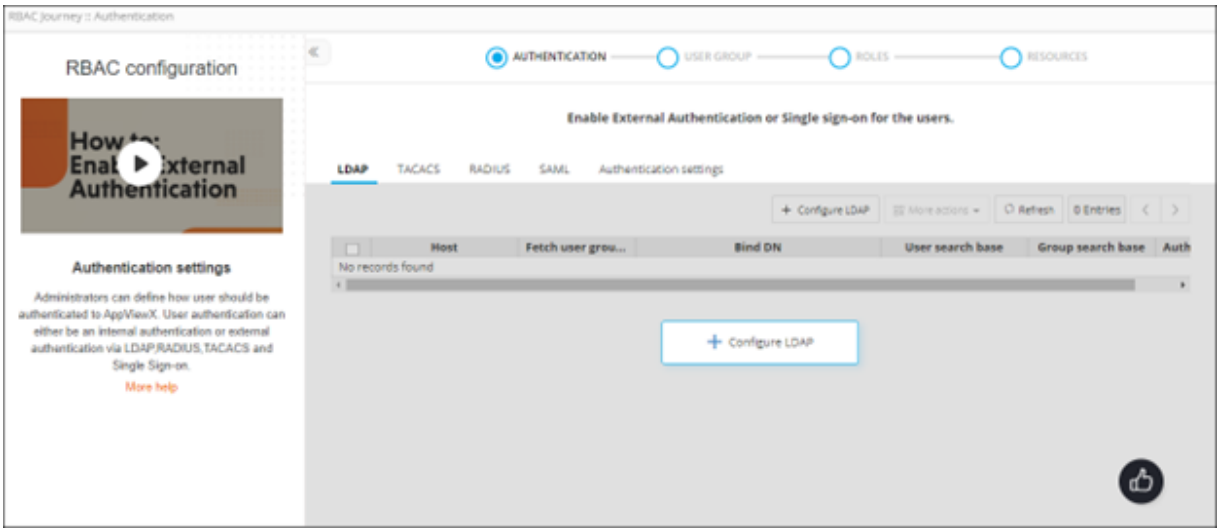
3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Authentication**.



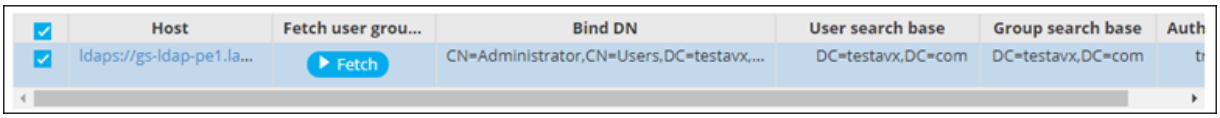
The **Settings :: Authentication** page is displayed, with the **LDAP** tab open by default.



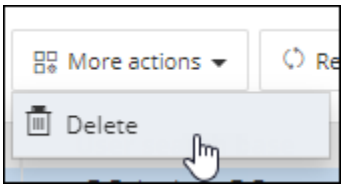
5. From the top-right corner of the screen, click **Quick Config**.
   The **RBAC Journey :: Authentication** page is displayed.



6. From the table of LDAP configurations, to delete a LDAP configuration, select the check box corresponding to that entry.



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

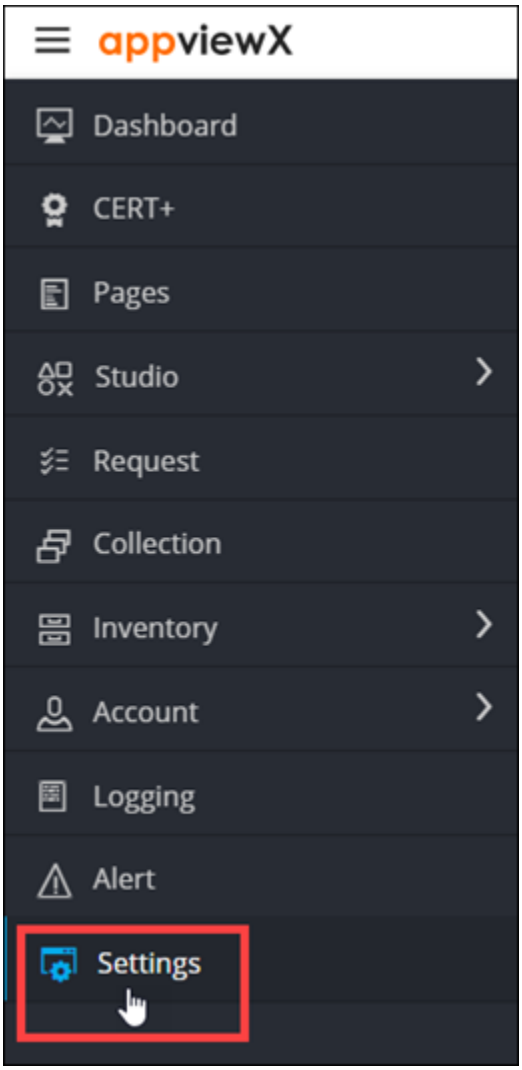


8. In the **Confirmation** dialog box, click **Delete**.
   The selected configuration is deleted.

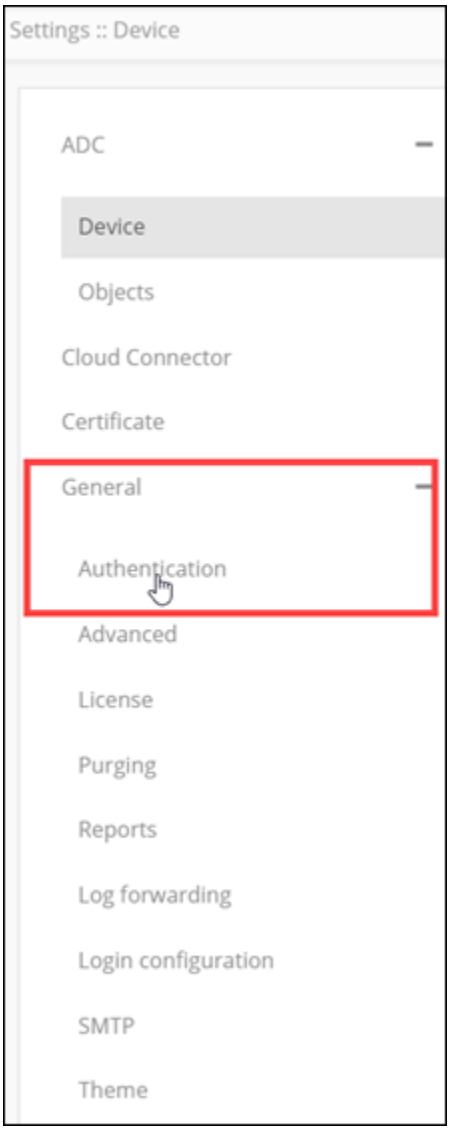
Configuring Role-Based Access Control for TACACS

To configure RBAC for TACACS authentication:

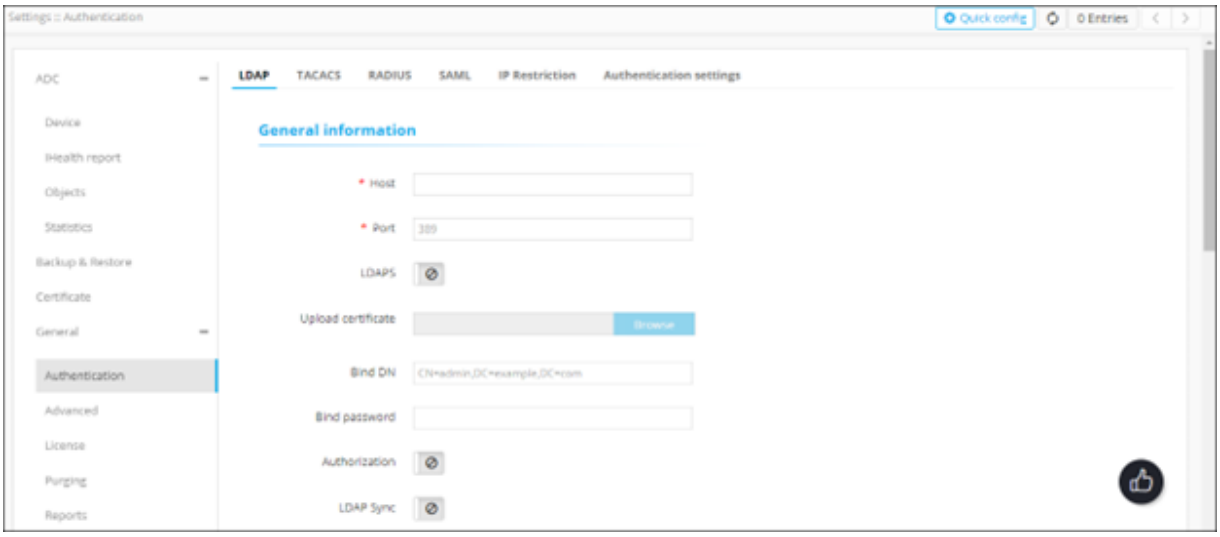
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Authentication**.

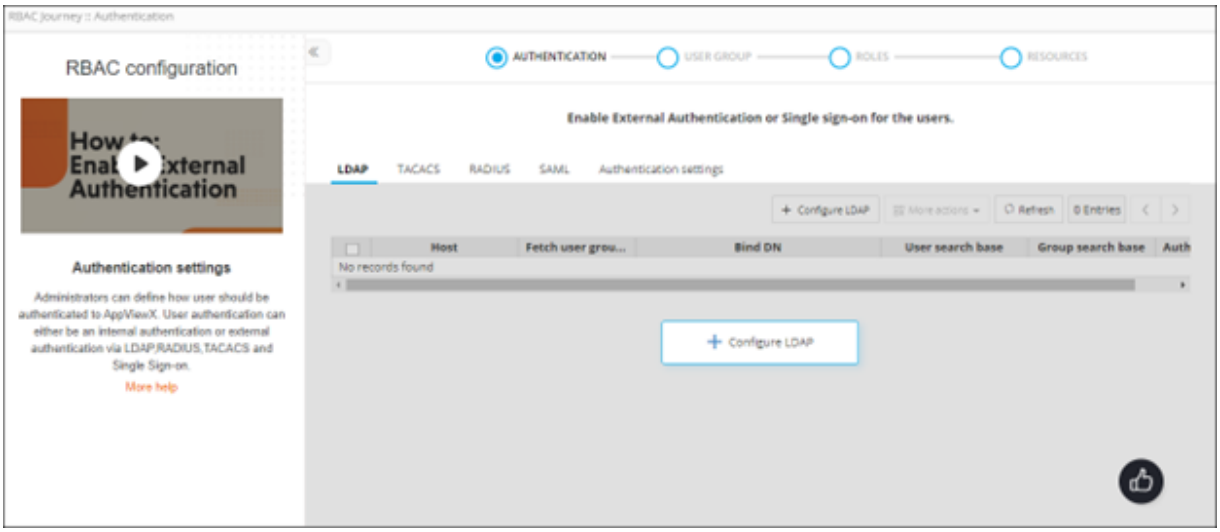


The **Settings :: Authentication** page is displayed, with the **LDAP** tab open by default.

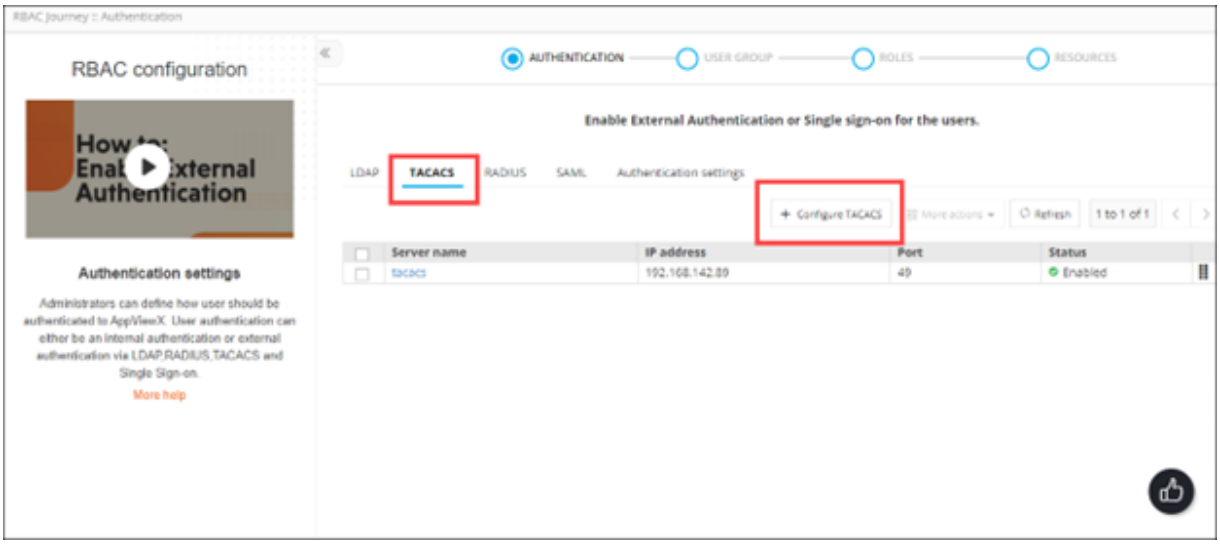


5. From the top-right corner of the screen, click **Quick Config**.

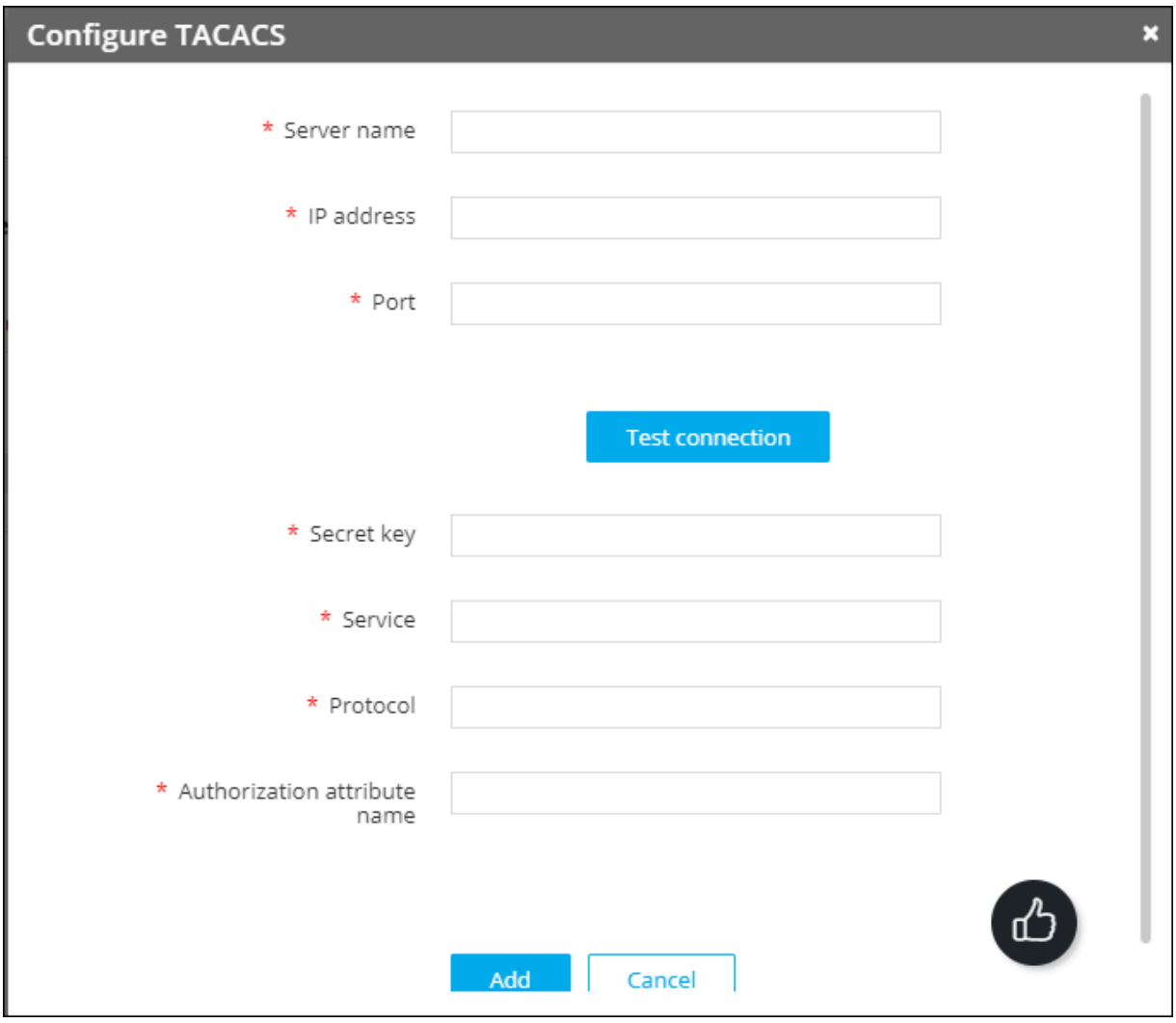
   The **RBAC Journey :: Authentication** page is displayed.



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



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



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

Field	Description
***Server name**	Name of the TACACS server.
***IP address**	IP address of the TACACS server.
***Port**	Port number of the TACACS server
All * marked fields are mandatory.	

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

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.
All * marked fields are mandatory.	

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

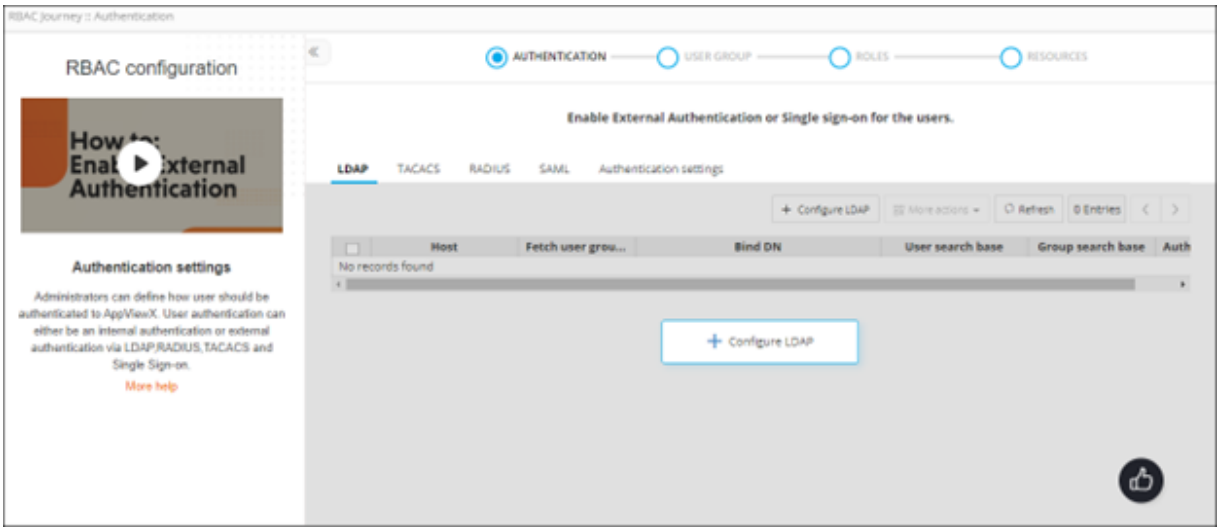
Note: In the case of multiple TACACS servers, to define/update the order in which the servers will be authenticated, drag and drop the entries in this table.

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

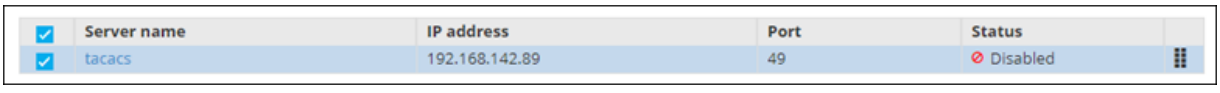
Enabling a TACACS Configuration

To enable a TACACS configuration:

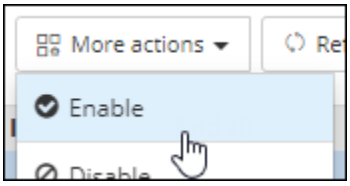
1. Navigate to the **Settings :: Authentication** page.
2. On the **Settings :: Authentication** page, from the top-right corner of the screen, click **Quick Config**. The **RBAC Journey :: Authentication** page is displayed.



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



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

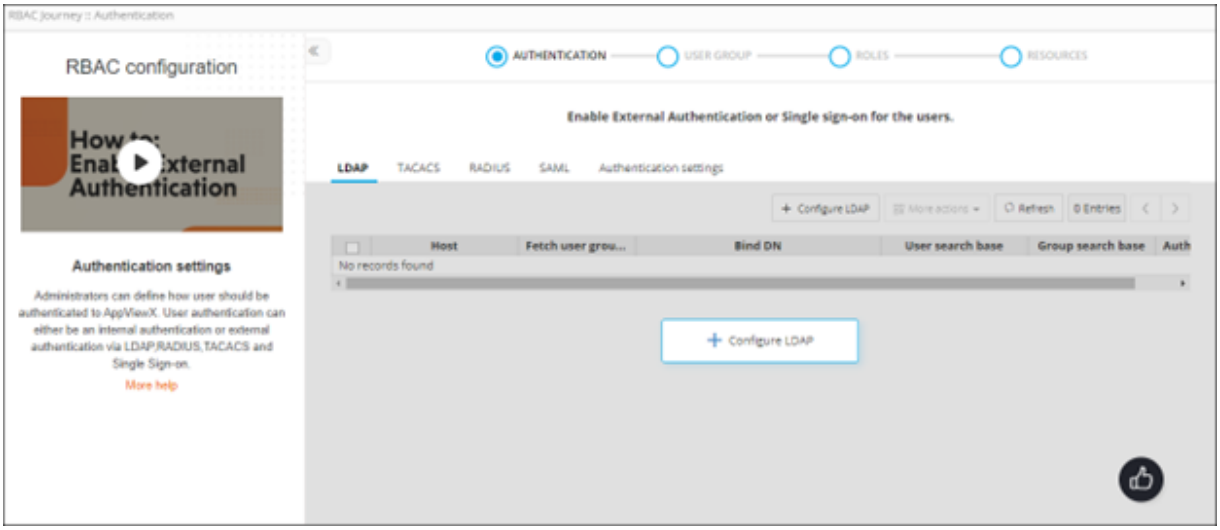


6. In the **Confirmation** message dialog box, click **Proceed**.
   The selected configuration is enabled.

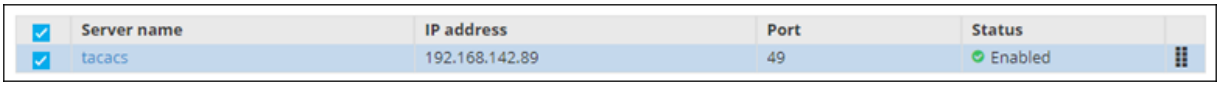
Disabling a TACACS Configuration

To disable a TACACS configuration:

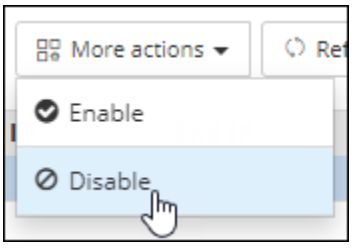
1. Navigate to the **Settings :: Authentication** page.
2. On the **Settings :: Authentication** page, from the top-right corner of the screen, click **Quick Config**.
   The **RBAC Journey :: Authentication** page is displayed.



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



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

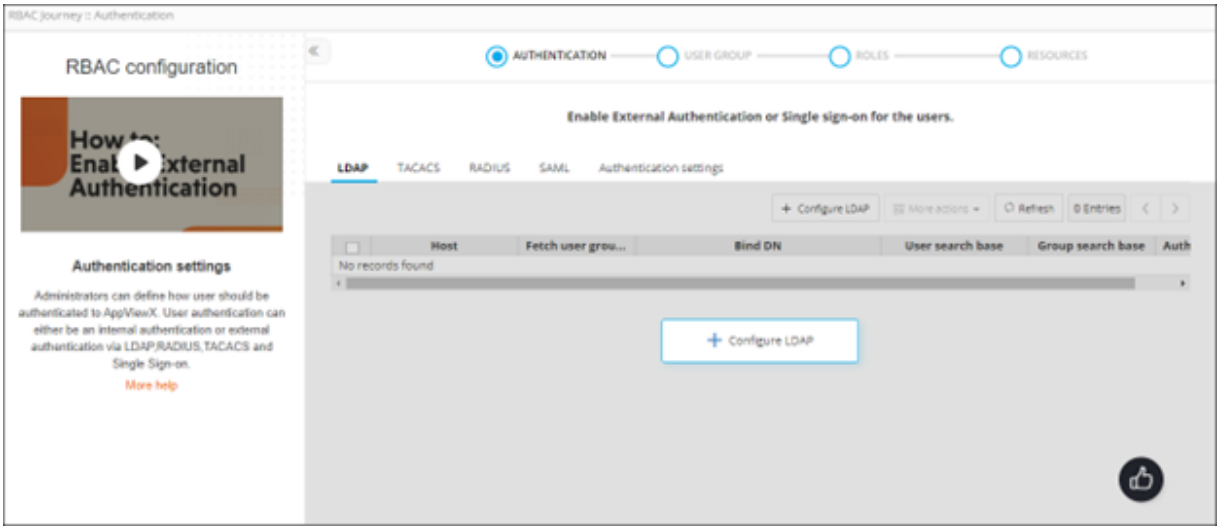


6. In the **Confirmation** message dialog box, click **Proceed**.
   The selected configuration is disabled.

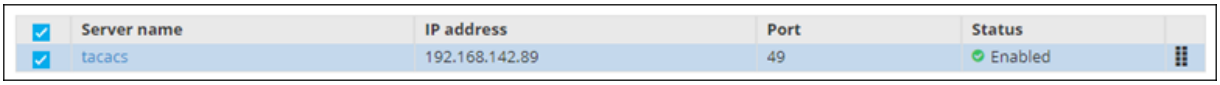
Deleting a TACACS Configuration

To delete a TACACS configuration:

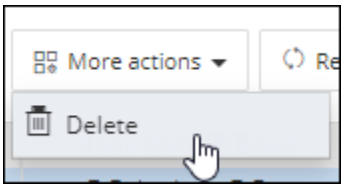
1. Navigate to the **Settings :: Authentication** page.
2. On the **Settings :: Authentication** page, from the top-right corner of the screen, click **Quick Config**.
   The **RBAC Journey :: Authentication** page is displayed.



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



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

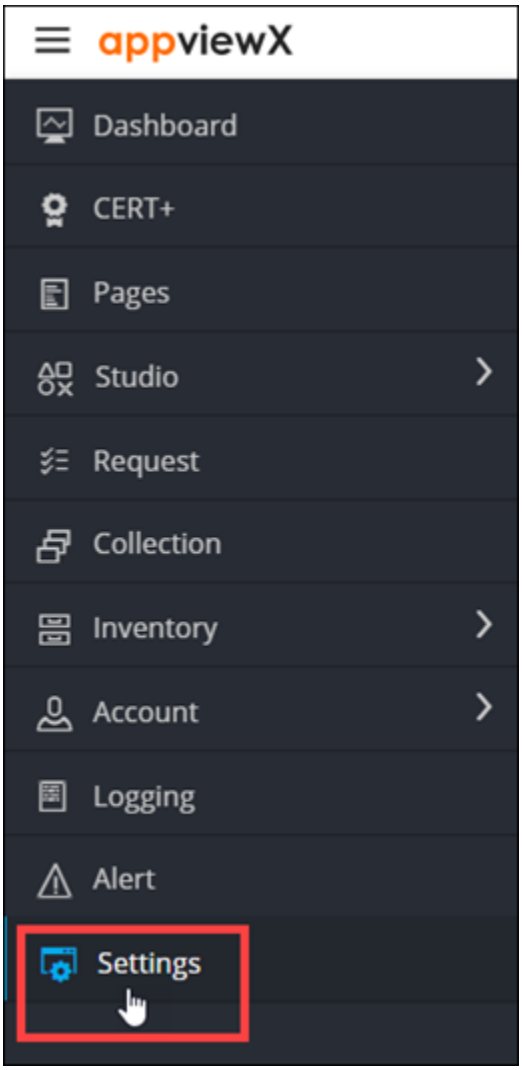


6. In the **Confirmation** message dialog box, click **Proceed**.
   The selected configuration is deleted.

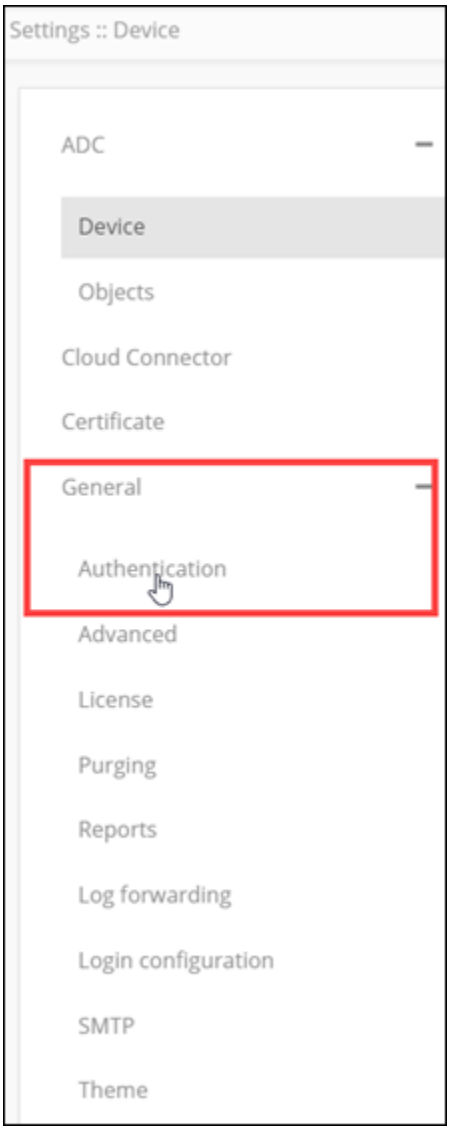
Configuring Role-Based Access Control for RADIUS

To configure RBAC for RADIUS authentication:

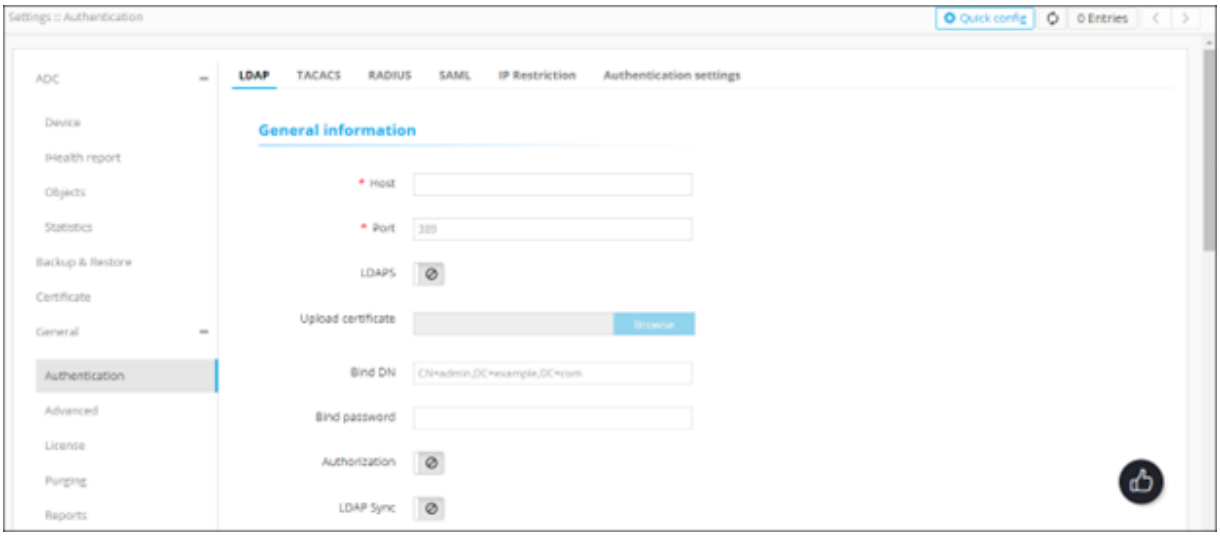
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Settings**.



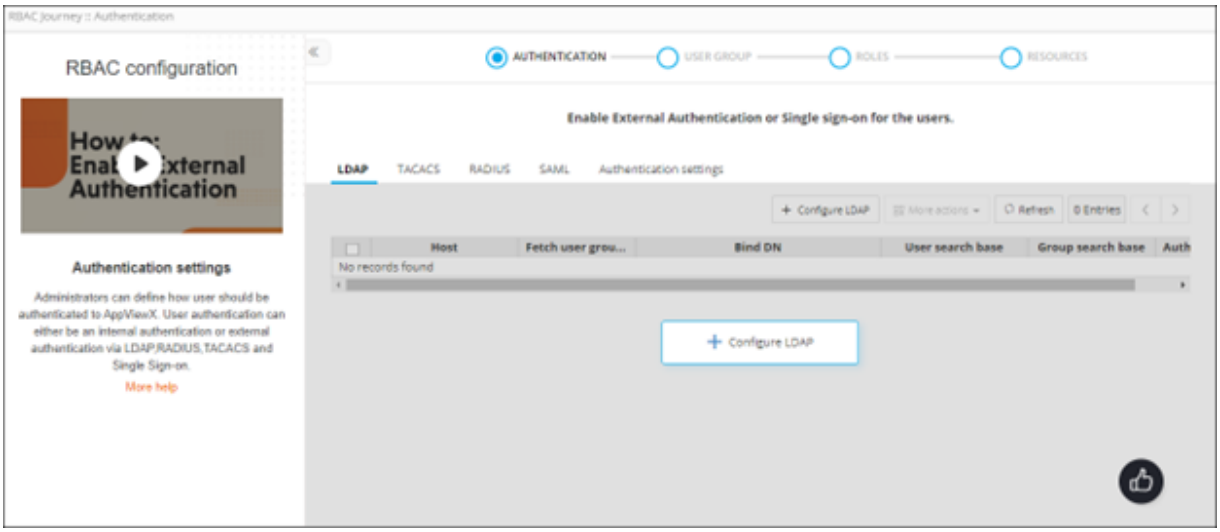
3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Authentication**.



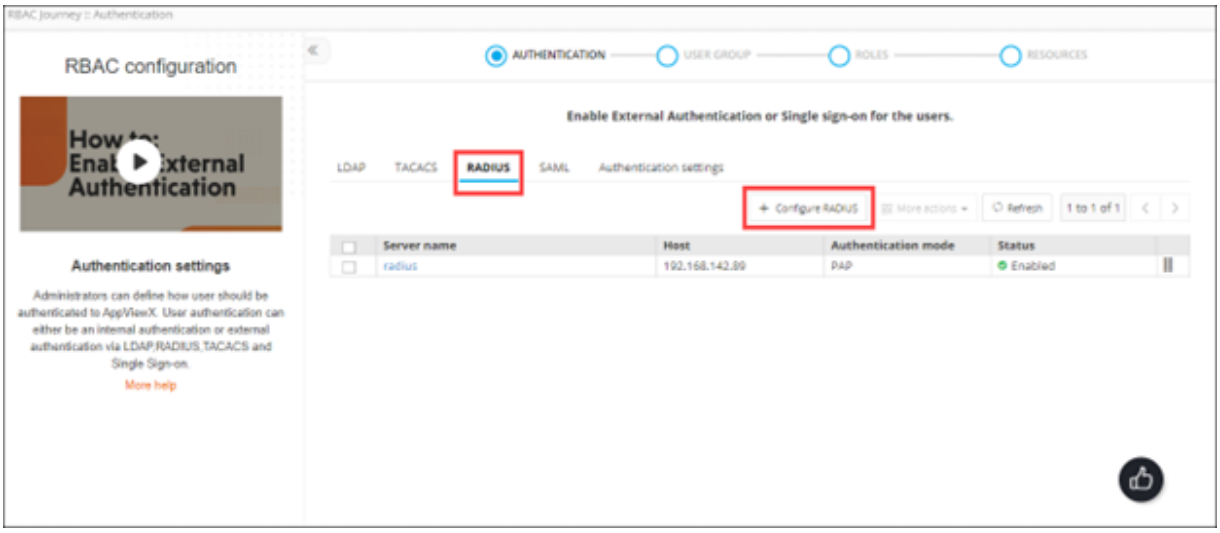
The **Settings :: Authentication** page is displayed, with the **LDAP** tab open by default.



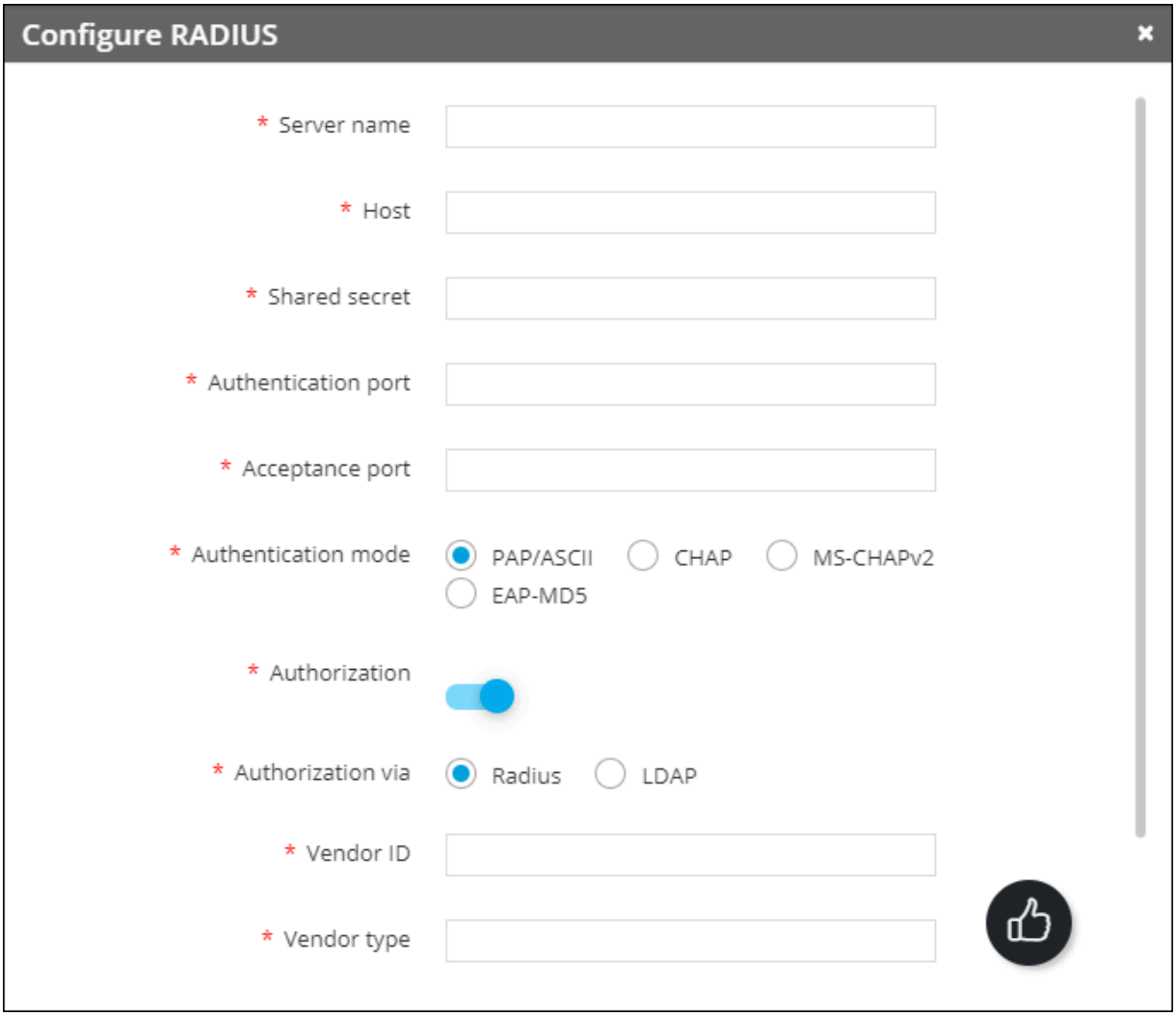
5. From the top-right corner of the screen, click **Quick Config**. The **RBAC Journey :: Authentication** page is displayed.



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



The Configure RADIUS action is displayed.

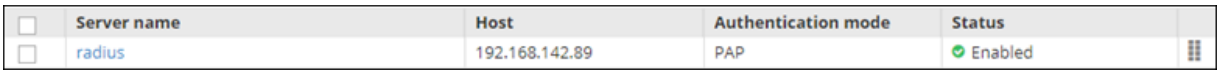


7. Enter the field information as described in the following table:

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 sysadmin 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 sysadmin 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 whrn the the Authorization toggle is turned on.
***Vendor ID**	Enter the vendor ID.

Field	Description
	Note: This field is enabled only whrn the 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 whrn the the Authorization toggle is turned on and authorization is done via the RADIUS server. **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 whrn the the Authorization toggle is turned on and authorization is done via the LDAP server.
All * marked fields are mandatory.	

8. 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:

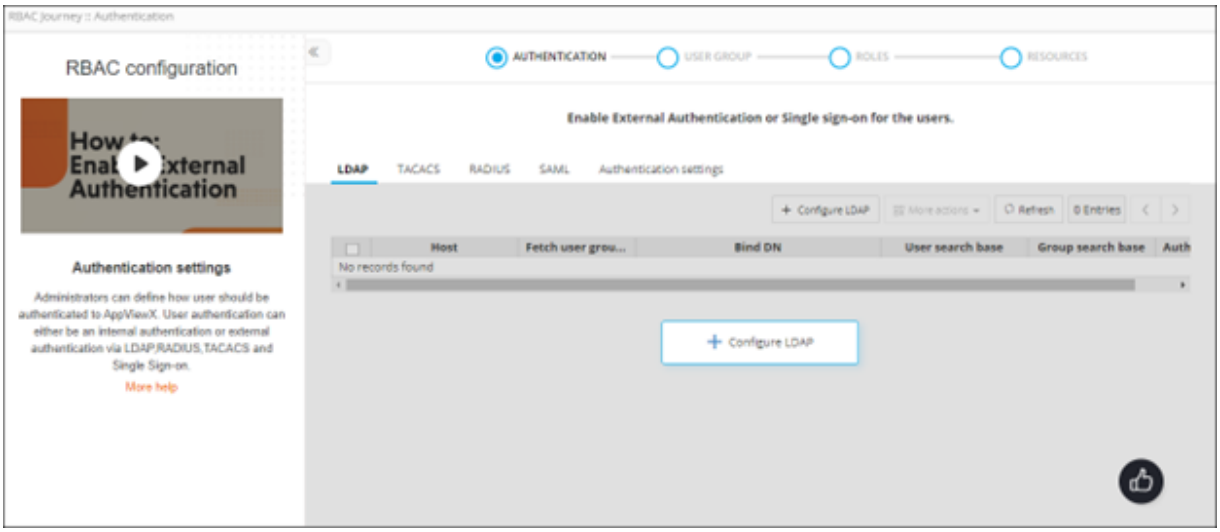


Note: In the case of multiple RADIUS servers, to define/update the order in which the servers will be authenticated, drag and drop the entries in this table.

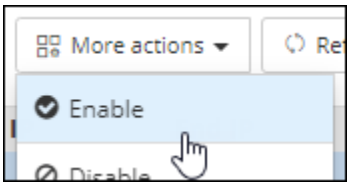
Enabling a RADIUS Configuration

To enable a RADIUS configuration:

1. Navigate to the **Settings :: Authentication** page.
2. On the **Settings :: Authentication** page, from the top-right corner of the screen, click **Quick Config**.
   The **RBAC Journey :: Authentication** page is displayed.



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

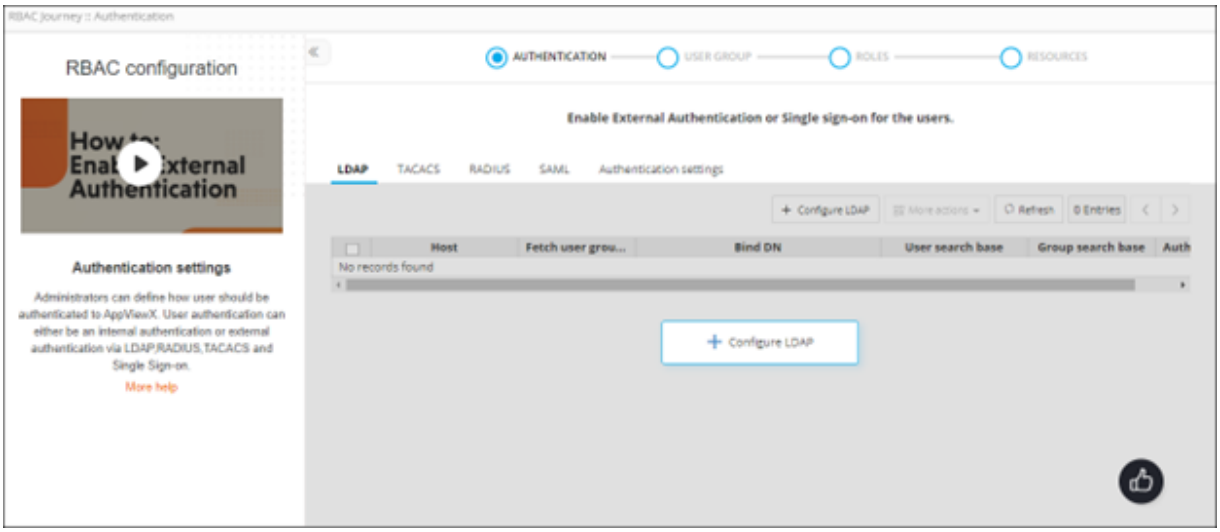


6. In the **Confirmation** message dialog box, click **Proceed**.
   The selected configuration is enabled.

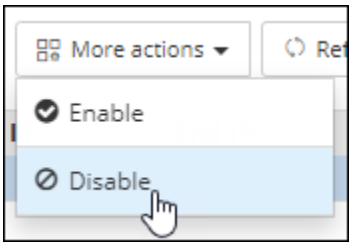
Disabling a RADIUS Configuration

To disable a RADIUS configuration:

1. Navigate to the **Settings :: Authentication** page.
2. On the **Settings :: Authentication** page, from the top-right corner of the screen, click **Quick Config**.
   The **RBAC Journey :: Authentication** page is displayed.



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

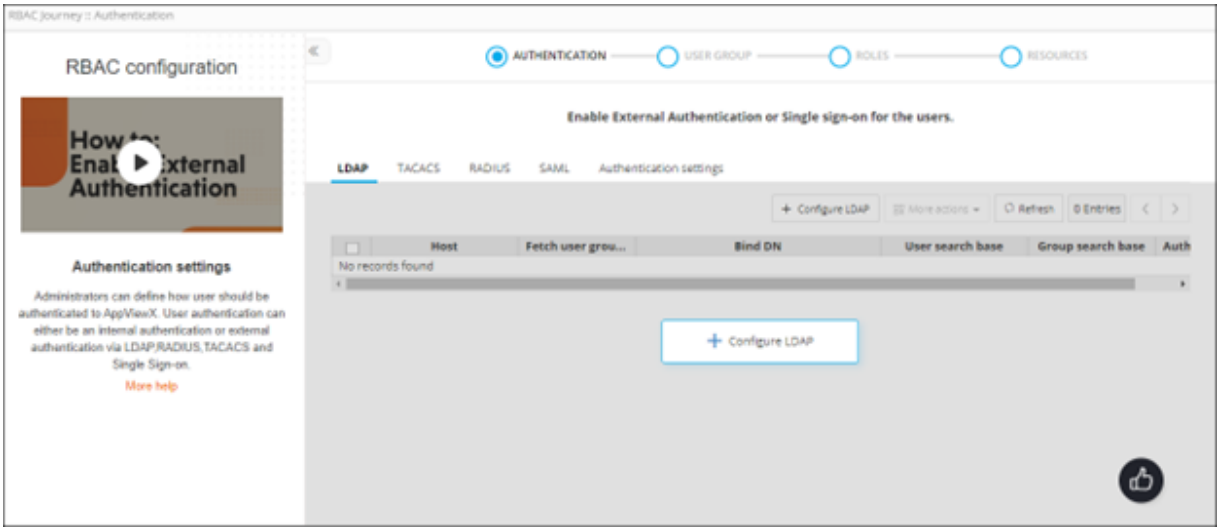


6. In the **Confirmation** message dialog box, click **Proceed**.
   The selected configuration is disabled.

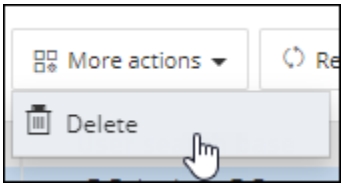
Deleting a RADIUS Configuration

To delete a RADIUS configuration:

1. Navigate to the **Settings :: Authentication** page.
2. On the **Settings :: Authentication** page, from the top-right corner of the screen, click **Quick Config**.
   The **RBAC Journey :: Authentication** page is displayed.



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

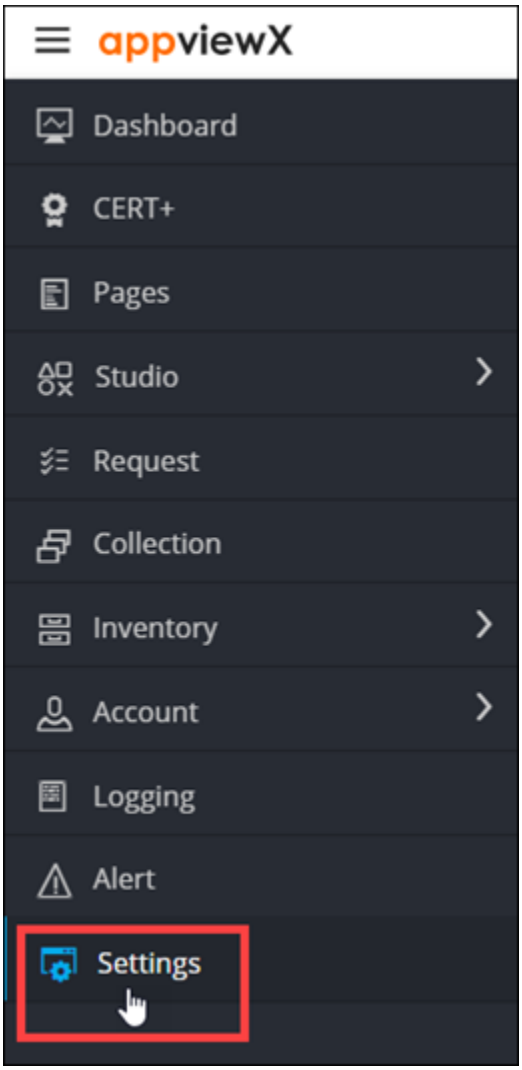


6. In the **Confirmation** message dialog box, click **Proceed**.
   The selected configuration is deleted.

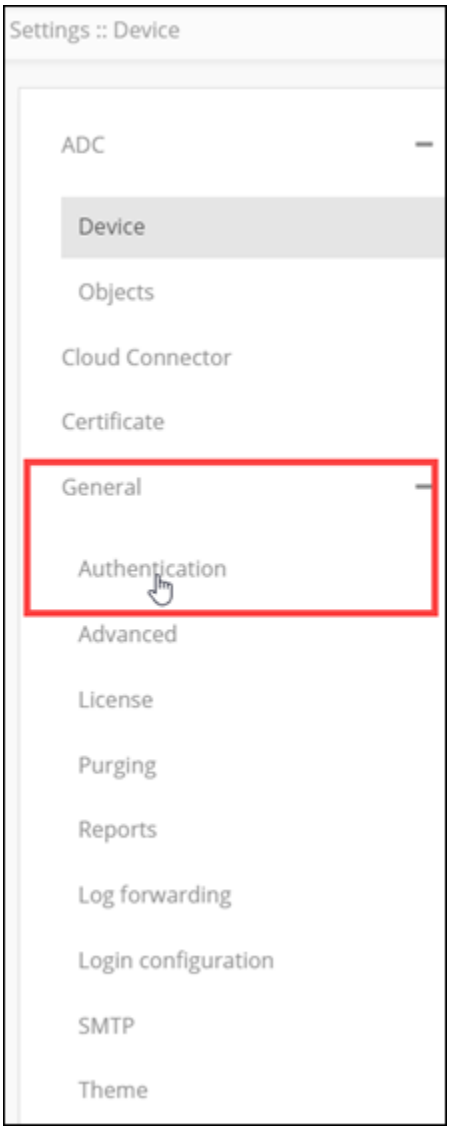
Configuring Single Sign On Settings with AppViewX

To configure single sign on settings with AppViewX:

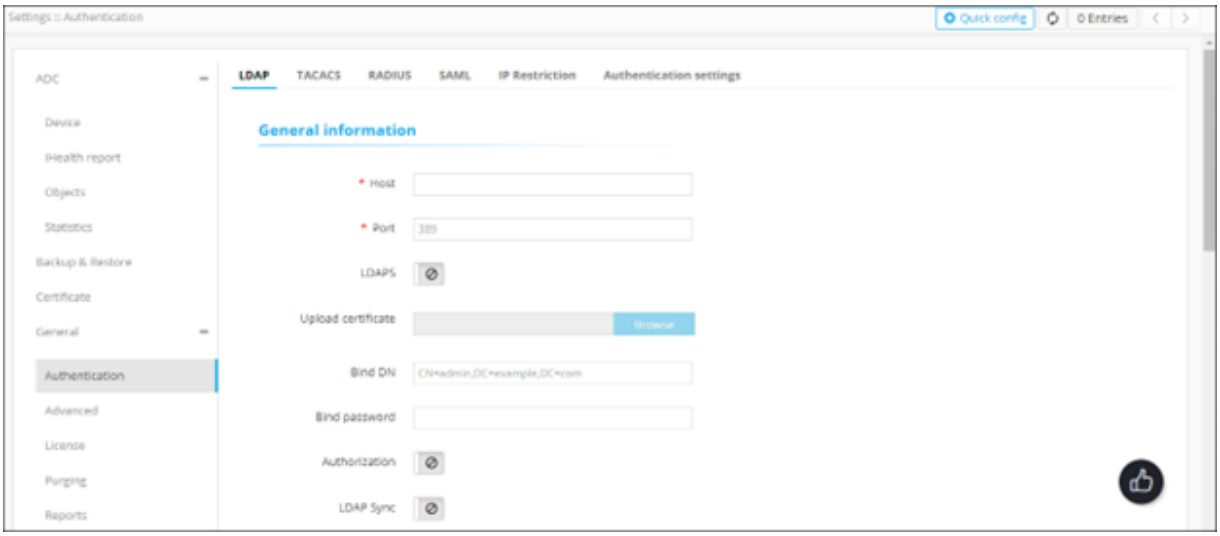
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Authentication**.

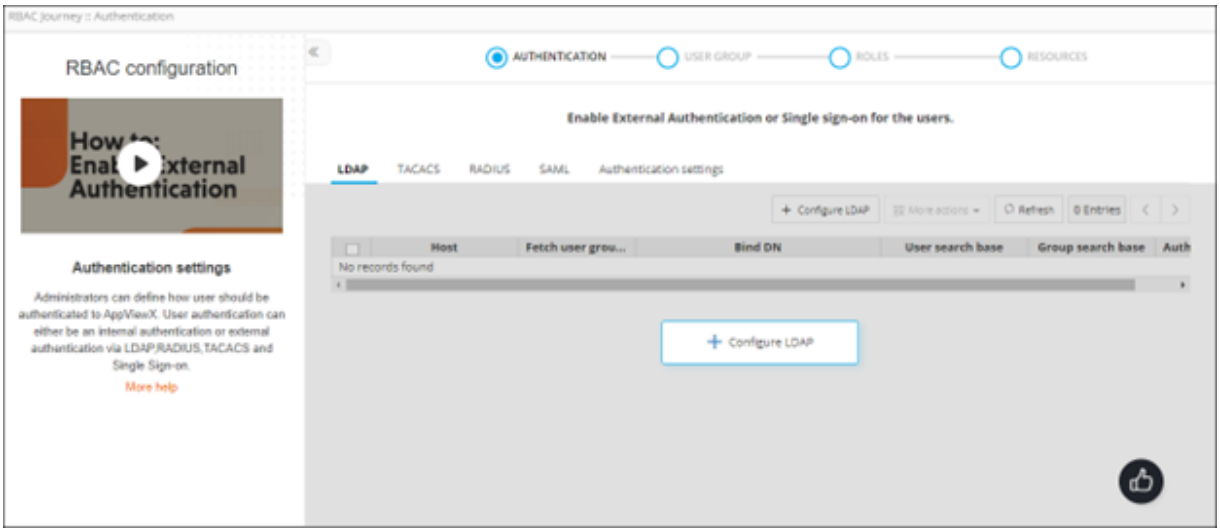


The **Settings :: Authentication** page is displayed, with the **LDAP** tab open by default.

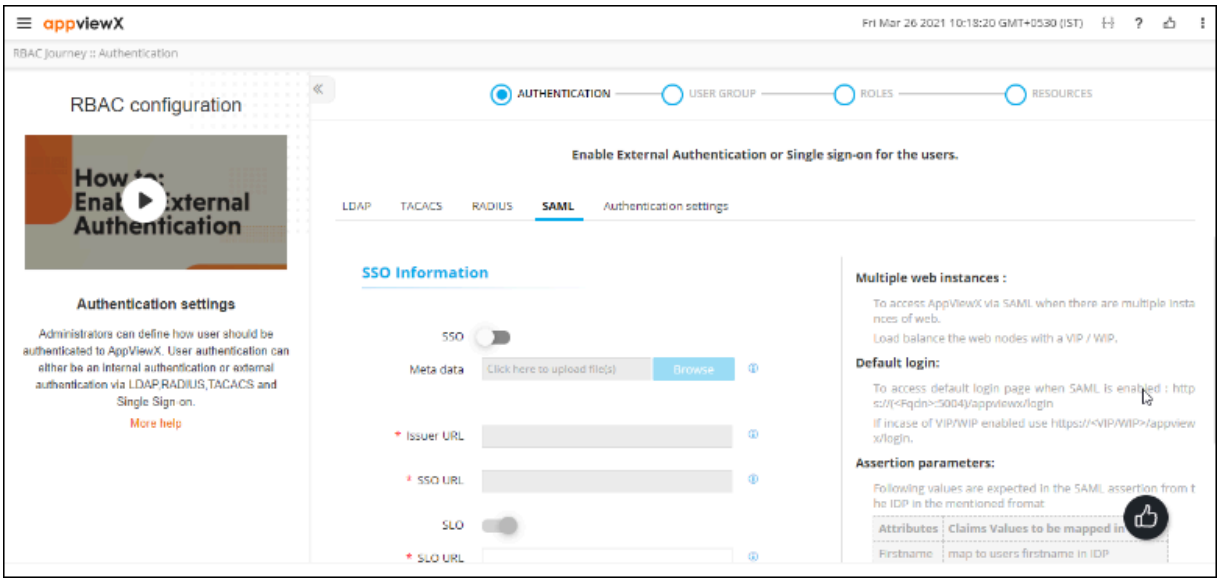


5. From the top-right corner of the screen, click **Quick Config**.

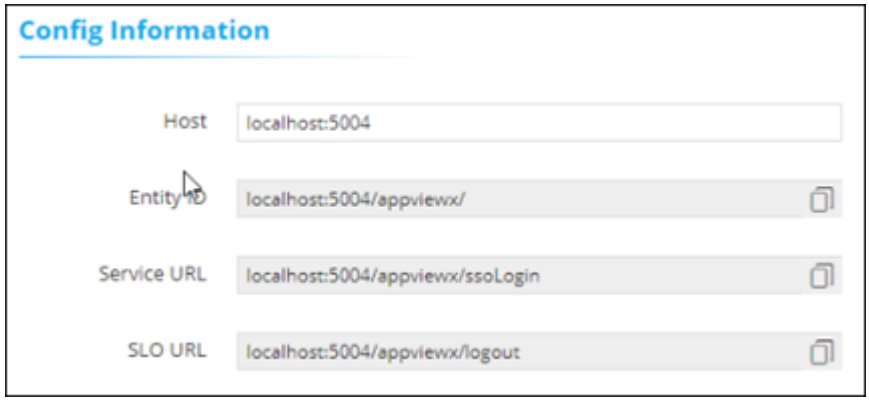
   The **RBAC Journey :: Authentication** page is displayed.



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



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

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: 
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**.

Field	Description
	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. **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.

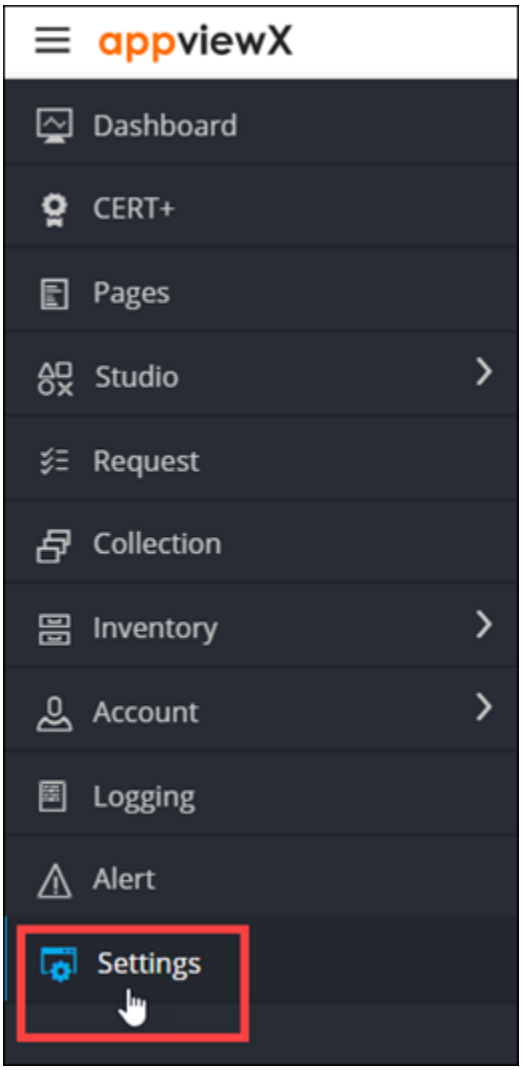
Field	Description
	Note: This field is enabled only when the **SSO** toggle in the **SSO Information** section is turned on.
Local authorization	To enable SAML only authentication in IdP and for authorization to be carried out in AppViewX, enable this toggle key. **Note:** Authorization can be done by assigning user groups manually to the user or enabling birthright role.
All * marked fields are mandatory.	

8. To save the SAML authentication settings, click **Save** or to cancel the authentication settings, click **Cancel**.

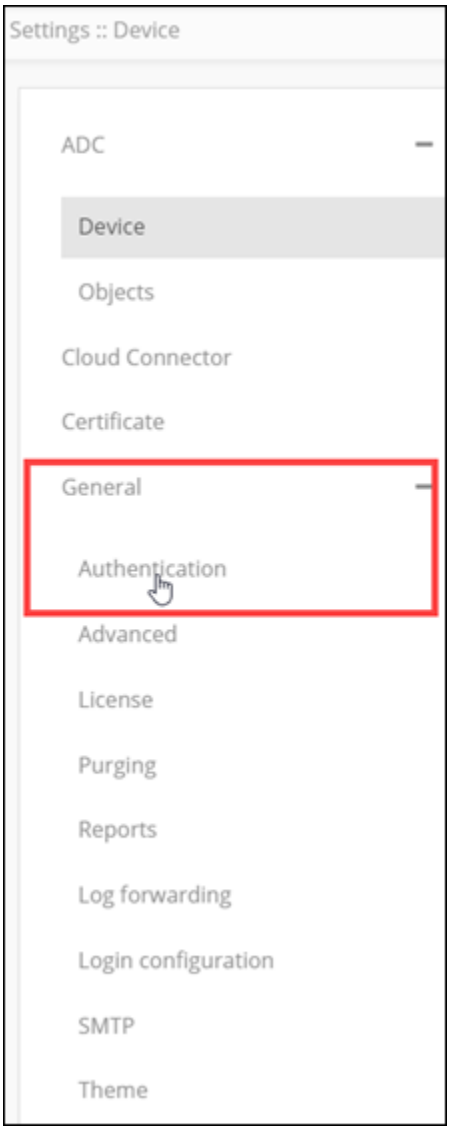
Configuring Authentication Settings rbac quick config

To configure the authentication settings:

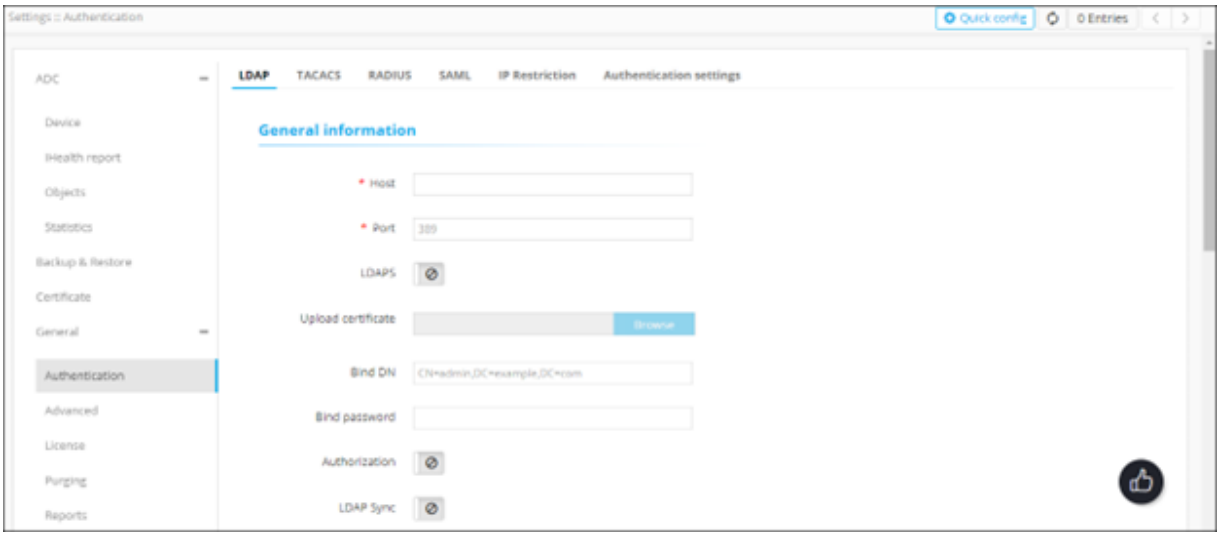
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Authentication**.

