appviewx

Platform User Guide

Version: 2022.1.0

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

Copyright AppViewX, Inc. ii

Copyright © 2022 AppViewX, Inc. All Rights Reserved. ii

Trademarks. ii

External Reference Links. ii

Contact Information. ii

Preface. viii

About the Documentation. viii

Audience. viii

Documentation Conventions. viii

Notice Icons. viii

Personas. viii

Chapter 1. Overview. 9

Chapter 2. Configuring Authentication Settings Overview. 10

Configuring the LDAP Authentication. 10

Configuring the TACACS Authentication. 19

Configuring the RADIUS Configuration. 22

Configuring Single Sign On Settings with AppViewX. 27

Security Assertion Markup Language. 31

Configuring Authentication Settings. 74

Configuring the IP Restrictions. 75

Chapter 3. Configuring Role and Resource Based Access Control . 78

Managing Users. 78

Creating a User. 78

Modifying a User. 82

Importing a Users. 86

Enabling a User. 88

Disabling a User. 90

Deleting a User....91
Managing Service Accounts....93
Client Credentials Grant Type....93
Configuring Managing Service Account....93
Configuring oAuth Settings....95
oAuth....96
oAuth Workflow....97
Managing User Groups....99
Creating a User Group....99
Cloning a User Group....102
Modifying a User Group....103
Deleting a User Group....105
Disabling a User Group....107
Enabling a User Group....108
Managing Roles....109
Creating a Role....109
Deleting a Role....112
Disabling a Role....114
Enabling a Role....115
Cloning a Role....117
Modifying a Role....119
RBAC Quick Configuration....121
Authentication....121
Resource....169
Role....186
User Group....202
Chapter 4. Configuring Privileged Access Management....219
AppViewX....219
CyberArk....221

Thycotic Secret..... 223
Chapter 5. Configuring General Settings..... 224
Configuring the SMTP Settings..... 224
Configuring the SMTP Settings for Google..... 224
Configuring the SMTP Settings for Microsoft 237
Managing Proxy Settings..... 256
Setting the Cryptographic Policy..... 259
Enabling Dashboard View for the User..... 262
Managing the Login Configuration..... 265
Managing User Activity..... 270
Chapter 6. Managing Logs..... 271
Viewing Logs-Overview..... 271
Viewing All Logs..... 271
Viewing ADC Logs..... 273
Viewing AppViewX Logs..... 274
Viewing Audit Logs..... 275
Viewing Certificate Logs..... 276
Viewing Self-Audit Logs..... 277
Viewing SSH Logs..... 278
Viewing Syslog Logs..... 279
Viewing Workflow Logs..... 280
Setting the Record Count Preference for Logs..... 281
Searching for Logs..... 281
Based on a Timestamp..... 282
Based on the Values Recorded for each Log..... 283
Forwading Logs..... 283
Configuring Server Inventory Settings..... 283
Deleting Server Inventory Settings..... 287
Disabling Server Inventory Settings..... 288

Enabling Server Inventory Settings..... 288
Configuring Forwarding Settings..... 289
Exporting Logs..... 289
Purging Logs..... 290
Chapter 7. HSM Integration for AppViewX SaaS..... 294
HSM Integration for AppViewX SaaS-Overview..... 294
HSM Architecture for the SaaS Deployment..... 295
Utimaco..... 295
Integrating the Utimaco HSM with the AppViewX SaaS 295
Fortanix..... 299
Integrating the Fortanix HSM with the AppViewX SaaS..... 299
Thales DPoD..... 303
Integrating the Thales DPoD HSM with the AppViewX SaaS..... 303
Thales GPN..... 308
Installing the Luna Client..... 308
Integrating the Thales GPN HSM with the AppViewX SaaS..... 310
Chapter 8. Managing Alerts..... 316
Viewing Existing Alerts..... 316
Viewing All Alerts..... 316
Viewing AppViewX Alerts..... 318
Viewing Certificate Alerts..... 320
Viewing SSH Alerts..... 321
Viewing Syslog Alerts..... 322
Setting the Record Count Preference for Viewing Alerts..... 323
Configuring Alerts..... 324
Configuring ADC Alerts..... 324
Configuring AppViewX Alerts..... 330
Configuring Certificate Alerts..... 333
Configuring SSH Alerts..... 336

Configuring Syslog Alerts..... 340
Editing Alerts..... 345
Deleting Alerts..... 346
Searching for Alerts..... 346
Based on a Timestamp..... 346
Based on the Values Recorded for each Alert..... 347
Purging Alerts..... 348
Chapter 9. Managing Licenses..... 352
Getting Started with a Free SaaS Trial..... 352
Viewing License Details..... 355
License Alerts..... 358
Upgrading Licenses..... 359
Chapter 10. Customizing the AppViewX User Interface..... 362
Customizing the Email Attachment Representation..... 362
Customizing the Login Screen..... 363
Customizing the Logo..... 365
Customizing the Screen Header..... 369
Chapter 11. Glossary..... 373

Preface

Revision	Description	Date
1.0	Initial Release of AppViewX_v2022.1.0 SaaS Platform.	09 May 2022

About the Documentation

The AppViewX SaaS 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.

Documentation Conventions

This section defines the Notice icon and text convention used in this guide.

Notice Icons

Convention	Description
Note	Indicates readers to take note. Notes contain helpful suggestions or references to material not covered in the document.
Tip	Indicates readers that they can save time by performing the action described in the paragraph affixed to this icon.
Warning	Indicates readers that they can save time by performing the action described in the paragraph affixed to this icon.
Best Practice	Alerts readers to a recommended use or implementation.

Personas

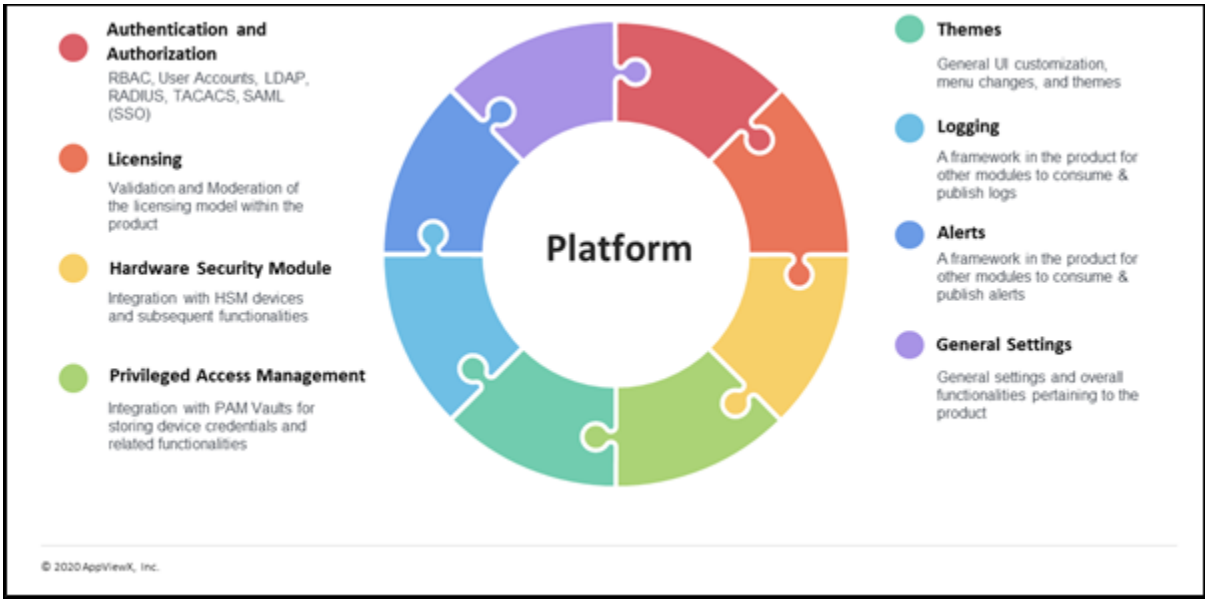
- PKI Security
- DevOps
- Application Teams

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 Overview

- Configuring the LDAP Authentication
- Configuring the TACACS Authentication
- Configuring the RADIUS Configuration
- Configuring Single Sign On Settings with AppViewX
- Configuring Authentication Settings
- Configuring the IP Restrictions

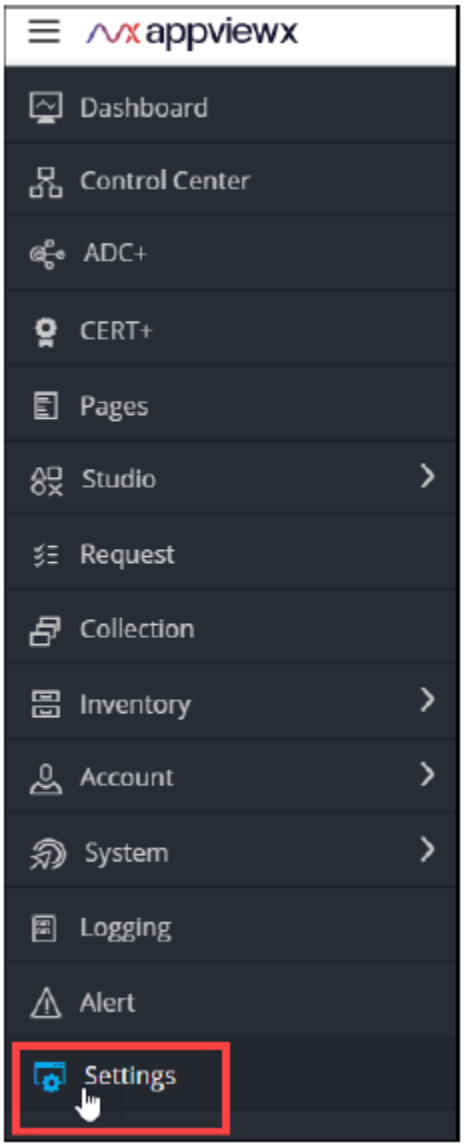
Configuring the LDAP Authentication

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.

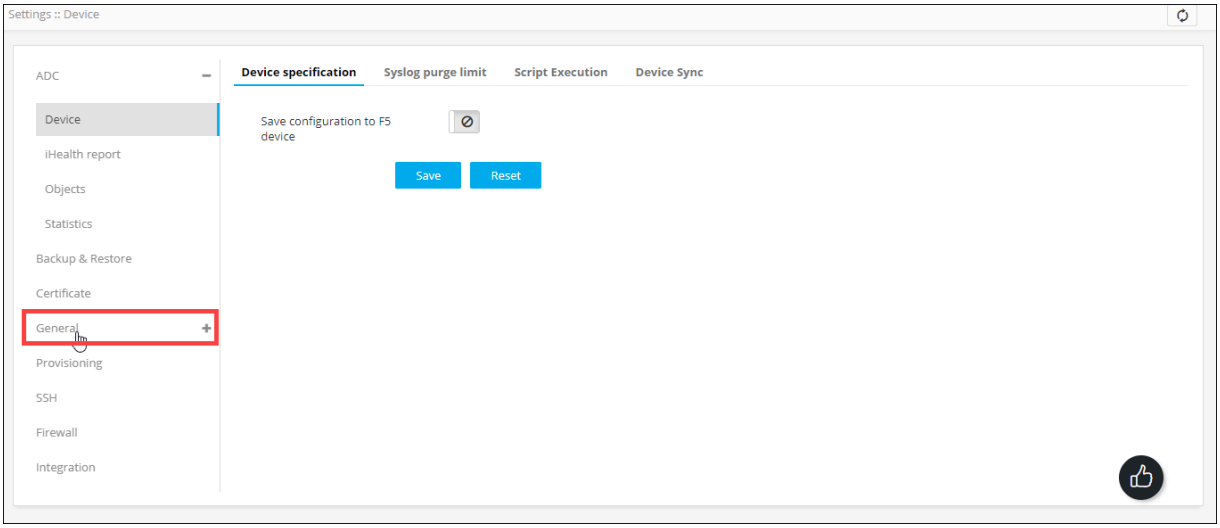
AppViewX integrates with the Active Directory and Open LDAP for authentication of external users. It also enables configuring multiple servers in the event that users belong to multiple domains.

To configure the LDAP authentication:

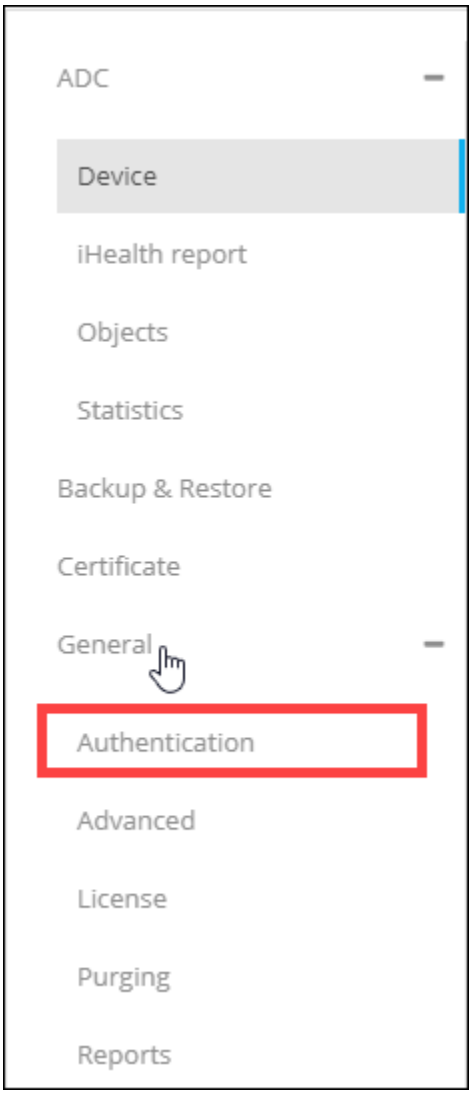
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Settings.



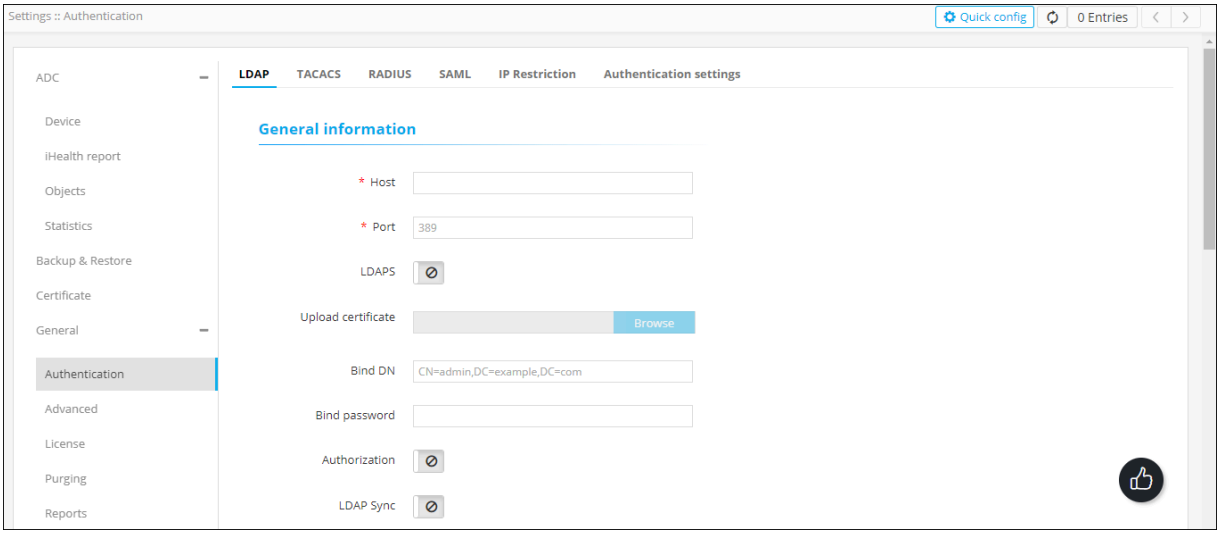
3. On the Settings page, from the navigation pane on the left, click General.



4. Under General settings, click Authentication.



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

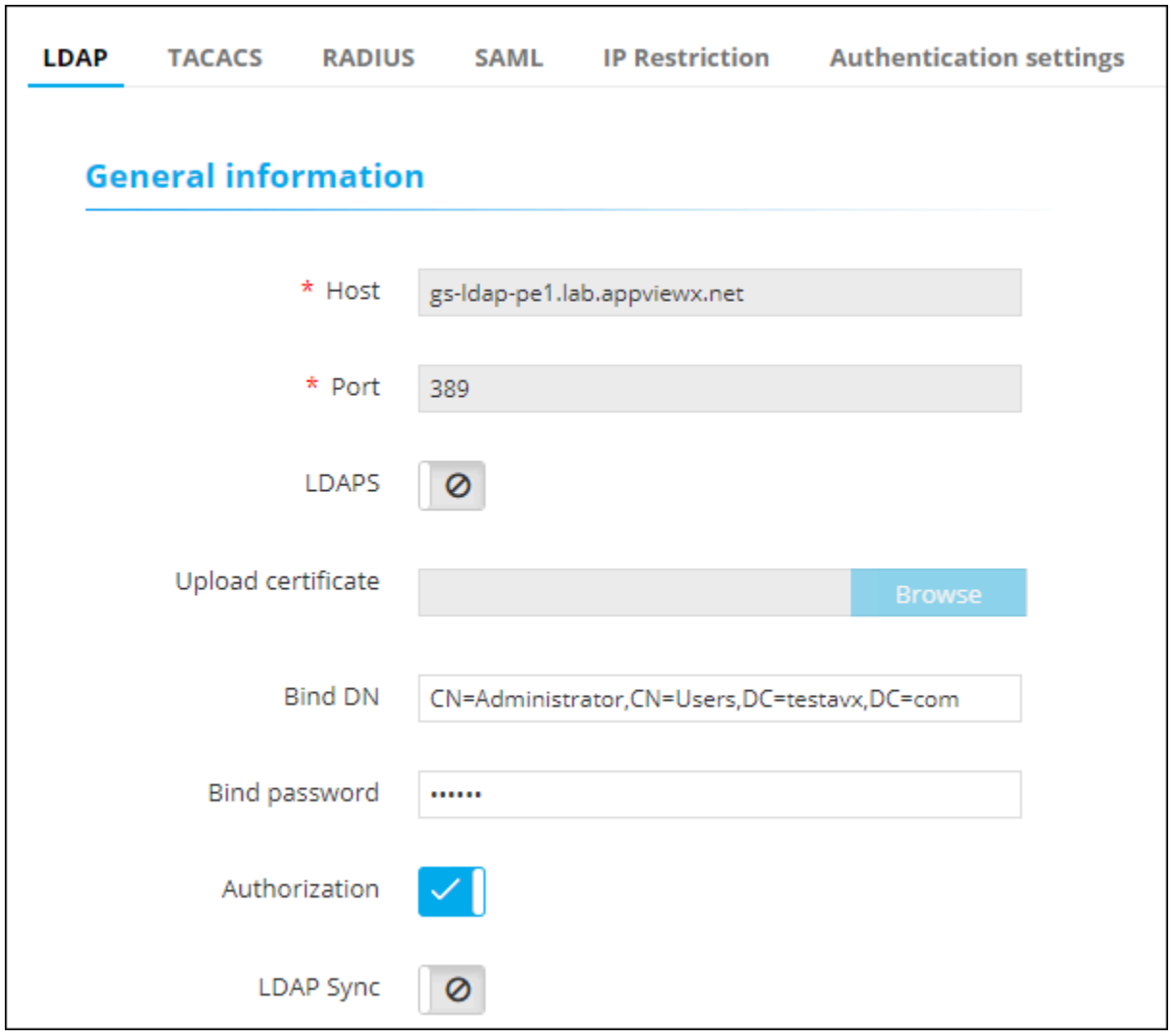


5. To configure the LDAP settings, in the General Information section, enter the following details (sample values are shown in the image below the table):

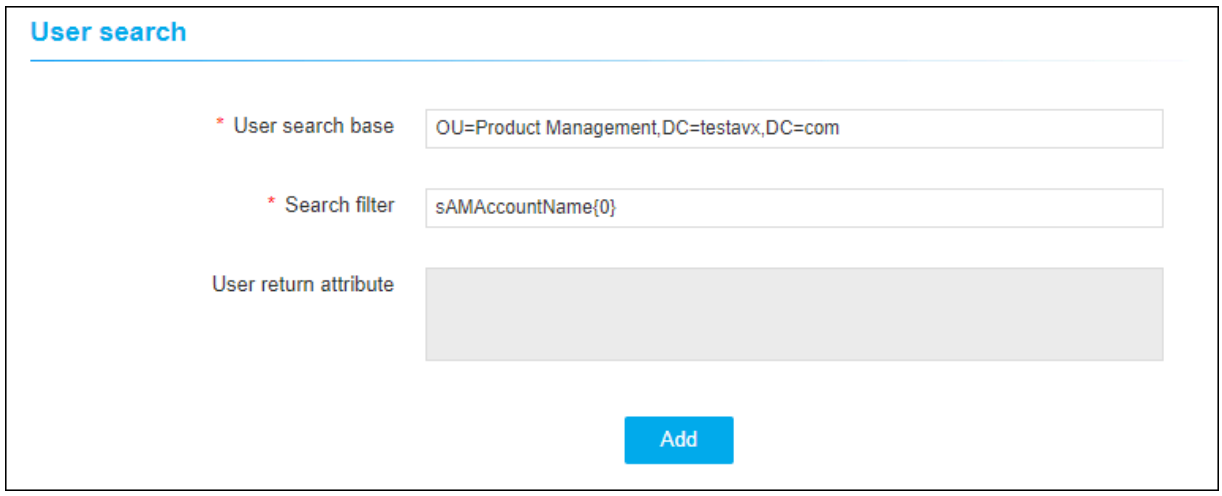
Field	Description
Host*	Hostname (domain name) of the LDAP server.
Port*	Port number of the LDAP server. **Note:** This value is entered based on the port number used in your deployment. By default, port number 389 is used for an LDAP configuration and port number 636 is used for an LDAPS configuration.
LDAPS	The LDAPS protocol is used for secure communication between AppViewX and Active Directory/Open LDAP. To enable the use of the LDAPS protocol, instead of the LDAP protocol, enable this toggle key.
Upload Certificate*	**Note:** This field is enabled only when the LDAPS is enabled. To upload an LDAP server certificate: • Click Browse Certificate. • 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. • Select the certificate to be uploaded and click Open.

Field	Description
	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	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, enable this toggle key.

***: Mandatory**



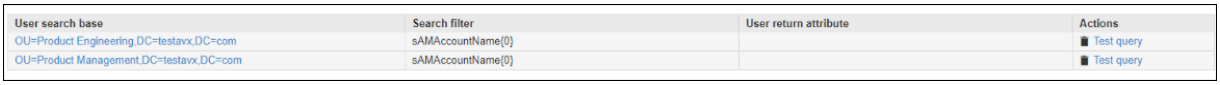
6. After entering the above connection details, to test if the host is reachable and the port is valid for establishing an LDAP/LDAPS connection, click Test Connection.



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):

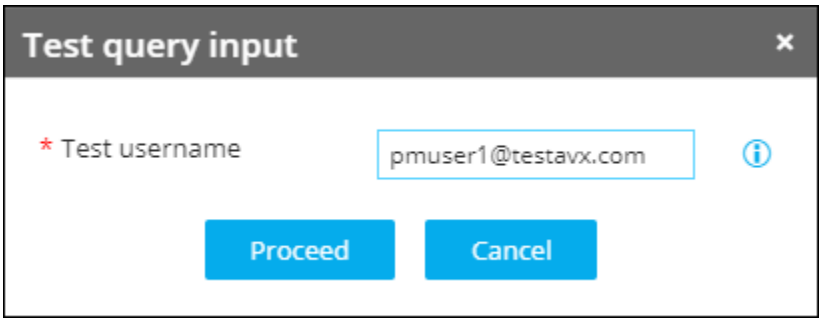
Field	Description
User search base*	Base directory where the user is present.
Search filter*	Criteria for searching for the user from the search base
User return attribute	User information to be retrieved from the search base. **Note:** This field is enabled only when **Authorization** toggle (in the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

***: Mandatory**

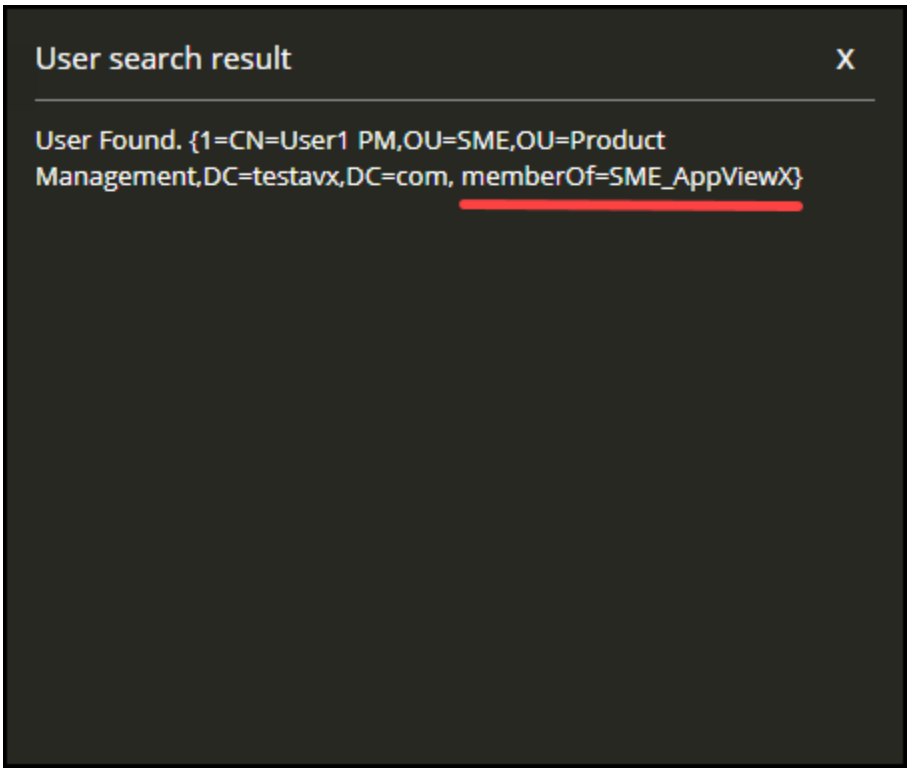


Note: You can now add multiple OUs in User search so that it checks multiple OUs to validate a user's presence in the Active Directory.

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 (sample values are shown in the image below the table):

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

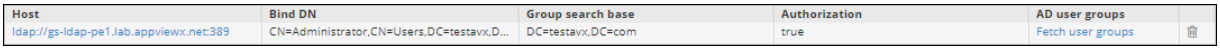
***: Mandatory**

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.

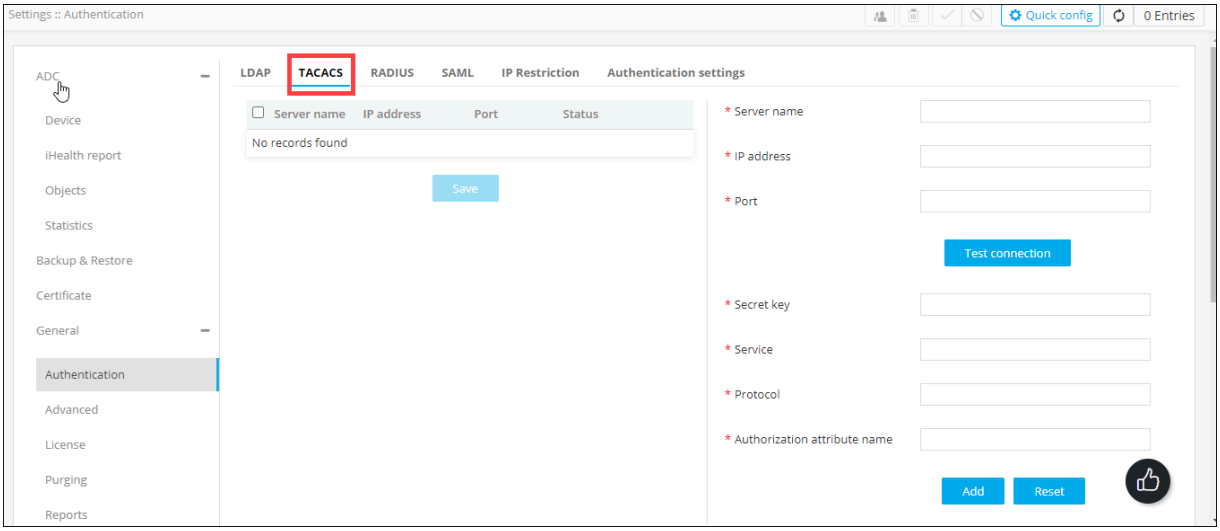
Configuring the TACACS Authentication

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:

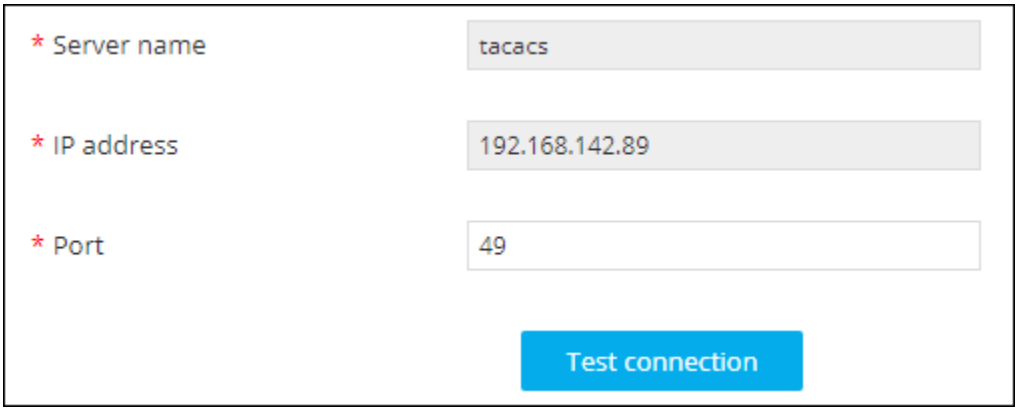
1. Navigate to the Settings :: Authentication page.
2. To configure the TACACS authentication settings, on the Settings :: Authentication page, click the TACACS tab.



3. 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

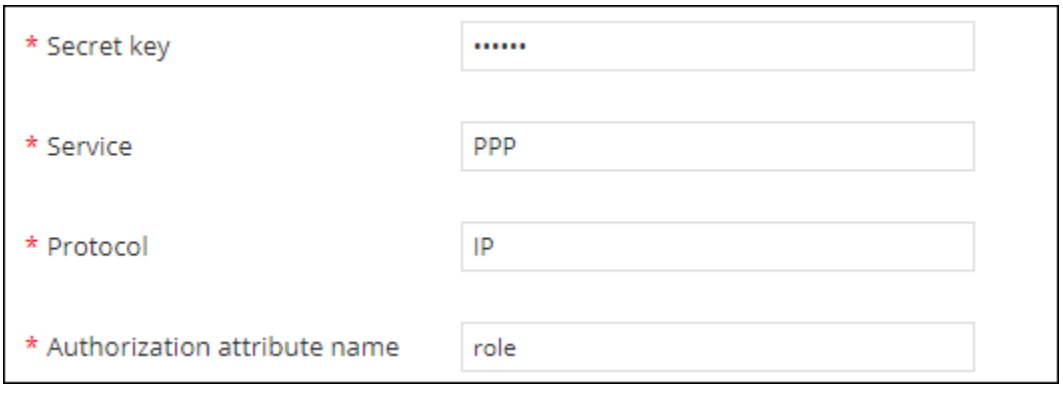
***:Mandatory**



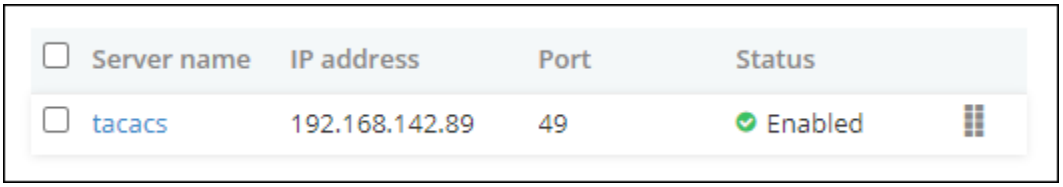
4. To test the connectivity between AppViewX and the IP address mentioned above, click Test connection.
5. Enter the following details (sample values are shown in the image below the table):

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

***Mandatory**



6. 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.

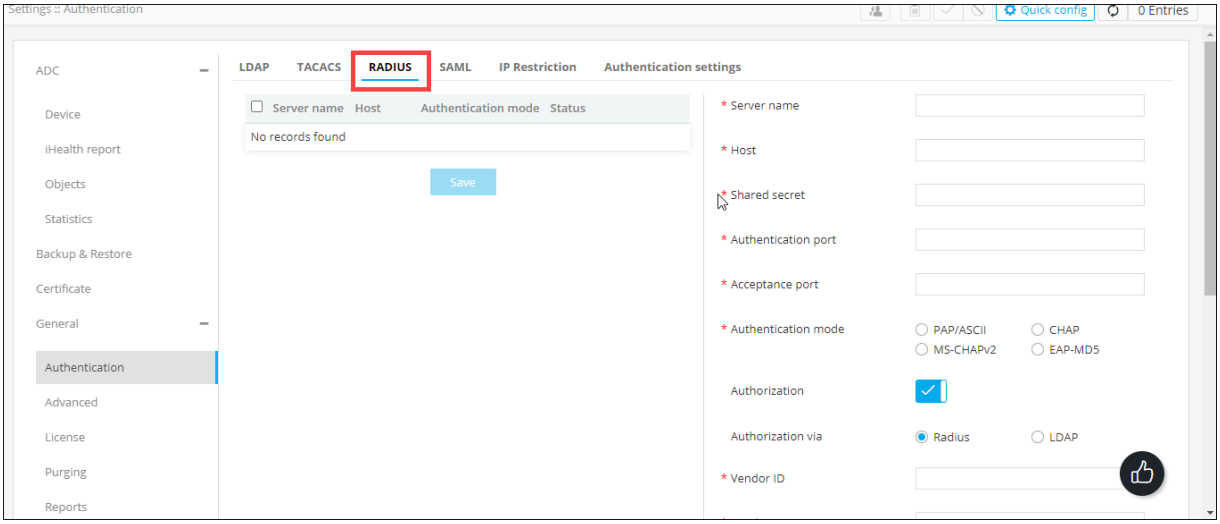
Configuring the RADIUS Configuration

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



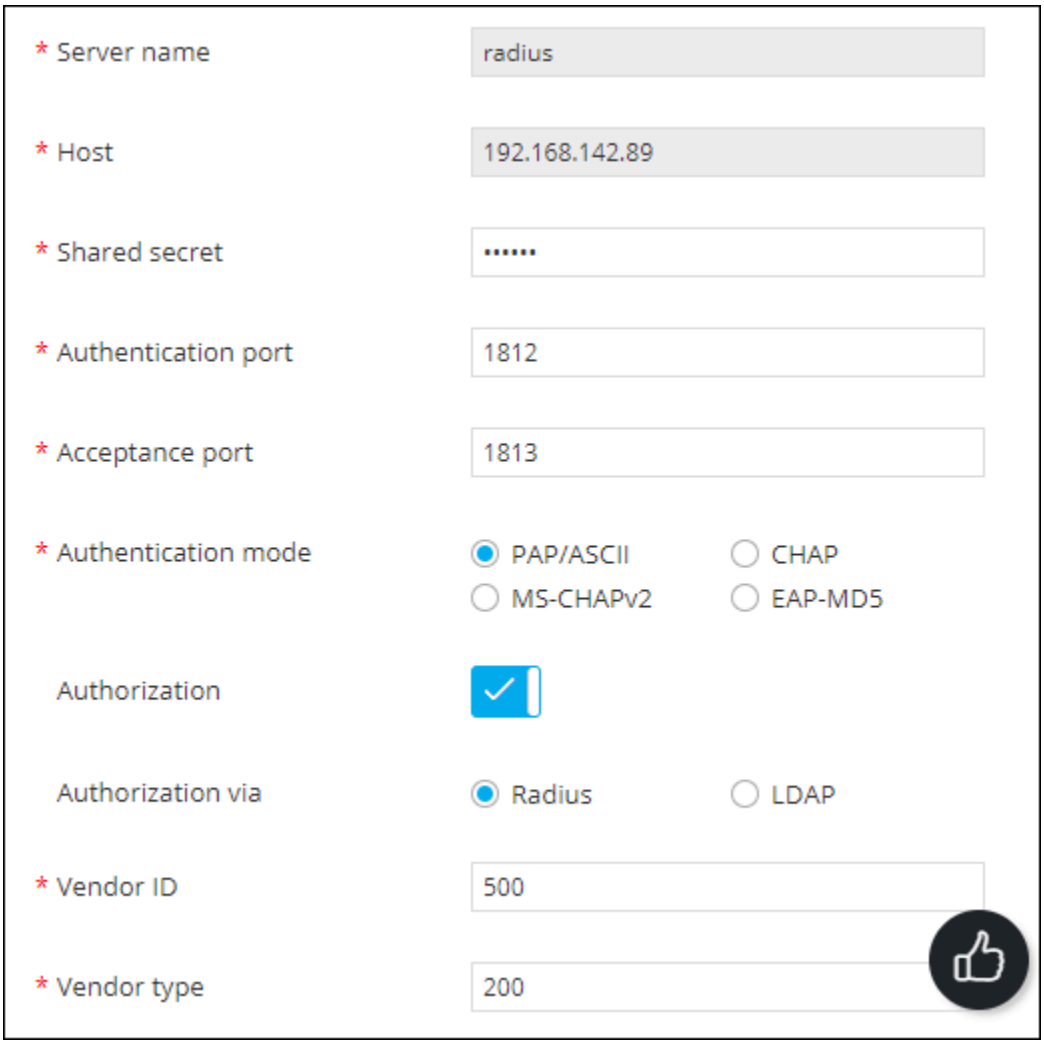
3. Enter the following details (sample values are shown in the image below the table):

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 **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.

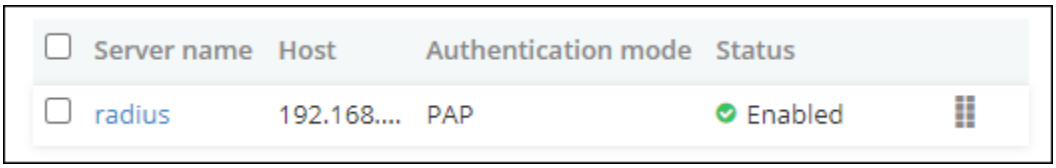
Field	Description
	To enable authorization along with authentication, select this check box. **Note:** If Authorization is not enabled, AppViewX will only carry out RADIUS authentication for the given user.
Authorization via	This field is enabled only when Authorization  is enabled. Select from one of the following authorization modes: • RADIUS • LDAP
Vendor ID*	This field is enabled only when Authorization  is enabled and authorization is done via the RADIUS server. 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.
Vendor type*	This field is enabled only when Authorization  is enabled and authorization is done via the RADIUS server. Enter the vendor type.

Field	Description
	Note: AppViewX does not have a unique vendor type. We use a free vendor ID: 200. Ensure that this is configured as part of the RADIUS server settings.
LDAP*	This field is enabled only when Authorization  is enabled and authorization is done via the LDAP server. From the drop-down menu, select the LDAP server to be used for the authorization.

***Mandatory**



4. 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.

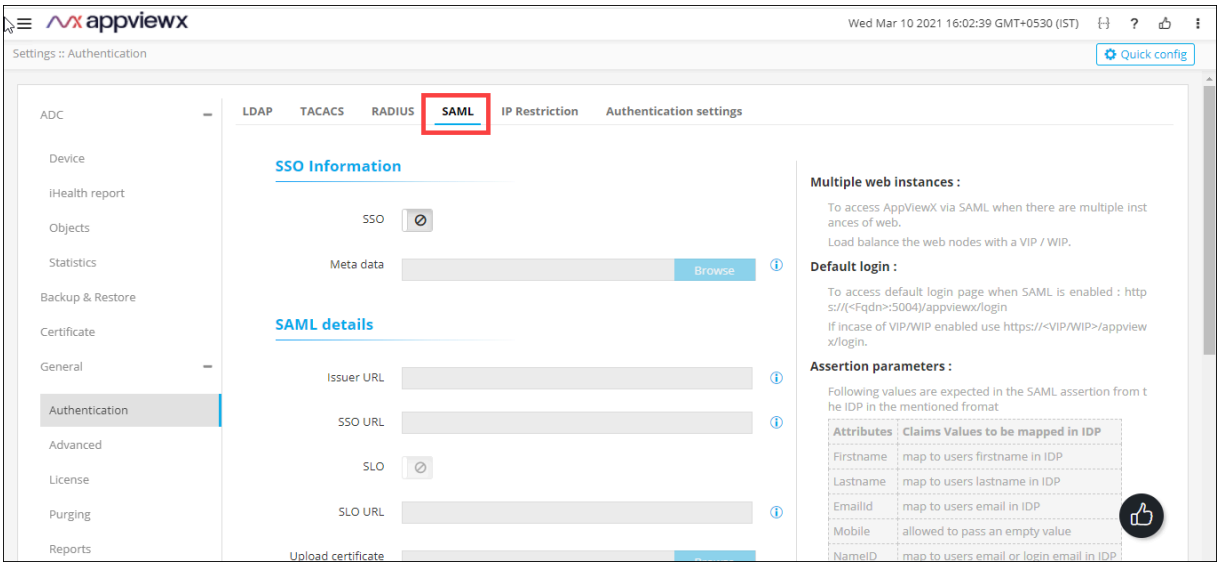
Configuring Single Sign On Settings with AppViewX

The SecurityAssertion 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.

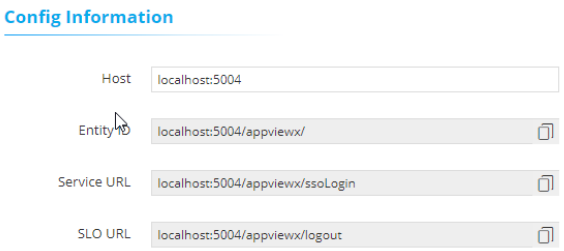
To configure single sign on settings with AppViewX:

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



3. In the SSO Information section, enter the following details:

Field	Description
SSO	To use SAML authentication for Single Sign On, enable this toggle key. The Service Provider (AppViewX) configuration information (Entity ID, Service URL, and SLO URL) is populated in the Config Informa-

Field	Description
	tion section, as shown in the image given below:  **Note:** Users can replace the host information with the actual AppViewX instance IP Address or DNS name followed with the web service's accessible port number (example: 31443 or 443) to derive the SP configuration from AppViewX.
Meta data	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.

***Mandatory**

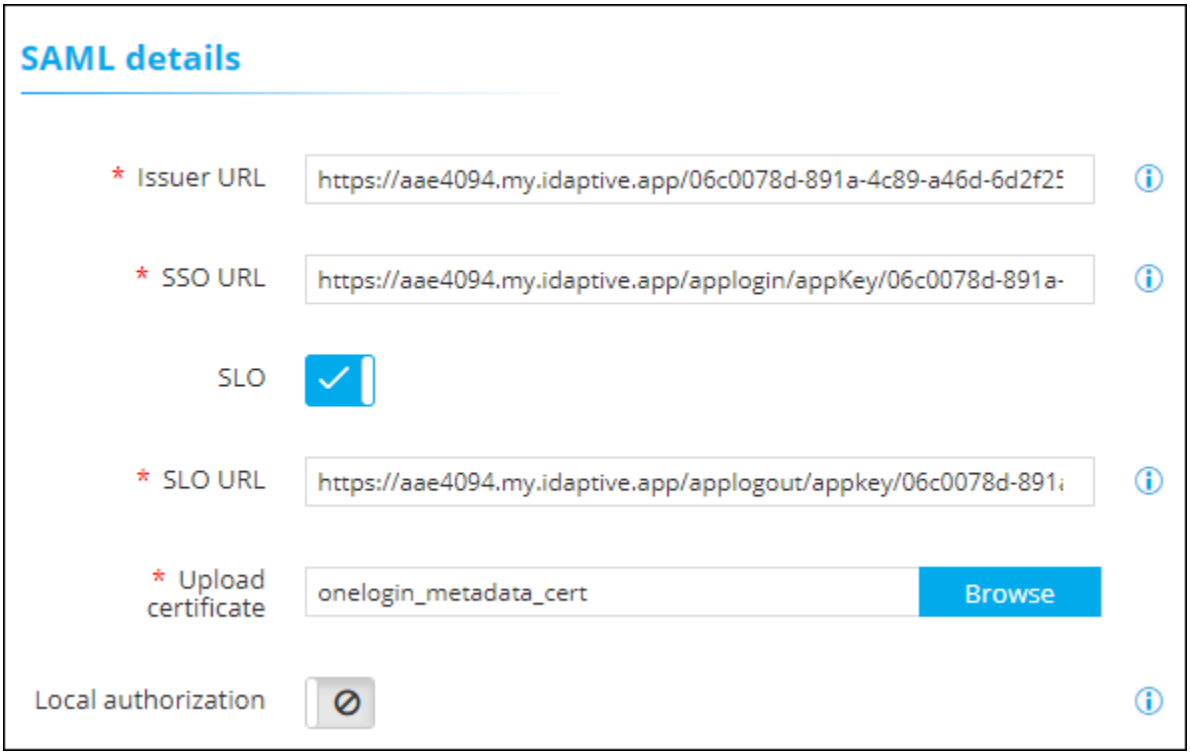
4. If the IdP is not able to pass the roles/user group as a part of of the SAML assertion and requires AppViewX to perform the authorization, in the SAML details section, to enable local authorization, enter the following details (sample values are shown in the image below the table):

Field	Description
Issuer URL*	**Note:** This field is applicable only when  (in the SSO Information section) is enabled. The field is automatically populated when the IdP metadata is uploaded. Entity ID of the IdP
SSO URL*	**Note:** This field is applicable only when  (in the SSO Information section) is enabled. The field is automatically populated when the IdP metadata is uploaded. For AppViewX to send the authentication request, enter the URL of the protected endpoint provided by your IdP. Protected endpoint provided by the IdP, to which AppViewX sends the authentication request
SLO	**Note:** This toggle button is enabled only when  (in the SSO Information section) is enabled. To enable single log out, enable this toggle key. It will log out the user from AppViewX and the IdP

Field	Description
SLO URL*	**Note:** This field is enabled only when  (in the SSO Information section) is enabled. **Note:** This field is mandatory only when  (in the SAML details section) is enabled. URL of the IdP protocol endpoint.
Upload certificate*	**Note:** This field is enabled only when  (in the SSO Information section) is enabled. **Note:** A certificate is to be uploaded only when the certificate of the IDP is not available as a part of the metadata. 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.
Local authorization	To enable SAML only authentication in IdP and for authorization to be carried out in AppViewX, enable this toggle key.

Field	Description
	Note: Authorization can be done by assigning user groups manually to the user or enabling birthright role.

***Mandatory**



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

- Security Assertion Markup Language

Security Assertion Markup Language

- SAML Overview
- Basic SAML Flow
- Configuration of SAML Parameters in AppViewX (Service Provider)
- Mapping User Groups for Local Authorization

• Troubleshooting
• Types of SAML Vendors

SAML Overview

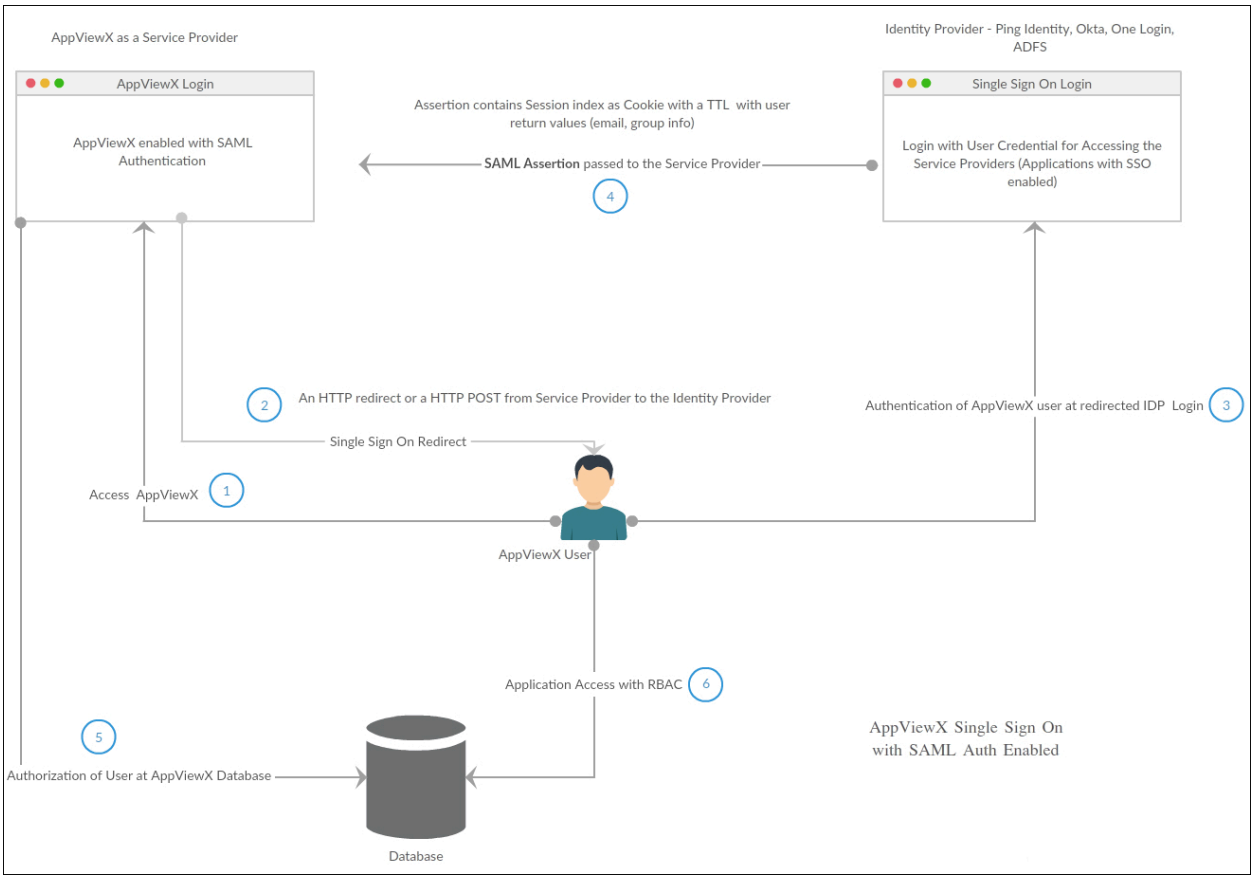
Security Assertion Markup Language (SAML) is a mechanism used for communicating identities between two web applications. It enables a web-based Single sign-on (SSO) and hence, it eliminates the need for maintaining credentials for various applications and reduces identity theft.

SAML integration requires the following parameters:

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

Basic SAML Flow

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



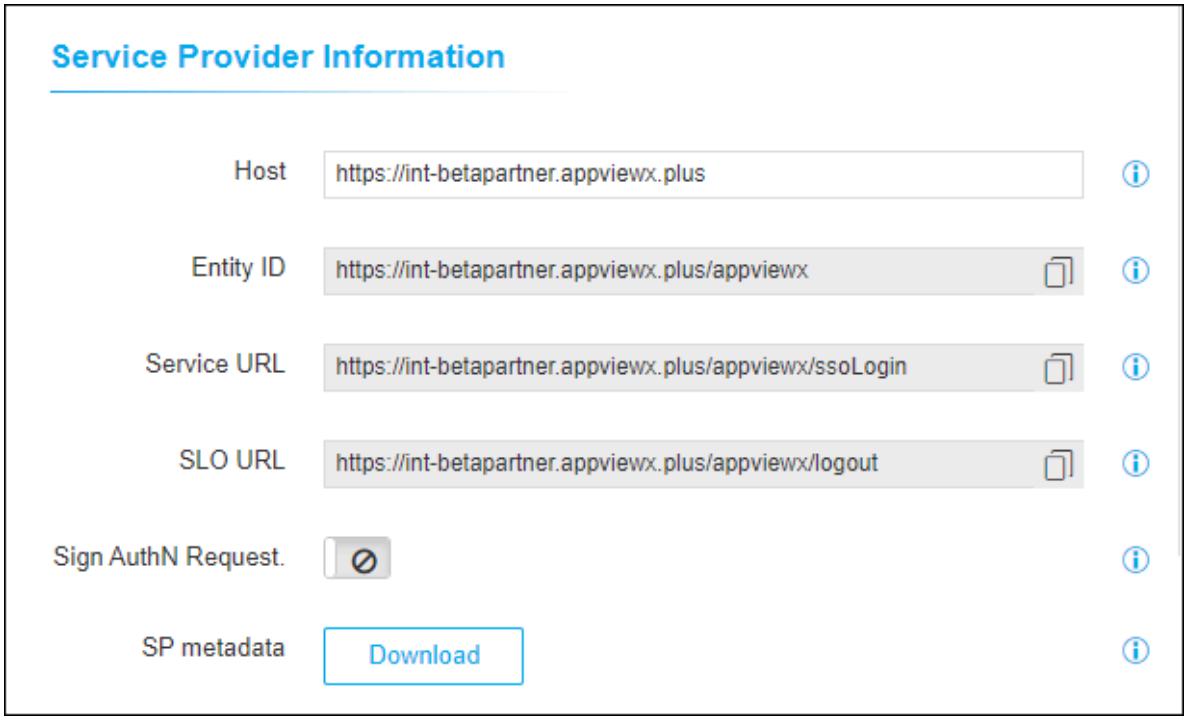
Configuration of SAML Parameters in AppViewX (Service Provider)

1. Navigate to Menu > Settings > General > Authentication > SAML.
2. Enable the Enable SSO. This action will populate the service provider contents for the integration.
3. Under the Service Provider Information section, fill in the below fields:
   a. Enter the host information for AppViewX in the Hostfield. The host information can be the Hostname/URL used to access the application.
   b. The Entity ID, SSO URL and the SLO URL will be automatically filled based on the Host information provided above.
   c. Enable/Disable the Sign AuthN Request toggle to send signed AuthN requests from AppViewX to your Identity Provider.

> **Note:** This is to be enabled only when your IdP requires a sign authN request from service provider.

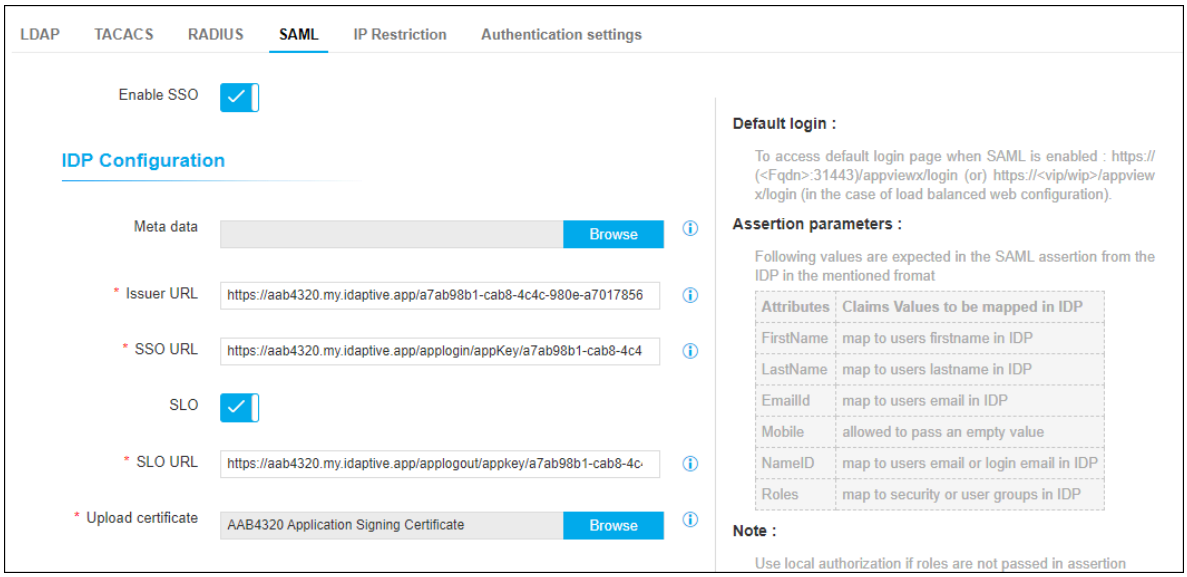
- Once the Sign AuthN Request is enabled, Upload a Service Provider certificate and private key in a p12 format and provide the p12 Password. Choose the Signing Algorithm (Recommended Algorithm: SHA-256) from the drop-down list. The Service provider certificate should be shared with the IDP to validate the Service Provider SAML assertion signature.

d. Copy/Download the Service Providerinformation (Entity Id, SSO/Service URL, SLO URL) to be consumed at IdP.



4. Under the IDP Configuration section,
   a. Upload Metadata which is downloaded from your Identity Provider.
   b. Upload of metadata automatically parses the fields SSO, SLO, and so on.
   c. In the case of IDP metadata is not available, copy and paste the below contents.
   d. Issue URL - Entity ID of the Identity Provider.
   e. Provide the SSO URL which is a single sign-on URL for the service provider to authenticate the users.
   f. SLO - Enable/Disable SLO only if required.
   g. Provide the SLO URL which is the SAML logout URL to send logout responses.

h. Upload the IdP certificate in .pem format If the certificate is not available as a part of your IdP metadata.

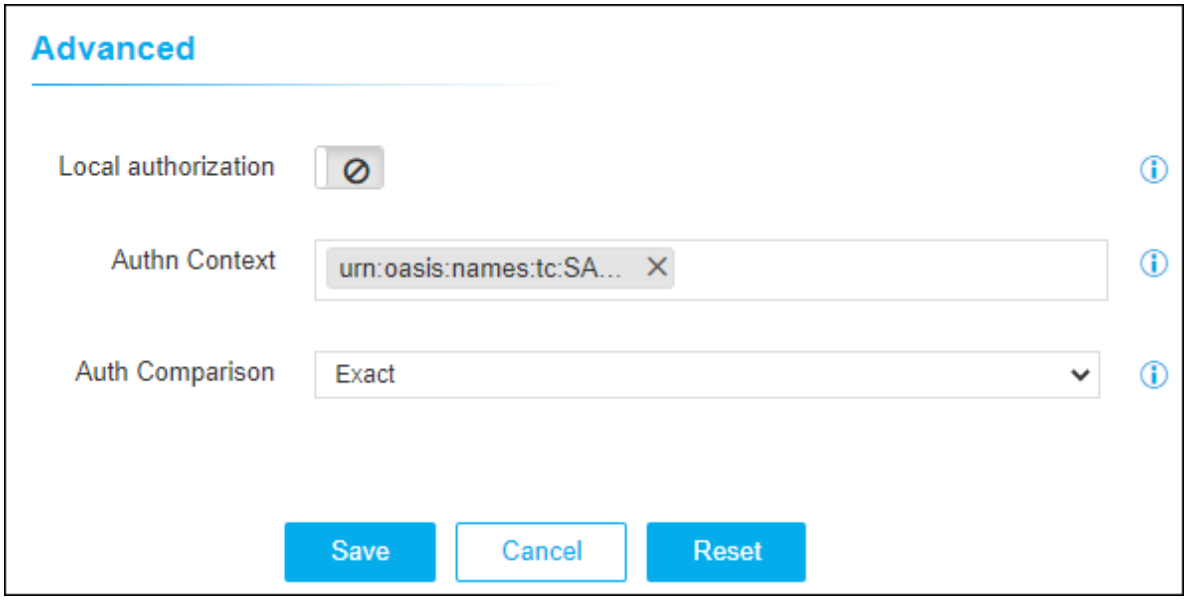


5. Under the Advanced section, fill in the below fields:
   a. Enable/Disable the Local authorization to authenticate in IdP and authorize in AppViewX. If the IDP is unable to pass the roles/usergroup as a part of the SAML assertion and requires AppViewX to perform the Authorization then the above feature can be used.

> **Note:** This feature is available from 20.1 version of AppViewX.

   b. Provide the Authn Context in the text field.
      • Use any one of the below values for a customized type of authnrequest needed by your IDP. Other RFC SAML2.0 standard authnrequest can also be used. (Copy and paste the below values or add values in the same format from RFC to the AuthNcontext field).
        • urn:oasis:names:tc:SAML:2.0:ac:classes:X509.
        • urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient.
        • urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
        • urn:oasis:names:tc:SAML:2.0:ac:classes:Password
        • urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos
        • urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol

c. Choose the Auth Comparison from the drop-down field. This indicates how the authentication context URI in the AuthnRequest message compares to the context defined at the asserting party. It is preferred to be exact.



6. Click the Save button.
7. If the configuration provided needs to be removed, click Reset button.

Mapping User Groups for Local Authorization

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

Manual Mapping

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

Birthright Role

The administrator can enable a birthright role and map a user group by default for all the sso users to log in initially when they do not have a role/user group passed in the SAML assertion. This would enable the user to login successfully and access the application with the access given in the specific user group.

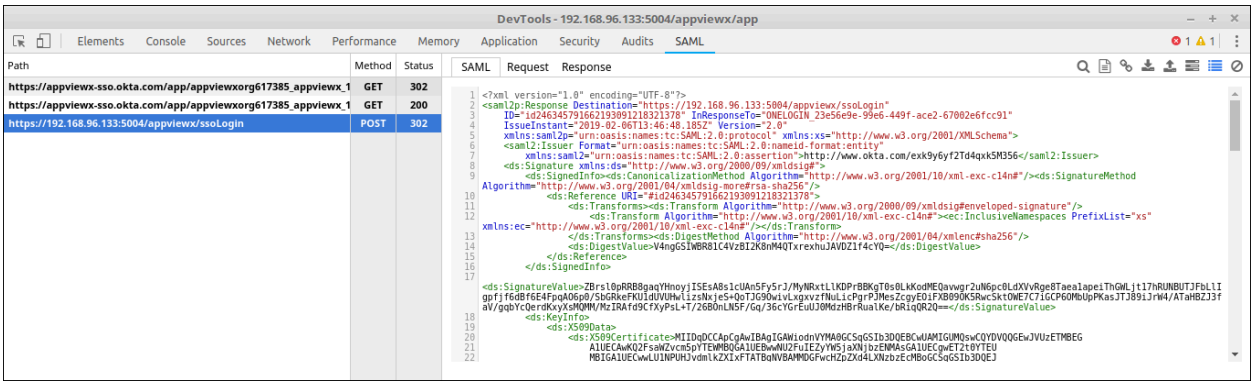
If required now the administrator can create different sets of user groups and assign manually to the respective users who do not need the birthright user group which will be reflected in the subsequent login.

Troubleshooting

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

Sample Configuration of SAML Assertion

Number of SAML Assertions in HTTP Headers



Sample SAML Assertion

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

<saml2p:Response Destination="https://192.168.x.x:31443/appviewx/ssoLogin"

   ID="id246345791662193091218321378" InResponseTo="ONELOGIN_23e56e9e-99e6-449f-ace2-67002e6fcc91"

   IssueInstant="2019-02-06T13:46:48.185Z" Version="2.0"

   xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:xs="http://www.w3.org/2001/XMLSchema">

   <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"

      xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">http://www.okta.com/exk9y6yf2Td4qxk5M356</saml2:Issuer>

   <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

      <ds:SignedInfo><ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/><ds:SignatureMethod

 Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>

         <ds:Reference URI="#id246345791662193091218321378">

            <ds:Transforms><ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
```

```
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ec:InclusiveNamespaces PrefixList="xs"
 xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/></ds:Transform>
          </ds:Transforms><ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
          <ds:DigestValue>V4ngGSIWBR81C4VzBI2K8nM4QTxrexhuJAVDZ1f4cYQ=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>

 <ds:SignatureValue>ZBrsl0pRRB8gaqYHnoyjISEsA8s1cUAn5Fy5rJ/MyNRxtLlKDPrBBKgT0s0LkKodMEQavwgr2uN6pc0LdXVvRge8Taea1apeiThGWLjt17hRU
NBUTJFbLllgpfjf6dBf6E4FpqAO6p0/SbGRkeFKU1dUVUHwlizsNxjeS+QoTJG9OwivLxgxvzfNuLicPgrPJMesZcgyEOiFXB09OK5RwcSktOWE7C7iGCP6OMbUpP
KasJTJ89iJrW4/ATaHBZJ3faV/gqbYcQerdKxyXsMQMM/MzIRAfd9CfXyPsL+T/26BOnLN5F/Gq/36cYGrEuUJ0MdzHBrRualKe/bRiqQR2Q==</ds:SignatureVal
ue>
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>MIIDqDCCApCgAwIBAgIGAWiodnVYMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYDVQQGEwJVUzETMBEG
            A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
            MBIGA1UECwwLU1NPUHJvdmlkZXIxFTATBgNVBAMMDGFwcHZpZXd4LXNzbzEcMBoGCSqGSIb3DQEJ
            ARYNaW5mb0Bva3RhLmNvbTAeFw0xOTAyMDEwOTQ4MjAwFw0yOTAyMDEwOTQ5MjJaMIGUMQswCQYD
            VQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsG
            A1UECgwET2t0YTEUMBIGA1UECwwLU1NPUHJvdmlkZXIxFTATBgNVBAMMDGFwcHZpZXd4LXNzbzEc
            MBoGCSqGSIb3DQEJARYNaW5mb0Bva3RhLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
            ggEBAIc22r1CR7gbMVcyYnRjkDLGRwHJ1zhQkWTVoEZdbk/KTHwVMXHpNinkOhUcxbzfHePBf6wx
            9jEThiNvvHZVIg6ZktYotG9DF/FF0fMxhzfweqR5yt27ihiuVTeGT8GjNcXwOoyzJdrDuZg27ybI
            jriqGPKrLiwrrot54R1LP2VclM0FdIOWdOoU1N5IEnFAd+2UECZZLQ0gJrDpFcbDisuhmp5bTKUS
            1RpIxarNeacH2klRY4efeqQdVgaghgs+zMN44iz+YGs8uELElKErOabEtoYiTJmsVnqEcs8fUvKx
            LLdZevPhh89v0MJiZl9gTjjt/f9N+NEUzyJsHfxqmnUCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEA
            RZo42X1gDE3d9xnftXr2LoUltdTQeVoFdkIJIqJla21kDRCwHis2OvuFwOW+QdUeh5uUIjGxbhaA
            cQIeJUvuD1aEK/ynUDKGA0jvdLR7IbwTK69i7c19F7pti6b5sq8yjl5fOavit1N3INIzZdkrPlP1
            hJnKcjOSVyMPv8a7rDXOtXxDoZgi+pWj0qlp4E9tKOrWJgKdjS8j03ulWwtOx4Jak4yYueaY8nH1
            +amyE6w96Qm6ScEGLcxXzboczS7BMjZ0M4Mr6zXOTS8pU+AX6NBmdNkdwO9JSeXm3U6lRWv59jet
            qMeKqf4aKRg+oqbw9hkH3X6qT69AeEiPz6YPmQ==</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </ds:Signature>
    <saml2p:Status xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"><saml2p:StatusCode
 Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></saml2p:Status>
    <saml2:Assertion ID="id24634579166299789832980116" IssueInstant="2019-02-06T13:46:48.185Z"
      Version="2.0" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
```

```
    xmlns:xs="http://www.w3.org/2001/XMLSchema">
    <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
      xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">http://www.okta.com/exk9y6yf2Td4qxk5M356</saml2:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo><ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/><ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
        <ds:Reference URI="#id246345791662997898329801l6">
          <ds:Transforms><ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ec:InclusiveNamespaces PrefixList="xs"
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/></ds:Transform>
          </ds:Transforms><ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
          <ds:DigestValue>hnTKZKSyxKC6WGZTK7iD+iQv4+nj/91eX8vhrkyi+1k=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>

<ds:SignatureValue>OtgpFXWkIIO0hSZiHpAdTDBg6v11+/unBzyPOFSBl+0+b2i22s3lHtzCqsEVp4Xn9J1XoL12tCr/uhg7b4kxcTslMsAYFVQipUZLKanEIaEOSv2
tnjQuAoE3fBMTm2d/3+nlXofyGiOMEY5OrFaGGjC9ZAMk2qJDAEzjZHhjOyooLQltzDocfVFvXeFSl/bAaDNSRPYT0B9dXsGpjpUlA6CMpmJXSxgAPwogaM20d48
o7iKi3THjTgm1L2z9nntQajfaRERkoTfAV0sGE6iKlUAhWmtMkUDOUXbMeBXo61cpQ5A/WsfxpbZKhJkDes/9lzcDoPkI7w+TshJnQMQA3A==</ds:SignatureVal
ue>
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>MIIDqDCCApCgAwIBAgIGAWiodnVYMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYDVQQGEwJVUzETMBEG
            A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
            MBIGA1UECwwLU1NPUHJvdmlkZXIxFTATBgNVBAMMDGFwcHZpZXd4LXNzbzEcMBoGCSqGSIb3DQEJ
            ARYNaW5mb0Bva3RhLmNvbTAeFw0xOTAyMDEwOTQ4MjJaFw0yOTAyMDEwOTQ5MjJaMIGUMQswCQYD
            VQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsG
            A1UECgwET2t0YTEUMBIGA1UECwwLU1NPUHJvdmlkZXIxFTATBgNVBAMMDGFwcHZpZXd4LXNzbzEc
            MBoGCSqGSIb3DQEJARYNaW5mb0Bva3RhLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
            ggEBAIc22r1CR7gbMVcyYnRjkDLGRwHJ1zhQkWTVoEZdbk/KTHwVMXHpNinkOhUcxbzfHePBf6wx
            9jEThiNvvHZVIg6ZktYotG9DF/FF0fMxhzfweqR5yt27ihiuVTeGT8GjNcXwOoyzJdrDuZg27ybI
            jriqGPKrLiwrrot54R1LP2VclM0FdIOWdOoU1N5IEnFAd+2UECZZLQ0gJrDpFcbDisuhmp5bTKUS
            1RplxarNeacH2klRY4efeqQdVgaghgs+zMN44iz+YGs8uELElKErOabEtoYiTJmsVnqEcs8fUvKx
            LLdZevPhh89v0MJiZI9gTjjt/f9N+NEUzyJsHfxqmnUCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEA
            RZo42X1gDE3d9xnftXr2LoUltdTQeVoFdklJlqJla21kDRCwHis2OvuFwOW+QdUeh5uUIjGxbhaA
            cQIeJUvuD1aEK/ynUDKGA0jvdLR7IbwTK69i7c19F7pti6b5sq8yjl5fOavit1N3INIzZdkrPlP1
            hJnKcjOSVyMPv8a7rDXOtXxDoZgi+pWj0qlp4E9tKOrWJgKdjS8j03ulWwtOx4Jak4yYueaY8nH1
            +amyE6w96Qm6ScEGLcxXzboczS7BMjZ0M4Mr6zXOTS8pU+AX6NBmdNkdwO9JSeXm3U6lRWv59jet
```

```
                qMeKqf4aKRg+oqbw9hkH3X6qT69AeEiPz6YPmQ==</ds:X509Certificate>
            </ds:X509Data>
        </ds:KeyInfo>
    </ds:Signature>
    <saml2:Subject xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
        <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">saml@appviewx.com</saml2:NameID>
        <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><saml2:SubjectConfirmationData
InResponseTo="ONELOGIN_23e56e9e-99e6-449f-ace2-67002e6fcc91"
            NotOnOrAfter="2019-02-06T13:51:48.185Z" Recipient="https://192.168.x.x:31443/appviewx/ssoLogin"/></saml2:SubjectConfirmation>
    </saml2:Subject>
    <saml2:Conditions NotBefore="2019-02-06T13:41:48.185Z" NotOnOrAfter="2019-02-06T13:51:48.185Z"
        xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
        <saml2:AudienceRestriction>
            <saml2:Audience>https://192.168.x.x:31443/appviewx/</saml2:Audience>
        </saml2:AudienceRestriction>
    </saml2:Conditions>
    <saml2:AuthnStatement AuthnInstant="2019-02-06T13:46:46.836Z"
        SessionIndex="ONELOGIN_23e56e9e-99e6-449f-ace2-67002e6fcc91"
        xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
        <saml2:AuthnContext>
            <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClassRef>
        </saml2:AuthnContext>
    </saml2:AuthnStatement>
    <saml2:AttributeStatement xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
        <saml2:Attribute Name="EmailId" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">saml@appviewx.com</saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute Name="FirstName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">saml</saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute Name="LastName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">appviewx</saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute Name="NameID" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
```