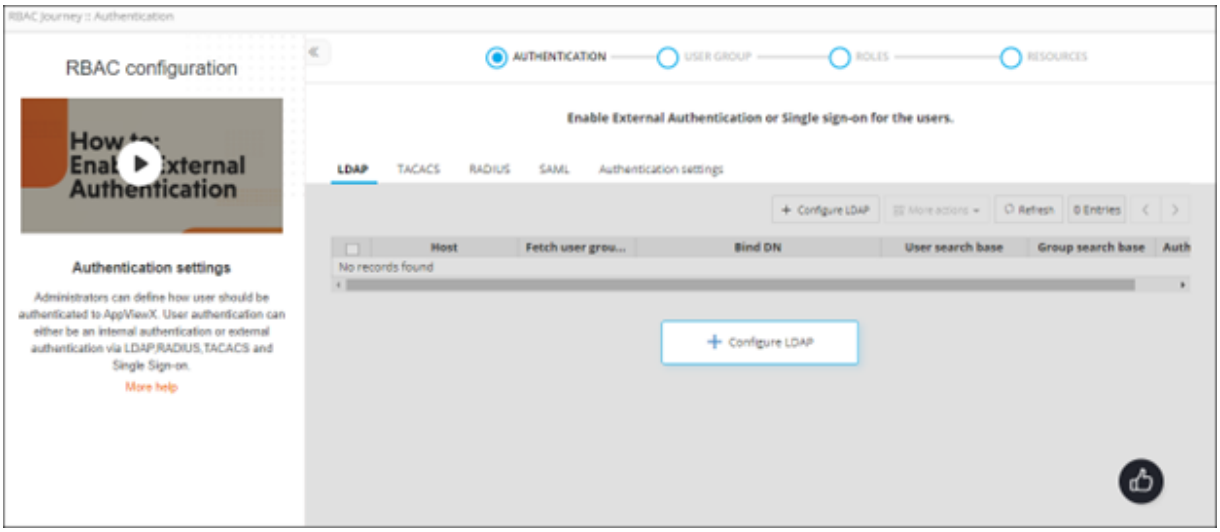


The **Settings :: Authentication** page is displayed, with the **LDAP** tab open by default.

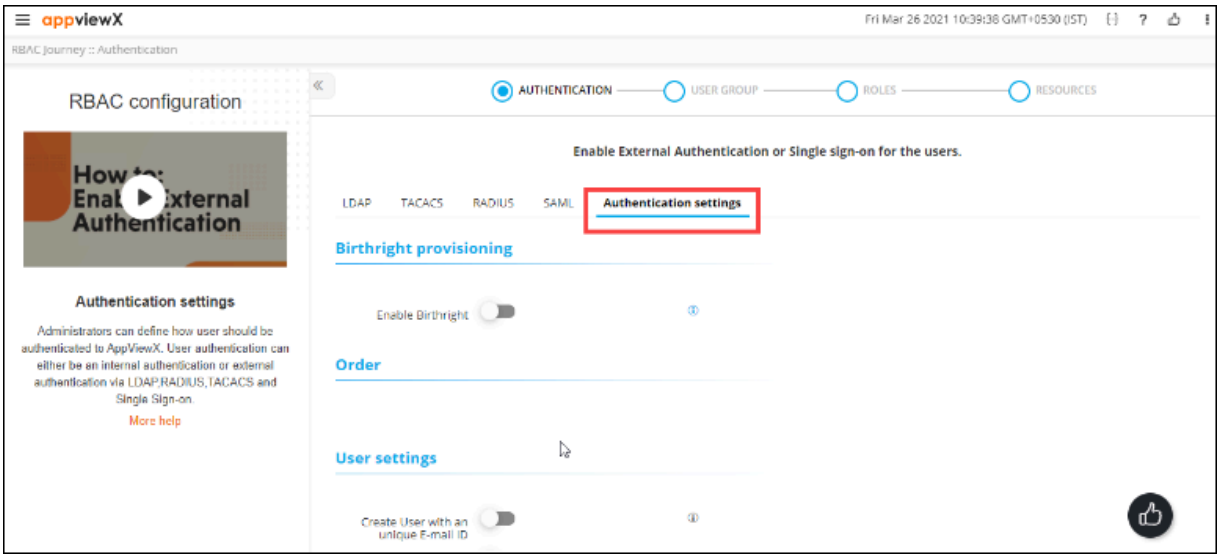


5. From the top-right corner of the screen, click **Quick Config**.

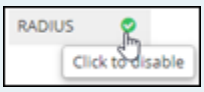
   The **RBAC Journey :: Authentication** page is displayed.



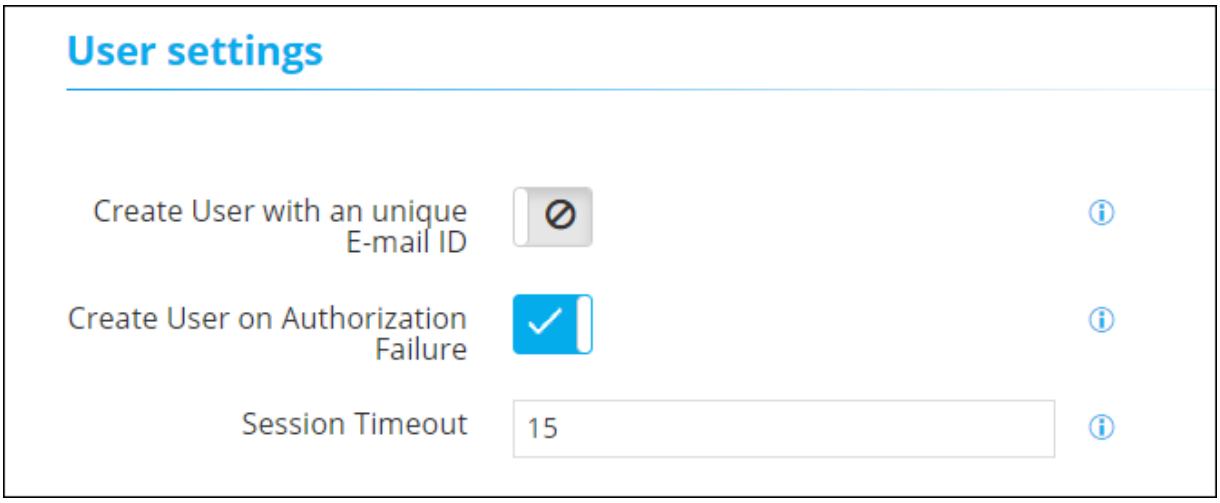
6. On the **RBAC Journey :: Authentication** page, click the **Authentication Settings** tab.



7. 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.
8. 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.

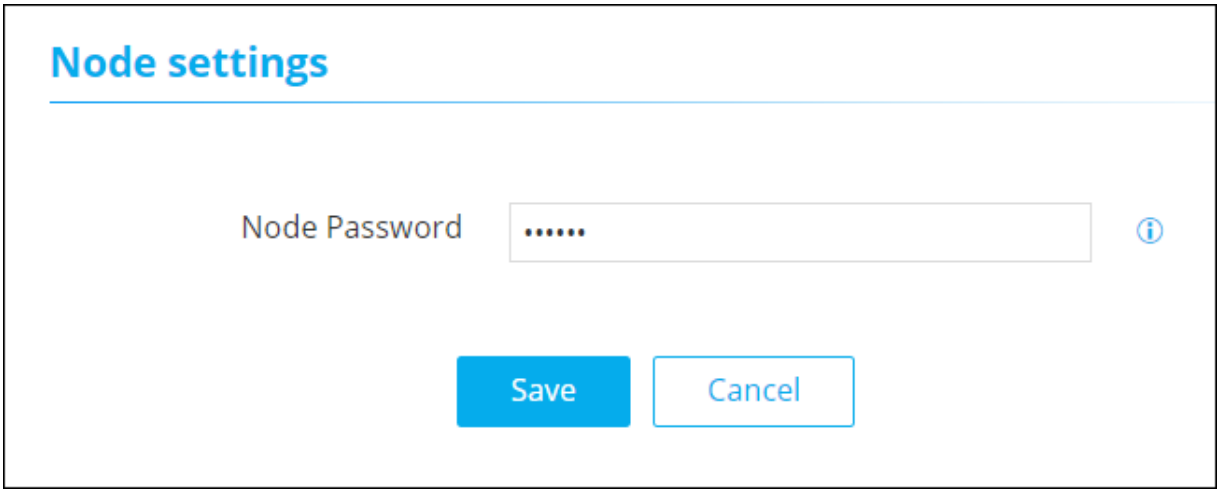
9. In the **User settings** section, enter the required field information.



The following table describes the field information in this section:

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.

10. 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.

11. 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.

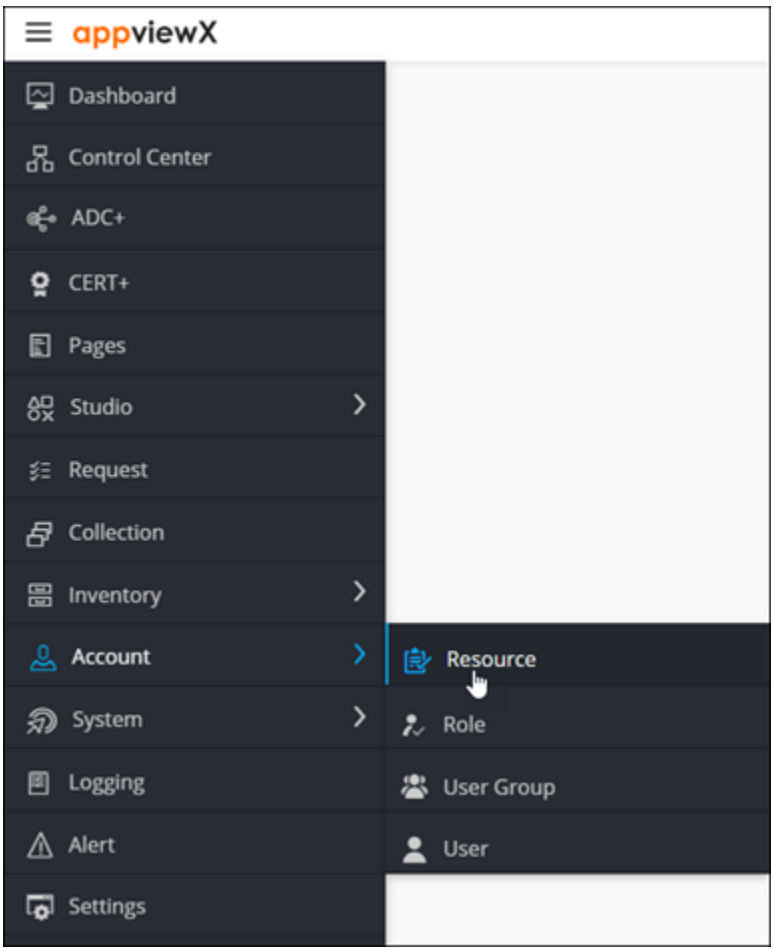
- Create an RBAC Rule to Tag ADC Objects Using a Query
- Configuring a Variable as a Filter Condition Value based on Patterns
- Configuring the Resource Name
- Create an RBAC Rule to Tag ADC Objects/Certificates using a Script
- Configuring the Certificate Group Name
- Configuring the Resource Name Based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

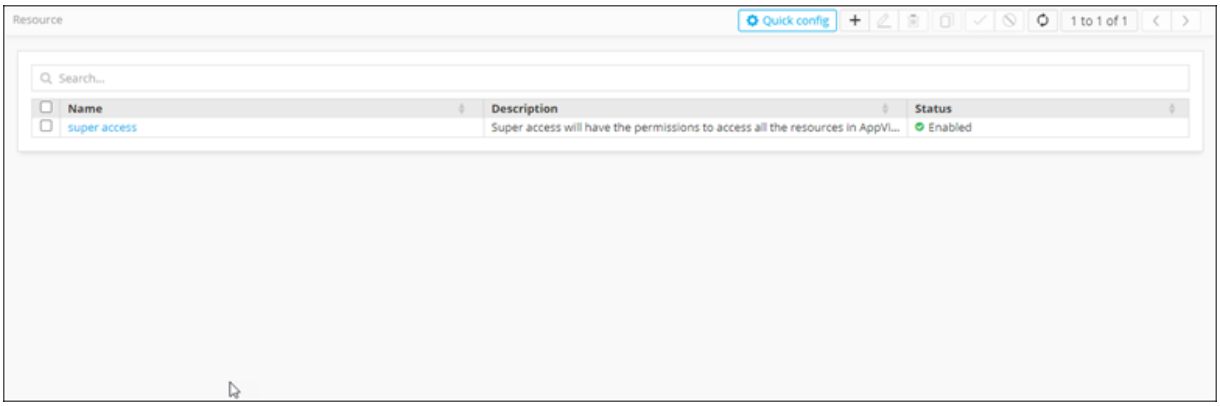
Create an RBAC Rule to Tag ADC Objects Using a Query

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

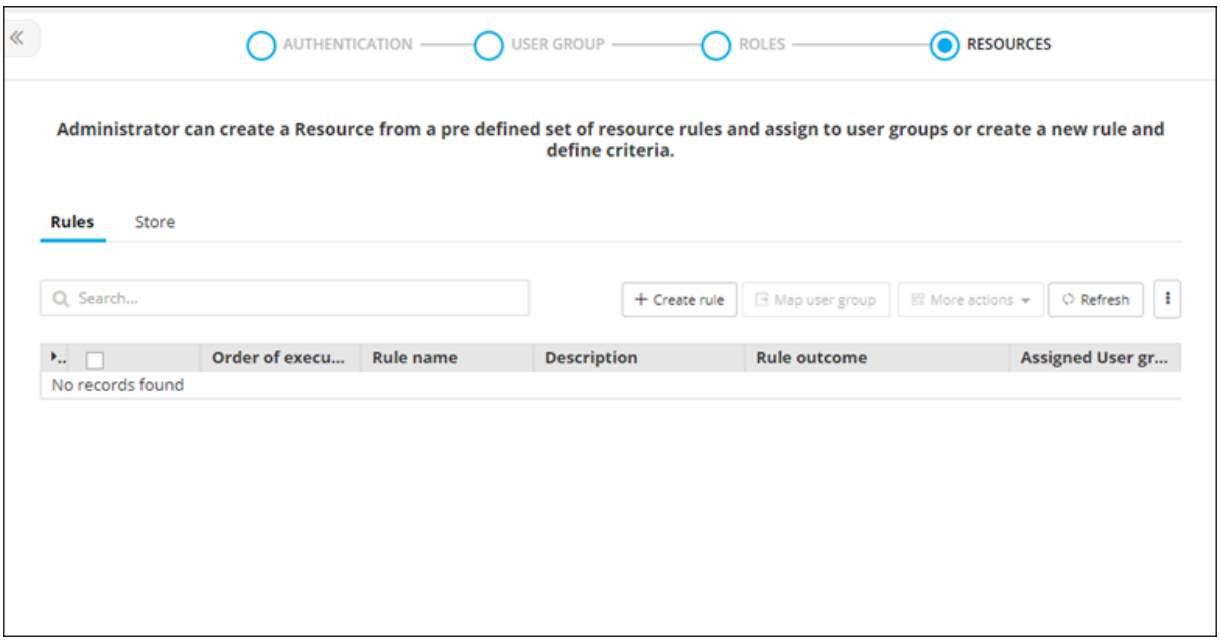
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Account** > **Resource**.



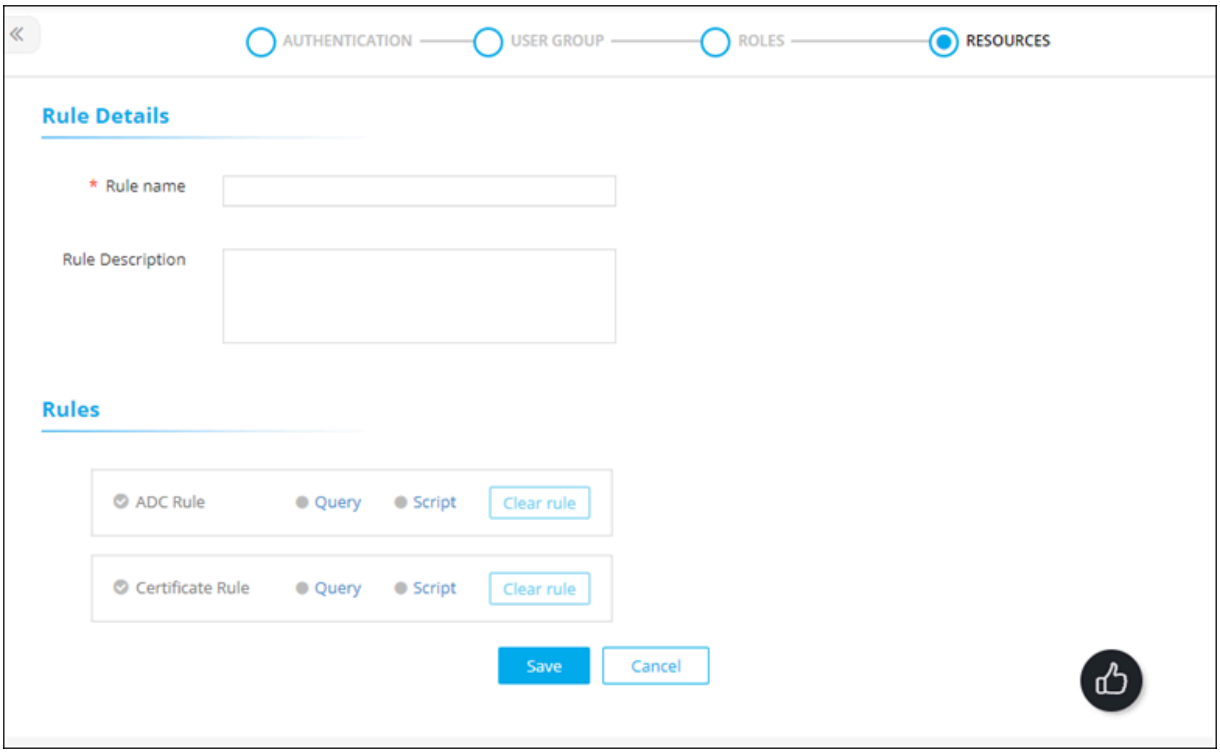
The **Resource** page is displayed.



3. From the top-right corner of the screen, click **Quick Config**.
   The **RBAC Journey :: Authentication** page is displayed.
4. Navigate to the **Resources** stage as part of the wizard flow to add roles into AppViewX, with the **Rules** tab displayed by default.



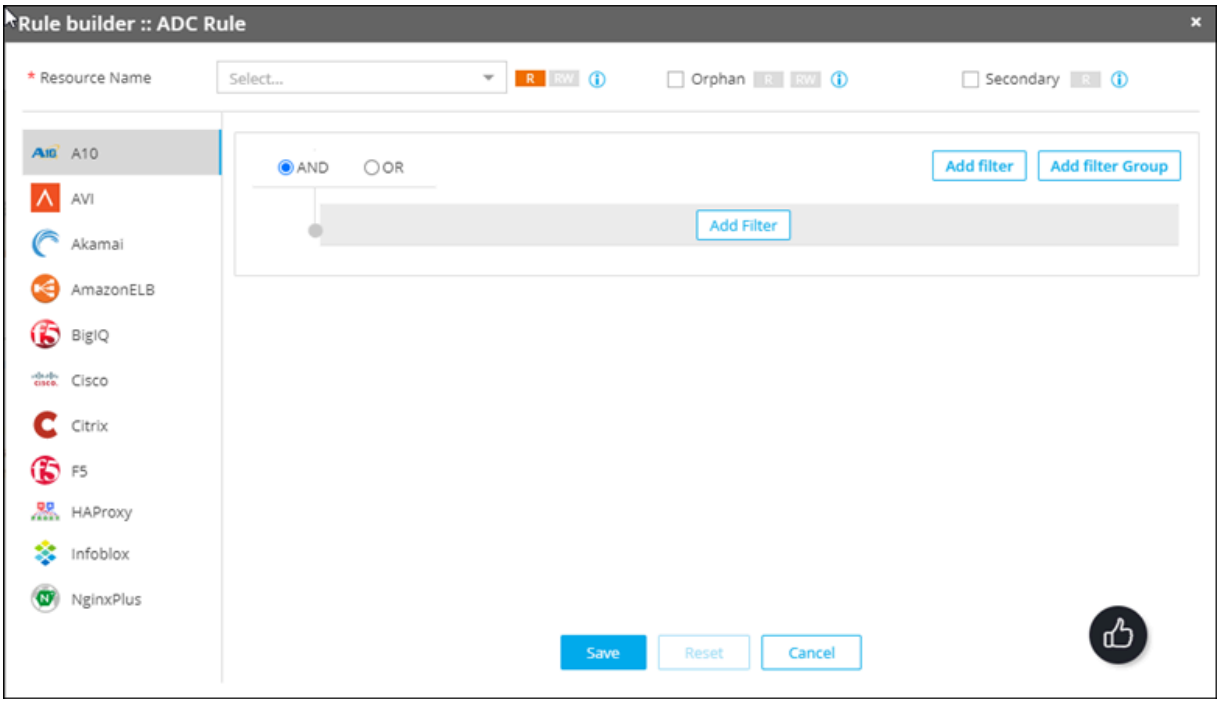
5. Click + Create rule.
   The **Rules :: Create** screen is displayed.



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

Field	Description
***Rule Name**	Resource name.
Rule Description	Brief description of the resource/granular level accesses associated with the resource.
All * marked fields are mandatory.	

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



9. On the **Rule builder :: ADC Rule** action pane, click **Add Filter**.
10. 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 alphanumerics [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

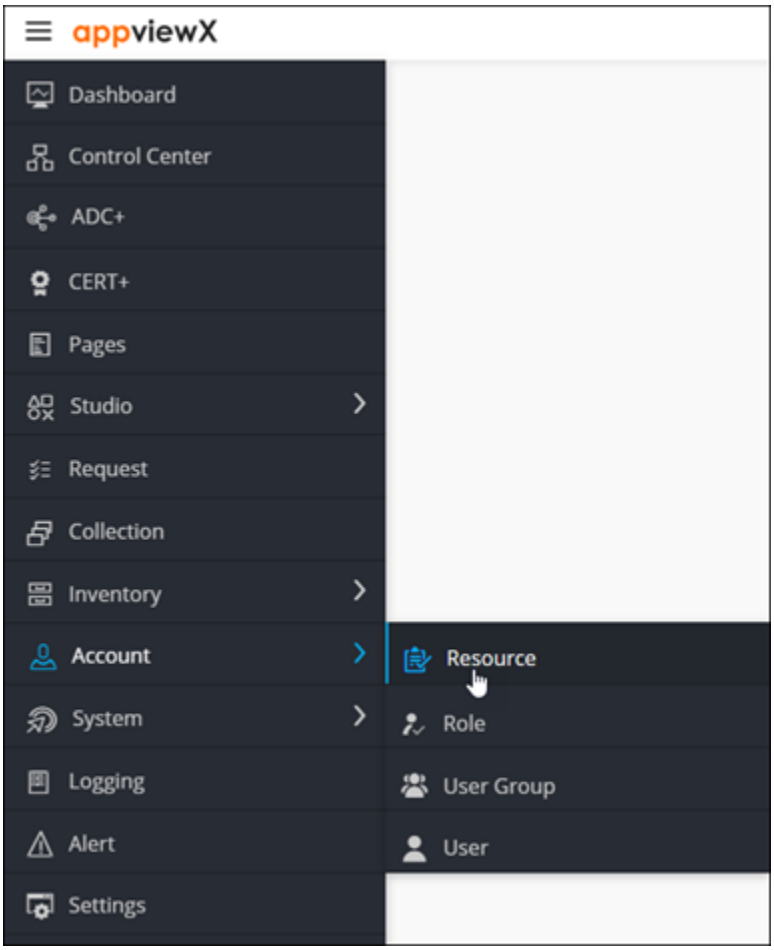
To create resources dynamically based on patterns, resource name can be configured in the following ways:

1. Provide the Resource Name of an existing resource by choosing the Resource Name from 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].
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.
   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**.
   f. Saved rules will be displayed in the **Rules** tab.
   g. Go to the Rules tab by clicking on Resource in the breadcrumb.
   h. Rule Summary details (Rule Name, Description, Rule Outcome) are displayed in the Rule Inventory table.
   i. Enable the rule by clicking on the respective status icon for the rule to be actively running.

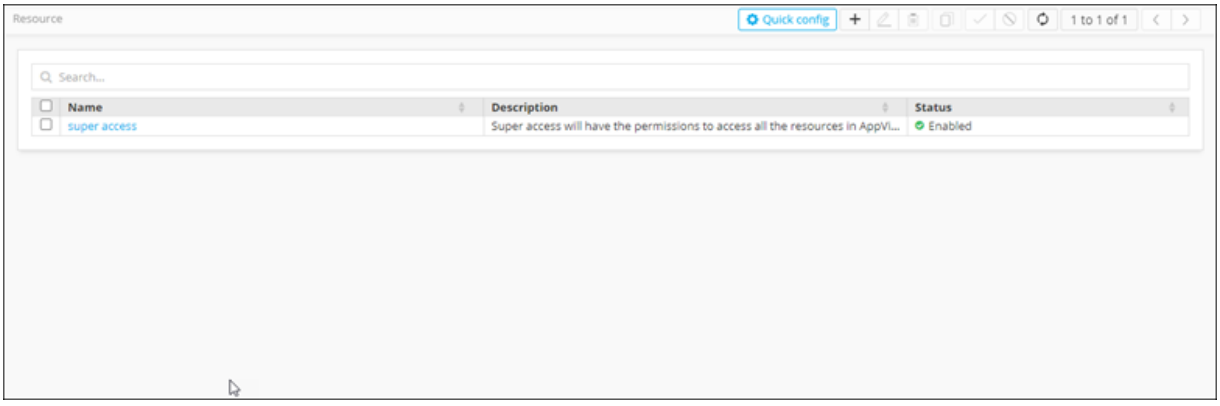
Create an RBAC Rule to Tag ADC Objects/Certificates using a Script

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

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the icon.
2. From the menu displayed, click **Account** > **Resource**.



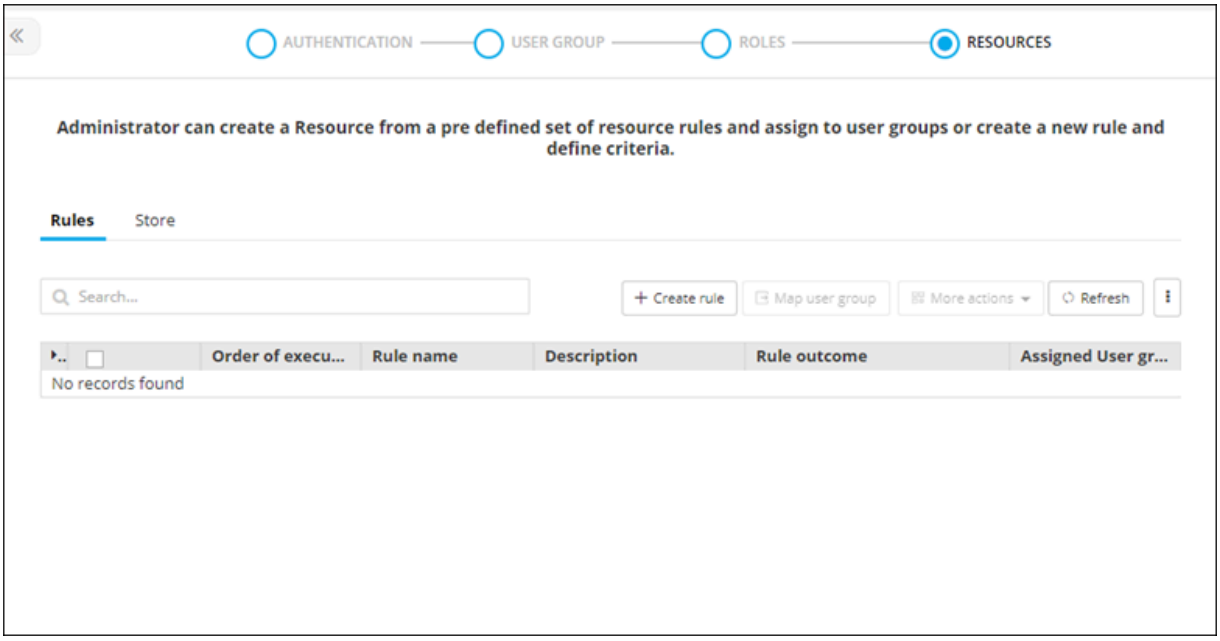
The **Resource** page is displayed.



3. From the top-right corner of the screen, click **Quick Config**.

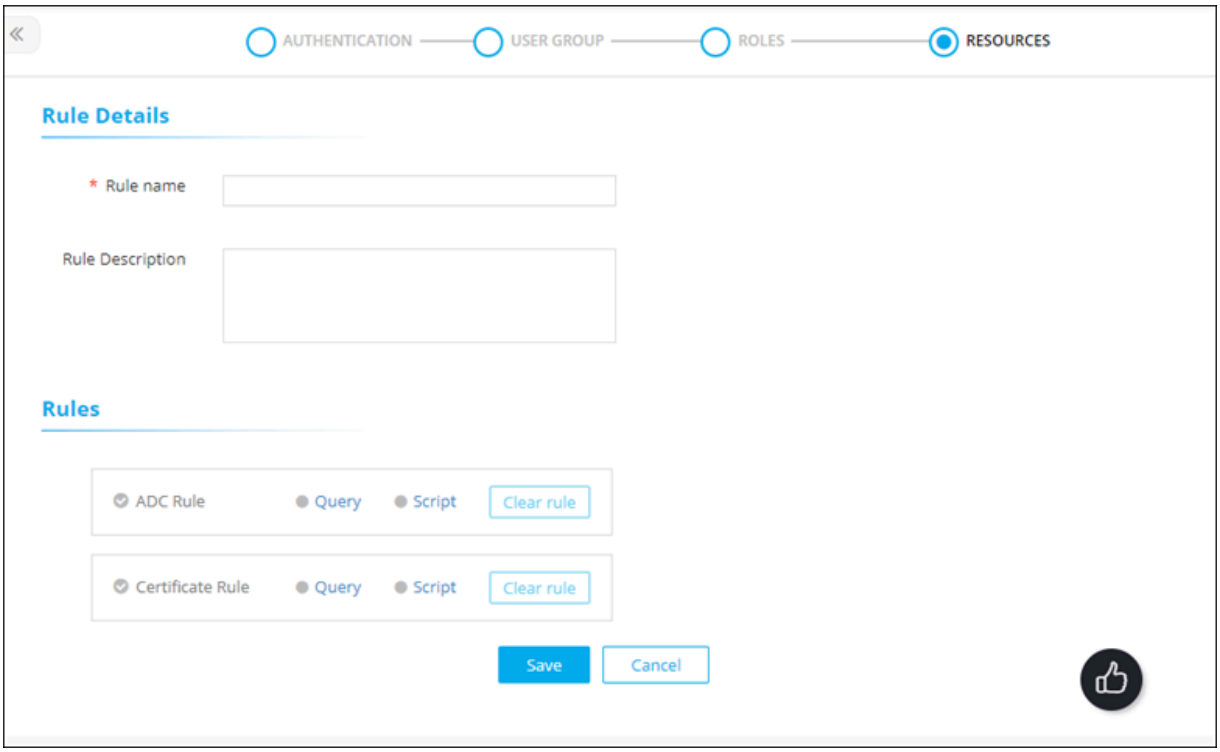
The **RBAC Journey :: Authentication** page is displayed.

4. Navigate to the **Resources** stage as part of the wizard flow to add roles into AppViewX, with the **Rules** tab displayed by default.



5. Click + Create rule.

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



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

Field	Description
***Rule Name**	Resource name.
Rule Description	Brief description of the resource/granular level accesses associated with the resource.
All * marked fields are mandatory.	

7. To configure a rule to dynamically tag ADC objects using Query, in the **Rules** section, for the **ADC Rule**, select **Script**.
8. 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.
9. Click **Save**.
10. Saved rules will be displayed in the **Rules** tab.
11. 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.
12. 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:

- Provide the certificate group name of an existing resource by choosing the certificate group name from the drop-down menu.
- Provide a Static Name to the certificate group name. [When Rule matches the Resource Name would be created on Demand].
- 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

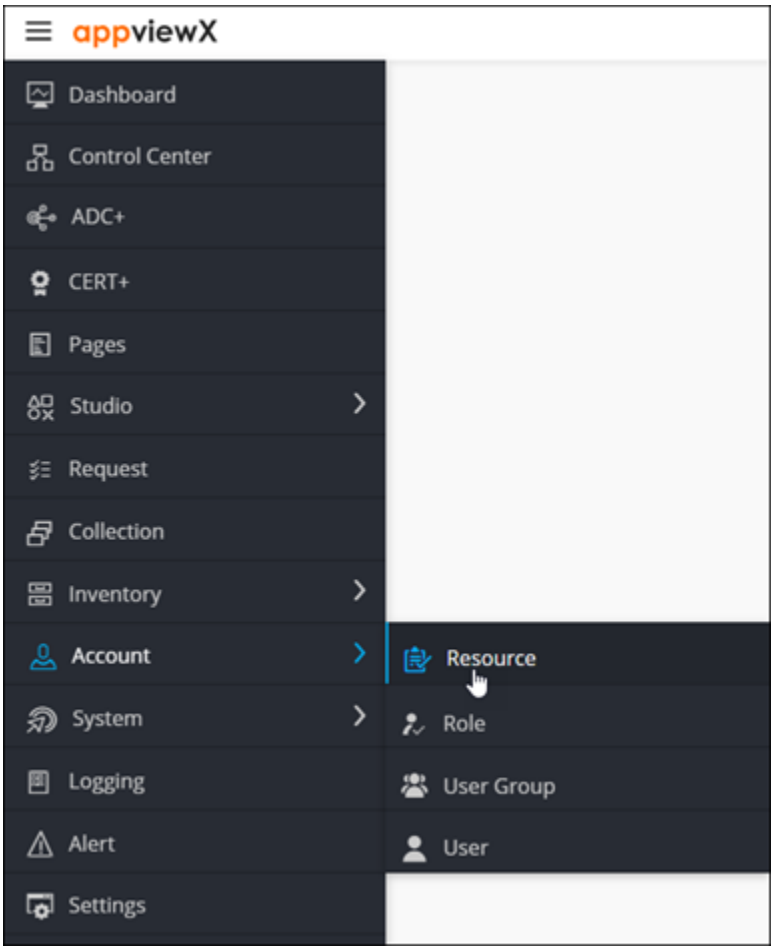
To create resources dynamically based on patterns, the resource name can be configured in the following ways:

- Provide the Resource Name of an existing resource by choosing the Resource Name from Drop Down.
- Provide a Static Name to the Resource. [When Rule matches the Resource Name would be created on Demand].
- 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%>.
- 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.
- When you are finished configuring the Certificate rule, click Save. Saved rules will be displayed in the Rules tab.
- 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.
- Enable the rule by clicking on the respective status icon for the rule to be actively running.

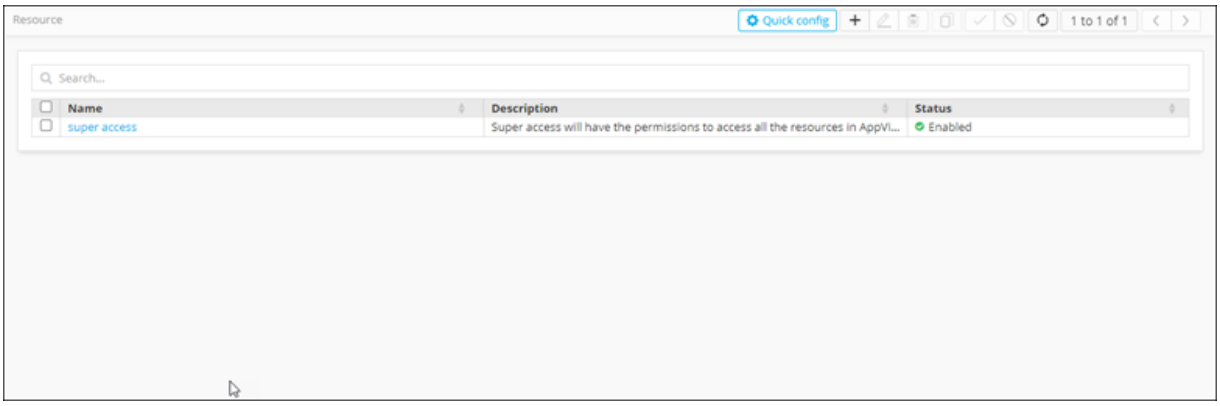
Clone a Rule

To clone a rule:

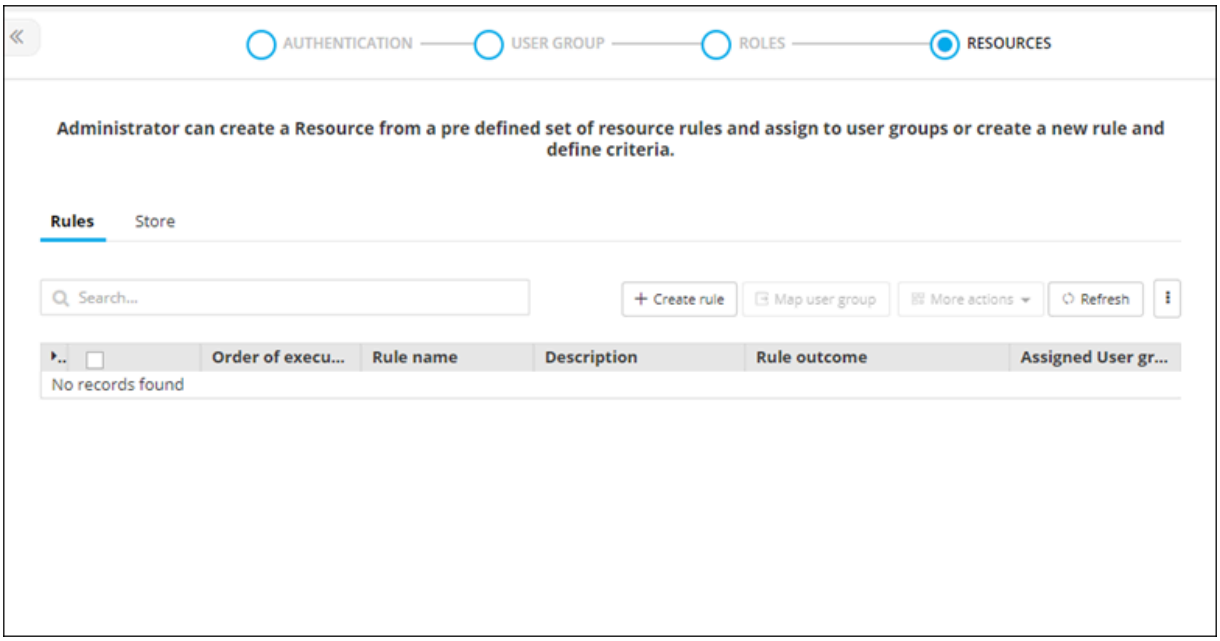
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the icon.
2. From the menu displayed, click **Account** > **Resource**.



The **Resource** page is displayed.



3. From the top-right corner of the screen, click **Quick Config**. The **RBAC Journey :: Authentication** page is displayed.
4. Navigate to the **Resources** stage as part of the wizard flow to add roles into AppViewX, with the **Rules** tab displayed by default.

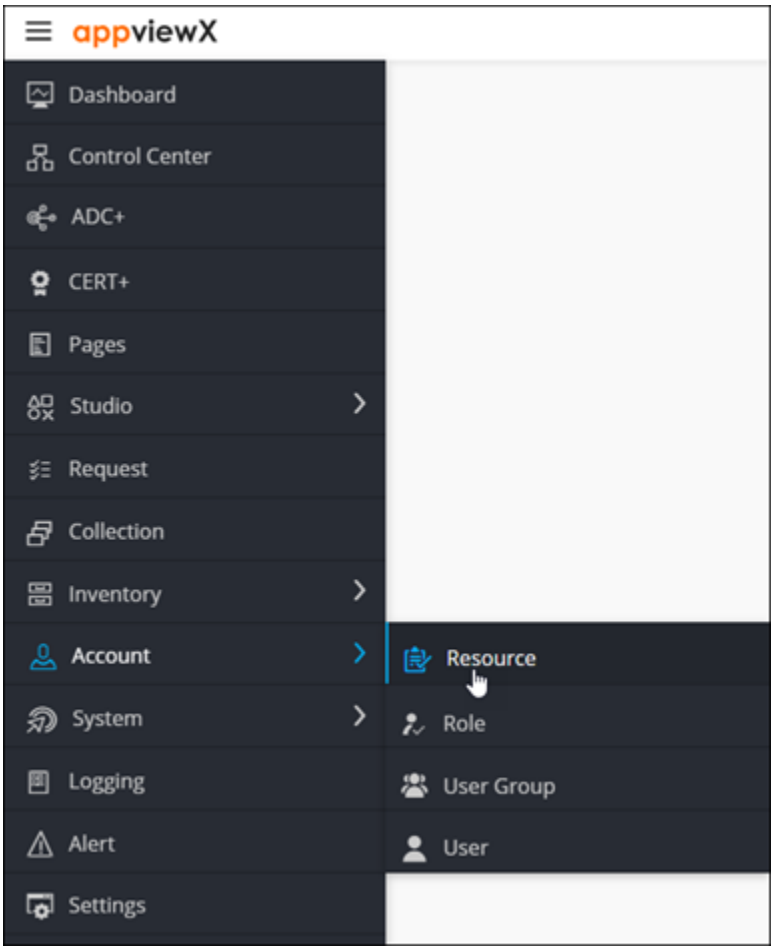


5. For the resource you want to clone, select the check box against that resource.
6. From the **More actions** drop-down menu, click **Clone**.
7. In the **Clone** rules dialog box, enter a name for the cloned rule and click **Save**.
   Rule details will be closed and will be opened in edit mode for any further modification on description/ rule conditions.
8. 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.

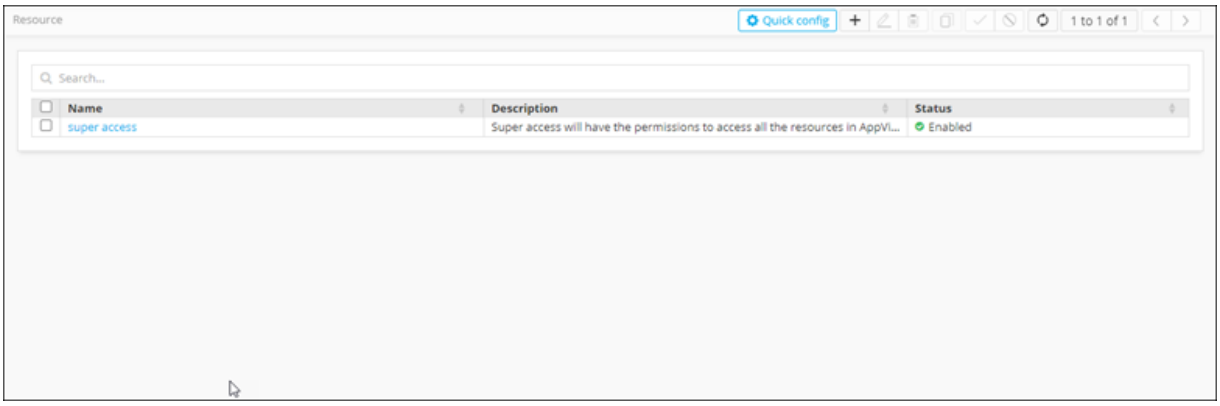
Delete a Rule

To delete a rule:

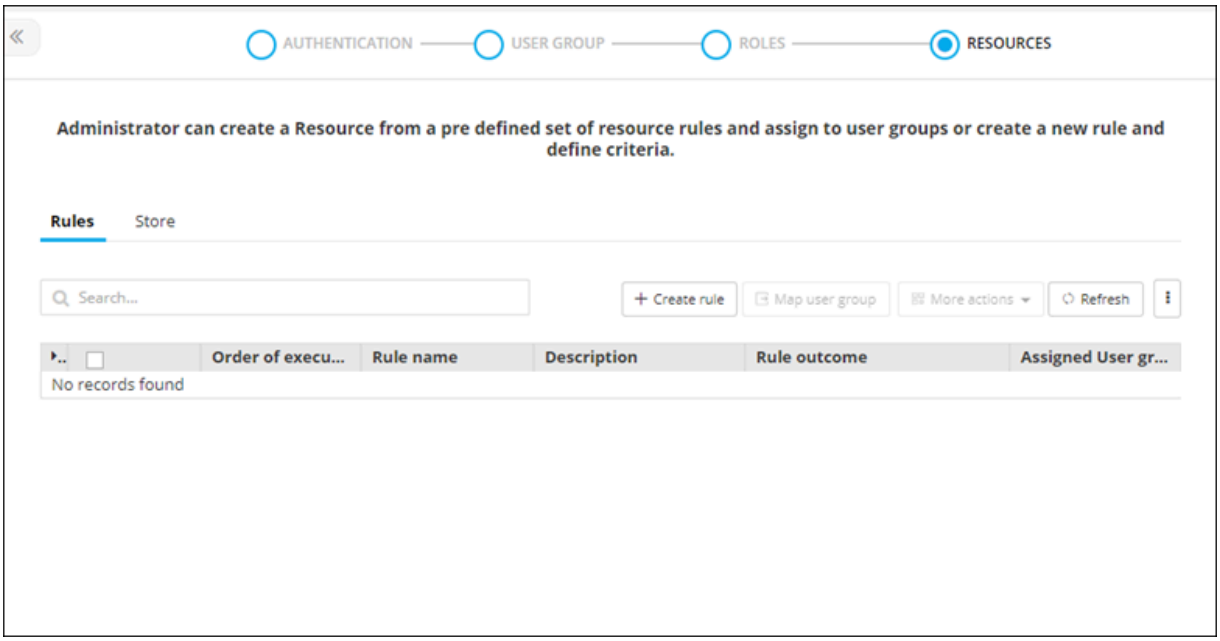
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Account** > **Resource**.



The **Resource** page is displayed.



3. From the top-right corner of the screen, click **Quick Config**. The **RBAC Journey :: Authentication** page is displayed.
4. Navigate to the **Resources** stage as part of the wizard flow to add roles into AppViewX, with the **Rules** tab displayed by default.

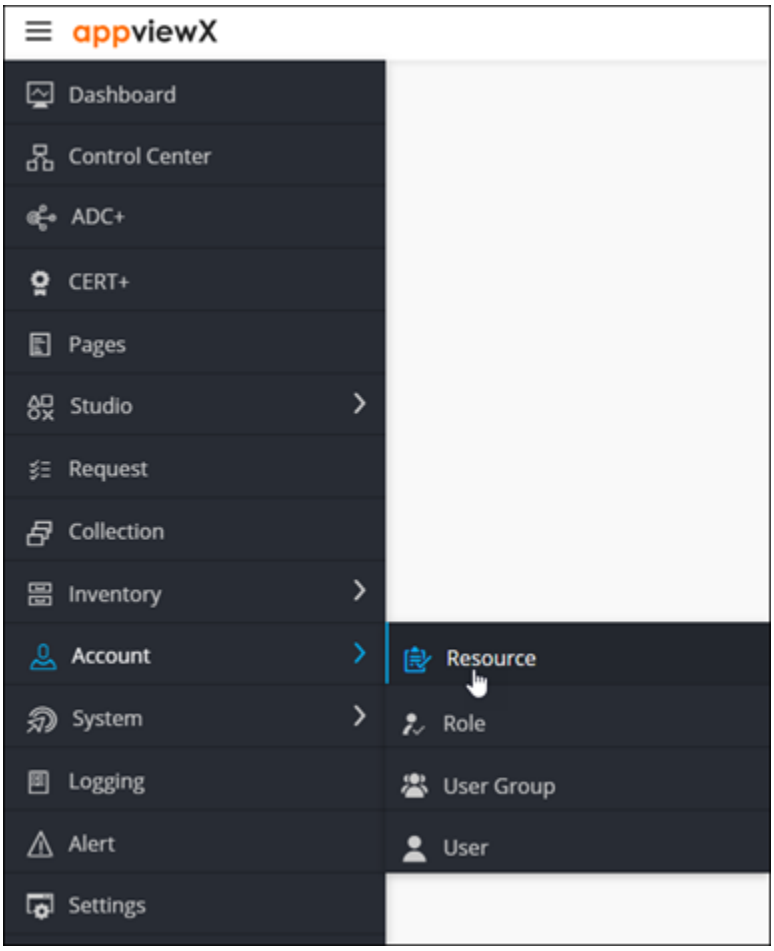


5. For the resource you want to delete, select the check box against that resource.
6. From the **More actions** drop-down menu, click **Delete**.
7. In the **Confirmation** dialog box, click **Yes**.

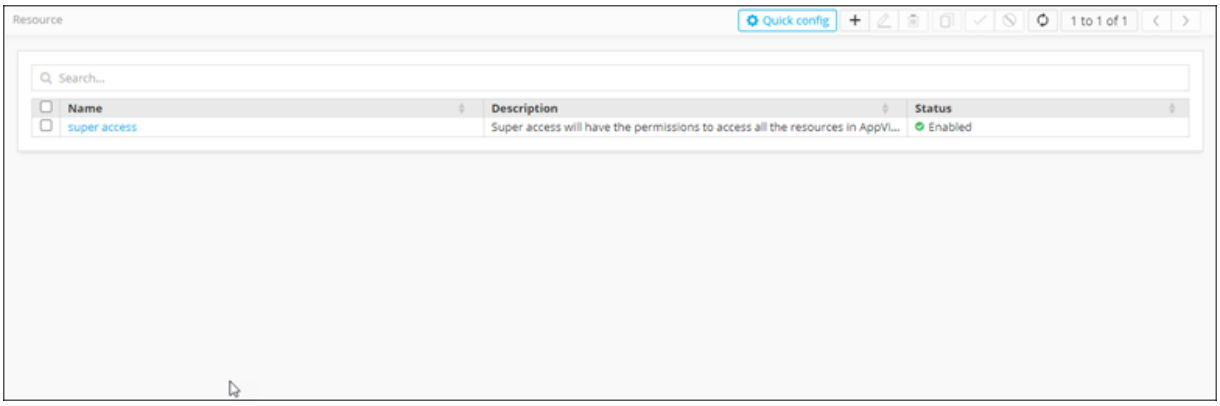
RBAC Rule Mapping to User Groups to Dynamically Provide Access for Resources to User Groups

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

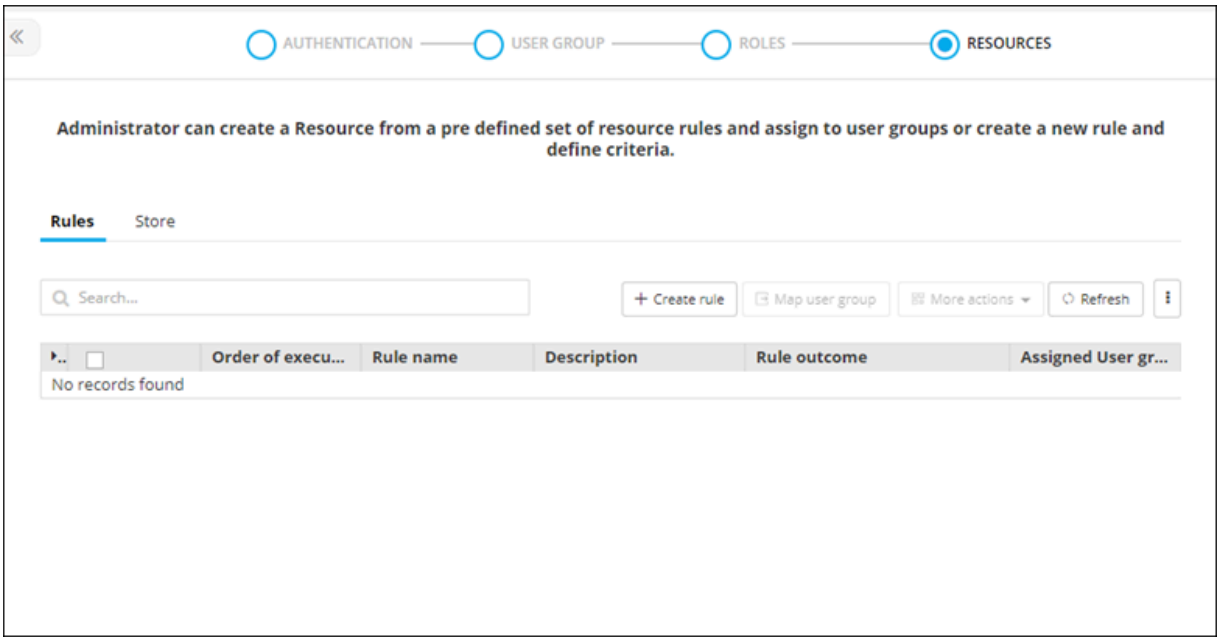
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Account** > **Resource**.



The **Resource** page is displayed.



3. From the top-right corner of the screen, click **Quick Config**. The **RBAC Journey :: Authentication** page is displayed.
4. Navigate to the **Resources** stage as part of the wizard flow to add roles into AppViewX, with the **Rules** tab displayed by default.



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

.
7. In the **Map user group** action pane, select the user groups the resource will be mapped to.
8. 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:

- 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.
- 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.

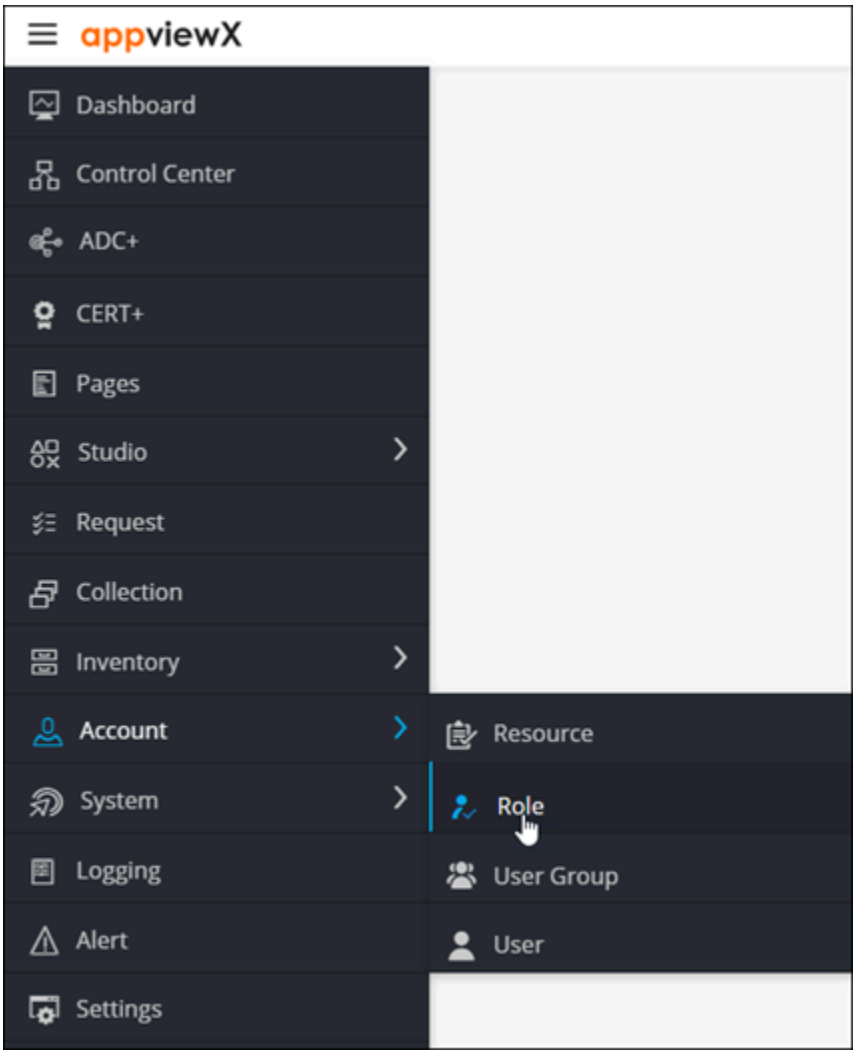
AppViewX enables the following role-related features:

- 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
- Cloning a Role
- Modifying a Role
- Enabling a Role
- Disabling a Role
- Mapping Role to User Groups

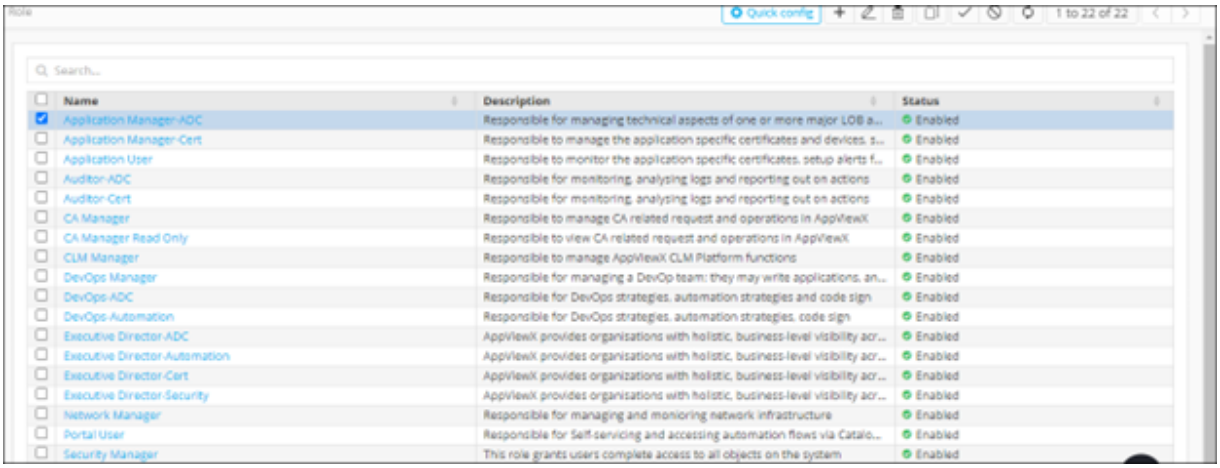
Creating a Custom Role

To create a custom role:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Account** > **Role**.



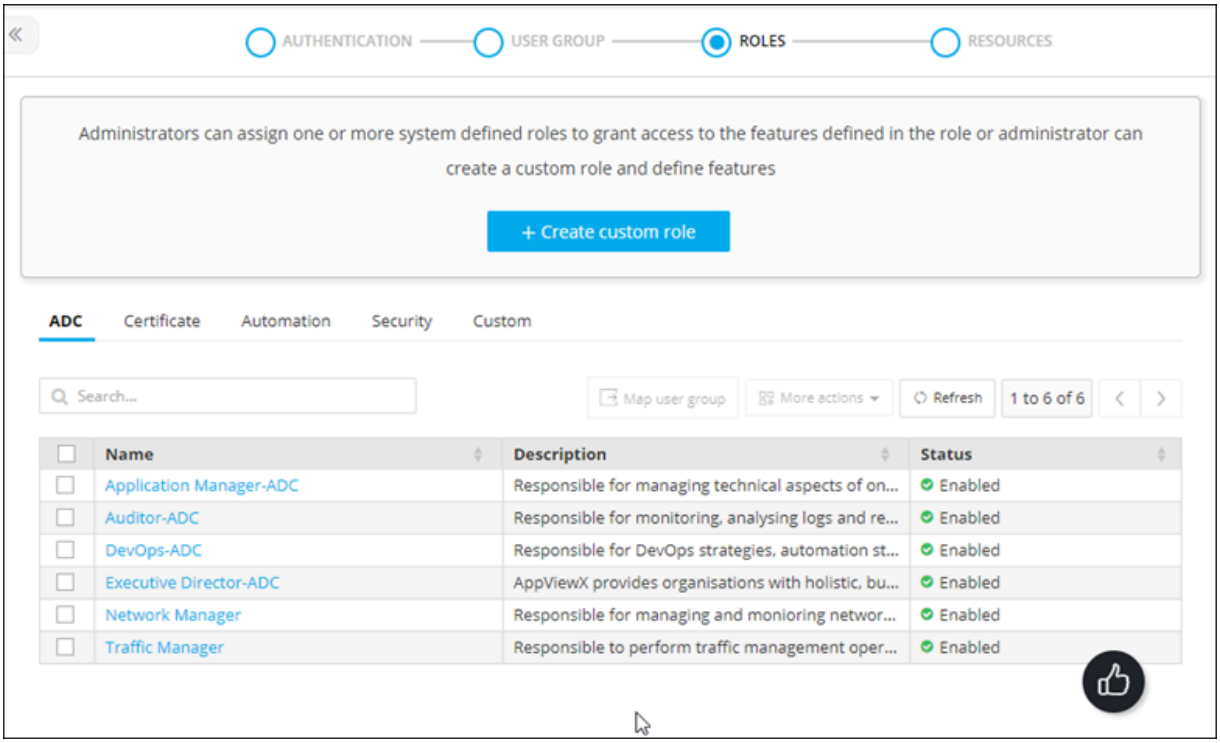
The **Role** page is displayed.



3. From the top-right corner of the screen, click **Quick Config**.

   The **RBAC Journey :: Authentication** page is displayed.

4. Navigate to the **Role** stage as part of the wizard flow to add roles into AppViewX.



5. Click 

.

   The **Create custom role** action pane is displayed.

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

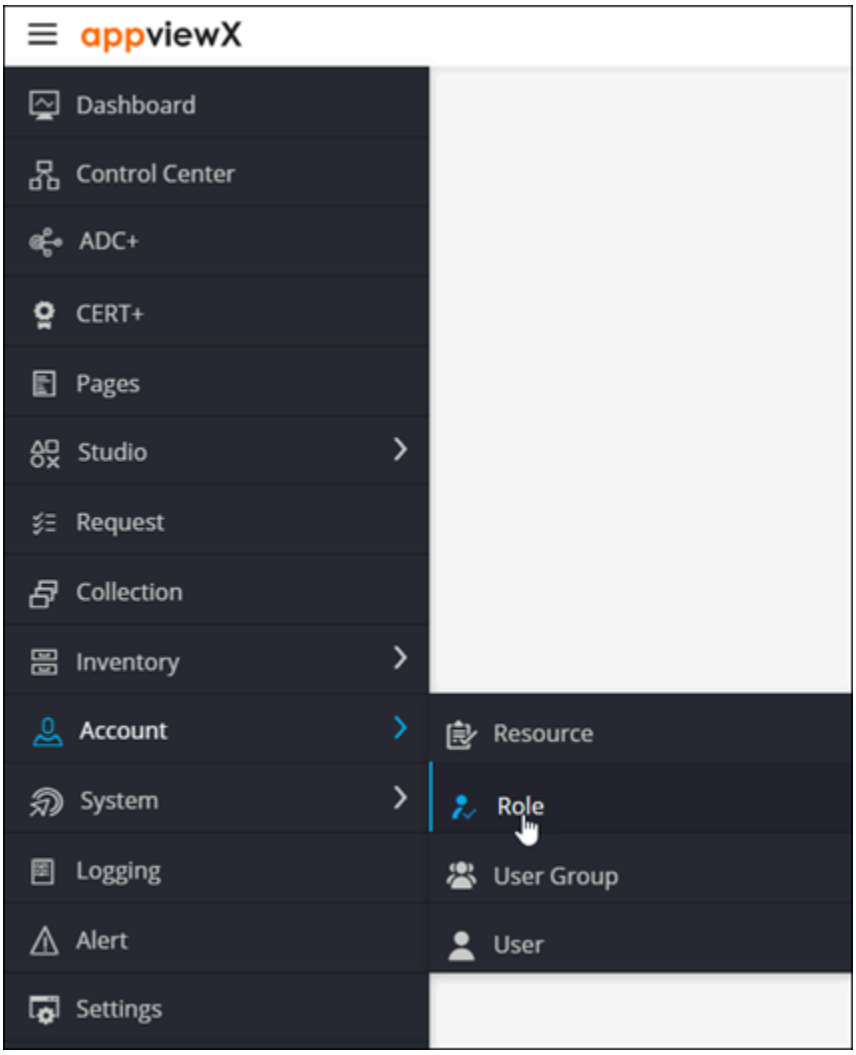
Field	Description
***Name**	Role name.
Description	Brief description of what users assigned to the role can do and/or what features or functionalities are associated with the role.
All * marked fields are mandatory.	