```
            <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">saml@appviewx.com</saml2:AttributeValue>
          </saml2:Attribute>
          <saml2:Attribute Name="Mobile" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">0</saml2:AttributeValue>
          </saml2:Attribute>
          <saml2:Attribute Name="Roles" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">oktarole</saml2:AttributeValue>
          </saml2:Attribute>
        </saml2:AttributeStatement>
      </saml2:Assertion>
    </saml2p:Response>
```

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

Vendors Certified with AppViewX

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

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

Types of SAML Vendors

Types of SAML Vendors

- Okta
- OneLogin
- ADFS

- Forgerock
- Idaptive

- ADFS Integration
- Okta Integration
- Forgerock Integration
- OneLogin Integration
- Idaptive Integration

ADFS Integration

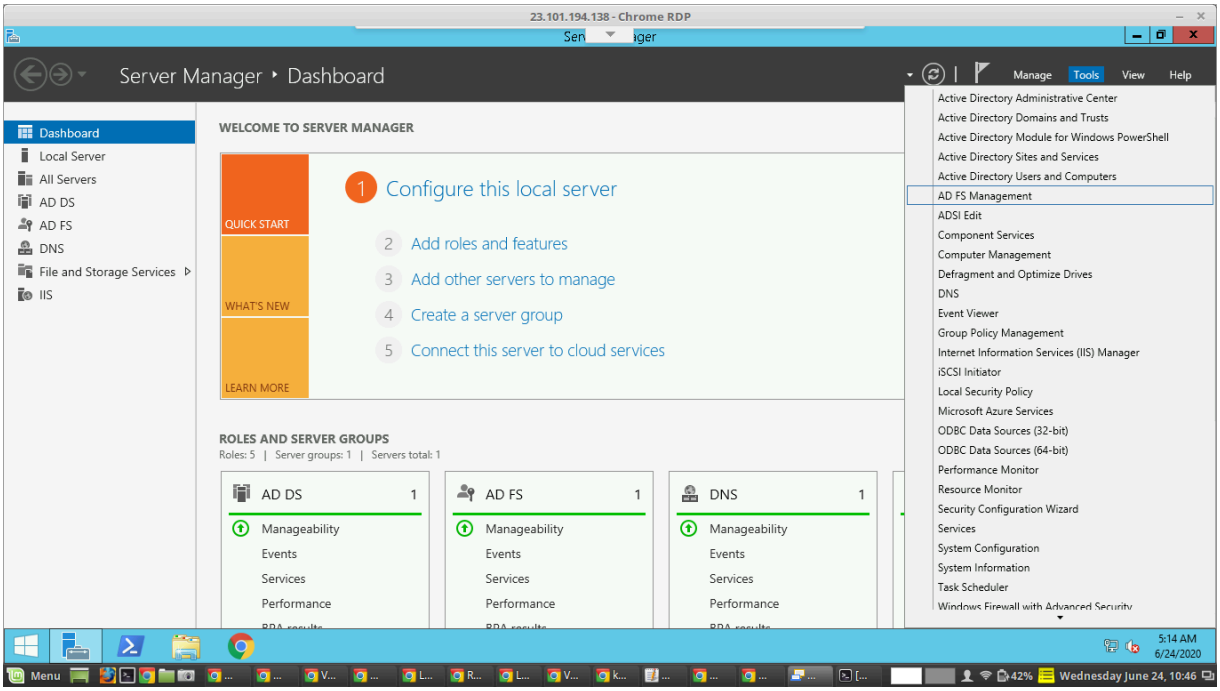
The below steps are performed at the IdP end. The navigation and screenshots might differ based on the version of the IdP. (This is just an example configuration)

Prerequisite

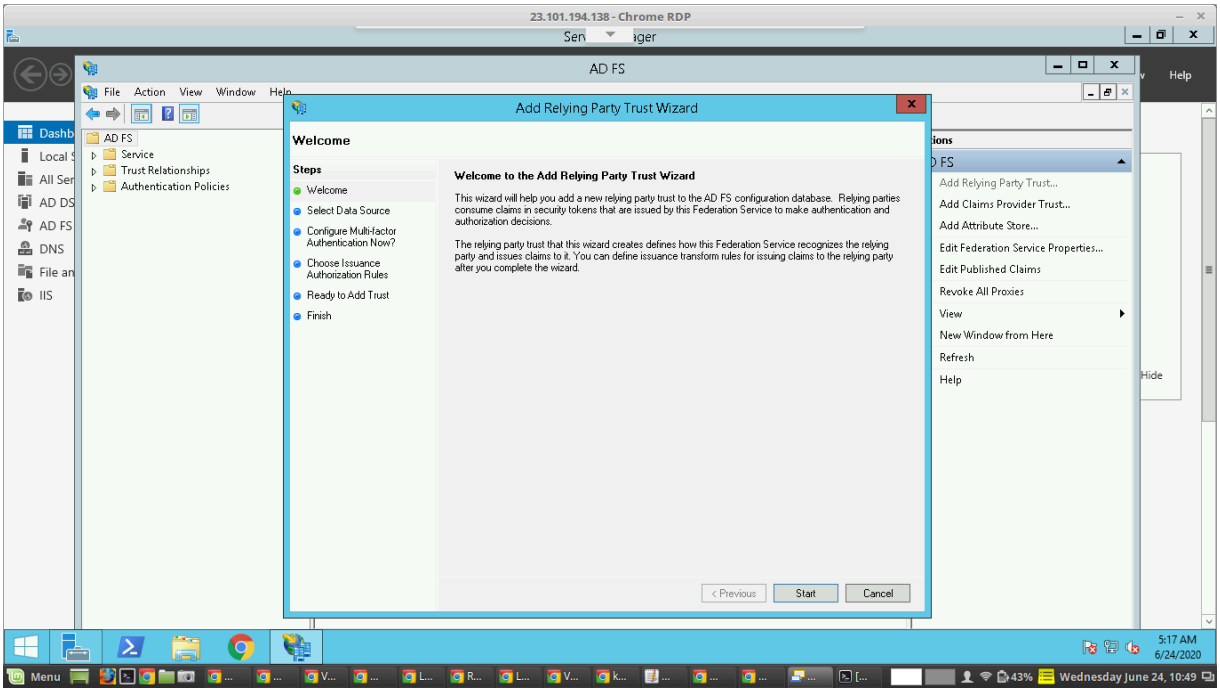
To enable ADFS based single sign-on, the ADFS service should be installed and configured with the respective Active Directory Domain.

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

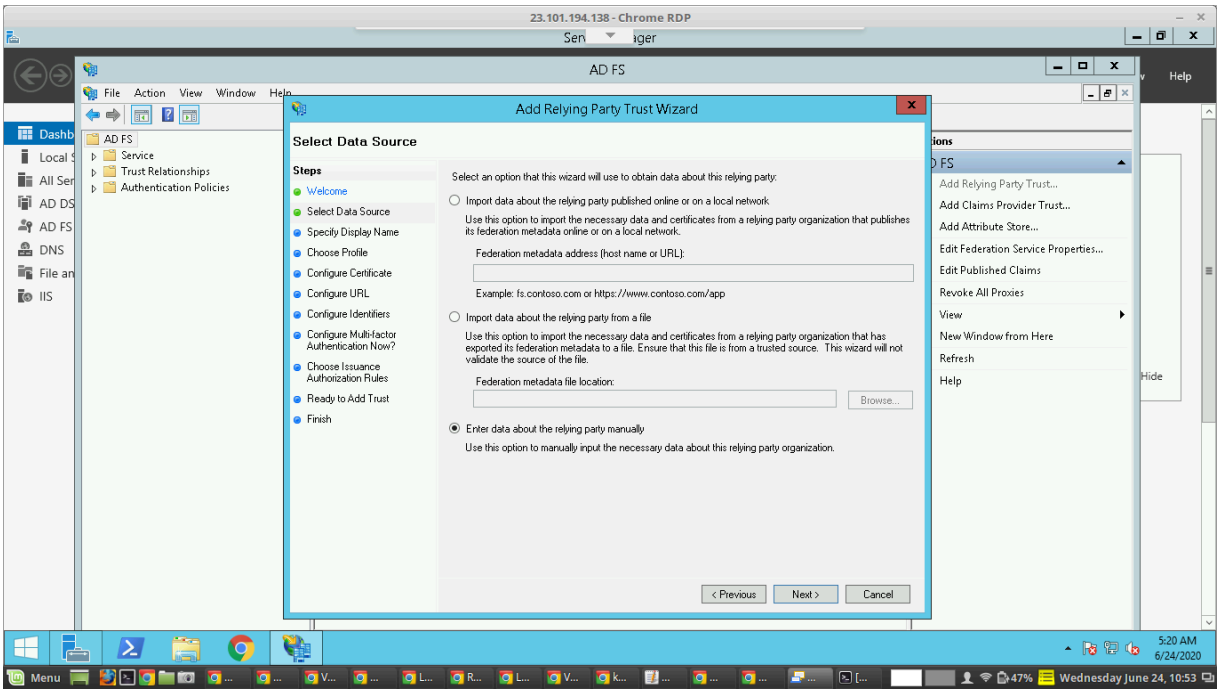
1. Navigate to Server Manager > Tools > AD FS Management.



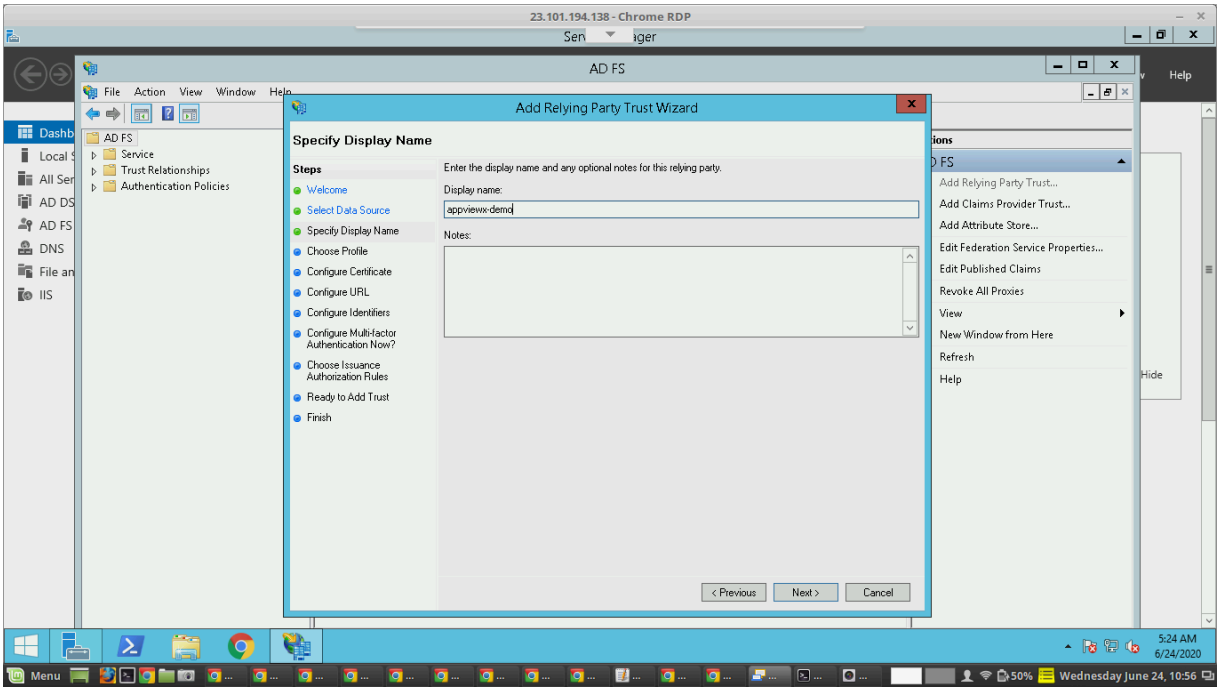
2. In AD FS under Actions select Add Relying Party Trust.



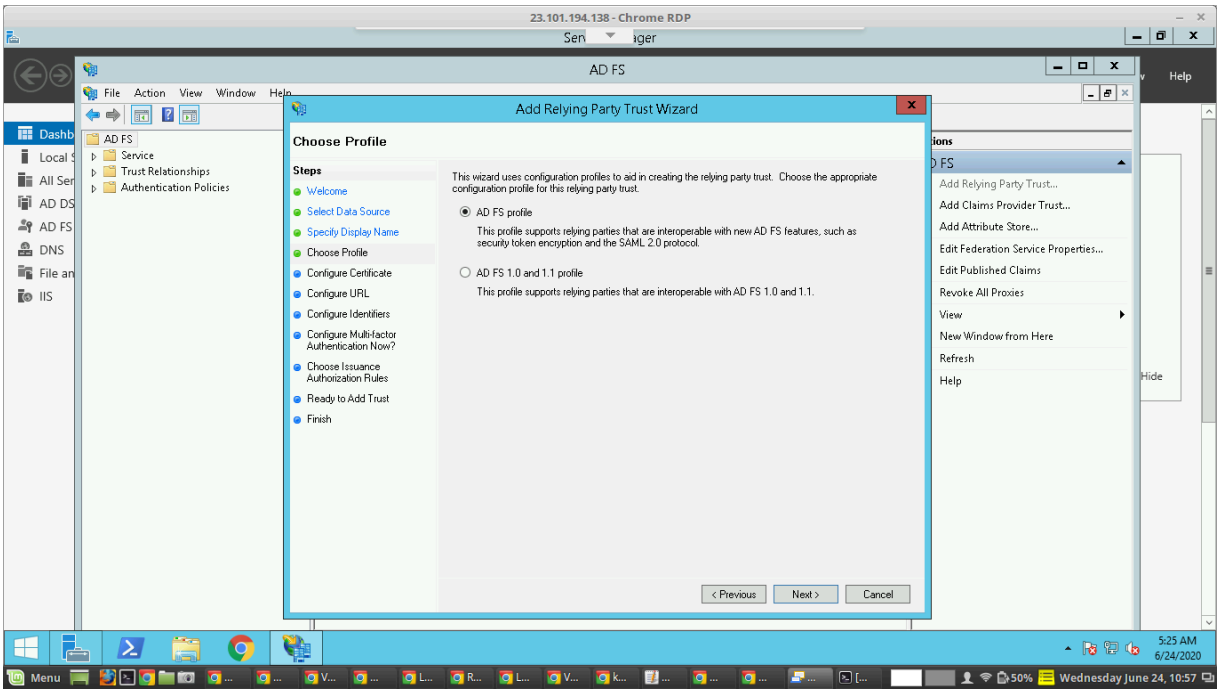
3. Start the wizard.
4. In Select Data Source choose the option Enter Data about the Relying Party Manually and select Next.



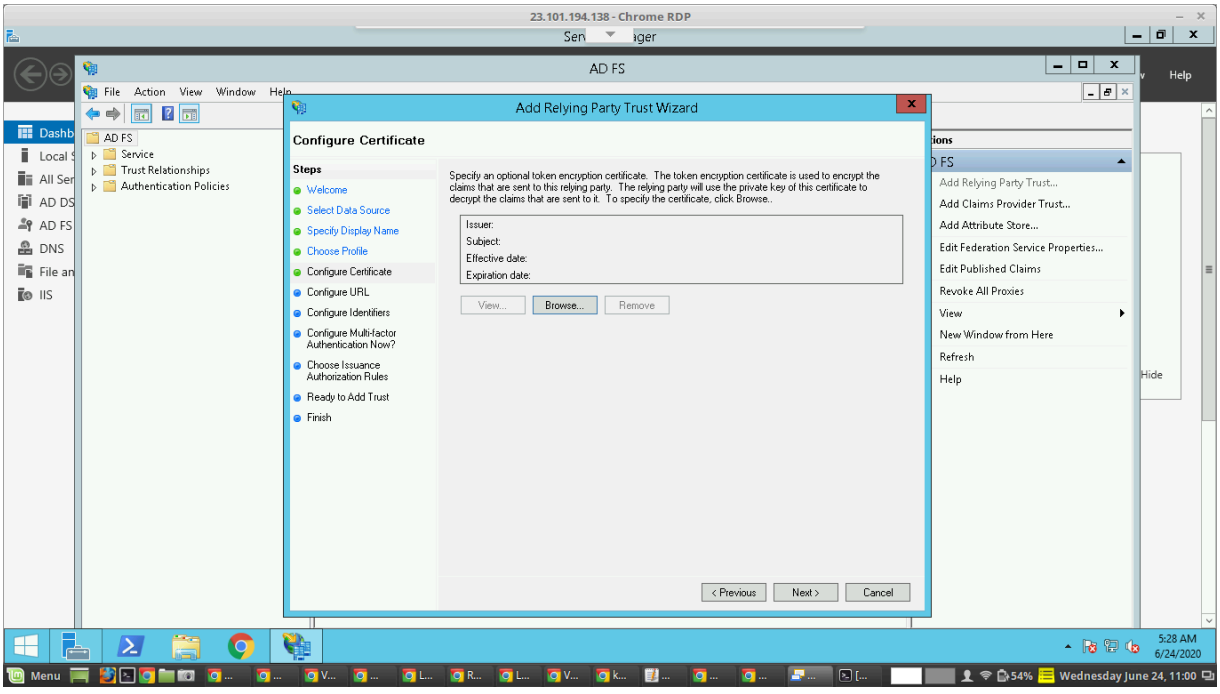
5. Provide a Display Name to the Configuration and select Next.



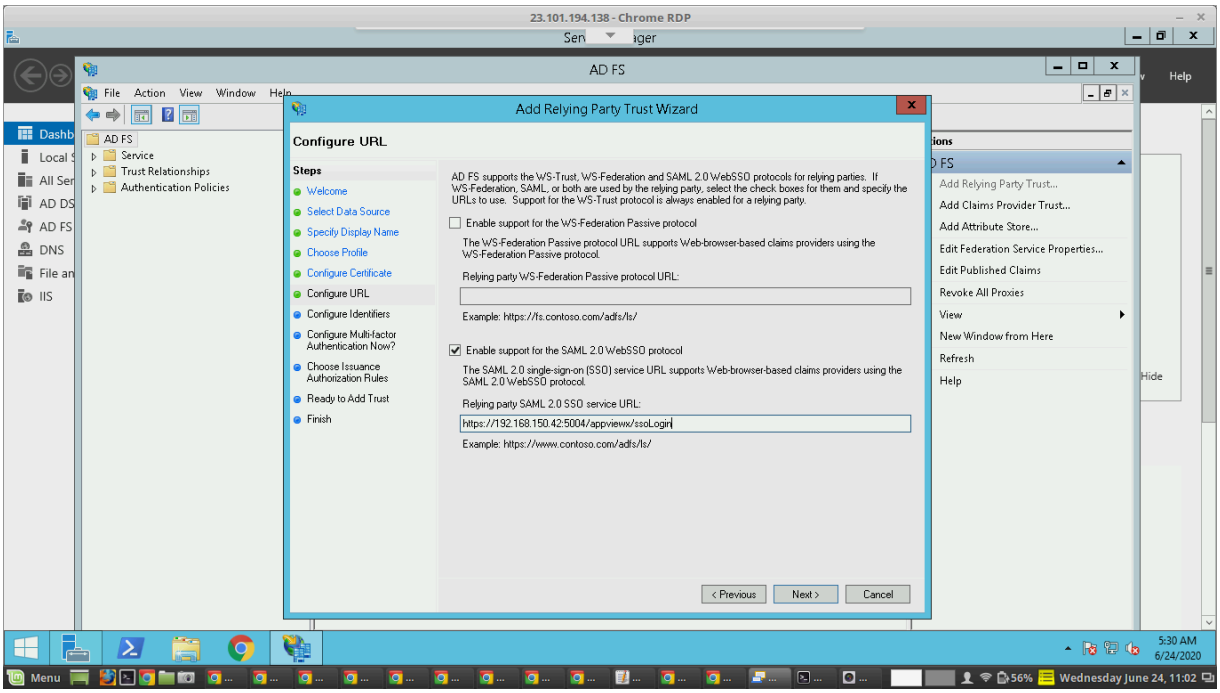
6. Under the Choose Profile Select the first configuration profile AD FS profile and select Next.



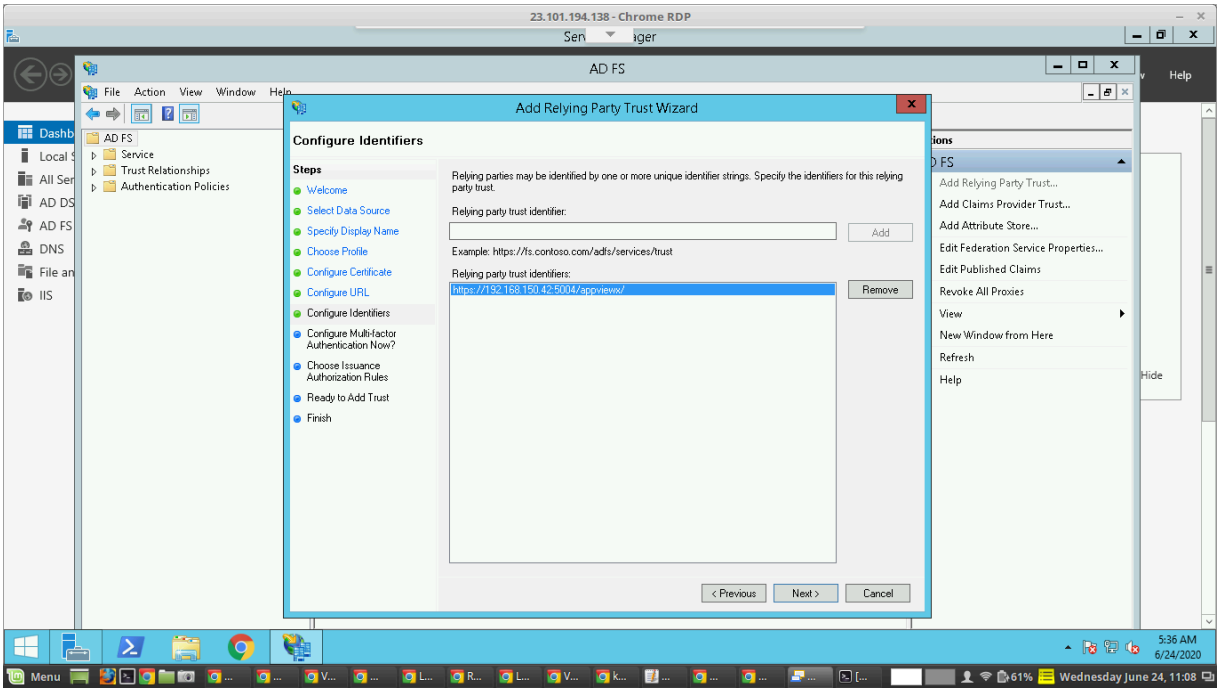
7. Add a new token encryption certificate if needed or leave it with the default setting and select Next.



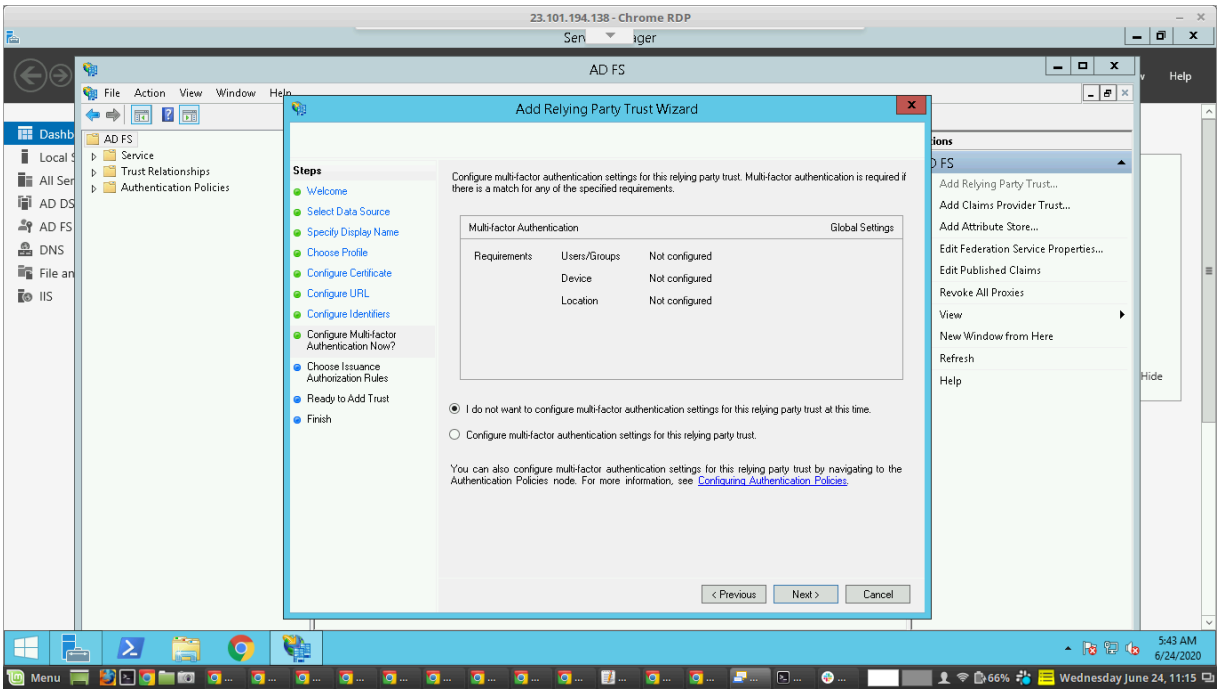
8. Under the configure URL, choose the third option Enable support for SAML 2.0 WebSSO protocol and enter the AppViewX Service URL which was copied in the previous step of Enabling SSO in AppViewX and select Next.



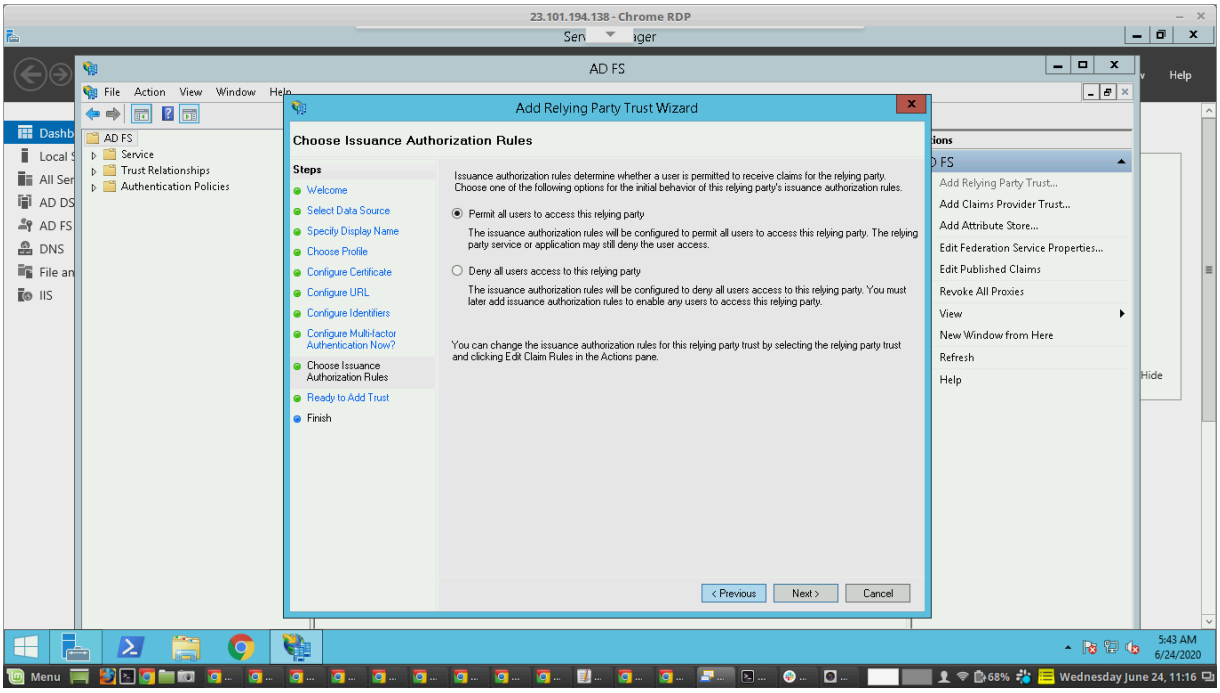
9. Under the configure identifiers enter the AppViewX Entity ID which was copied in the previous step of Enabling SSO in AppViewX and select Add and select Next.



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

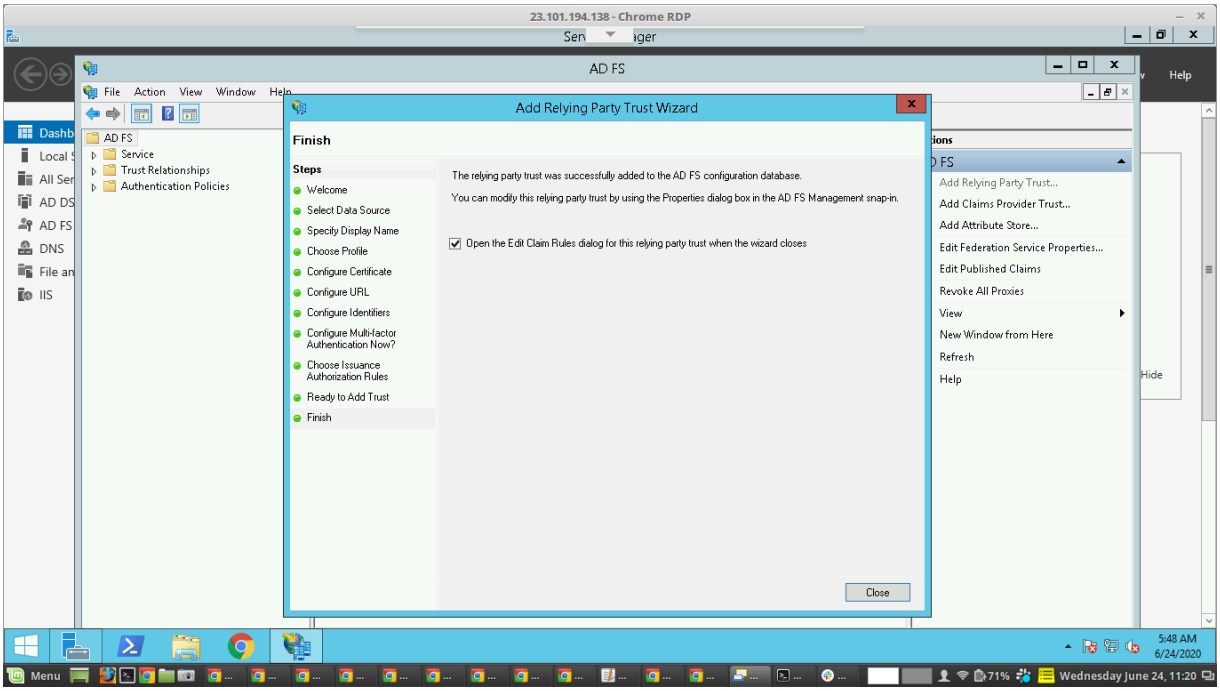


11. Under Choose Issuance Authorization Rules select Permit All Users to access this relying party and select Next.



12. Under Ready to Add Trust review the configuration done in the wizard and select Next.

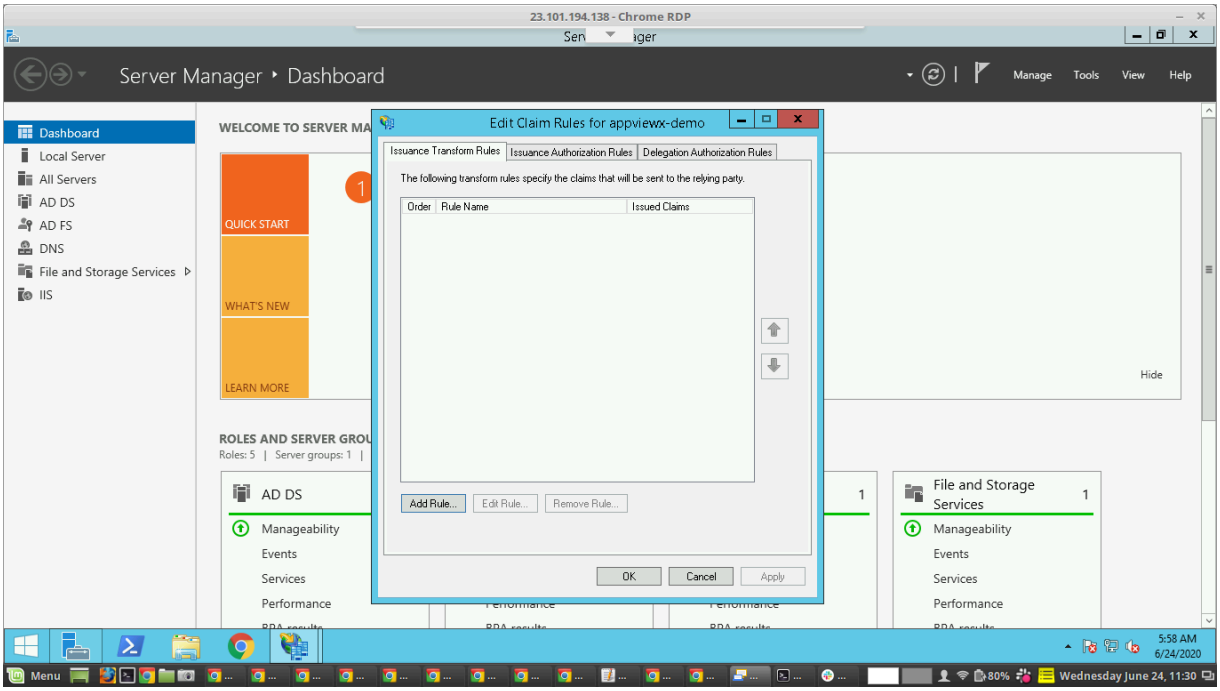
13. Under Finish enable the checkbox Open the Edit Claims and select close.



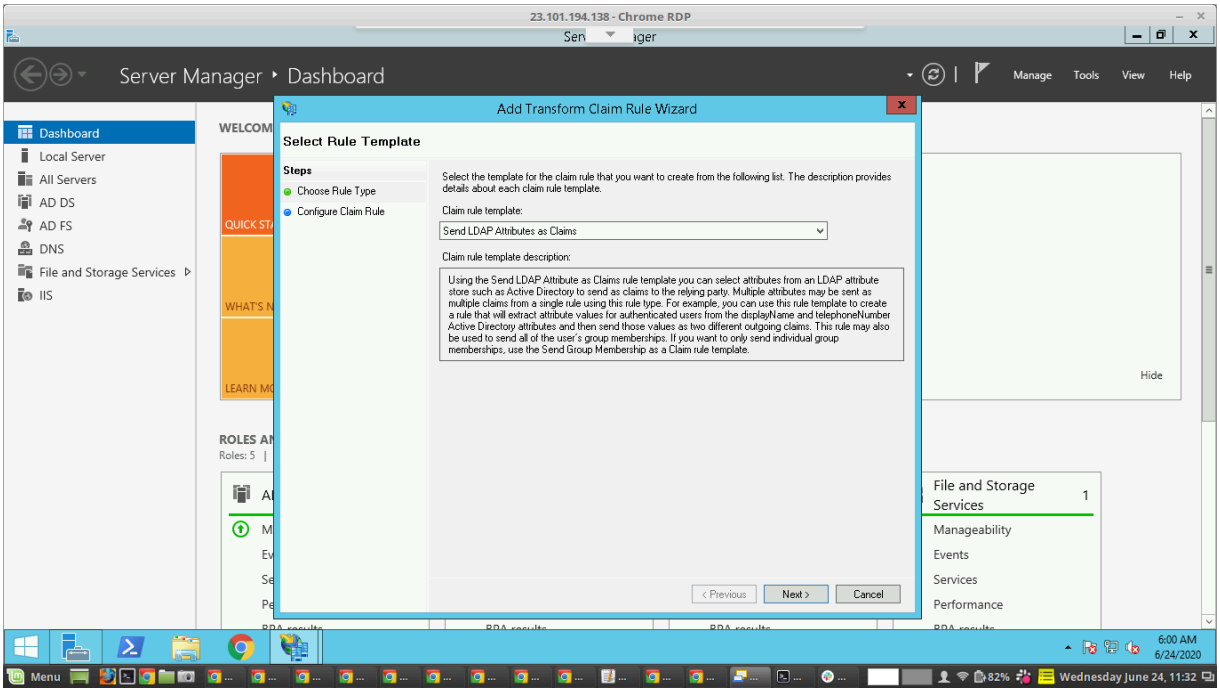
Add Claim Rules

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.



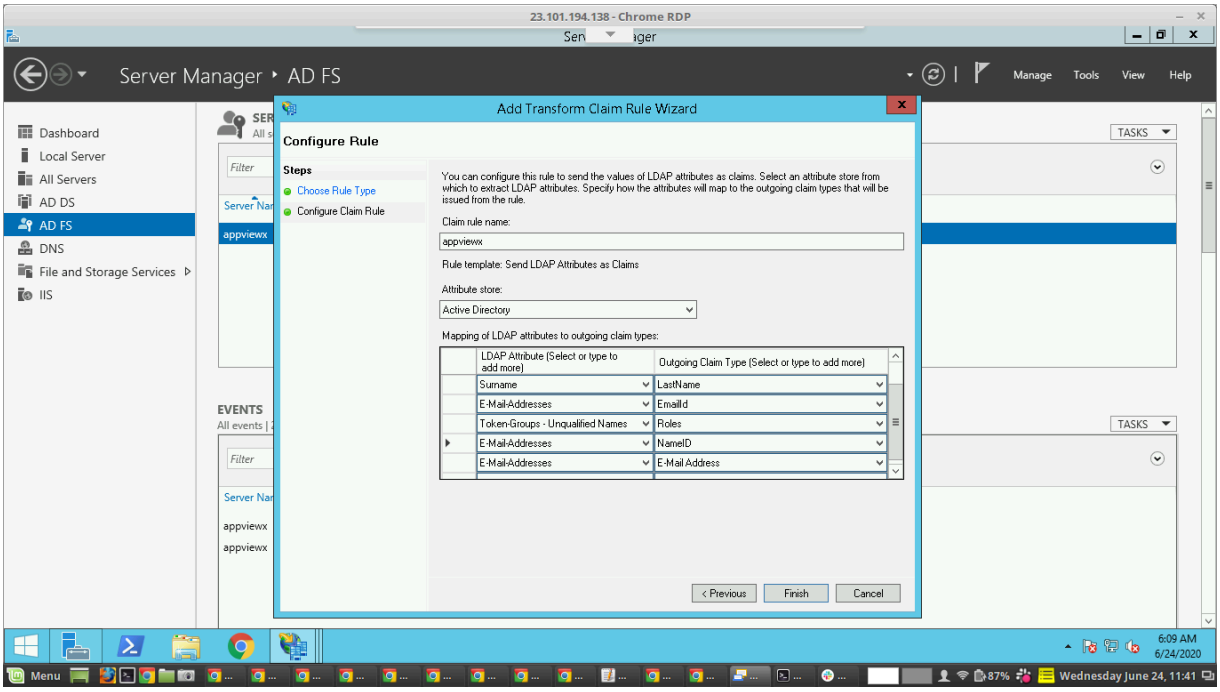
2. Under the Rule Template choose Rule Type as Send LDAP attributes as Claims and select Next.



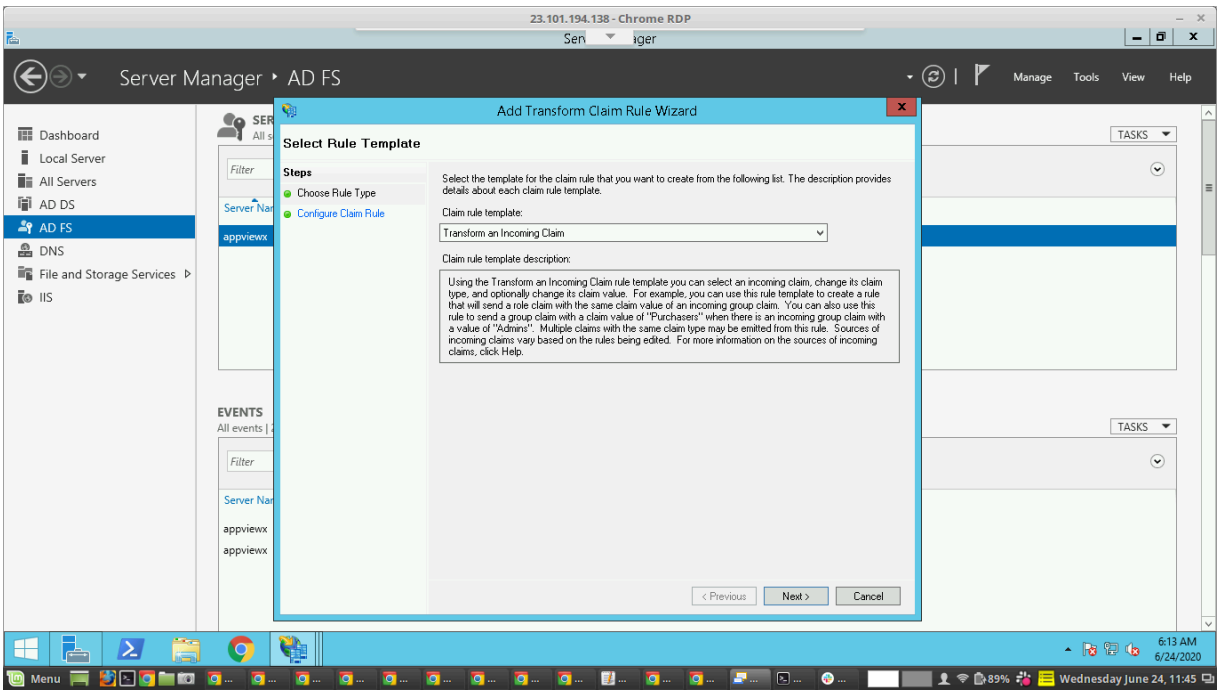
3. Provide a Rule name and select the attribute store as Active Directory and provide the claim types as below and select Finish. Display-Name > FirstName, Surname > LastName, E-Mail-address >

EmailId, Token-Groups-Unqualified Names > Roles, E-Mail-address > NameID, E-Mail-address > E-Mail-address.

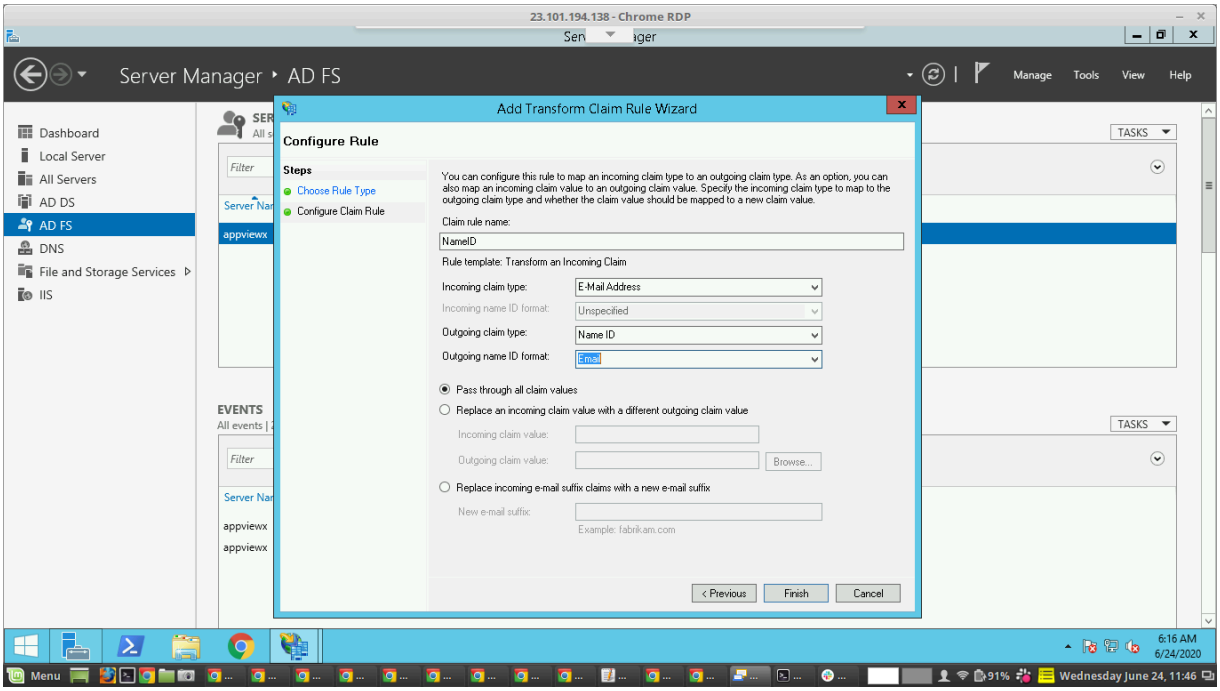
4. Create another rule to transform the incoming claim by clicking Add Rule > Rule Template (Transform an Incoming Claim) and select Next.



5. Provide a Rule Name and select the Incoming Claim Type as E-Mail-Address and Outgoing Claim Type as Name ID and Outgoing Name ID Format as Email and select Finish.

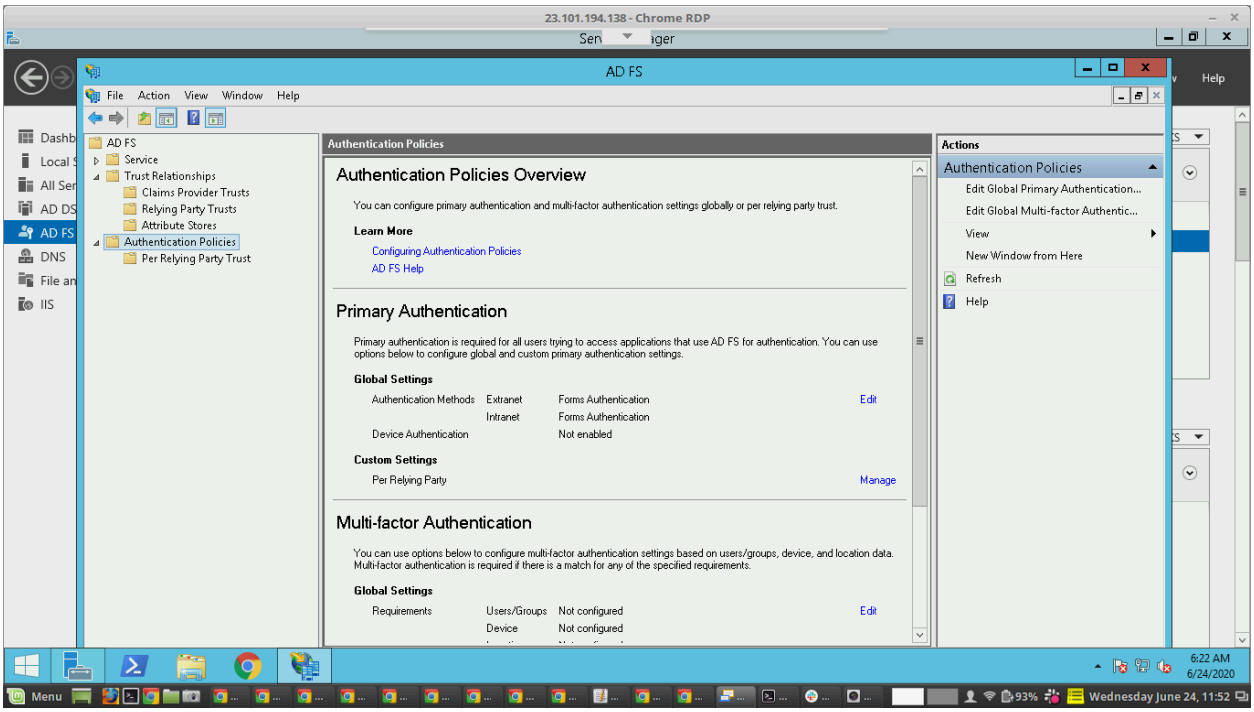


6. Now select Apply and OK in the Edit Claims pane.



Enable Form-Based Authentication

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



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

Sample URL:

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

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

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

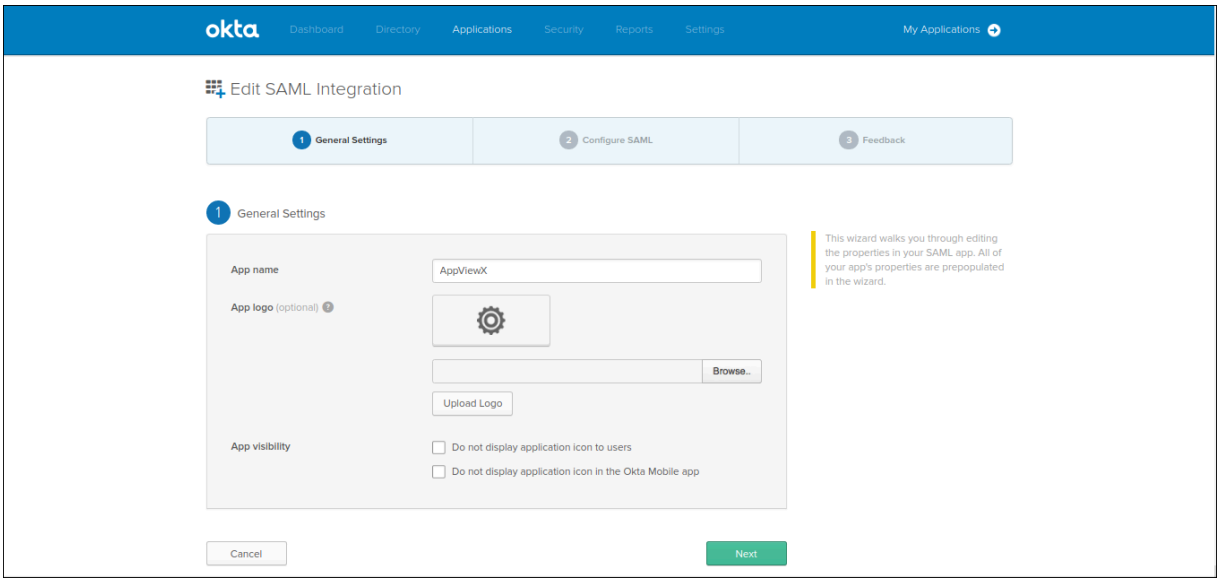
Okta Integration

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

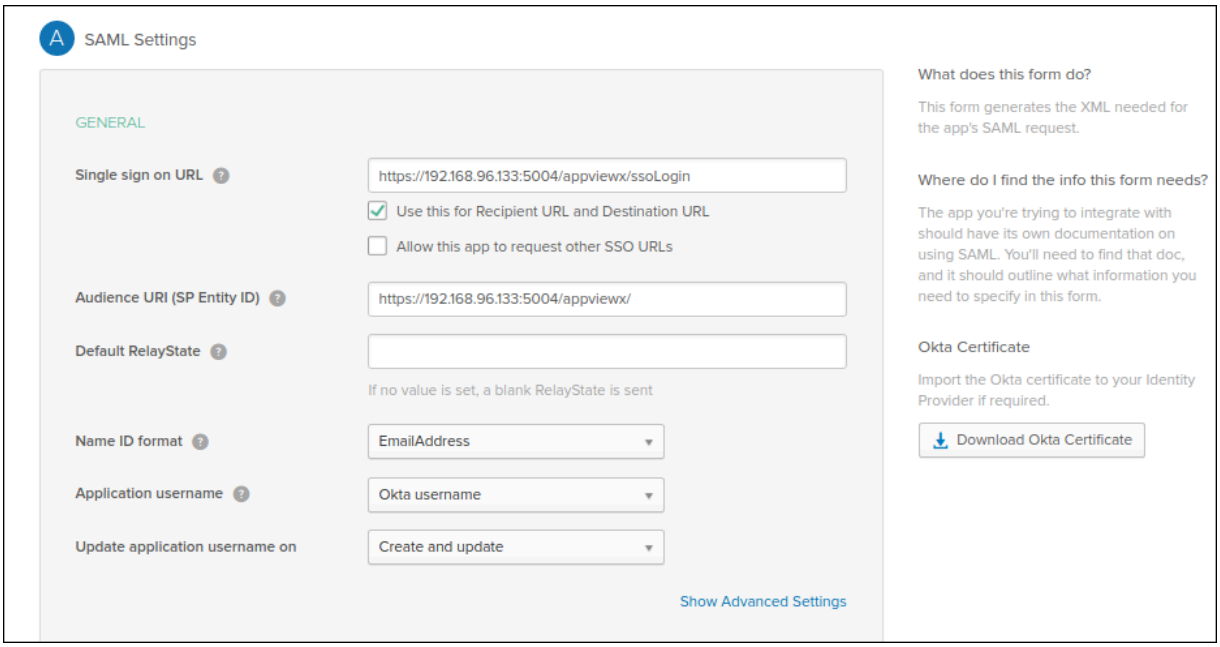
Complete the following steps to begin the IDP configuration:

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.

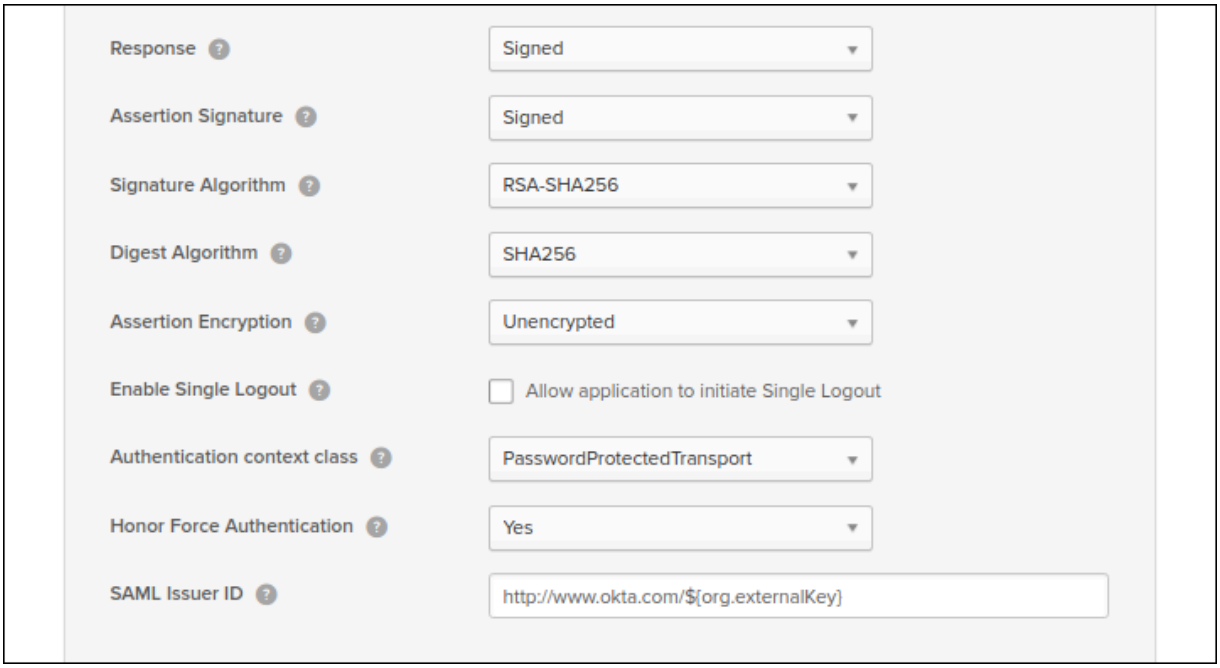
1. Create an application.



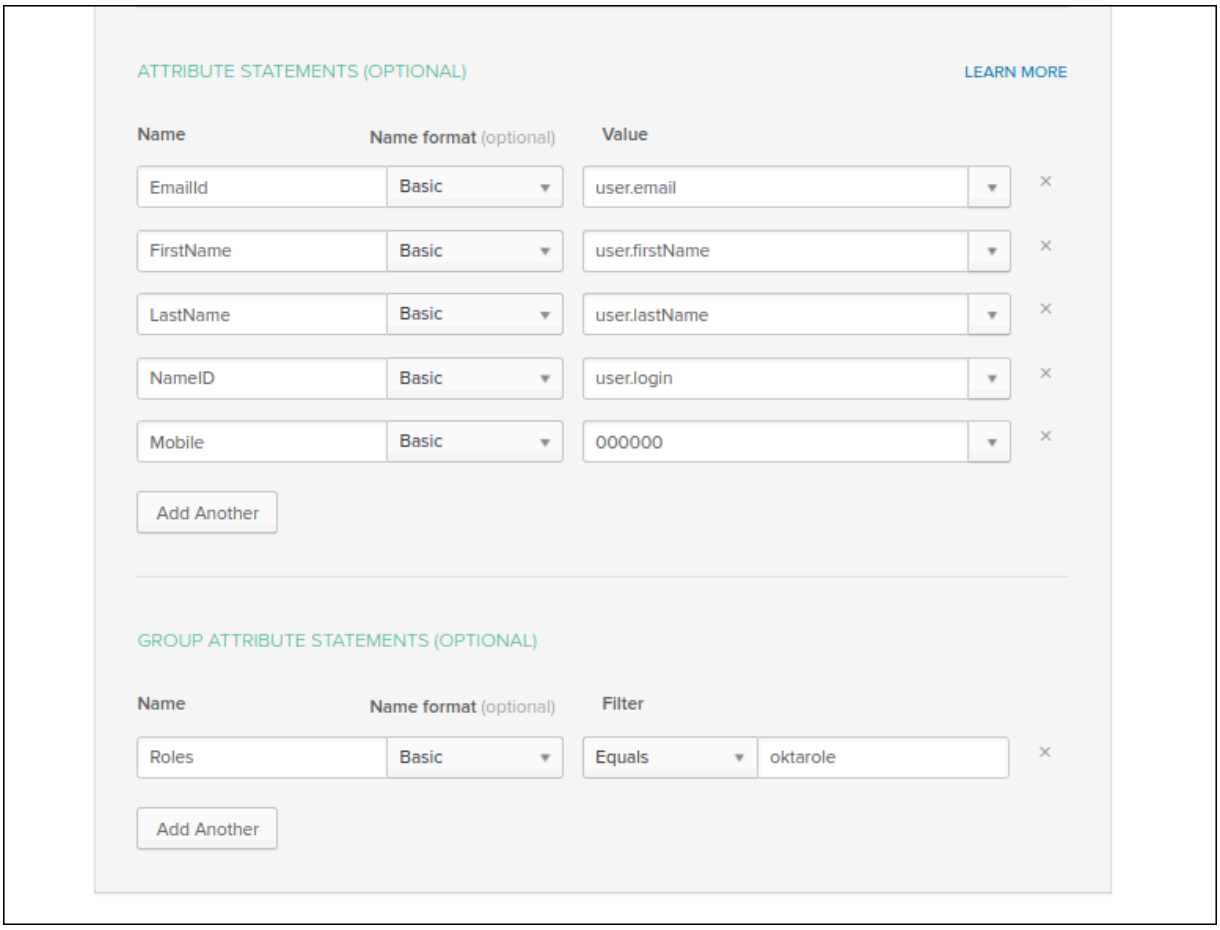
2. Configure service provider details.



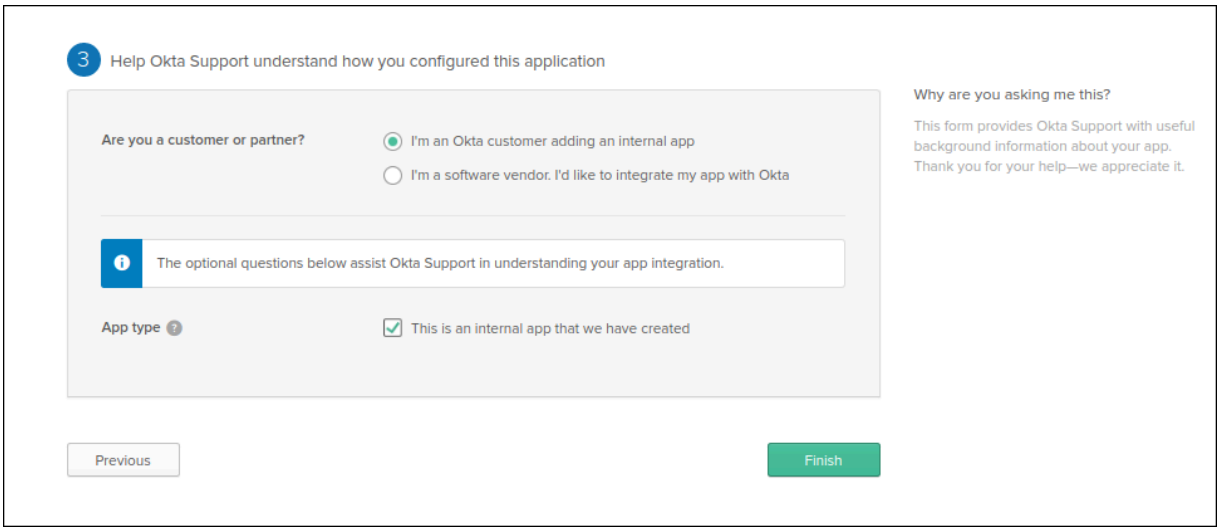
3. Show Advanced Settings screen.



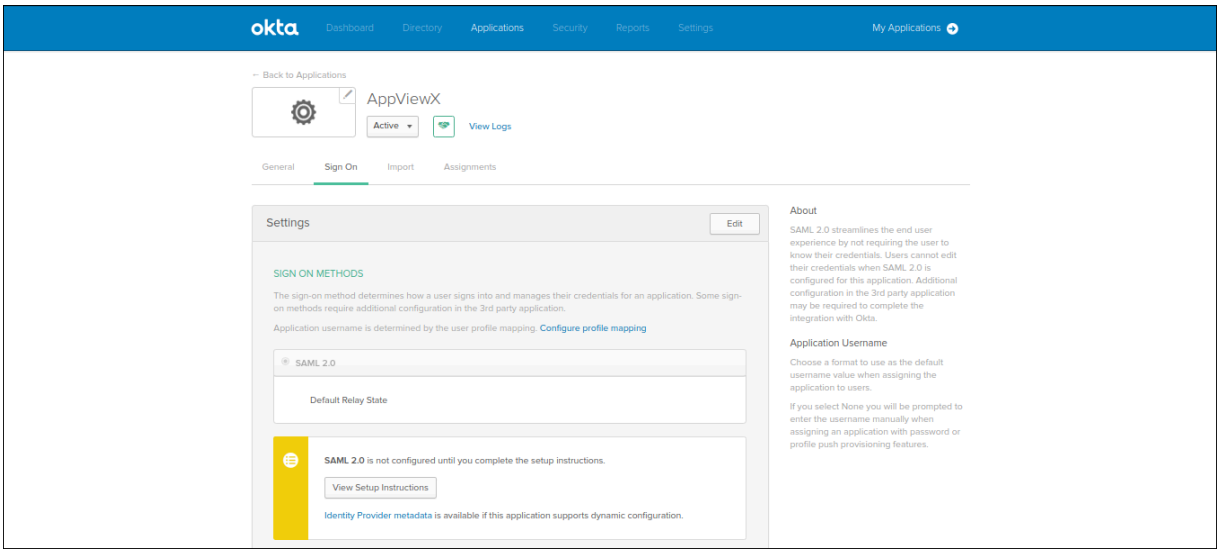
4. Configure the User Attributes to be passed during the SAML assertion.



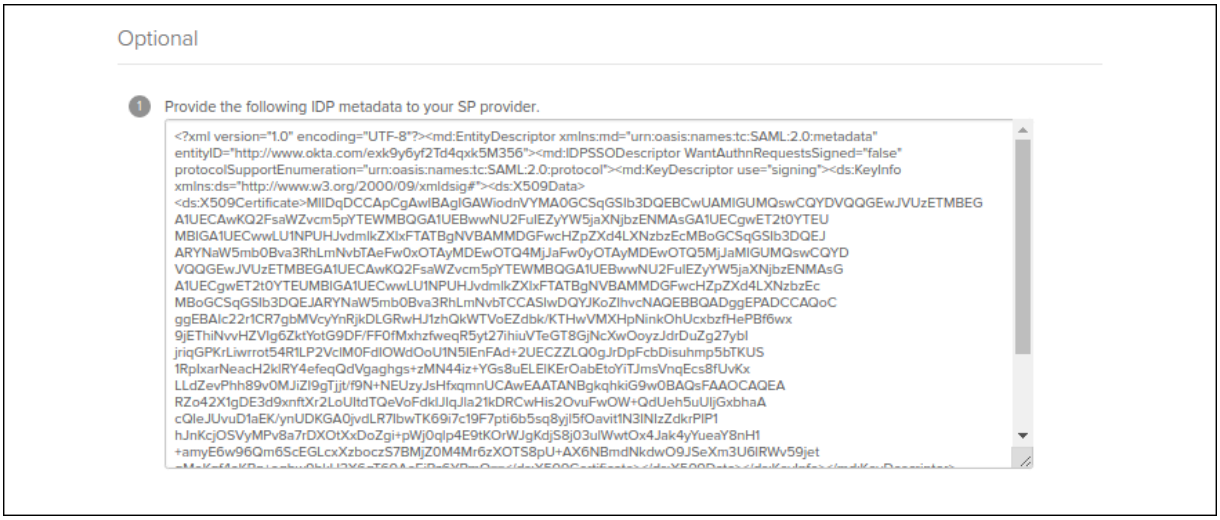
5. Finish the IDP configuration.



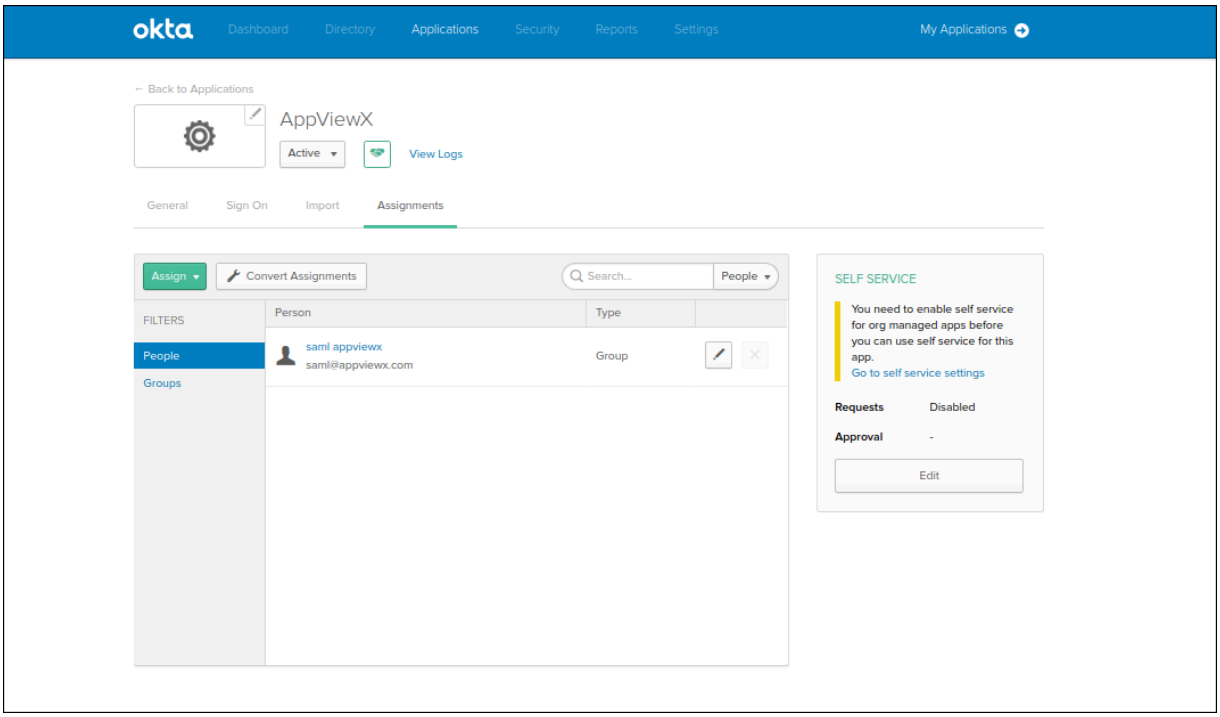
6. Click the View Setup Instructions in the Sign On tab.

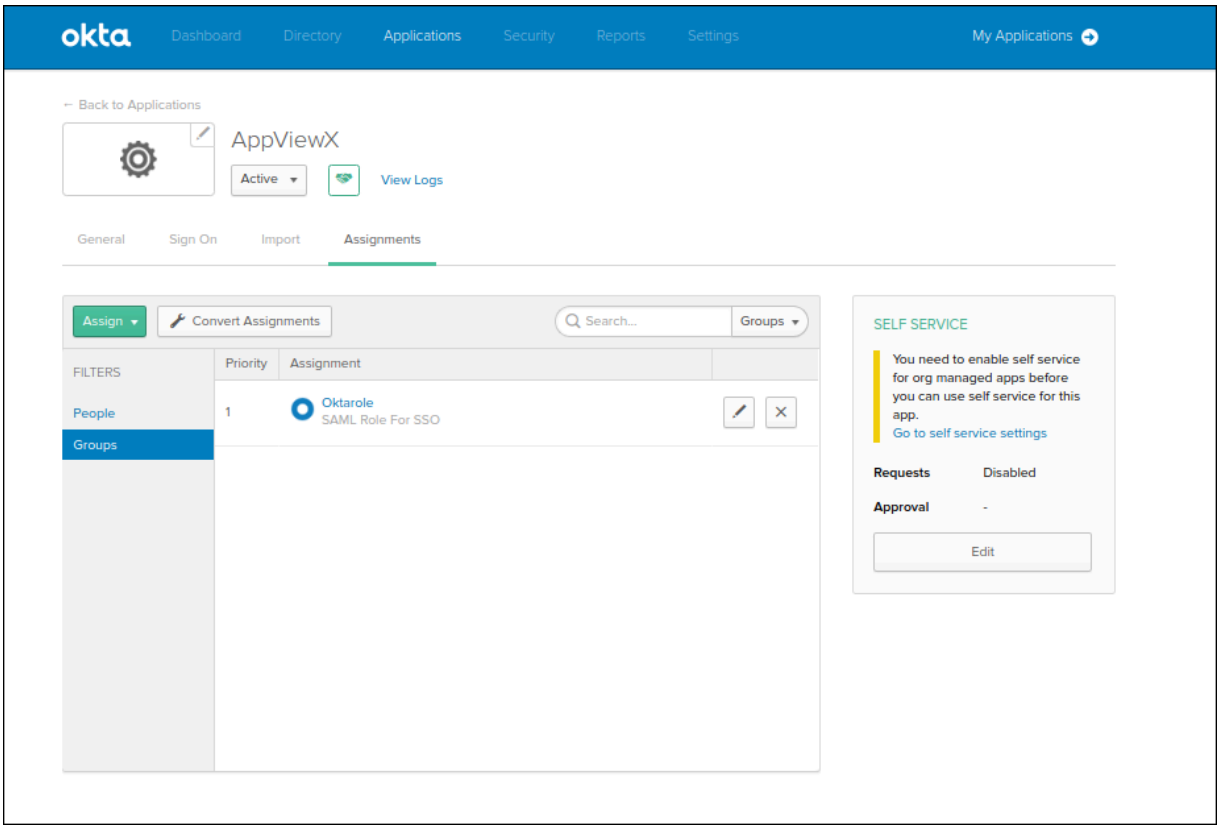


7. Copy and paste the content from the Optional section and save it as an XML file.

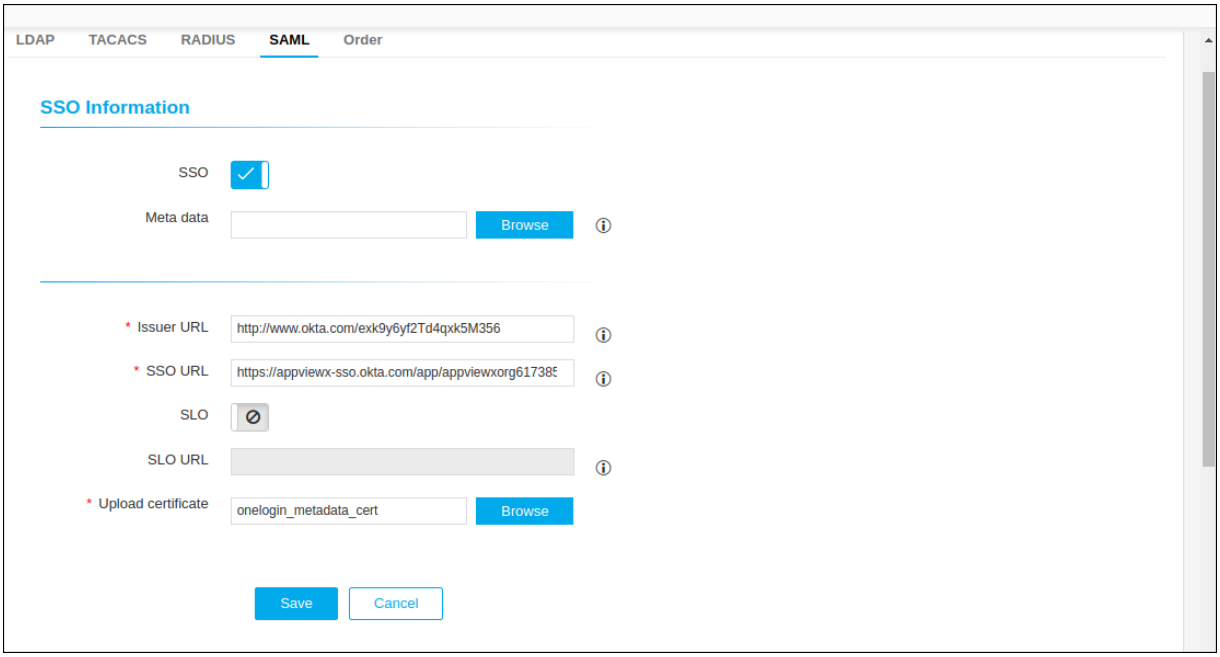


8. Map the application to a User/User Group.



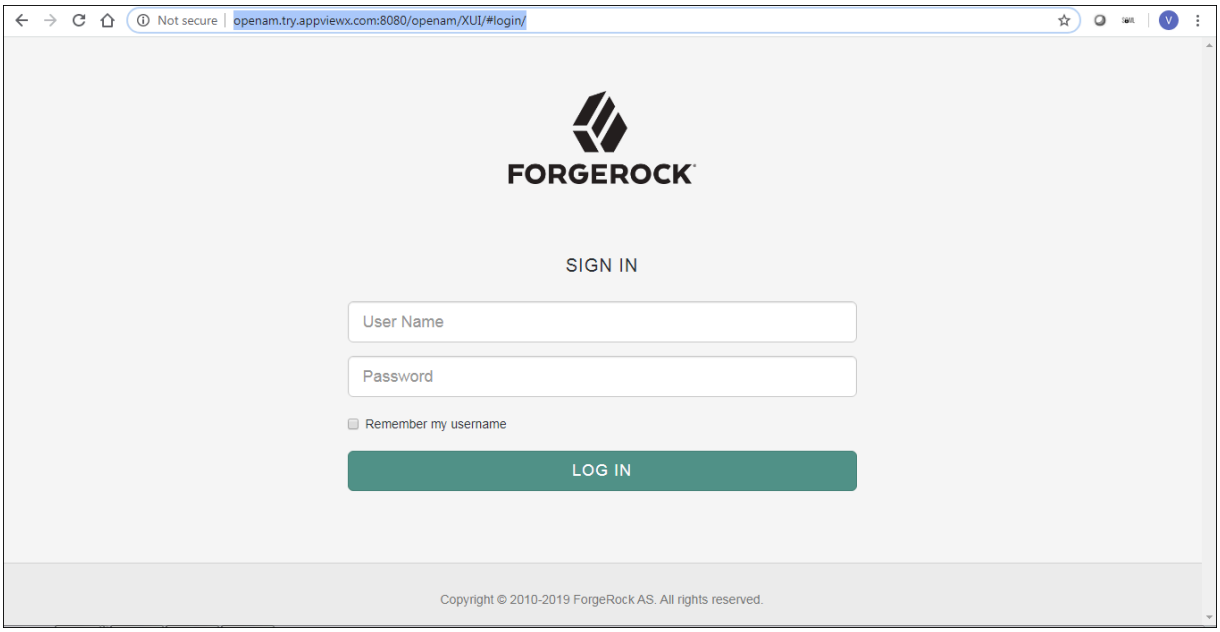


9. Browse and upload the IDP metadata to AppViewX. Then, click Save.

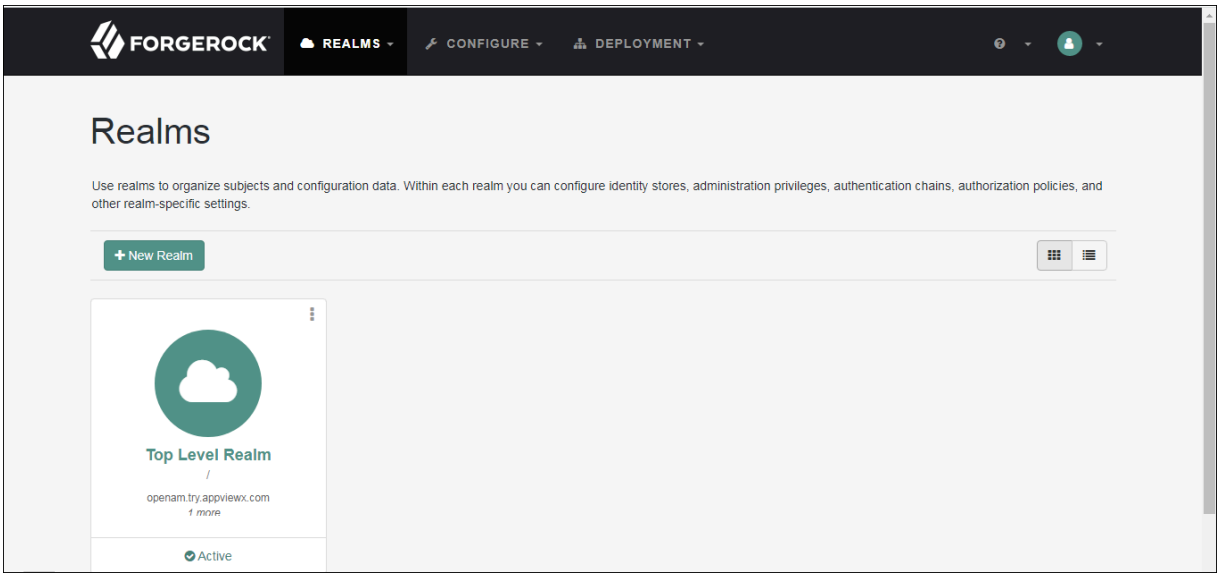


Forgerock Integration

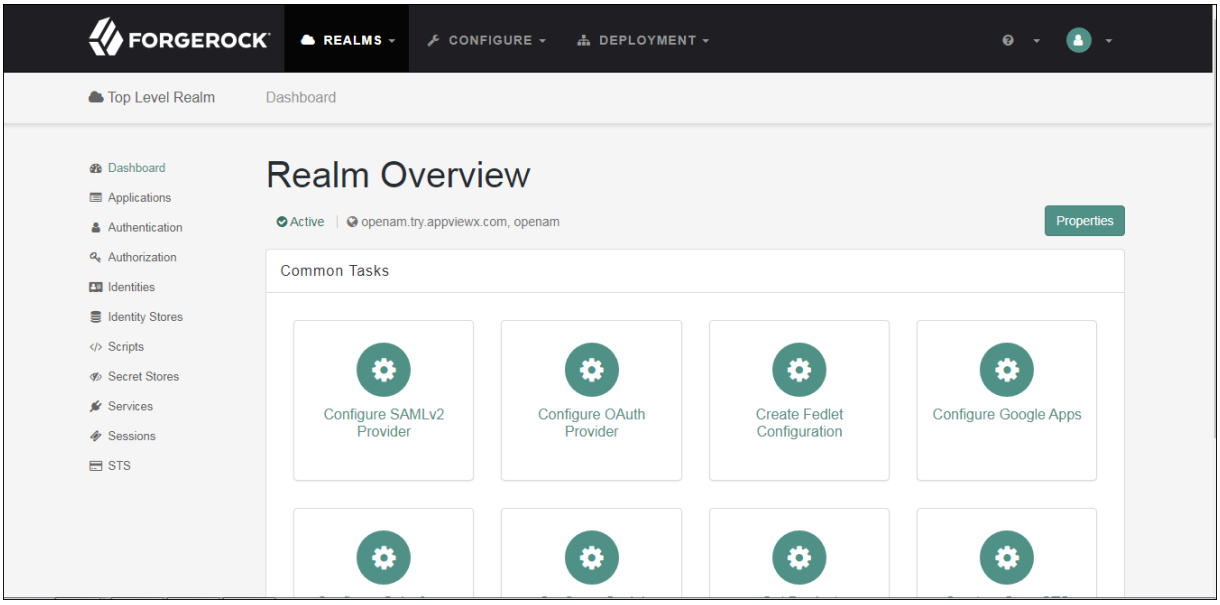
1. Login to the Forgerock IDP intense / console.



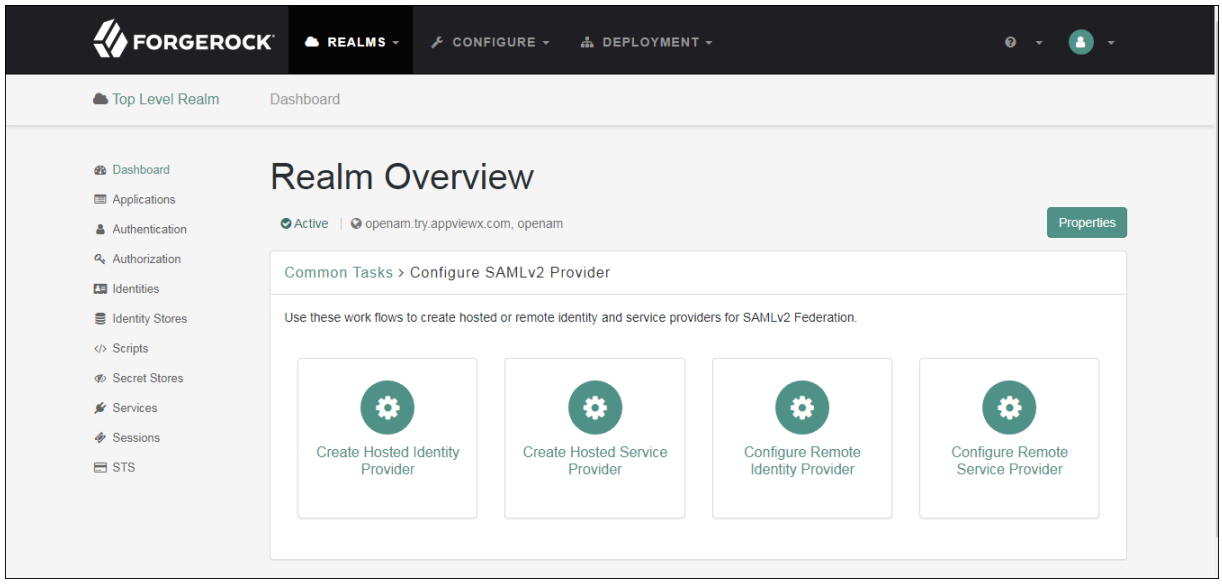
2. Select the respective Realm.



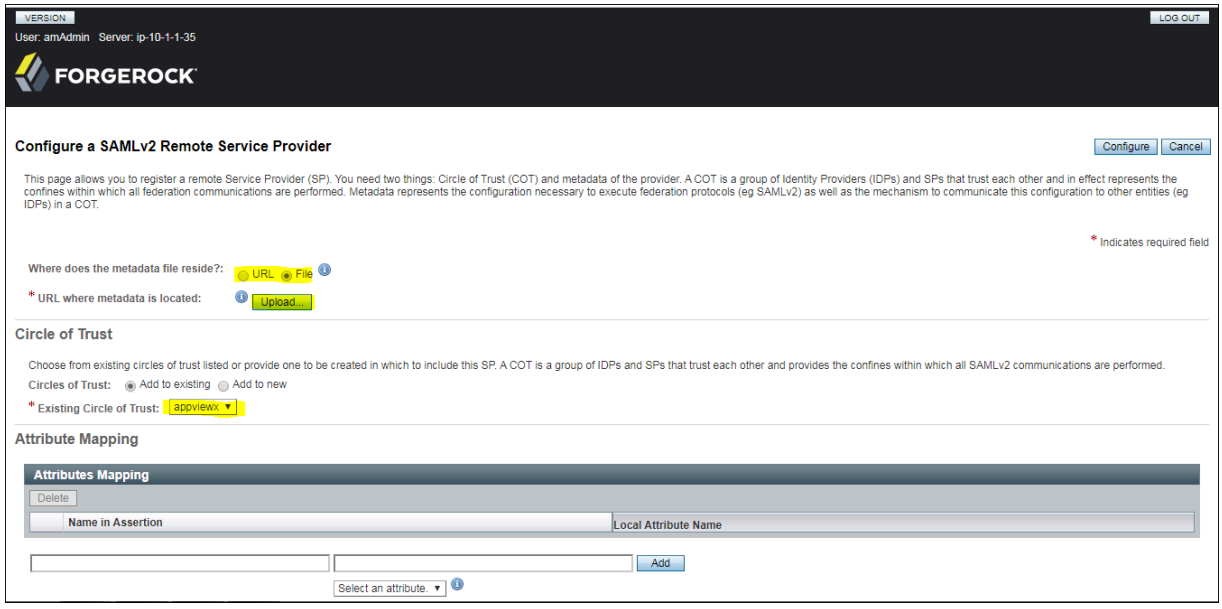
3. Select Configure SAML v2 provider under Common Tasks.



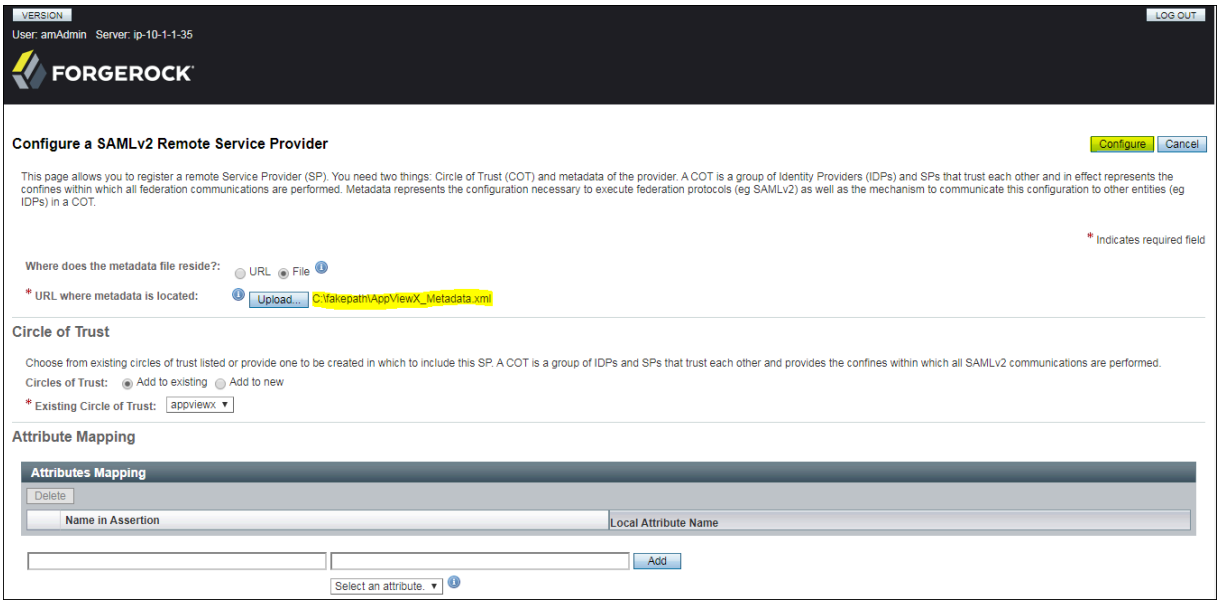
4. Select Configure Remote Service Provider for Configuring AppViewX configuration.



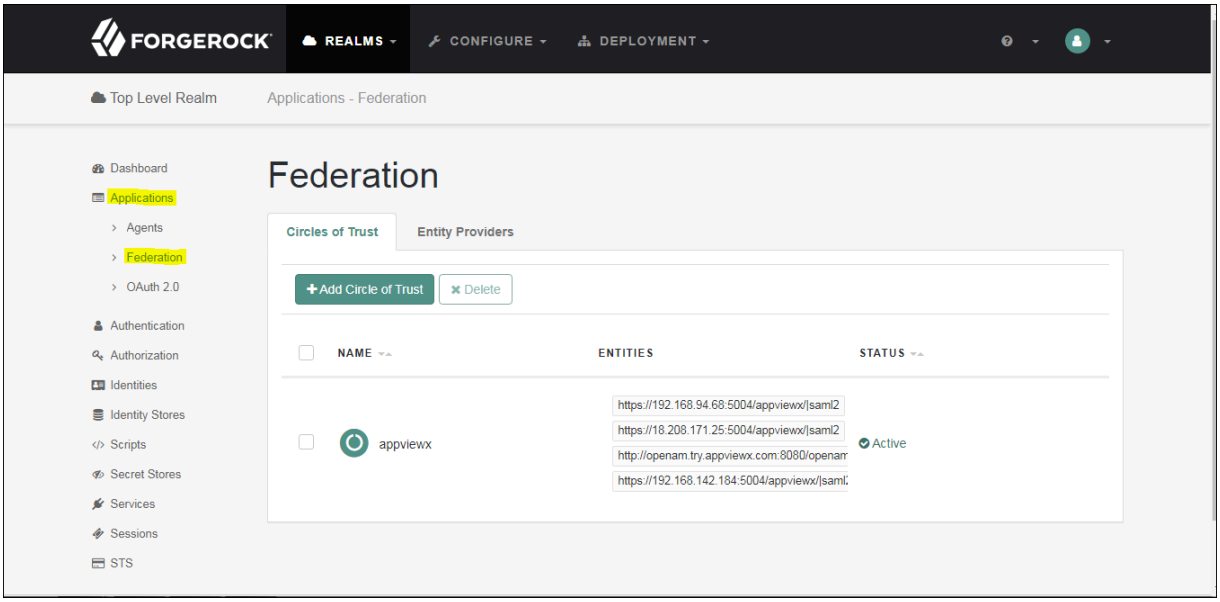
5. Choose File option for metadata upload and select/create the circle of trust for mapping AppViewX to the IDP and click upload.



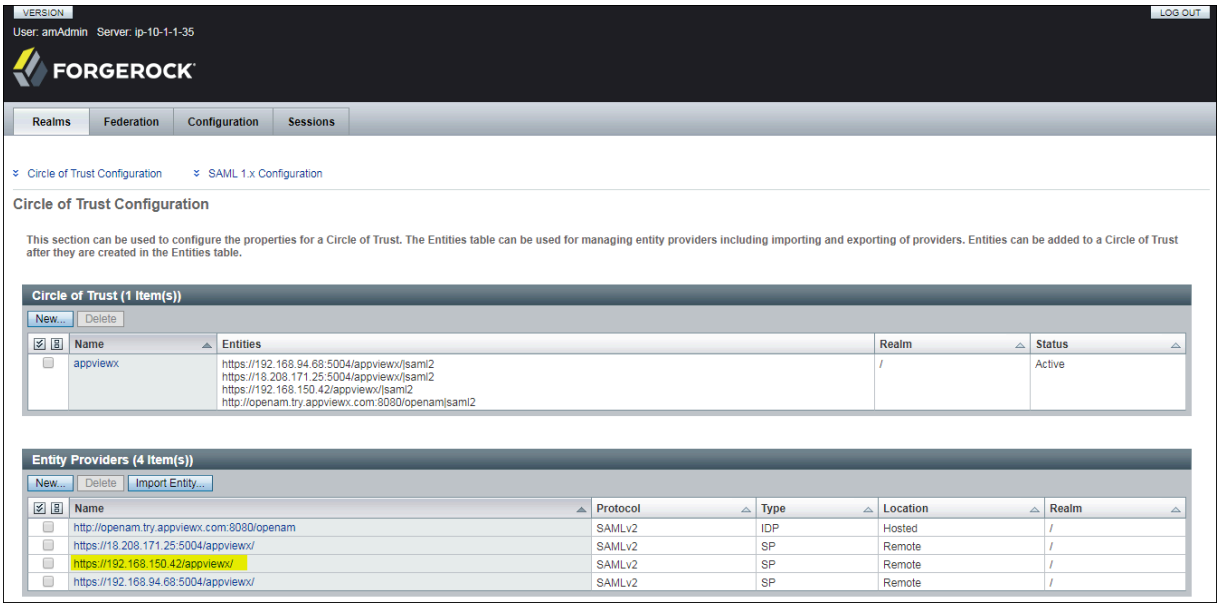
6. Upload the AppViewX Metadata which was downloaded earlier and click configure to save the settings.



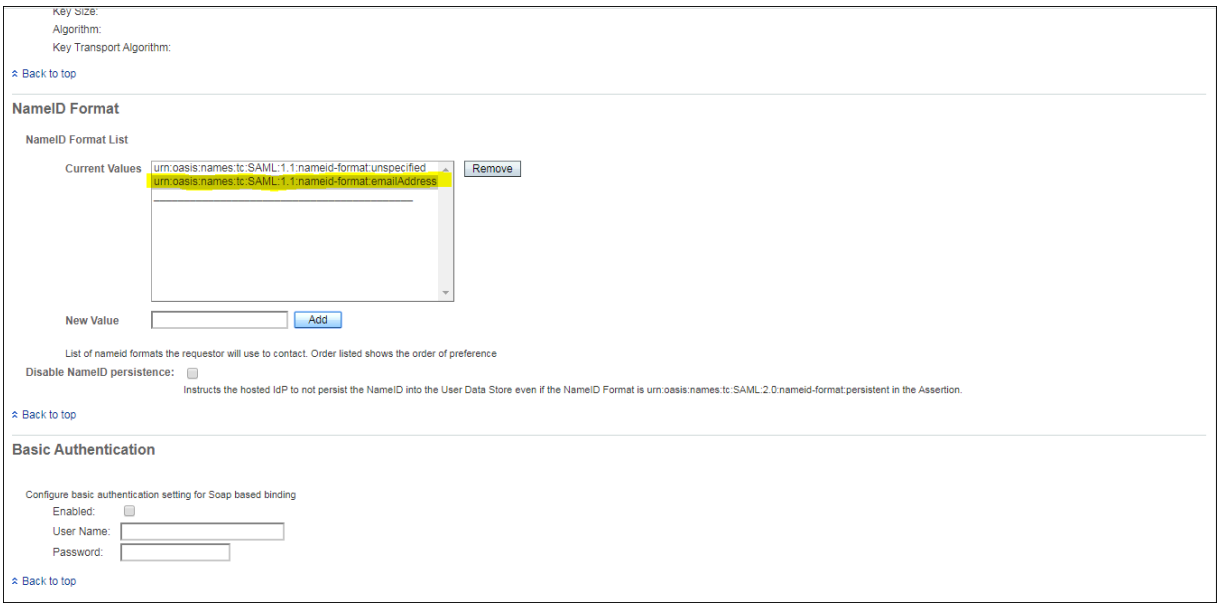
7. Once done the page will redirect to the common tasks under the specific realm. Now access the Applications > Federation from the left-hand side of the IDP.



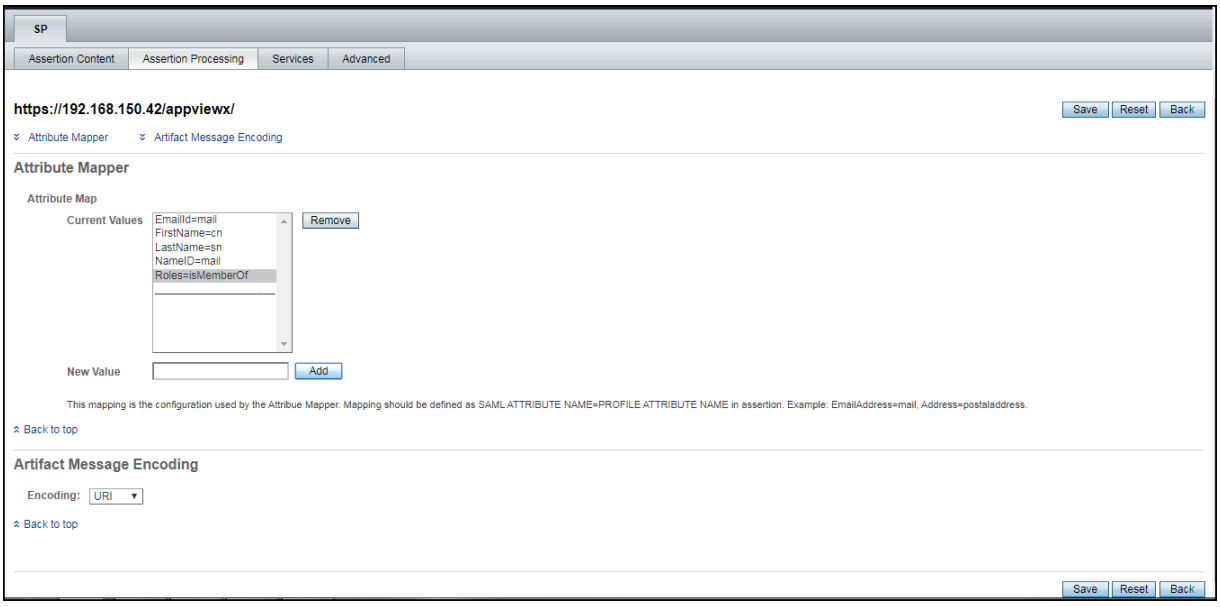
8. Now select the entity providers tab. This will redirect to the Federation tab with the list of Service providers and IDP configuration.



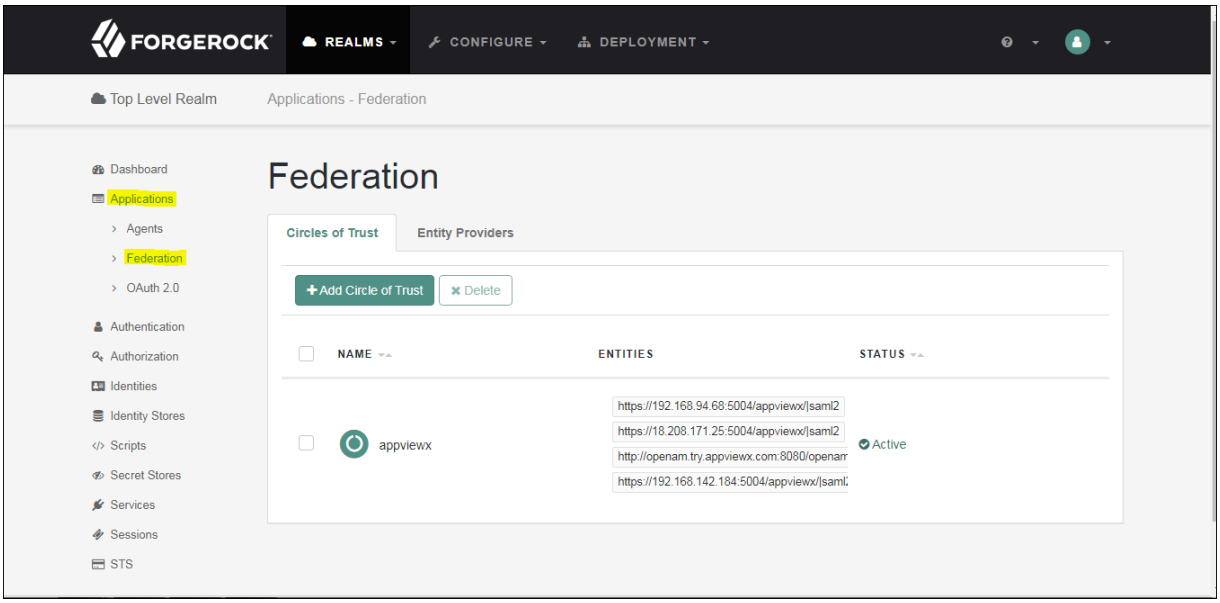
9. Select the respective Entity ID which will navigate to the settings of the respective entity configuration.
10. On the Assertion Content tab add the following in the NameID Format and click Save on the top right.
    urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress



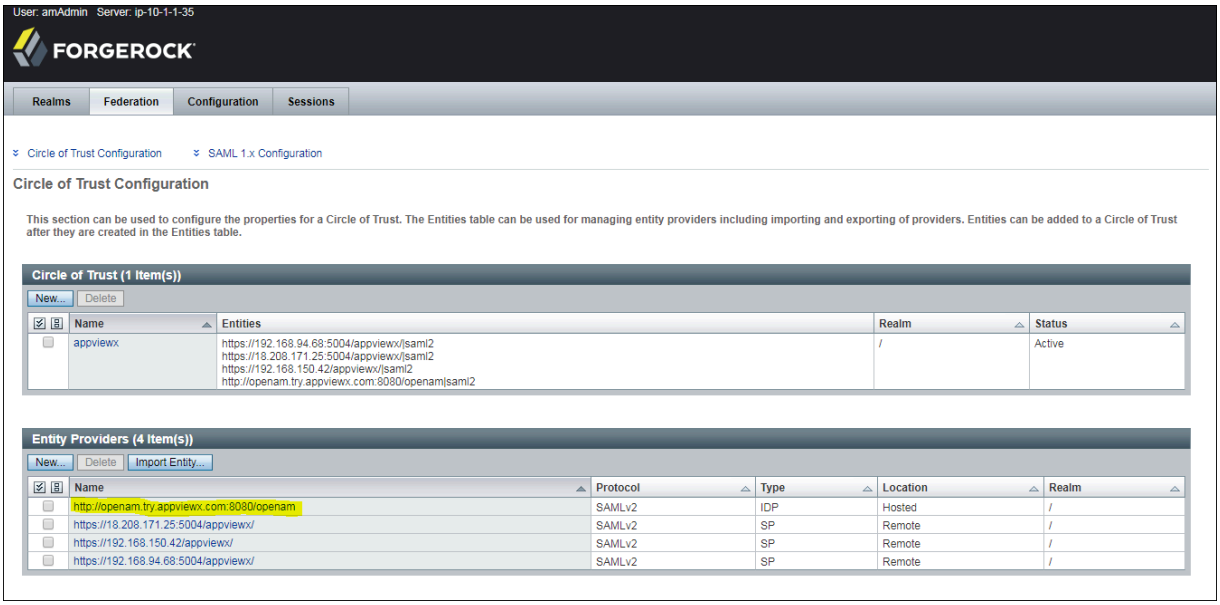
11. On the Assertion Processing tab add the below assertion parameter which has to be passed as a part of the SAML assertion and click save. EmailId=mail ; FirstName=cn ; LastName=sn ; NameID=mail ; Roles=isMemberOfAuthentication.



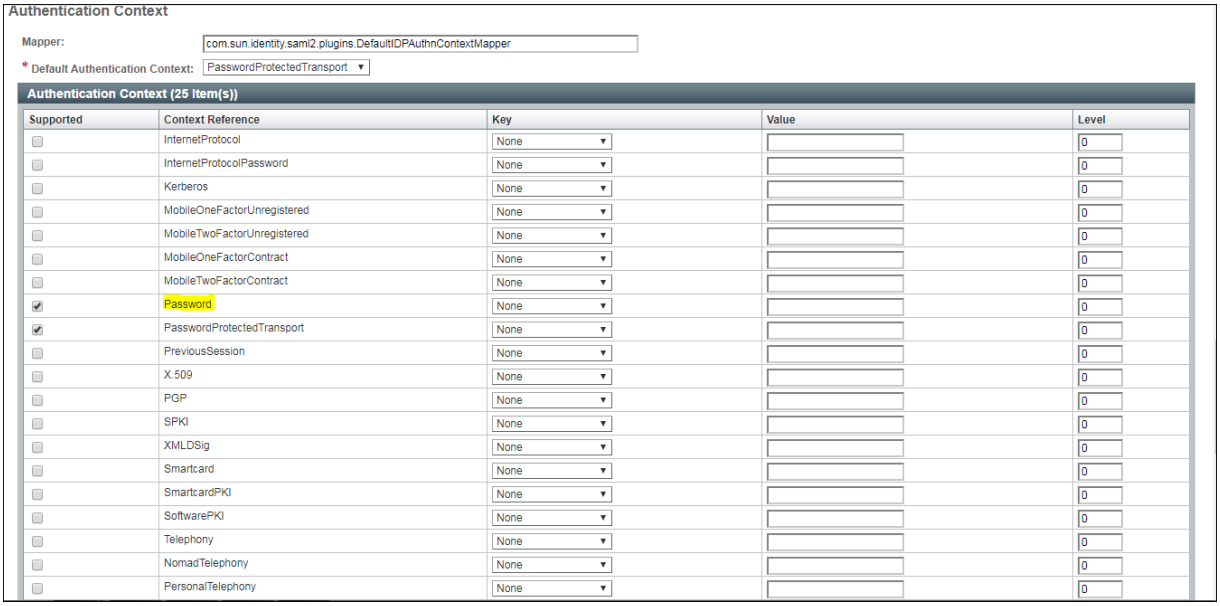
12. Modify IDP configuration to accept a password-based Authentication Context. Navigate to Applications > Federation and select Entity Provider TAB.



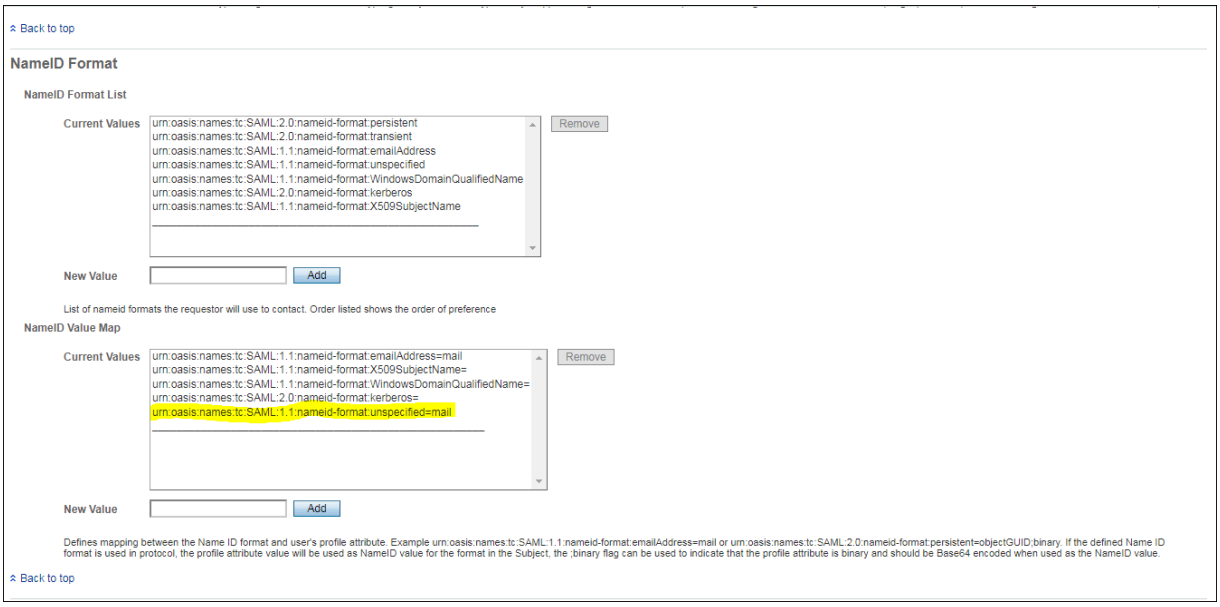
13. On the Federation TAB select the IDP config under the Entity Providers.



14. Under the Authentication Context check the Password-based context.



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



16. Now access AppViewX with the SSO authentication with Forgerock.
17. 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

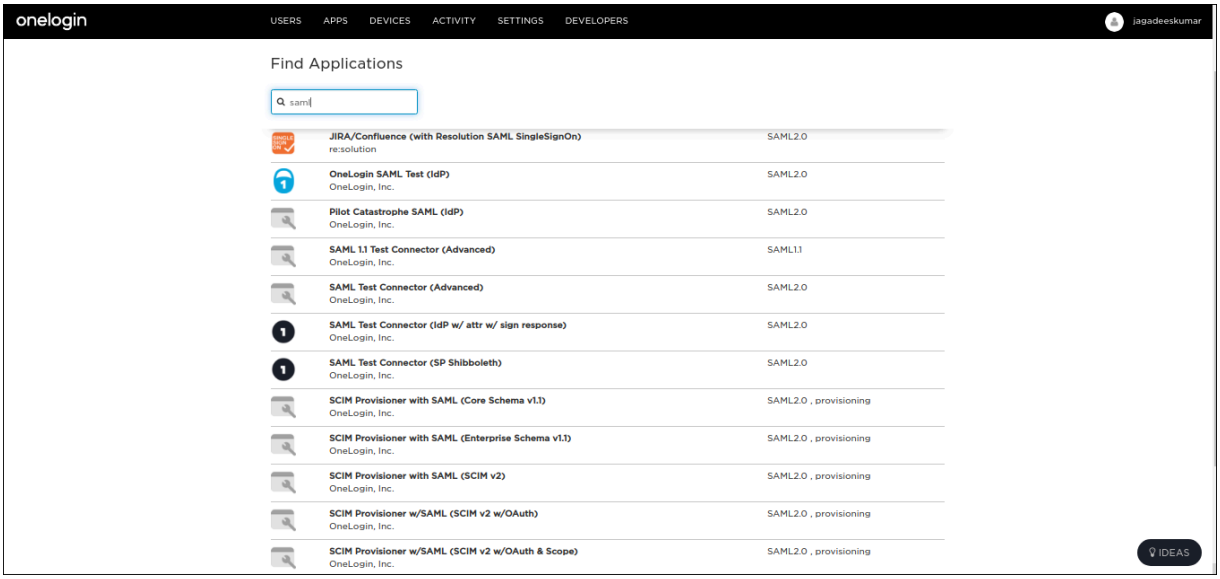
> **Note:** Role name passed in as a part of the SAML assertion should be configured in appviewx on the Accounts > UserGroup and assign a role for accessing the application. For an IDP initiated SSO the following structure like URL should be used. **Sample IDP initiated URL:** http://openam.try.appviewx.com:8080/openam/idpssoinit?metaAlias=/idp&spEntityID=https: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

OneLogin Integration

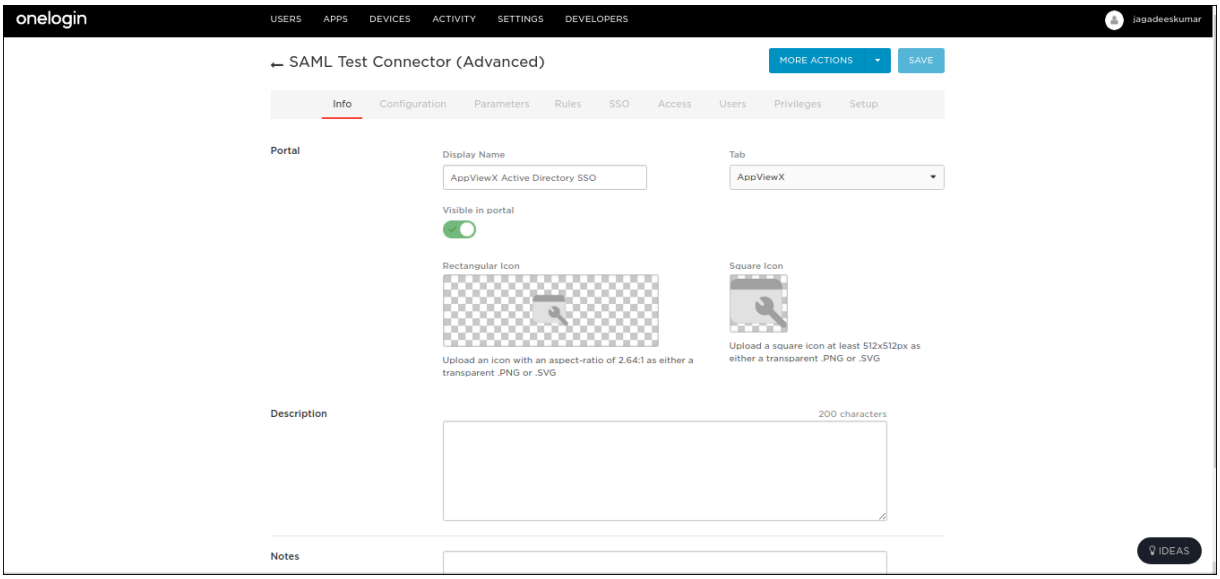
The below steps are performed at the IdP end. The navigation and screenshots might differ based on the version of the IdP. (This is just an example configuration)

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

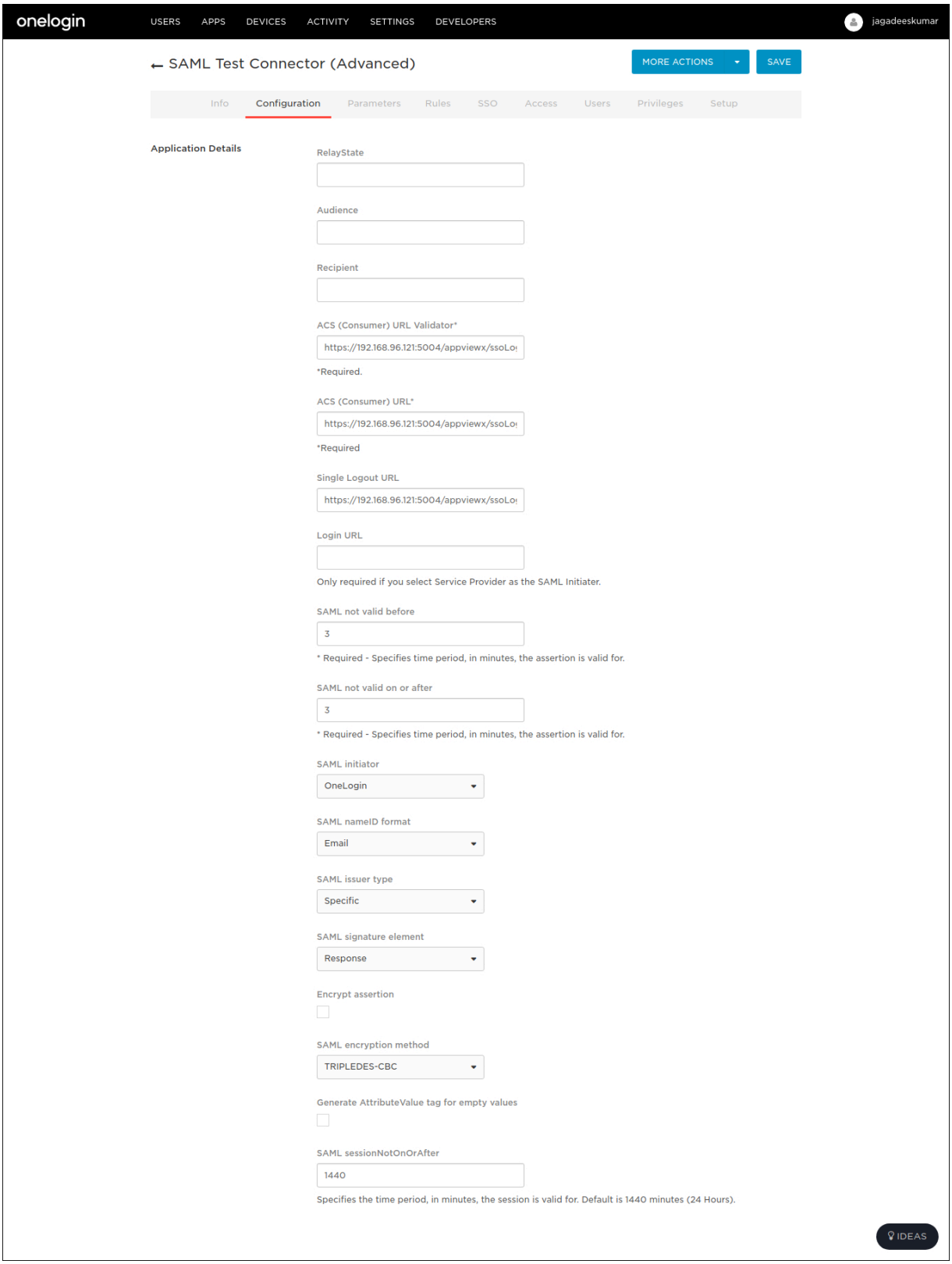
1. Create a new application. Click Add application and search for SAML Test Connector.



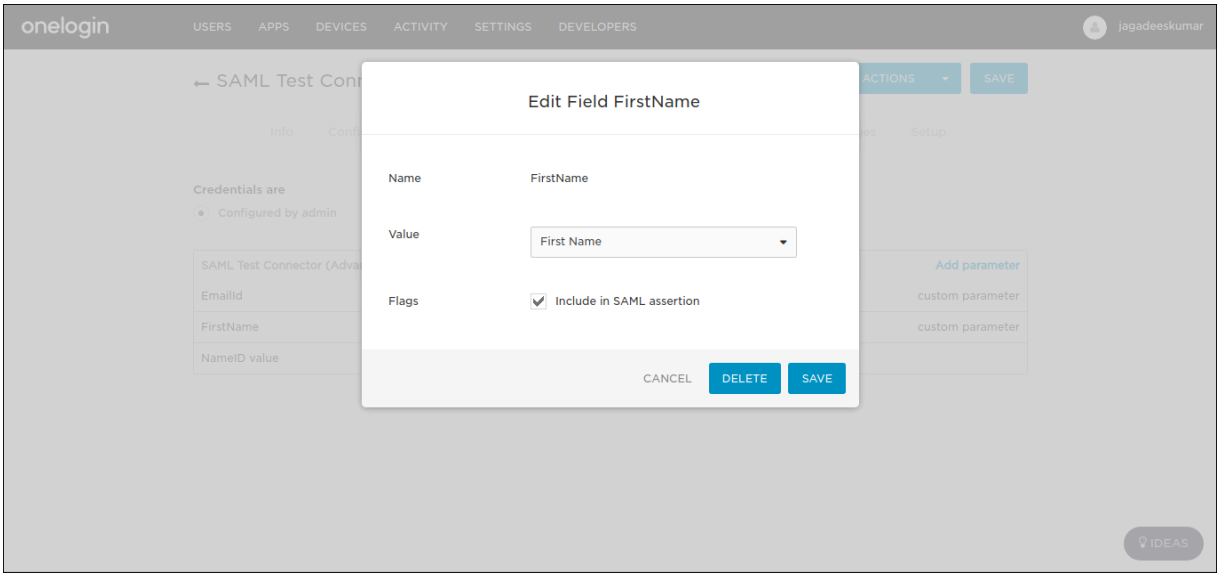
2. Provide the application name and application details of AppViewX on the information page.



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.

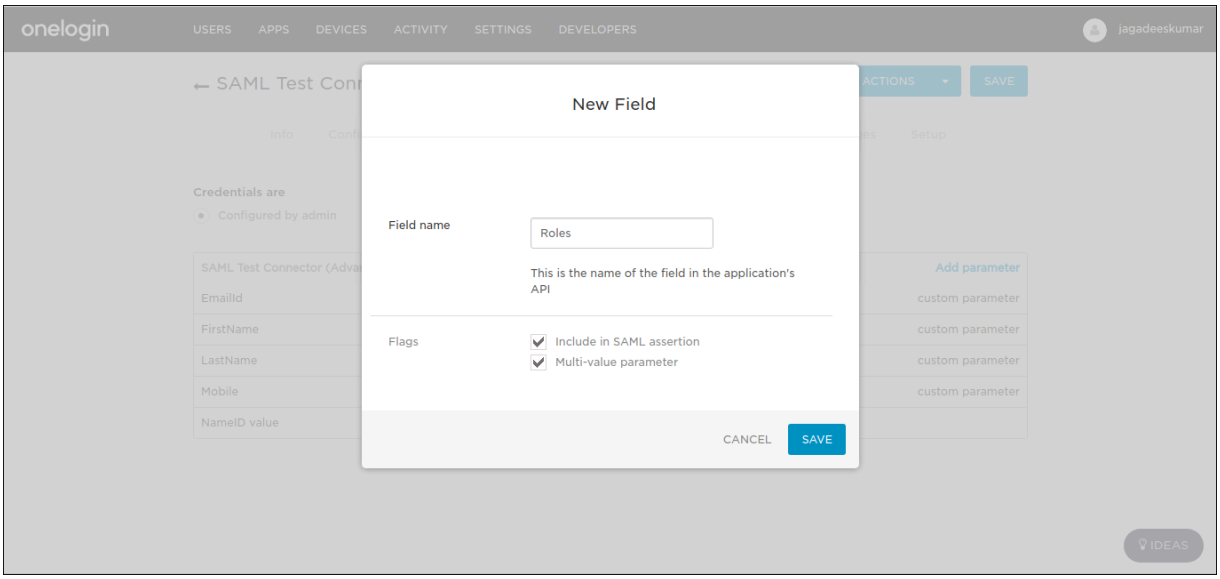


4. **Parameters to be sent to AppViewX:**The following parameters are samples that have been sent to AppViewX. Create a parameter called FirstName which sends the user's first name to AppViewX in the SAML Assertion.

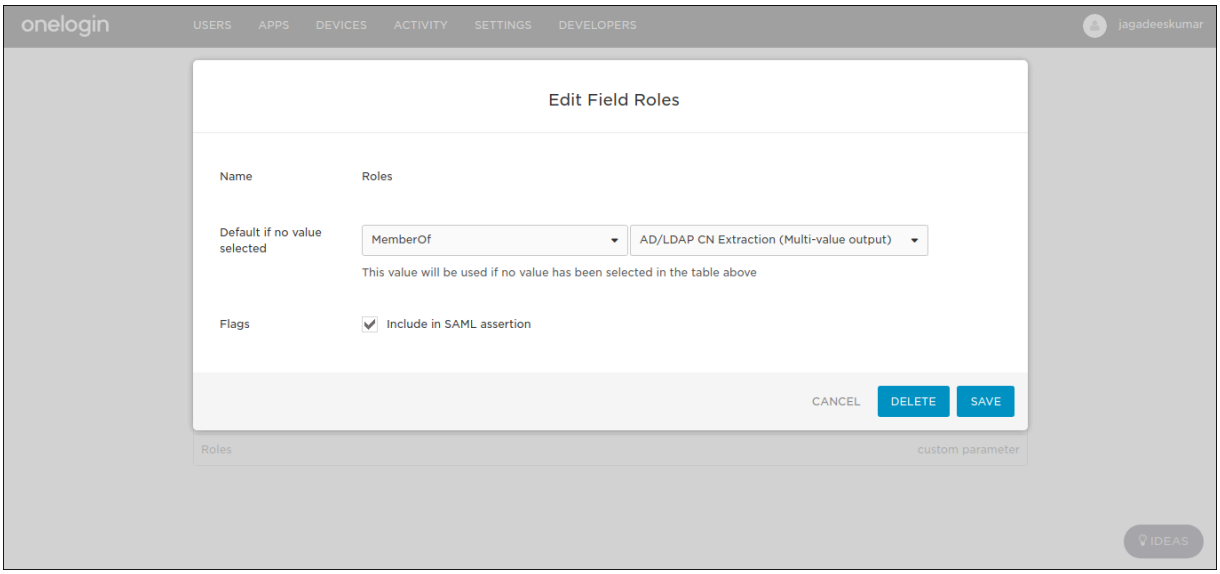


Include the flag in SAML Assertion for all the added parameters.

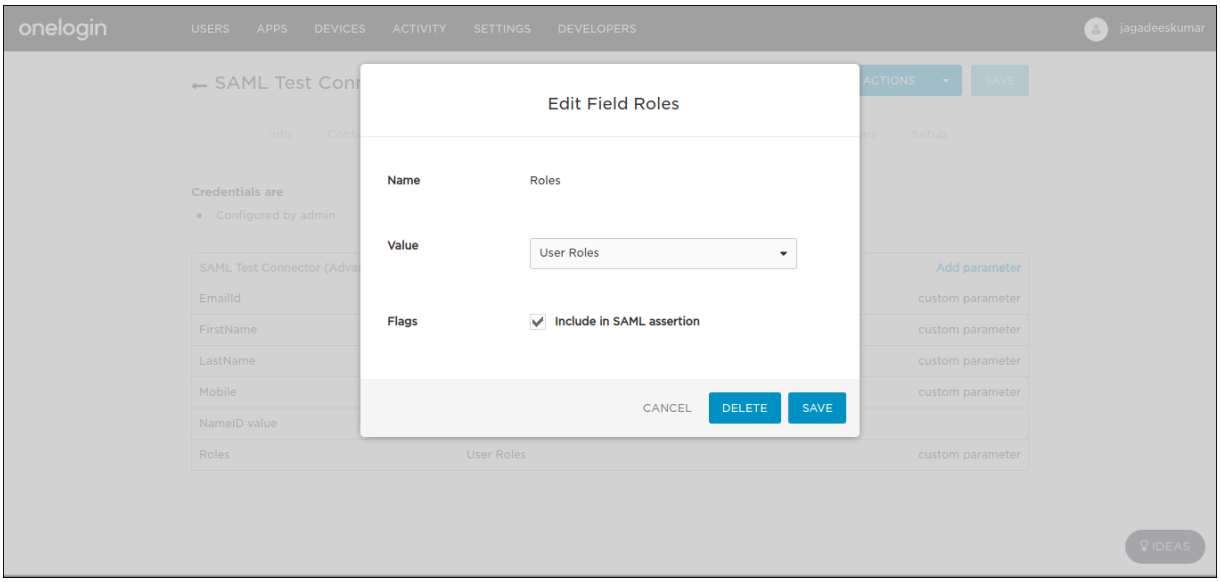
5. **Sending User Groups to AppViewX:** To send User Groups to AppViewX from OneLogin through SAML Assertion, the following configuration has to be performed. OneLogin should be integrated with the Active Directory. Provide the field name as Roles and enable the Flags SAML assertion and multi-value parameter.



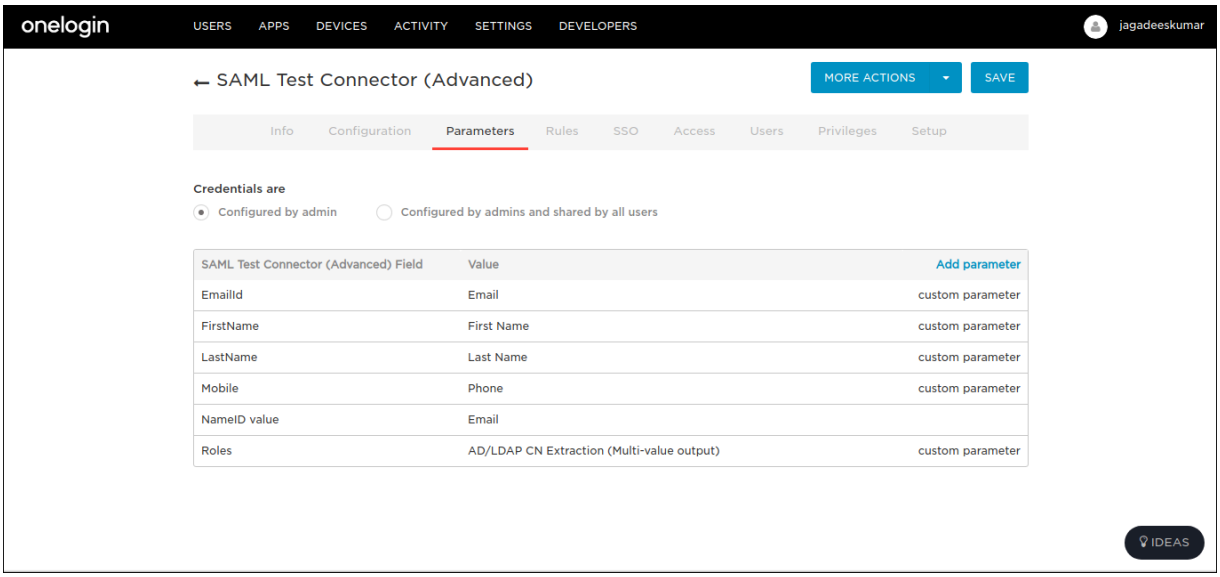
6. To pass the respective user's MemberOf attribute as Role, provide the field name as MemberOf and select the AD/LDAP CN Extractor.



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



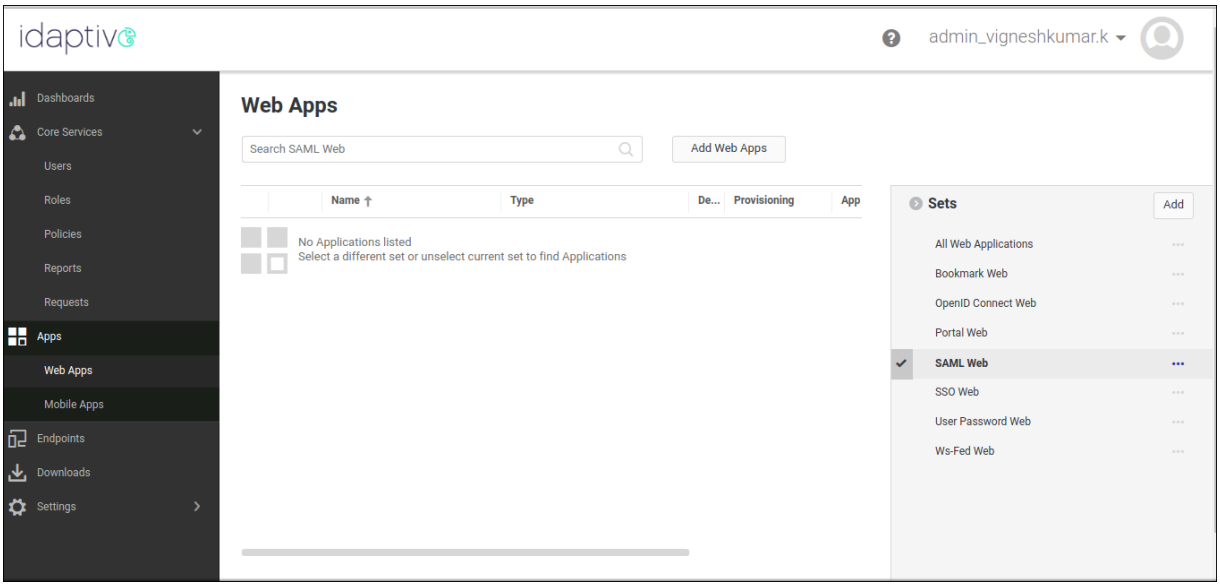
7. **Other parameters that have to be passed:** The following parameters have to be passed to AppViewX through the SAML assertion.



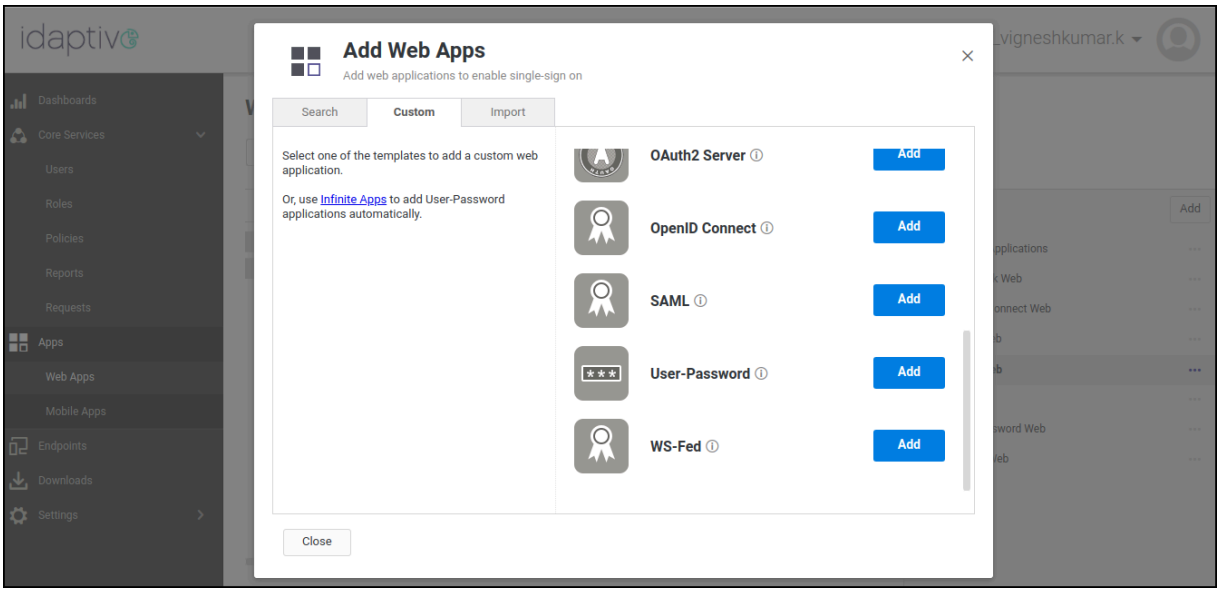
8. **Assign application to User and Role:** Once the federation metadata is downloaded, click Save. Create the UserGroup under Roles in the Administration section. The created application is then assigned to the user group and the synced users will be added to it.

Idaptive Integration

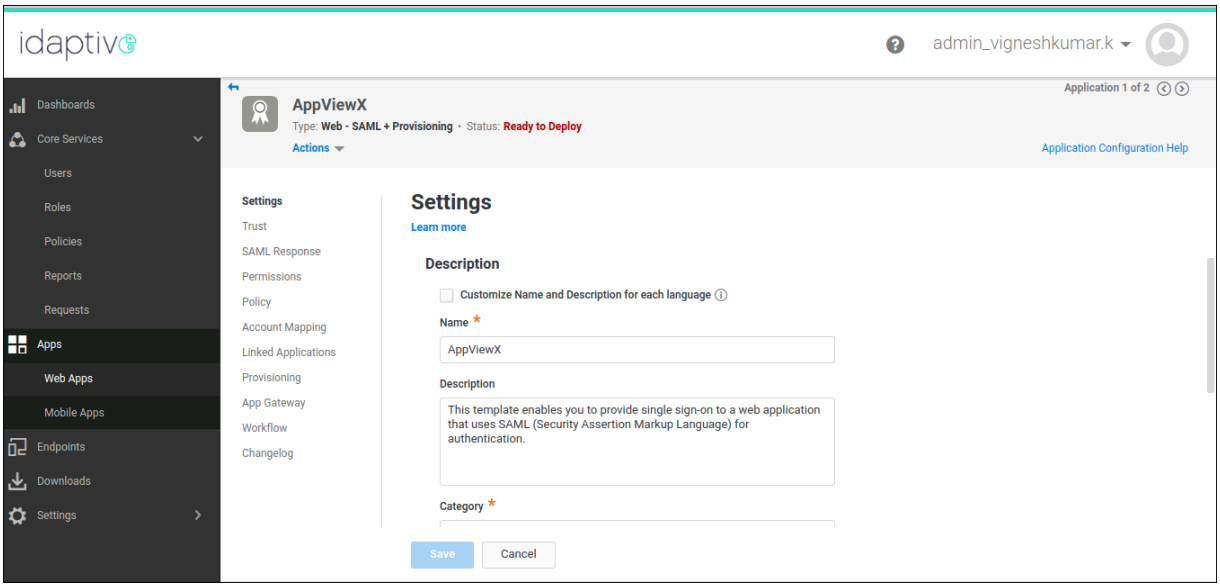
1. Login to the Idaptive SSO platform.
2. Navigate to Apps > WebApps > Select SAML Web > Click Add Web Apps.



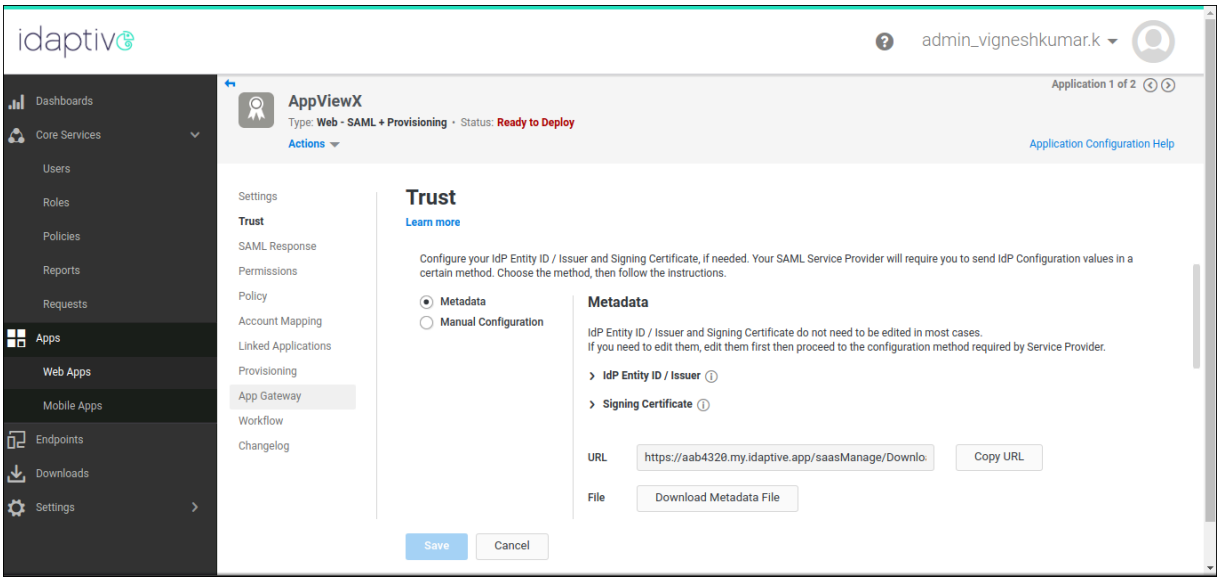