7. Click **Save**.
8. In the **Authorized functions** section, select the check box against the functionalities that you want to associate with the role.
9. To assign functions at a granular level, click the icon for the functions' check box and then select individual sub-options within the functions.
10. Click **Save**.

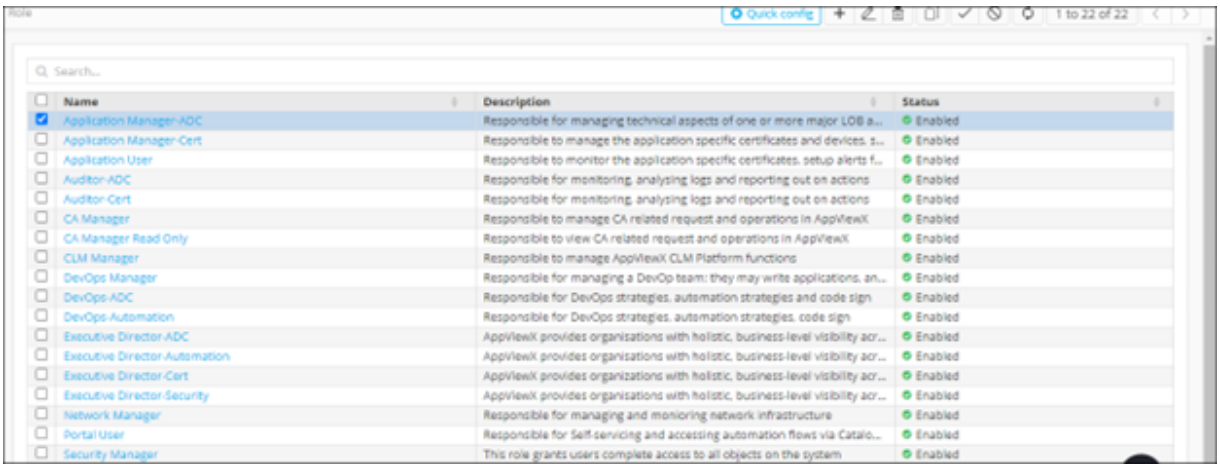
Cloning a Role

To clone an existing role to a custom role:

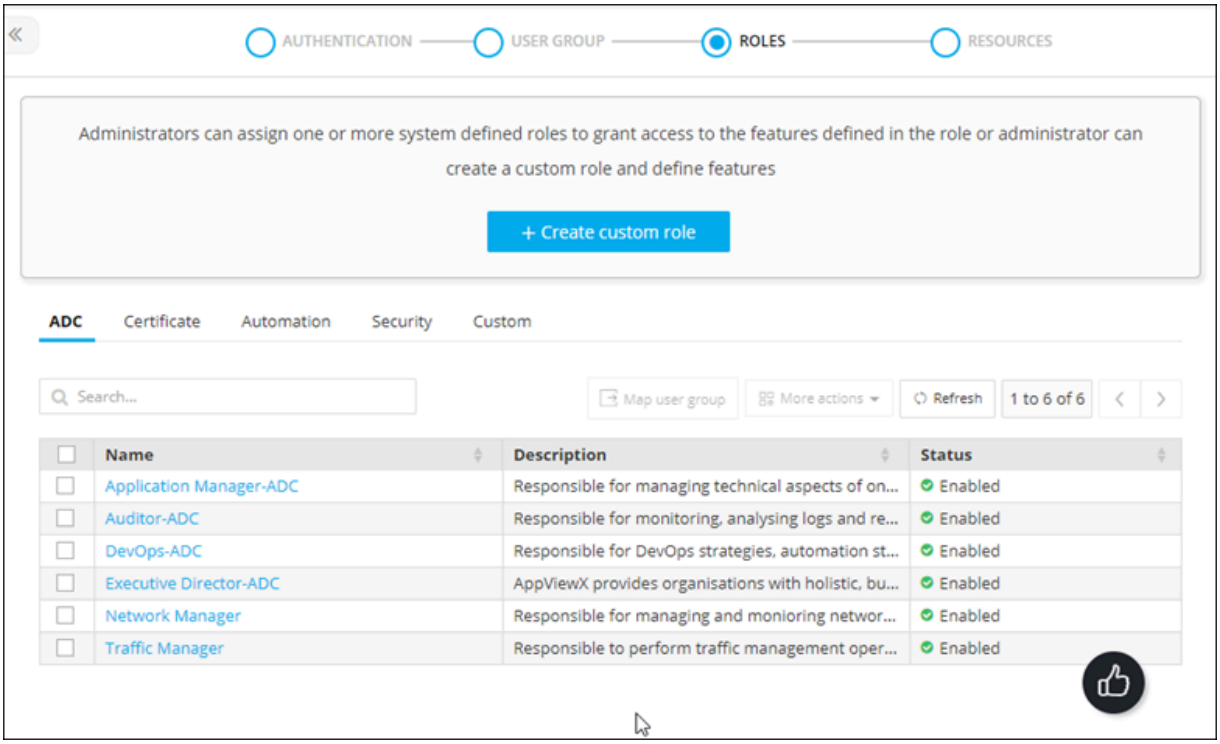
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the icon.
2. From the menu displayed, click **Account** > **Role**.



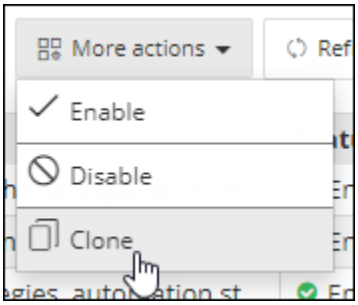
The **Role** page is displayed.



3. From the top-right corner of the screen, click **Quick Config**.
   The **RBAC Journey :: Authentication** page is displayed.
4. Navigate to the **Role** stage as part of the wizard flow to add roles into AppViewX.



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

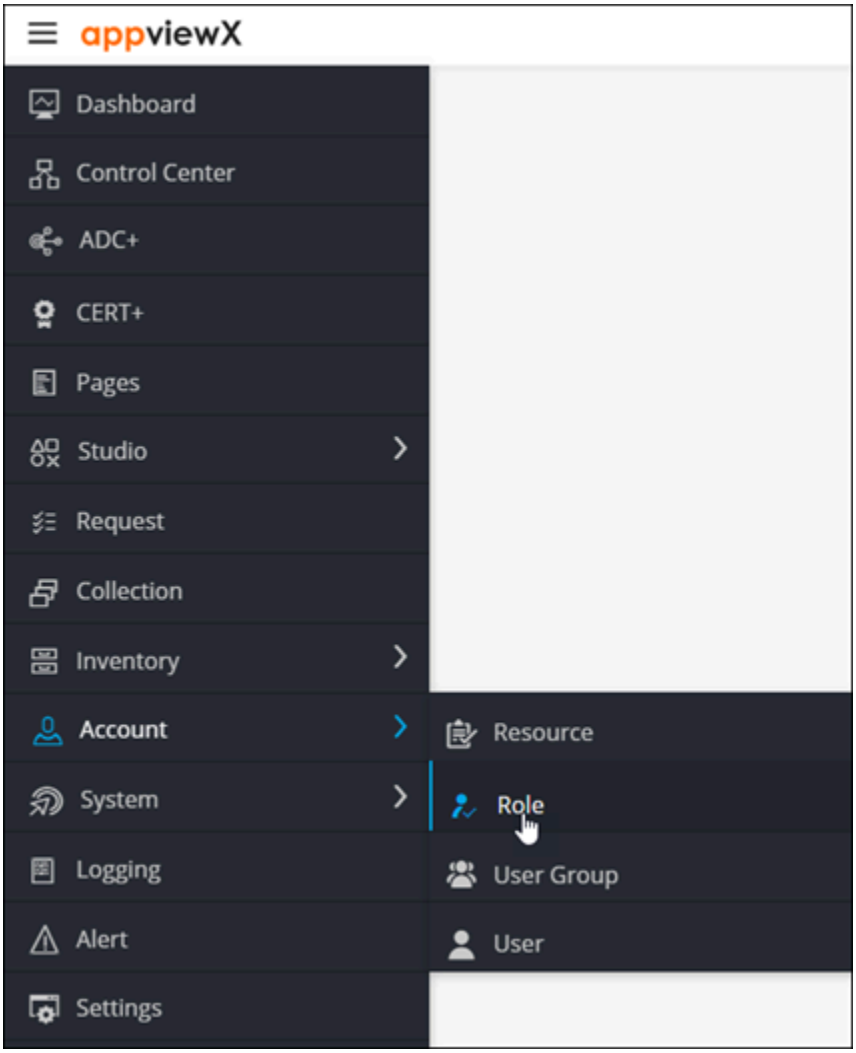


7. In the **Clone** action pane, modify the details in the **Information** and **Authorized functions** sections as required.
8. Click **Save**.

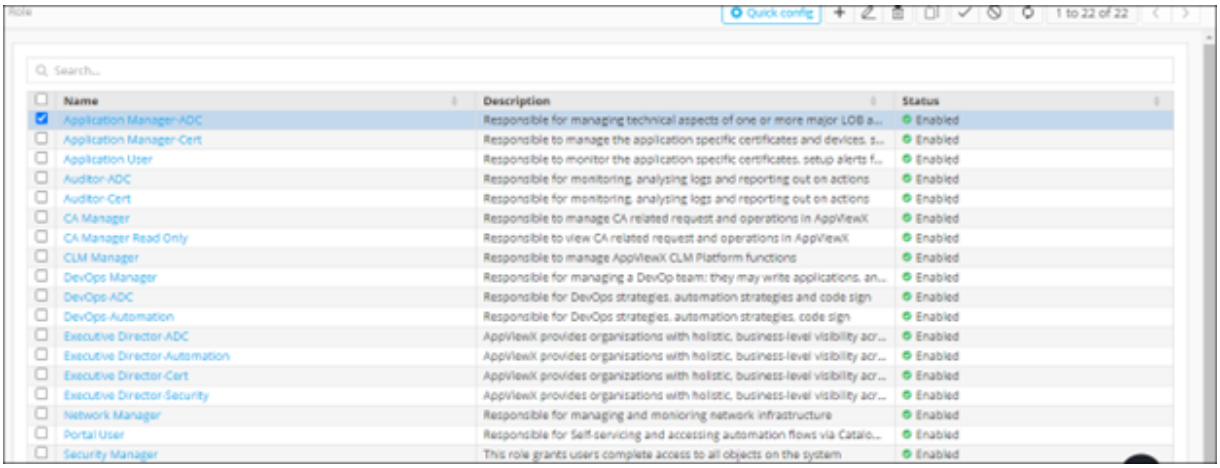
Modifying a Role

To modify a custom role:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Account** > **Role**.



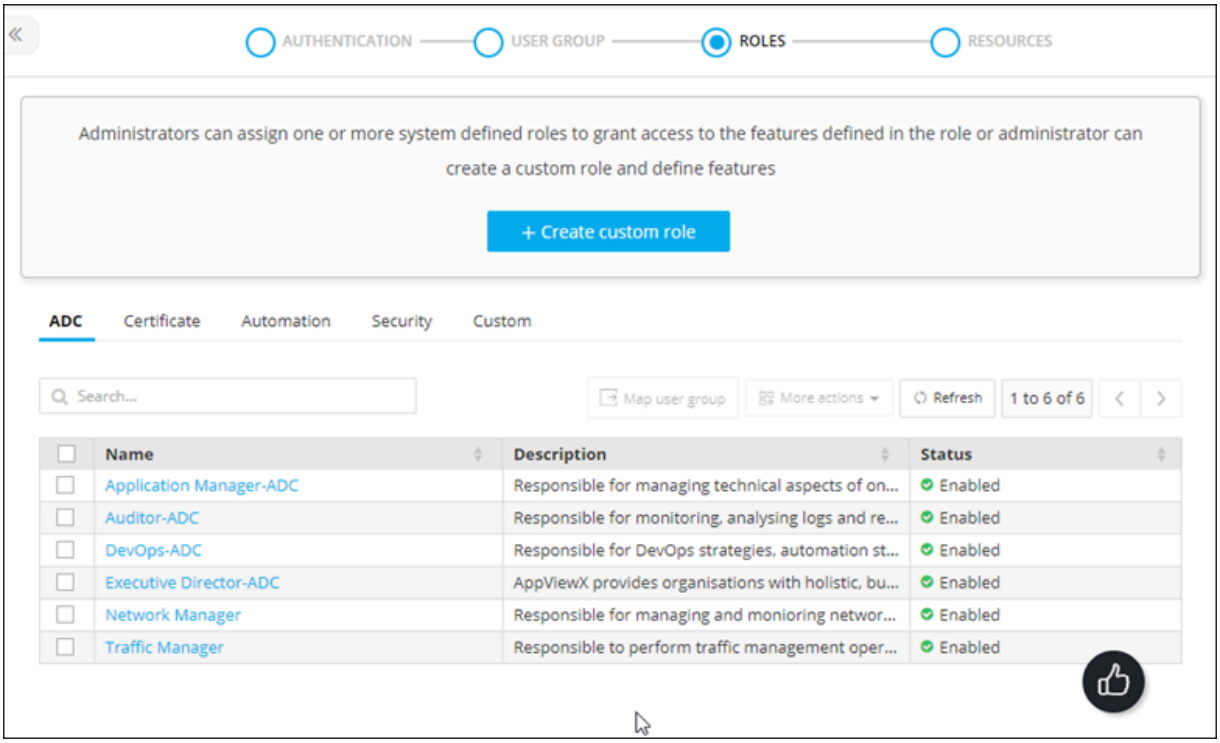
The **Role** page is displayed.



3. From the top-right corner of the screen, click **Quick Config**.

   The **RBAC Journey :: Authentication** page is displayed.

4. Navigate to the **Role** stage as part of the wizard flow to add roles into AppViewX.



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

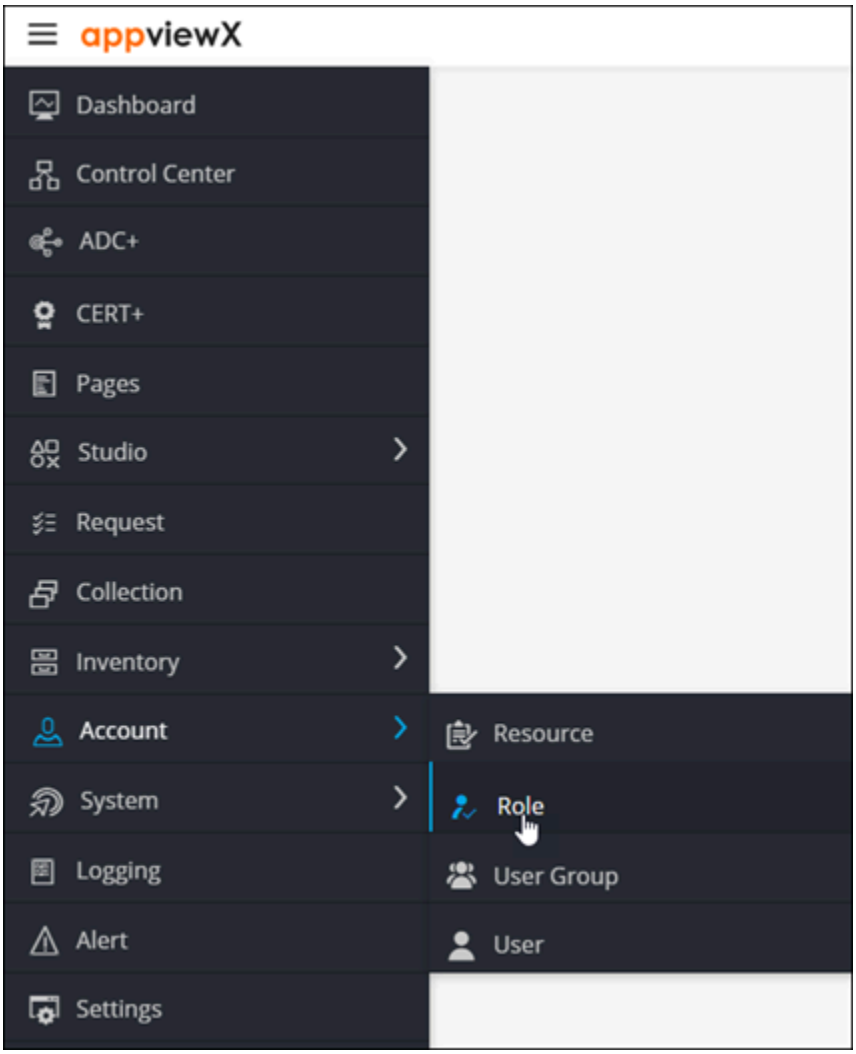
8. Click **Save**.

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

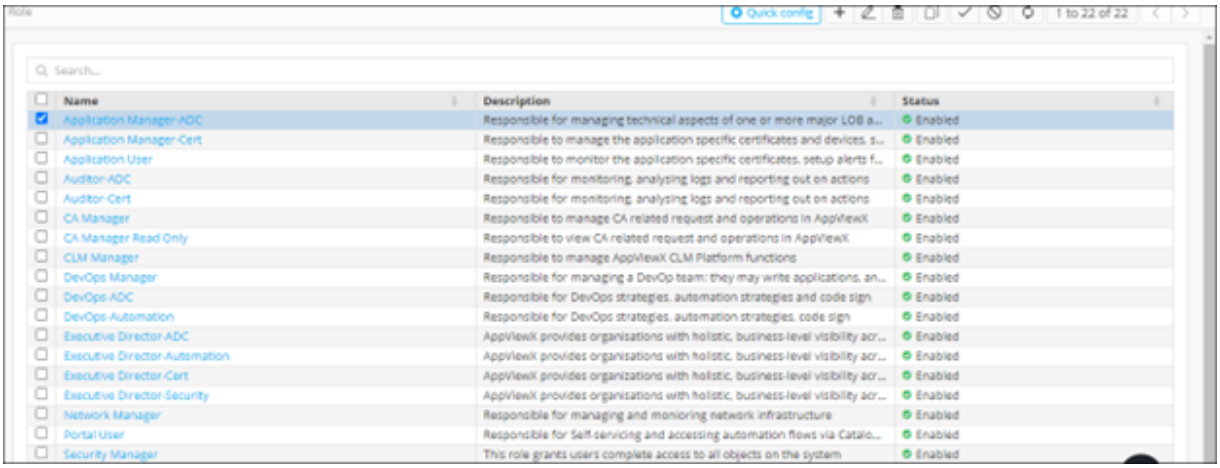
Enabling a Role

To enable a role:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Account** > **Role**.



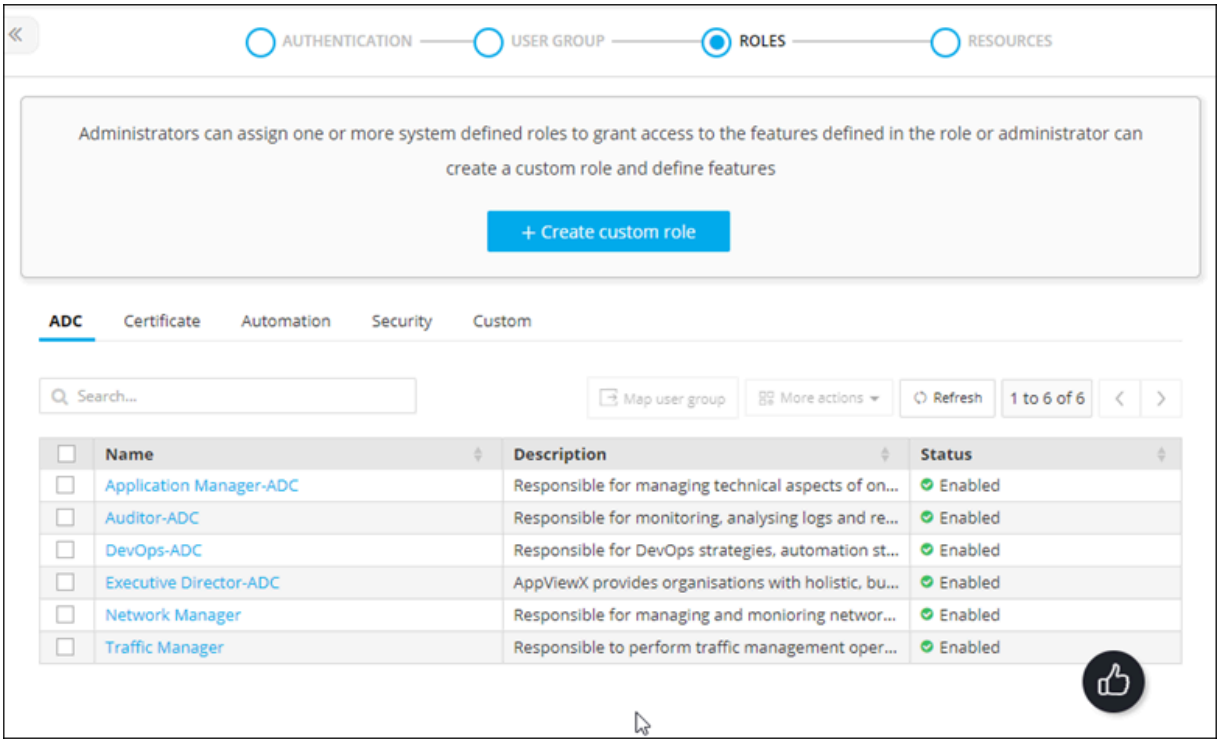
The **Role** page is displayed.



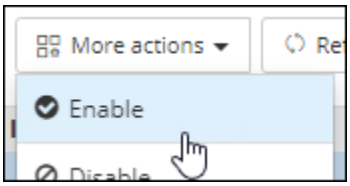
3. From the top-right corner of the screen, click **Quick Config**.

   The **RBAC Journey :: Authentication** page is displayed.

4. Navigate to the **Role** stage as part of the wizard flow to add roles into AppViewX.



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



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

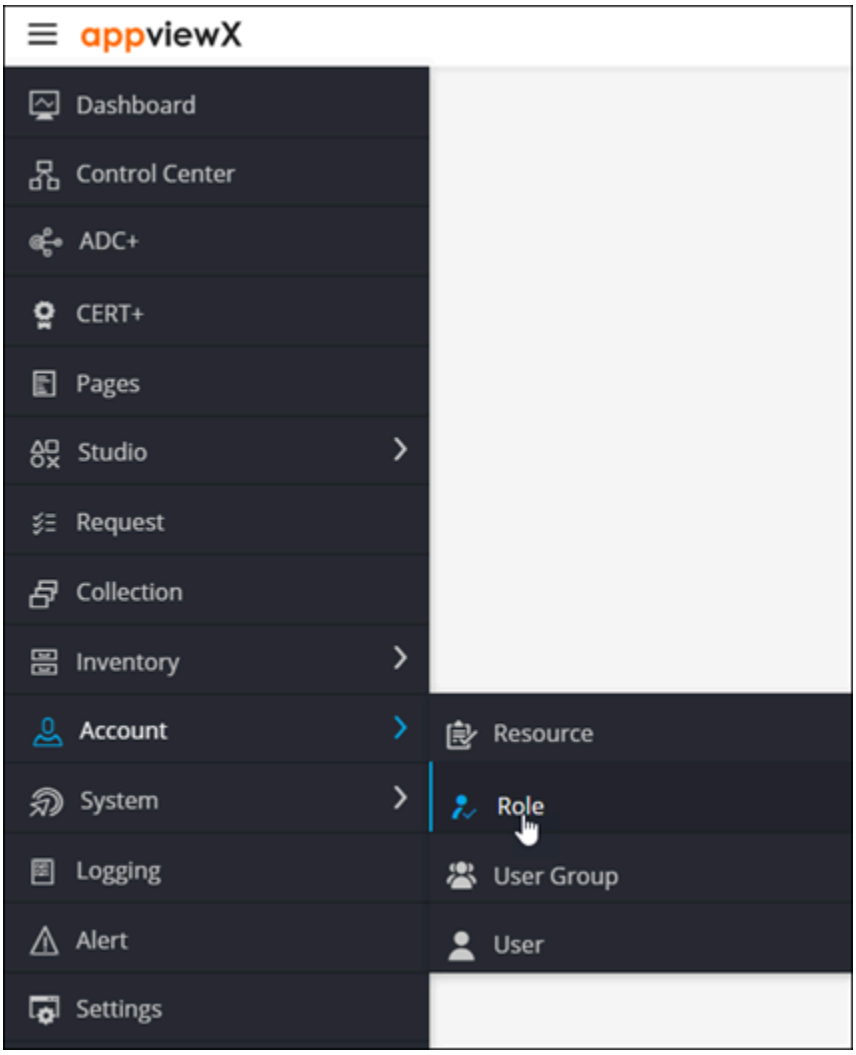
Disabling a Role

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

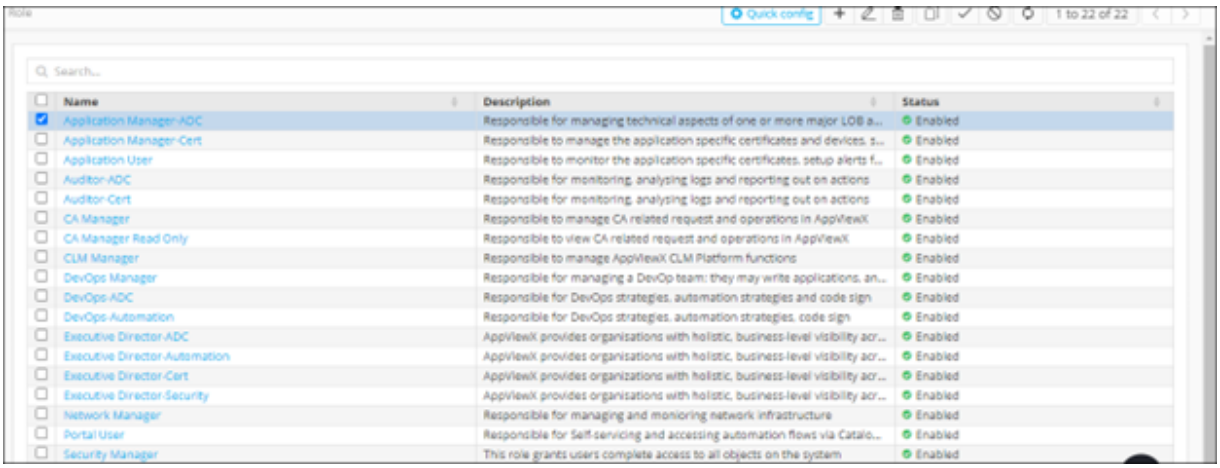
Note: The users associated with a disabled role through a user group will not be allowed to log in to AppViewX.

To disable a role:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Account** > **Role**.



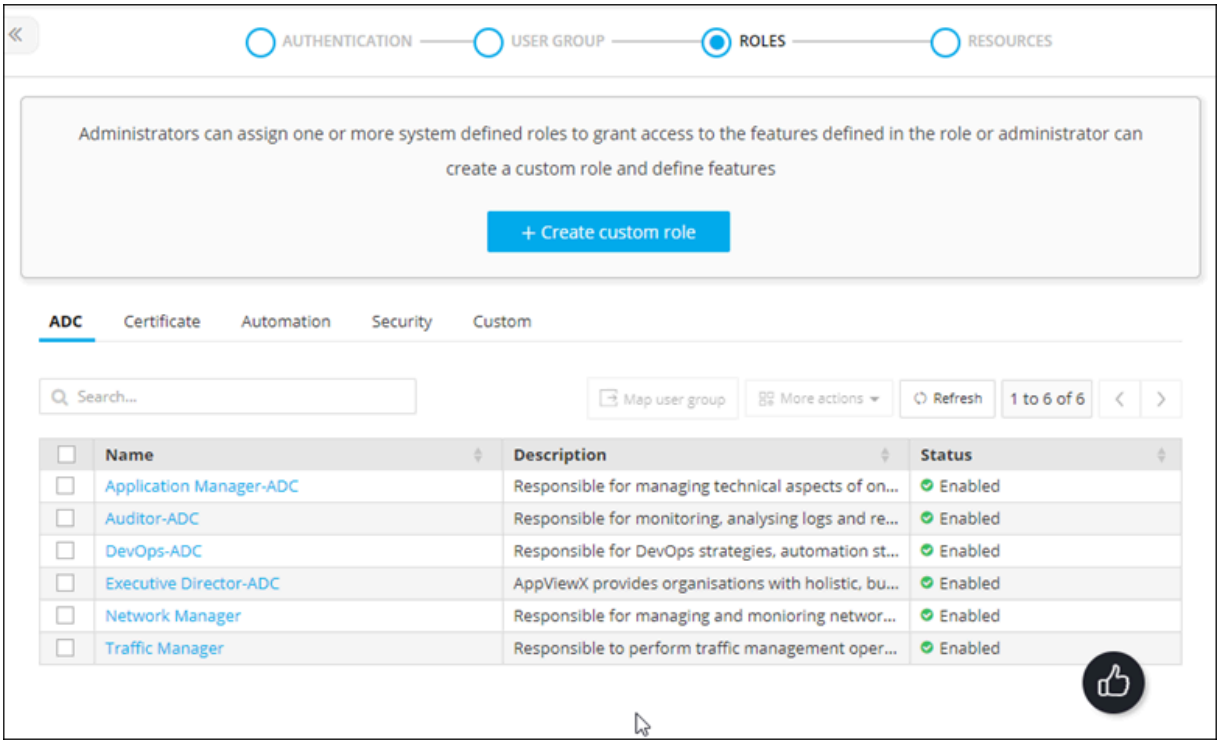
The **Role** page is displayed.



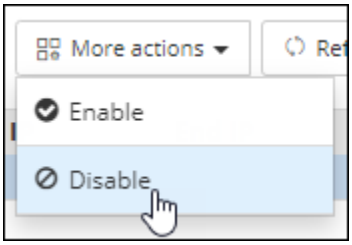
3. From the top-right corner of the screen, click **Quick Config**.

   The **RBAC Journey :: Authentication** page is displayed.

4. Navigate to the **Role** stage as part of the wizard flow to add roles into AppViewX.



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

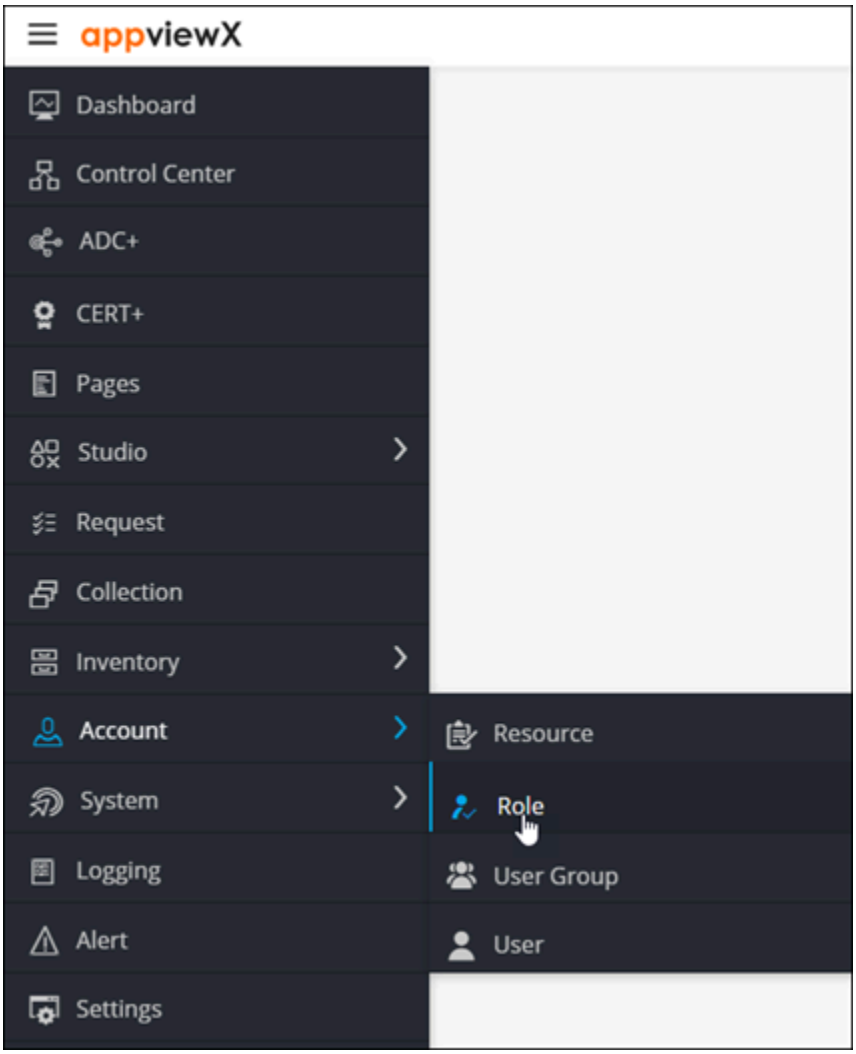


7. In the **Disable** role(s) dialog box, click **Yes**.

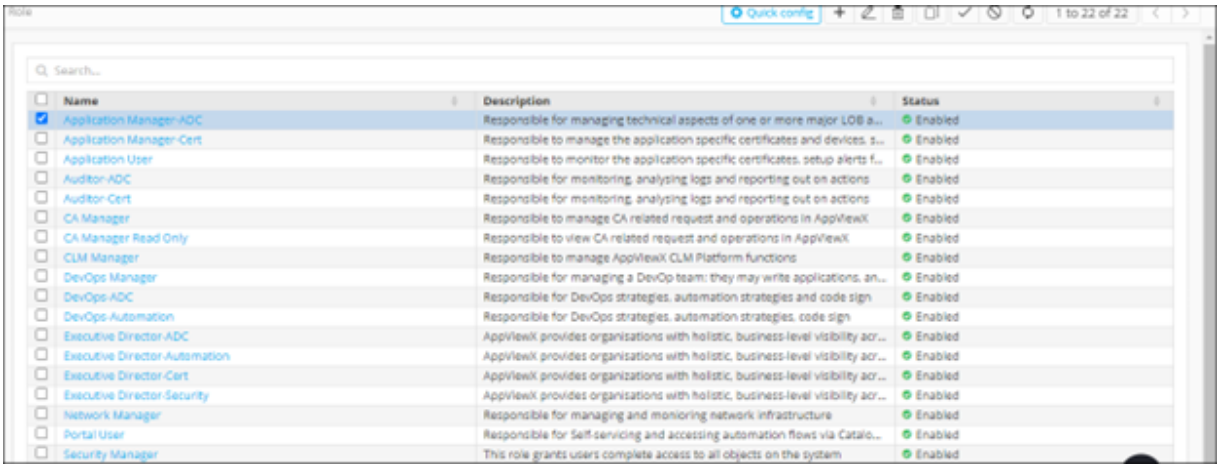
Mapping Role to User Groups

To map roles to user groups:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Account** > **Role**.



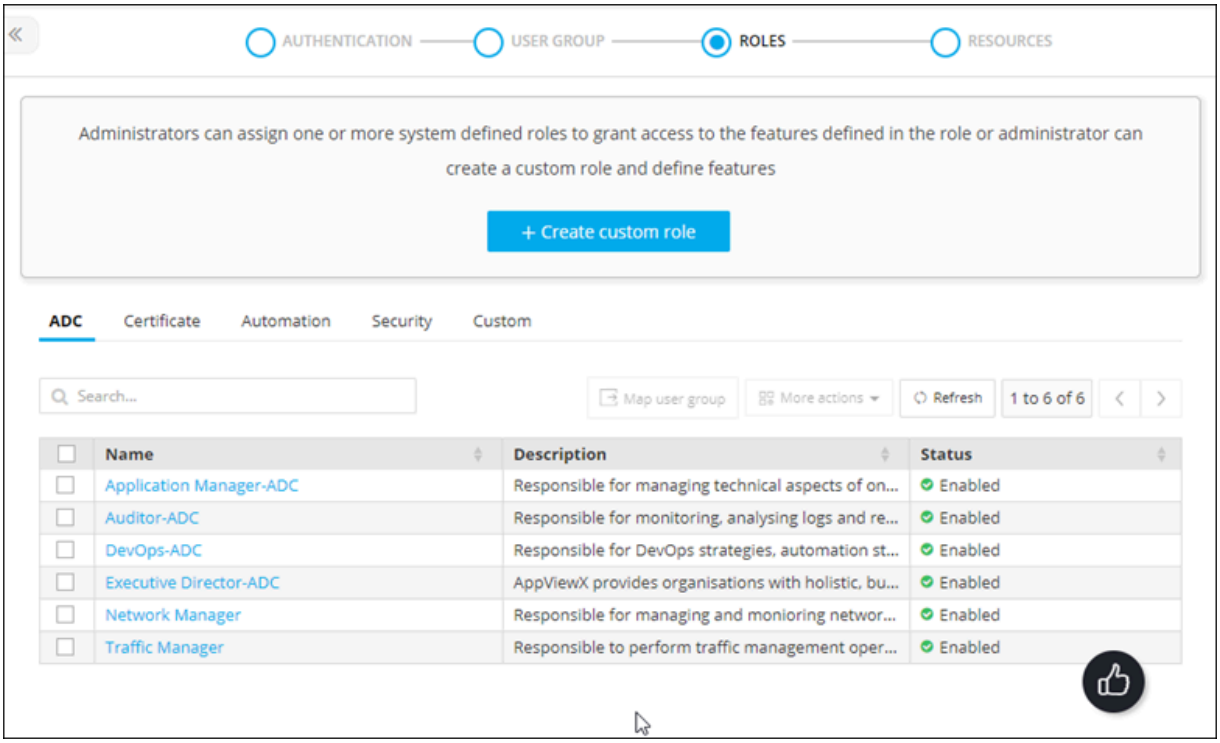
The **Role** page is displayed.



3. From the top-right corner of the screen, click **Quick Config**.

   The **RBAC Journey :: Authentication** page is displayed.

4. Navigate to the **Role** stage as part of the wizard flow to add roles into AppViewX.



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

.
7. In the **Mapping user group** action pane, select the user groups the role will be mapped to.

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

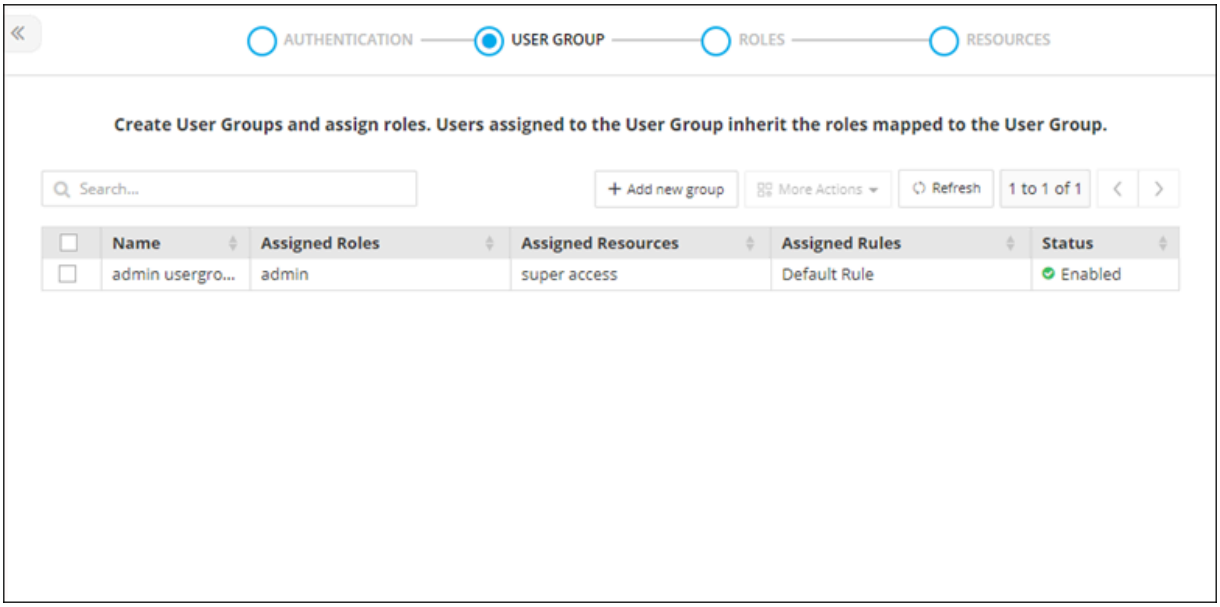
User Group

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



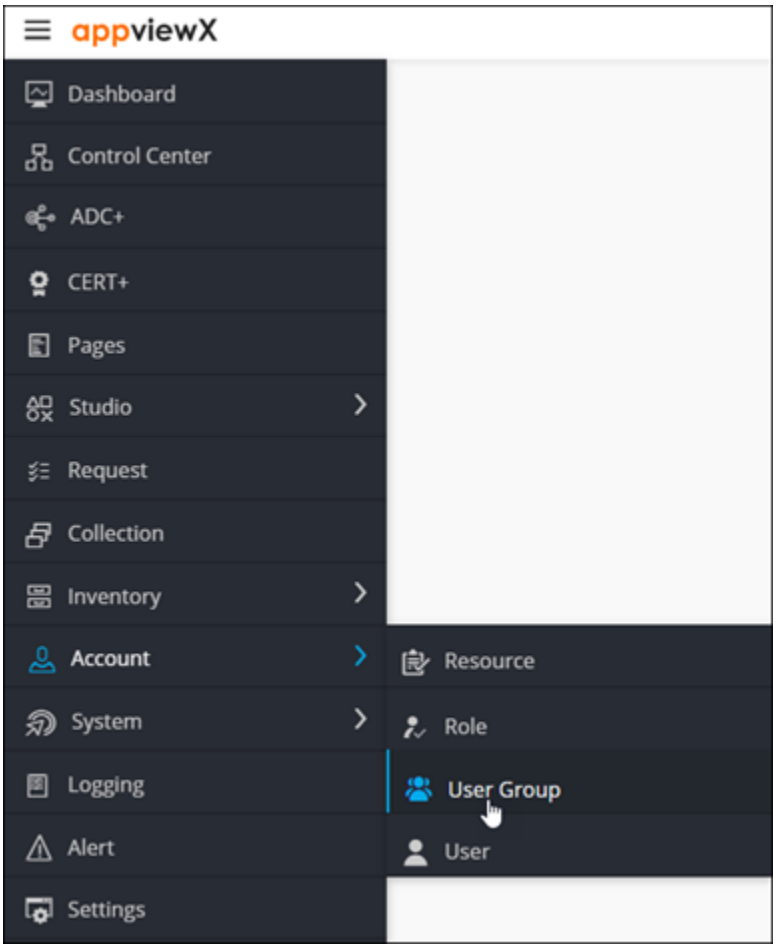
2. The User group inventory table is displayed with the list of available user groups in AppViewX along with corresponding roles and resources mapping.
3. In the User group stage, user group creation can be done by fetching groups from LDAP or through bulk import.
4. In addition to this, existing user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

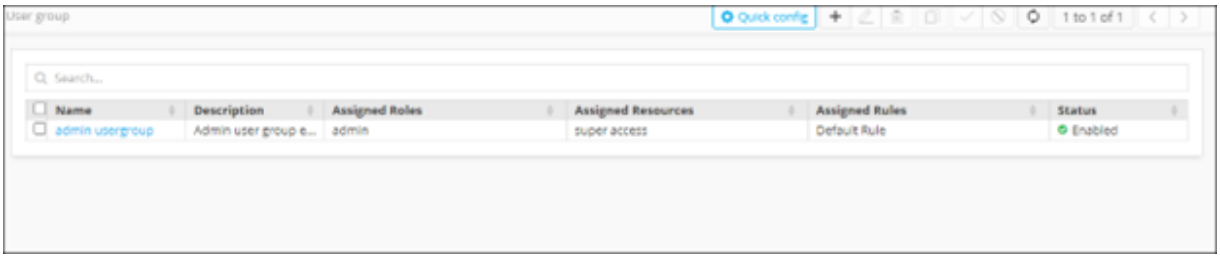
Adding a New User Group by Syncing Groups from LDAP

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

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Account** > **User Group**.



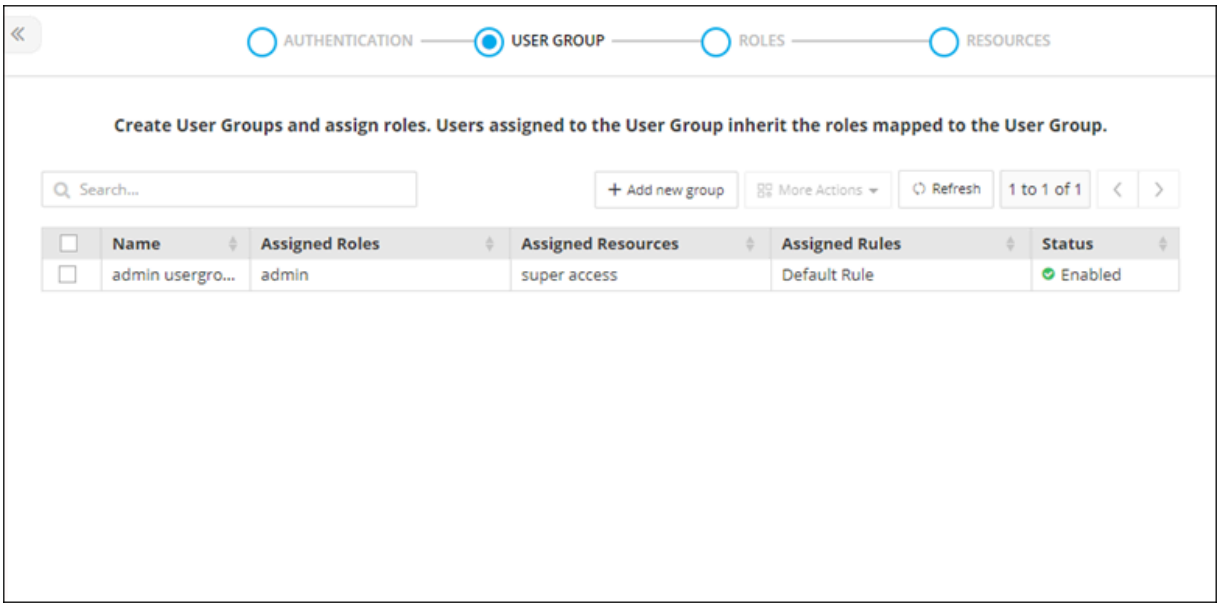
The **UserGroup** page is displayed.



3. From the top-right corner of the screen, click **Quick Config**.

   The **RBAC Journey :: Authentication** page is displayed.

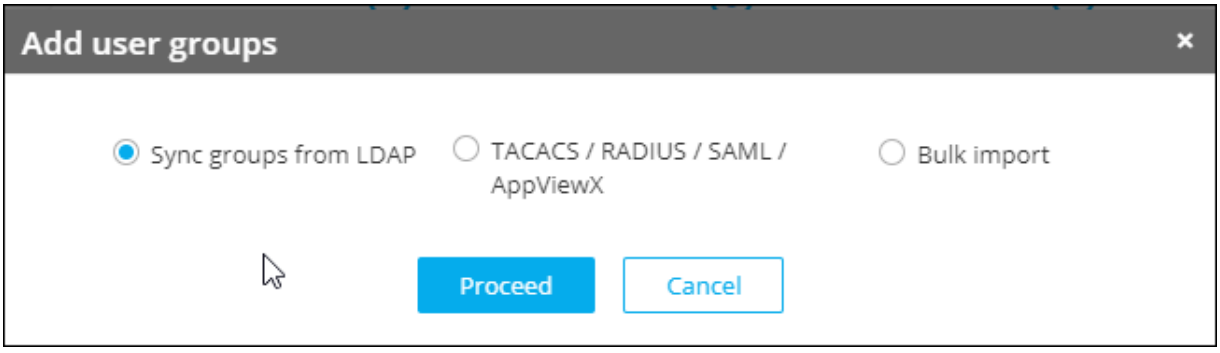
4. Navigate to the **User Group** stage as part of the wizard flow to add user groups into AppViewX.



5. Click 

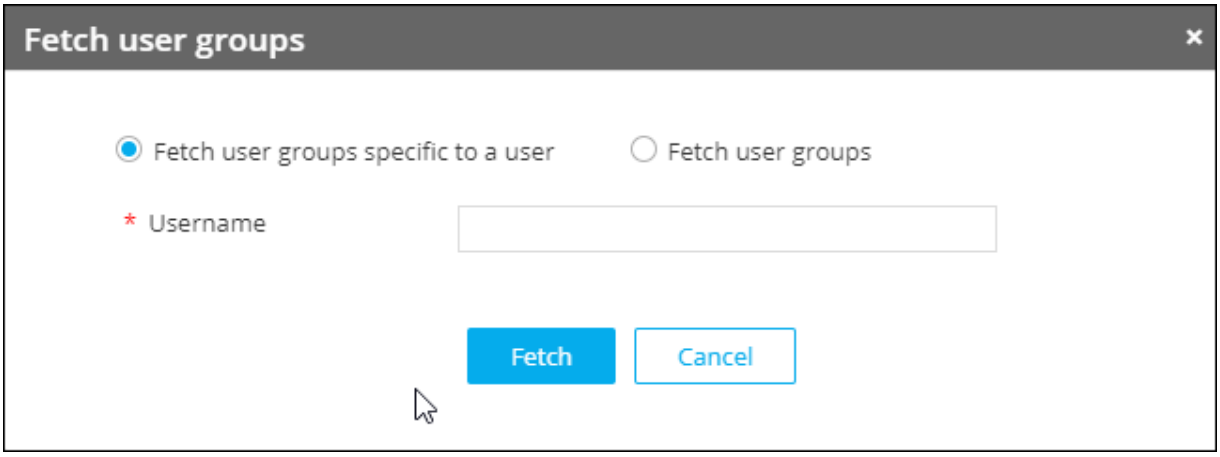
.

6. From the **Add user groups** dialog box, select **Sync groups from LDAP** and click **Proceed**.



The LDAP inventory table is displayed.

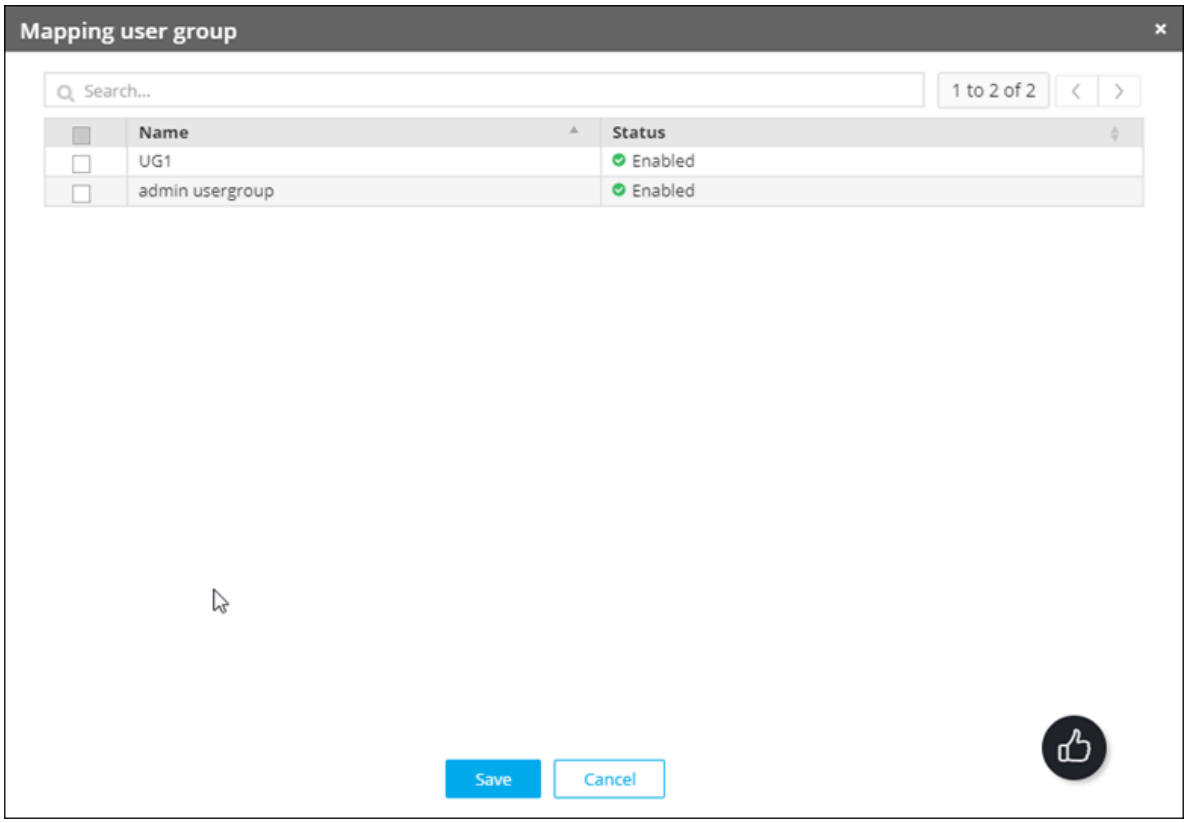
7. To view the user groups available in the AD and create or map them with the existing user groups in AppViewX, from the LDAP inventory table, click Fetch.
   The **Fetch user groups** dialog box is displayed.



8. 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 enter 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 (*).

9. Click **Fetch**.
   A table containing the AD group names and their corresponding AppViewX user group names is displayed.
10. Select the AD user group(s) that must be created with the same name in AppViewX and click Save to Appviewx.
11. 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**.

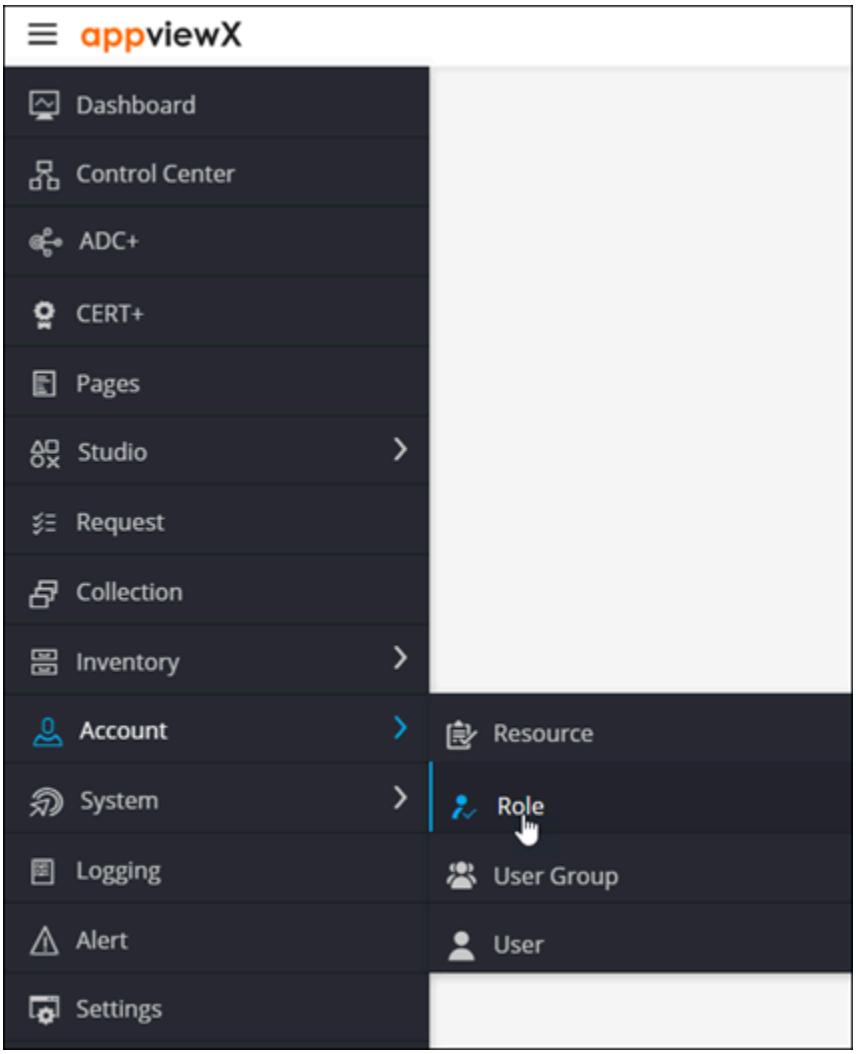
Selected AD user group(s) will be now mapped to the existing AppViewX user group and the same mapping will reflect in the AD group names table.

12. 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** or to export all user groups, select the **All User Group(s)** option and click **Yes**.
    c. The selected/all user group(s) should be automatically exported in (.CSV) Format.

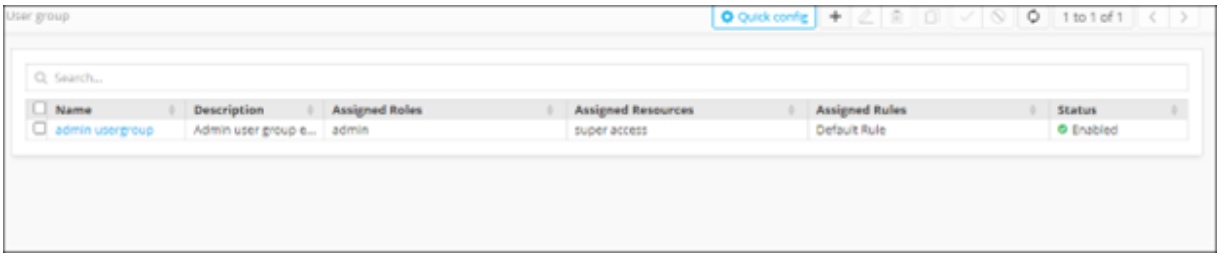
Adding a New User Group using the TACACS/RADIUS/SAML/AppViewX Option

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

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Account** > **Role**.



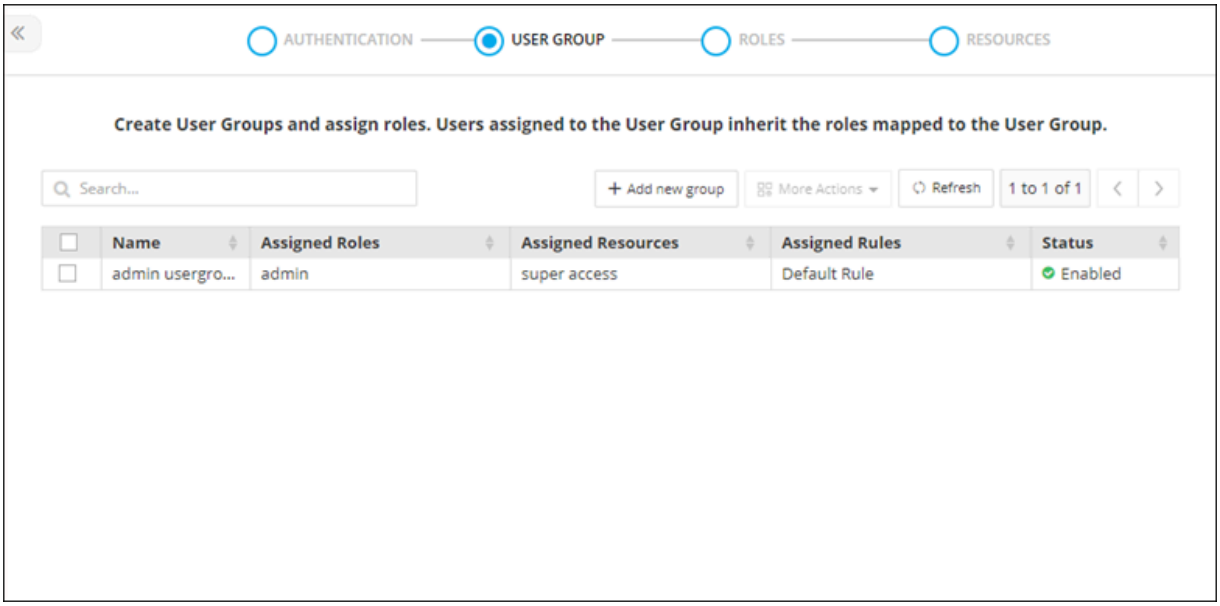
The **UserGroup** page is displayed.



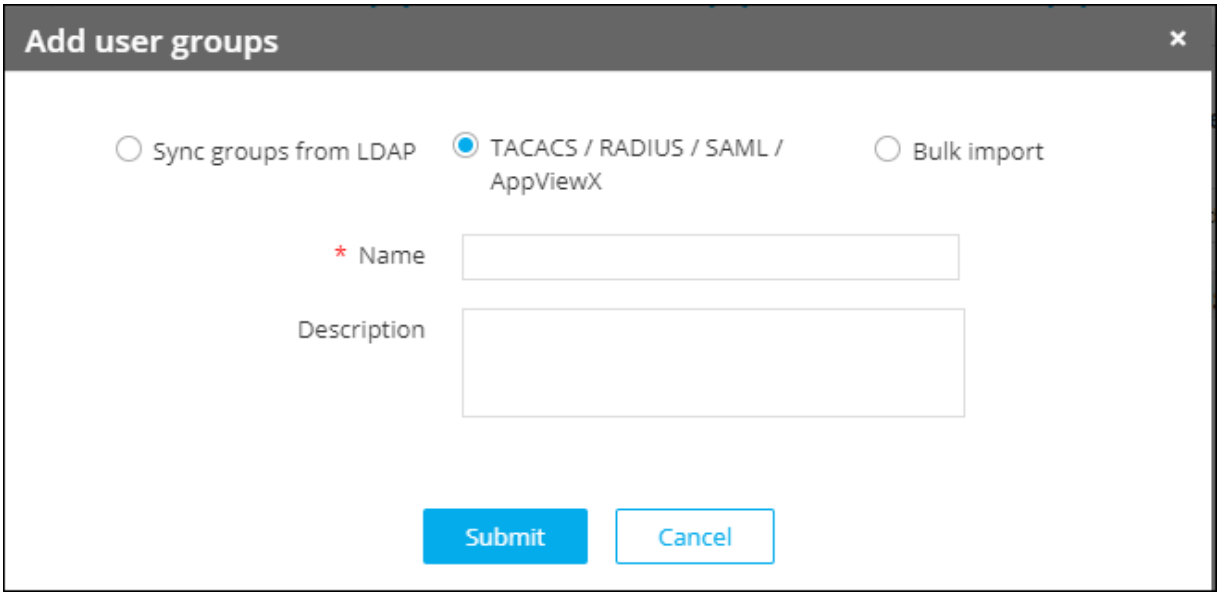
3. From the top-right corner of the screen, click **Quick Config**.

   The **RBAC Journey :: Authentication** page is displayed.