3. In Add Web Apps > Custom > SAML > Add.



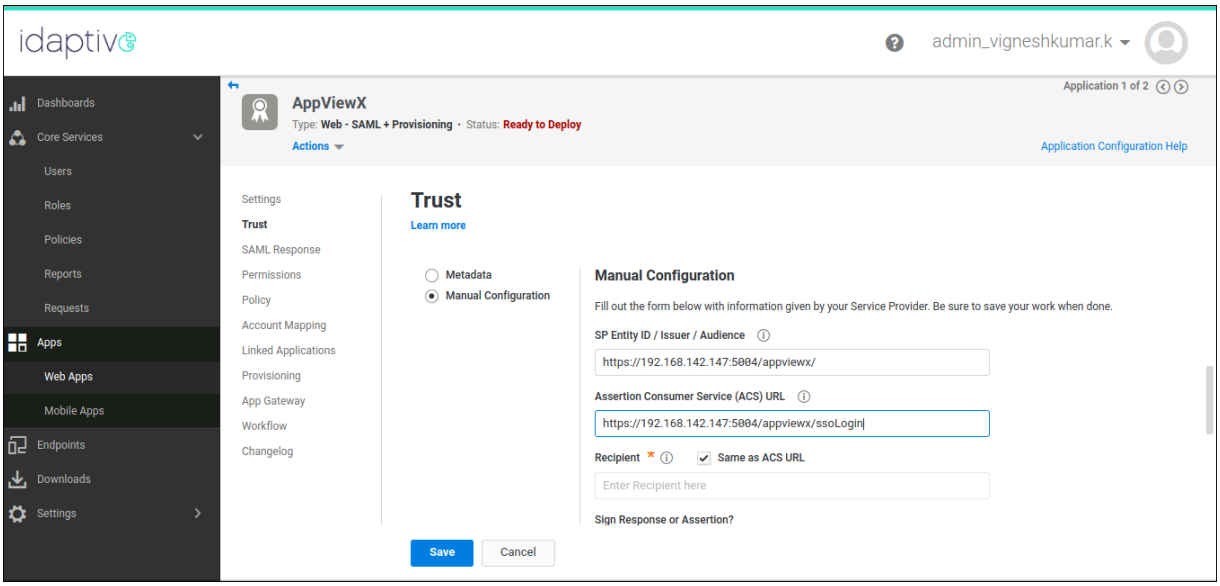
4. This will add the SAML app to the Web Apps Inventory.
5. Select the SAML app in the Web Apps Inventory and proceed with the configuration.
6. In the Settings tab, provide the name to the app as AppViewX and save the configuration.



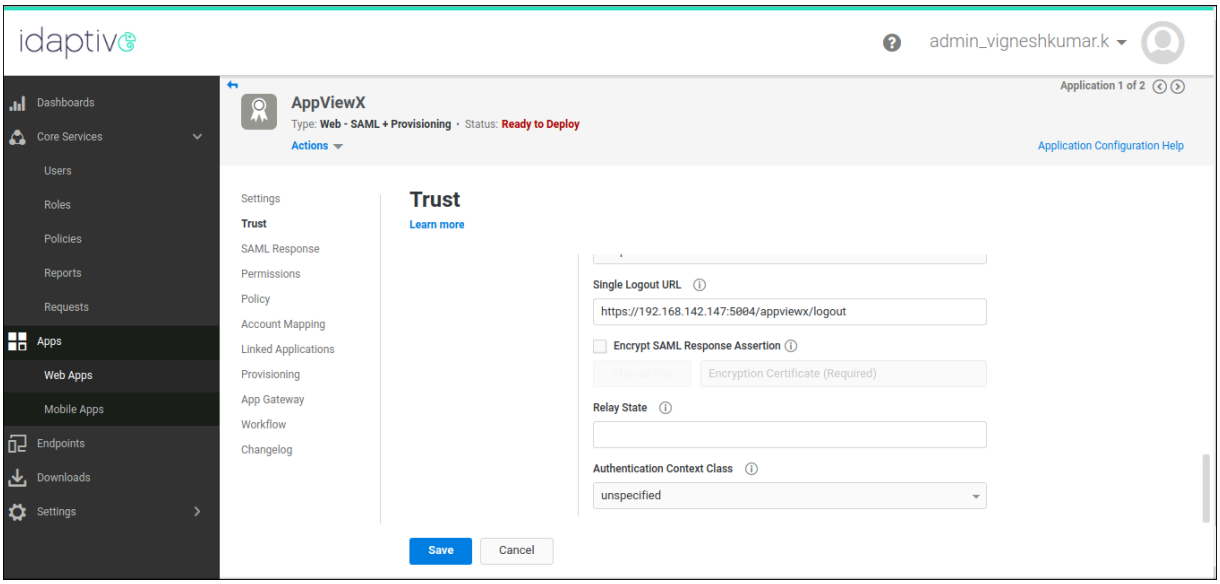
7. In the Trust tab, under Identity Provider Configuration click Download Metadata File.



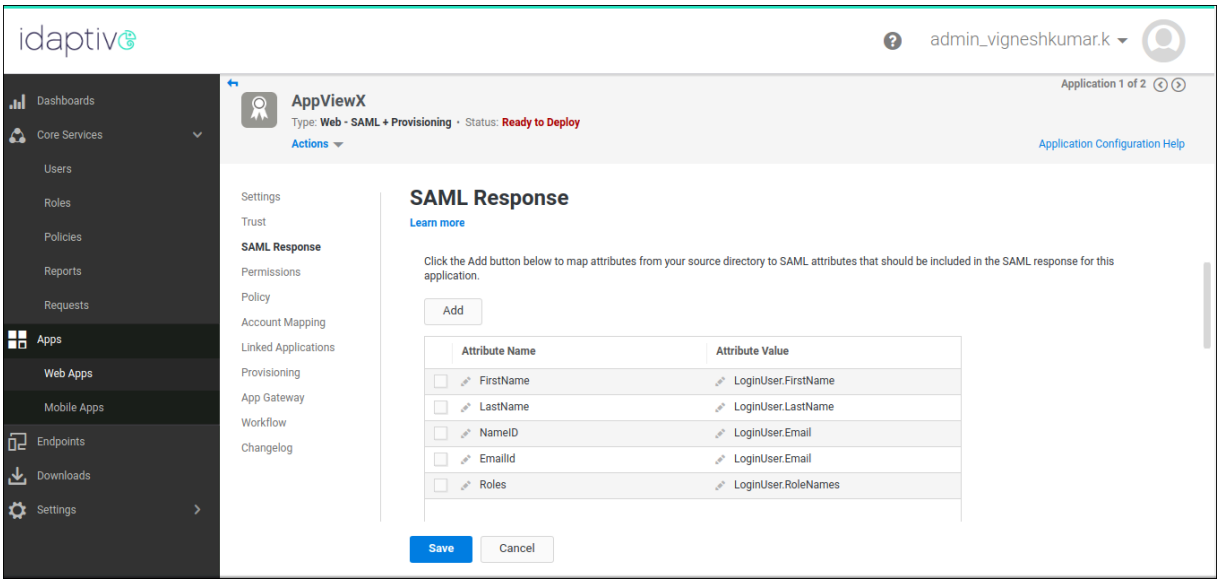
8. Continue in the Trust tab, under Service Provider Configuration, select the radio button Manual Configuration. Copy and paste the Entity ID URL from AppViewX on the SP Entity ID field in Idaptive portal and the Service URL from AppViewX on the ACS URL field in the Idaptive portal.



9. 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.



10. 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). Then save the configuration.



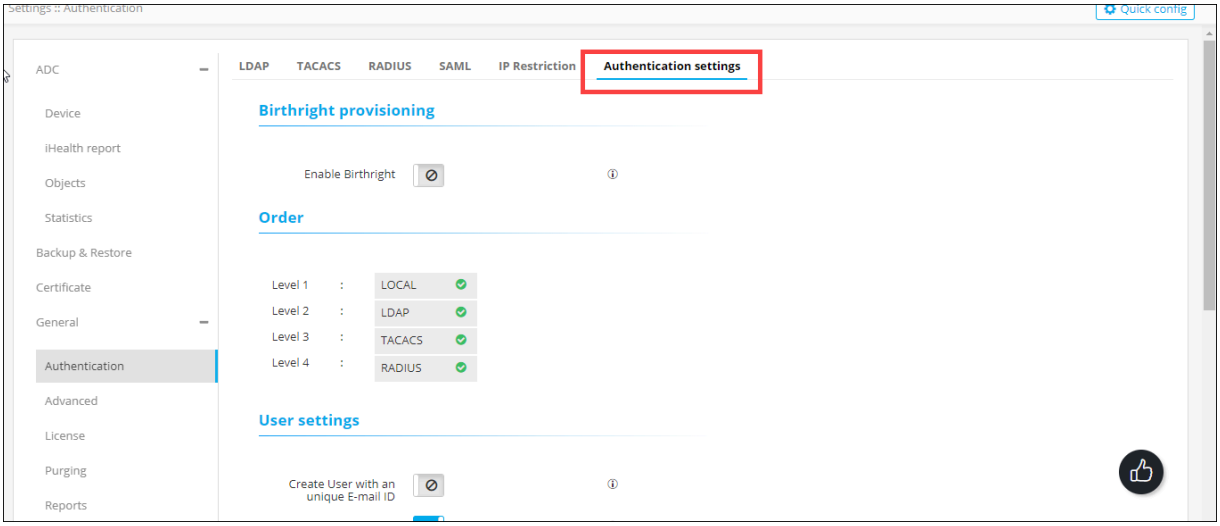
11. Assign the application to the respective Role and the Role to the respective Users. Once done configure the same Role in AppViewX in the Account > User Group module and assign respective AppViewX Role permission to the User Group.
12. Now access AppViewX with the help of External login using SAML.

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. Navigate to the Settings :: Authentication page.
2. On the Settings page, click the Authentication settings tab.



3. To enable birthright provisioning for new users who log into the system with a predefined set of permissions (associated with the user group), enable the Enable Birthright toggle key.
   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.
4. 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.

5. In the User settings section, enter the following details:

Field	Description
Create User an unique E-mail ID	To create a user even if authorization fails (but the user is authenticated successfully), enable this toggle key.
Create User on Authorization Failure	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.
Session Timeout	

***Mandatory**

6. For A10 support, in the Node Password field, enter the password of the node where the AppViewX Cloud Connector instance is deployed. A10 devices are protected using the Secure Shell mechanism and, in order to upload and/or download certificates from thesedevices, login is mandatory.

> **Note:** If you have multiple AppViewX Cloud Connector instances deployed, all of them should have the same password.

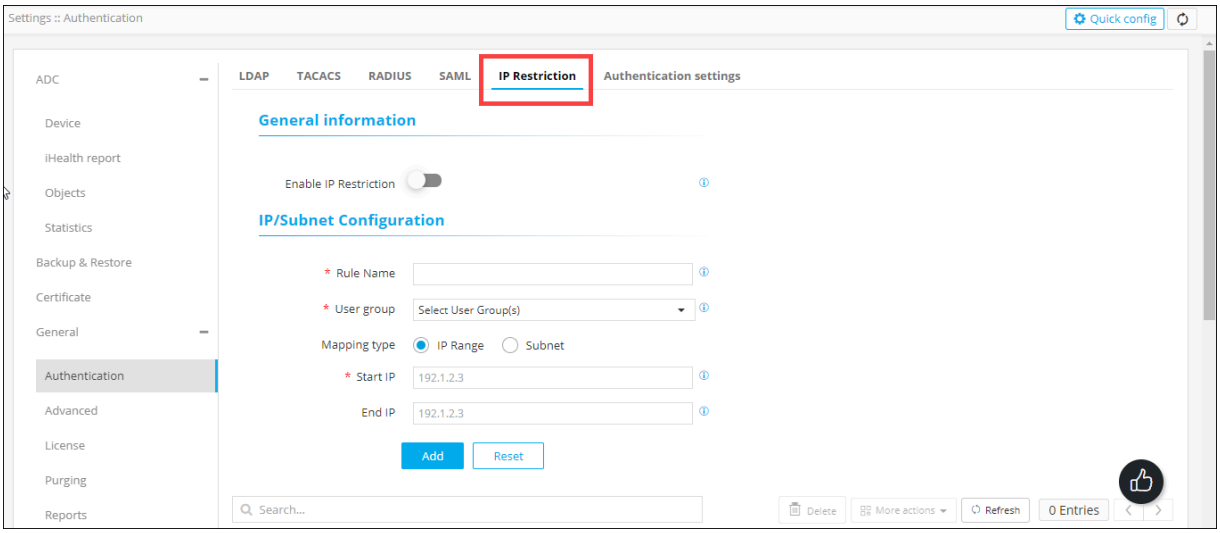
7. To save the authentication settings, click Save.

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

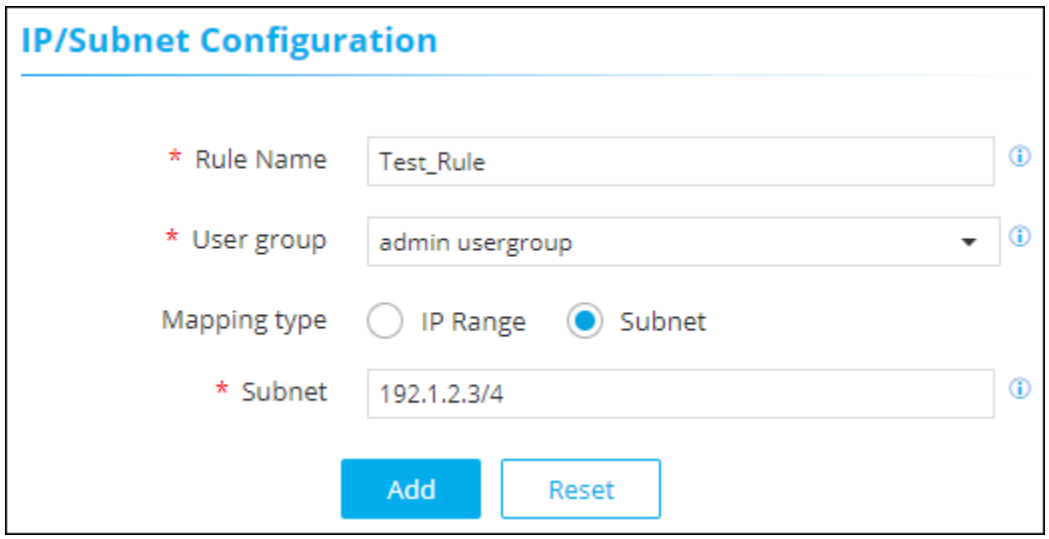


3. In the General Information section, enable the Enable IP Restriction toggle key.
4. In the IP/Subnet Configuration section, enter the following details (sample values are shown in the image below the table):

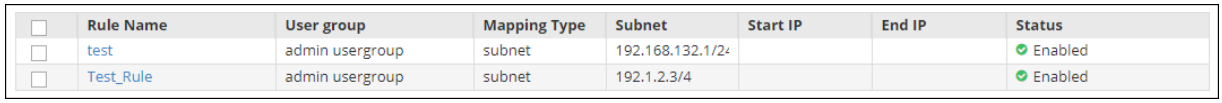
Field	Description
Rule Name*	Rule name for a whitelisting condition
User group*	From the drop-down menu, select the user group to which this rule will apply. Only the users from the selected user group will be allowed to login to AppViewX from the whitelisted IP address/subnet range.
Mapping Type	Select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

Field	Description
End IP	For the whitelisted IP/subnet range, enter the ending IP address of the range. **Note:** The IP/subnet range should be specified in the ascending order.
Subnet*	**Note:** Note: This field is displayed when the Subnet mapping type is selected. Subnet network range to whitelist

***Mandatory**



5. 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 this 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

Chapter 3: Configuring Role and Resource Based Access Control

- Managing Users
- Managing Service Accounts
- Managing User Groups
- Managing Roles
- RBAC Quick Configuration

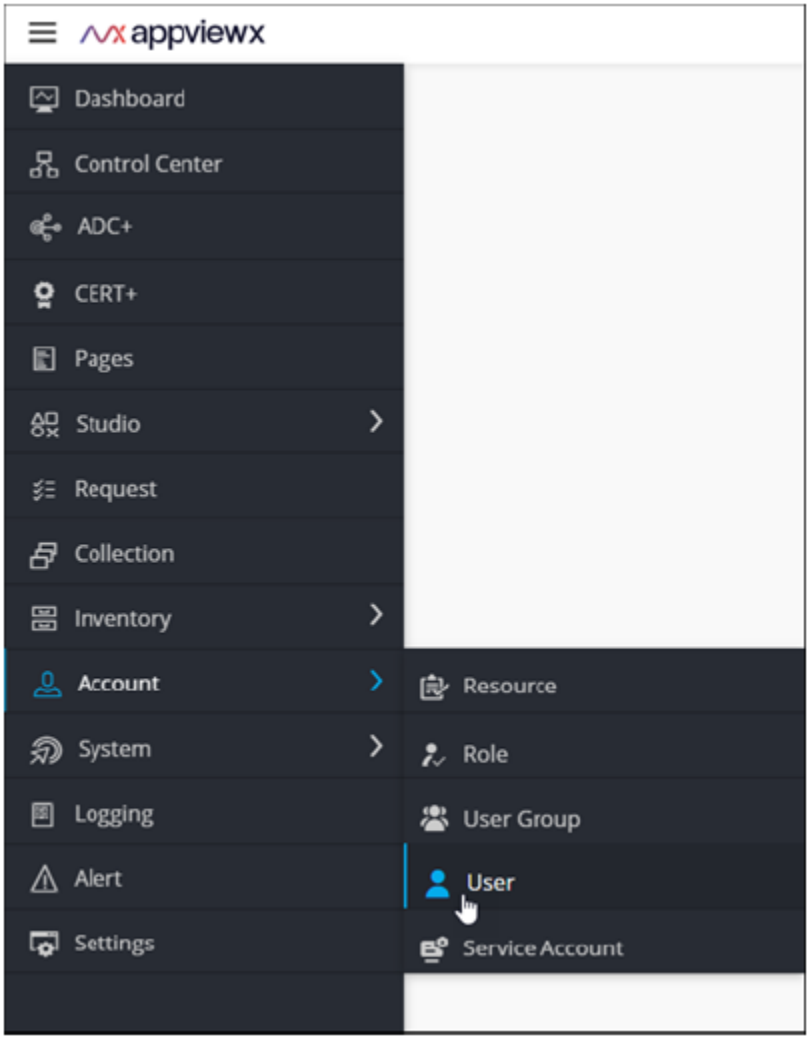
Managing Users

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

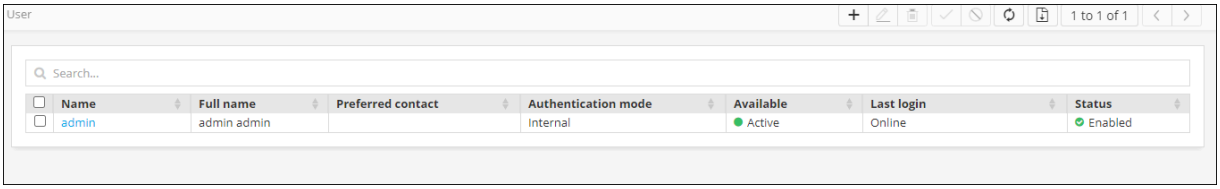
Creating a User

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.

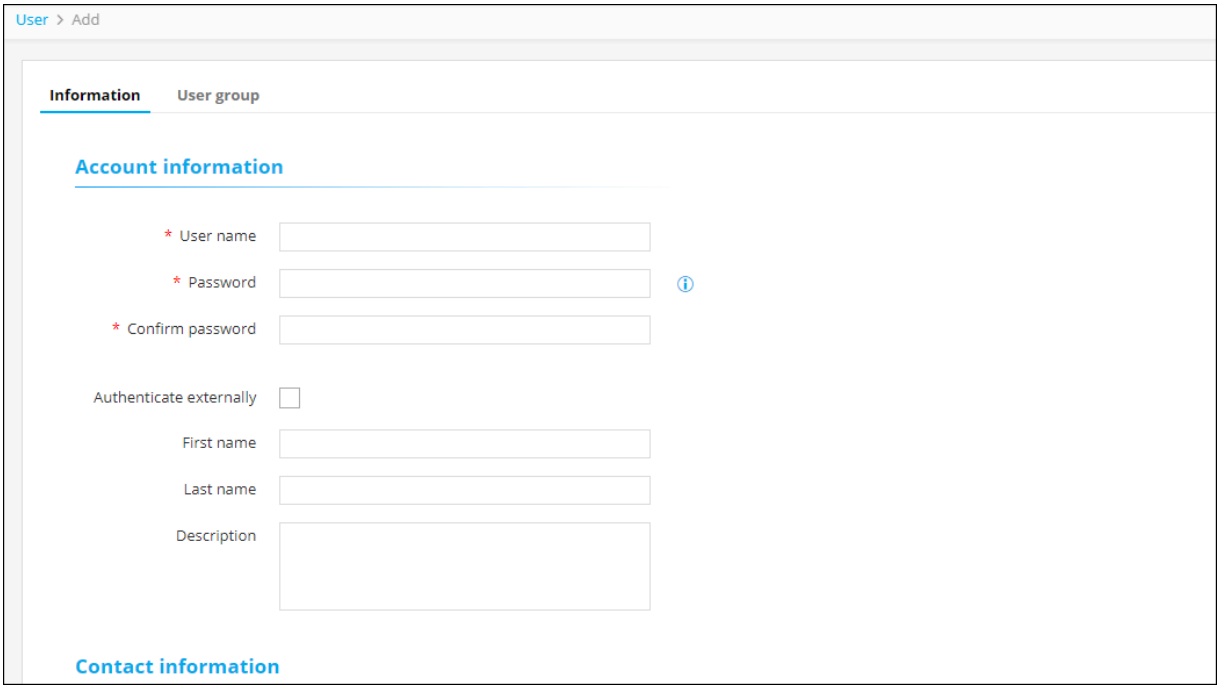


3. The User page is displayed.



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

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



6. In the Account Information section, enter the following details:

Field	Description
User name*	User name for the new user
Password*	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 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

Field	Description
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 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

***: Mandatory**

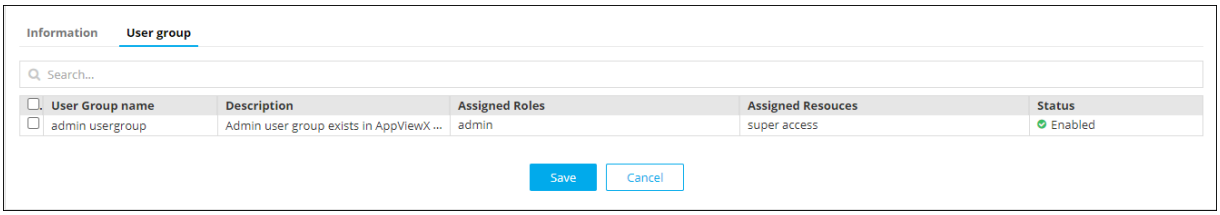
7. In the Contact Information section, enter the following details:

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.

***:Mandatory**

8. Click Save.

9. 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.

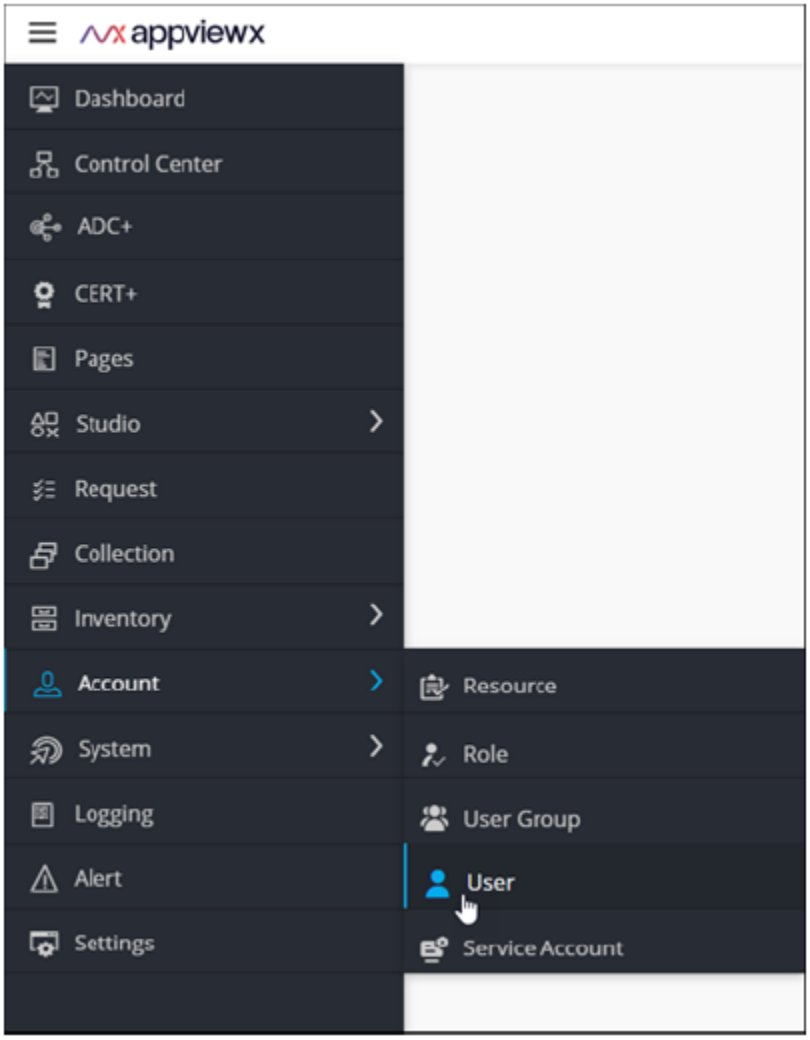


10. To add the user to a group, select the check box for that user group.
11. Click Save.

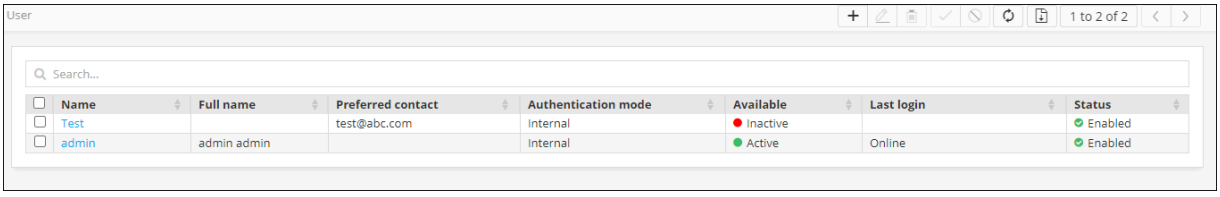
Modifying a User

To modify a user:

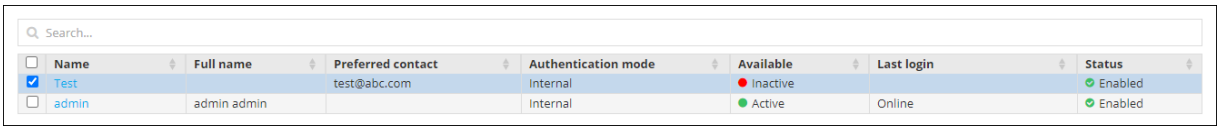
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Account > User.



3. The User page is displayed.

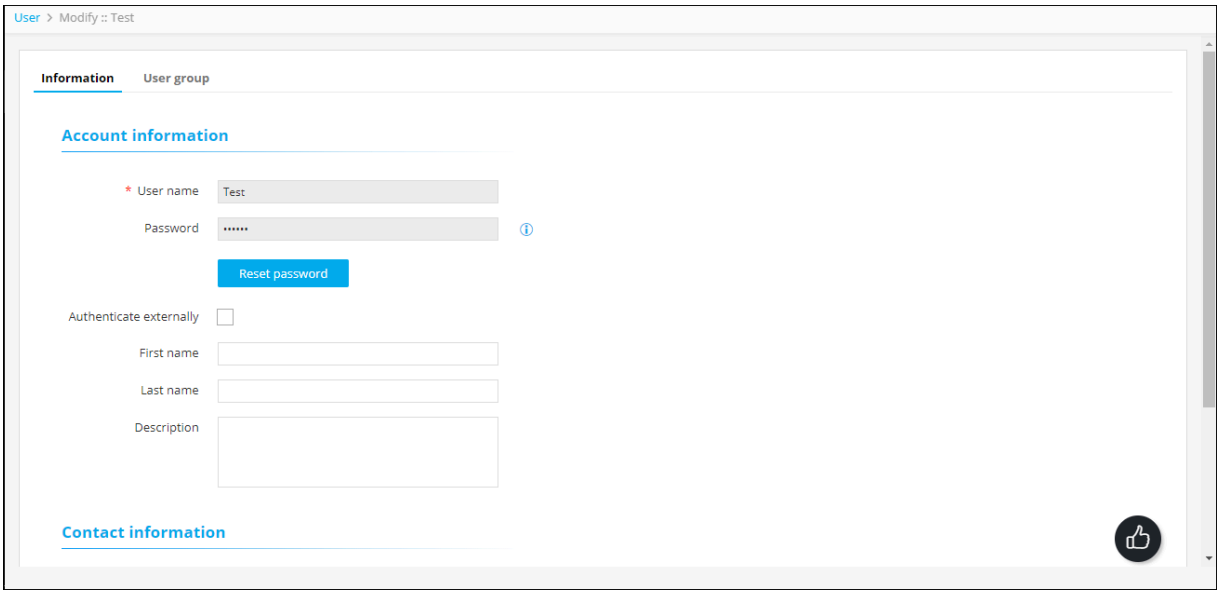


4. From the User page, select the check box against the user you want to modify.



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

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



7. In the Account Information section, update the required details:

Field	Description
User name*	User name for the new user
Password*	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 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

Field	Description
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 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

***: Mandatory**

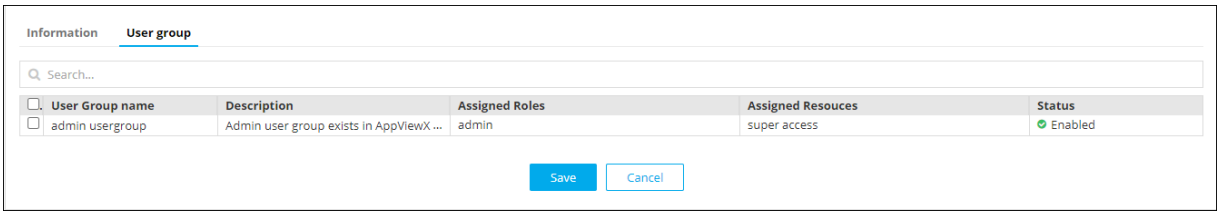
8. In the Contact information section, update the required details:

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 **Note:** This field is mandatory only if the preferred mode of contact is Phone number.

***:Mandatory**

9. Click Save.

10. To modify the user and user group mapping, by adding a new user group/deleting an existing user group, click the User group tab.

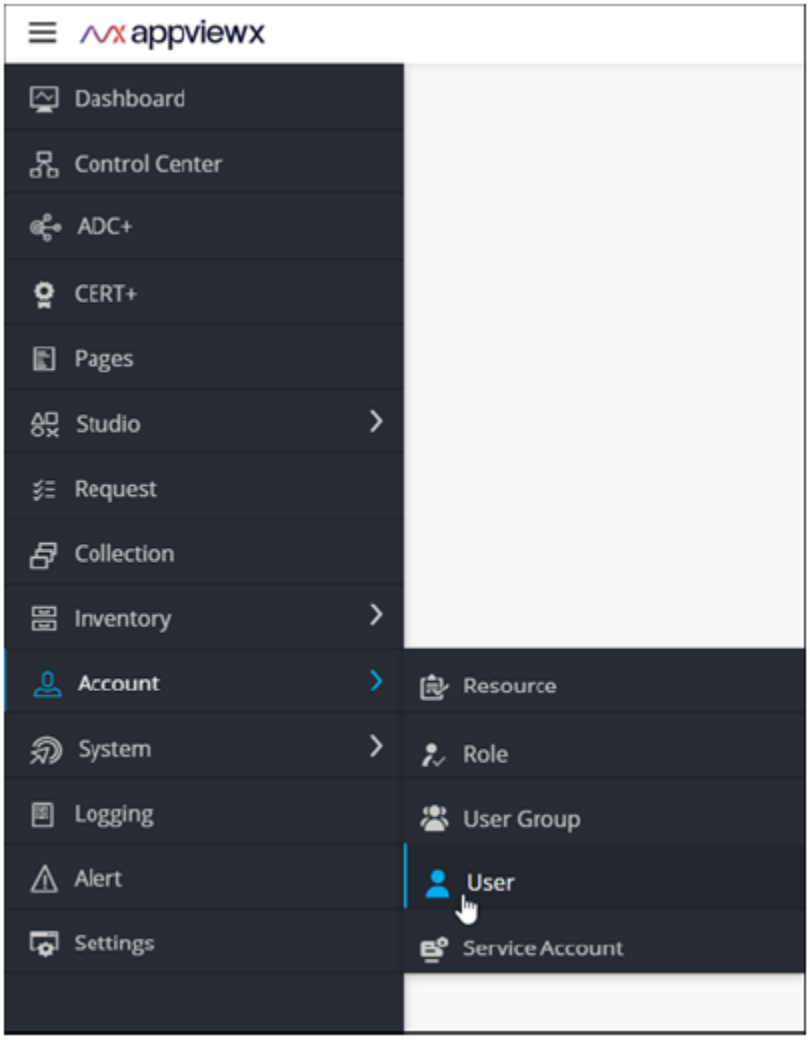


11. To add the user to a group, select the check box for that user group.
12. Click Save.

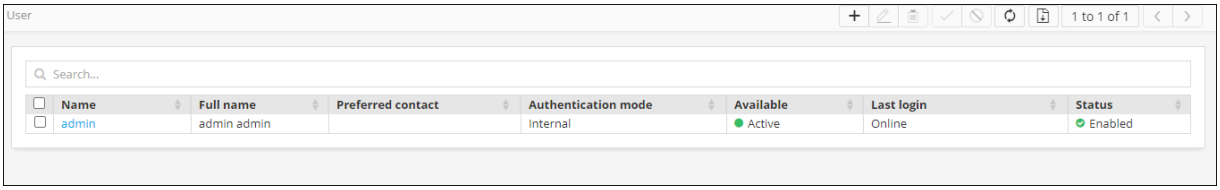
Importing a Users

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.

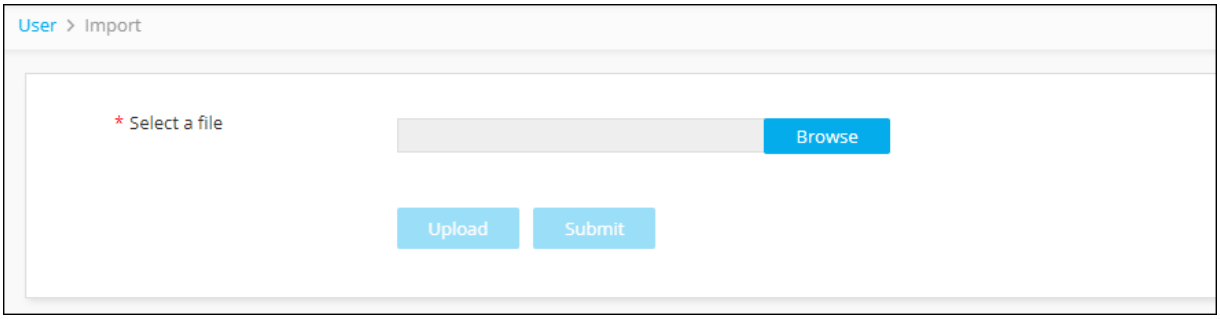


3. The User page is displayed.



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

5. The Import screen is displayed.



6. 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) button in the Command bar of the Import screen, modify the contents, save it, and then import it into the system. This reduces the chance that error messages appear during the import process.

7. Click Upload to see the user details displayed in the user interface.

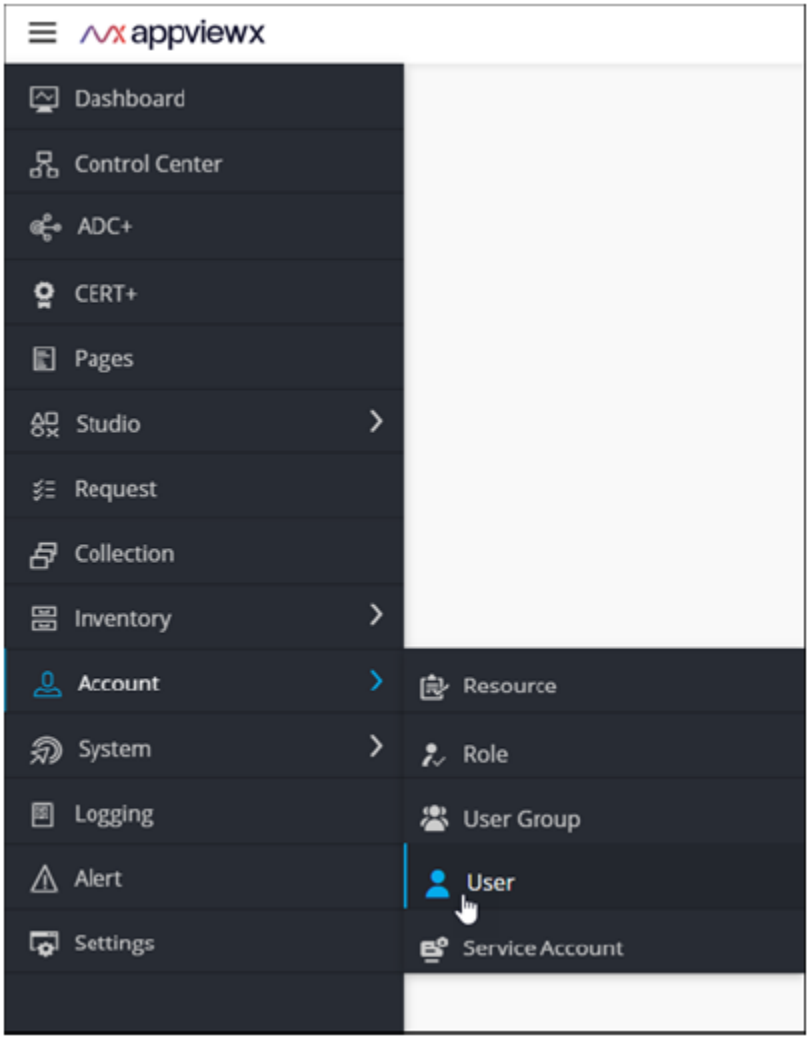
Note: The user details displayed at this point are only for review; the user details have not been imported yet.

8. 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.
9. Click Submit.

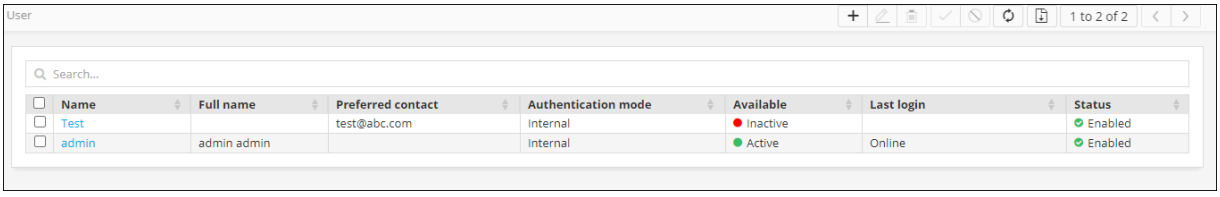
Enabling a User

To enable a user:

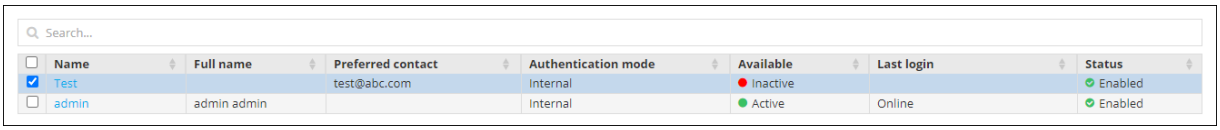
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Account > User.



3. The User page is displayed.



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



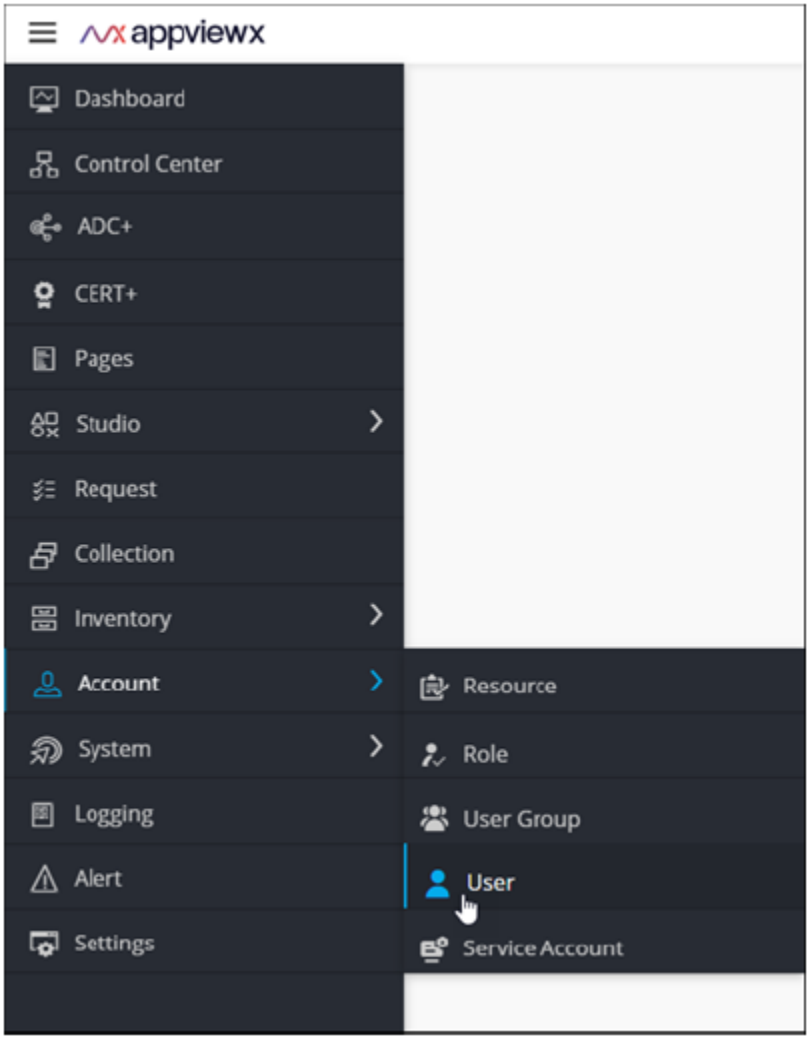
5. From the top right corner of the screen, click 

6. In the Confirmation dialog box, click Yes.

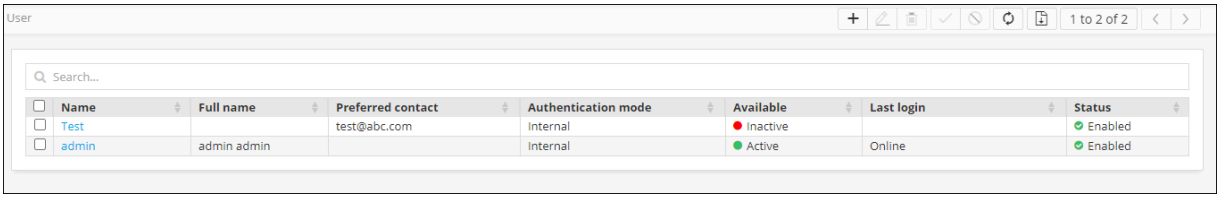
Disabling a User

To disable a user:

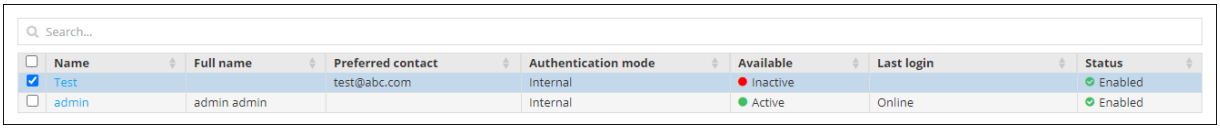
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Account > User.



3. The User page is displayed.



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



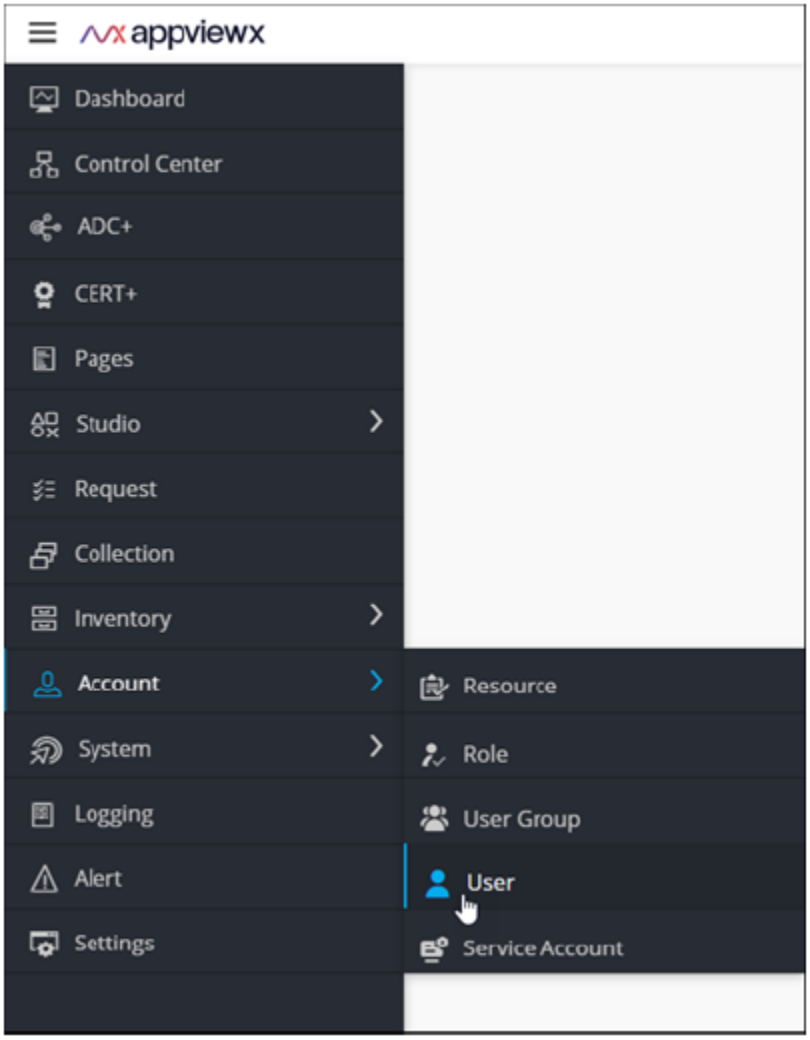
5. From the top right corner of the screen, click 

6. In the Confirmation dialog box, click Yes.

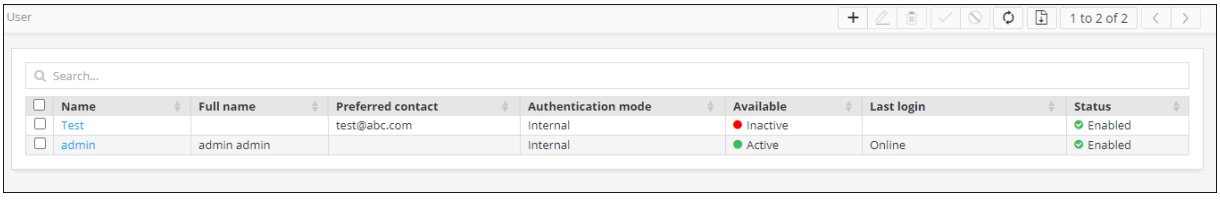
Deleting a User

To delete a user:

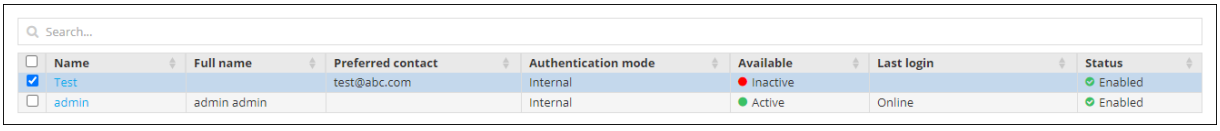
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Account > User.

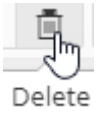


3. The User page is displayed.



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



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

6. In the Confirmation dialog box, click Yes.

Managing Service Accounts

• Client Credentials Grant Type
• Configuring Managing Service Account
• Configuring oAuth Settings
• oAuth
• oAuth Workflow

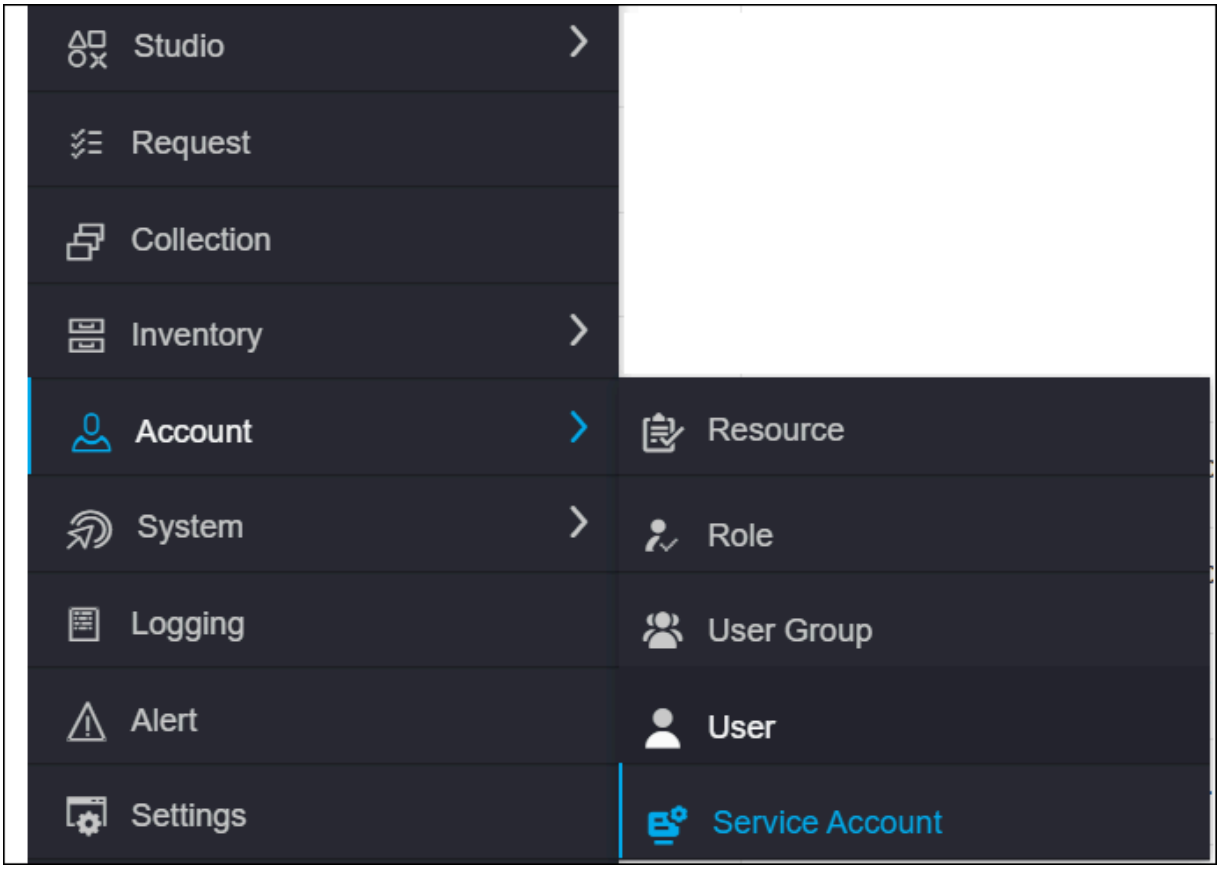
Client Credentials Grant Type

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

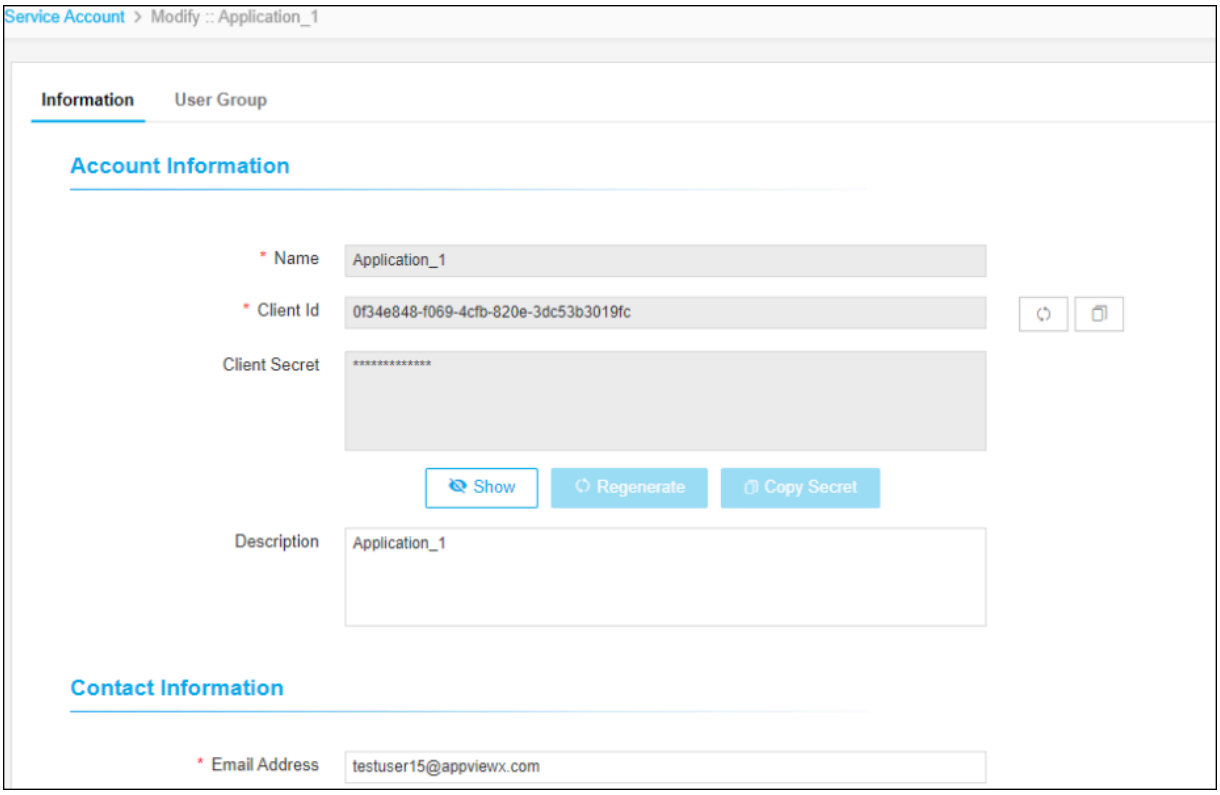
Configuring Managing Service Account

To configure managing service accounts, follow the below steps:

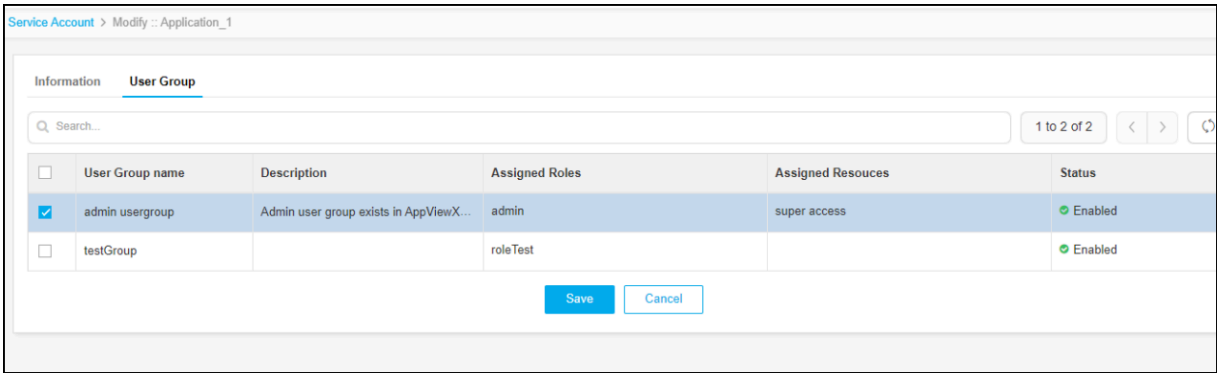
1. To create a service account in AppViewX, navigate to Menu > Accounts > Service Account



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



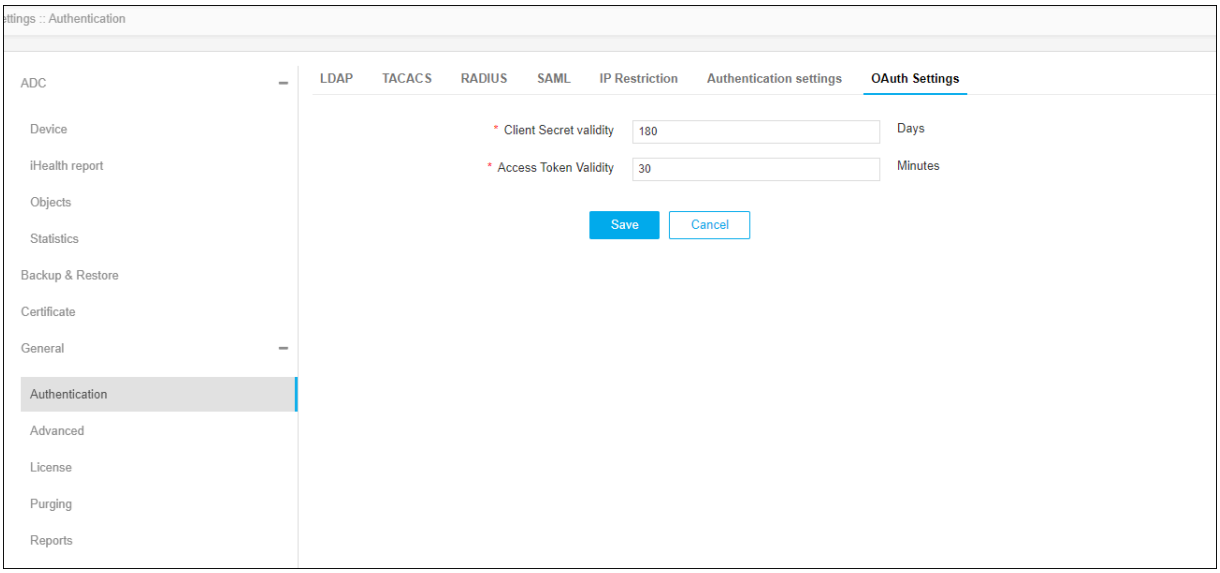
3. The access privileges and scope for this service account can be defined by assigning the required User Groups to this account.



Configuring oAuth Settings

To configure oAuth settings, follow the below steps:

1. To define the validity of Access Token and Client Secret from AppViewx, navigate to Settings > General > Authentication > oAuth settings.



2. By default, Client Secret expires in 180 days and the Access token expires in 30 Minutes. It is customizable.
3. Whenever an Access Token expires, an HTTP Error Code 401 is displayed in the API response. The client application can generate a new Access Token using the Client ID and Client Secret.
4. When the Client Secret expires, you can regenerate a new Client Secret from AppViewX in Account > Service Account > Account Name > Client Secret > Regenerate.

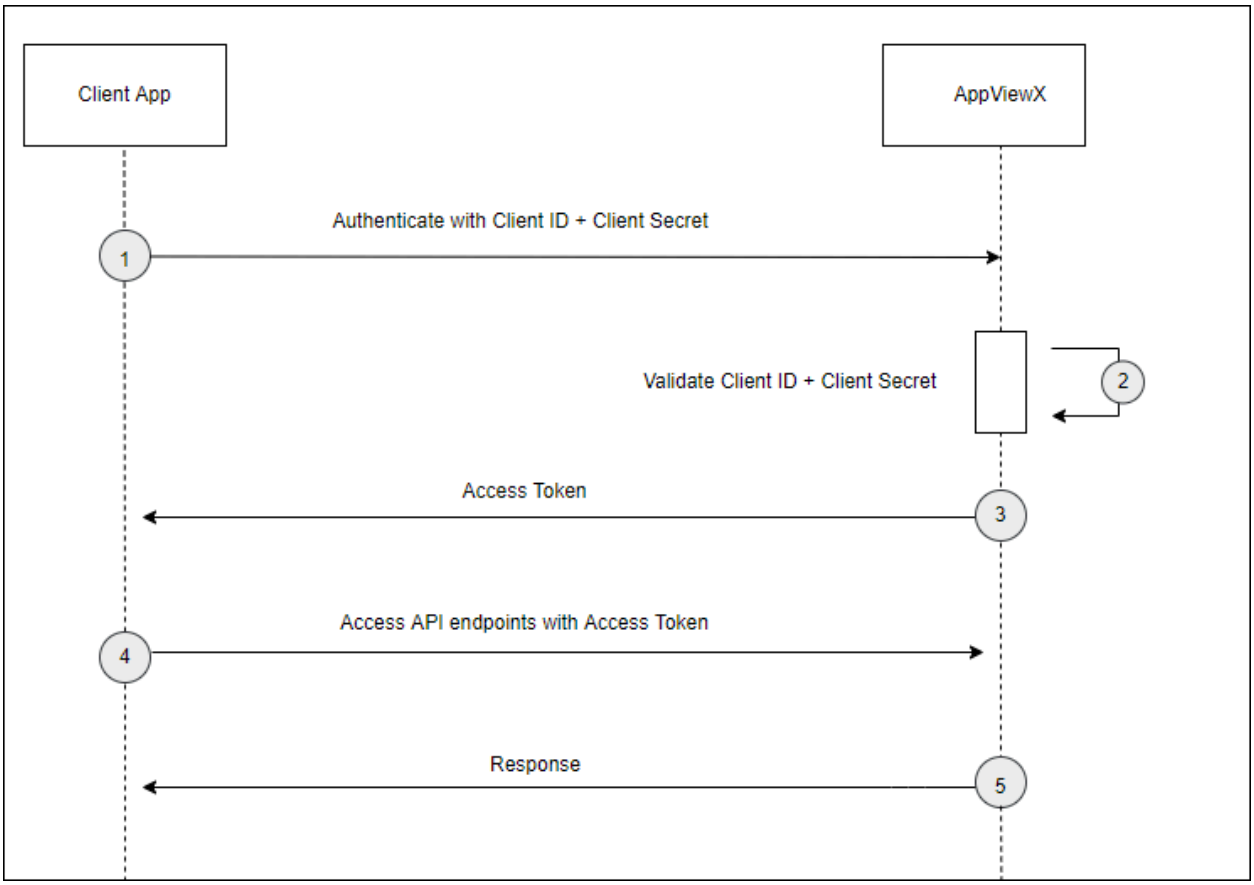
oAuth

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

AppViewX can be managed using web console and API endpoints.

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

oAuth Workflow



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

   API: acctmgmt-get-service-token

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

   Method: POST

   Header:

   Basic Authentication : (base64(clientId:clientsecret))

   Payload:

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