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



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

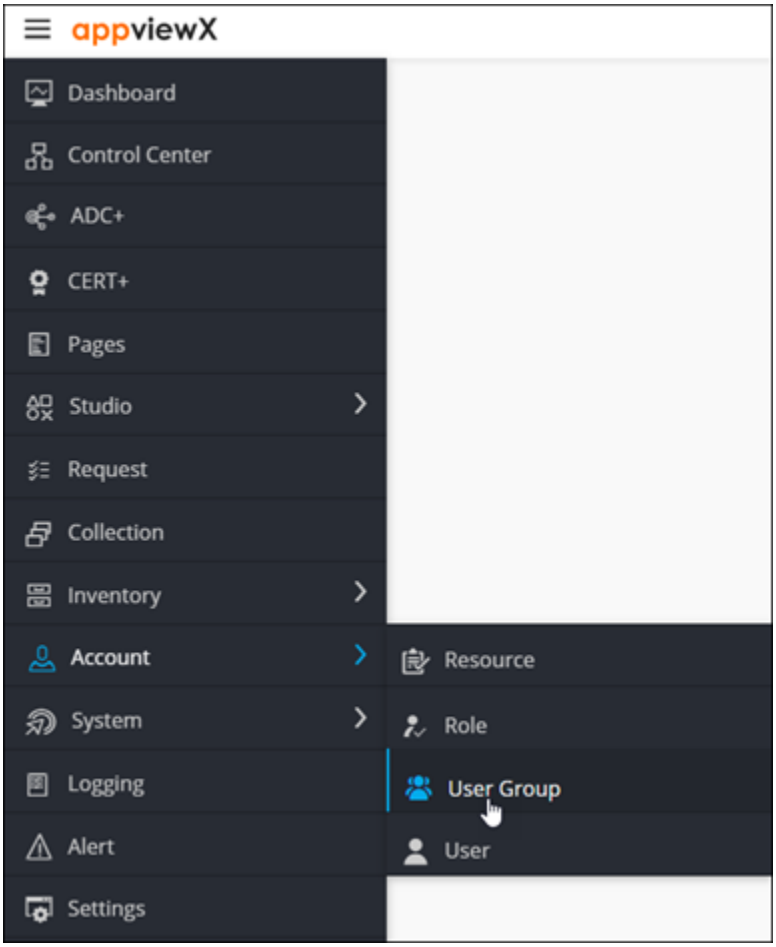


8. Click **Submit**.

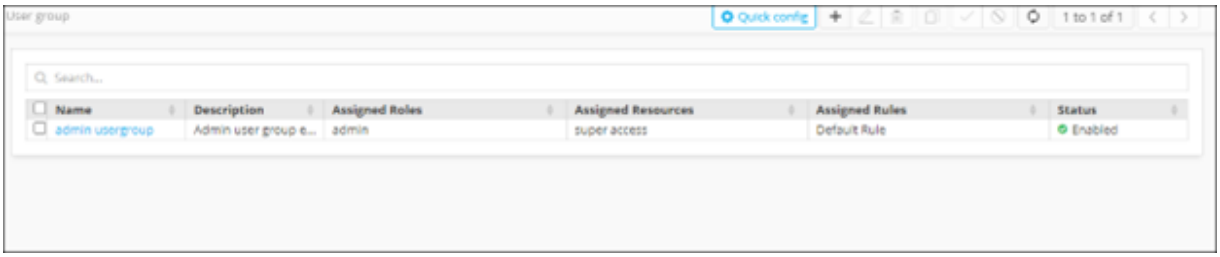
Add New User Group by Bulk Import

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

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Account** > **User Group**.



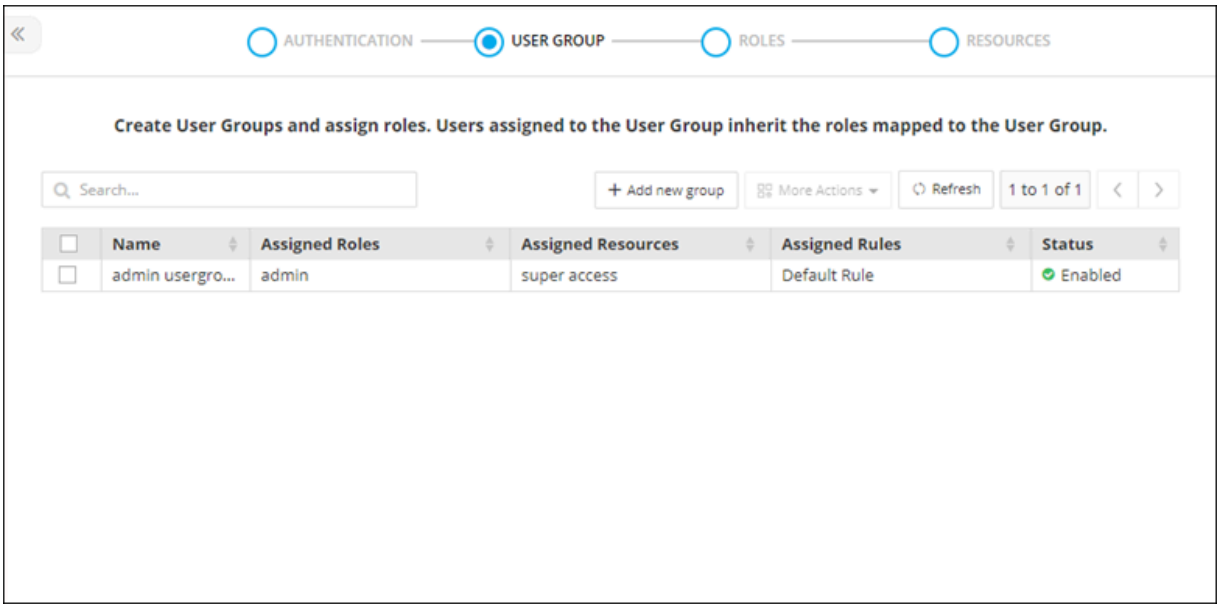
The **UserGroup** page is displayed.



3. From the top-right corner of the screen, click **Quick Config**.

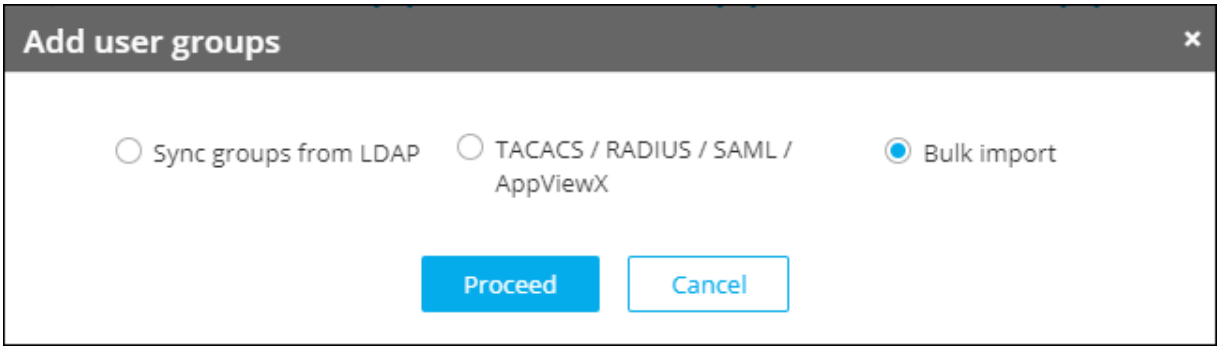
The **RBAC Journey :: Authentication** page is displayed.

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



5. Click 

.
6. From the **Add user groups** dialog box, select **Bulk import** and click **Proceed**.



7. Click **Browse**.
8. 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 .

9. 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).

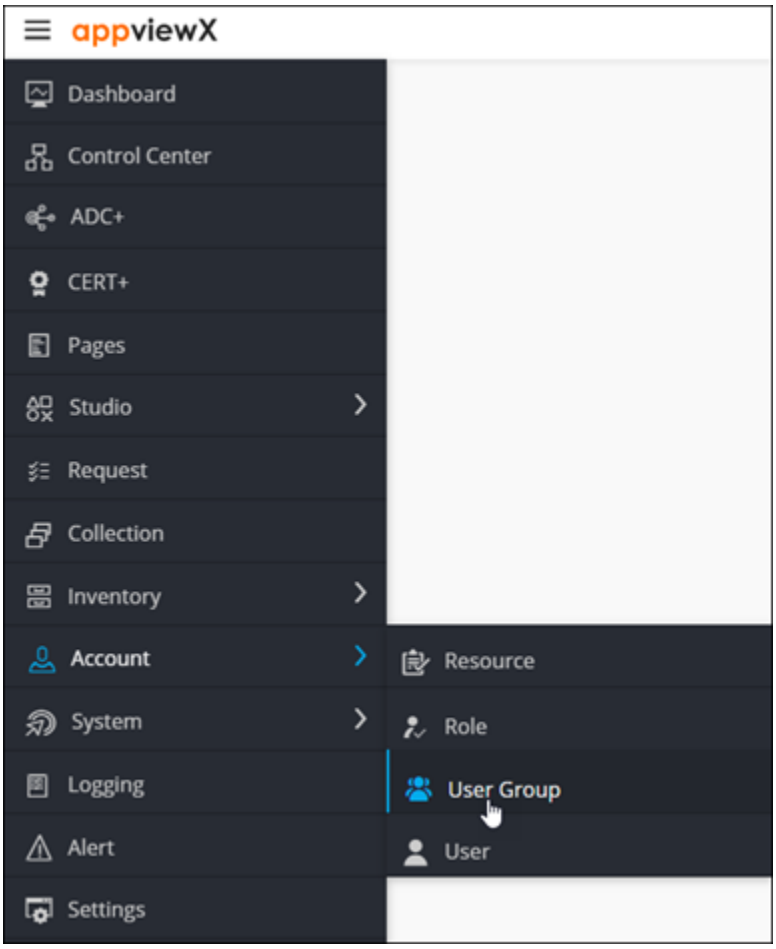
10. To save the user groups, select the list of user groups and click **Submit**.
    All user groups with the valid status will be saved into AppViewX.

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

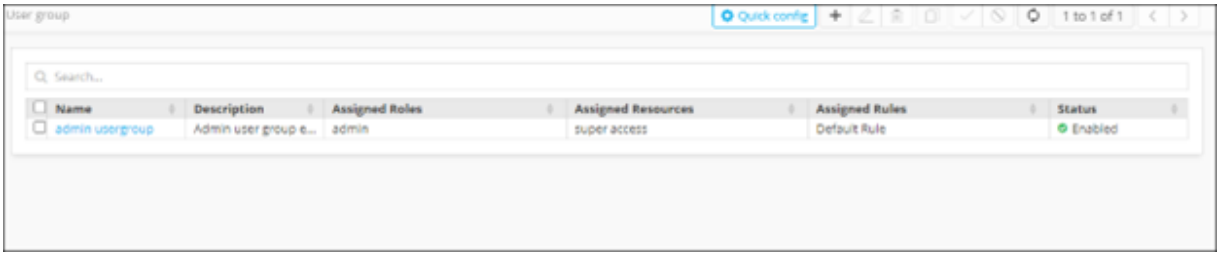
Disabling a User Group

To disable a user group:

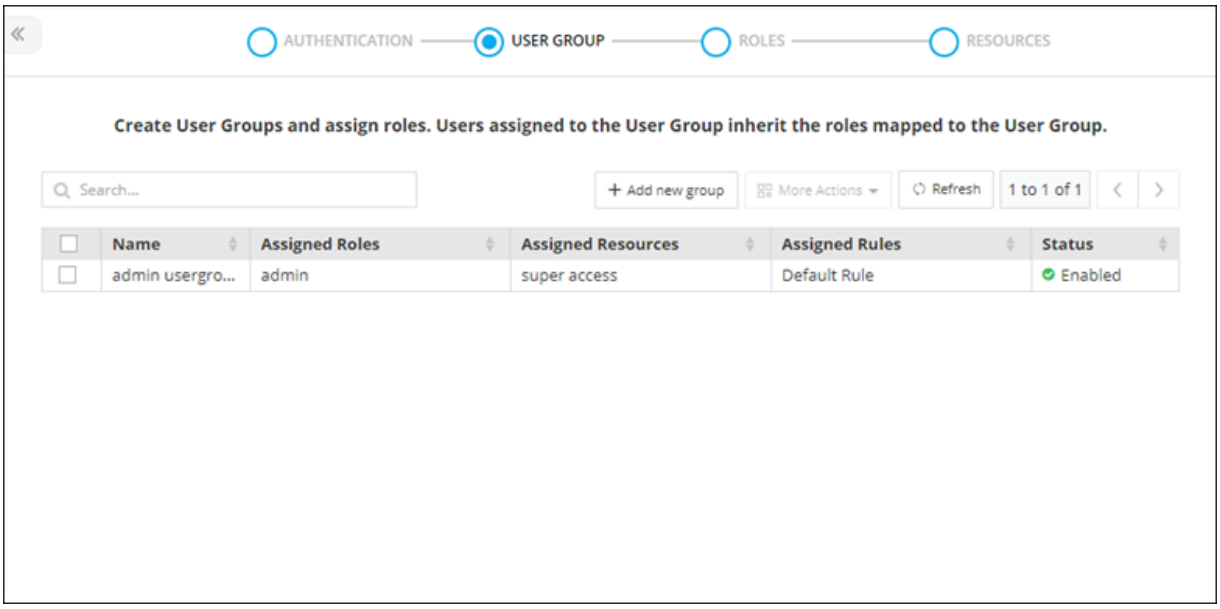
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Account** > **User Group**.



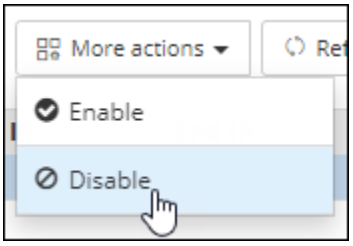
The **UserGroup** page is displayed.



3. From the top-right corner of the screen, click **Quick Config**.
   The **RBAC Journey :: Authentication** page is displayed.
4. Navigate to the **User Group** stage as part of the wizard flow to add user groups into AppViewX.



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

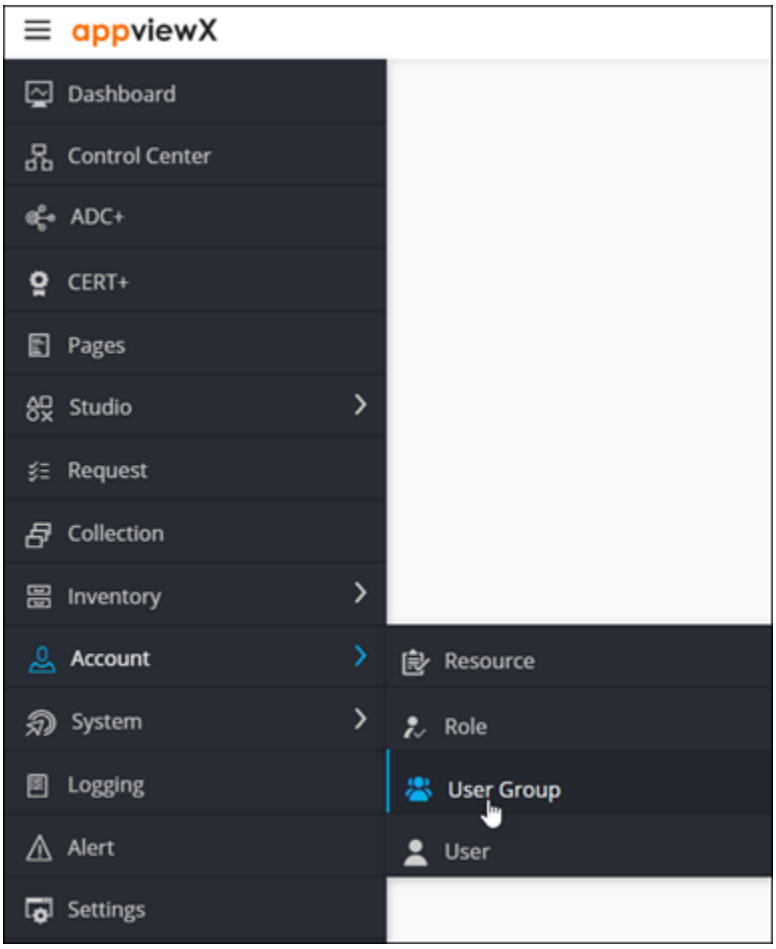


7. From the **Disable user group** dialog box, click **Yes**.

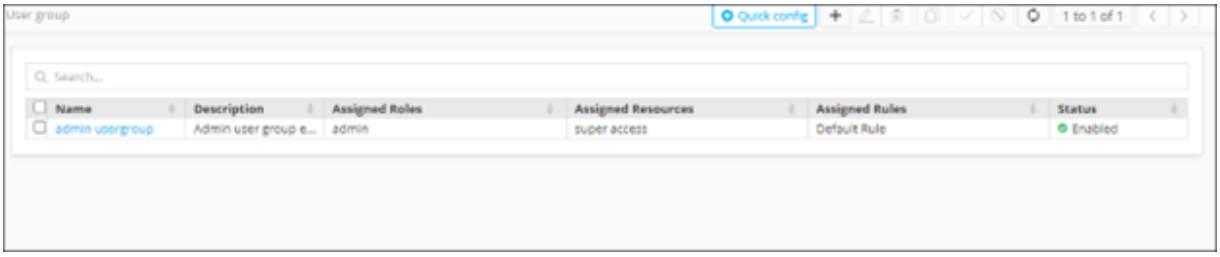
Enabling a User Group

To enable a user group:

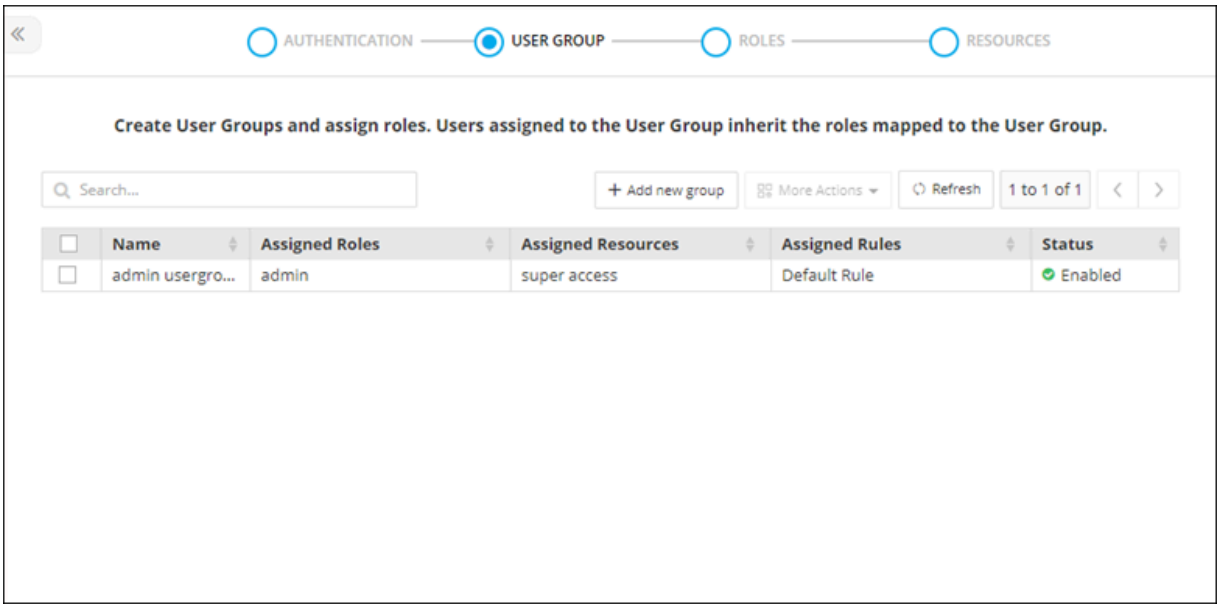
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Account** > **User Group**.



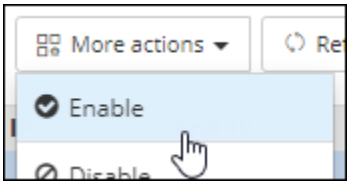
The **UserGroup** page is displayed.



3. From the top-right corner of the screen, click **Quick Config**.
   The **RBAC Journey :: Authentication** page is displayed.
4. Navigate to the **User Group** stage as part of the wizard flow to add user groups into AppViewX.



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

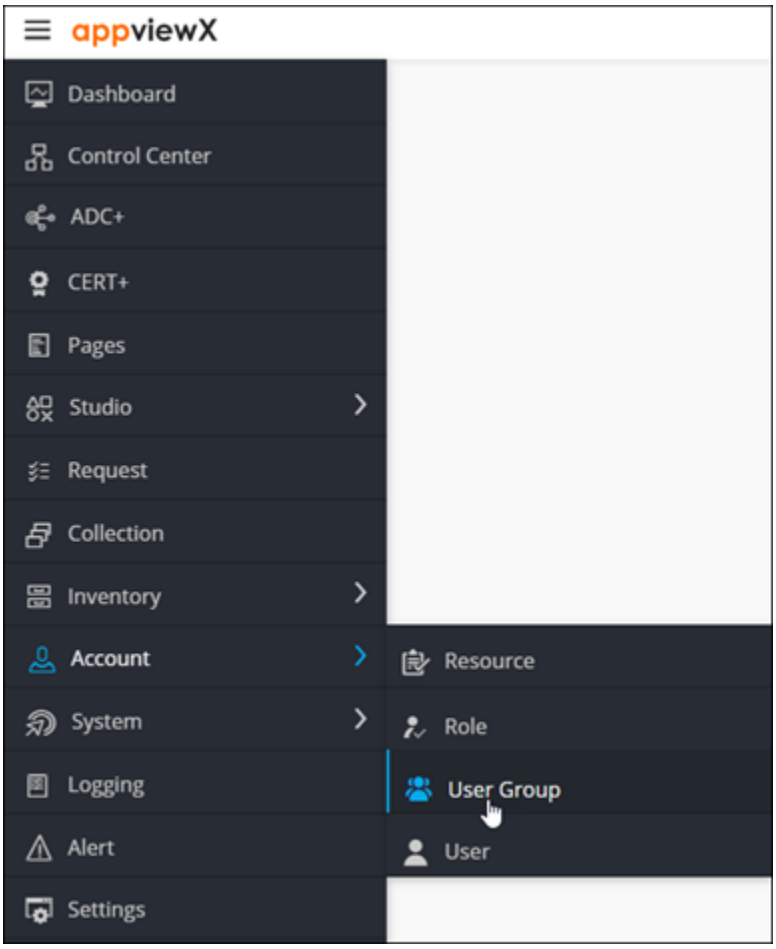


7. From the **Enable user group** dialog box, click **Yes**.

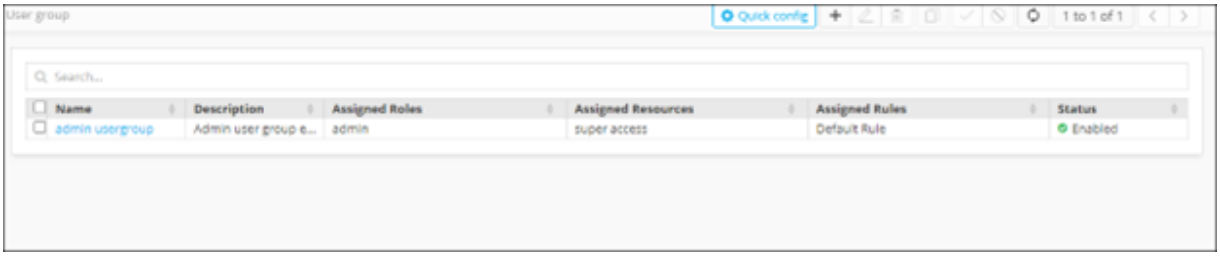
Cloning a User Group

To clone a user group:

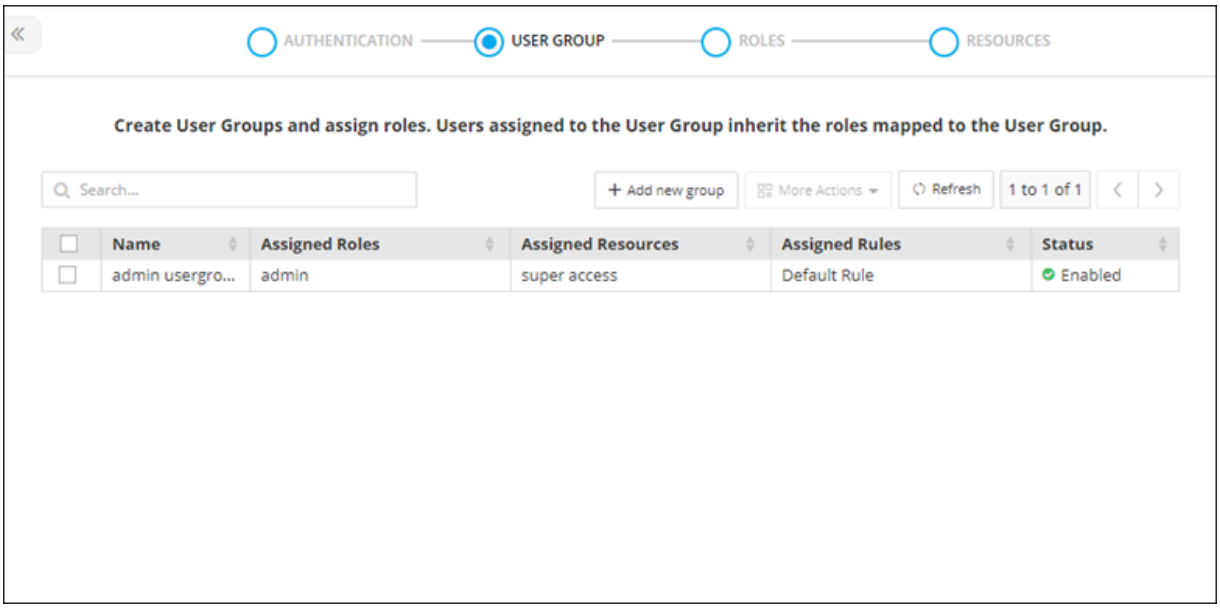
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Account** > **User Group**.



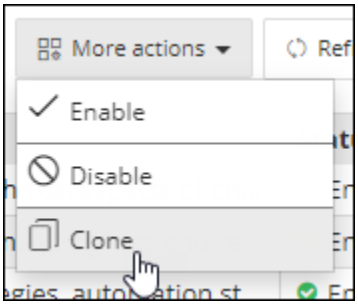
The **UserGroup** page is displayed.



3. From the top-right corner of the screen, click **Quick Config**.
   The **RBAC Journey :: Authentication** page is displayed.
4. Navigate to the **User Group** stage as part of the wizard flow to add user groups into AppViewX.



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

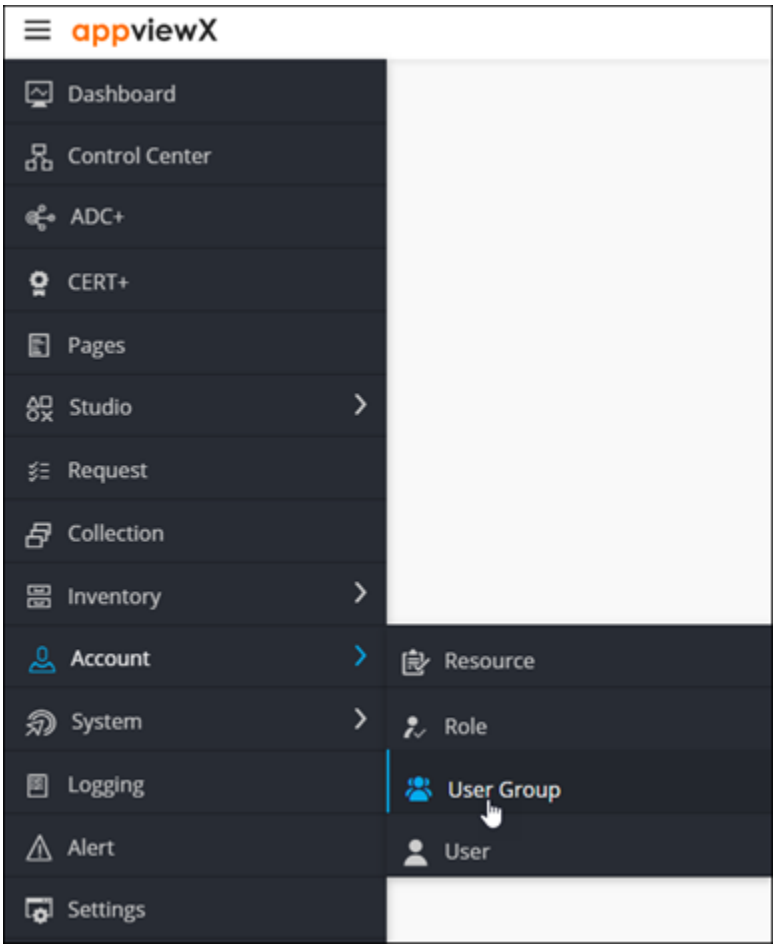


7. In the **Clone** dialog box, enter a name for the cloned user group and update the description, if required.
8. Click **Save**.

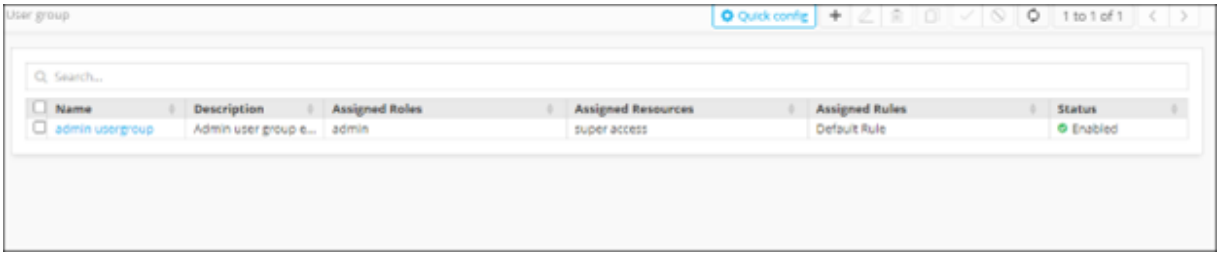
Deleting a User Group

To delete a user group:

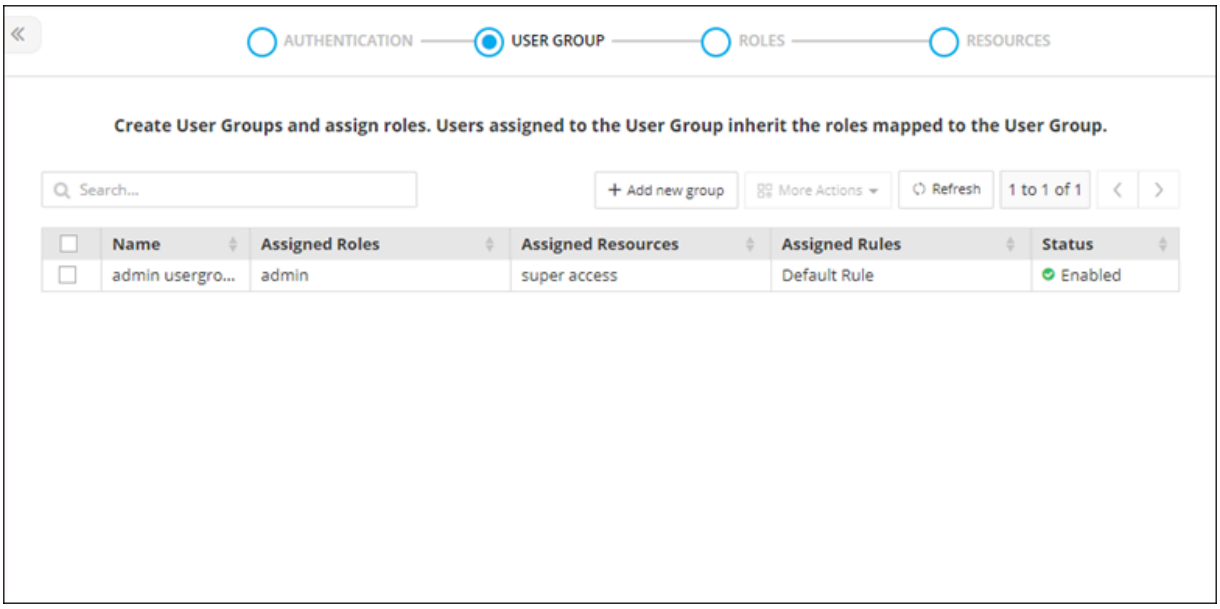
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Account** > **User Group**.



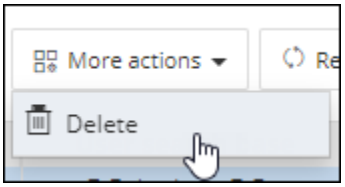
The **UserGroup** page is displayed.



3. From the top-right corner of the screen, click **Quick Config**.
   The **RBAC Journey :: Authentication** page is displayed.
4. Navigate to the **User Group** stage as part of the wizard flow to add user groups into AppViewX.



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



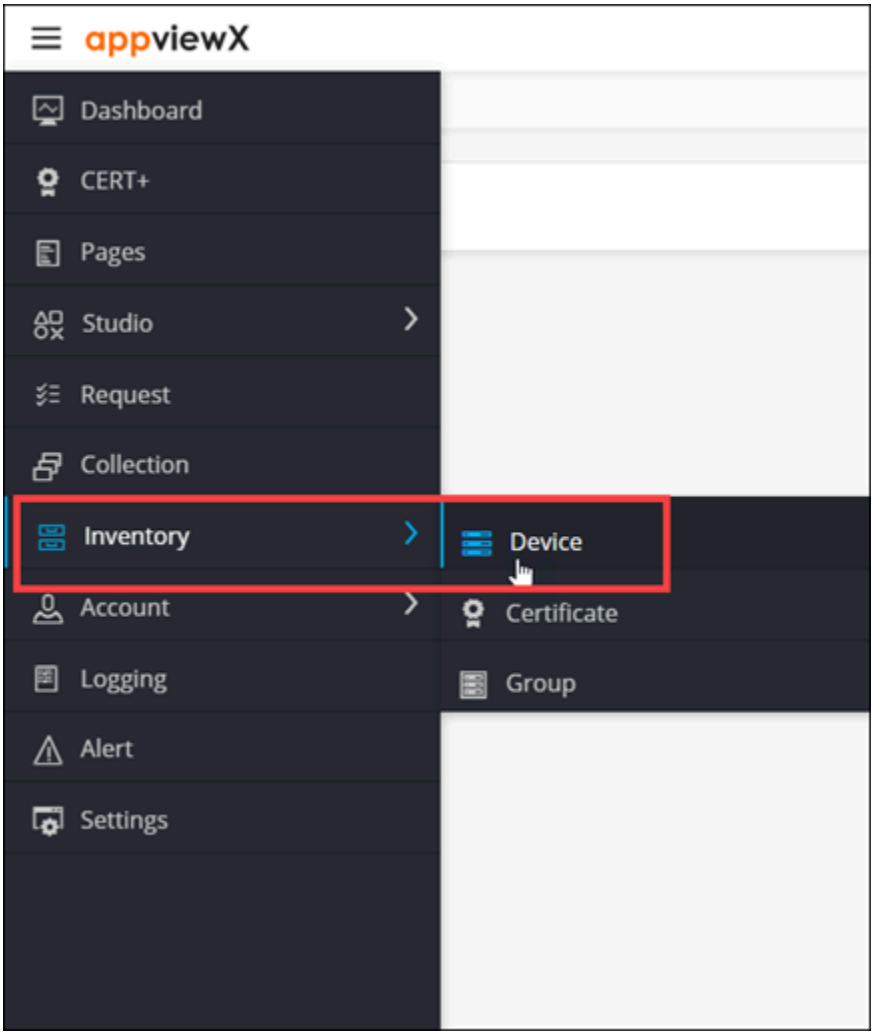
7. From the **Delete user group** dialog box, click **Yes**.

Chapter 4: Managing HSM Integration

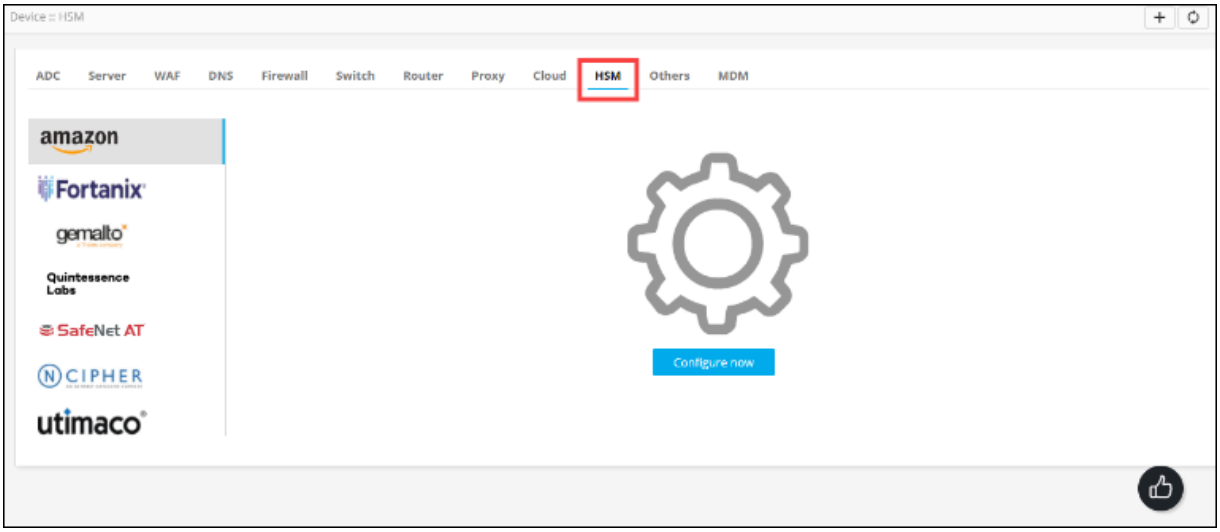
An HSM (Hardware Security Module) is a piece of hardware and associated software or firmware that usually resides in a PC or server and provides at least the minimal cryptographic functions. These functions include (but are not limited to) encryption, decryption, key generation, and hashing. The physical 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.

To integrate a HSM device:

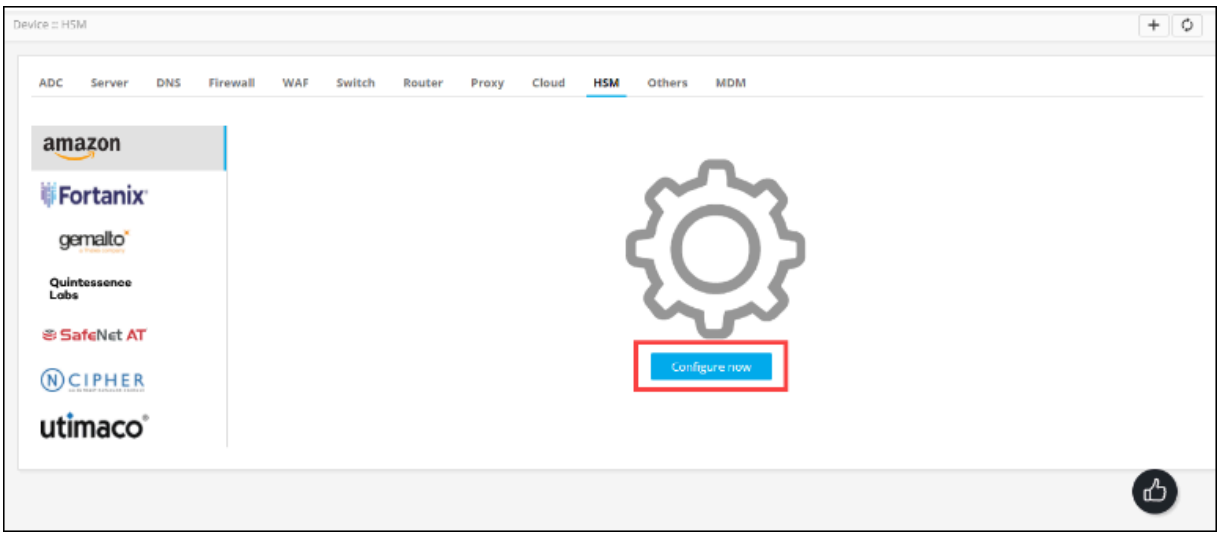
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Inventory** > **Device**.
   The **Device :: ADC** page is displayed.



3. On the **Device :: ADC** page, to configure the HSM settings, click the **HSM** tab.
   The **Device :: HSM** page is displayed.



4. From the left pane, select the vendor for integrating the HSM device.
5. For the selected vendor, click **Configure Now**.



6. For all vendors, in the **General information** section, enter the following details:

Field	Description
***Name**	Name of the device/settings being integrated
Description	Description/purpose of adding the device

Field	Description
Implementation type	From the drop-down menu, select one of the following options: • CSR Generation • Private key encryption • Both
Default	
Data center	From the drop-down menu, select the data center where the HSM AppViewX VM is deployed
All * marked fields are mandatory.	

7. In the **Vendor specific details** section, enter the required details.
   - To enter vendor specific details for **Fortanix**, click here.
   - To enter vendor specific details for **Gemalto**, click here.
   - To enter vendor specific details for **SafeNet AT**, click here.
   - To enter vendor specific details for **Utimaco**, click here.
8. To save the HSM integration details, click **Save**.

Chapter 5: HSM Integration for AppViewX

Overview

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. 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
- Fortinax
- Thales - DPoD
- Thales - GPN

Utimaco

To integrate a HSM device from Amazon, enter the following details:

Field	Description
Slot Id*	Unique identification number of the slot in the HSM Luna client that will be used to communicate with the end HSM device

Field	Description
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.
All * marked fields are mandatory.	

• Integrating the Utimaco HSM with the AppViewX

Integrating the Utimaco HSM with the AppViewX

To integrate the Utimaco HSM with the AppViewX:

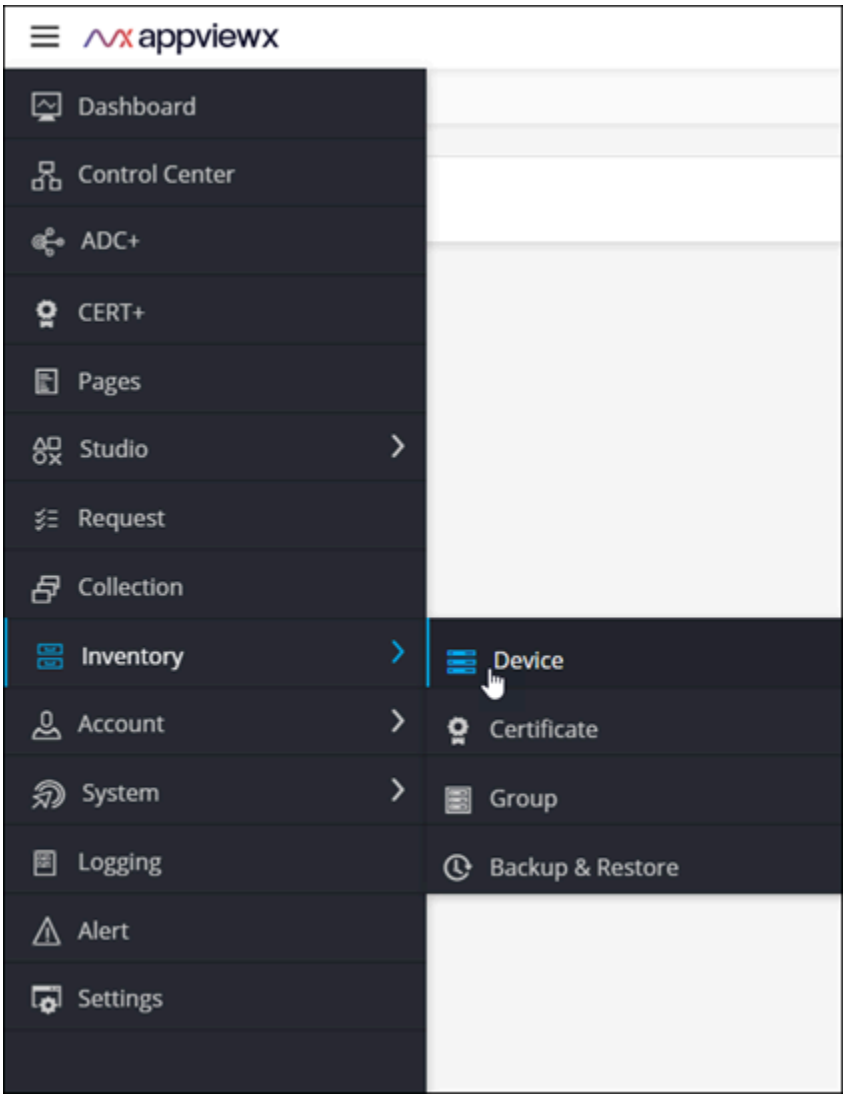
1. Login to the AppViewX server on which the AppViewX Cloud Connector is installed.
2. From the command line interface, navigate to the properties folder. Path:
   {CC_INSTALLATION_PATH}/deps/properties
3. Open the **hsm** file using the following command:

```
vi hsm
```

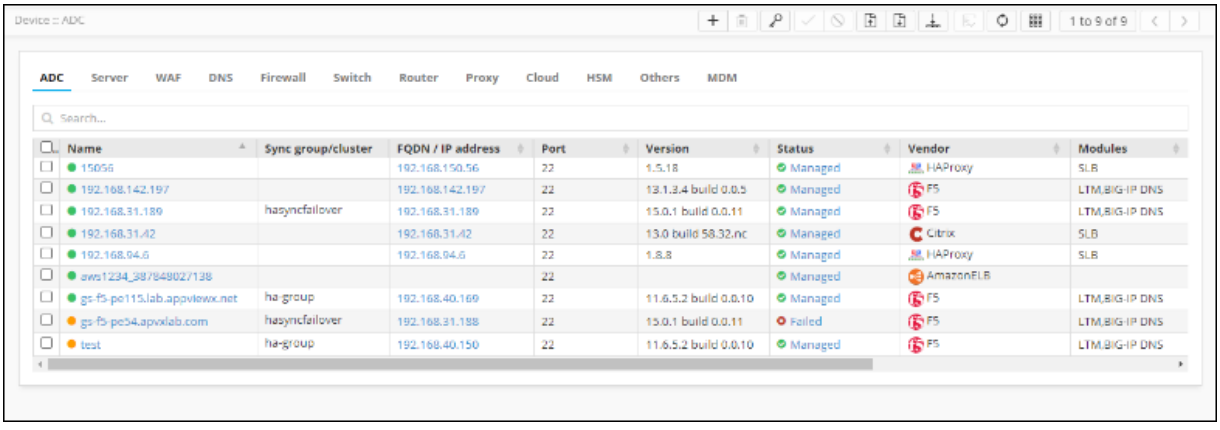
4. Uncomment the following lines:

```
export CS_PKCS11_R2_CFG= /appviewx/dependencies/external_libs/hsm/utimaco/cs_pkcs11_R2.cfg

echo "UTIMACO Config Path : $CS_PKCS11_R2_CFG"
```

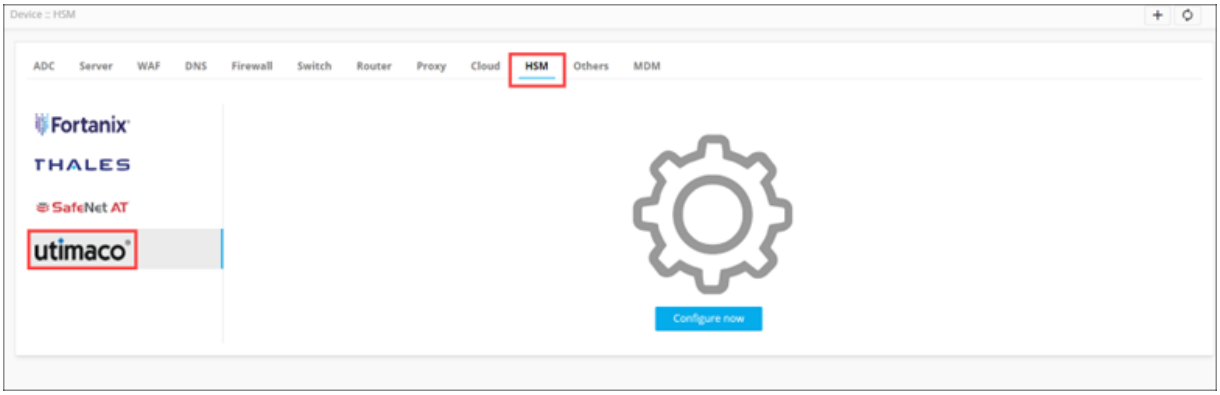
5. Login to the AppViewX UI using valid credentials. B
   The **Dashboard** page is displayed by default.
6. From the top-left corner of the page, click ☰.
7. From the menu displayed, select **Inventory** > **Device**.



The **Device :: ADC** page is displayed.



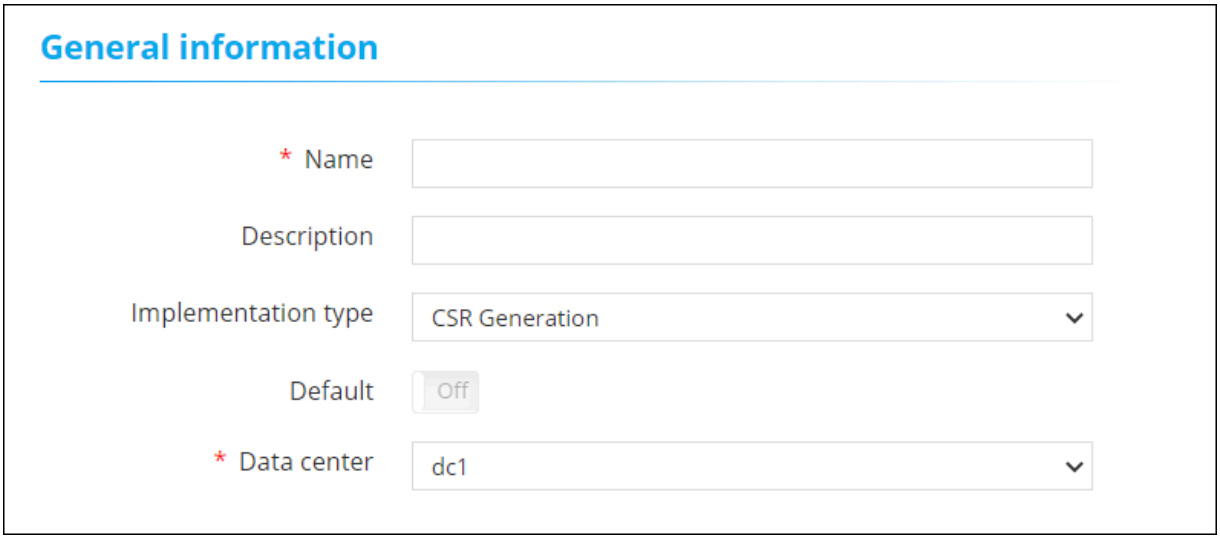
8. Under the **HSM** tab, from the navigation pane on the left, select **Utimaco**.



9. Click **Configure now**.

   The **Device :: HSM** page is updated to display the fields required to integrate Thales-DPoD with the AppViewX CLMaaS.

10. In the **General Information** section, enter/select the required field information.

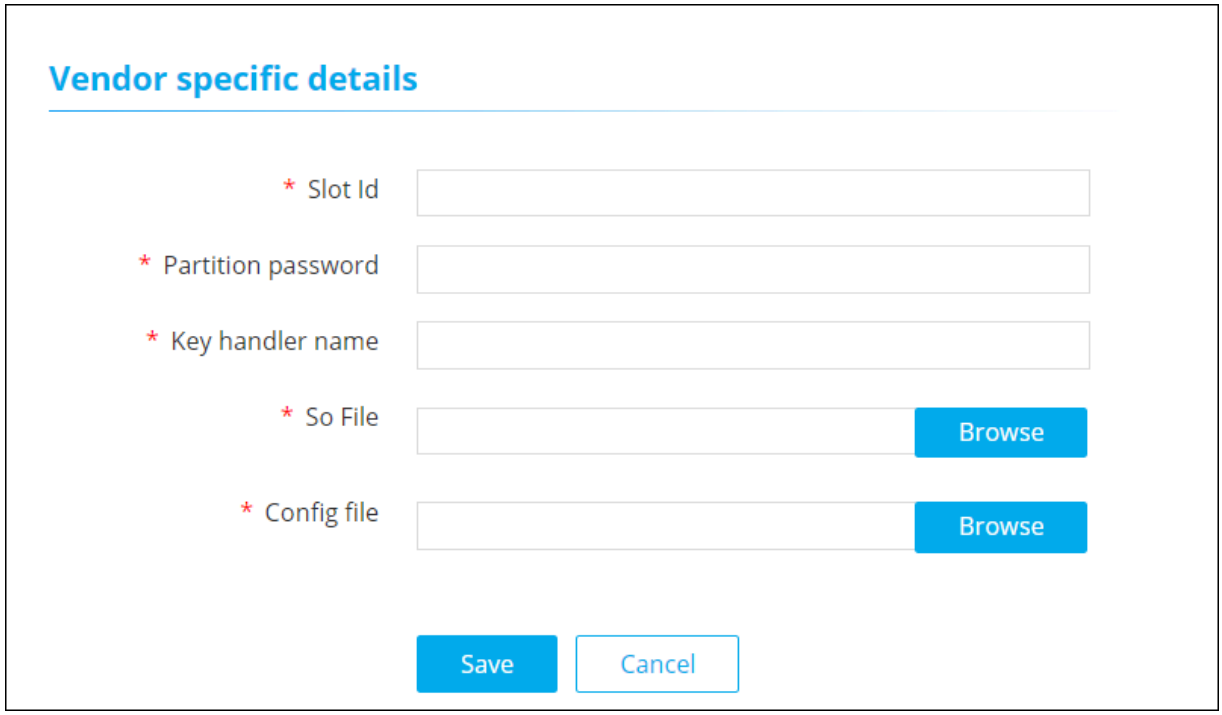


The following table describes the field information in this section:

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:

Field	Description
	• CSR generation • Private key generation • Both
Default	Turn on the toggle to make this the default setting.
***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.
All * marked fields are mandatory.	

11. In the Vendor specific details section, enter/select the required field information.



The following table describes the field information in this section:

Field	Description
***Slot Id**	Unique identification number of the slot in the HSM Luna client that will be used to communicate with the end HSM device.

Field	Description
***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**.
All * marked fields are mandatory.	

12. Click **Save**.
13. Scroll to the end of this page to view the table that will be populated with all the details of this HSM. 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**:
    • Check the installation path for the HSM.
    • Ensure that all required permissions have been enabled.
14. If the implementation type is CSR Generation, refer to the Cert+ User Guide for steps on how to generate a CSR.

Fortanix

To integrate a HSM device from Amazon, enter the following details:

Field	Description
***API Key**	Unique identification number of the slot in the HSM Luna client that will be used to communicate with the end HSM device.
***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.

Field	Description
All * marked fields are mandatory.	

Integrating the Fortanix HSM with the AppViewX

To integrate the Fortanix HSM with the AppViewX:

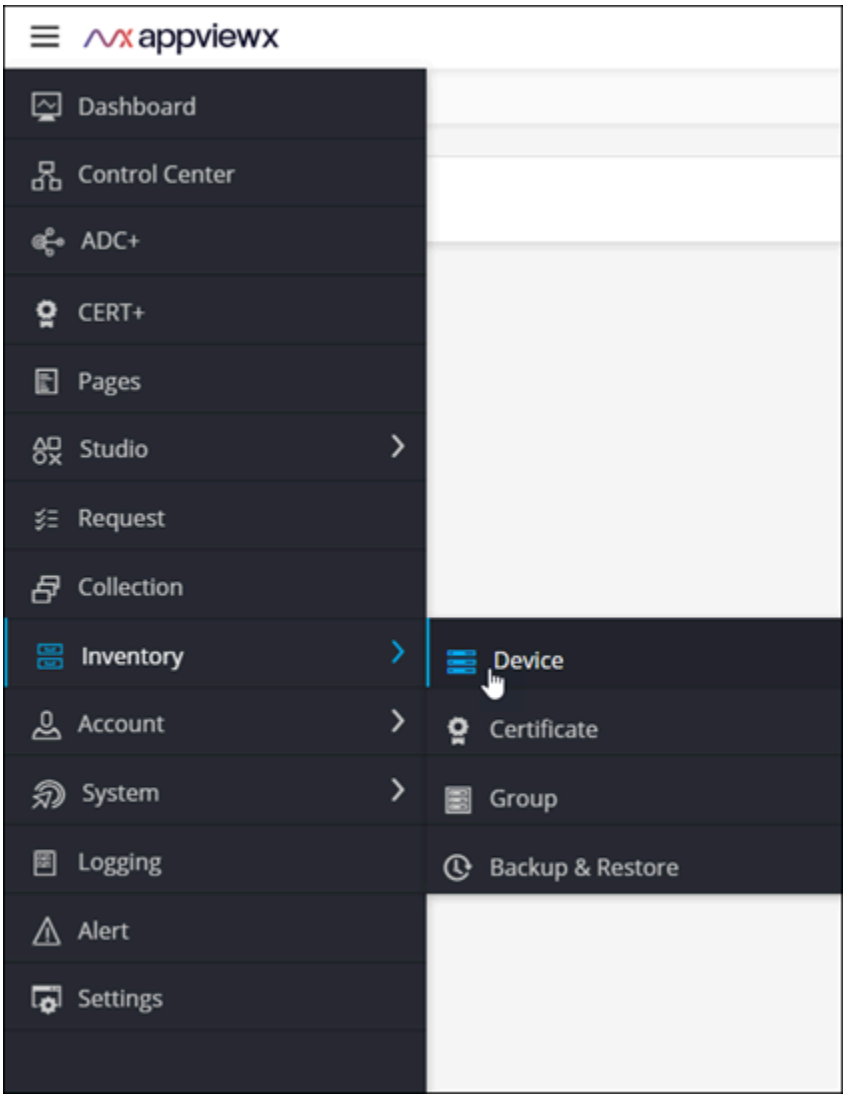
1. Login to the AppViewX server on which the AppViewX Cloud Connector is installed.
2. From the command line interface, navigate to the properties folder. Path:
   {CC_INSTALLATION_PATH}/deps/properties
3. Open the **hsm** file using the following command:

```
vi hsm
```

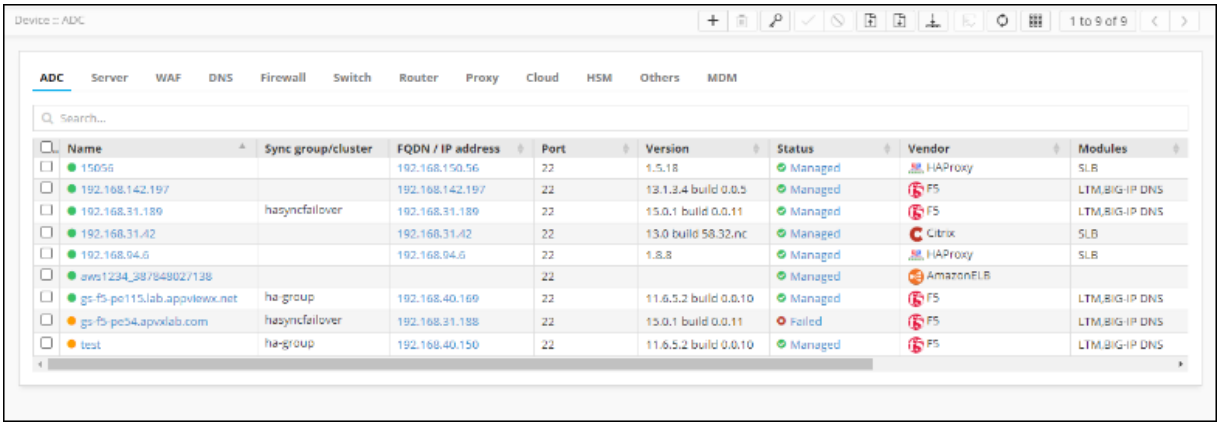
4. Uncomment the following lines:

```
export FORTANIX_PKCS11_CONFIG_PATH= /appviewx/dependencies/hsm/fortanix/pkcs11.conf

echo "FORTANIX Config Path : $FORTANIX_PKCS11_CONFIG_PATH"
```

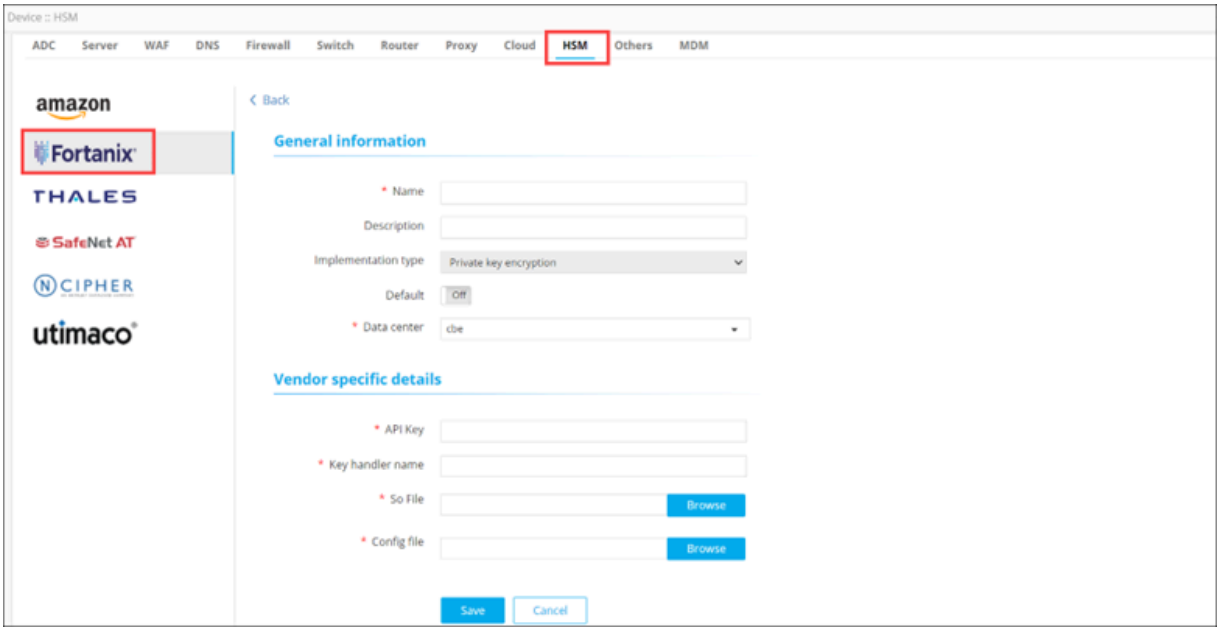
5. Login to the AppViewX UI using valid credentials.
6. From the top left corner of the screen, click ☰
7. From the menu displayed, select **Inventory** > **Device**.



The **Device :: ADC** page is displayed.



8. Under the **HSM** tab, from the navigation pane on the left, select **Fortanix**.



9. Click **Configure now**.

   The **Device :: HSM** page is updated to display the fields required to integrate Thales-DPoD with the AppViewX CLMaaS.

10. In the **General Information** section, enter/select the following details:

Field	Description
***Name**	Enter a name for this integration.
Description	Enter a description for this integration.
Implementation type	Select an implementation type from the options available in the dropdown menu.
Default	Turn on the toggle to make this the default setting.
***Data center**	Select the required data center from the list of applicable values in the dropdown menu.
All * marked fields are mandatory.	

11. In the **Vendor specific details** section, enter/select the following details:

Field	Description
***API Key**	Enter the API key.

Field	Description
***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**.
All * marked fields are mandatory.	

12. Click **Save**.
13. Scroll to the end of this page to view the table that will be populated with all the details of this HSM. 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**:
    - Check the installation path for the HSM.
    - Ensure that all required permissions have been enabled.
14. If the implementation type is CSR Generation, refer to the Cert+ User Guide for steps on how to generate a CSR.

Thales DPoD

In this section, you will be guided to integrate the Thales DPoD HSM with the AppViewX CLMaaS.

- Integrating the Thales DPoD HSM with the AppViewX

Integrating the Thales DPoD HSM with the AppViewX

To integrate the Thales DPoD HSM with the AppViewX CLMaaS:

1. Login to the AppViewX server on which the AppViewX 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. In the **hsm** file, uncomment the following lines:

```
cd /appviewx/dependencies/external_libs/hsm/safenet/dpod/

source setenv

export ChrystokiConfigurationPath=/appviewx/dependencies/hsm/safenet/dpod/
```

> **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. Navigate to the hsm folder. Path: **{installation_path}/deps/external_libs/hsm/**
6. Install the Luna client in this location.

> **Note:** If the Luna client is already installed location, you will have to uninstall and reinstall the Luna client at the location: {appviewx_installation_path}/hsm/.

7. Untar the **DPoD** tar file.
8. After successful installation, copy the **Chrystoki.conf** file to the location cp /etc/Chrystoki.conf {CC_INSTALLATION_PATH}/deps/external_libs/hsm/.
9. Edit the **Chrystoki.conf** file to replace the custom path with the above new mount path.
10. For version 7.2, enable the folder permissions using the command given below:

```
"cd  {appviewx_installation_path}/hsm/safenet/lunaclient"

"sudo find . -type d -exec chmod +rx {} \;"
```

11. Update the permissions for the **Chrystoki.conf** file using the command given below:

```
SaaS : " cd {appviewx_installation_path}/hsm/"

"sudo chmod 755 Chrystoki.conf"
```

AppViewX can now communicate with all HSM devices.