```
 }
}
```

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

Response:

```
{
"response":
 "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJBcHBsaWNhdGlvbl8xIiwiYXVkIjoiYXZ4IiwiY2xpZW50SWQiOiIwZjM0ZTg0OC1mMDY5LTRjZmItO
DIwZS0zZGM1M2IzMDE5ZmMiLCJpc3MiOiJhdngiLCJleHAiOjE2NDMxMDc3OTQsImdyYW50IHR5cGUiOiJjbGllbnRfY3JlZGVudGlhbHMifQ.EC6my35MCU
sMVC0gsylFqWVzqjgs5Js87Owf1esoano",
"message": null,
"appStatusCode": null,
"tags": null,
"headers": null
}
```

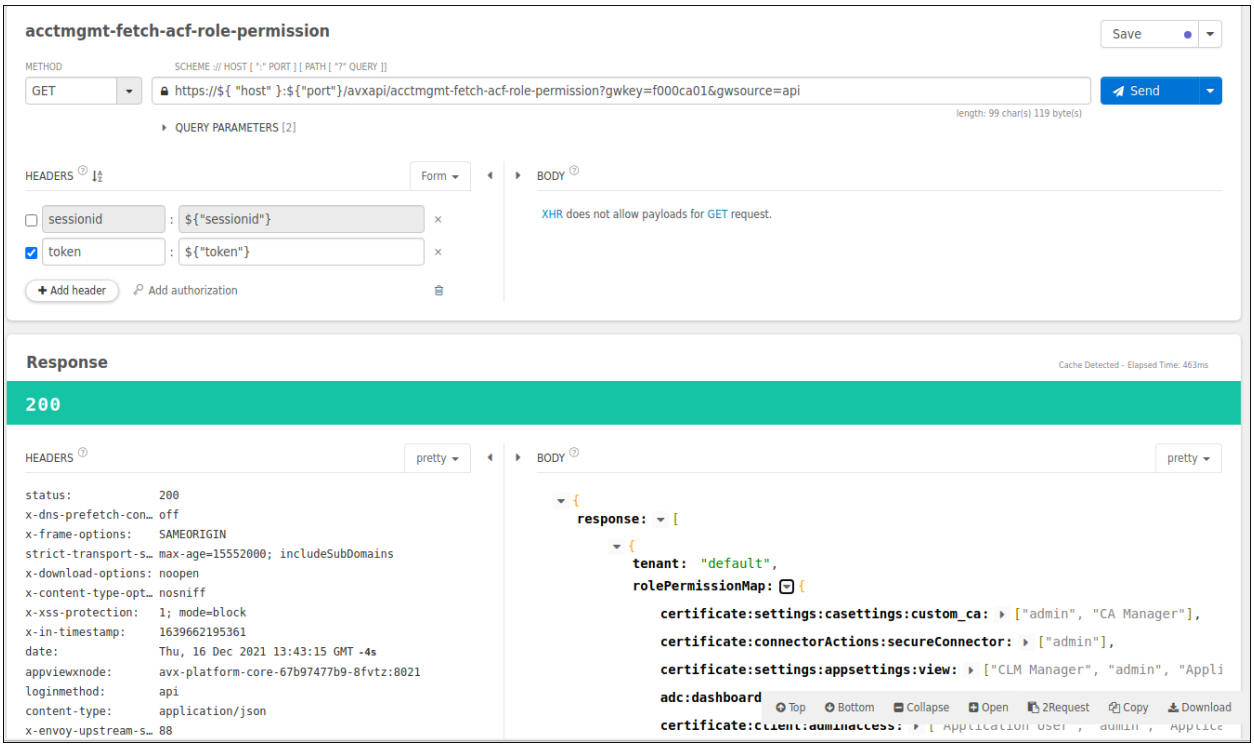
Access Token JWT Claims:

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

4. The Client application then accesses the API endpoints with the Access Token in the **“token”** header of the API. Then AppViewX provides the response.

Example

Refer to the below sample screenshot for reference.



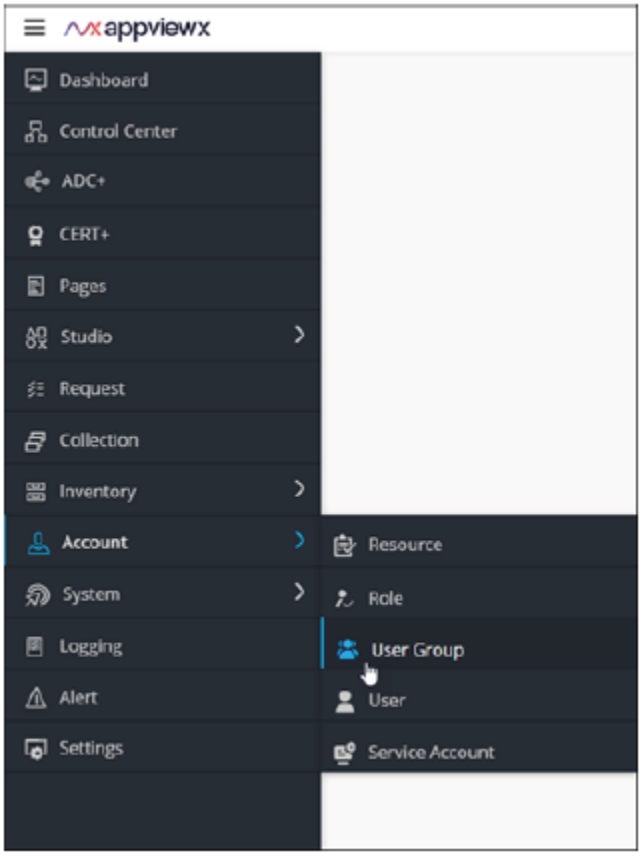
Managing User Groups

- Creating a User Group
- Cloning a User Group
- Modifying a User Group
- Deleting a User Group
- Disabling a User Group
- Enabling a User Group

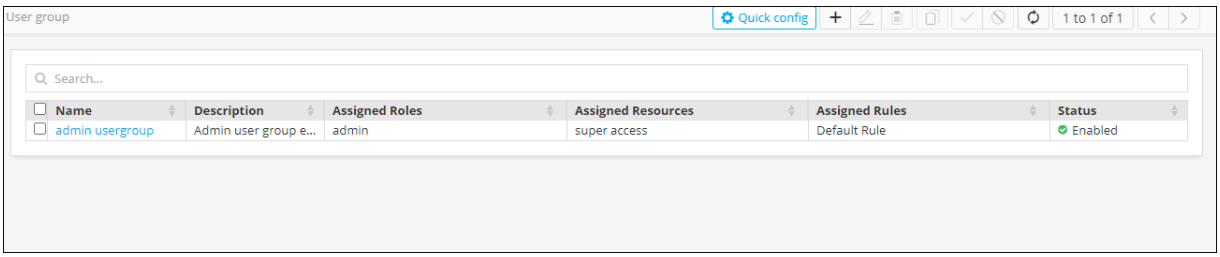
Creating a User Group

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, click Account > User Group.

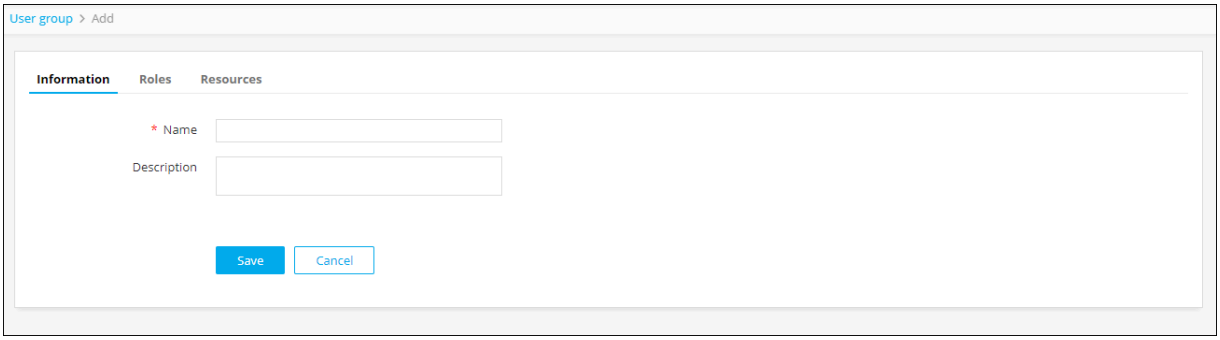


3. The User Group page is displayed.



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

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

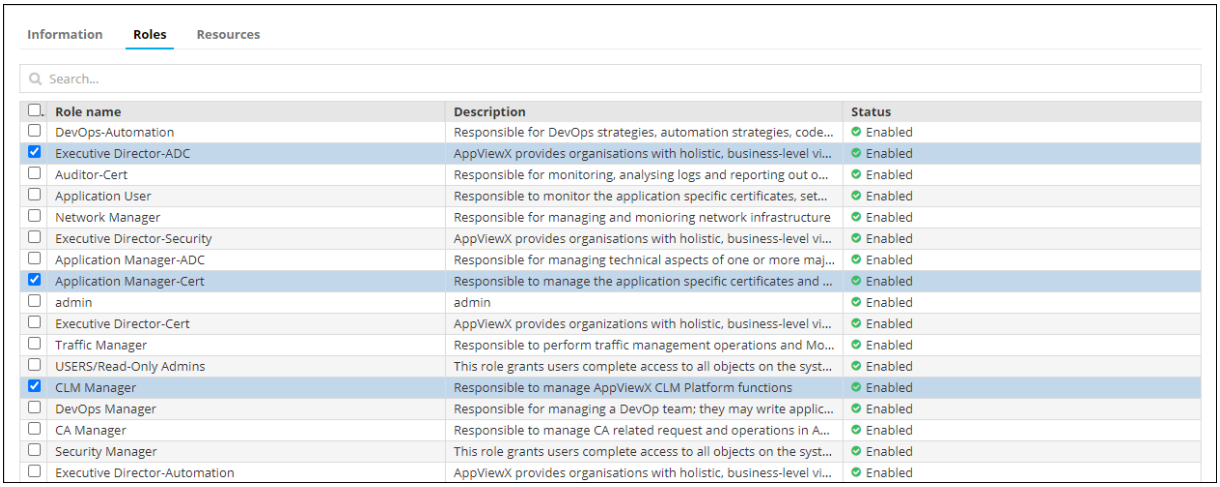


6. Enter the following details:

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)

***Mandatory**

7. Click Save.
8. 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,

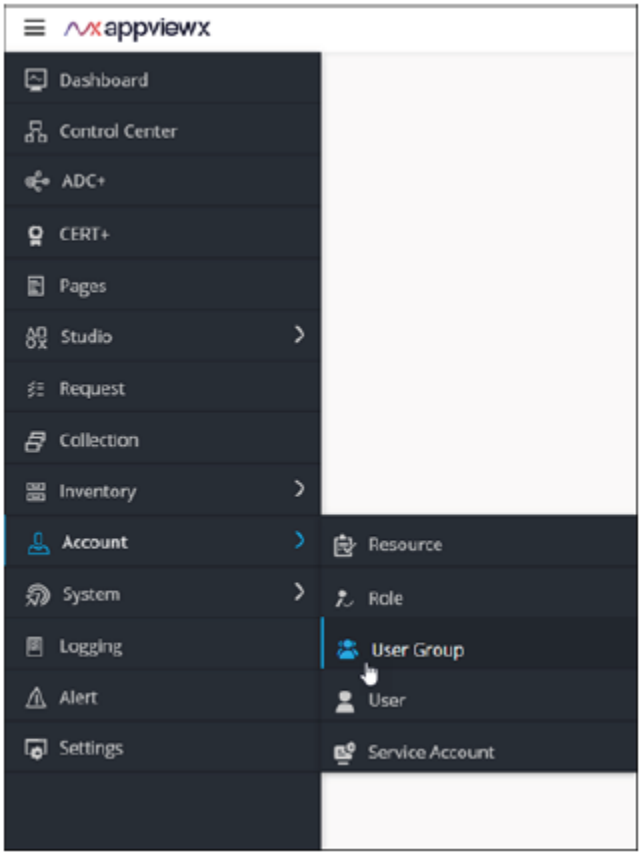
the higher-level access permissions (Read/Write) take precedence and the user has Read/Write access.

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.

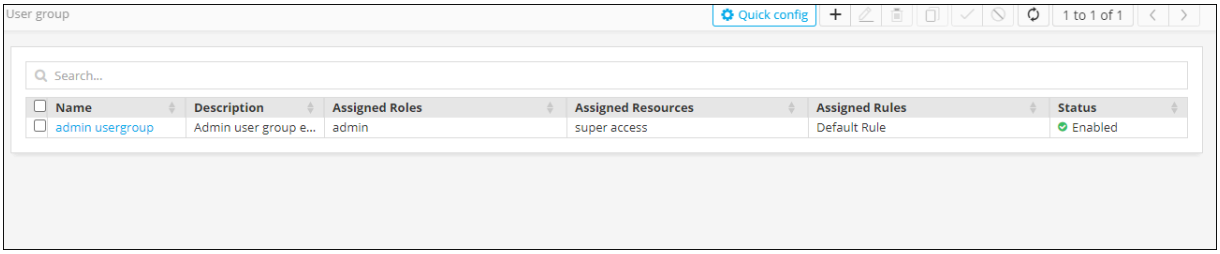
Cloning a User Group

To clone a user group:

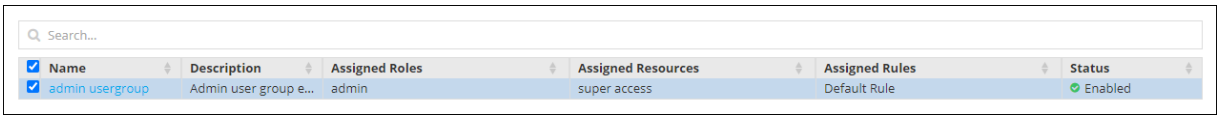
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Account > User Group.



3. The User Group page is displayed.

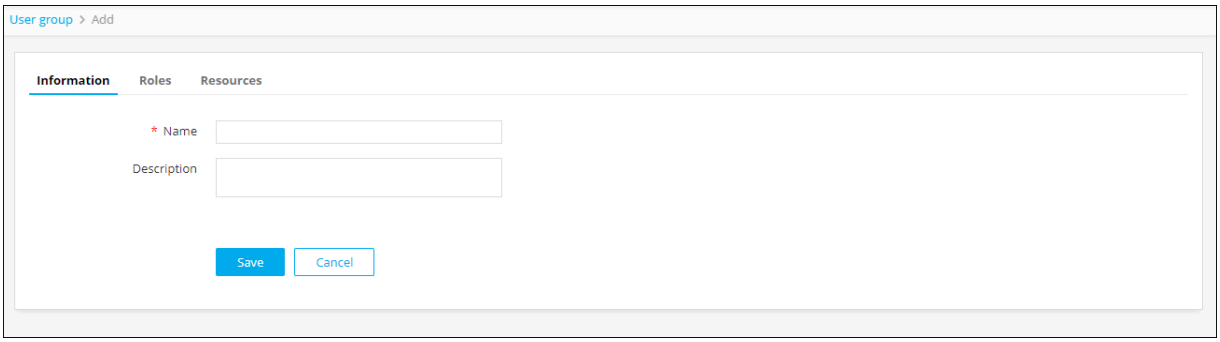


4. From the User Group page, select the user group you want to clone.



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

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



7. 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)

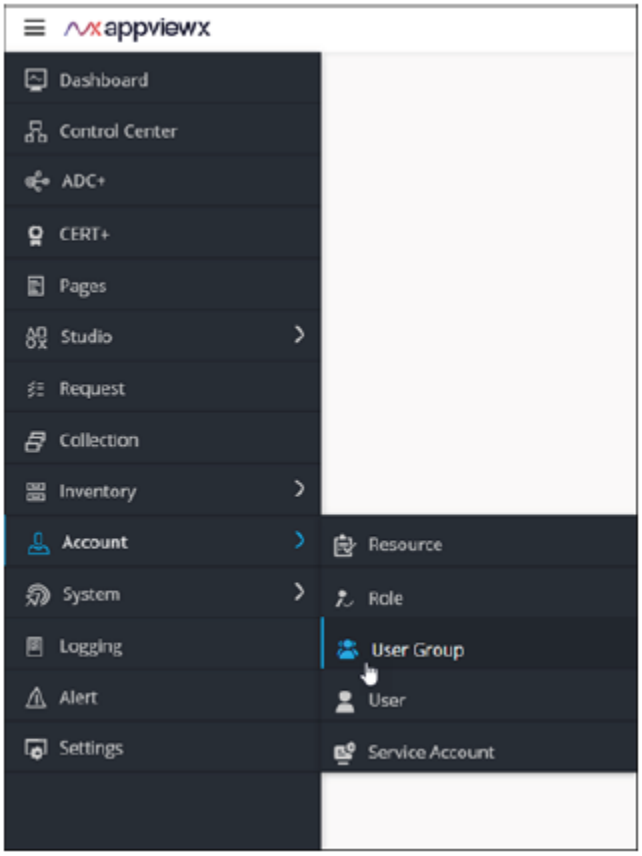
***Mandatory**

8. Click Save.

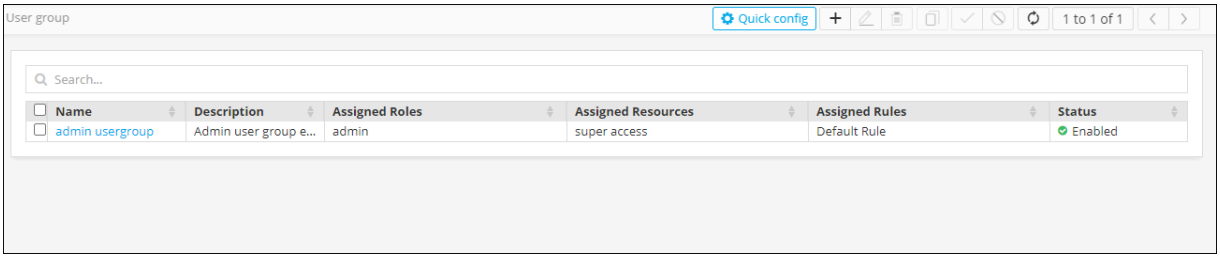
Modifying a User Group

To create a user group:

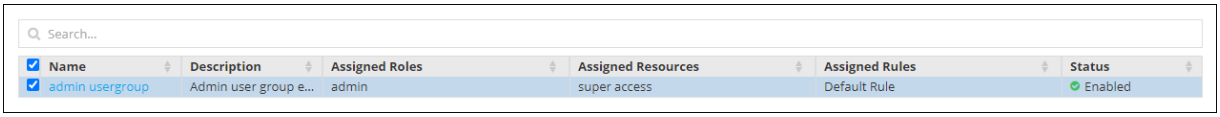
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Account > User Group.



3. The User Group page is displayed.

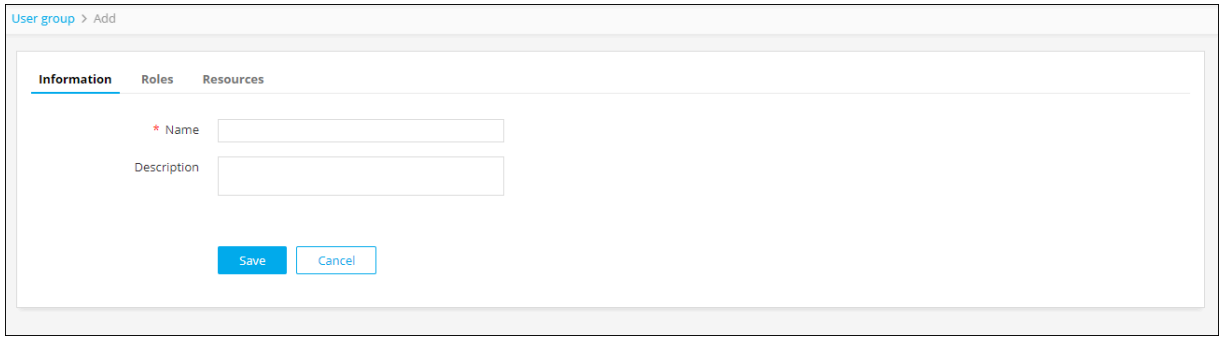


4. From the User Group page, select the user group you want to modify.



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

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

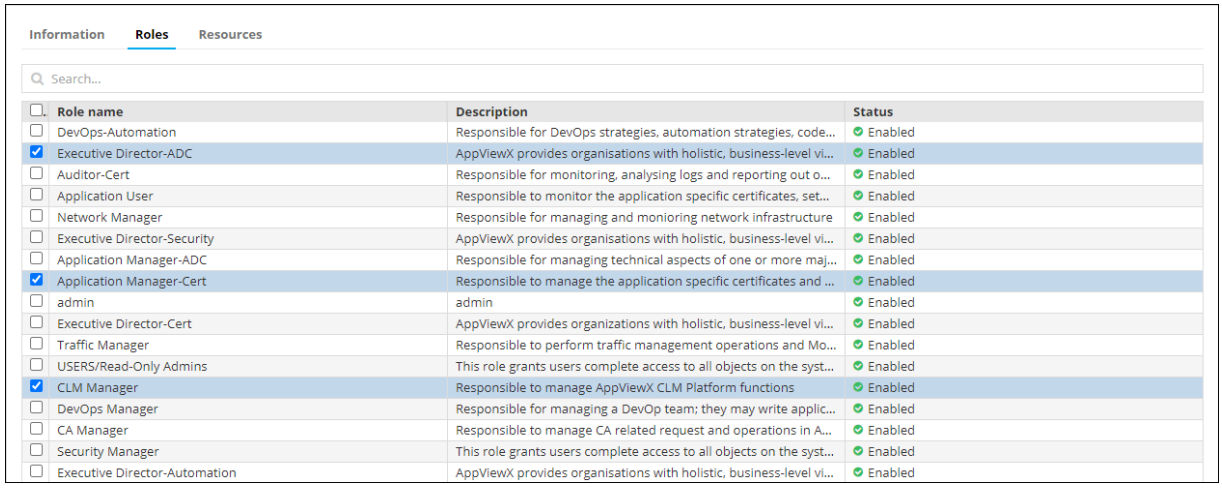


7. Update the required details:

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)

***Mandatory**

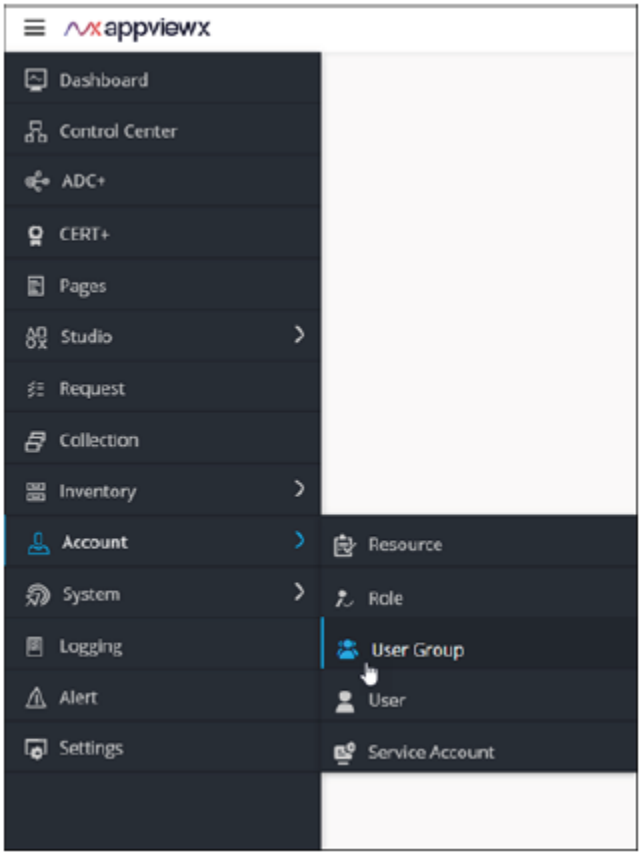
8. Click Save.
9. To modify the role assignment for this user group, in the Roles tab, select/clear the check boxes against the required roles and resources.



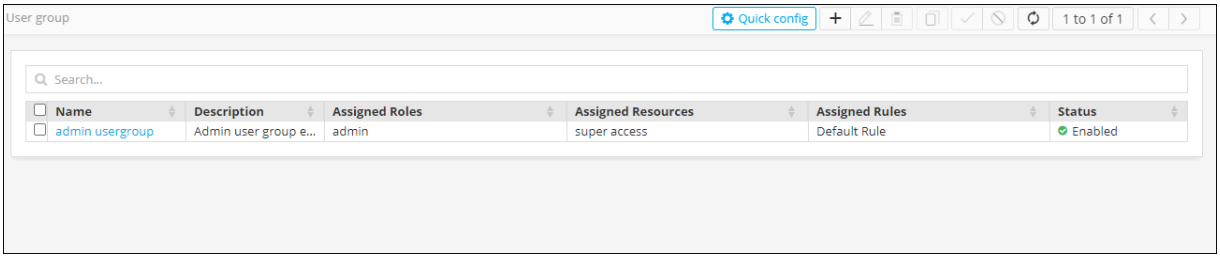
Deleting a User Group

To delete a user group:

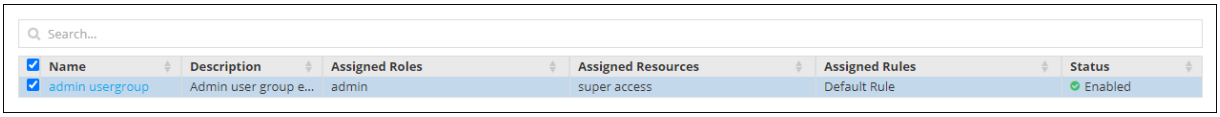
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Account > User Group.



3. The User Group page is displayed.



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



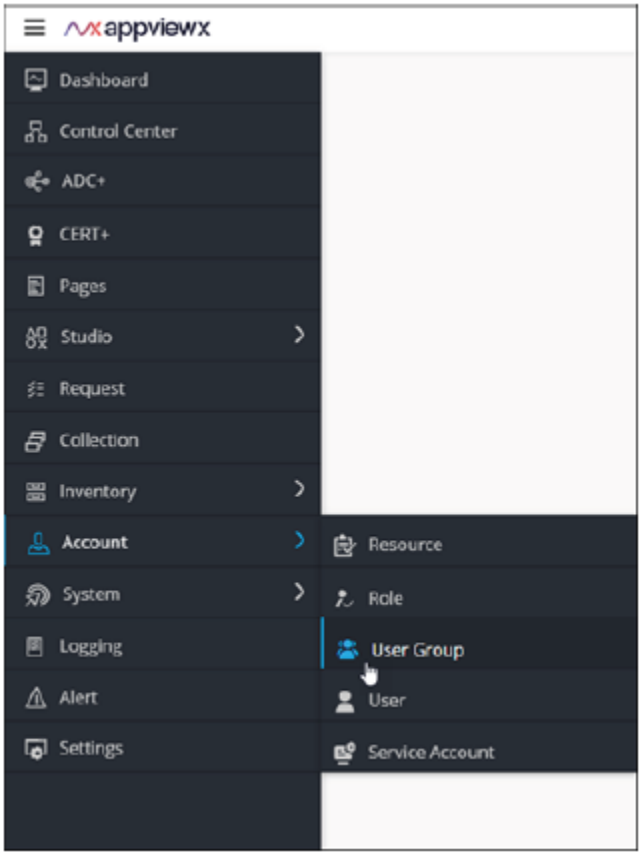
5. From the top right corner of the screen, click 

6. In the Confirmation dialog box, click Yes.

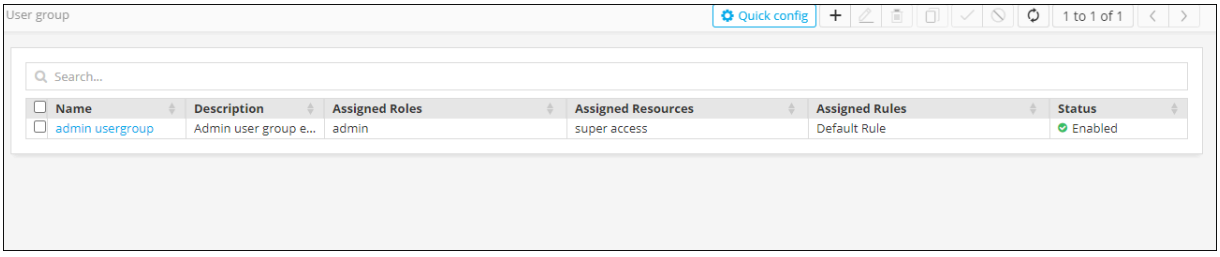
Disabling a User Group

To disable a user group:

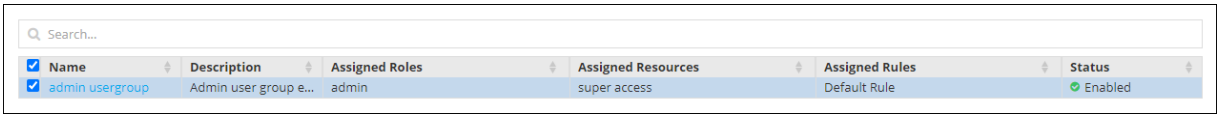
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Account > User Group.



3. The User Group page is displayed.



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



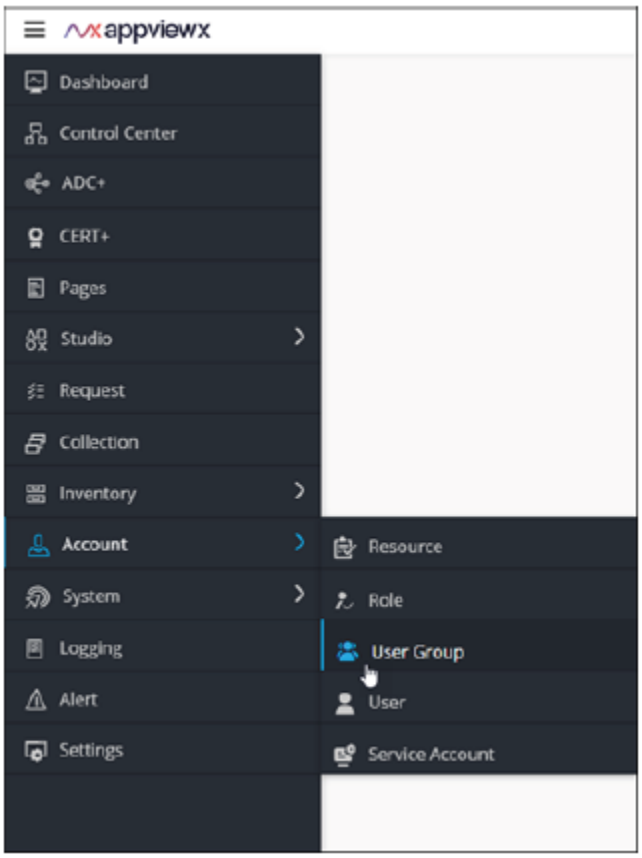
5. From the top right corner of the screen, click 

6. In the Confirmation dialog box, click Yes

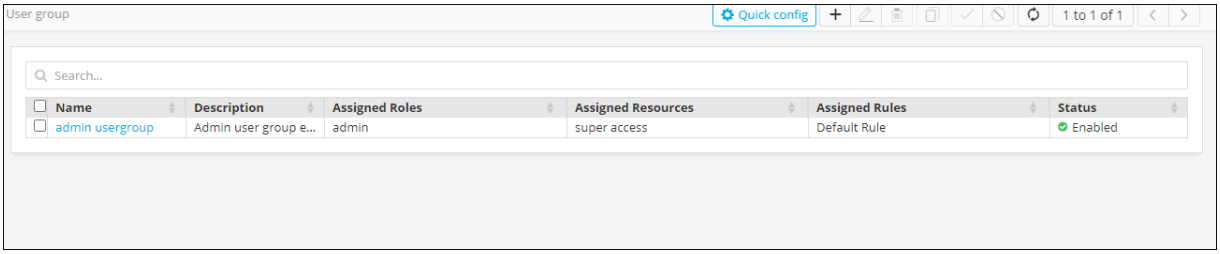
Enabling a User Group

To enable a user group:

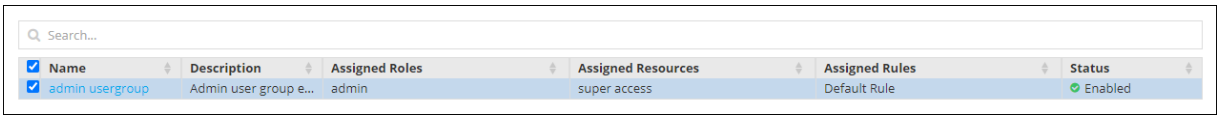
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Account > User Group.



3. The User Group page is displayed.



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



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

6. In the Confirmation dialog box, click Yes

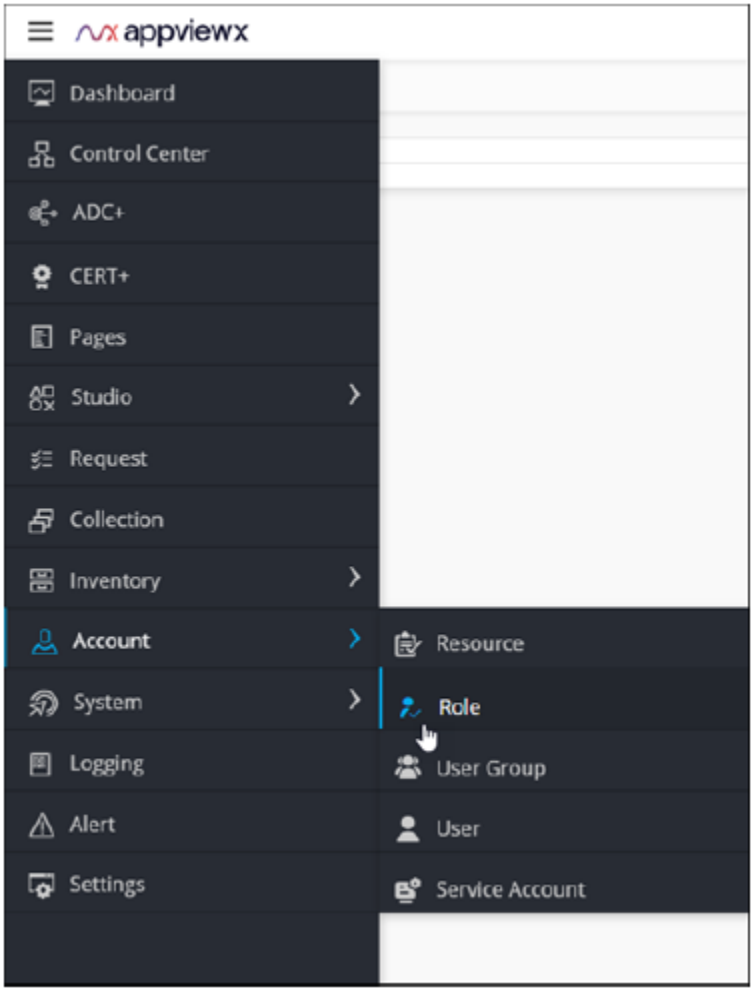
Managing Roles

- Creating a Role
- Deleting a Role
- Disabling a Role
- Enabling a Role
- Cloning a Role
- Modifying a Role

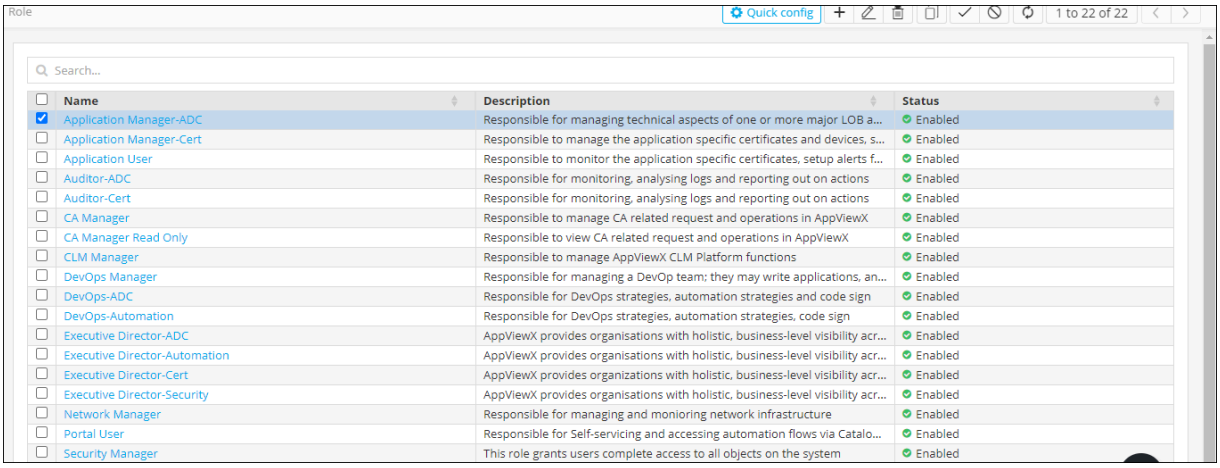
Creating a Role