12. Restart the avx-platform-hsm pod, using the following commands:

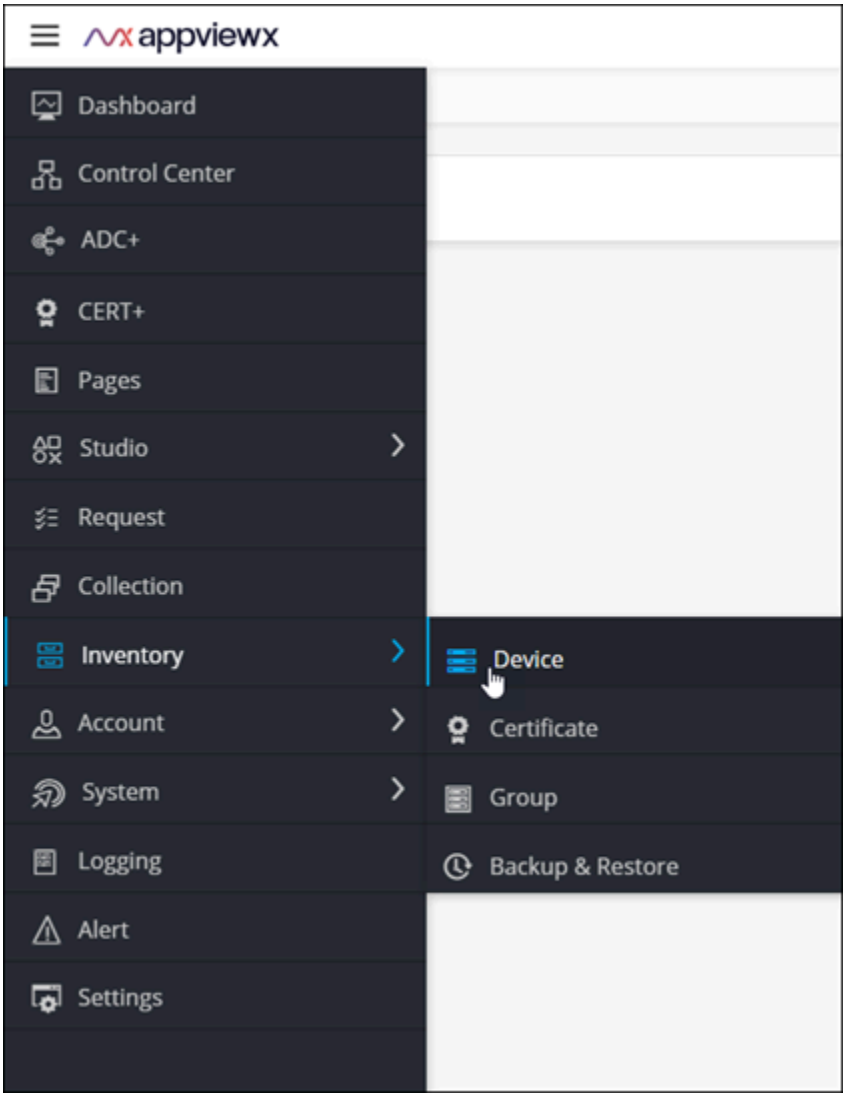
```
list kubectl get pods -n <namespace>

kubectl delete pods -n <namespace> <PodName>
```

13. Login to the AppViewX UI using valid credentials.

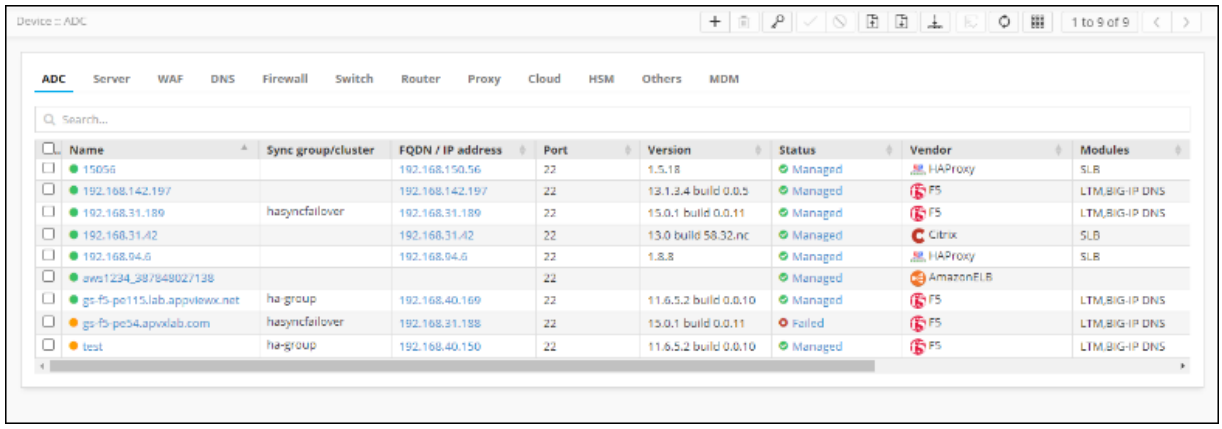
The **Dashboard** page is displayed by default.

14.

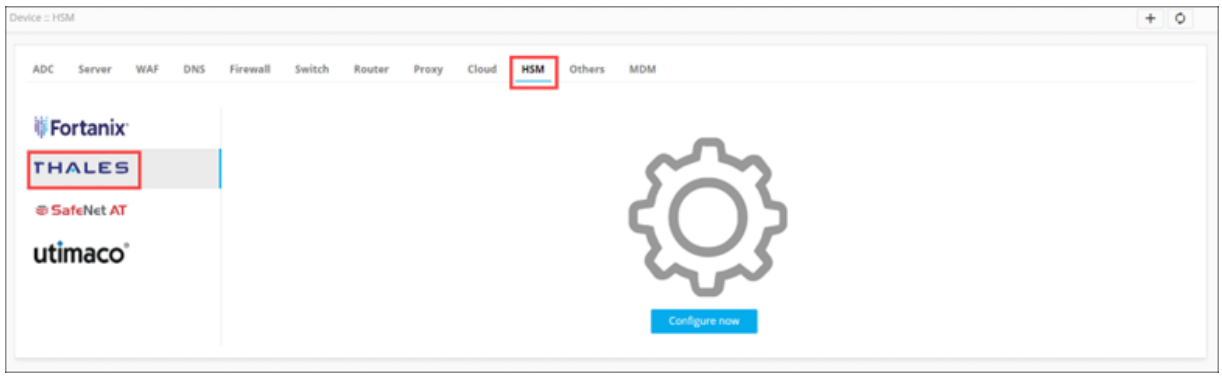
15. From the menu displayed, select **Inventory** > **Device**.



The **Device :: ADC** page is displayed.



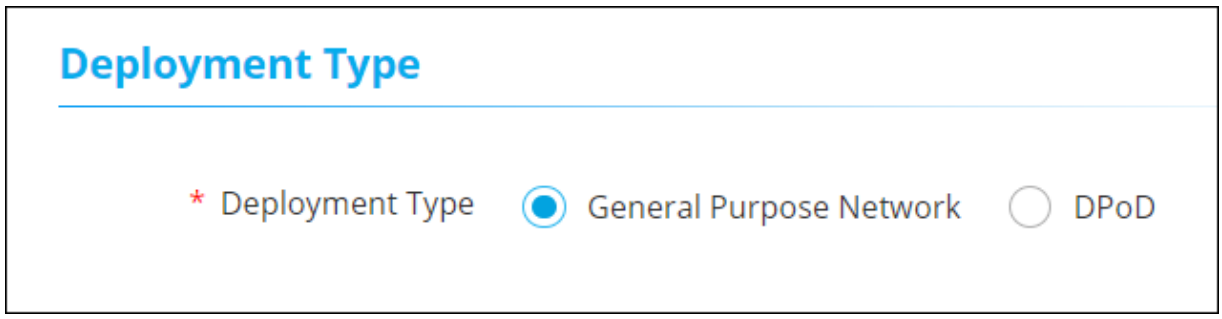
16. Under the **HSM** tab, from the navigation pane on the left, select **Thales**.



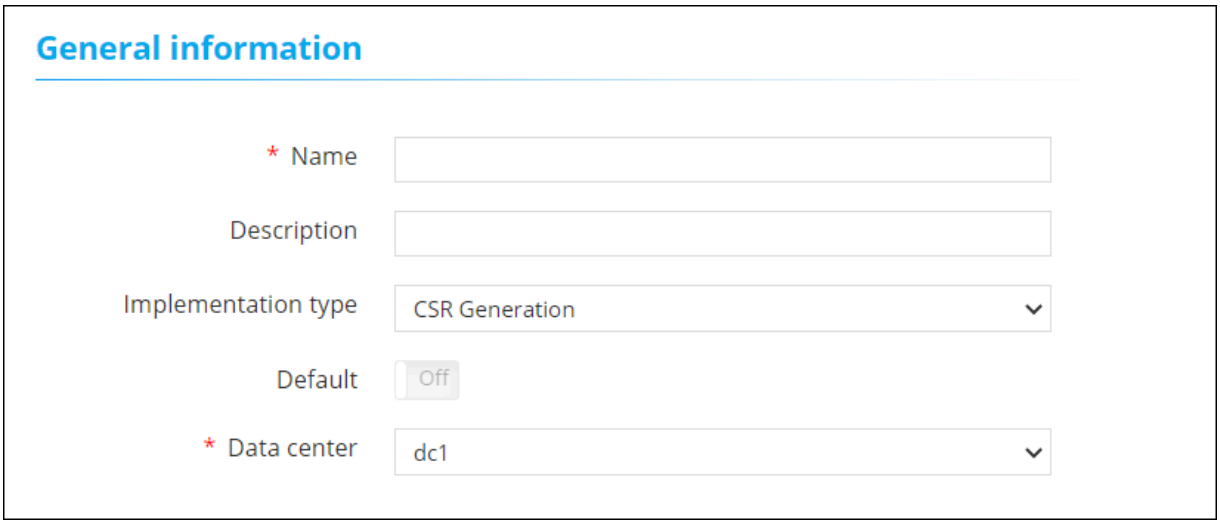
17. Click **Configure now**.

    The **Device :: HSM** page is updated to display the fields required to integrate Thales-DPoD with the AppViewX CLMaaS.

18. In the **Deployment Type** section, for the **Deployment Type** field, select **General Purpose Network**.



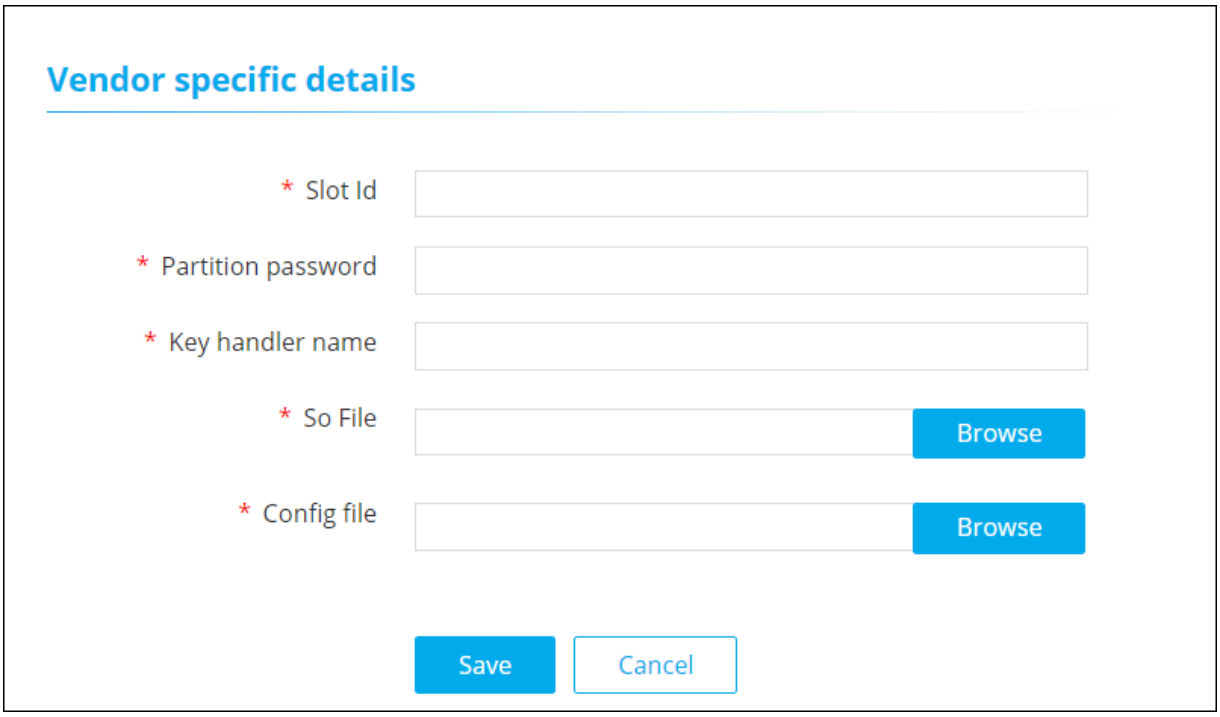
19. In the **General Information** section, enter/select the required field information.



The following table describes the field information in this section:

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 • Private key generation • Both
Default	Turn on the toggle to make this the default setting.
***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.
All * marked fields are mandatory.	

20. In the **Vendor specific details** section, enter/select the required field information.



The following table describes the field information in this section:

Field	Description
***Slot Id**	Unique identification number of the slot in the HSM Luna client that 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:

Field	Description
	a. Click **Browse**. b. Navigate to the location of the .conf file. c. Select the .conf file and click **Open**.
All * marked fields are mandatory.	

21. Click **Save**.
22. Scroll to the end of this page to view the table that will be populated with all the details of this HSM. 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**:
    - Check the installation path for the HSM.
    - Ensure that all required permissions have been enabled.
23. If the implementation type is CSR Generation, refer to the Cert+ User Guide for steps on how to generate a CSR.

Thales GPN

In this section, you will be guided to integrate the Thales GPN HSM with the AppViewX CLMaaS.

- Installing the Luna Client
- Integrating the Thales GPN HSM with the AppViewX

Installing the Luna Client

In order to communicate with the HSM in the customers' premises, install the Luna client on the node where the AppViewX Cloud Connector is installed.

Prerequisites

- The Alien and RPM packages should be installed in the environment.
- Users should have either root access or sudo access.
- Environment should have access to communicate with HSM through the ports 22, 1792.

Integrating the Thales GPN HSM with the AppViewX

1. Login to the AppViewX server on which the AppViewX 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. In the hsm file, 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. Navigate to the hsm folder. Path: `{APPVIEWX_INSTALLATION_PATH}/hsm/`
6. Install the Luna client in this location.

   Note: If the Luna client is already installed location, you will have to uninstall and reinstall the Luna client at the location: `{AppViewX_installed_path)_deps/external_lib/hsm/`

7. After successful installation, copy the **Chrystoki.conf** file to the location `cp /etc/Chrystoki.conf {CC_INSTALLATION_PATH}/deps/external_libs/hsm/`.
8. Edit the **Chrystoki.conf** file to replace the custom path with the above new mount path.
9. For version 7.2, enable the folder permissions using the command given below:

   ```
   "cd  {AppViewX_INSTALLATION_PATH}/hsm/safenet/lunaclient"

   "sudo find . -type d -exec chmod +rx {} \;"
   ```

10. Update the permissions for the **Chrystoki.conf** file using the command given below:

    ```
    SaaS : " cd {AppViewX_INSTALLATION_PATH}/hsm/"

    "sudo chmod 755 Chrystoki.conf"
    ```

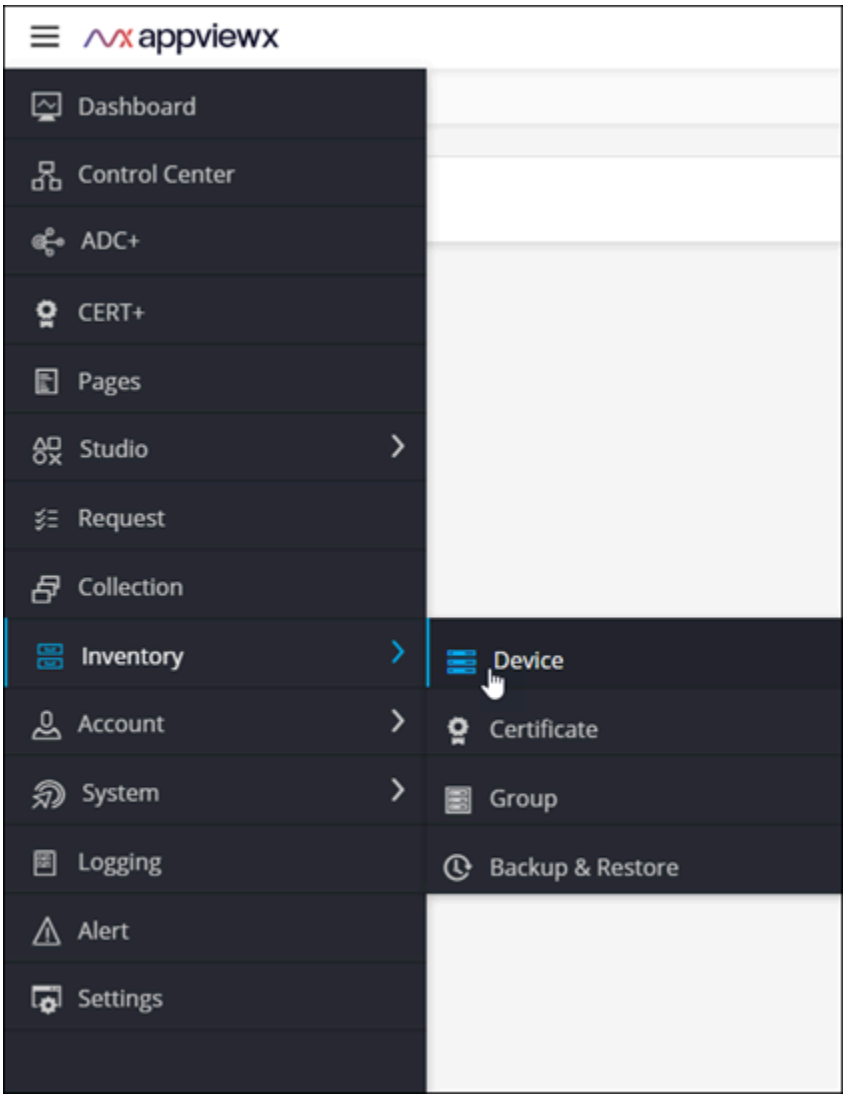
    AppViewX can now communicate with all HSM devices.

11. Restart the avx-midserver-platform pod, using the following commands:

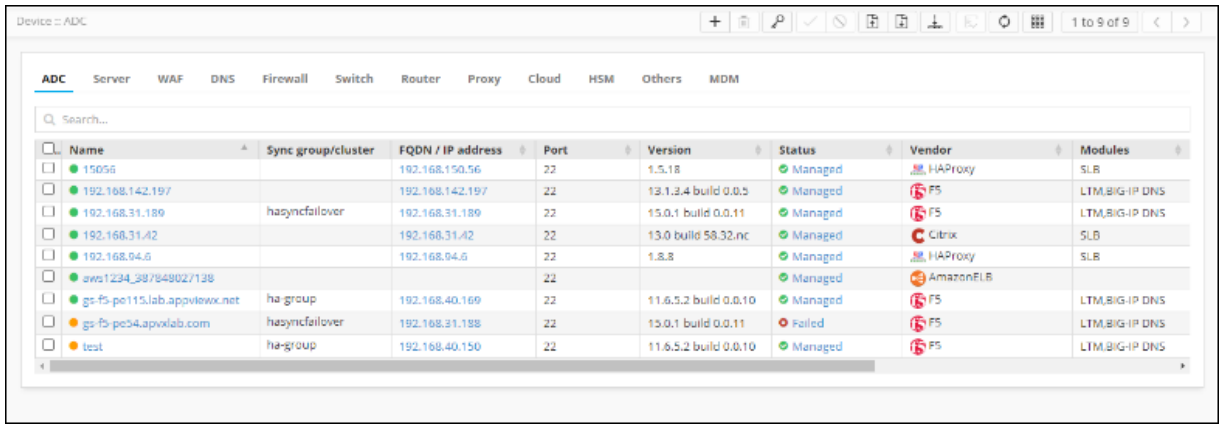
    ```
    list kubectl get pods -n <namespace>

    kubectl delete pods -n <namespace> <PodName>
    ```

12. Login to the AppViewX UI using valid credentials.
    The **Dashboard** page is displayed by default.

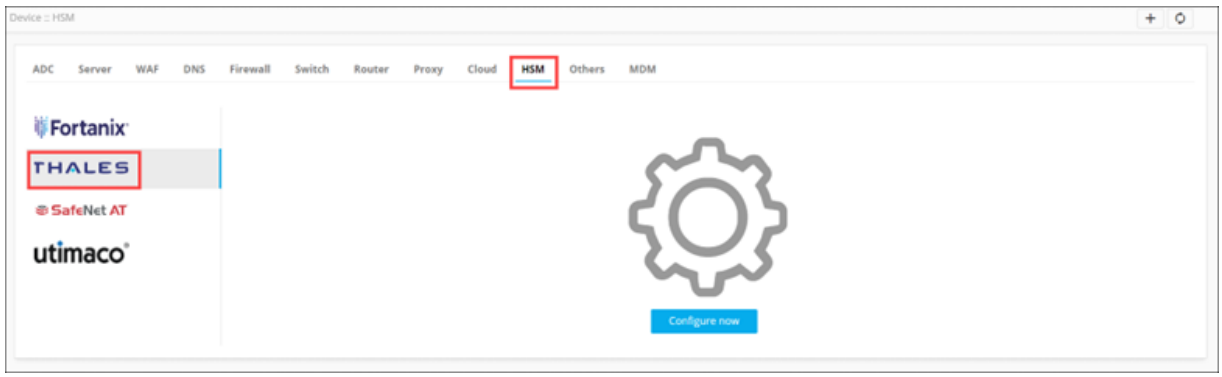
13. From the top-left corner of the page, click ☰.
14. From the menu displayed, select **Inventory** > **Device**.



The **Device :: ADC** page is displayed.



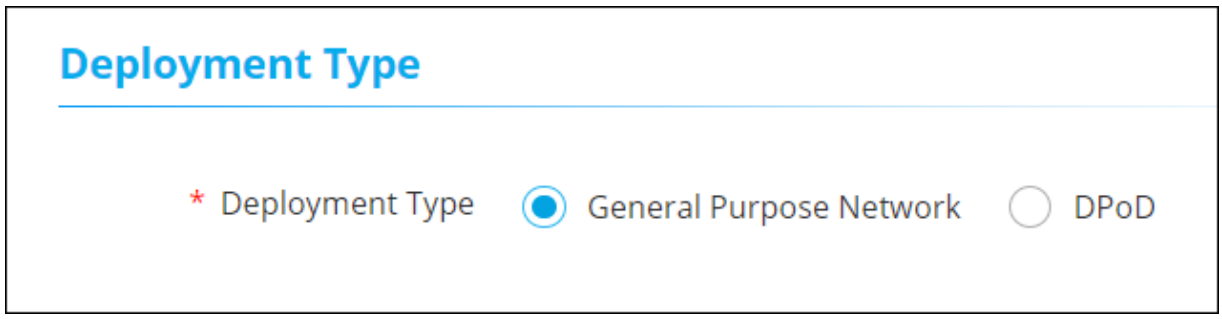
15. Under the **HSM** tab, from the navigation pane on the left, select **Thales**.



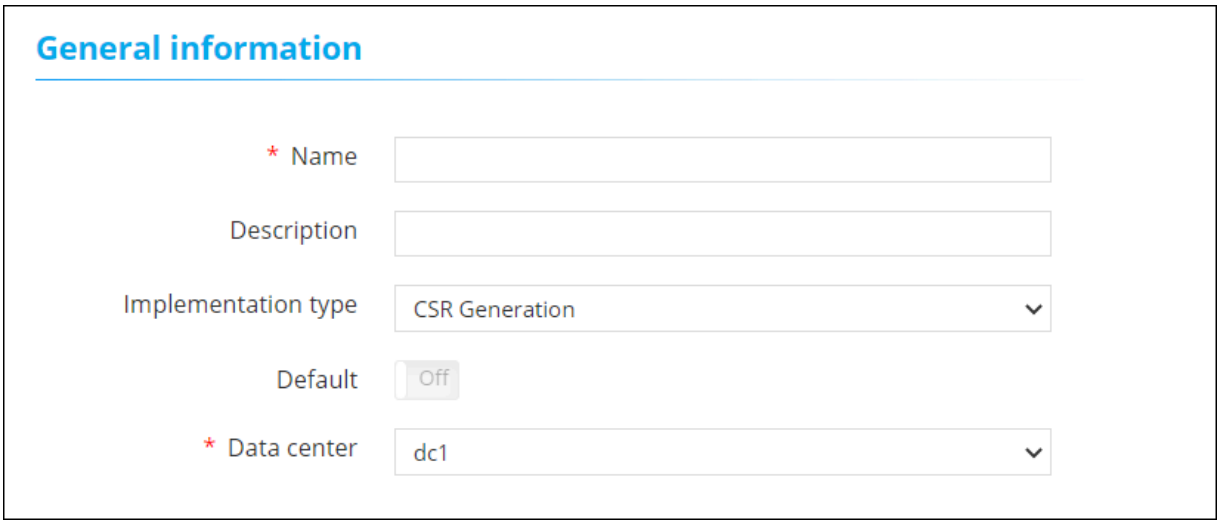
16. Click **Configure now**.

    The **Device :: HSM** page is updated to display the fields required to integrate Thales-DPoD with the AppViewX CLMaaS.

17. In the **Deployment Type** section, for the **Deployment Type** field, select **General Purpose Network**.



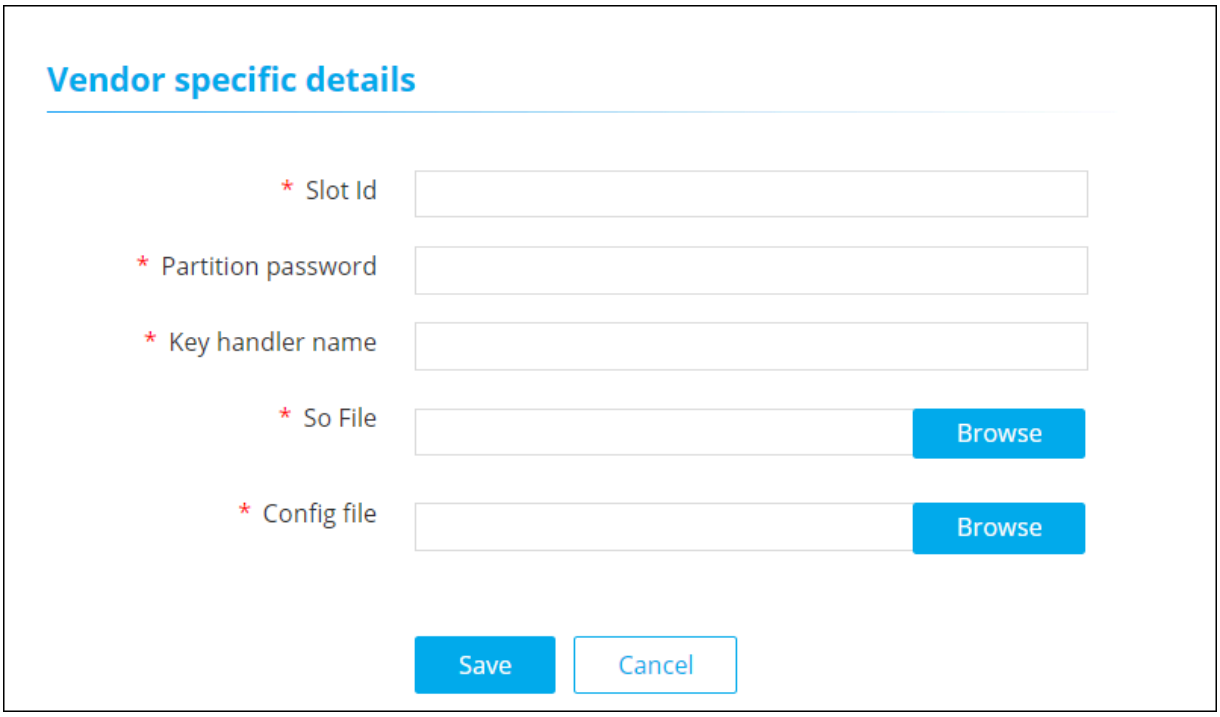
18. In the **General Information** section, enter/select the required field information.



The following table describes the field information in this section:

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 • Private key generation • Both
Default	Turn on the toggle to make this the default setting.
***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.
All * marked fields are mandatory.	

19. In the Vendor specific details section, enter/select the required field information.



The following table describes the field information in this section:

Field	Description
***Slot Id**	Unique identification number of the slot in the HSM Luna client that 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
All * marked fields are mandatory.	

20. Click **Save**.
21. Scroll to the end of this page to view the table that will be populated with all the details of this HSM. 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**:
    • Check the installation path for the HSM.
    • Ensure that all required permissions have been enabled.
22. If the implementation type is CSR Generation, refer to the Cert+ User Guide for steps on how to generate a CSR.

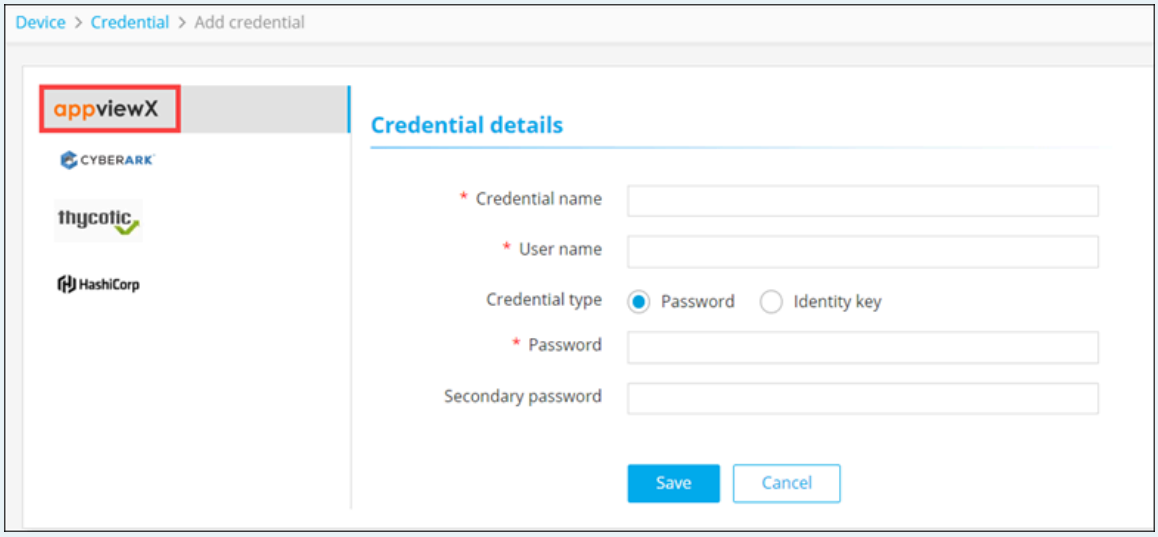
Chapter 6: Configuring Privileged Access Management

- AppViewX
- CyberArk
- Thycotic Secret
- HashiCorp

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.

Note: For more details on how the HashiCorp vault integrates with AppViewX, click here.



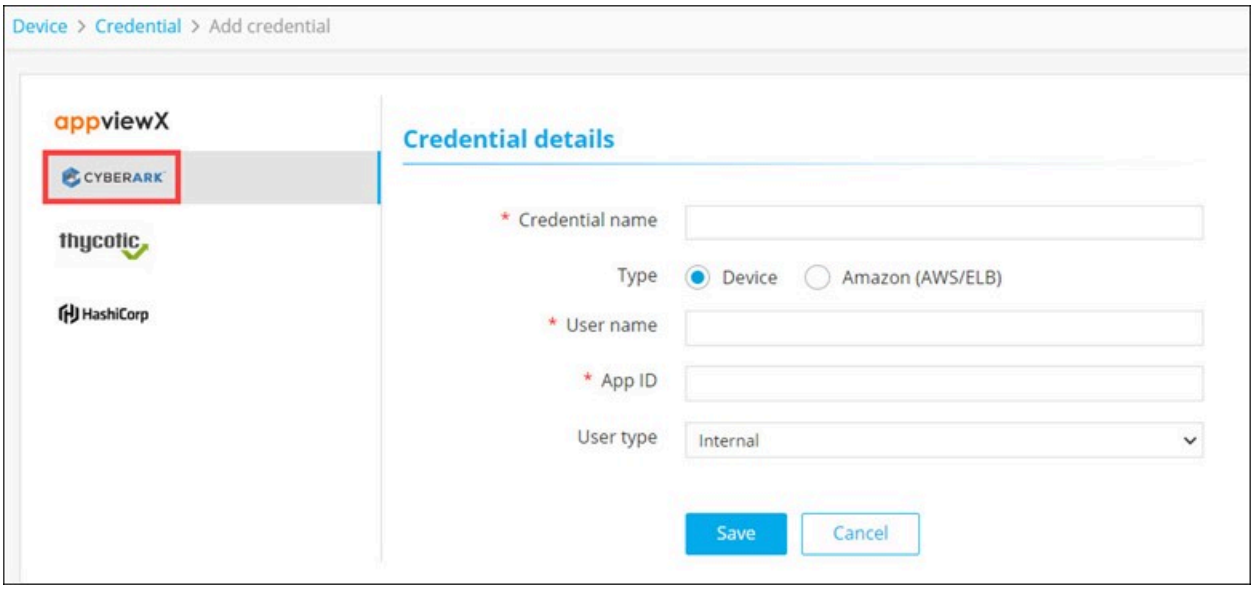
To configure credential details for the AppViewX vault:

1. In the **Credential details** section, enter the following field information:

Field	Description
***Credential name**	Name for the credential for the users to identify it.
***User name**	User name used for device onboarding.

Field	Description
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 (private key in the **.pem** or **.txt** format) 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**.
All * marked fields are mandatory.	

2. Click **Save**.



To configure credential details for the CyberArk vault:

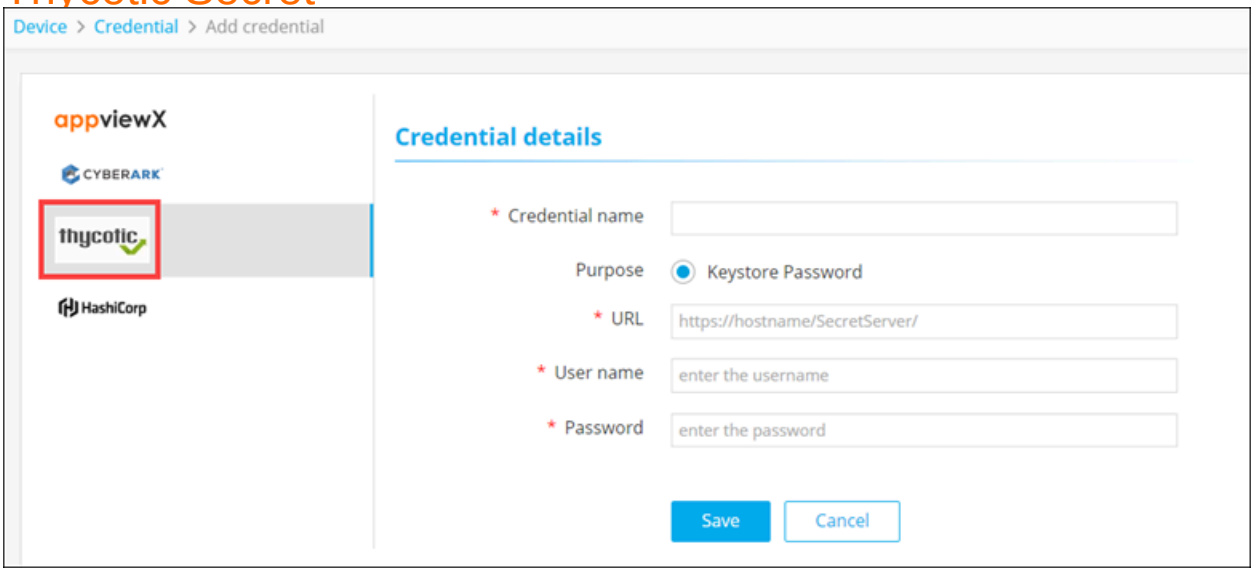
1. In the **Credential details** section, enter the following field information:

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

Field	Description
	• Internal (user created directly in the device) • External (user created in the Active Directory) **Note:** This field is displayed when the **Amazon** (AWS/ELB) type is selected.
***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.
All * marked fields are mandatory.	

2. Click **Save**.

Thycotic Secret



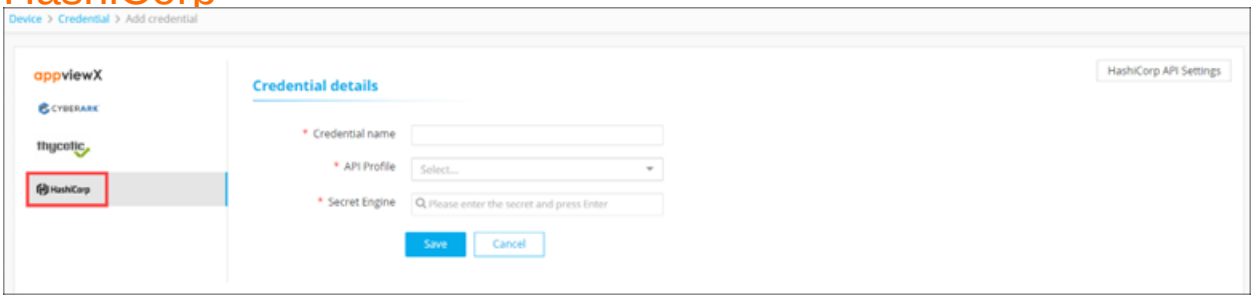
To configure credential details for the Thycotic vault:

1. In the **Credential details** section, enter the following field information:

Field	Description
***Credential name**	Unique name for the credential for the users to identify it
Purpose	
***URL**	URL of the Thycotic Secret server.
***User name**	Username for accessing the Thycotic Secret server.
Password	Password for accessing the Thycotic Secret server.
All * marked fields are mandatory.	

2. Click **Save**.

HashiCorp



To configure credential details for the HashiCorp vault:

1. In the **Credential details** section, enter the following field information:

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 setting
***Secret Engine**	Type path and click enter. It will suggest a list of secrets and the desired secret can be se

Field	Description
All * marked fields are mandatory.	

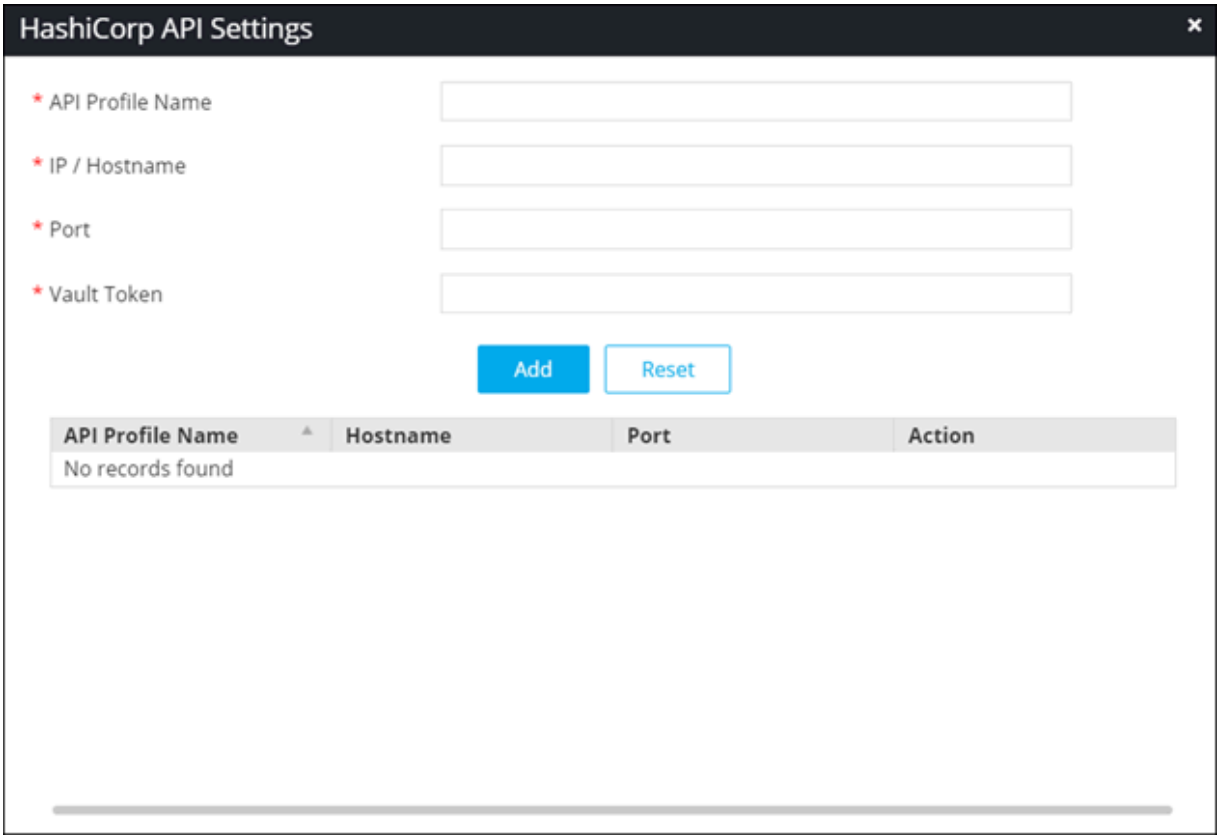
2. Click **Save**.

• Configuring HashiCorp API Settings

Configuring HashiCorp API Settings

1. From the top right corner of the screen, click **HashiCorp API Settings**.

   The **HashiCorp API Settings** window is displayed.



   The following table describes the field information required here:

Field	Description
API Profile Name*	Enter a unique API profile name.
IP/Hostname	Enter the HashiCorp vault hosted IP address or hostname.

Field	Description
Port	Enter the port in which the HashiCorp vault is running.
Vault Token	Enter the vault token for authentication.
All * marked fields are mandatory.	

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

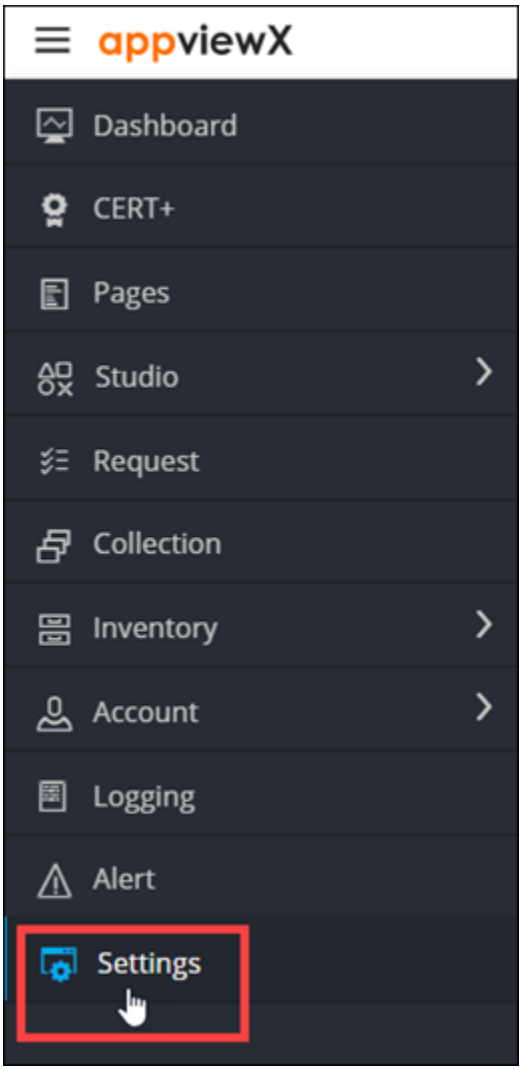
Chapter 7: Configuring General Settings

Configuring the SMTP Server Settings

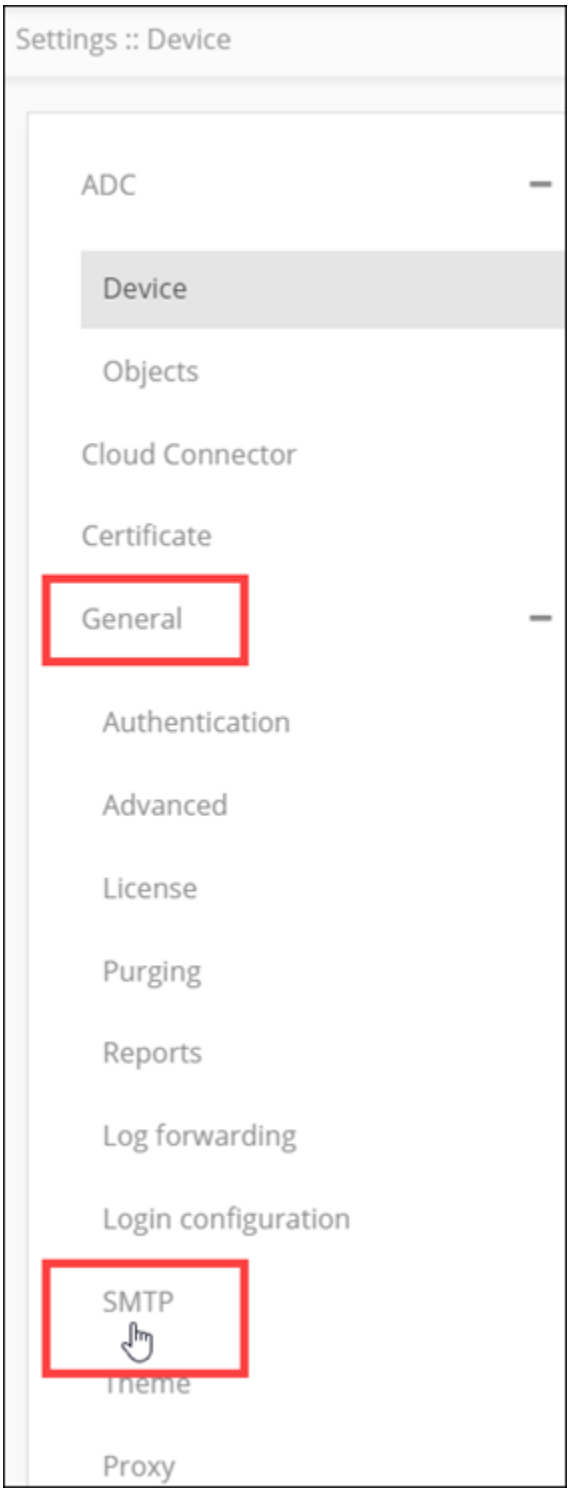
The SMTP configuration is required for AppViewX to be able to send logs and alerts via email.

To configure the SMTP server:

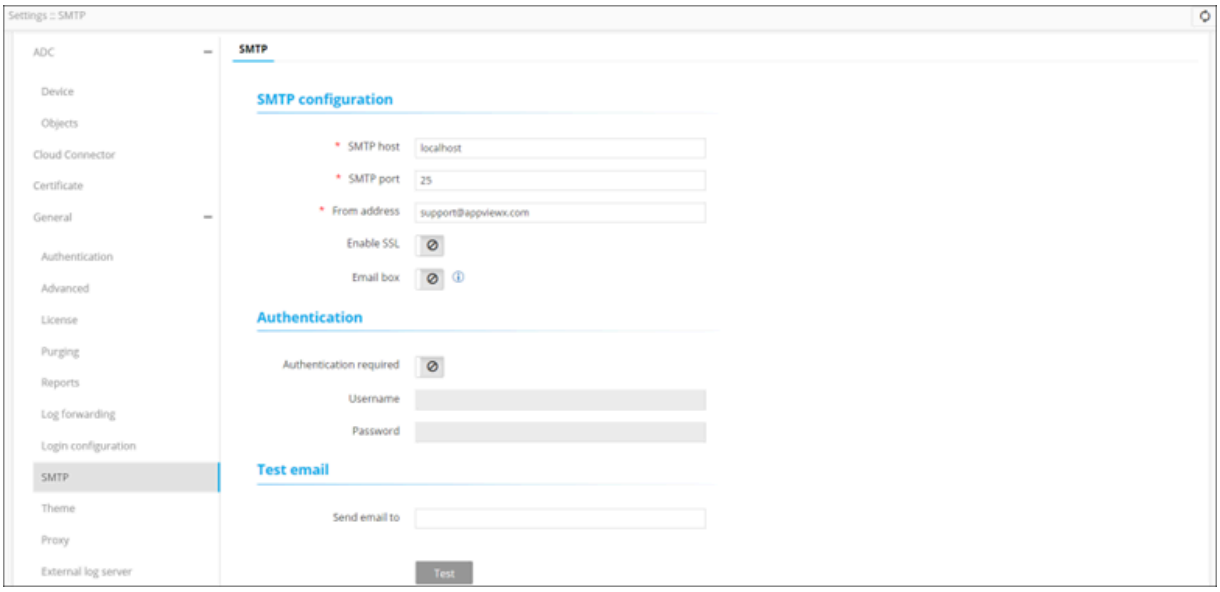
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **SMTP**.



The **Settings :: SMTP** page is displayed.



5. In the **SMTP configuration** section, enter the following details:

Field	Description
***SMTP host**	Host name of the SMTP server.
***SMTP port**	Port number of the SMTP server.
***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.
Email box	To use the mailbox feature to read emails in Visual Workflow, turn on this toggle.
***Email**	**Note:** This field is displayed only if the Email box key is enabled.
***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.

Field	Description
All * marked fields are mandatory.	

6. In the **Authentication** section, enter the following details:

Field	Description
Authentication required	To enable authenticated mail server communication, turn on this toggle.
***Username**	Username for the authenticated mail server. **Note:** This field is enabled only if the Authentication required key is turned on.
***Password**	Password for the authenticated mail server. **Note:** This field is enabled only if the Authentication required key is turned on.
All * marked fields are mandatory.	

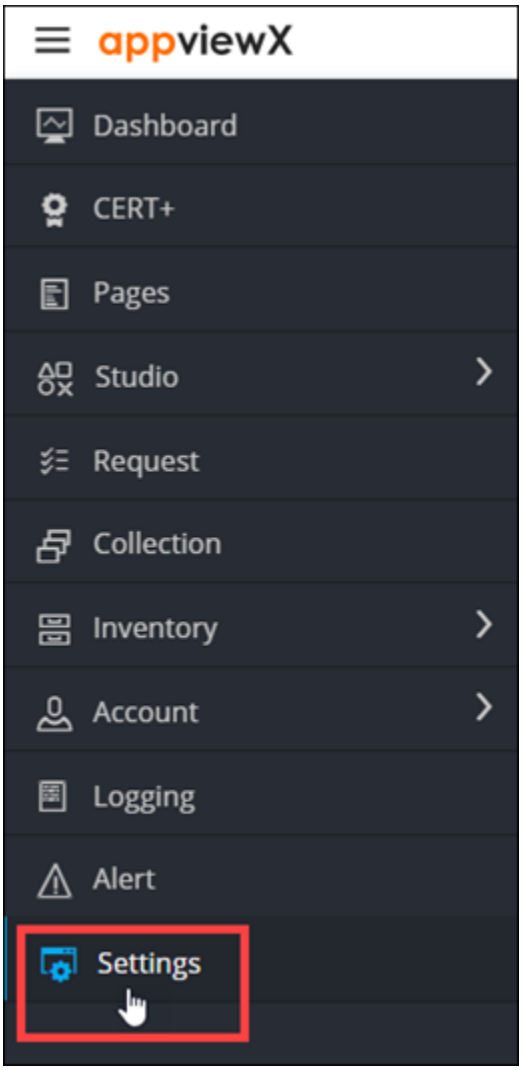
7. In the **Test email** section, to test the SMTP settings,enter the email address to which a test email should be sent.
8. Click **Test** to send the test email.
9. To save the SMTP configuration settings, click **Save**.

Managing Proxy Settings

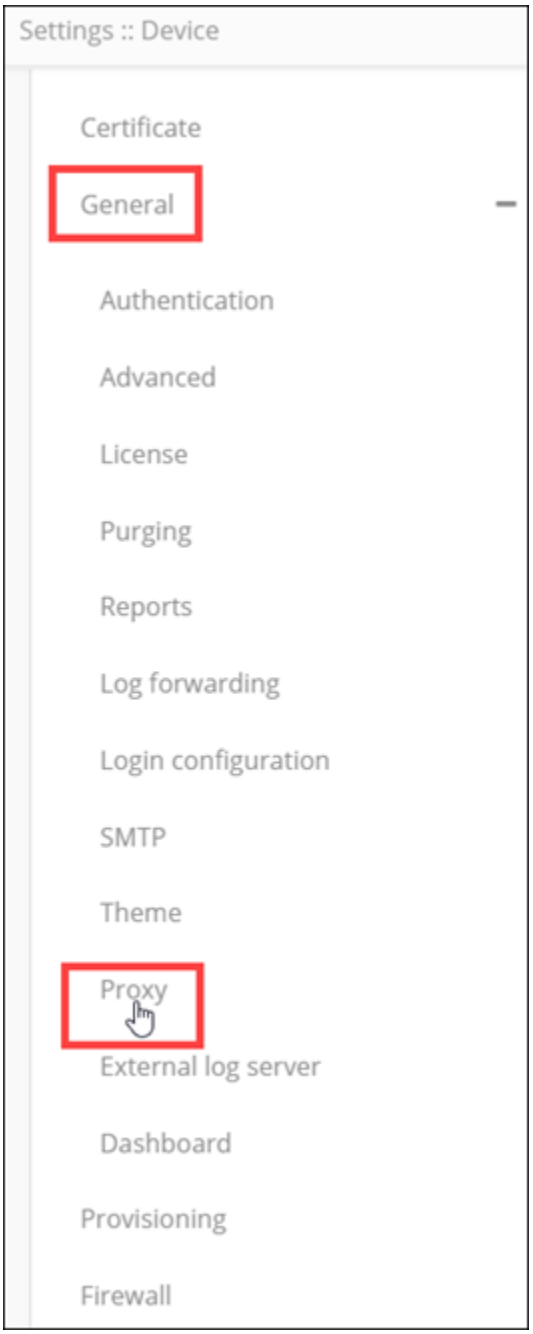
When AppViewX is deployed at a customer's, in order to prevent exposure of the customer's IP address to the internet, AppViewX communicates with the internet using a proxy server.

To configure the proxy settings:

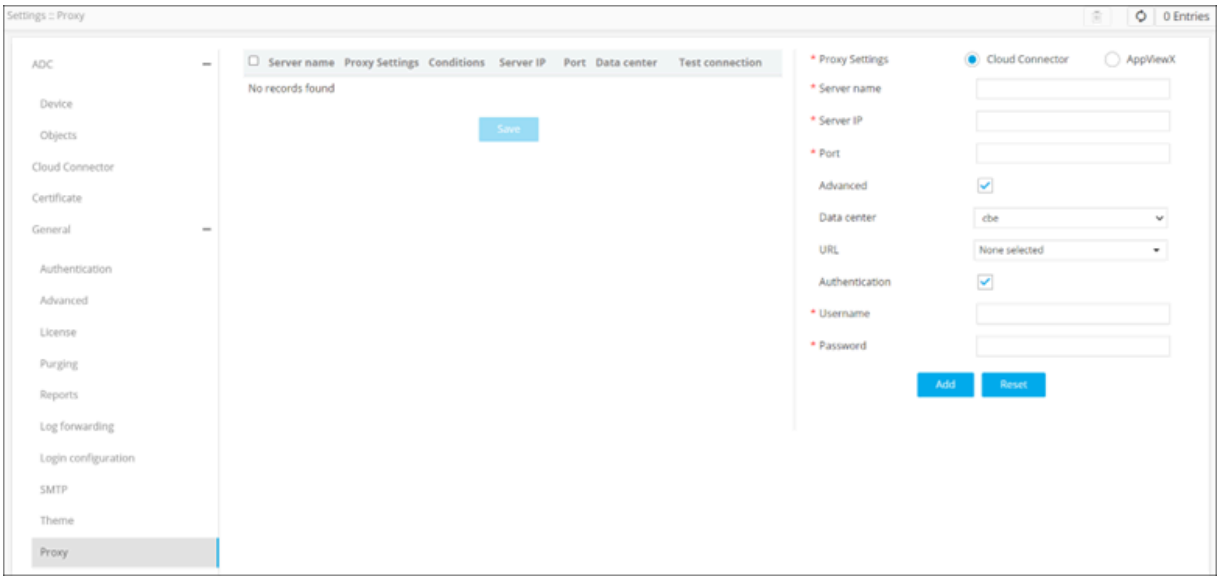
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Proxy**.



The **Settings :: Proxy** page is displayed.

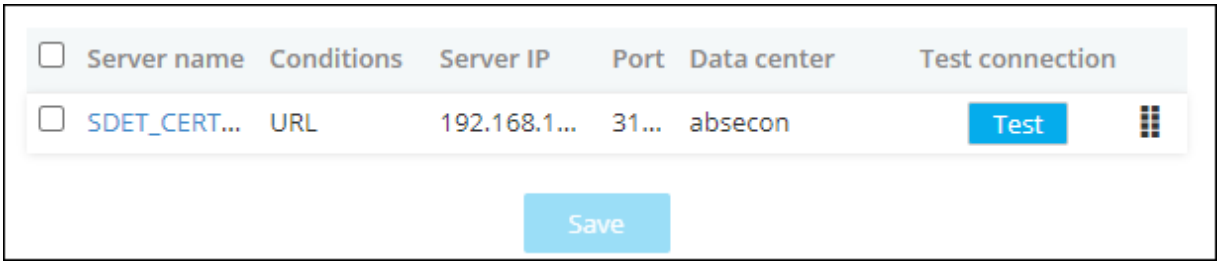


5. Enter the following details:

Field	Description
***Proxy Settings**	Select the Proxy settings from the following options: • Cloud Connector • AppViewx
***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. **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.

Field	Description
	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.
All * marked fields are mandatory.	

6. To save the proxy settings configured above, click **Add**.
   The settings are saved and displayed in the table shown in the left half of the screen.



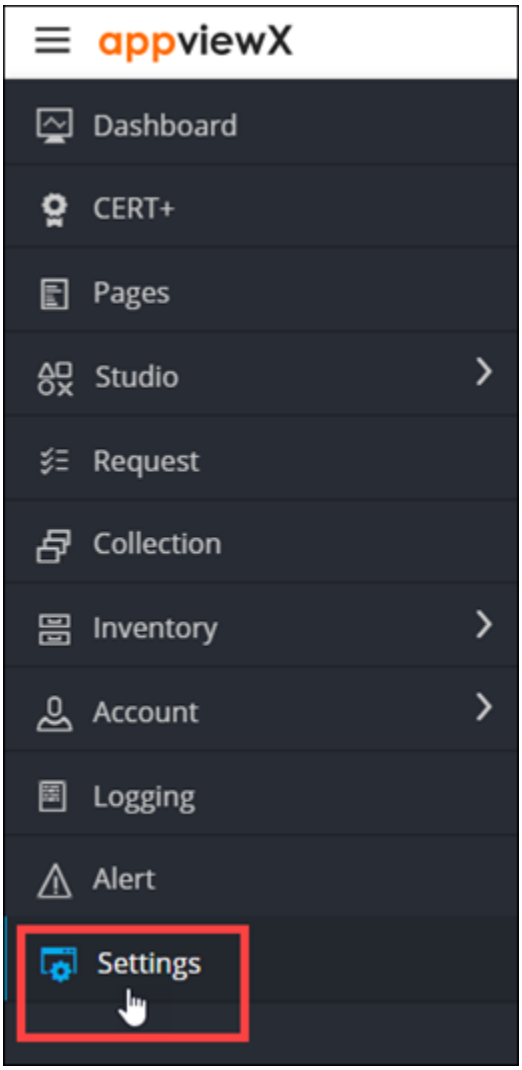
7. To reconfigure the proxy settings, click **Reset**.

Setting the Cryptographic Policy

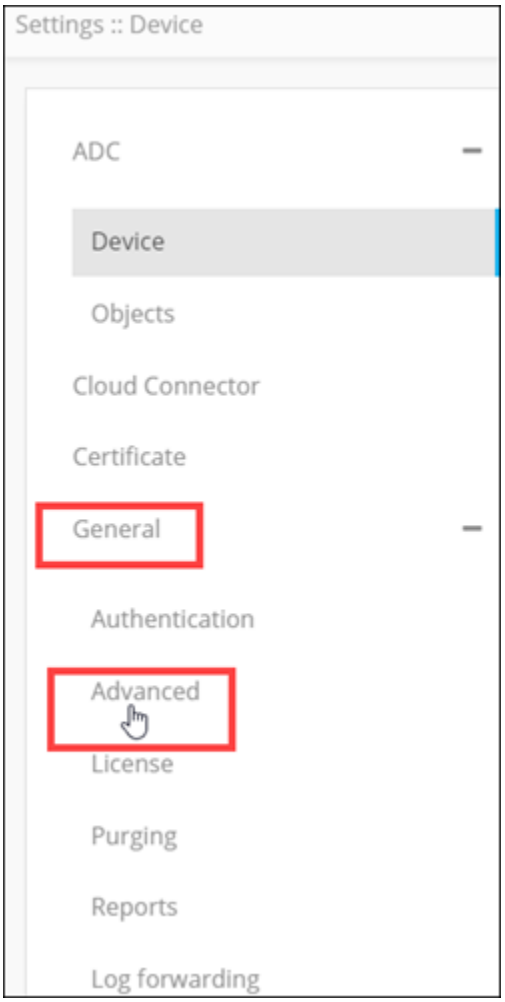
AppViewX enforces a SFTP-based cryptographic policy for protection of sensitive data. Ciphers are used for performing any file operations within AppViewX's functionality and to communicate with devices added in AppViewX.

To set the cryptographic policy:

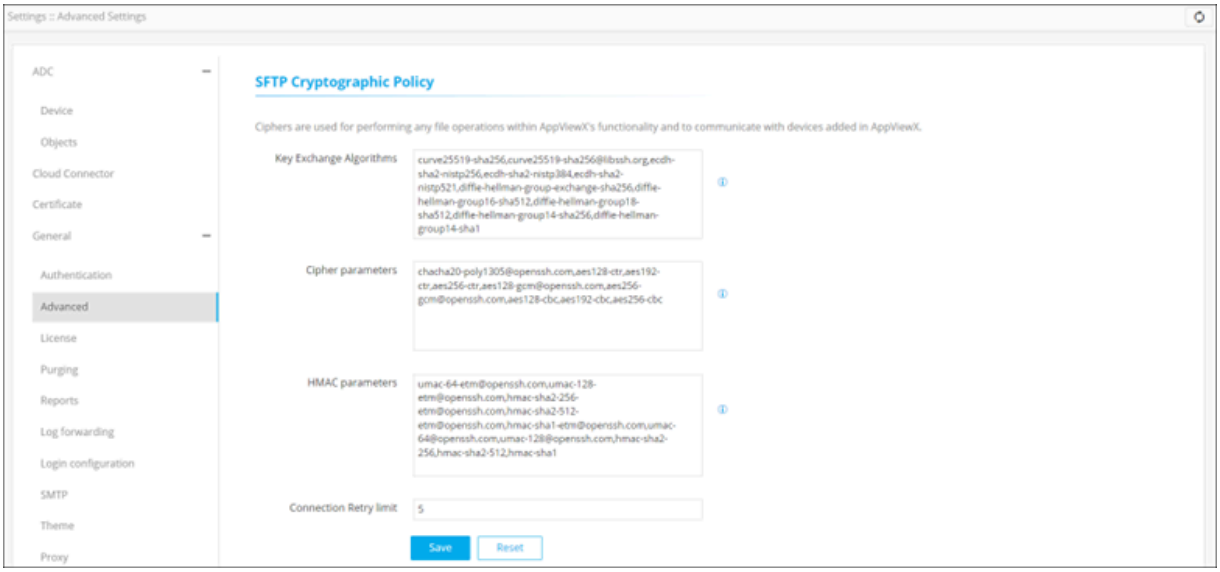
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Advanced**.



The **Settings :: Advanced Settings** page is displayed.



5. In the **SFTP Cryptographic Policy** section, enter the following details:

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.

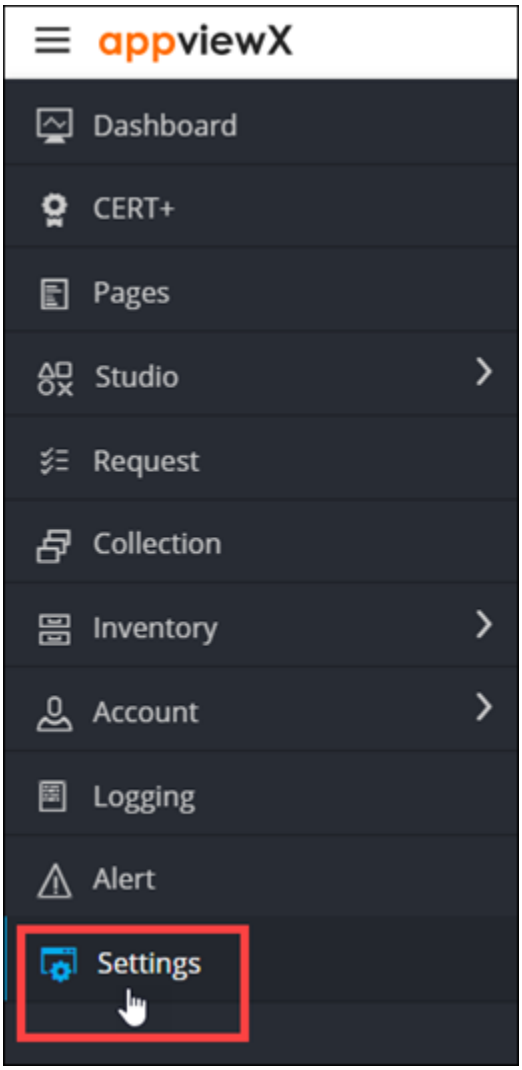
6. Click **Save**.

Enabling Dashboard View for the User

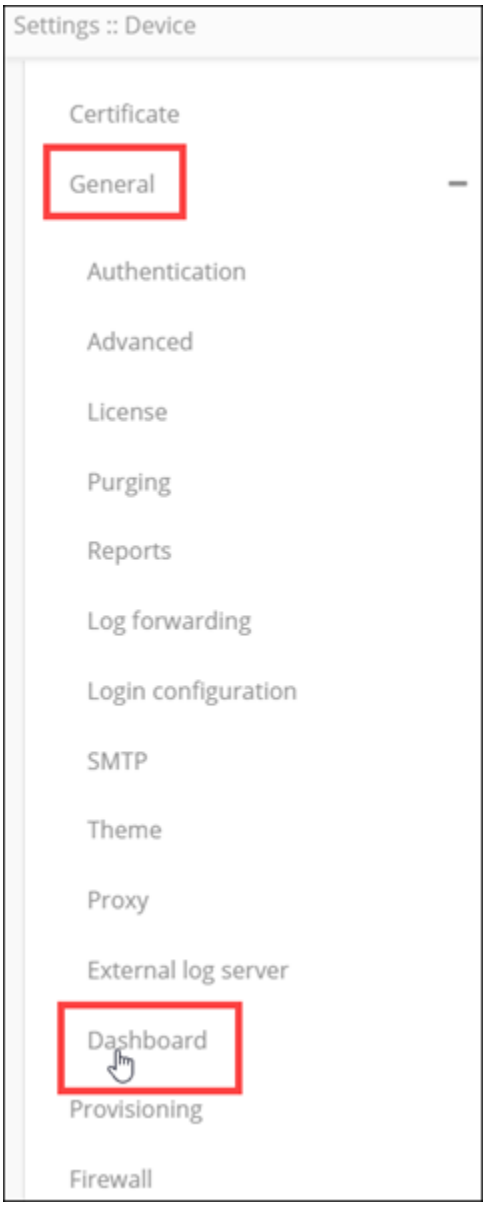
To prevent loss of control over organizational data in the event that a resource leaves the organization, AppViewX lets the admin user have default access to all user dashboard, private as well as public.

To enable default admin access to all dashboards:

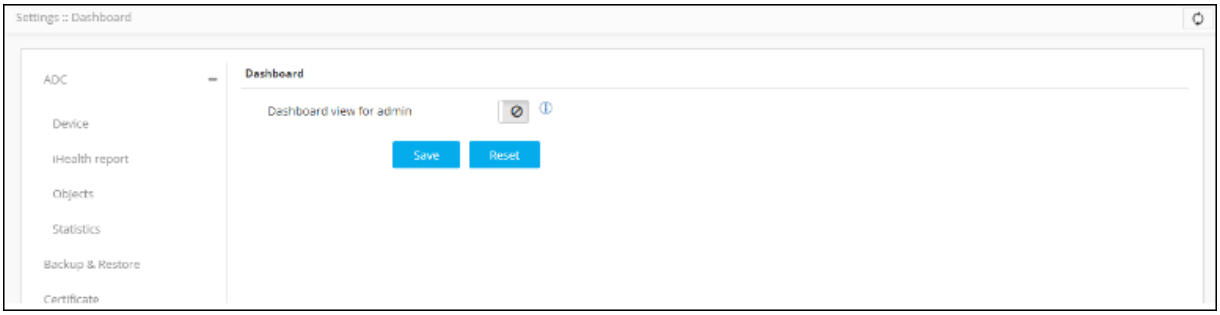
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Dashboard**.



The **Settings :: Dashboard** page is displayed.



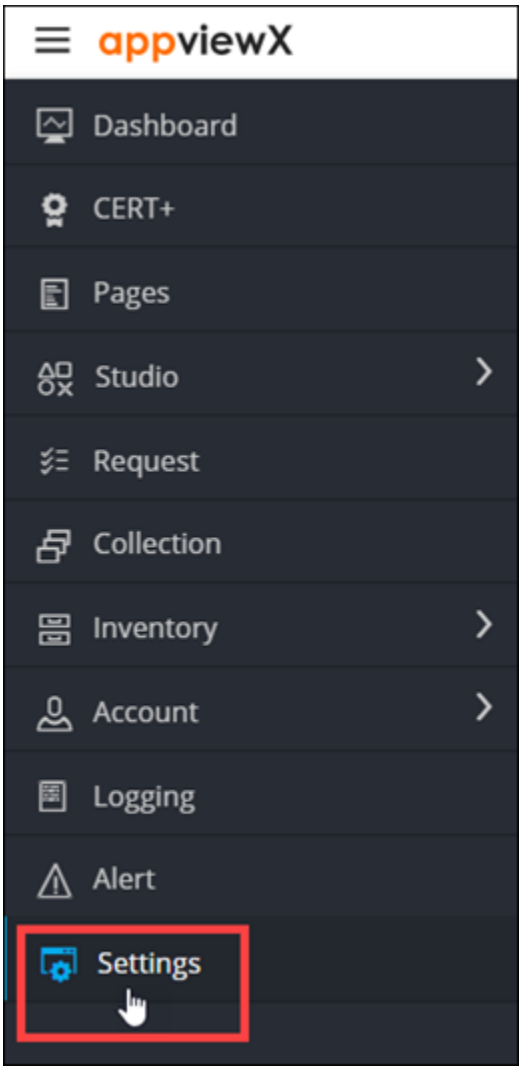
5. Turn on the **Dashboard view for admin** toggle and click **Save**.

Managing the Login Configuration

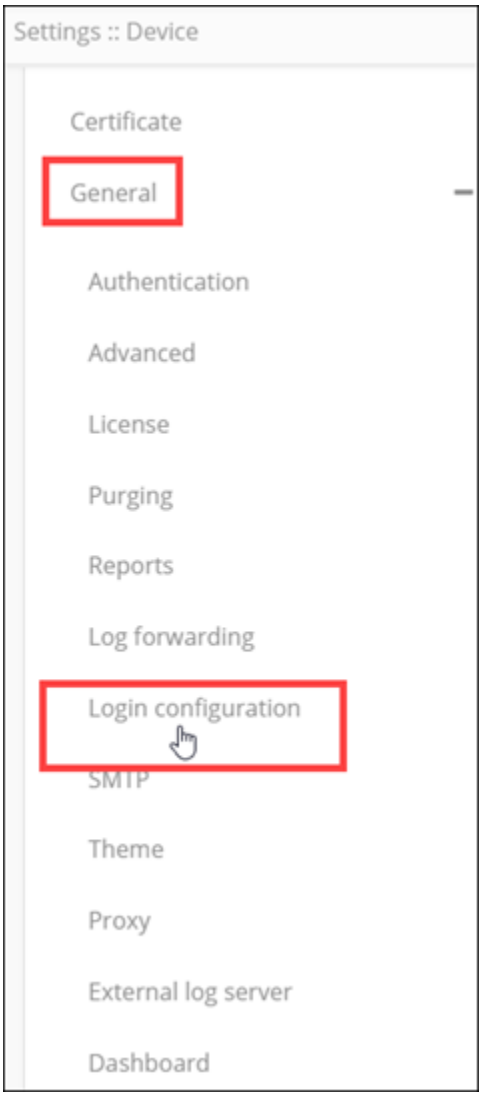
Restricting the Number of User Sessions

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.

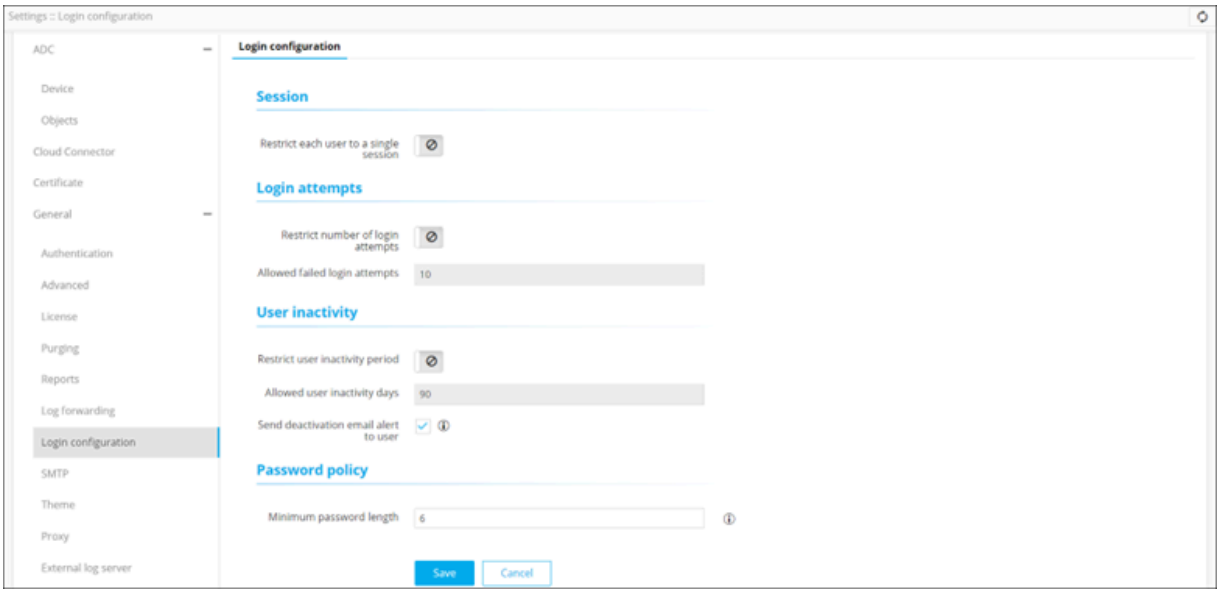
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Login configuration**.



The **Settings :: Login configuration** page is displayed.



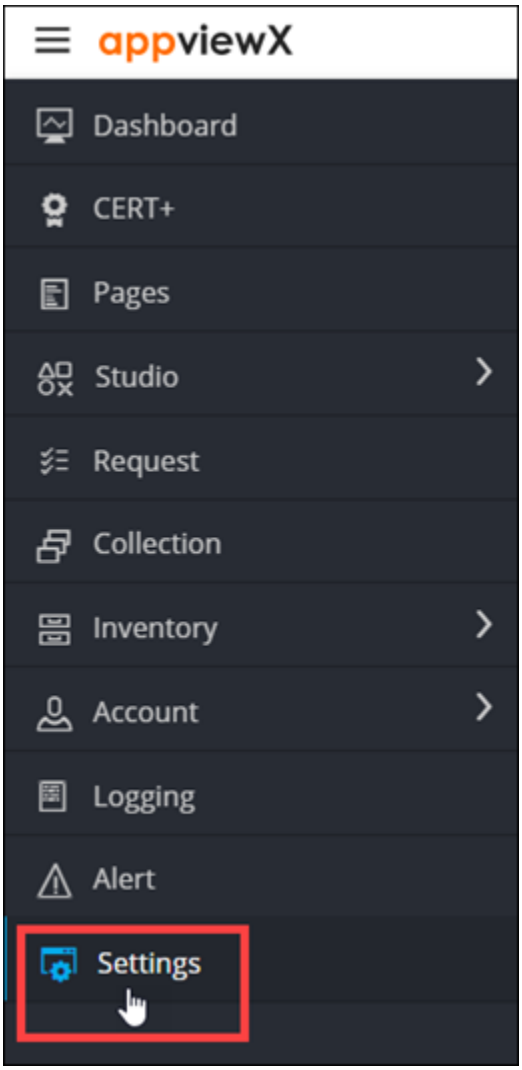
5. In the **Session** section, turn on the **Restrict each user to a single session** toggle.
6. Click **Save**.
7. In the **Confirmation** pop-up, click **OK**.

   The Login setting is modified and will be applied from next login for internal users.

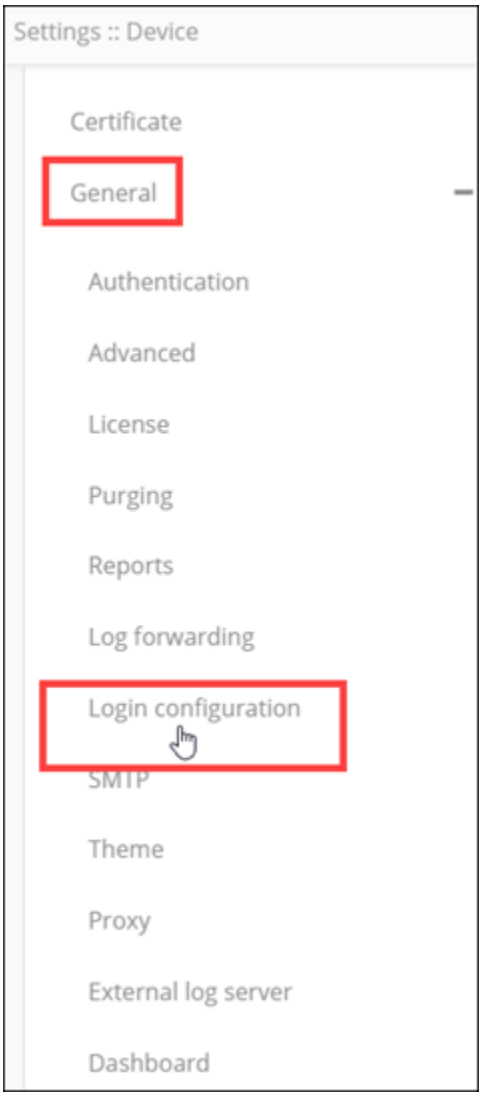
Restricting the Number of Login Attempts

The **Restrict number of login attempts** toggle is turned off be default. The number of login attempts can be restricted by enabling this feature.

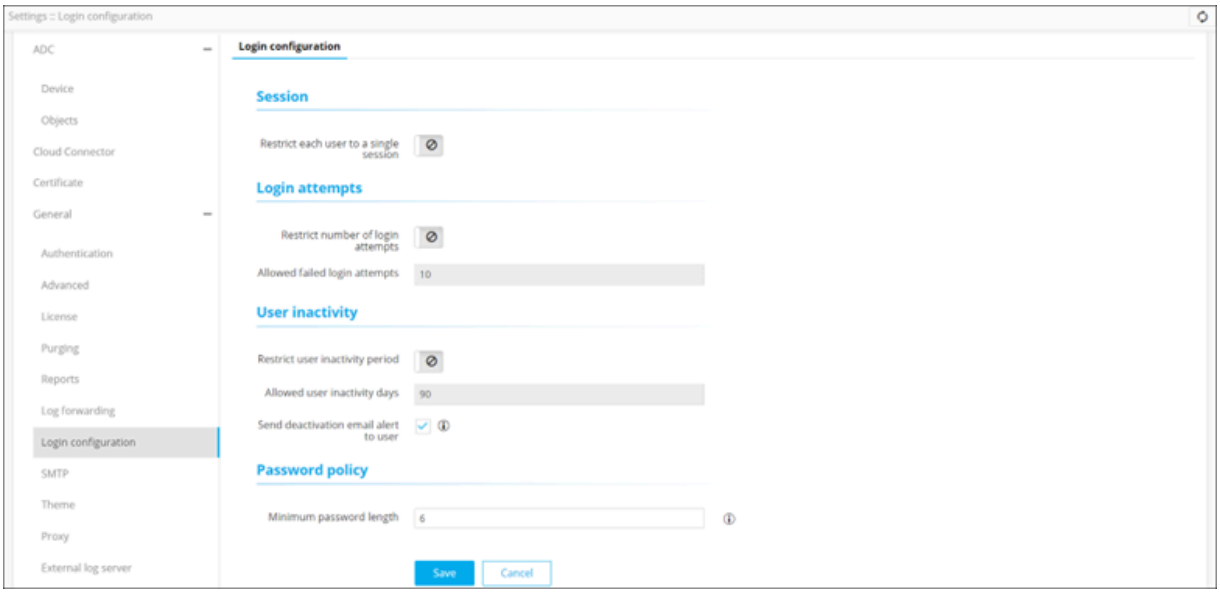
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Login configuration**.



The **Settings :: Login configuration** page is displayed.



5. In the **Login attempts** section, enter the following field information:

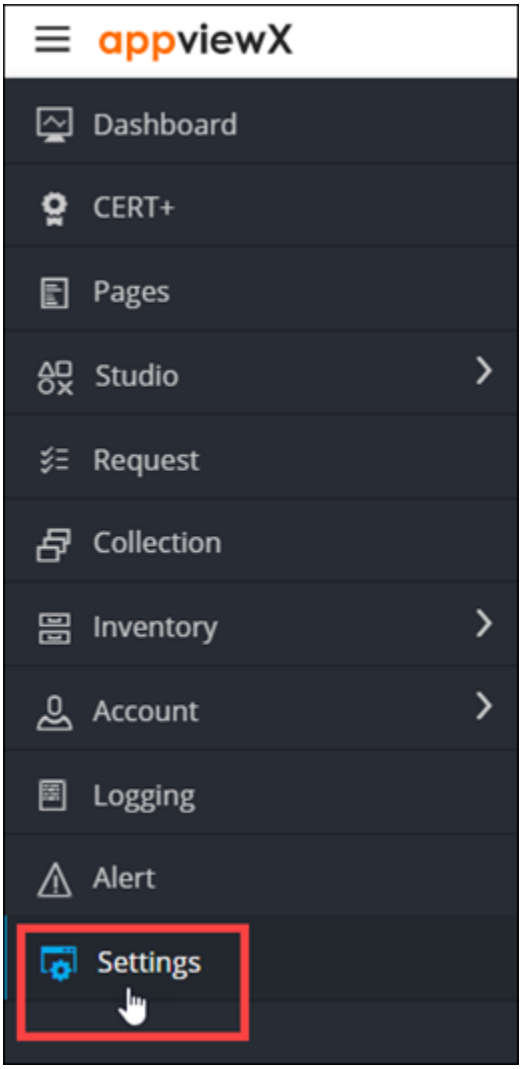
Field	Description
Restrict number of login attempts	Turn on this toggle to restrict the number of login attempts by a user.
Allowed failed login attempts	Enter any number between 0 and 99 to set the number of login attempts permitted. **Note:** By default, this value is set to 10. If the user enters incorrect details more than 10 times, he/she will get locked out.

6. Click **Save**.

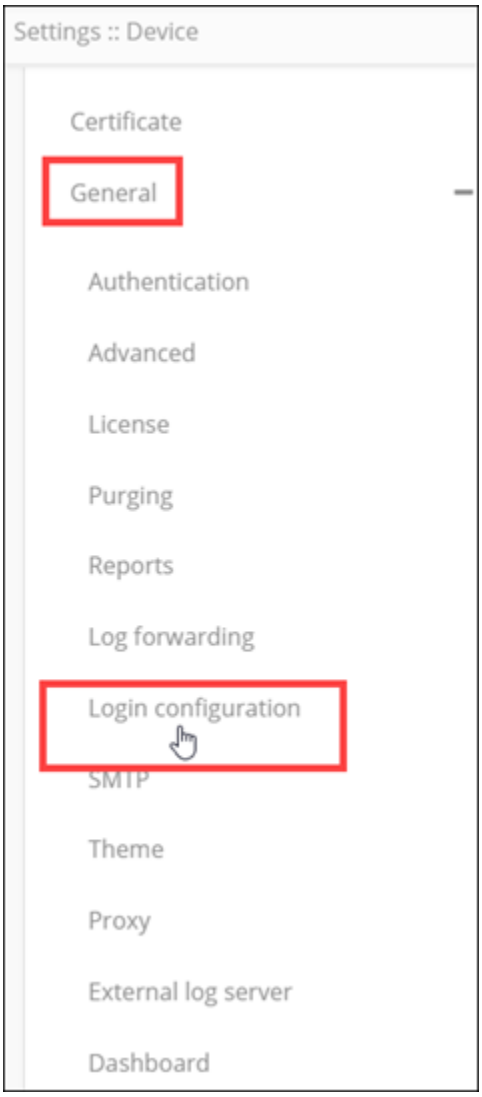
Managing User Inactivity

AppViewX lets you restrict a user from logging in to the system if they have been inactive for a predefined duration.

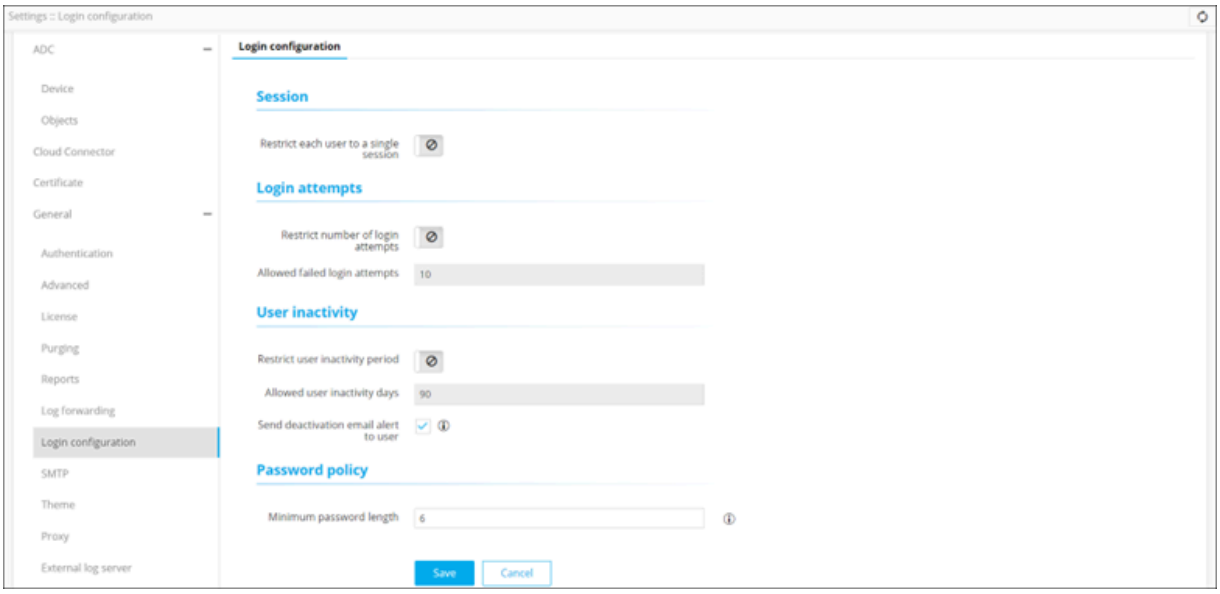
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Login configuration**.



The **Settings :: Login configuration** page is displayed.



5. In the **User inactivity** section, turn on the **Restrict user inactivity period** toggle.
6. 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).
7. 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.
8. Click **Save**.

Chapter 8: Managing Logs

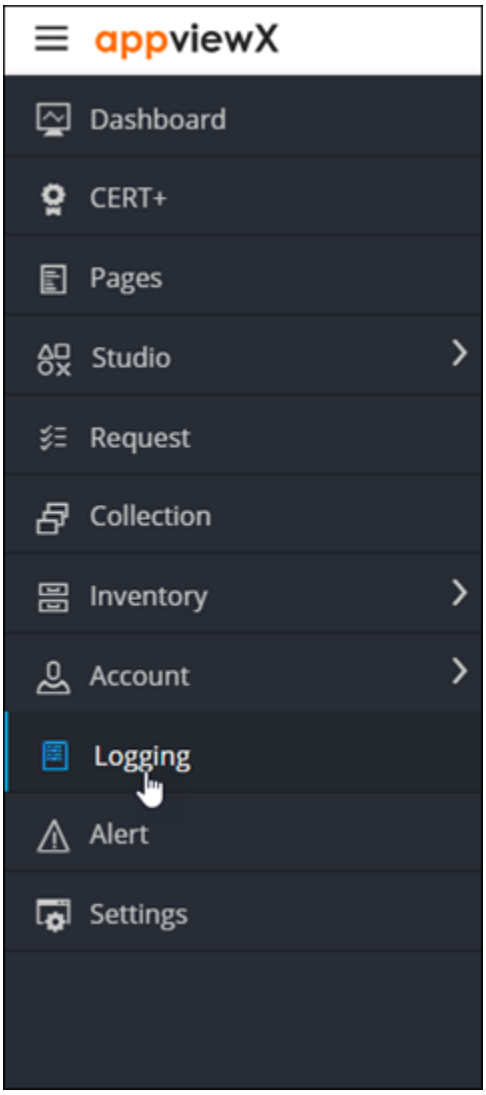
Viewing Logs

AppViewX supports only role-based (and not user-based) access for logs, which means that if a user role has permission to view logs, all users under that user role can view all AppViewX logs.

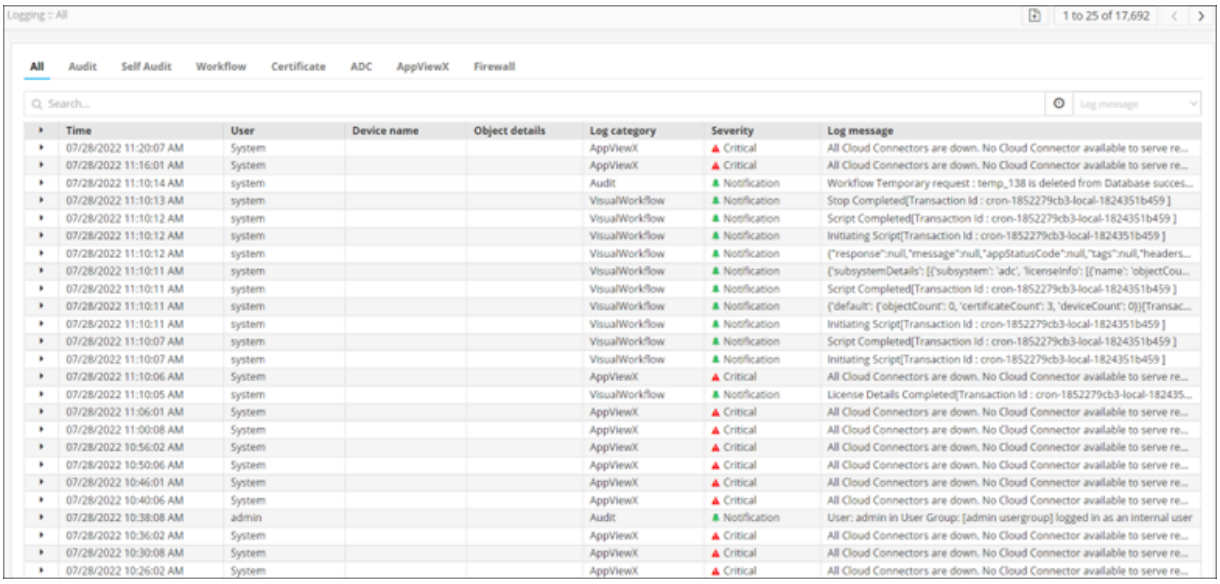
Viewing All Logs

To view all logs:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Logging**.



The **Logging :: All** page is displayed (by default).



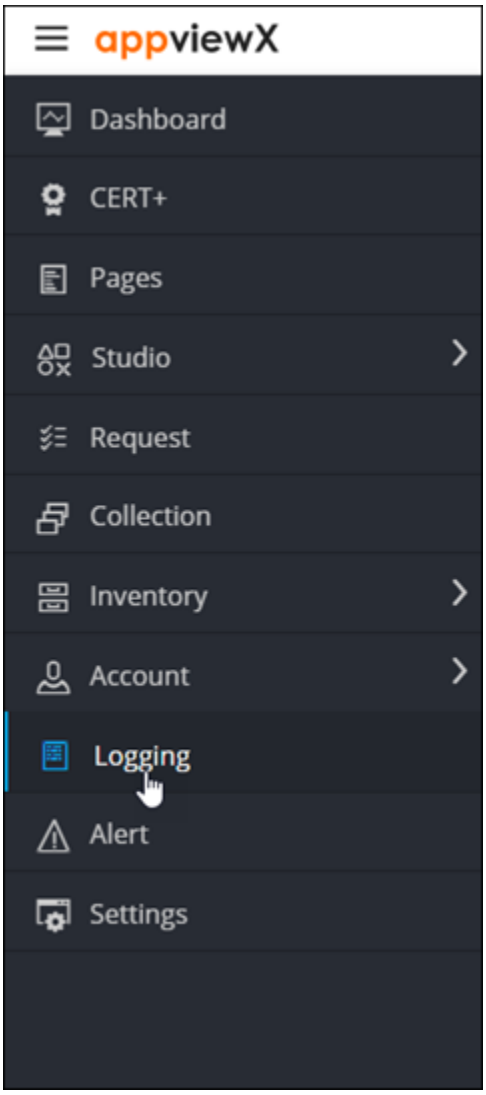
For each activity, this page displays the following details:

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 category	Category under which this log record will be filed
Severity	Severity of the activity logged (Notification, Debug, Warn, Error, Fatal, Critical)
Log Message	Description of the activity logged

Viewing Audit Logs

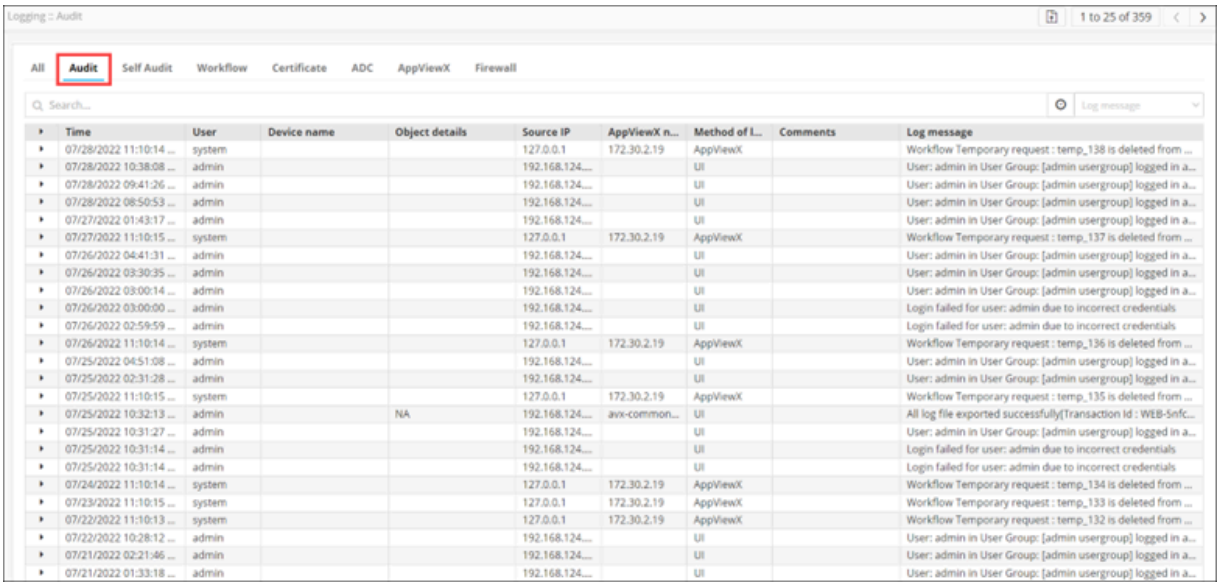
To view Audit logs,

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Logging**.



The **Logging :: All** page is displayed (by default).

3. On the **Logging** page, click the **Audit** tab.
   The **Logging :: Audit** page is displayed.



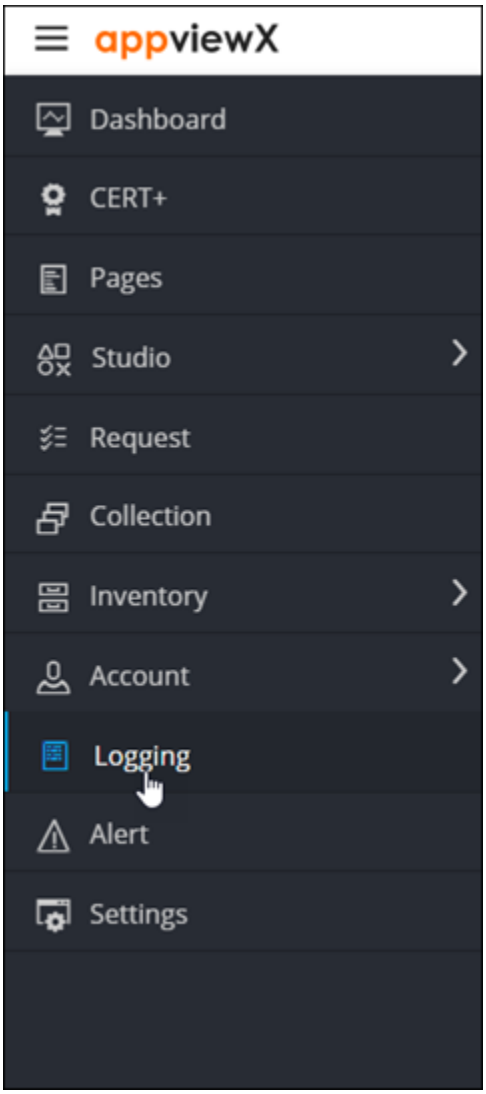
The page displays the following details for the Audit logs:

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
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

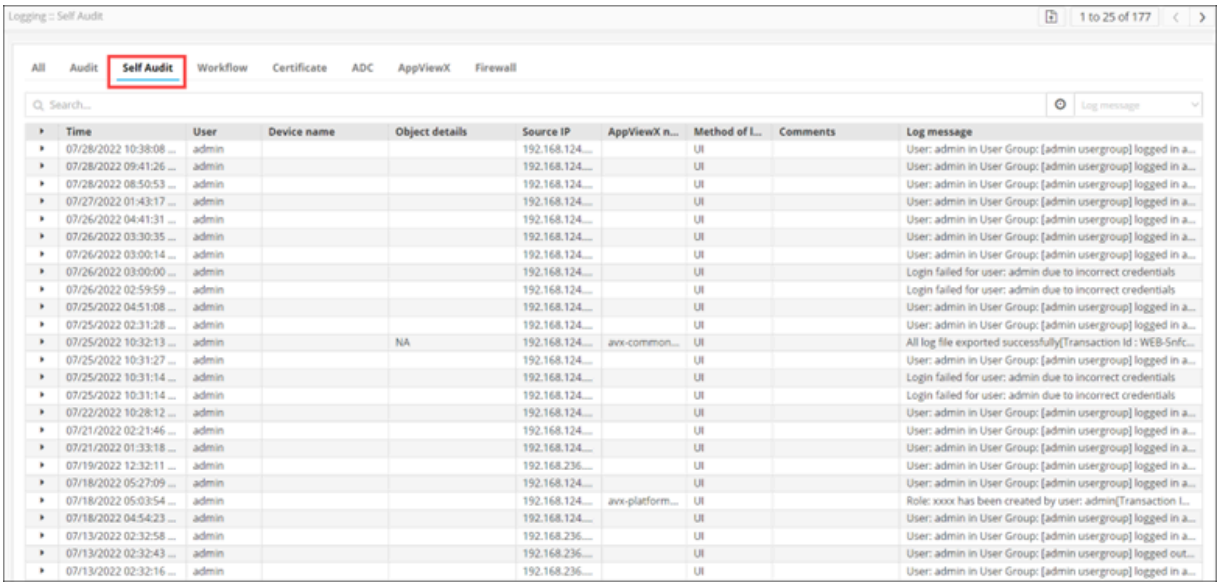
Viewing Self-Audit Logs

To view Self Audit logs:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Logging**.



   The **Logging :: All** page is displayed (by default).
3. On the **Logging** page, click the **Self Audit** tab.
   The **Logging :: Self Audit** page is displayed.



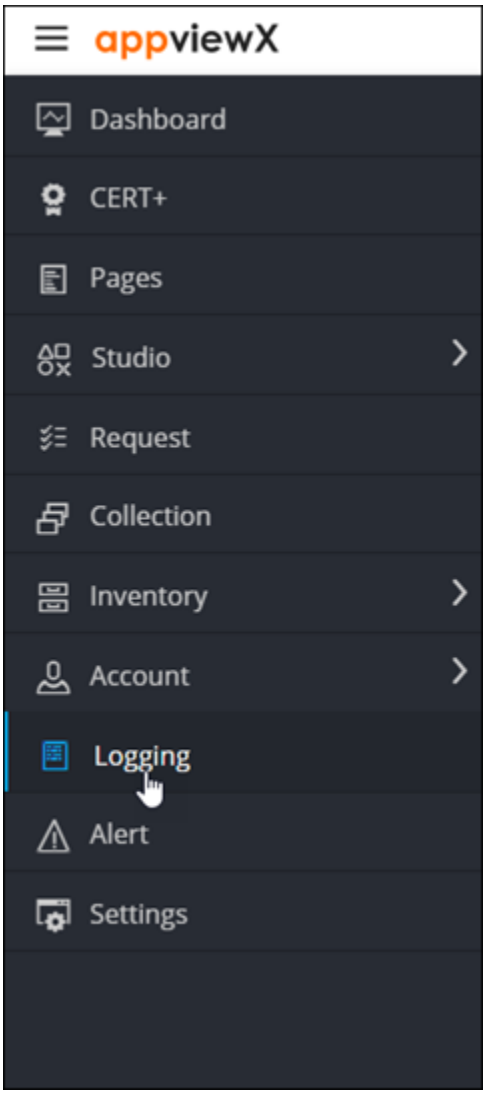
The page displays the following details for the Self Audit logs:

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
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

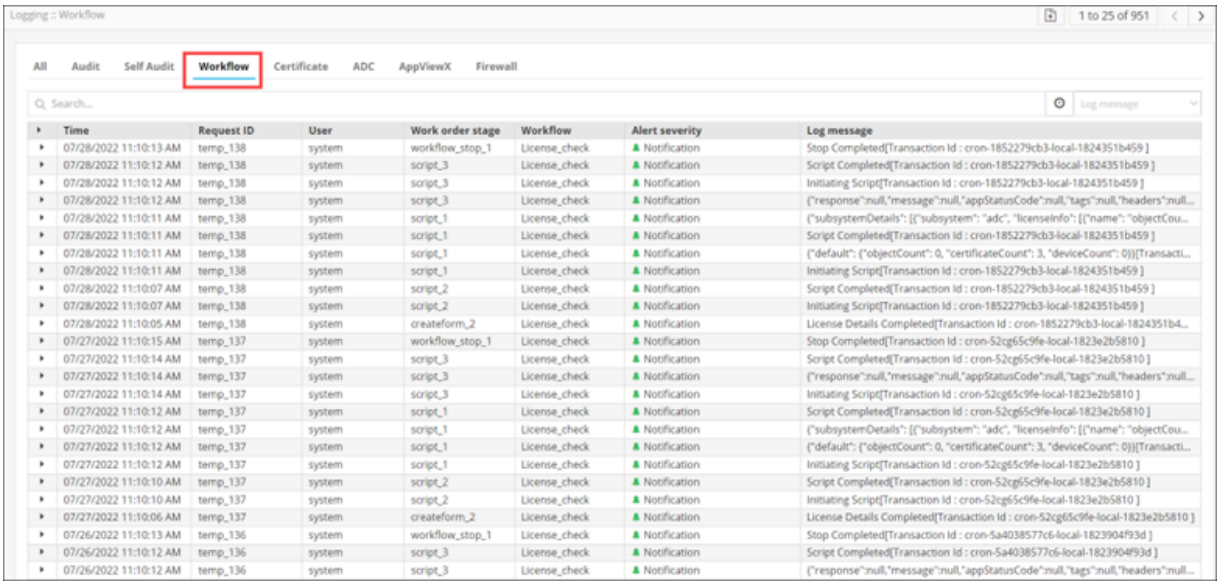
Viewing Workflow Logs

To view the workflow logs:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Logging**.



   The **Logging :: All** page is displayed (by default).
3. On the **Logging** page, click the **Workflow** tab.
   The **Logging :: Workflow** page is displayed.



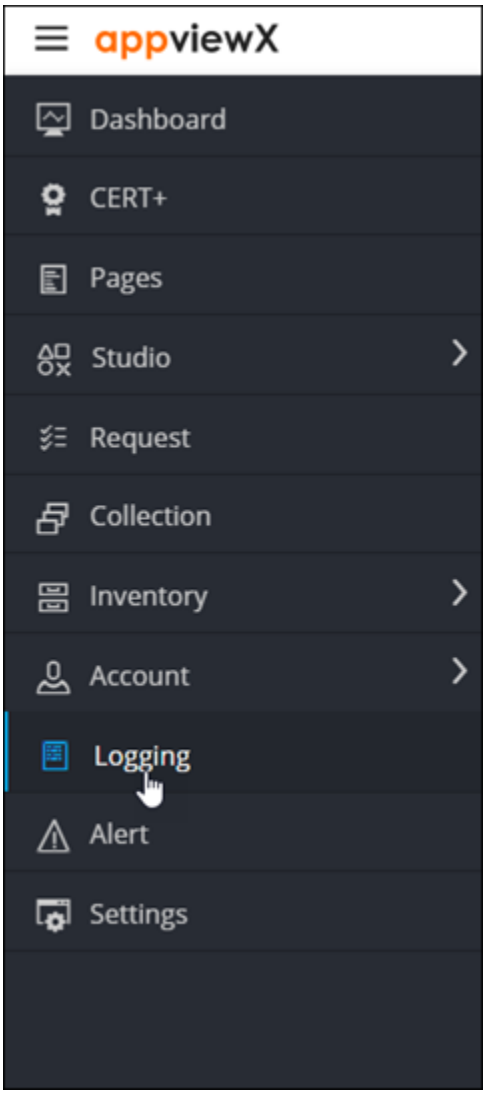
The page displays the following details for the Workflow logs:

Category	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.
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

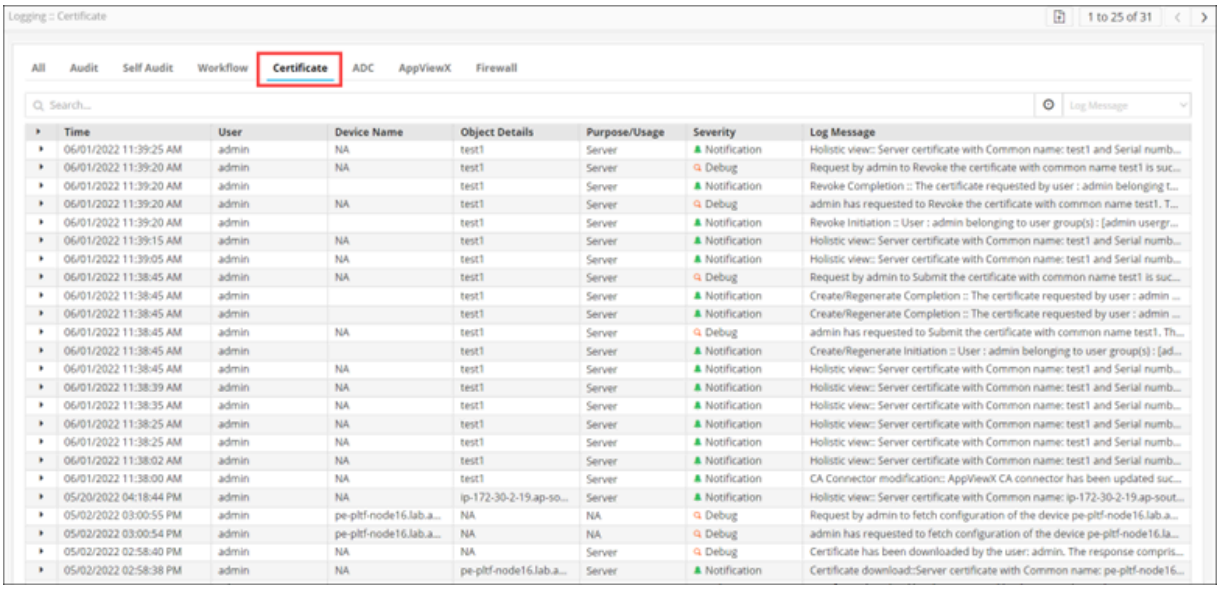
To view Certificate logs:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Logging**.



The **Logging :: All** page is displayed (by default).

3. On the **Logging** page, click the **Certificate** tab.
   The **Logging :: Certificate** page is displayed.



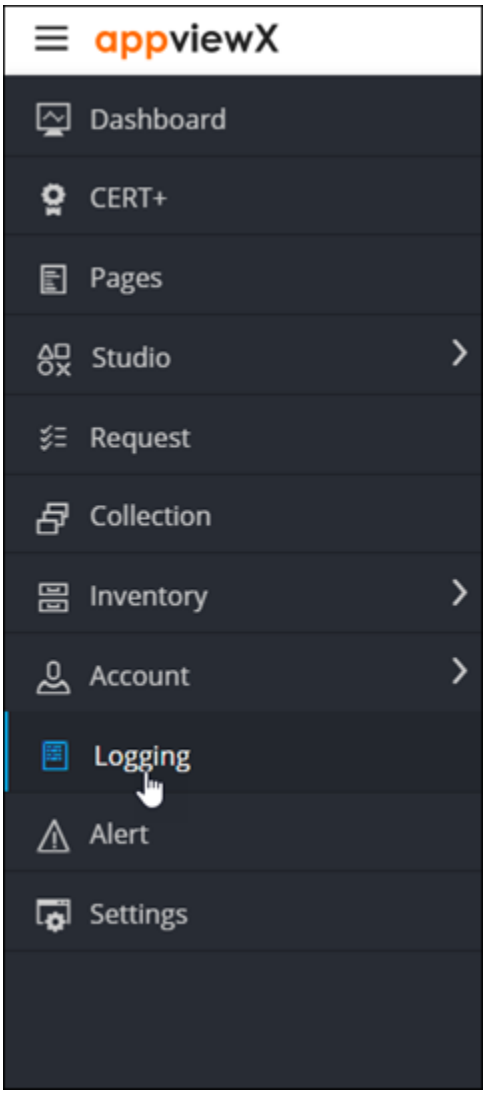
The page displays the following details for the Certificate logs:

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.
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 ADC Logs

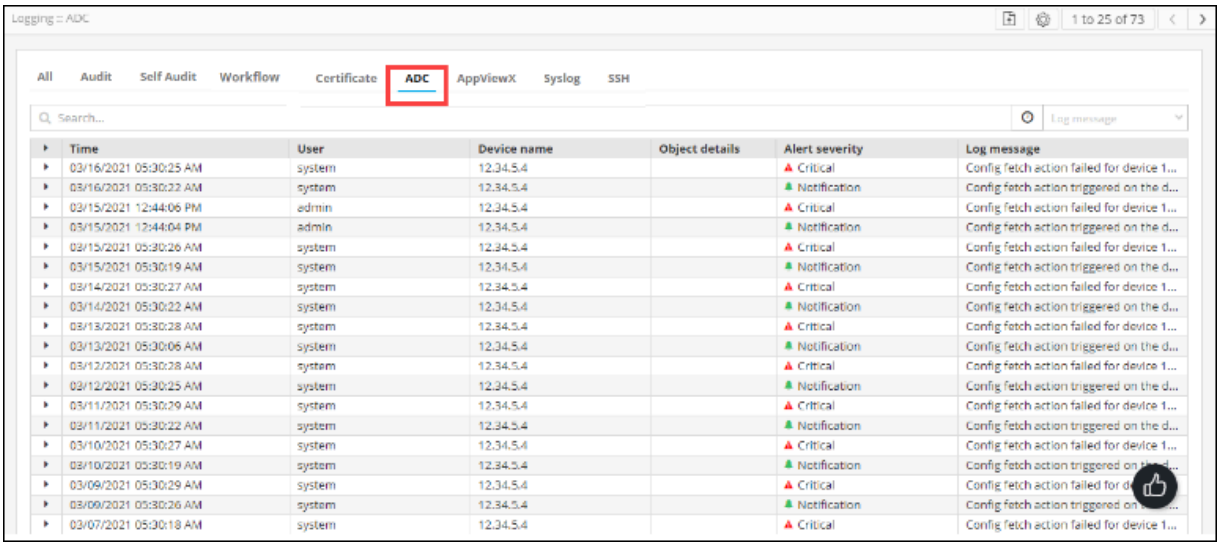
To view the ADC logs:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Logging**.



The **Logging :: All** page is displayed (by default).

3. On the **Logging** page, click the **ADC** tab.
   The **Logging :: ADC** page is displayed.



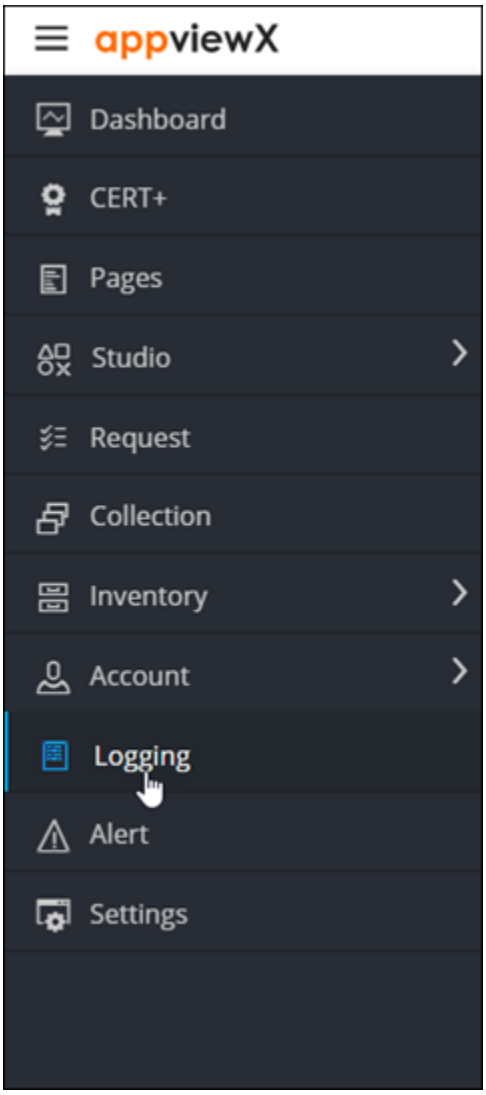
The page displays the following details for the ADC logs:

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
Alert severity	Severity of the activity logged (Notification, Debug, Warn, Error, Fatal, Critical)
Log Message	Description of the activity logged

Viewing AppViewX Logs

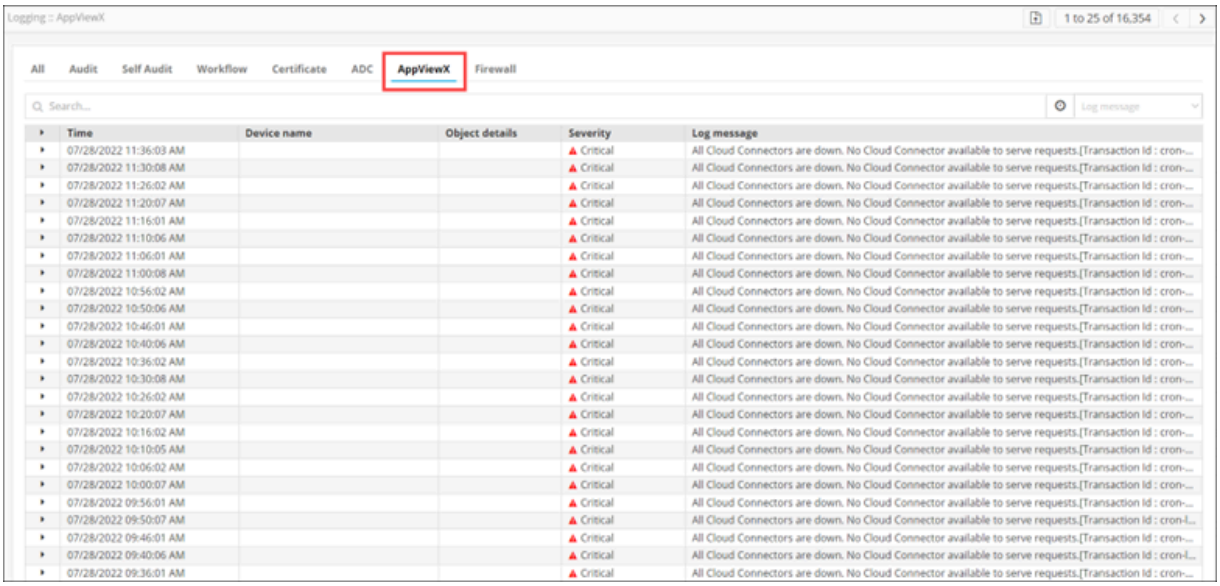
To view the AppViewX logs:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Logging**.



The **Logging :: All** page is displayed (by default).

3. On the **Logging** page, click the **AppViewX** tab.
   The **Logging :: AppViewX** page is displayed.



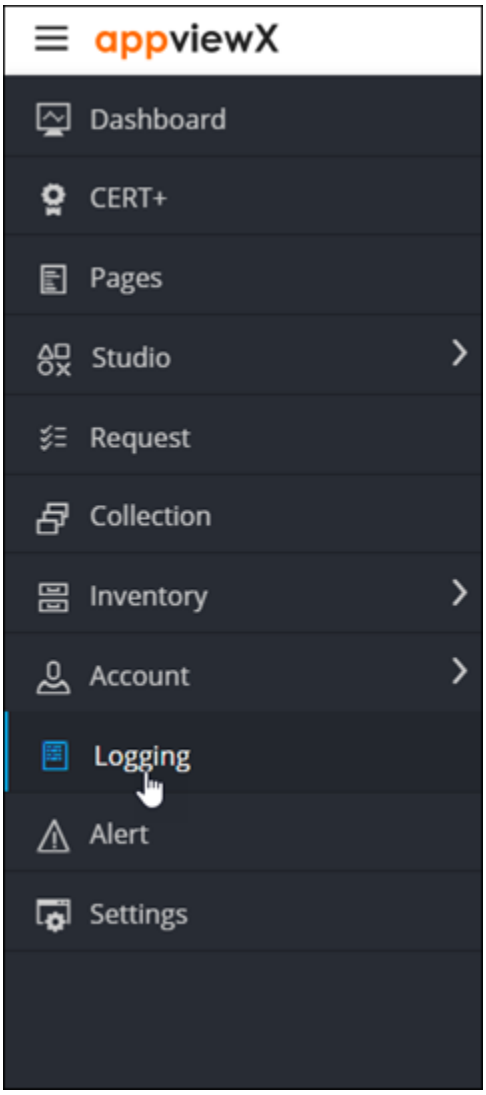
The page displays the following details for the AppViewX logs:

Category	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 Firewall Logs

To view the workflow logs:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Logging**.



The **Logging :: All** page is displayed (by default).

3. On the **Logging** page, click the **Firewall** tab.

   The **Logging :: Firewall** page is displayed. The page displays the following details for the 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

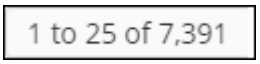
Category	Description
Object details	Name of the object, if the log is of a object-related activity
Log Message	Description of the activity logged.

Setting the Record Count Preference for Logs

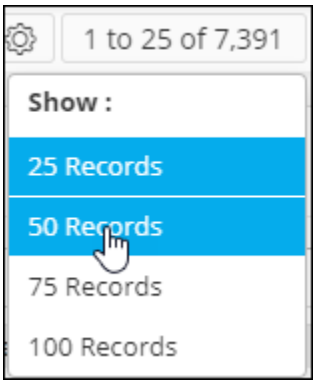
For easier viewing of records, AppViewX lets you set the record count preference, which is the number of log records that will be displayed on one page.

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

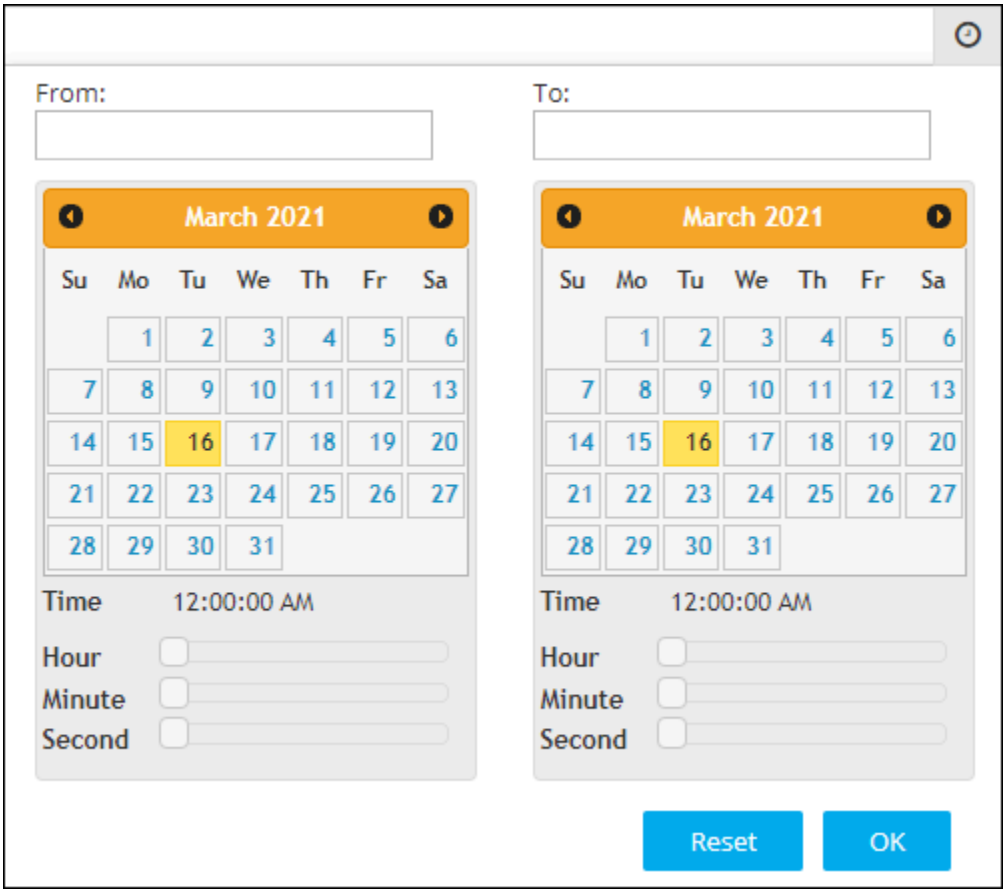
AppViewX lets you search for logs in two ways:

- 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  .
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**.

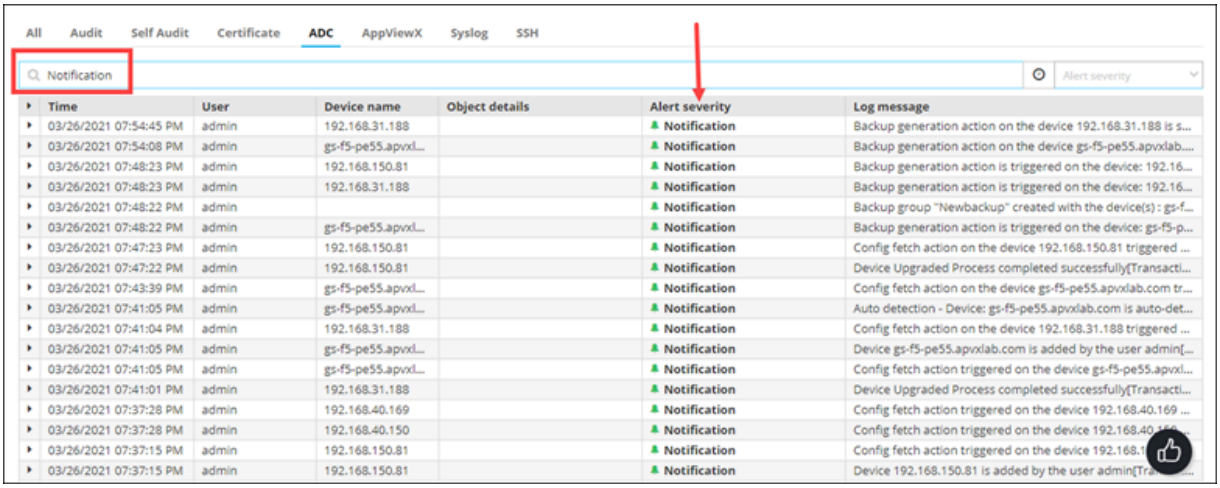
The page is updated to display log records from the selected timestamp.

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. Navigate to the **Logging :: ADC** page.
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.



Forwading Logs

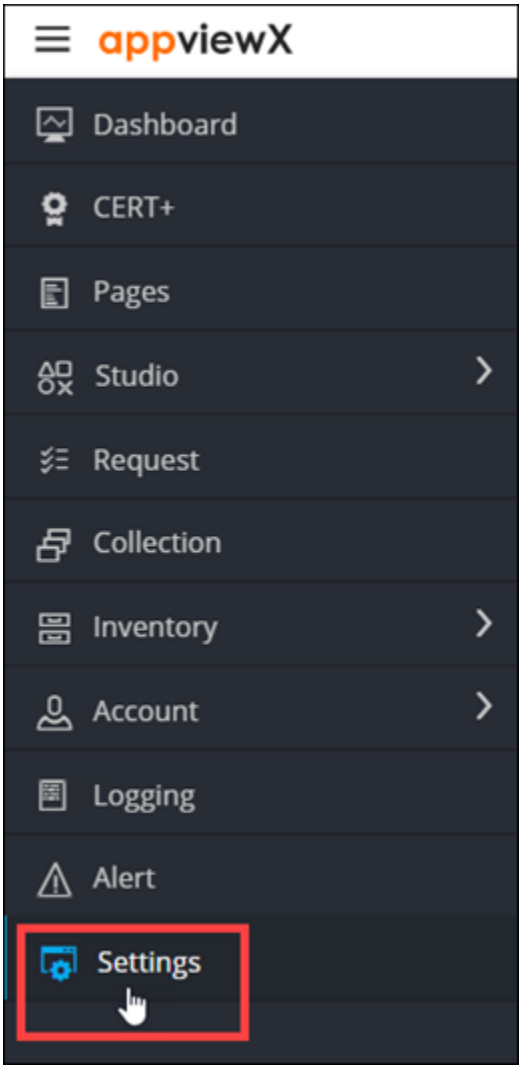
Before logs are purged, AppViewX enables forwarding logs to external servers, like SIEM, that allows for a detailed analysis and, therefore, better identification of problem areas. This gives an advantage when configuring alerts; new alerts can be created to target and resolve the problem areas identified.

Configuring Server Inventory Settings

Server inventory settings are used to configure settings for forwarding logs to a specific external server.

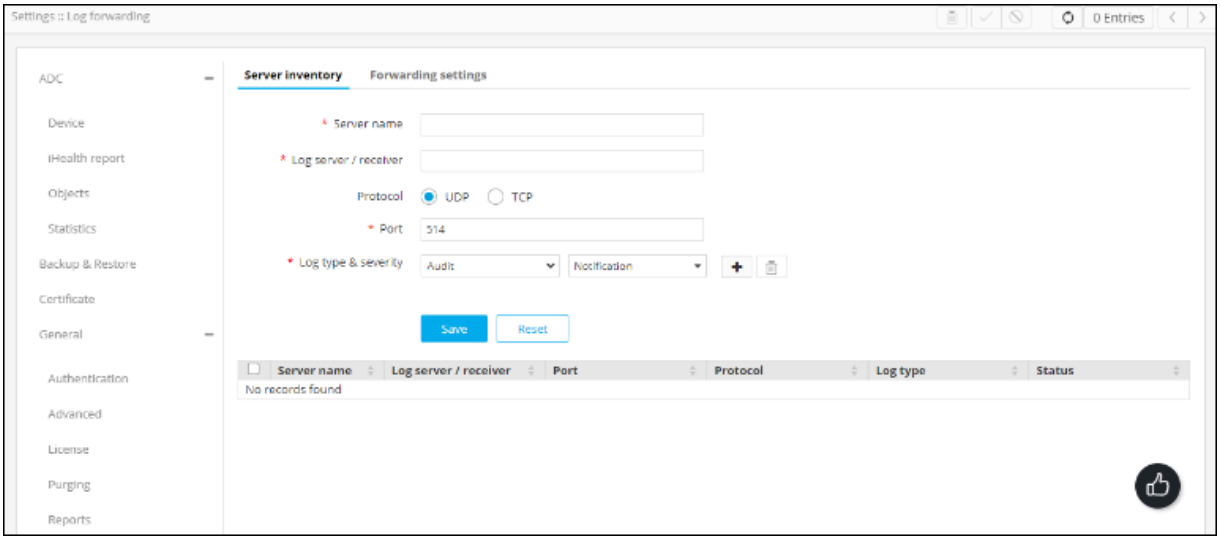
To configure server inventory settings:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General** and select **Log Forwarding**.

The **Settings :: Log Forwarding** page is displayed, with the **Server inventory** tab open by default.



4. In the **Server inventory** tab, enter the following details (sample values are shown in the image below the table):

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

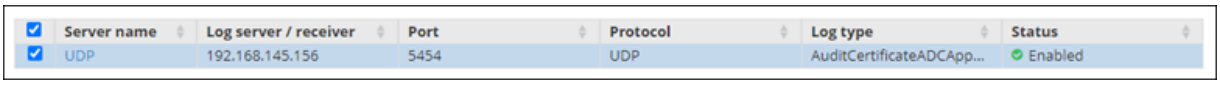
Field	Description
***Log type & severity**	You can choose to forward logs of a specific type and a specific severity to an external server. **To add a log type and severity entry:** a. From the first drop-down menu, select a log type from the following: • Audit (default) • Certificate • ADC • AppViewX b. From the second drop-down menu, select the severity of the log type from the following: • Notification (default) • Debug • Warn • 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  . 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  . **Note:** It is mandatory to have at least one log type and severity entry.
All * marked fields are mandatory.	

5. 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

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.



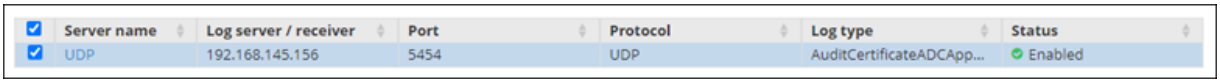
2. From the top right corner of the screen, click  .

> **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.



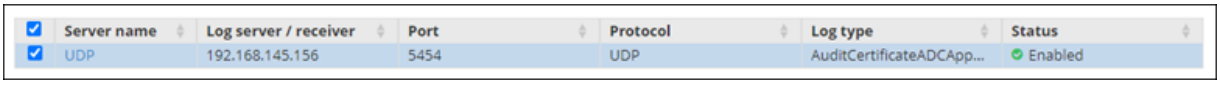
2. From the top right corner of the screen, click  .

> **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.



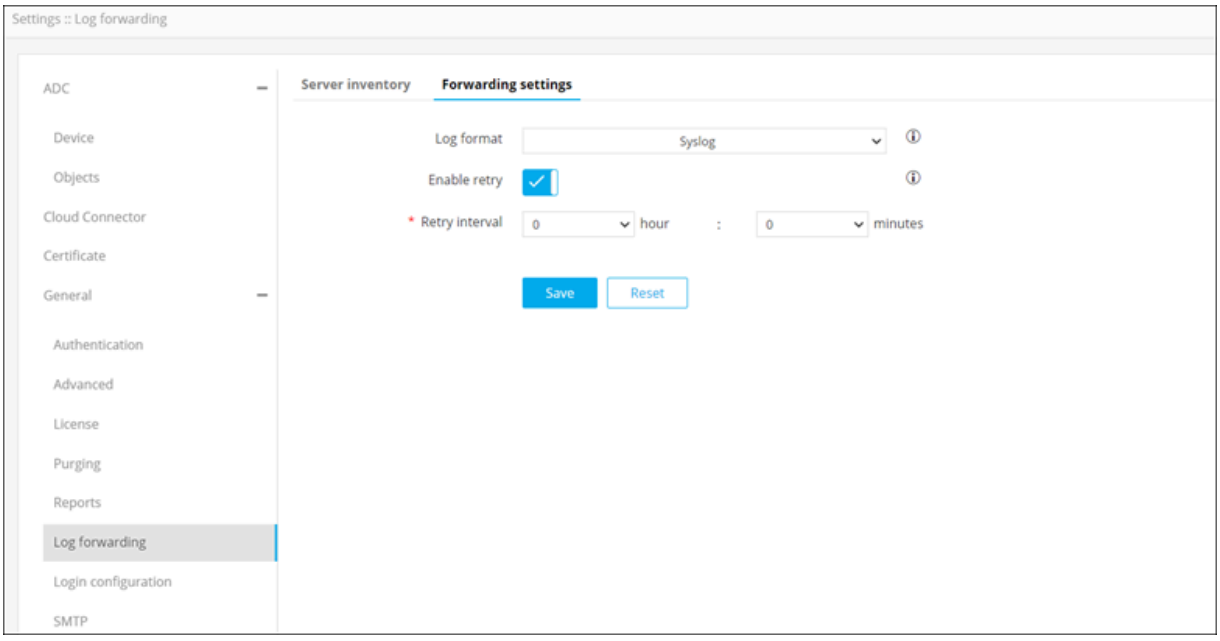
2. From the top right corner of the screen, click  .

> **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:

1. On the **Settings :: Log Forwarding** page, under the **Forwarding settings** tab, enter the following details:



Field	Description
Log format	To select the format in which logs should be forwarded to the external server, from the drop-d 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 ret which logs will be forwarded again. To enable this retry, turn on the **Enable retry** toggle.
***Retry interval**	To set a retry interval, from the **hour** and **minutes** drop-down menus, select the required valu **Note:** This field is displayed when the **Enable retry** toggle is turned on.
All * marked fields are mandatory.	

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.

To export logs:

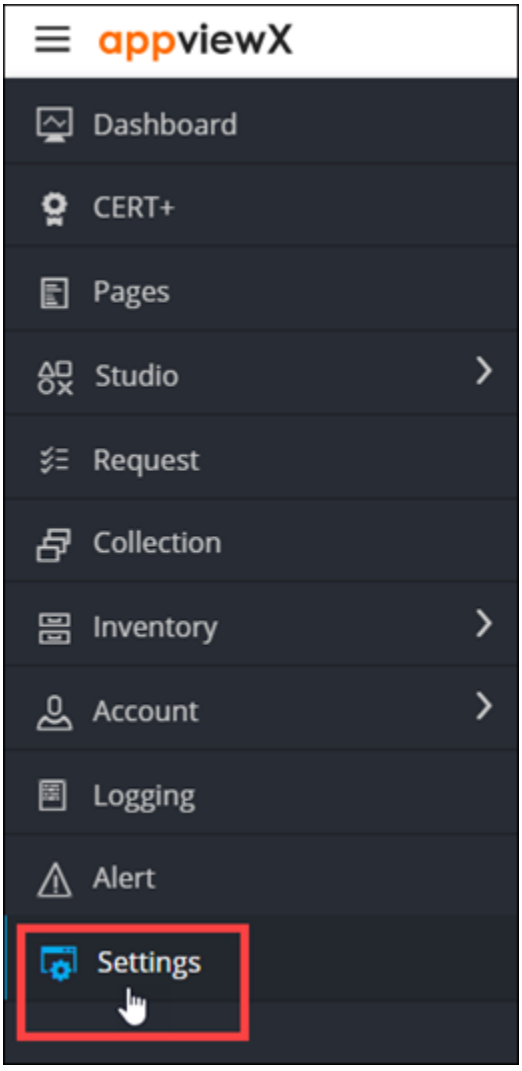
1. Go to the **Logging** page for the log type you want to export.
2. From the top right corner of the **Logging** page, click  .
3. Navigate to the location to save the log file and click **Save**.
   All logs of the selected log type are downloaded and saved.

Purging Logs

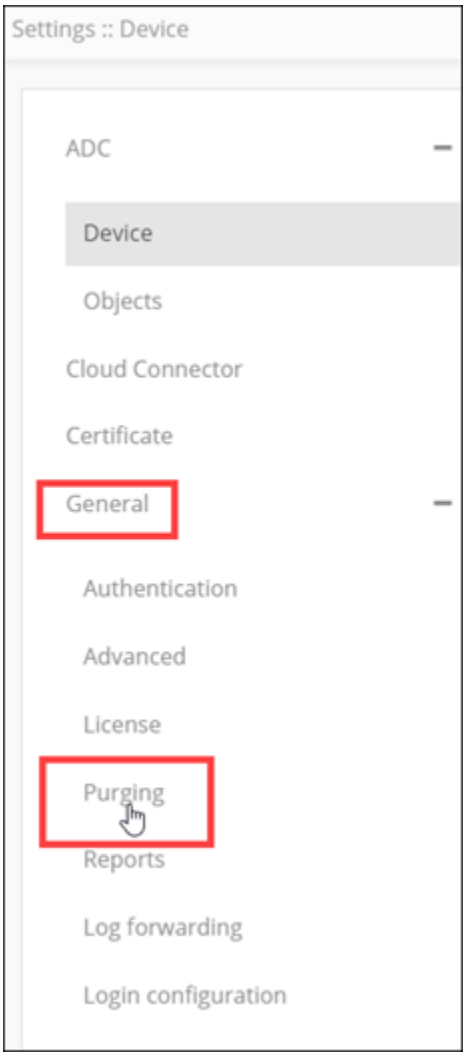
With a large number of log entries being recorded each day, a system can soon become vulnerable to threats like a compromise of confidential information, a surplus of outdated information, and so on. For security reasons, regular purging of old data comes as a highly recommended practice.

To enable purging of log records:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the icon.
2. From the menu displayed, click **Settings**.

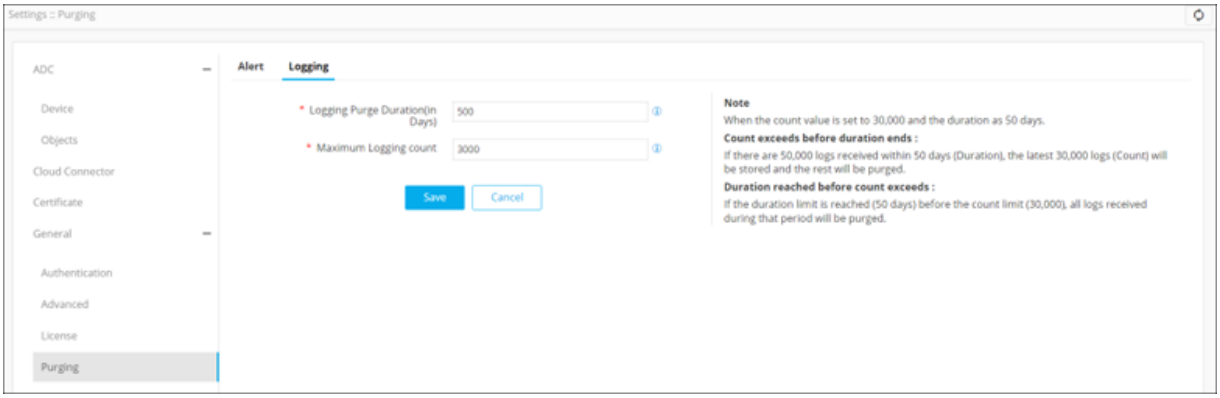


3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Purging**.



The **Settings :: Purging** screen is displayed.

5. To configure the log purging settings, on the **Settings :: Purging** page, click the **Logging** tab.
6. Under the **Logging** tab, enter the following details:



Field	Description
***Logging Purge Duration (in Days)**	Enter the number of days, the interval, after which logs will be purged.
***Maximum Logging count**	Enter the maximum number of the most recent logs that have to be retained. For example, if you set this value to 10,000, all logs after the first 10,000 logs will be purged.
All * marked fields are mandatory.	

Note: Excess logs will be purged even if the maximum logging count is exceeded before the next purging cycle is scheduled.

7. Click **Save**.

Chapter 9: Managing Alerts

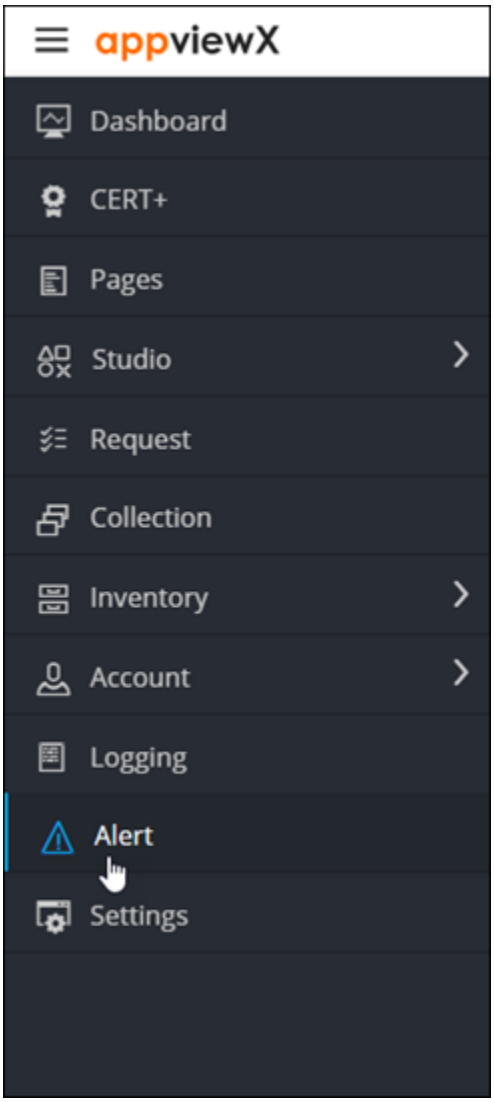
Viewing Existing Alerts

AppViewX lets you view all alerts in one place as well as groups them under the above mentioned categories for a segregated viewing.

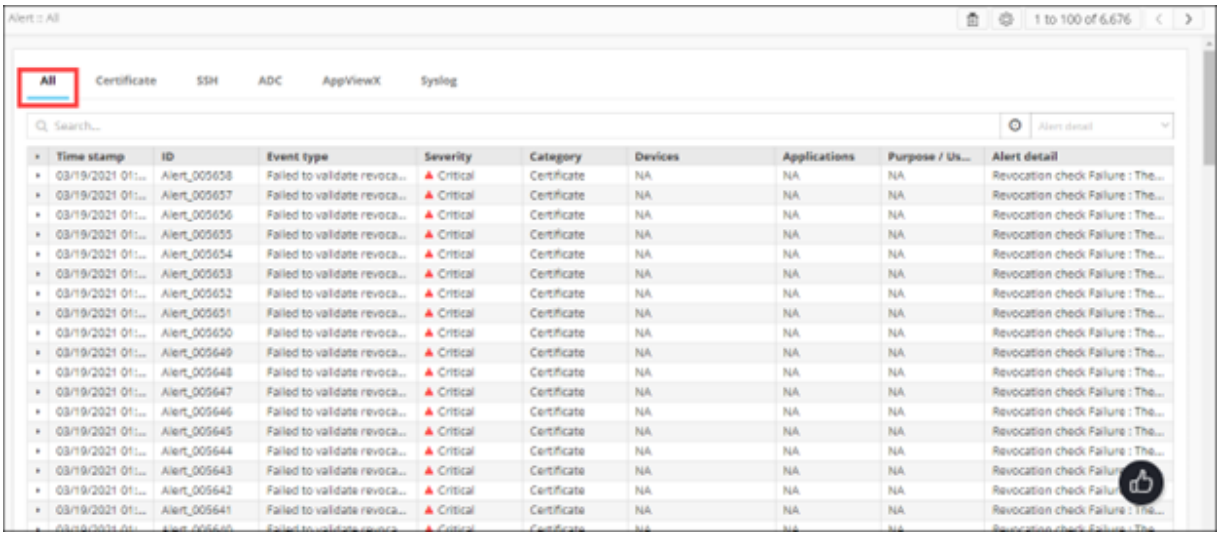
Viewing All Alerts

To view all existing alerts:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Alert**.



The **Alert :: All** page is displayed (by default).



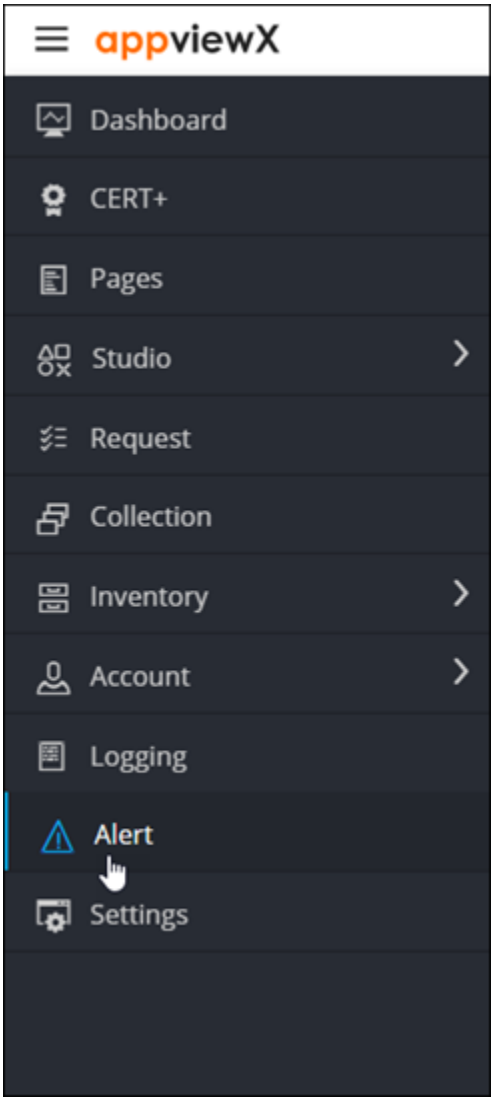
For each alert, this page displays the following details:

Field	Description
Time stamp	Date and time at which the event, which triggered the alert, occurred.
ID	Alert ID
Event type	Type of the event that triggered the alert.
Severity	Alert severity AppViewX identifies the following severity levels (as described above): • Critical • Fatal • Major • Minor
Category	Alert category.
Devices	Name of the device, if the alert is to notify of a device-related activity.
Applications	Application that triggered the alert.
Purpose/Usage	Purpose of the alert.
Alert detail	Description of the alert.

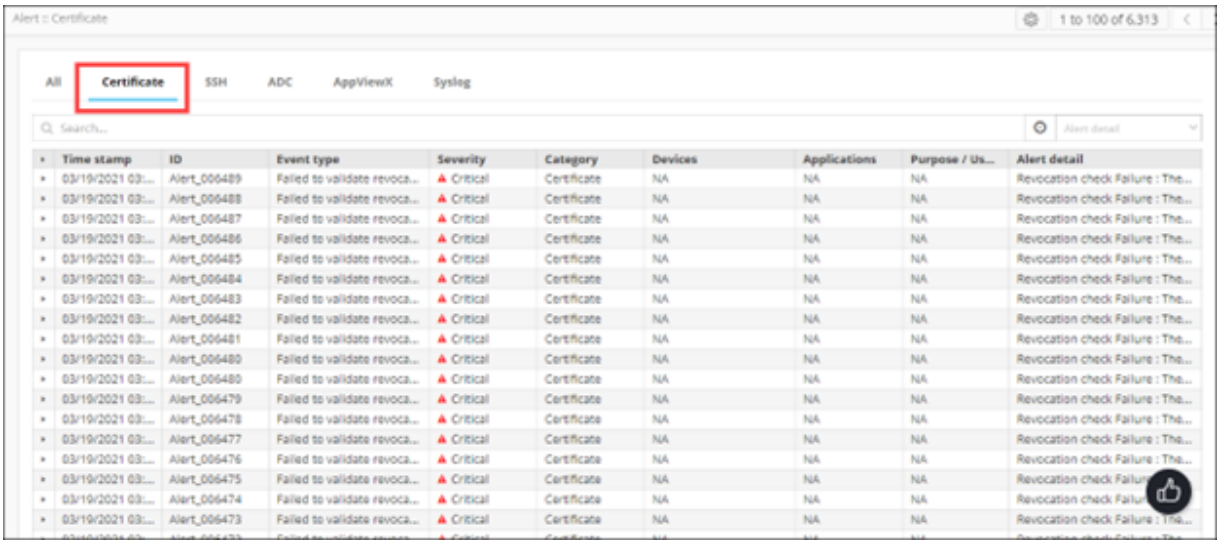
Viewing Certificate Alerts

To view the Certificate alerts:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Alert**.



   The **Alert :: All** page is displayed (by default).
3. On the **Alert :: All** page, click the **Certificate** tab.
   The **Alert :: Certificate** page is displayed.



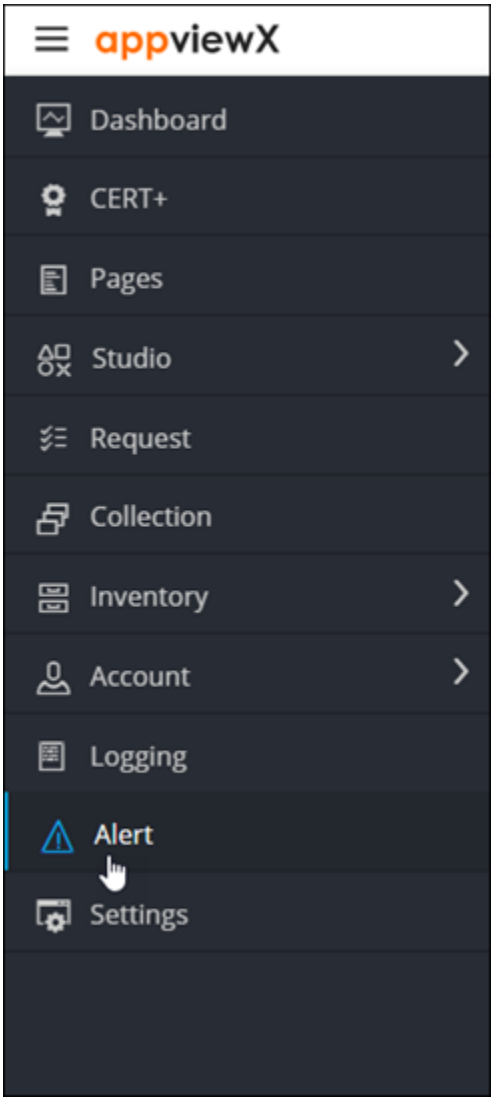
For the Certificate alerts, the page displays the following details:

Field	Description
Timestamp	Date and time at which the event, which triggered the alert, occurred.
ID	Alert ID
Event type	Type of the event that triggered the alert.
Severity	Alert severity. AppViewX identifies the following severity levels (as described above): • Critical • Fatal • Major • Minor
Category	Alert category.
Devices	Name of the device, if the alert is to notify of a device-related activity.
Applications	Application that triggered the alert.
Purpose/Usage	Purpose of the alert.
Alert detail	Description of the alert.

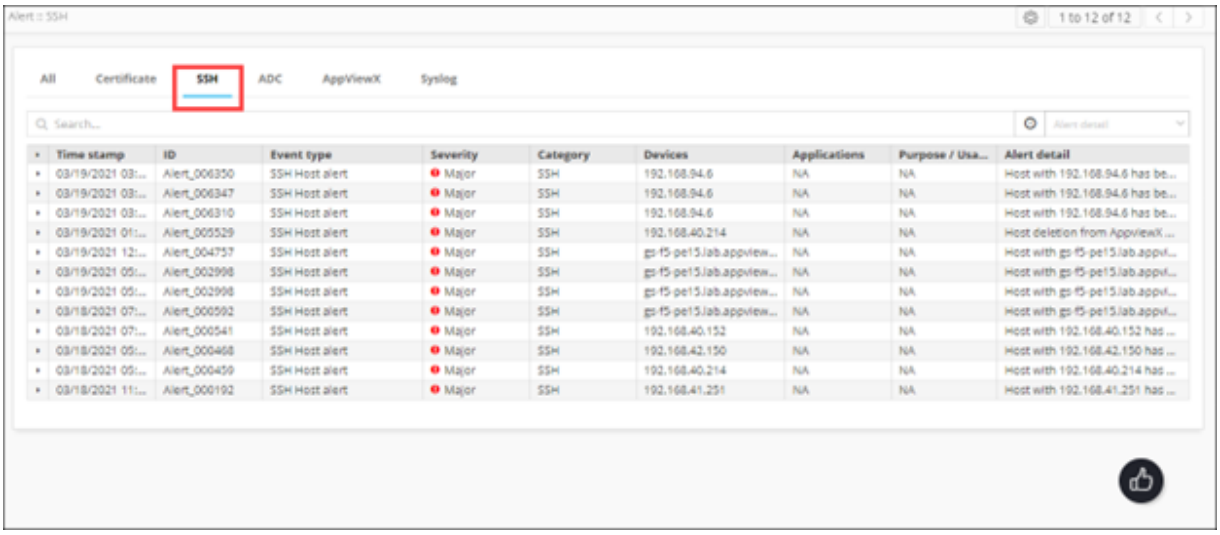
Viewing SSH Alerts

To view the SSH alerts:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Alert**.



   The **Alert :: All** page is displayed (by default).
3. On the **Alert :: All** page, click the **SSH** tab.
   The **Alert :: SSH** page is displayed.



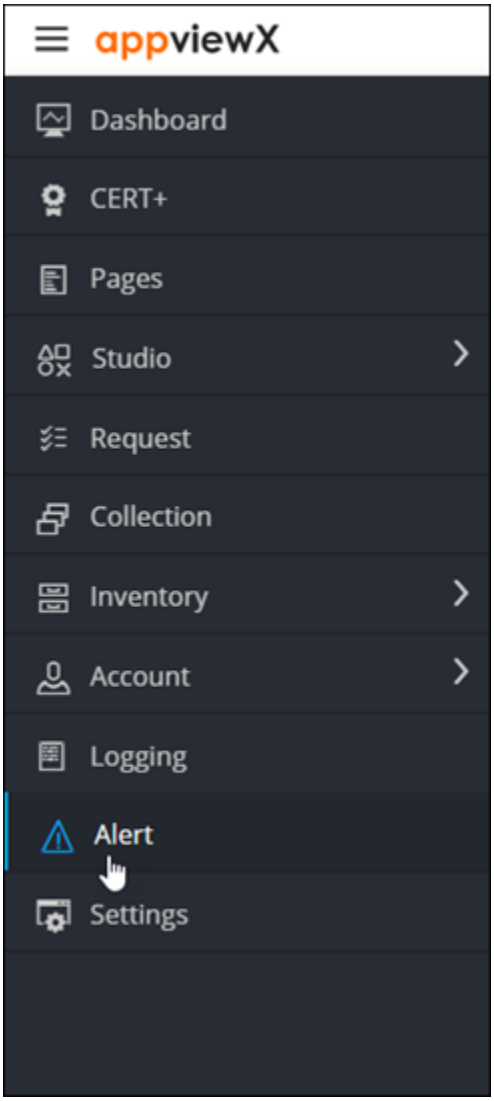
For the SSH alerts, the page displays the following details:

Field	Description
Timestamp	Date and time at which the event, which triggered the alert, occurred.
ID	Alert ID
Event type	Type of the event that triggered the alert.
Severity	Alert severity. AppViewX identifies the following severity levels (as described above): • Critical • Fatal • Major • Minor
Category	Alert category.
Devices	Name of the device, if the alert is to notify of a device-related activity.
Applications	Application that triggered the alert.
Purpose/Usage	Purpose of the alert.
Alert detail	Description of the alert.

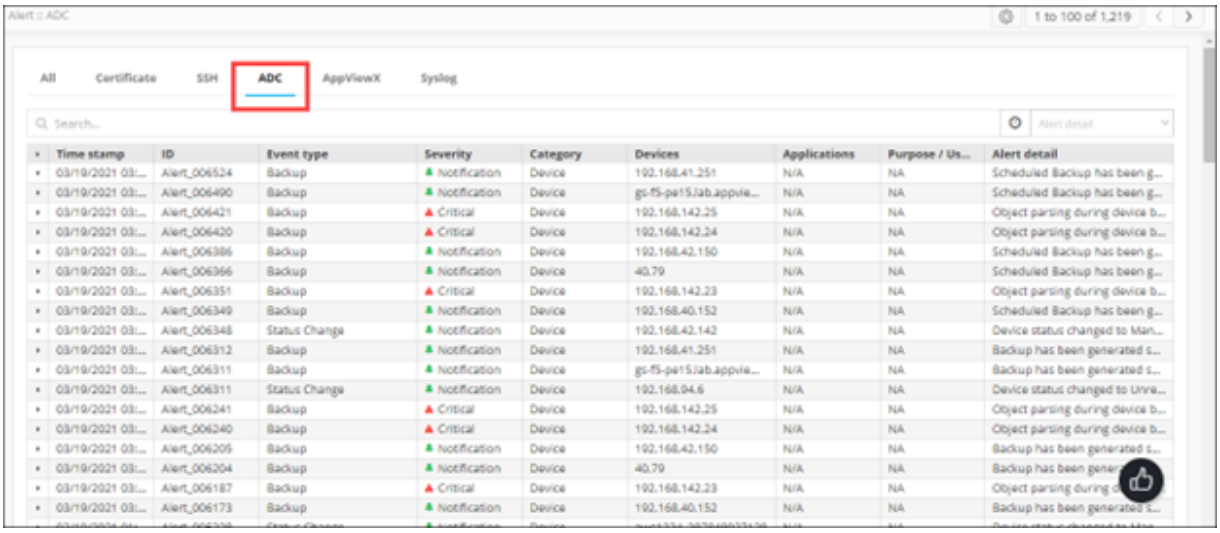
Viewing ADC Alerts

To view the ADC alerts:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Alert**.



   The **Alert :: All** page is displayed (by default).
3. On the **Alert :: All** page, click the **ADC** tab.
   The **Alert :: ADC** page is displayed.



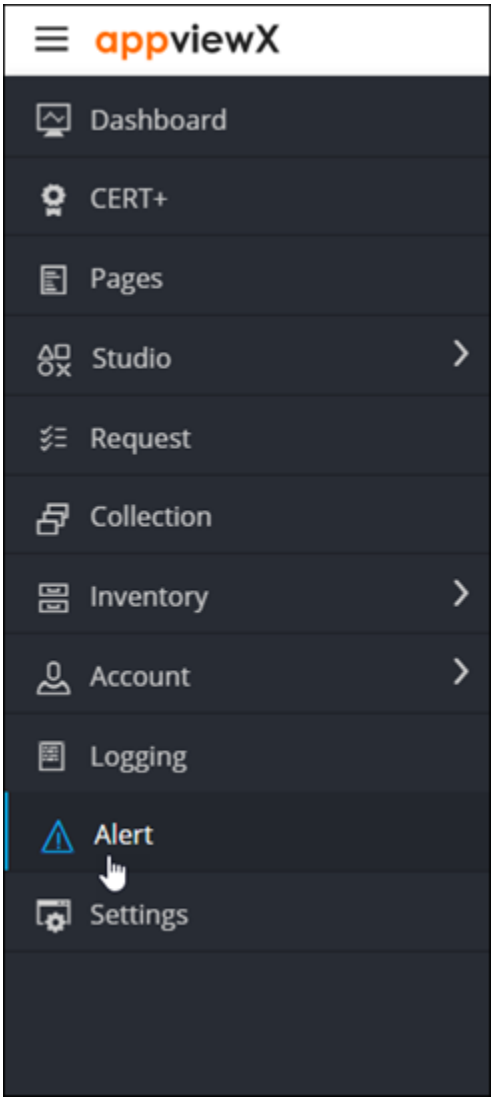
For the ADC alerts, the page displays the following details:

Field	Description
Timestamp	Date and time at which the event, which triggered the alert, occurred.
ID	Alert ID
Event type	Type of the event that triggered the alert.
Severity	Alert severity. AppViewX identifies the following severity levels (as described above): • Critical • Fatal • Major • Minor
Category	Alert category.
Devices	Name of the device, if the alert is to notify of a device-related activity.
Applications	Application that triggered the alert.
Purpose/Usage	Purpose of the alert.
Alert detail	Description of the alert.

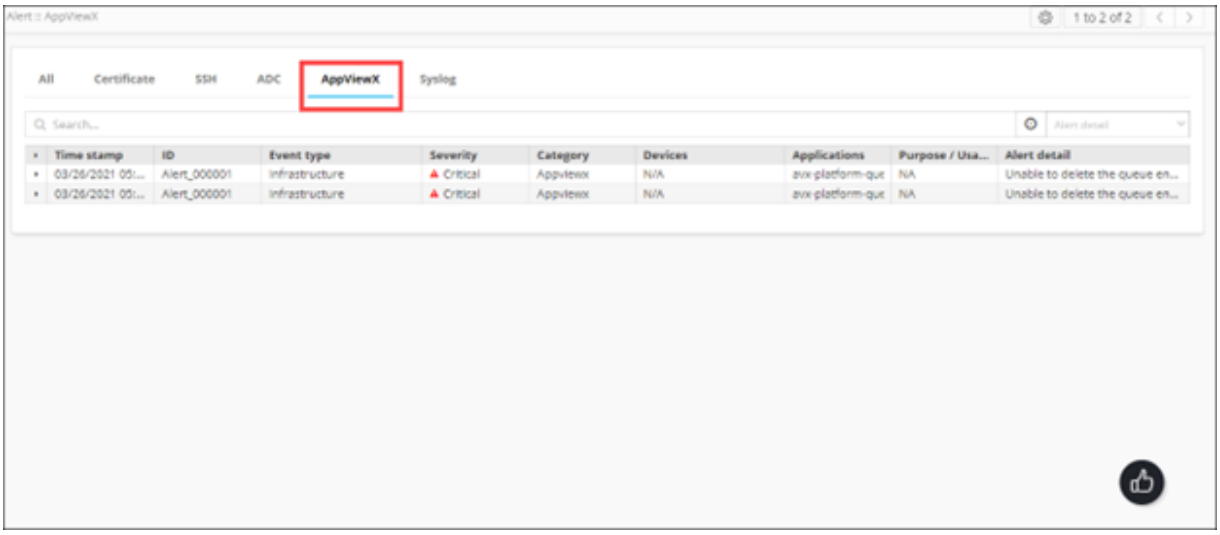
Viewing AppViewX Alerts

To view the AppViewX alerts:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the icon.
2. From the menu displayed, click **Alert**.



   The **Alert :: All** page is displayed (by default).
3. On the **Alert :: All** page, click the **AppViewX** tab.
   The **Alert :: AppViewX** page is displayed.



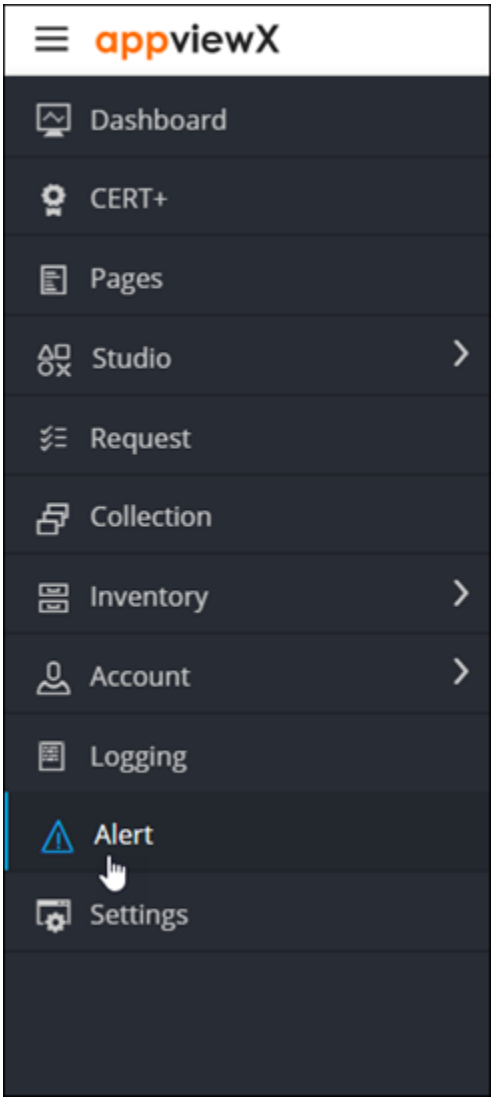
For the AppViewX alerts, the page displays the following details:

Field	Description
Timestamp	Date and time at which the event, which triggered the alert, occurred.
ID	Alert ID
Event type	Type of the event that triggered the alert.
Severity	Alert severity. AppViewX identifies the following severity levels (as described above): • Critical • Fatal • Major • Minor
Category	Alert category.
Devices	Name of the device, if the alert is to notify of a device-related activity.
Applications	Application that triggered the alert.
Purpose/Usage	Purpose of the alert.
Alert detail	Description of the alert.

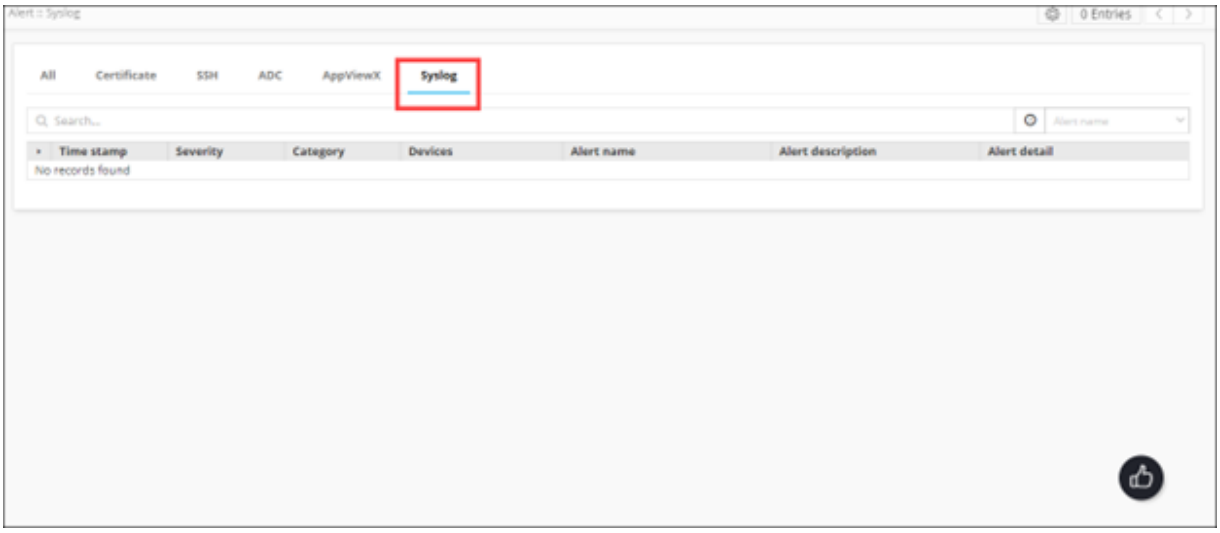
Viewing Syslog Alerts

To view the Syslog alerts:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Alert**.



   The **Alert :: All** page is displayed (by default).
3. On the **Alert :: All** page, click the **Syslog** tab.
   The **Alert :: Syslog** page is displayed.



For the Syslog alerts, the page displays the following details:

Field	Description
Timestamp	Date and time at which the event, which triggered the alert, occurred.
ID	Alert ID
Event type	Type of the event that triggered the alert.
Severity	Alert severity. AppViewX identifies the following severity levels (as described above): • Critical • Fatal • Major • Minor
Category	Alert category.
Devices	Name of the device, if the alert is to notify of a device-related activity.
Applications	Application that triggered the alert.
Purpose/Usage	Purpose of the alert.
Alert detail	Description of the alert.

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.

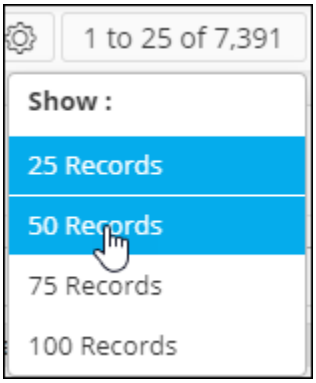
To set the record count preference:

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

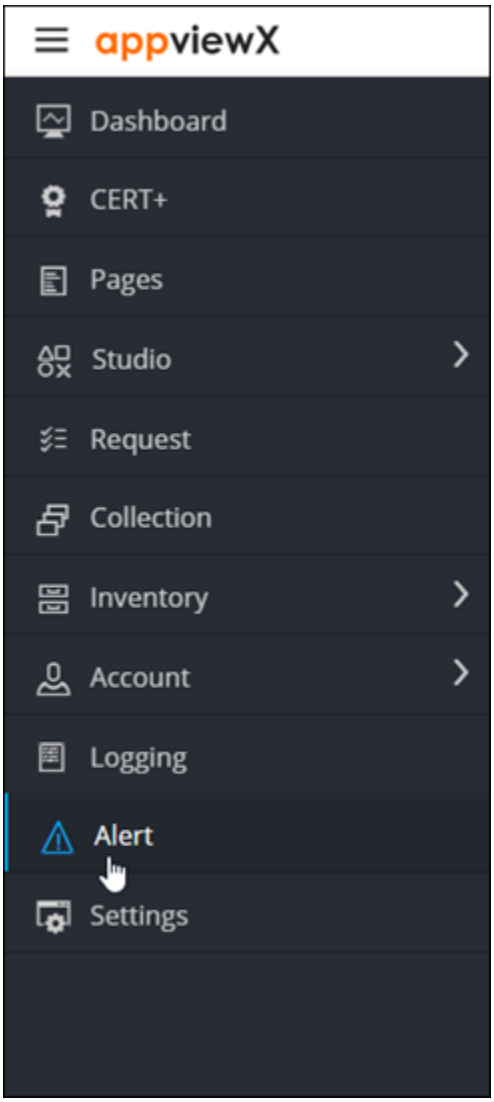
Configuring Certificate Alerts

Certificate alerts are generated to notify users of certificate events that require the user to take a remedial action. Certificate alerts are sent when:

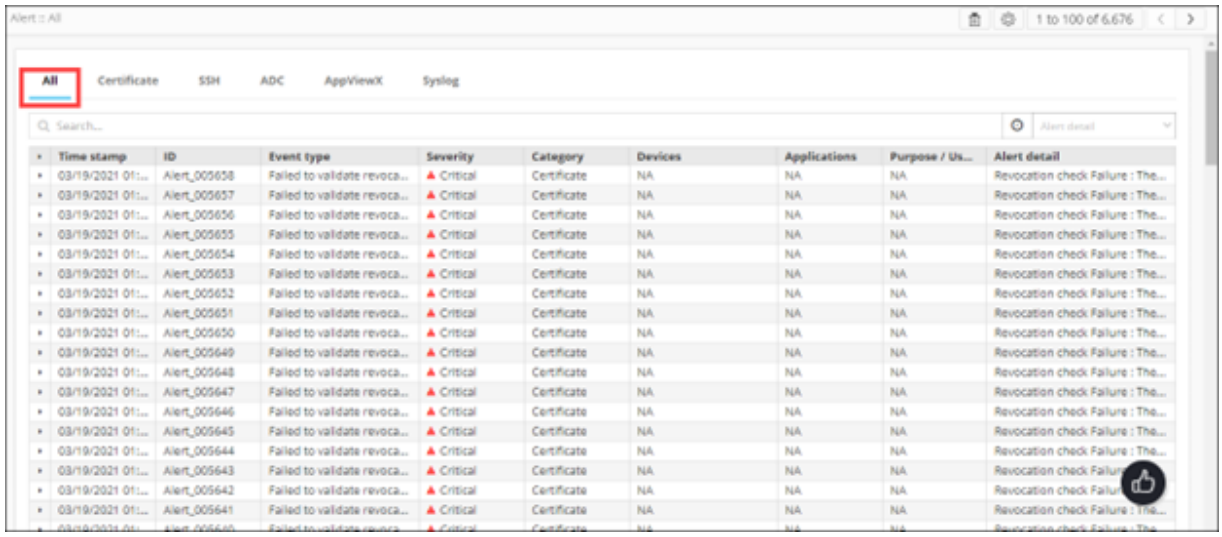
- Certificates need to be validated
- Certificates are set to expire
- Certificates cannot be synchronized

To configure certificate alerts:

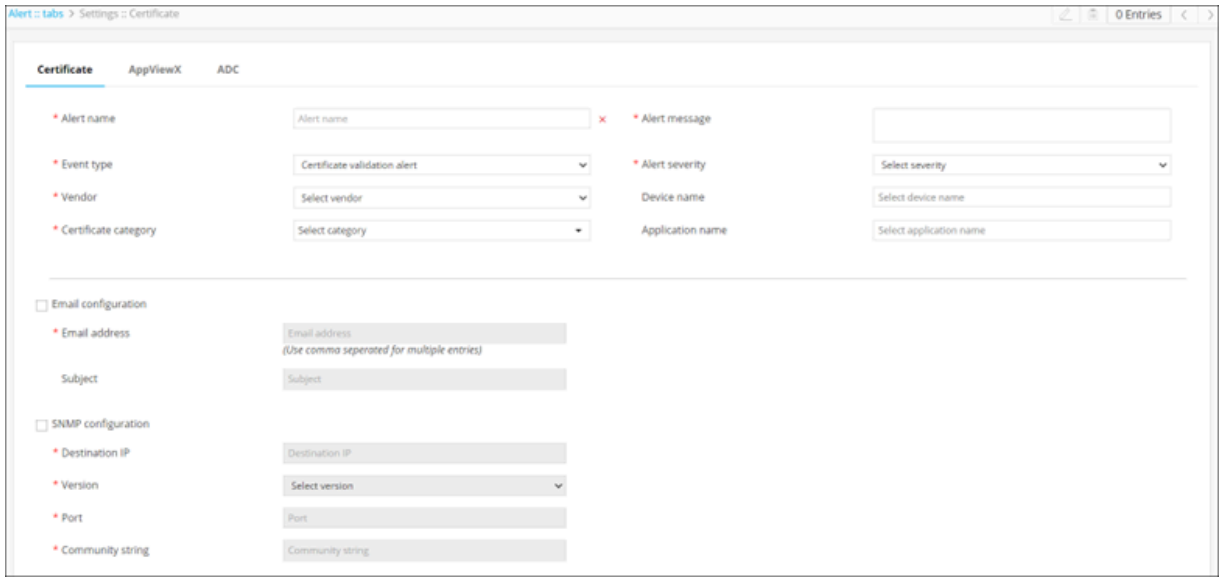
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the  icon.
2. From the menu displayed, click **Alert**.



The **Alert :: All** page is displayed (by default).



3. From the top-right corner of the screen, click  .
4. The **Settings :: Certificate** page is displayed, with the **Certificate** tab open by default.



5. To configure certificate alerts, enter the following details:

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.
All * marked fields are mandatory.	

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.

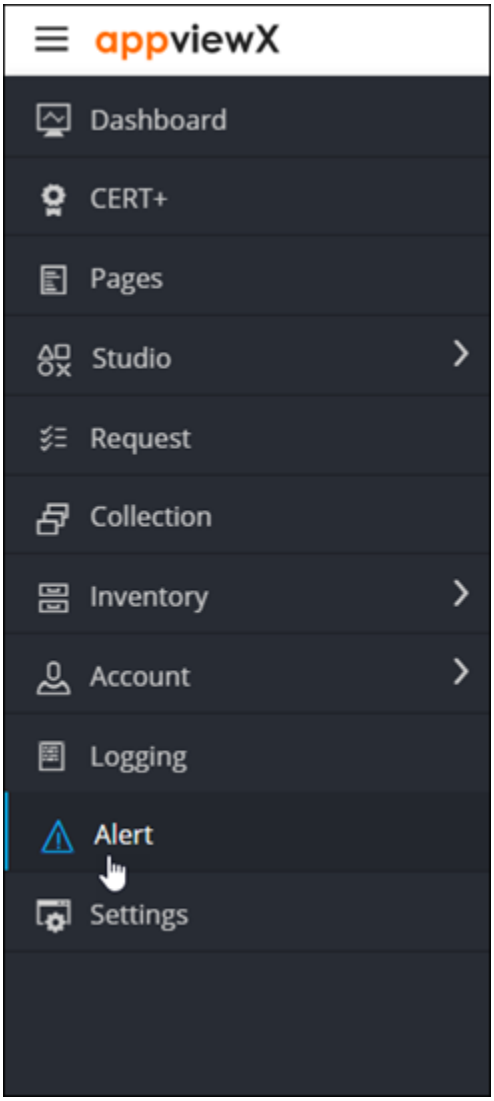
Configuring Syslog Alerts

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 syslogs. However, devices tend to generate a huge amount of

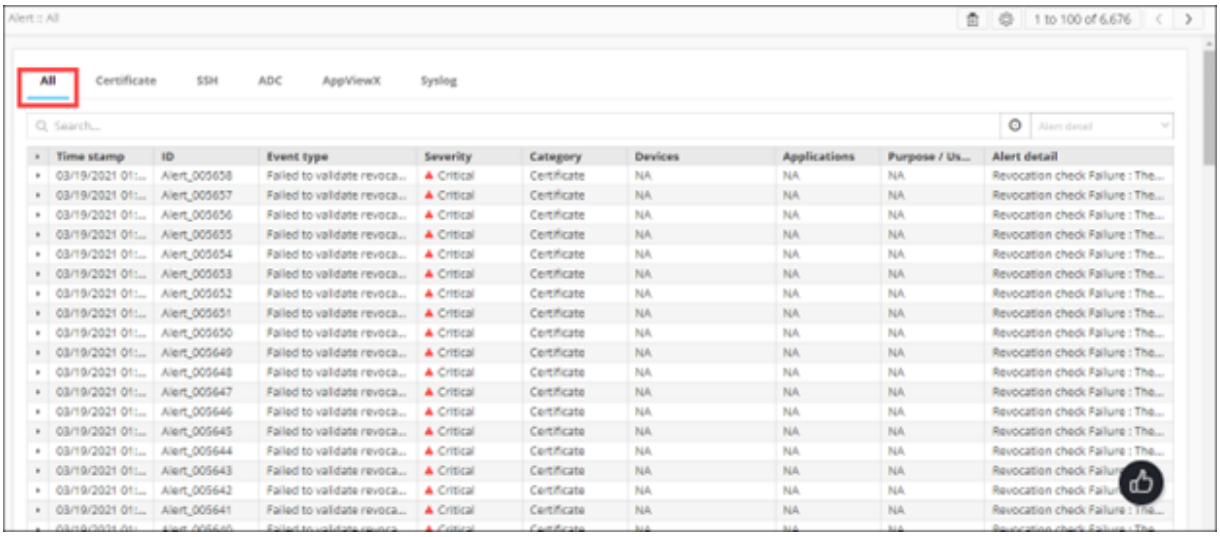
data. To resolve this, a Syslog Alert is a convenient way to notify about specific syslog information that is of importance to you.

To configure syslog alerts:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Alert**.



The **Alert :: All** page is displayed (by default).

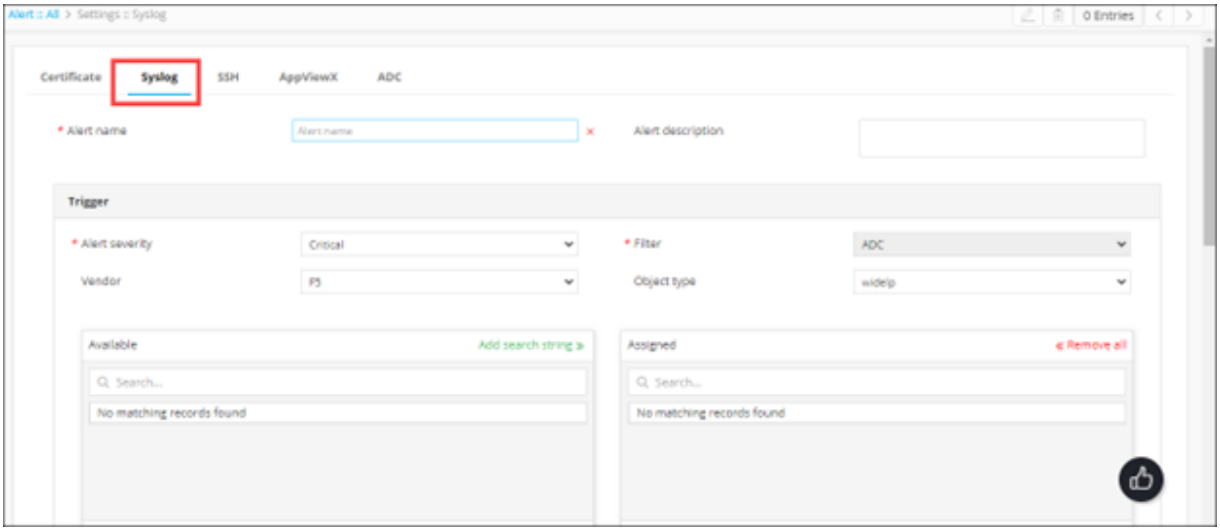


3. From the top-right corner of the screen, click the  icon.

   The **Settings :: Certificate page** is displayed.

4. To configure Syslog alerts, click **Syslog**.

   The **Settings :: Syslog** page is displayed.



5. Enter the following details:

Field	Description
***Alert name**	Enter the name you want to give this alert.
Alert description	Enter a description for the alert.

Field	Description
All * marked fields are mandatory.	

6. In the **Trigger** section, enter the following details:

Table 1.

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.
Assigned	To add an object to the Assigned column, click the check box corresponding to that object.
Regex	Enter single/multiple regex patterns/strings.

Field	Description
	Note: When entering multiple regex patterns/strings, separate the regex strings using commas. The comma works as the **BOOLEAN AND** operator.
All * marked fields are mandatory.	

7. In the **Action** section, enter the following details:

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  . 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 .

8. To send the Syslog alert as an email, execute the steps for configuring SMTP for email alerting.
9. Enter the following details:

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.

Field	Description
Email configuration	To send the syslog alert as an email, enter a subject line.
All * marked fields are mandatory.	

10. To use the Simple Network Management Protocol (SNMP) to send the alert, enter the following details:

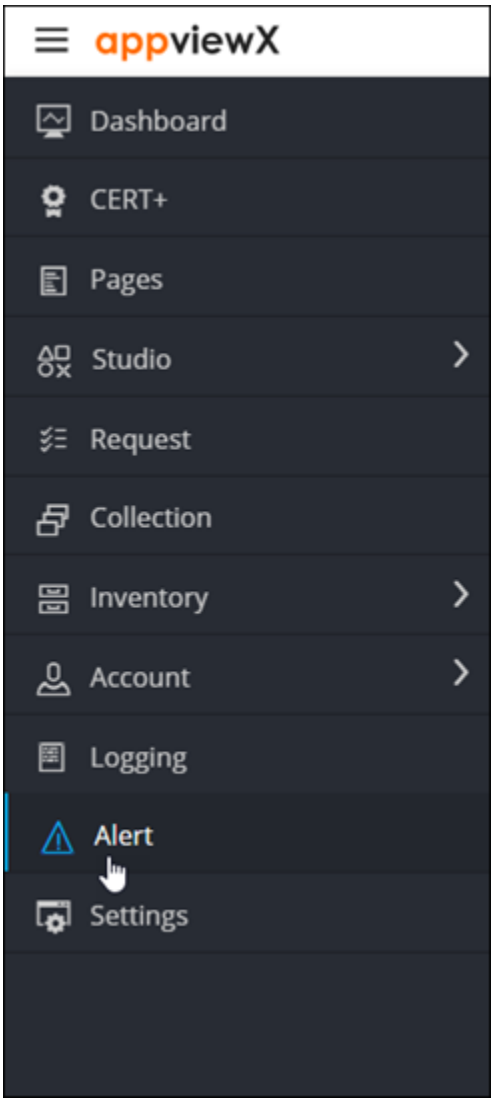
Field	Description
SNMP configuration	To use the Simple Network Management Protocol for sending the alert, select this check box.
***Destination IP**	Enter the destination IP address for the alert.
***Version**	From the drop-down menu, from the following options, select the SNMP version to be used: • 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 reque device.
All * marked fields are mandatory.	

11. To save the Syslog alerts configuration details, click **Add**.
    The saved details are displayed in the table shown at the bottom of the screen.

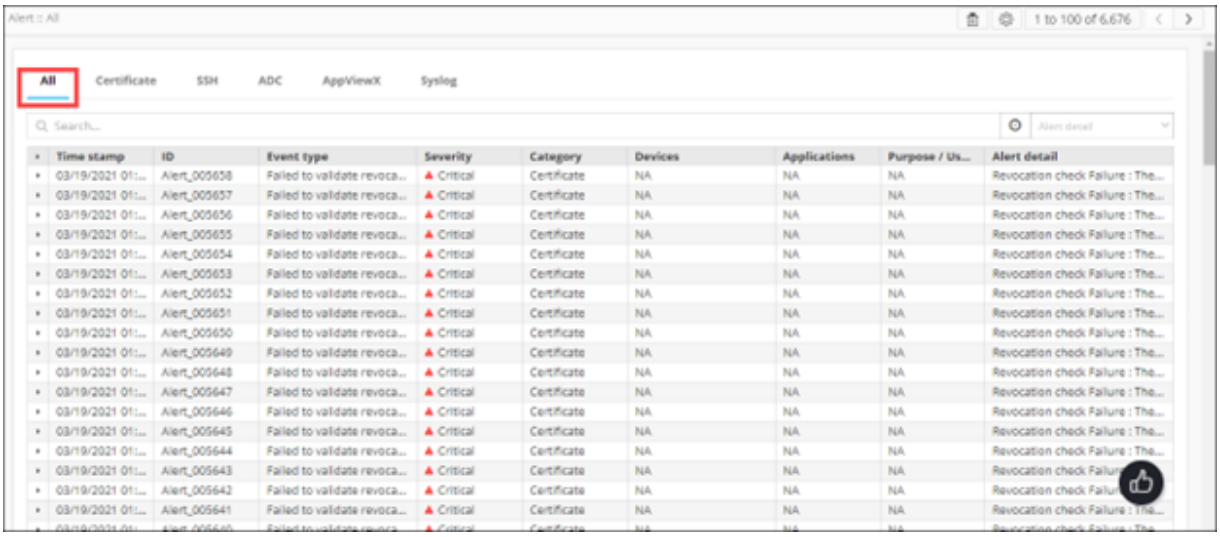
Configuring SSH Alerts

To configure syslog alerts:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the
   ☰ icon.
2. From the menu displayed, click **Alert**.



The **Alert :: All** page is displayed (by default).

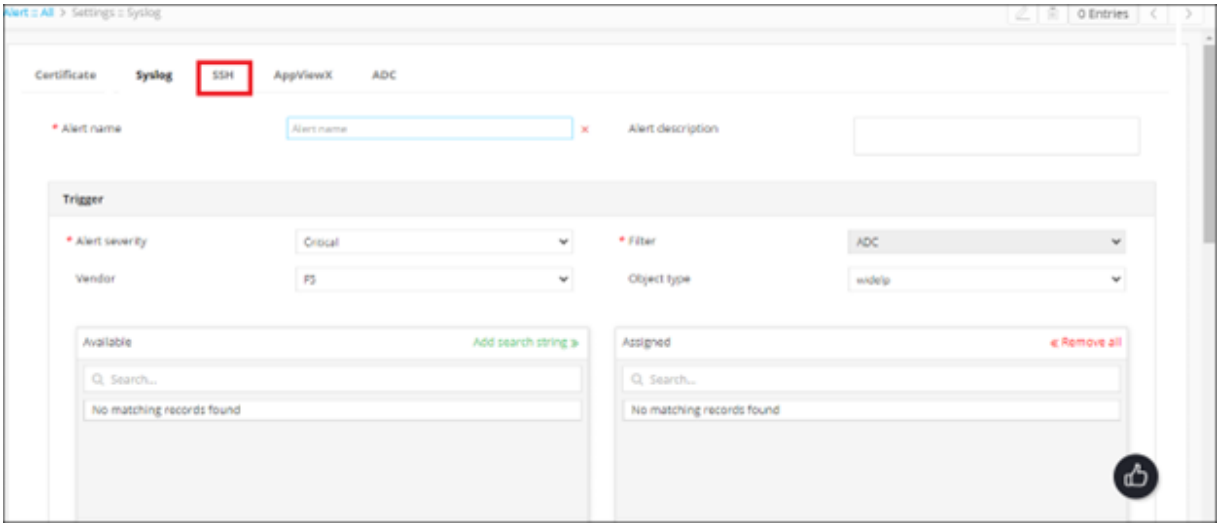


3. From the top-right corner of the screen, click  .

   The **Settings :: Certificate** page is displayed.

4. To configure SSH alerts, click **SSH**.

   The **Settings :: SSH** page is displayed.



5. Enter the following details:

Field	Description
***Alert name**	Enter the name you want to give this alert.
***Alert severity**	From the drop-down menu, select a severity for the alert from one of the following op

Field	Description
	• Critical • Fatal • Major • Minor • Notification
***Event type**	From the drop-down menu, select the event type that will trigger the alert: • SSH key expiry alert • Compliance alert • SSH key push failure alert • SSH discovery failure alert • SSH key deletion alert • SSH host modify/delete alert
***Expires in (days)**	**Note:** This field is applicable only for the **SSHkey expiry alert**. From the drop-down menu, select the number of days until the SSH key expires. The when this value is reached.
***SSH keygroup**	**Note:** This field is applicable only for the **Compliance alerts**, **SSHkey push f** From the drop-down menu, select the key group to be used as the basis for the alert.
***Key alert criterion**	**Note:** This field is applicable only for the **SSH key push failure alert** and the Select the keys you want to include in the alert, from the following options: • Logged in user keys • All user keys
***SSH host group**	**Note:** This field is applicable only for the **SSH host modify/delete alert** only. Enter the host group you want to use as the basis for the alert.
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 sy

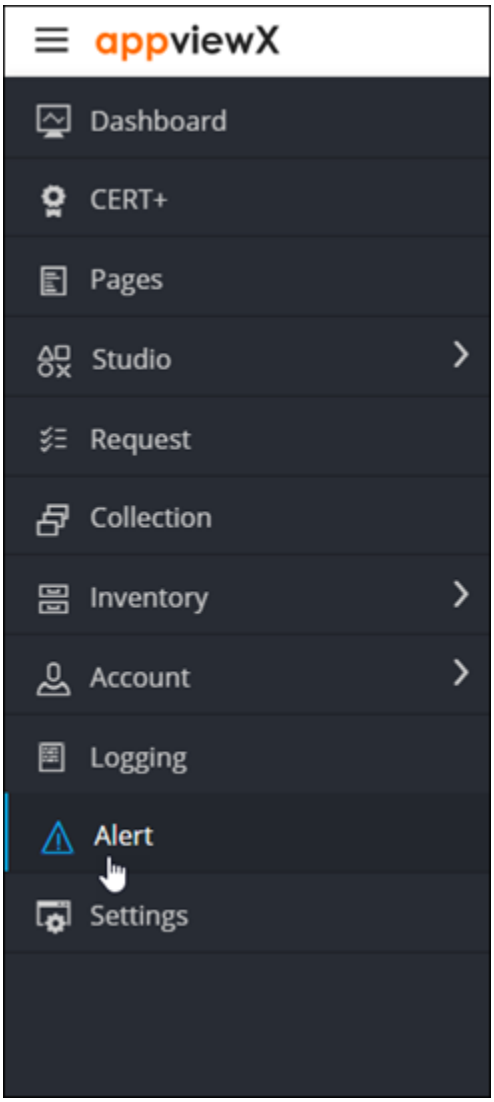
Field	Description
	Note: Separate multiple email addresses with a comma.
Subject	To send the syslog alert as an email, enter a subject line.
SNMP configuration	To use the Simple Network Management Protocol for sending the alert, select this ch
***Destination IP**	Enter the destination IP address for the alert.
***Version**	From the drop-down menu, from the following options, select the SNMP version to be • 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 requested information on the device.
All * marked fields are mandatory.	

6. To save the SSH alerts configuration details, click **Add**.
   The saved details are displayed in the table shown at the bottom of the screen.

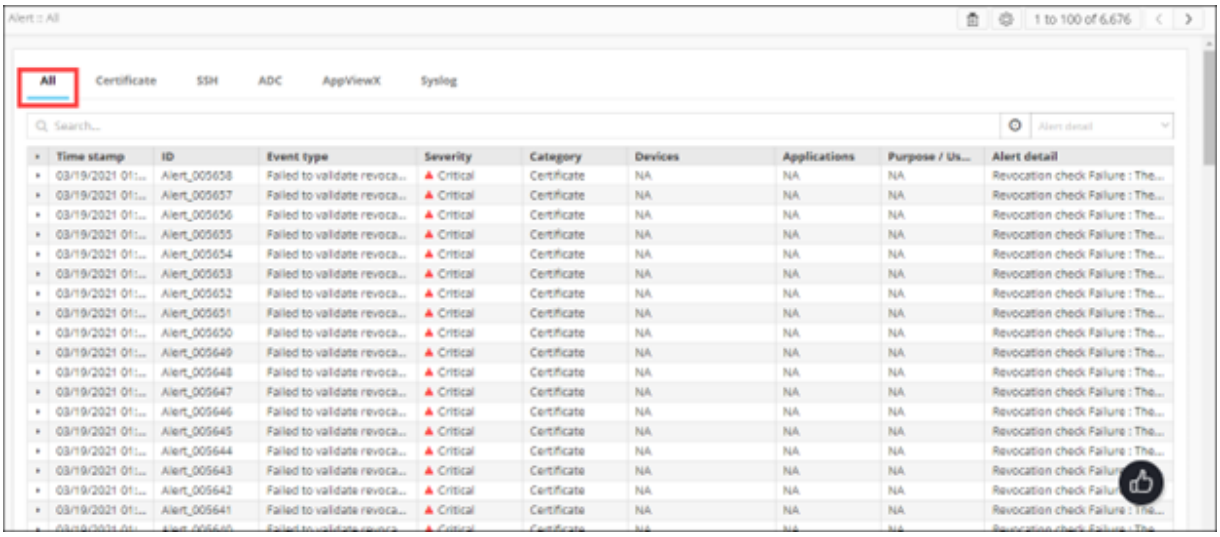
Configuring AppViewX Alerts

To configure AppViewX alerts:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the
    icon.
2. From the menu displayed, click **Alert**.



The **Alert :: All** page is displayed (by default).

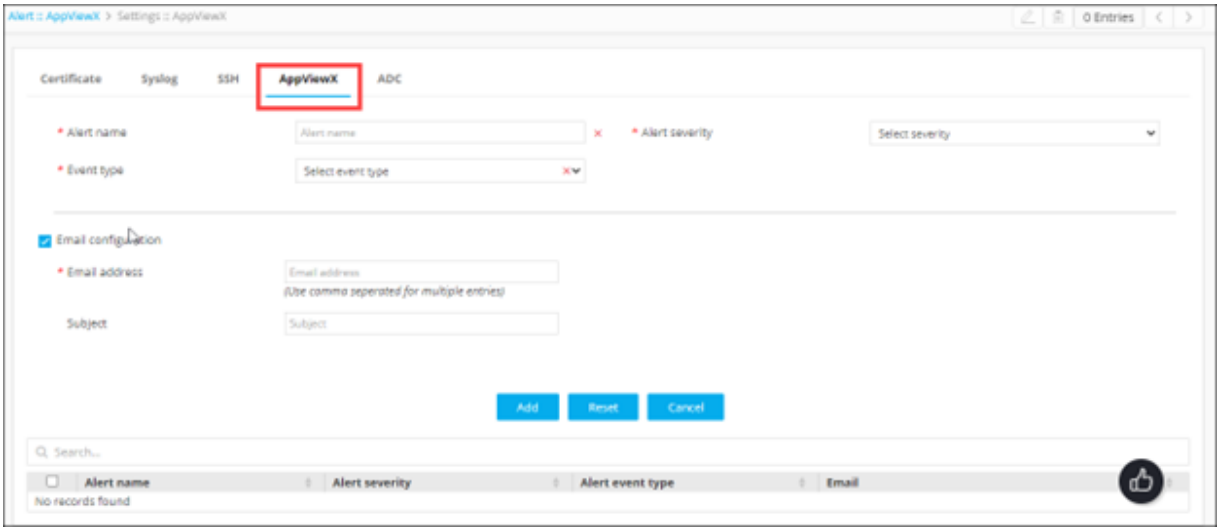


3. From the top-right corner of the screen, click  .

   The **Settings :: Certificate** page is displayed.

4. To configure AppViewX alerts, click the AppViewX tab.

   The **Settings :: AppViewX** page is displayed.



5. Enter the following details:

Field	Description
***Alert name**	Enter the name you want to give this alert.
***Alert severity**	From the drop-down menu, select a severity for the alert from the following options:

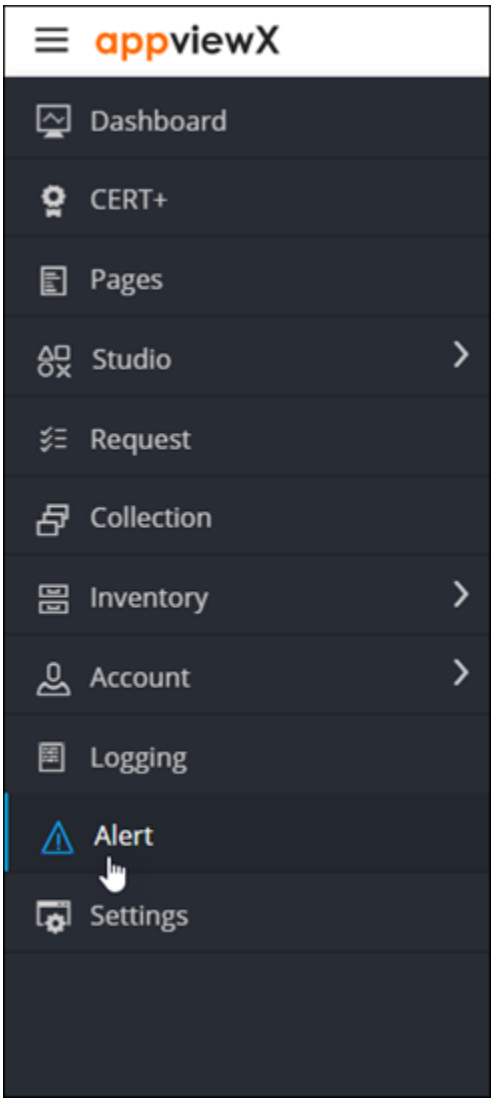
Field	Description
	• Critical • Fatal • Major • Minor • Notification
***Event type**	From the drop-down menu, from the following options, select the event type that will trigg • Infrastructure • Application Discovery
Email configuration	To send the certificate alert as an email, select this check box. **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 ce **Note:** Separate multiple email addresses with a comma.
Subject	To send the certificate alert as an email, enter a subject line.
All * marked fields are mandatory.	

6. 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.

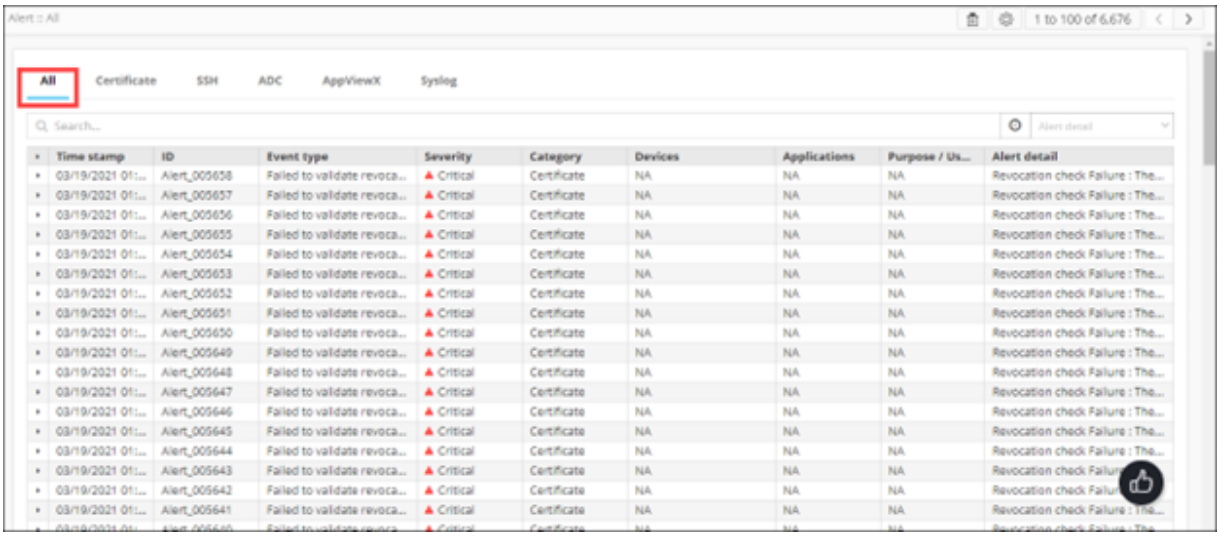
Configuring ADC Alerts

To configure ADC alerts:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the
   ☰ icon.
2. From the menu displayed, click **Alert**.



The **Alert :: All** page is displayed (by default).

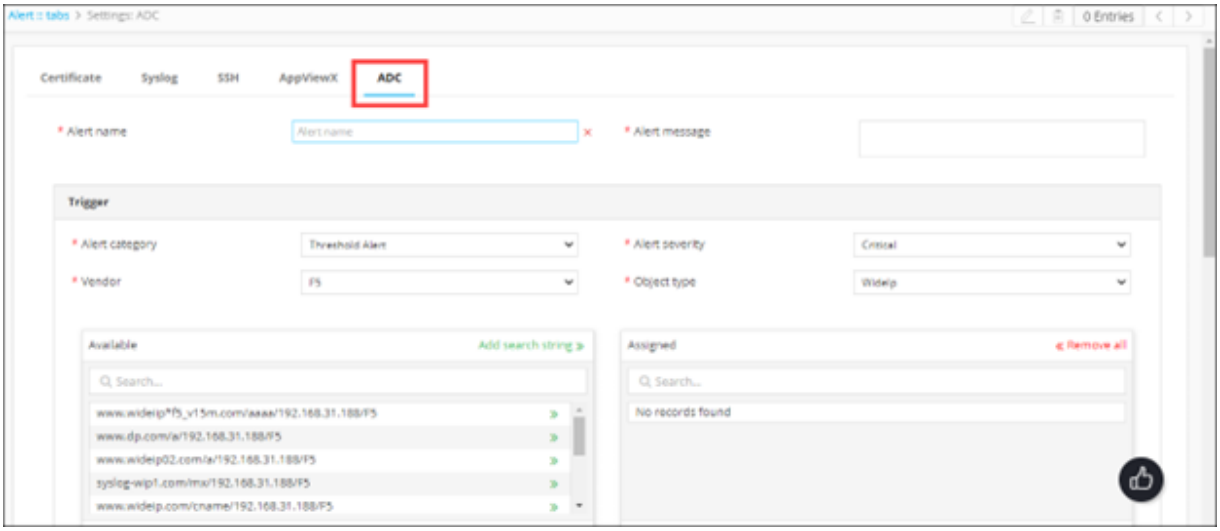


3. From the top-right corner of the screen, click  .

   The **Settings :: Certificate** page is displayed.

4. To configure ADC alerts, click **ADC**.

   The **Settings :: ADC** page is displayed.



5. Enter the following details:

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.

Field	Description
All * marked fields are mandatory.	

6. In the **Trigger** section, enter the following details:

Field	Description
***Alert category**	From the drop-down menu, select one of the following alert categories: • Threshold alert • Application alert • Device alert
***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 s
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 objec 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 exist match your criteria. To do this: a. In the **Available** section, in the **Search** field, enter the search criteria. b. Click **Add search string**.

Field	Description
	Note: The benefit of using a search string rather than selecting devices manu continues to work in the background and auto-assigns all new devices that ma
Assigned	To add an object to the Assigned column, click the check box corresponding to that c

7. In the **Alert condition** section, enter the following details:

Table 2.

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
All * marked fields are mandatory.	

Note: This section is applicable only for the Threshold Alert category.

8. 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 +.
   - To delete a condition, click .

9. In the **Action** section, to send the syslog alert as an email, execute the steps for configuring SMTP for email alerting.
10. Enter the following details:

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.
All * marked fields are mandatory.	

11. To use the Simple Network Management Protocol (SNMP) to send the alert, enter the following details:

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.
All * marked fields are mandatory.	

12. 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. Navigate to the Settings page for the alert you want to edit (certificate, syslog, SSH, AppViewX, or ADC).
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  .
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. Navigate to the Settings page for the alert you want to delete (certificate, syslog, SSH, AppViewX, or ADC).
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  .
5. In the **Confirmation** dialog box, click **Yes**.

Searching for Alerts

AppViewX lets you search for alerts in two ways:

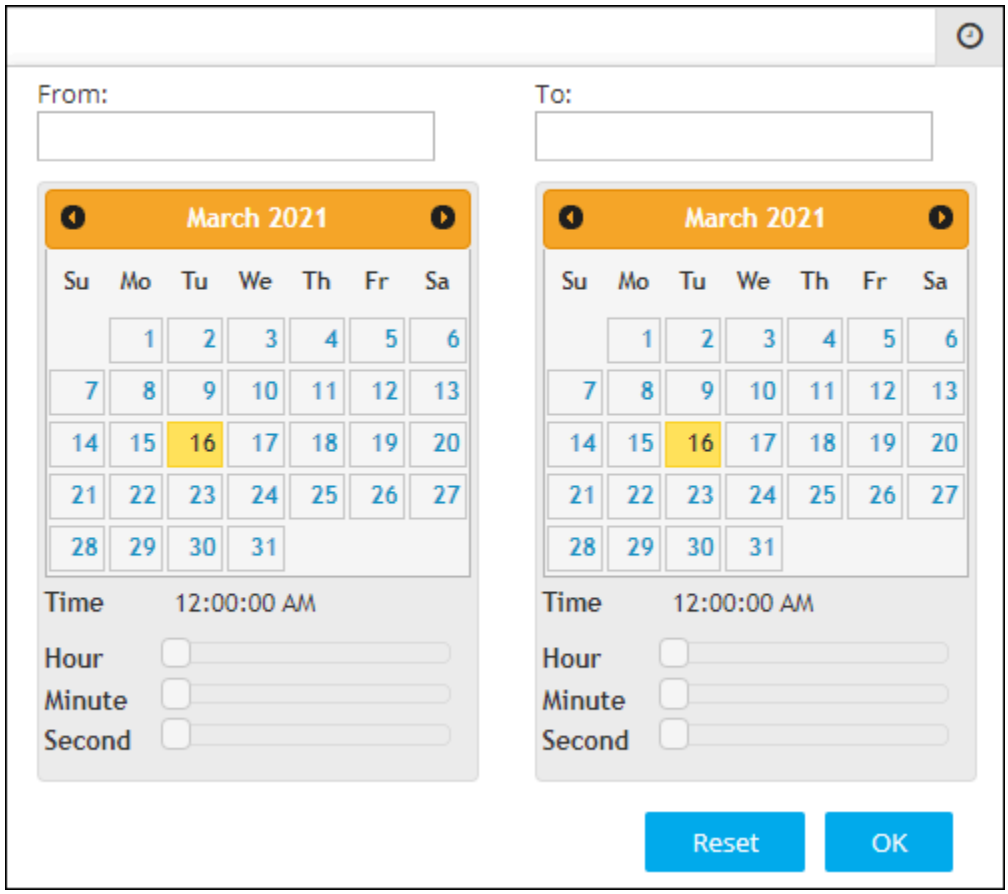
- Based on a timestamp
- Based on the values recorded for each alert

- 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  .
   Widgets to select the date and time are displayed.

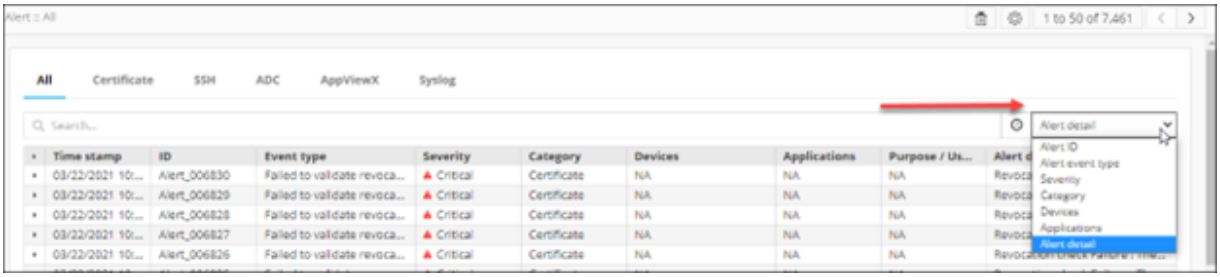


2. To select a date range, in the **From** and **To** fields, select the required dates.
3. To set a time, use the **Hour**, **Minute**, and **Second** slider controls.
4. Click **OK**.
5. The page is updated to display alerts from the selected timestamp.

> **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**.



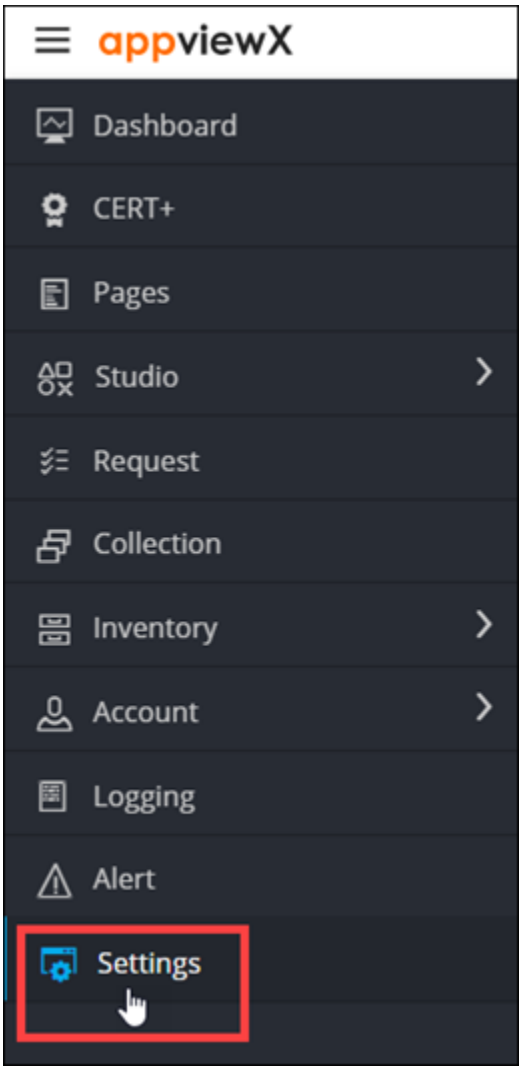
2. In the **Search** field , enter the search value. For our example, in the Search field, enter the required alert ID.
   The page is updated to display alerts that fulfil the search criteria.

Purging Alerts

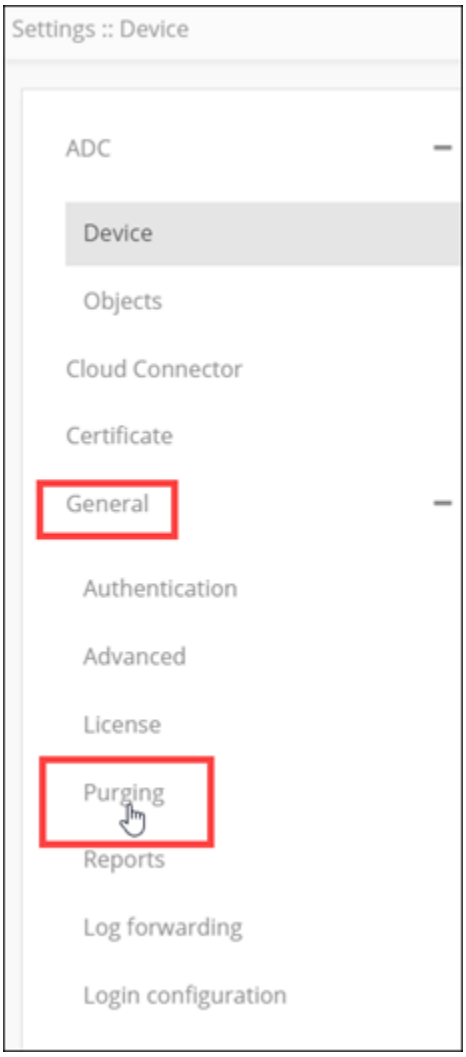
With a large number of alerts being recorded each day, a system can soon become vulnerable to threats like compromise of confidential information, a surplus of outdated information, and so on. For security reasons, regular purging of old data comes as a highly recommended practice.

To enable purging of alert records:

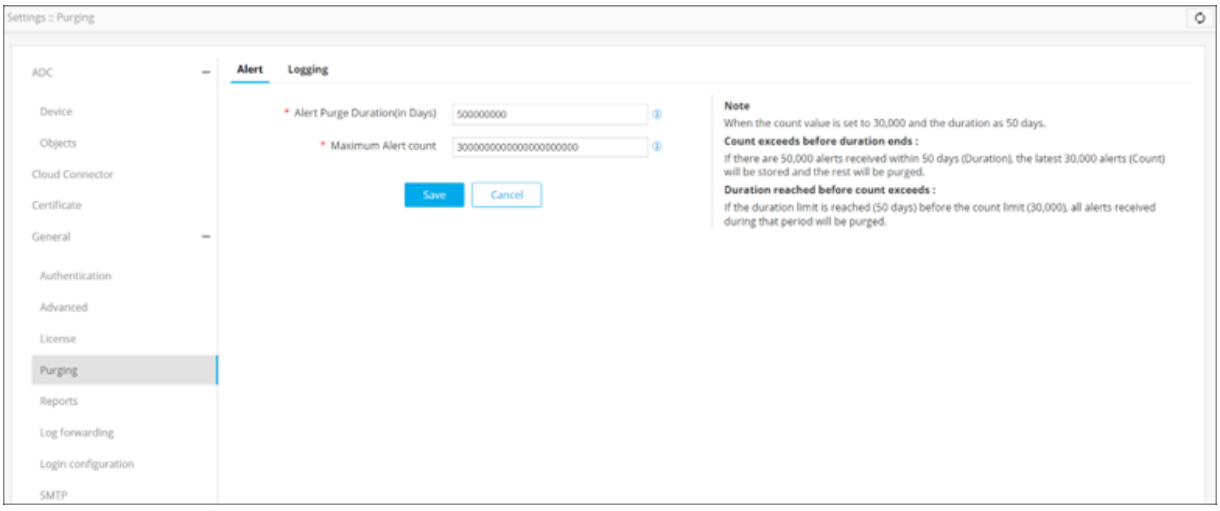
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **Purging**.



The **Settings :: Purging** screen is displayed, with the **Alert** tab open by default



.

5. Enter the following details:

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.
All * marked fields are mandatory.	

Note: Excess alerts will be purged even if the maximum alert count is exceeded before the next purging cycle is scheduled.

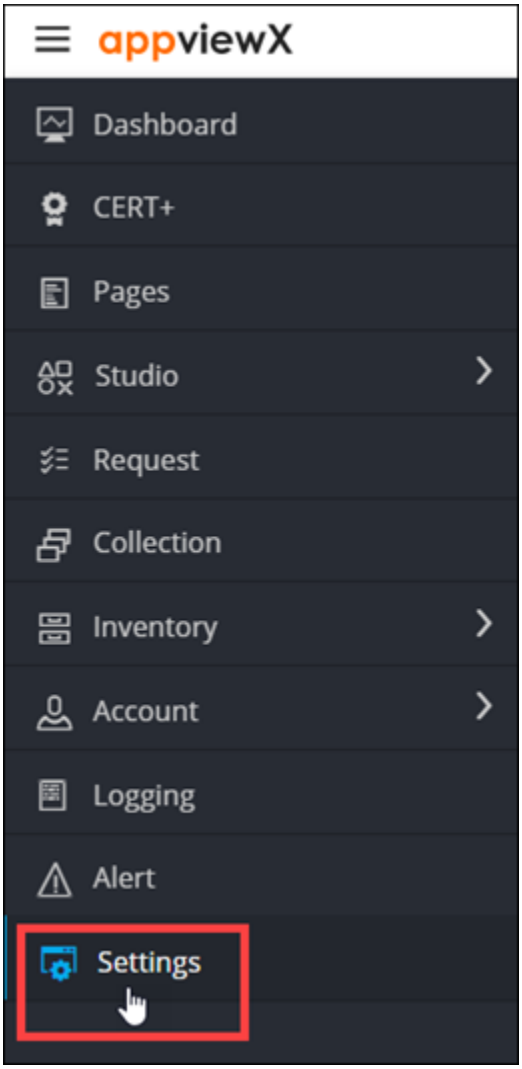
6. Click **Save**.

Chapter 10: Managing Licenses

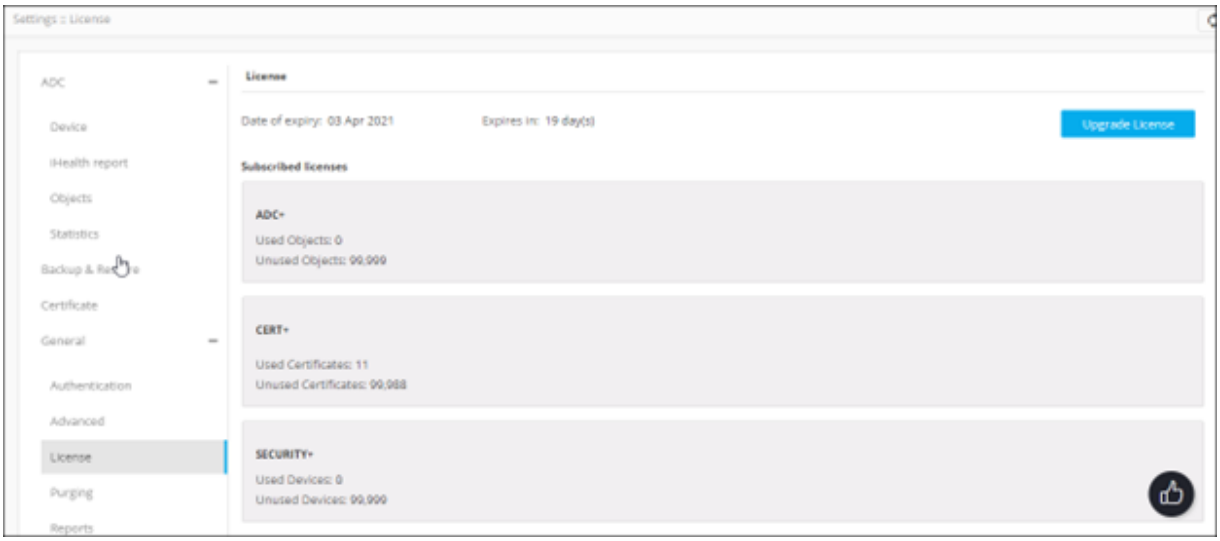
Viewing Licensing Details

To view the list and details of subscribed licenses:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General** and select **License**.
   The **Settings :: License** page is displayed.



The page shows the following details:

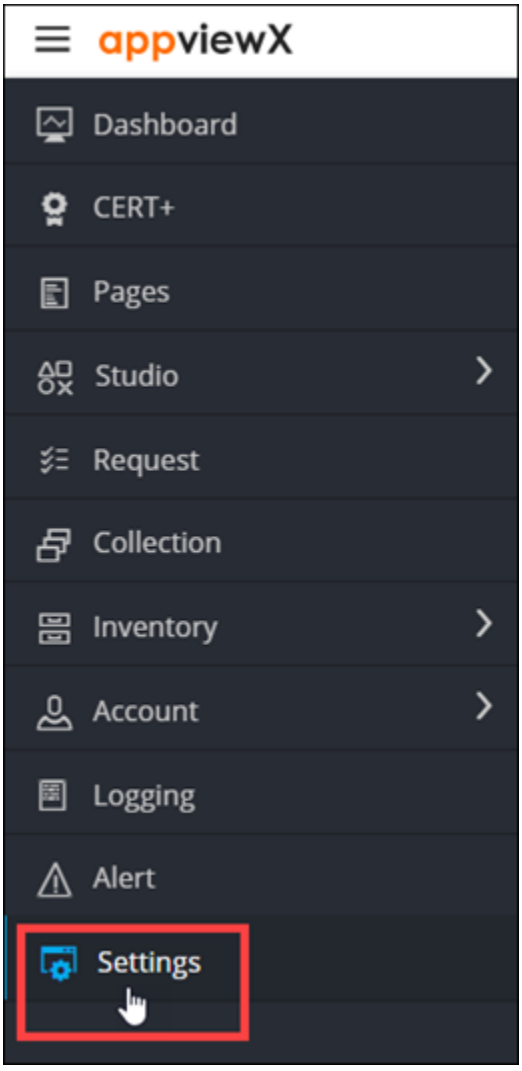
License Detail	Description
Date of expiry	Date of expiry of the licenses
Expires in	Number of days till the license expires
Subscribed licenses	This includes the details of licenses of all AppViewX products.
Used Objects (for ADC+ licenses)	Each ADC+ license subscription allows the user a fixed number of objects that they ca ADC+ objects currently in use.
Unused Objects (For ADC+ licenses)	Each ADC+ license subscription allows the user a fixed number of objects that they ca ADC+ objects left for use.
Used Certificates (for CERT + licenses)	Each CERT+ license subscription allows the user a fixed number of certificates that the license. This is the number of CERT+ certificates currently being managed by the licen
Unused Certificates (for CERT+ licenses)	Each CERT+ license subscription allows the user a fixed number of certificates that the license. This is the number of CERT+ certificates left.
Used Devices (for SECURITY+ licenses)	Each SECURITY+ license subscription allows the user a fixed number of devices that subscription. This is the number of devices currently in use.
Unused Devices (for SECURITY+ licenses)	Each SECURITY+ license subscription allows the user a fixed number of devices that subscription. This is the number of devices left for use.

Upgrading Licenses

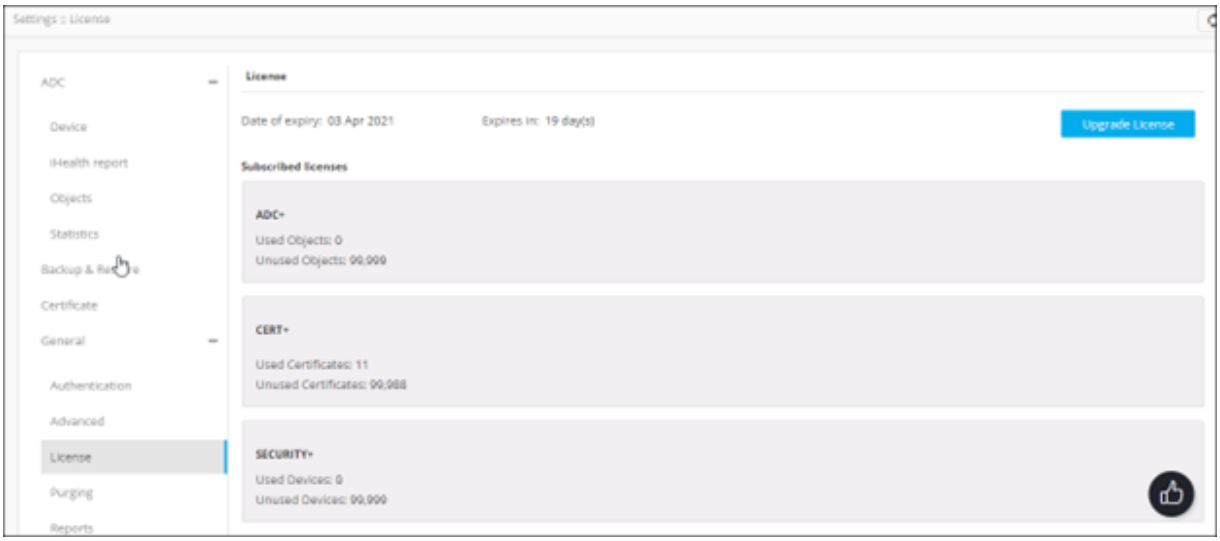
Note: AppViewX blocks the usage of the license if the license has expired. If an organization exceeds the threshold of license (maximum number of ADC+ objects, CERT+ certificates, and/or SECURITY+ devices allowed), a warning is issued as a reminder. A pop-up warning is issued for both the scenarios.

To upgrade a license:

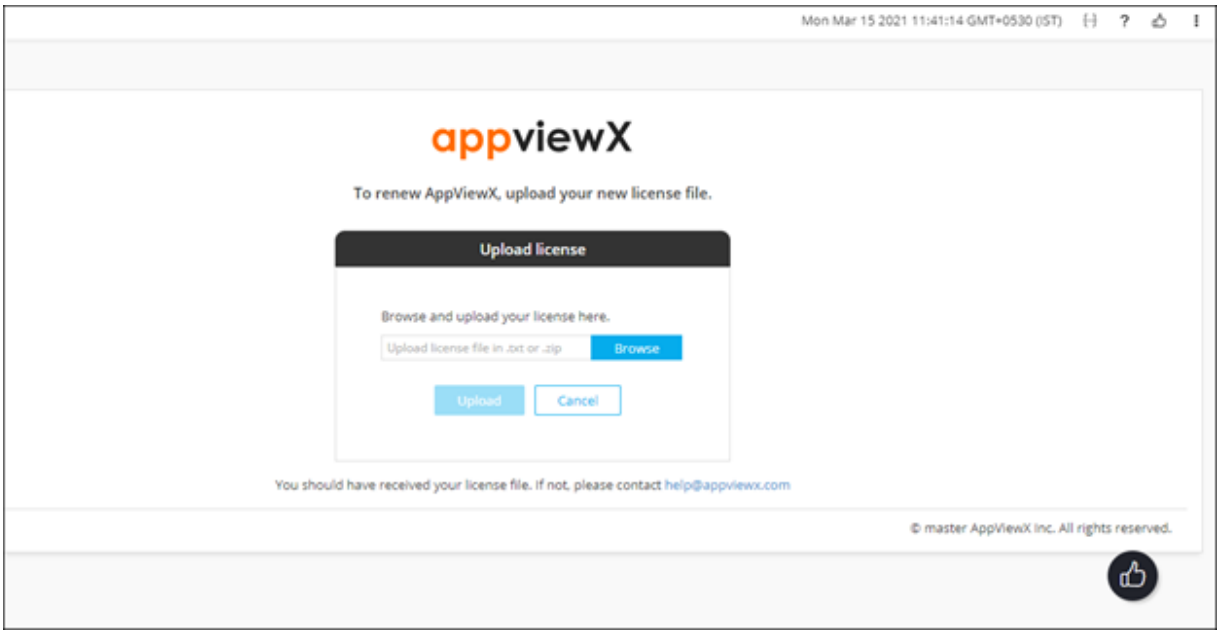
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Settings**.



3. On the **Settings** page, from the navigation pane on the left, click **General** and select **License**.
   The **Settings :: License** page is displayed.



4. 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.



5. 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.

6. Navigate to the location of the license file, select the file , and click **Open**.
7. Click **Upload**.

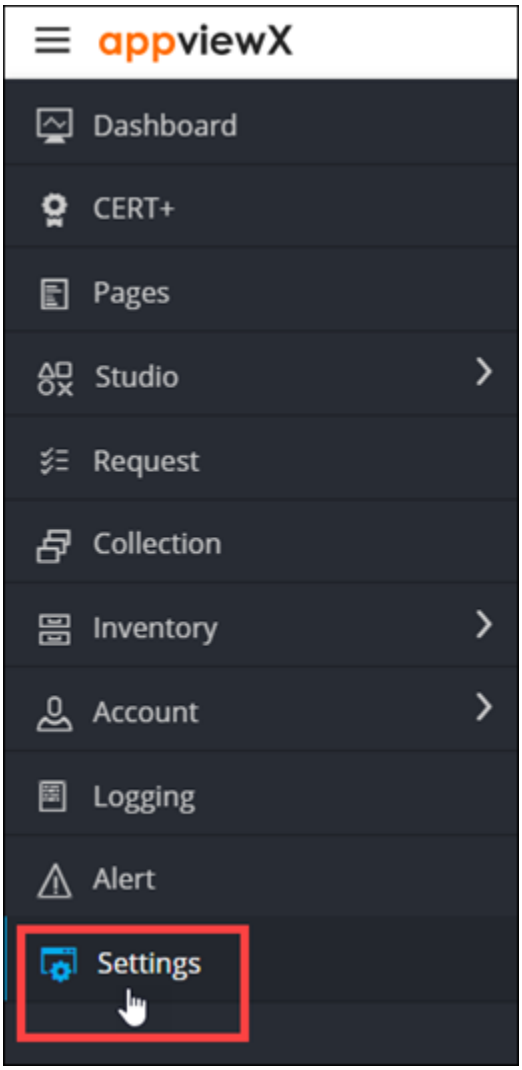
Chapter 11: Customizing the AppViewX User Interface

Customizing the Logo

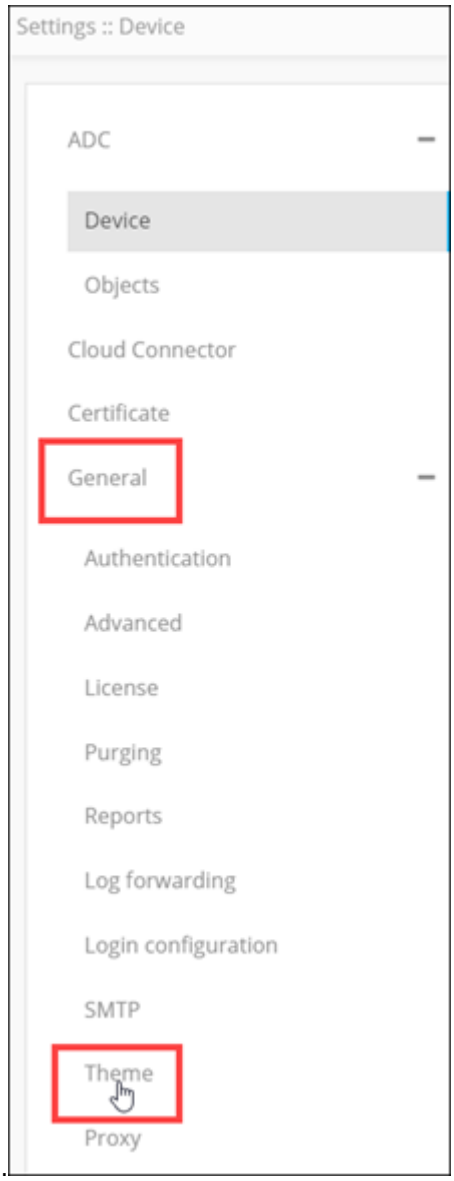
You can replace the AppViewX logo with the logo of your organization.

To add a custom logo:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the icon.
2. From the menu displayed, click **Settings**.

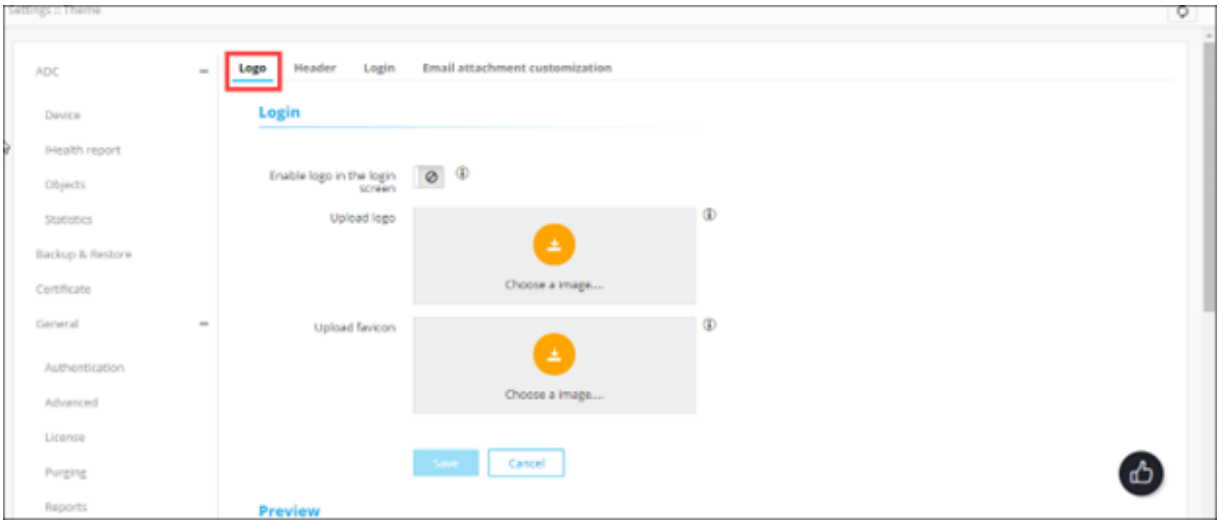


3. On the **Settings** page, from the navigation pane on the left, click **General**.



4. Under **General** settings, click **Theme**.

   The **Settings :: Theme** page is displayed, with the **Logo** tab open by default.



5. In the **Login** section, enter the following details:

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  . 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)

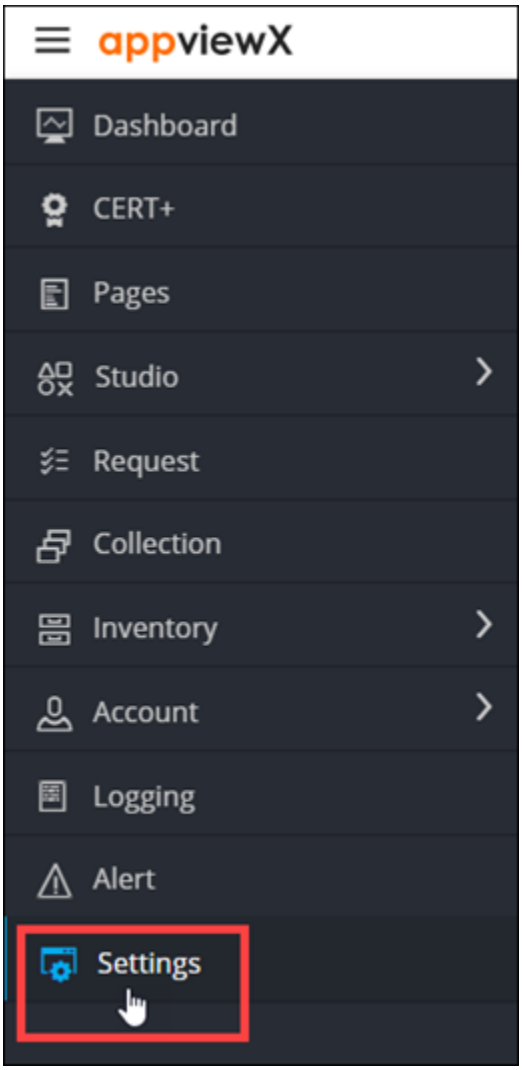
Field	Description
	• Image size: < 5 MB • Recommended image dimensions: 175 X 37 (width X height) c. In the **Confirmation Message** dialog box, click **Yes**.
Upload favicon	**Note:** This field is enabled only when the Enable logo in the toggle screen toggle is turned on. To choose a favicon image: a. Click  . 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)Ima • Image size: < 5MB c. In the **Confirmation Message** dialog box, click **Yes**.

6. In the **Preview** section, view a preview of the login screen after your custom logo and favicon have been uploaded.
7. To apply the changes, click **Save**.

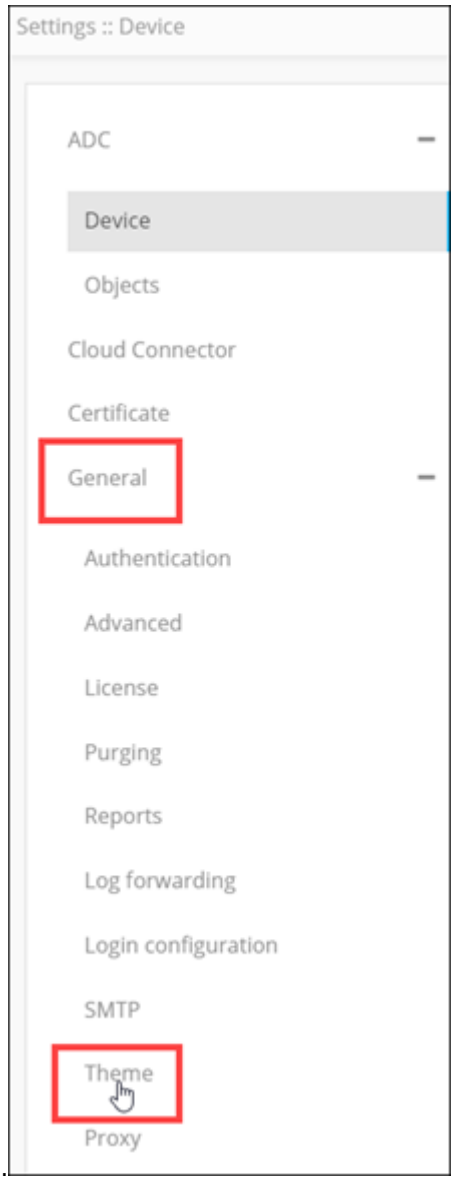
Customizing the Screen Header

To customize the screen header:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Settings**.

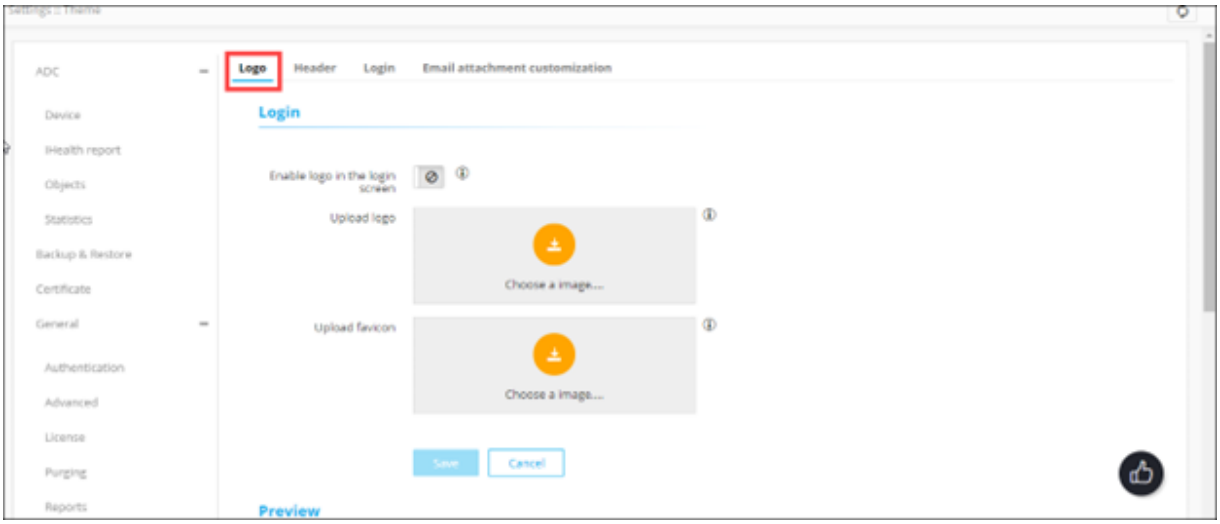


3. On the **Settings** page, from the navigation pane on the left, click **General**.

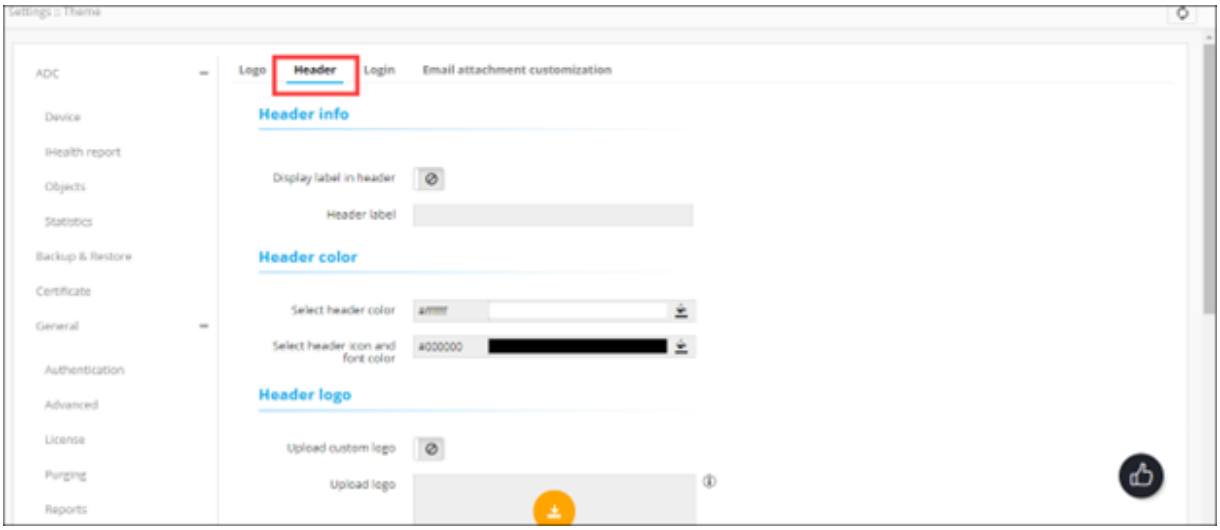


4. Under **General** settings, click **Theme**.

   The **Settings :: Theme** page is displayed, with the **Logo** tab open by default.



5. To customize the screen header, click the **Header** tab.



6. In the **Header Info** section, enter the following details:

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.

7. In the **Header color** section, enter the following details:

Field	Description
Select header color	To set a color for the header text: • Enter the hex code of the required header color. **OR** • To select a color, click  .
Select header icon and font color	To set a color for the header icon and the font: • Enter the hex code of the required color. **OR** • To select a color, click  .

8. In the **Header logo** section, enter the following details:

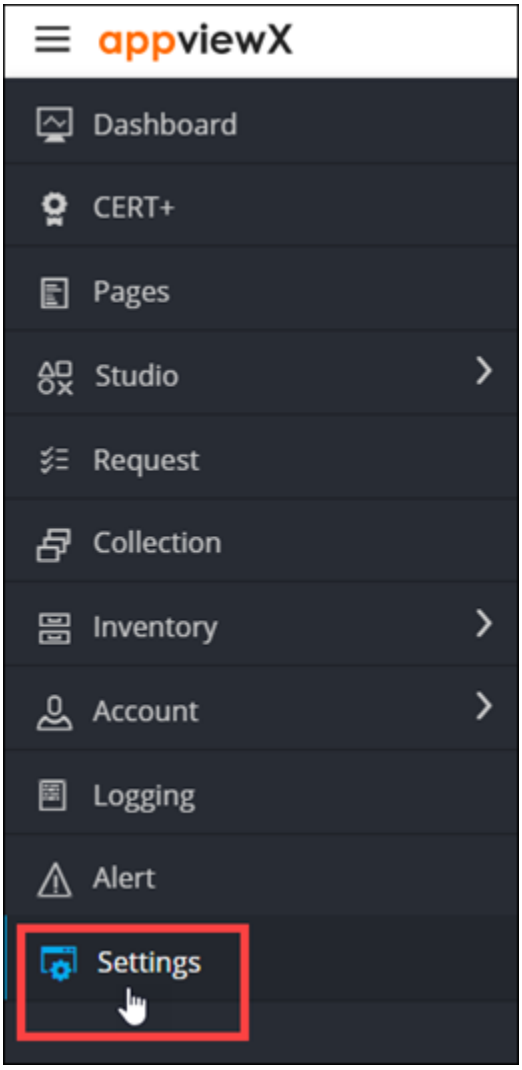
Field	Description
Upload custom logo	To insert a custom logo image in the header, turn on this toggle.
Upload logo	**Note:** This field is enabled only when the Upload custom logo toggle is turned on. To upload a logo image: a. Click  . b. From Windows Explorer, navigate to the location of the image, 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) c. In the **Confirmation Message** dialog box, click **Yes**.

9. In the **Preview** section, view a preview of your header customization.
10. To apply the changes, click **Save**.

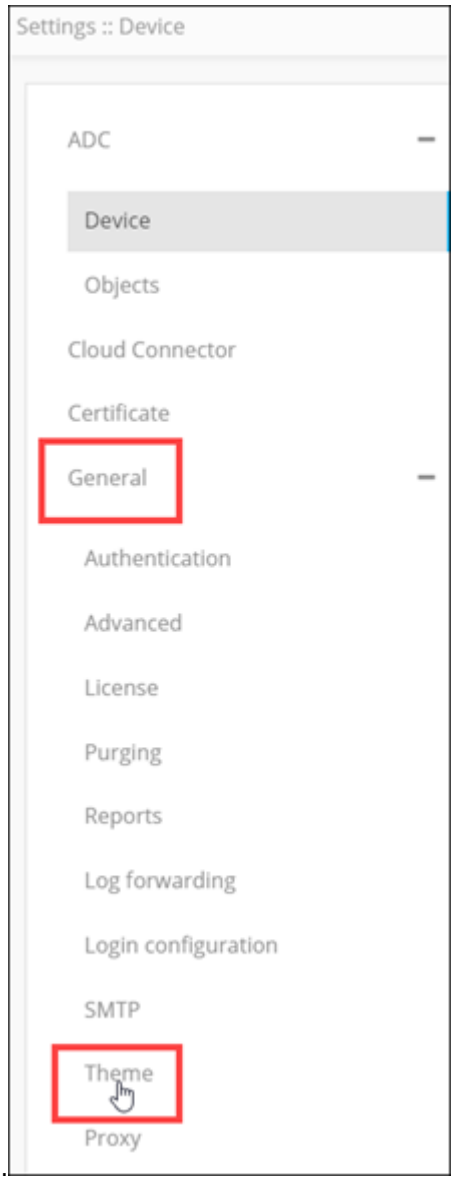
Customizing the Login Screen

To customize the login screen:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Settings**.

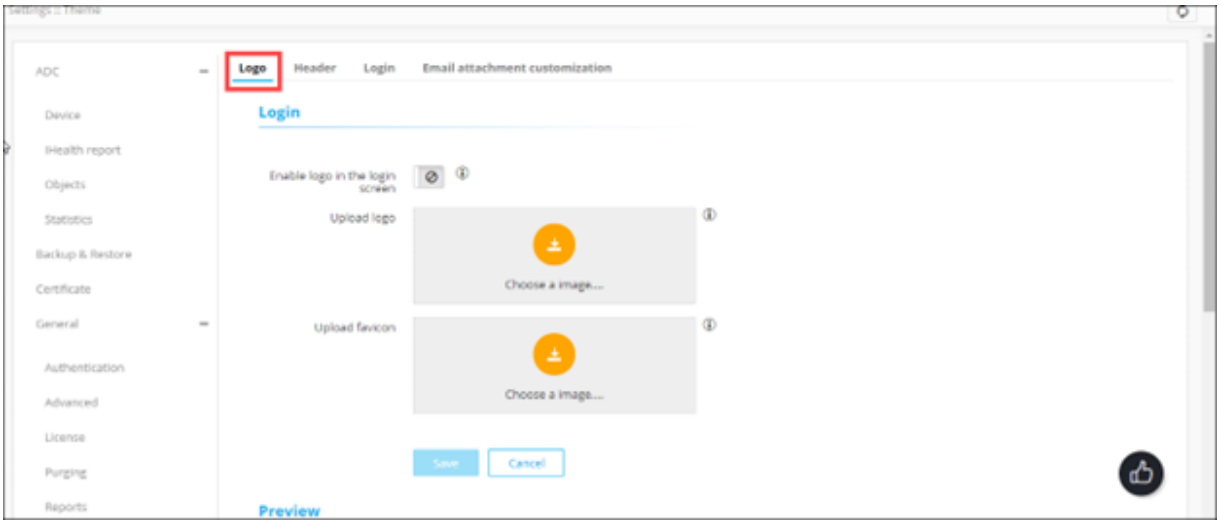


3. On the **Settings** page, from the navigation pane on the left, click **General**.

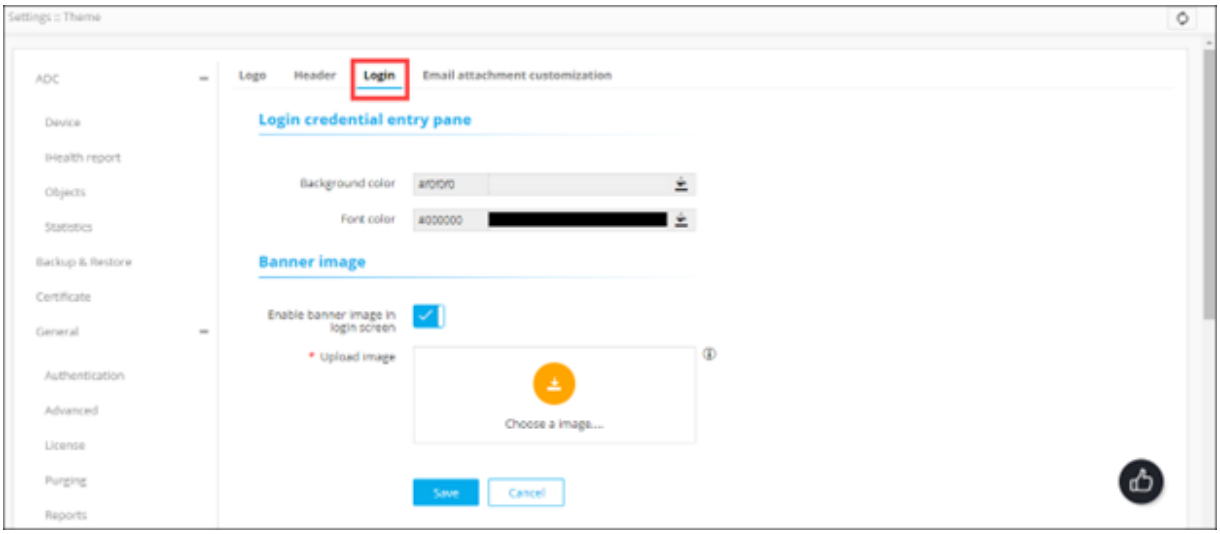


4. Under **General** settings, click **Theme**.

   The **Settings :: Theme** page is displayed, with the **Logo** tab open by default.



5. To customize the login screen, click the **Login** tab.



6. In the **Login credential entry pane** section, enter the following details:

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  .
Font color	To set a font color for the text on the login screen:

Field	Description
	a. Enter the hex code of the required font color. **OR** b. To select a color, click  .

7. In the **Banner image** section, enter the following details:

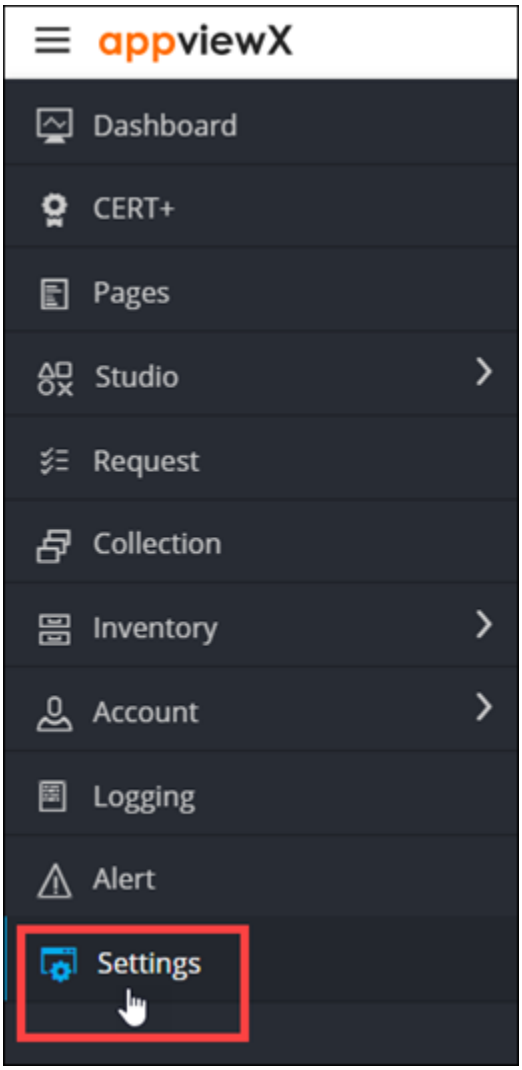
Field	Description
Enable banner image in login screen	To display a banner image on the login screen, turn on this toggle.
Upload image*	**Note:** This field is enabled only when the **Enable banner image in login screen** is tur To upload a banner image: a. Click  . b. From Windows Explorer, navigate to the location of the image, select the image, and click **O** **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**.

8. In the **Preview** section, view a preview of your customization for the login screen.
9. To apply the changes, click **Save**.

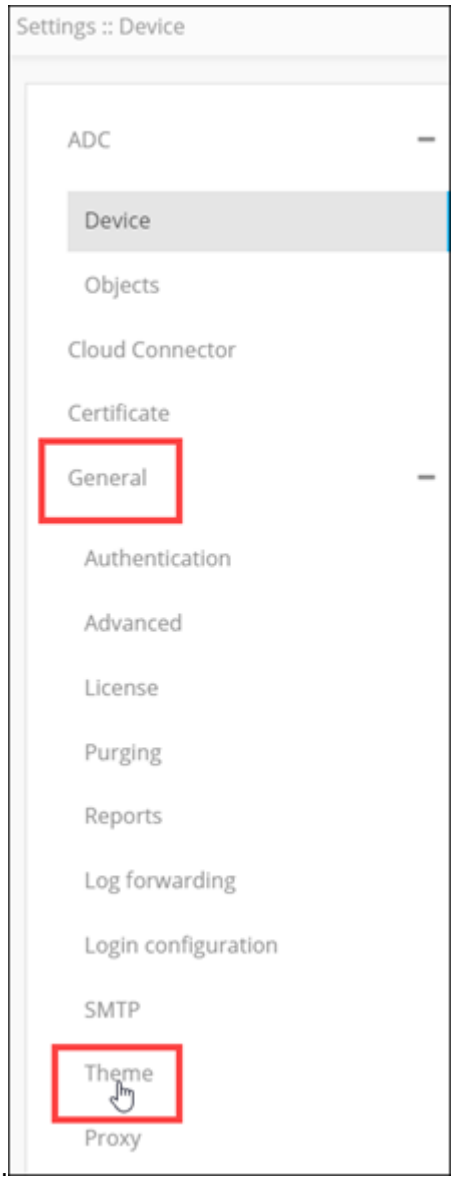
Customizing the Email Attachment Representation

To customize the cosmetics of how email attachments are represented:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Settings**.

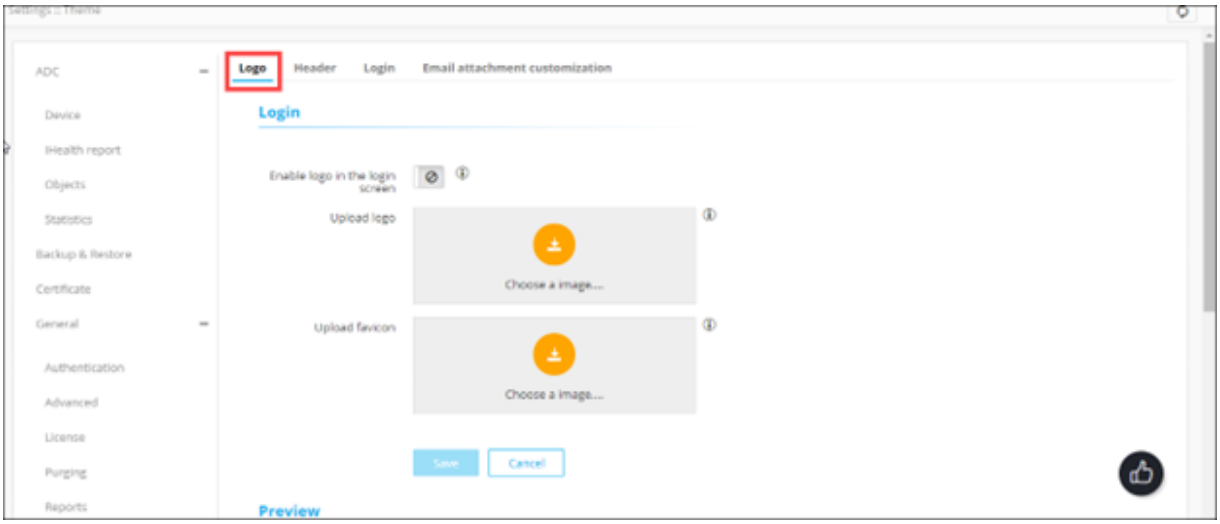


3. On the **Settings** page, from the navigation pane on the left, click **General**.

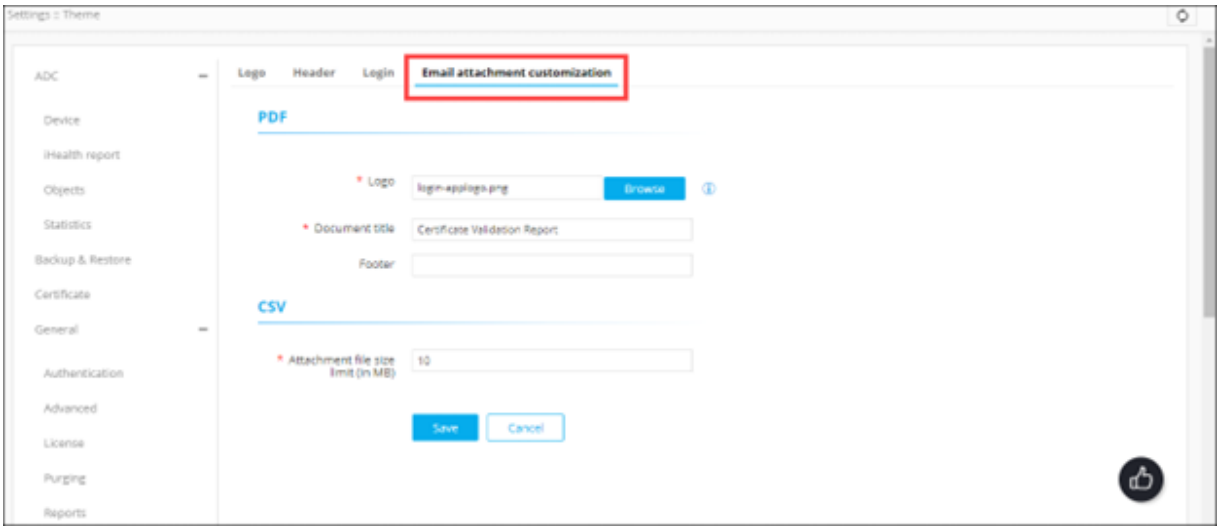


4. Under **General** settings, click **Theme**.

   The **Settings :: Theme** page is displayed, with the **Logo** tab open by default.



5. Click the **Email attachment customization** tab.



6. In the PDF section, enter the following details:

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 5 MB.
***Document title**	Name to be assigned to the PDF when is it is downloaded.

Field	Description
Footer	Footer content to be added to the PDF.

7. In the **CSV** section, enter the **Attachment file size limit (in MB)**.

Note: This is a mandatory field.

8. To apply the changes configured above, click **Save**.

Chapter 12: Glossary

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.

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.