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, click Account > Role.

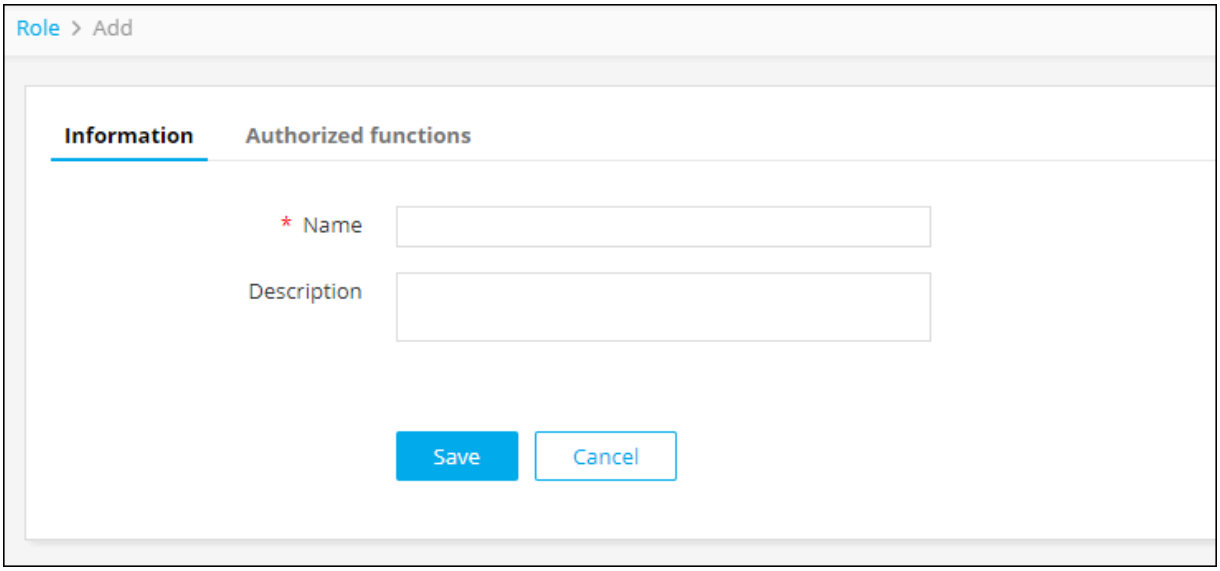


3. The Role page is displayed.



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

5. The Add page is displayed.



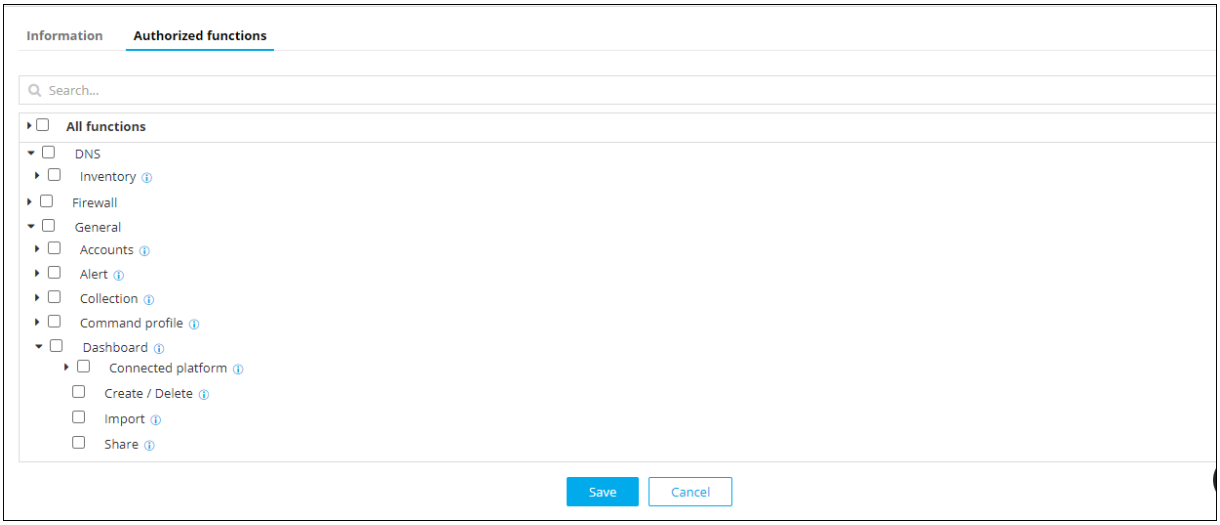
6. Under the Information tab, enter the following details:

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

***Mandatory**

7. Click Save.
8. In the Authorized functions section, select the checkbox beside 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.

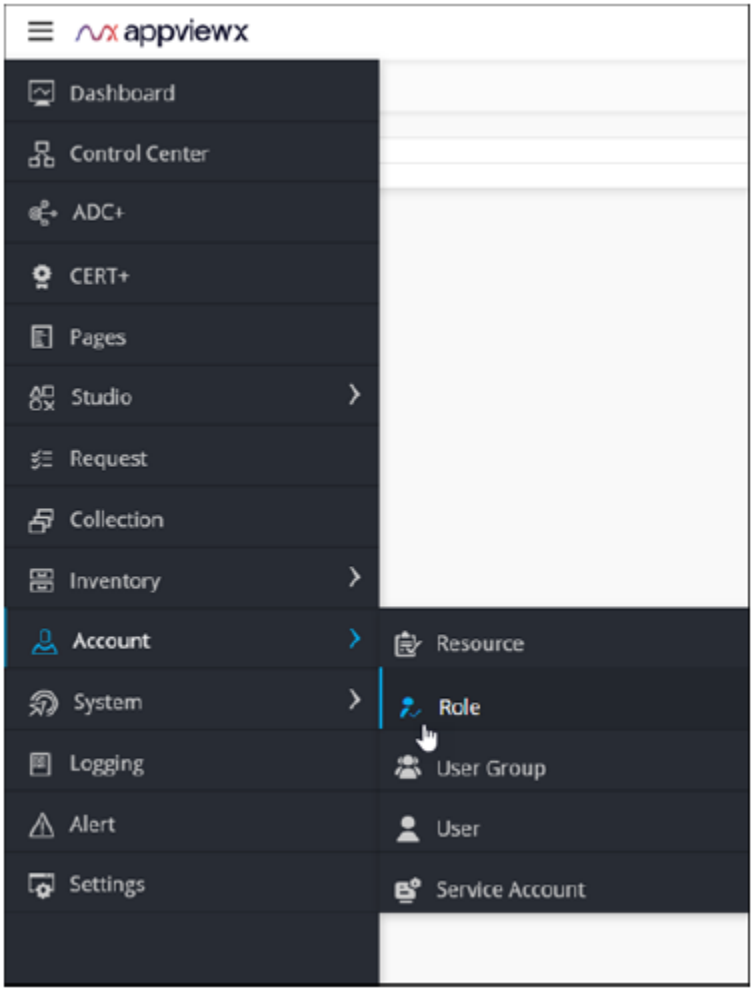
10. Click Save. Details of the new role are displayed in the list on the Role page.

Deleting a Role

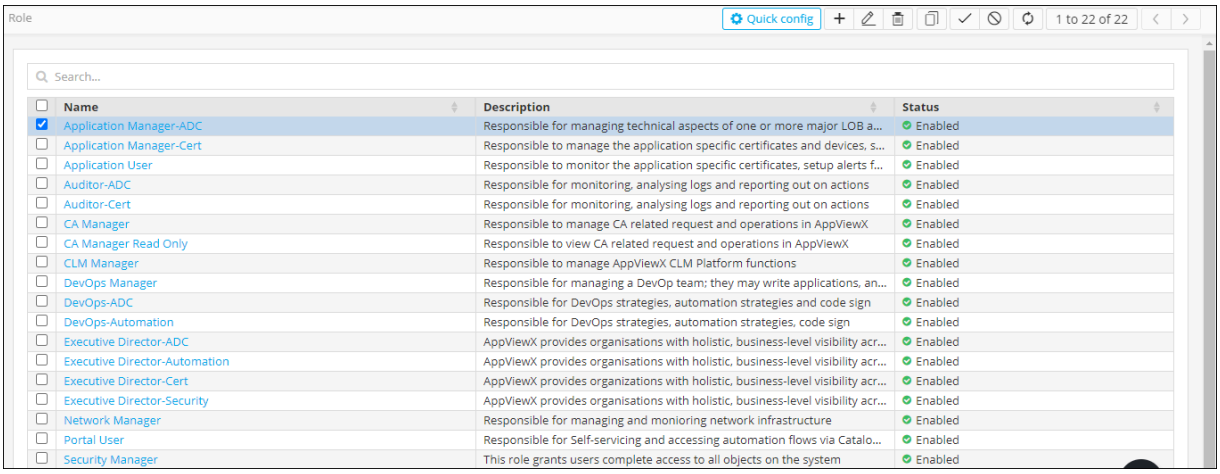
Note: A role that has active users belonging to it cannot be deleted.

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, click Account > Role.



3. The Role page is displayed.



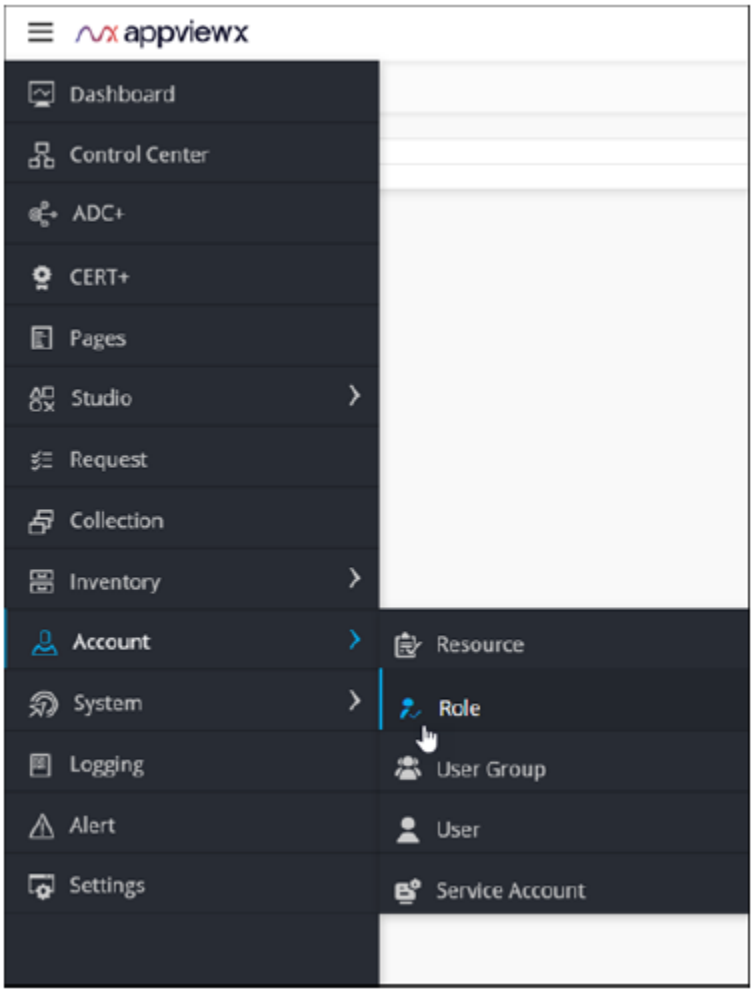
4. For the record you want to delete, select the corresponding check box.
5. From the top right corner of the screen, click 

6. In the Confirmation dialog box, click Yes.

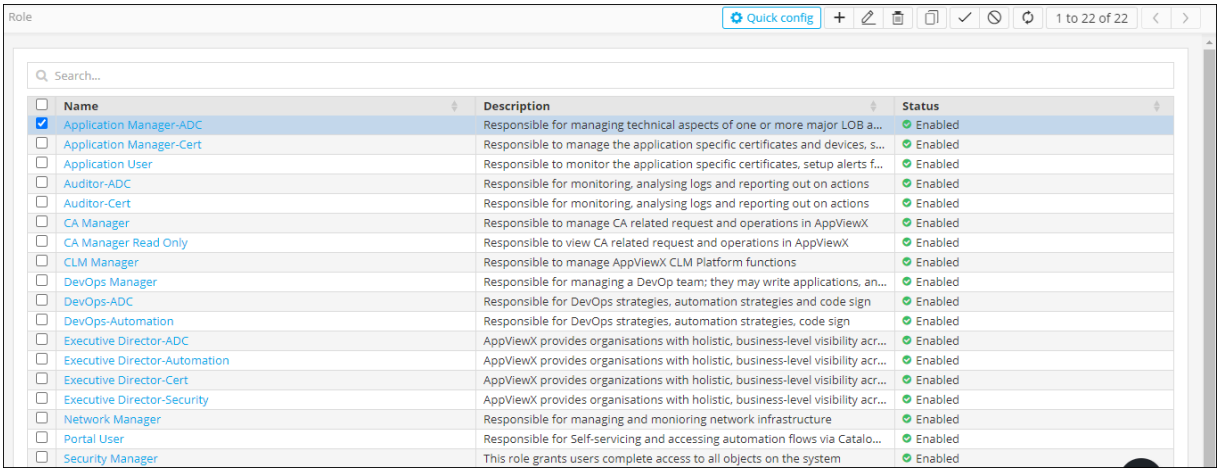
Disabling a Role

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.



3. The Role page is displayed.



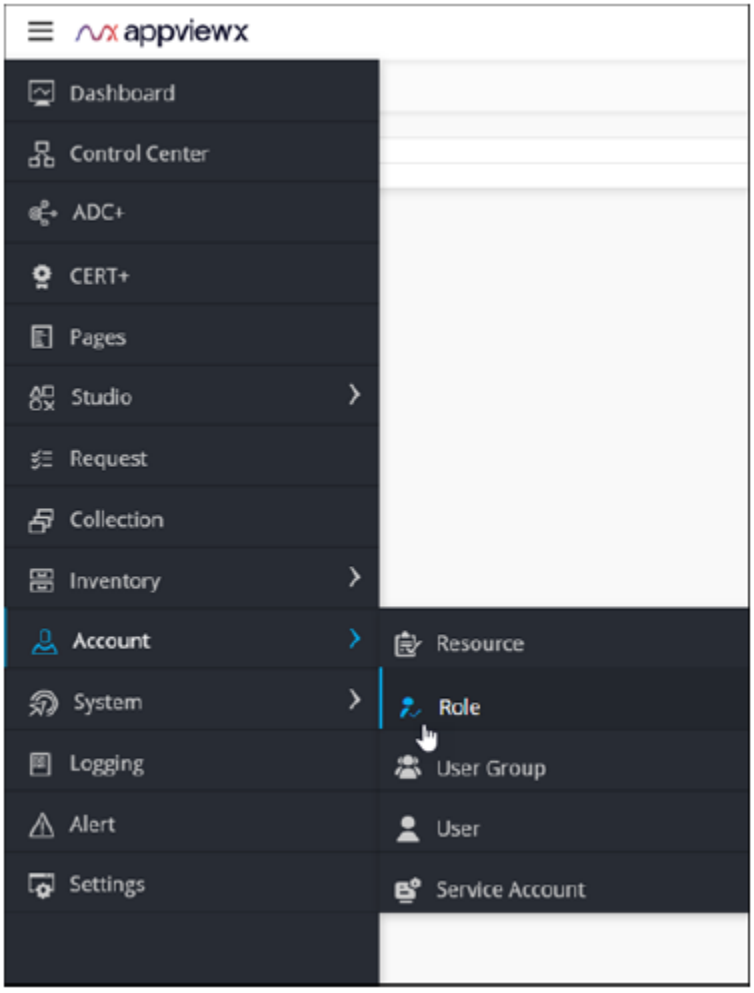
4. For the (enabled) role you want to disable, select the corresponding check box.
5. From the top right corner of the screen, click 

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

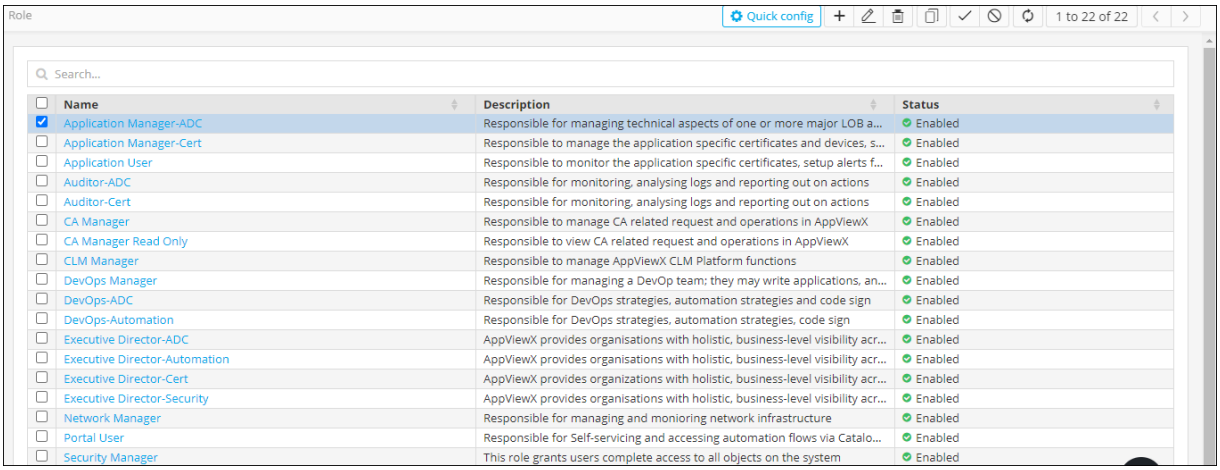
Enabling a Role

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.



3. The Role page is displayed.



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

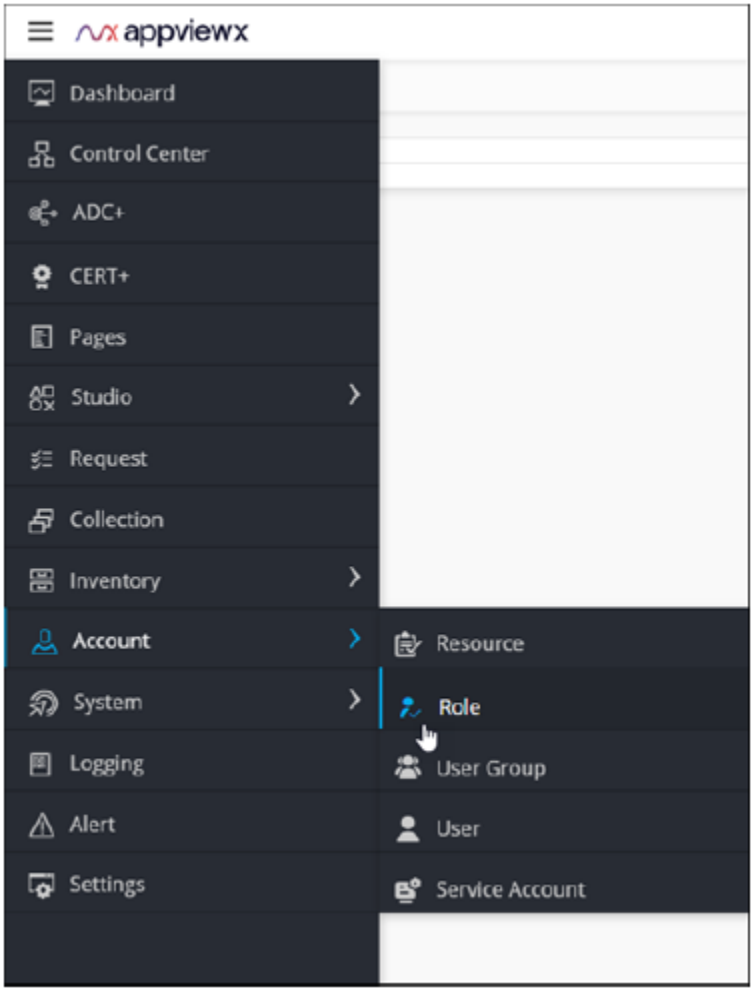
6. In the Confirmation dialog box, click Yes. The selected role is enabled.

Cloning a Role

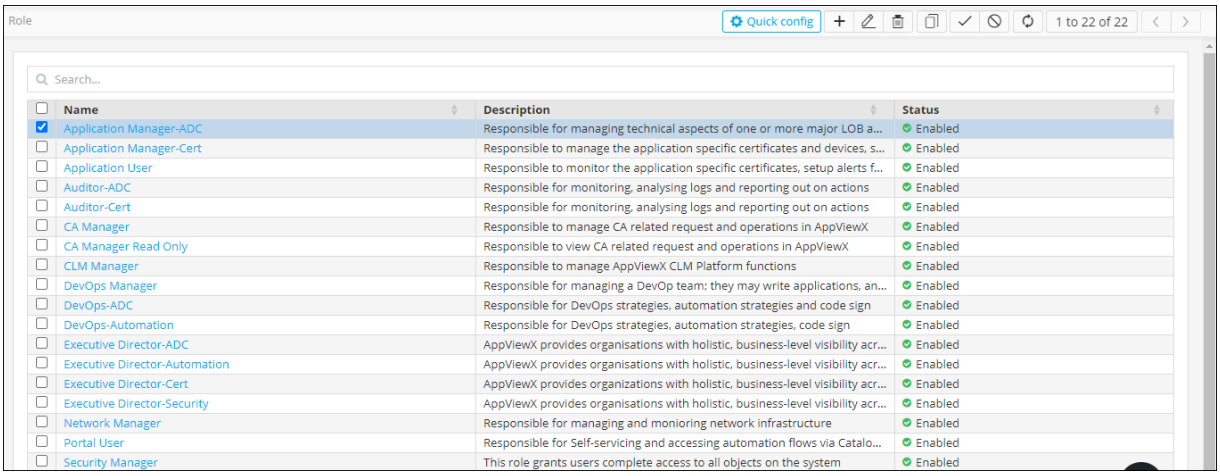
Cloning lets you create a copy of an existing role with a different name. You can modify the permissions and tasks that can be performed while cloning a role.

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.

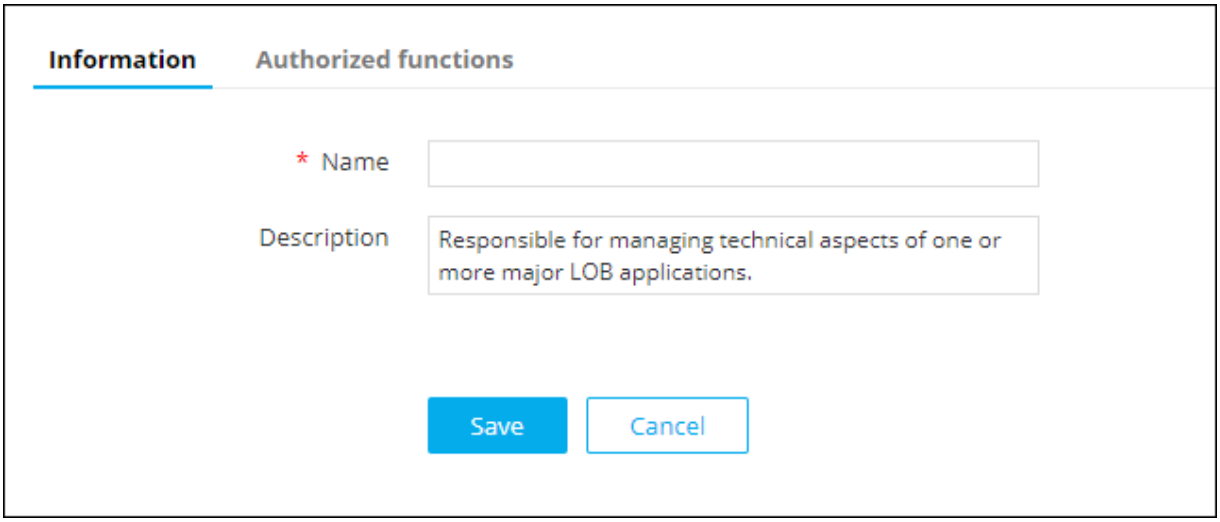


3. The Role page is displayed.



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

6. In the Information section, enter a new name for the role.

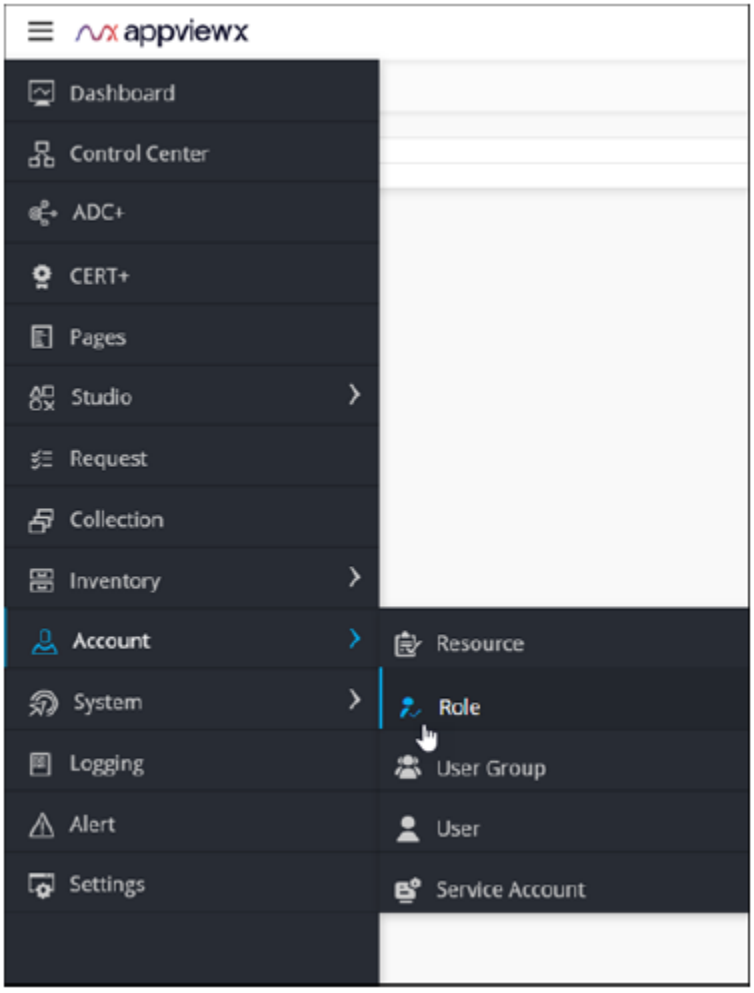


7. Click Save.

Modifying a Role

To modify a role:

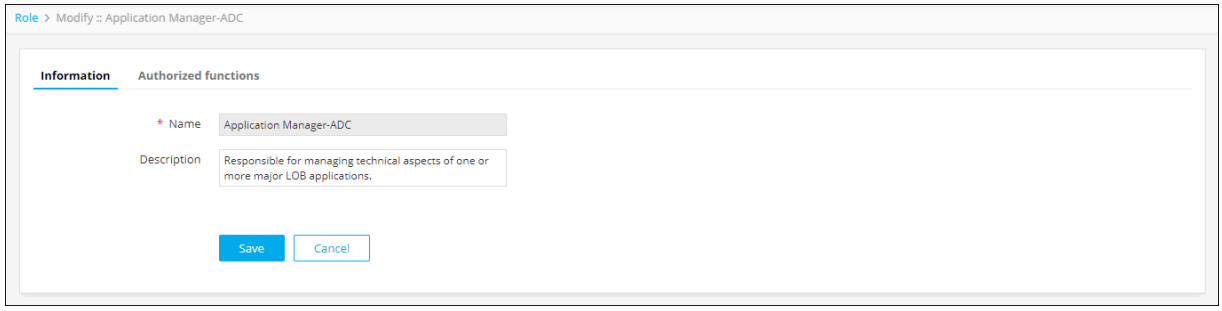
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Account > Role. The Role page is displayed.



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

5. The Modify :: Application Manager-ADC page is displayed (because we selected the Application Manager role)

6. Modify the details in the Information and Authorized functions as required.



7. Click Save.

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.

- Authentication
- Resource
- Role
- User Group

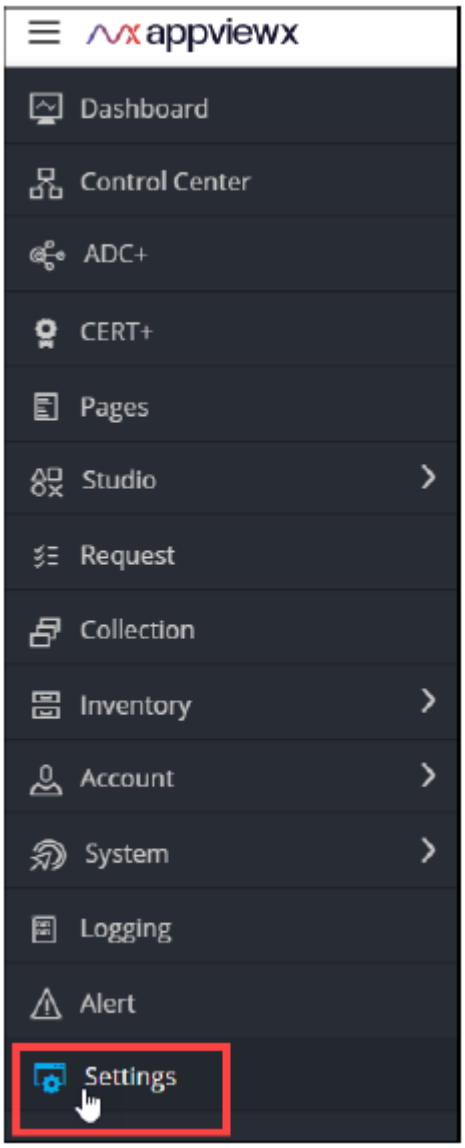
Authentication

• Configure the Role-Based Access Control for LDAP
• Configuring Role-Based Access Control for TACACS
• Configuring Role-Based Access Control for RADIUS

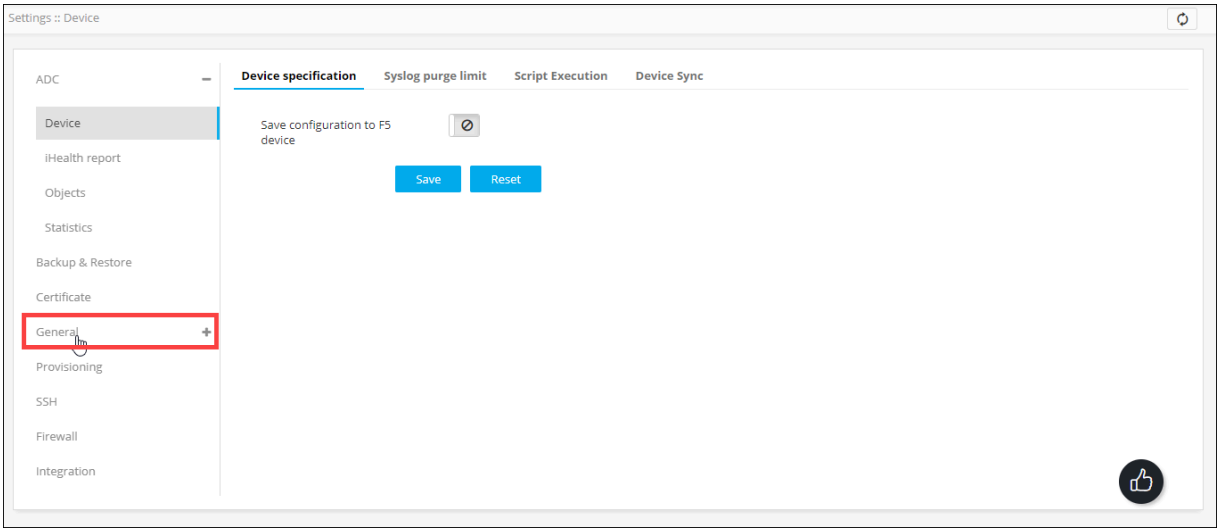
Configure the Role-Based Access Control for LDAP

To configure the RBAC settings for LDAP:

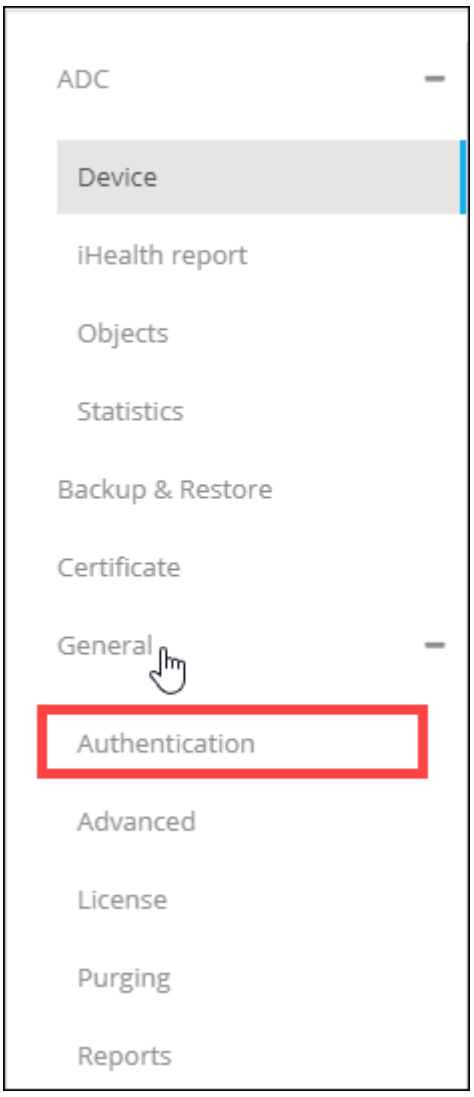
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Settings.



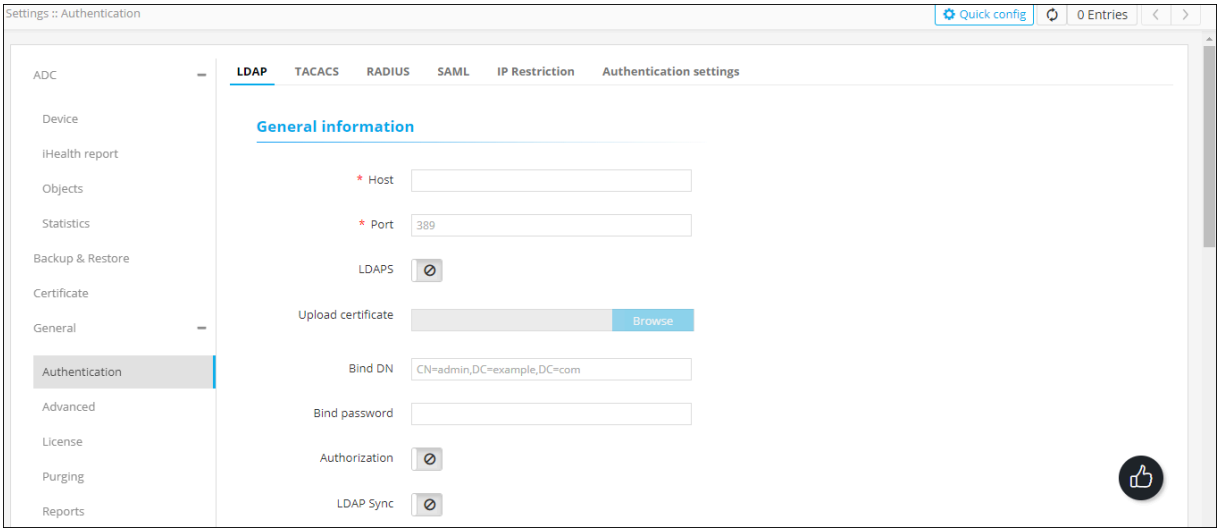
3. On the Settings page, from the navigation pane on the left, click General.



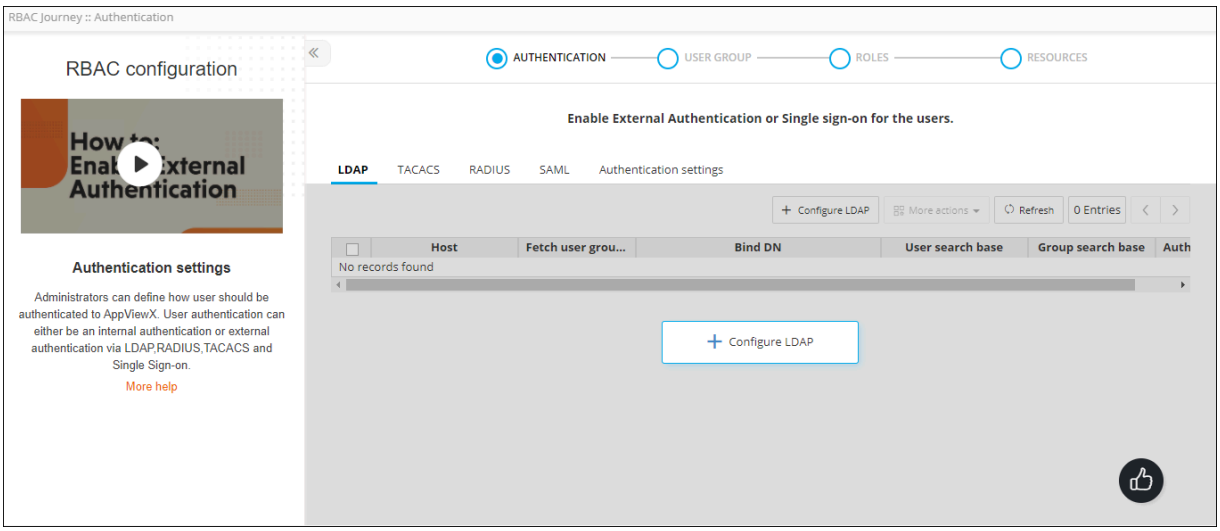
4. Under General settings, click Authentication.



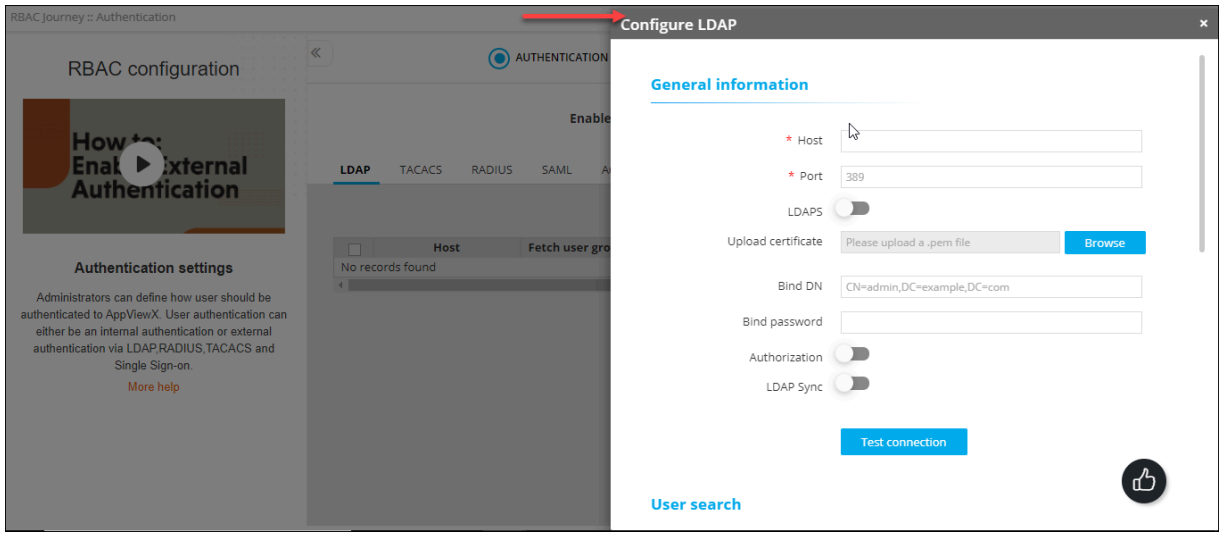
5. The Settings :: Authentication page is displayed, with the LDAP tab open by default.



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



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



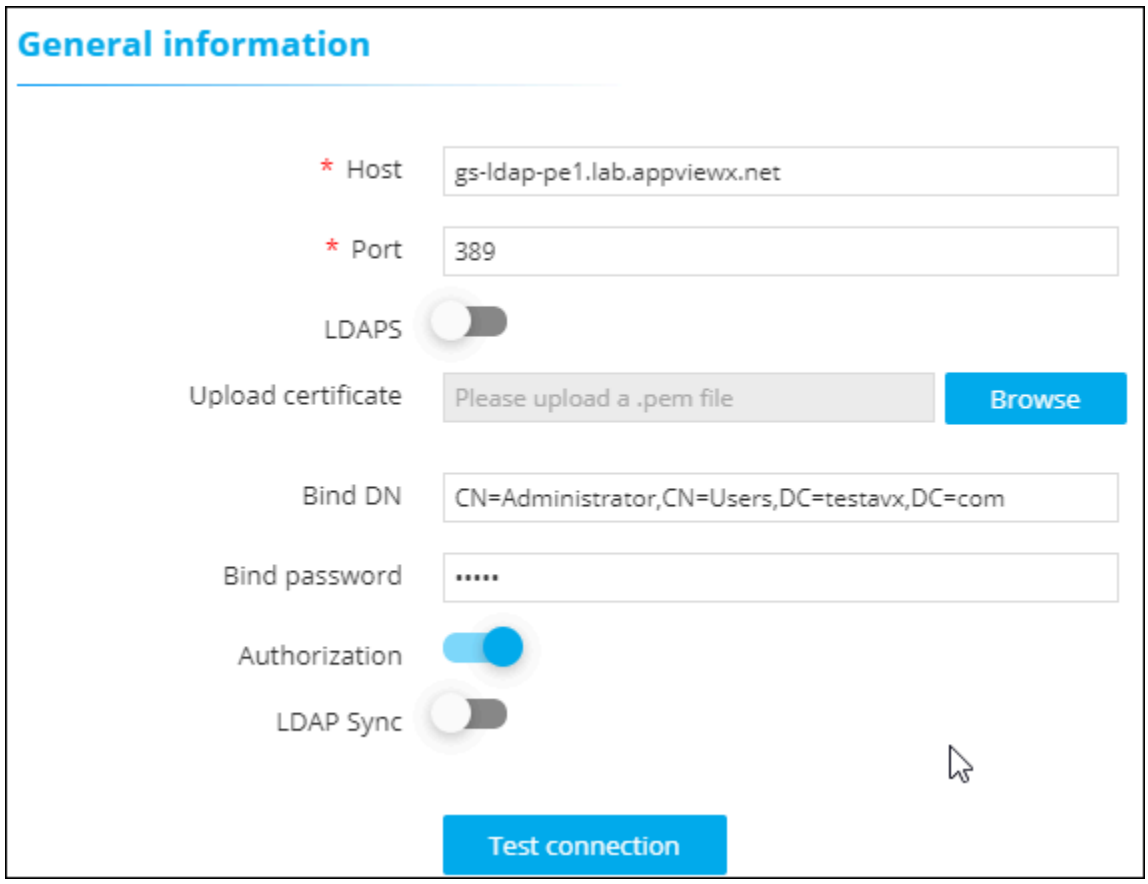
8. In the General Information section, enter the following details (sample values are shown in the image below the table):

Field	Description
Host*	Hostname (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 an LDAP configuration and port number 636 is used for an LDAPS configuration.
LDAPS	The LDAPS protocol is used for secure communication between AppViewX and Active Directory/Open LDAP. To enable the use of the LDAPS protocol, instead of the LDAP protocol, enable this toggle key.
Upload Certificate*	**Note:** This field is enabled only when the LDAPS is enabled.

Field	Description
	To upload an LDAP server certificate: • Click Browse Certificate. • 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. • 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.

Field	Description
LDAP Sync	To enable the use of the SSH module in App-ViewX for SSH key discovery use case, enable this toggle key.

***: Mandatory**



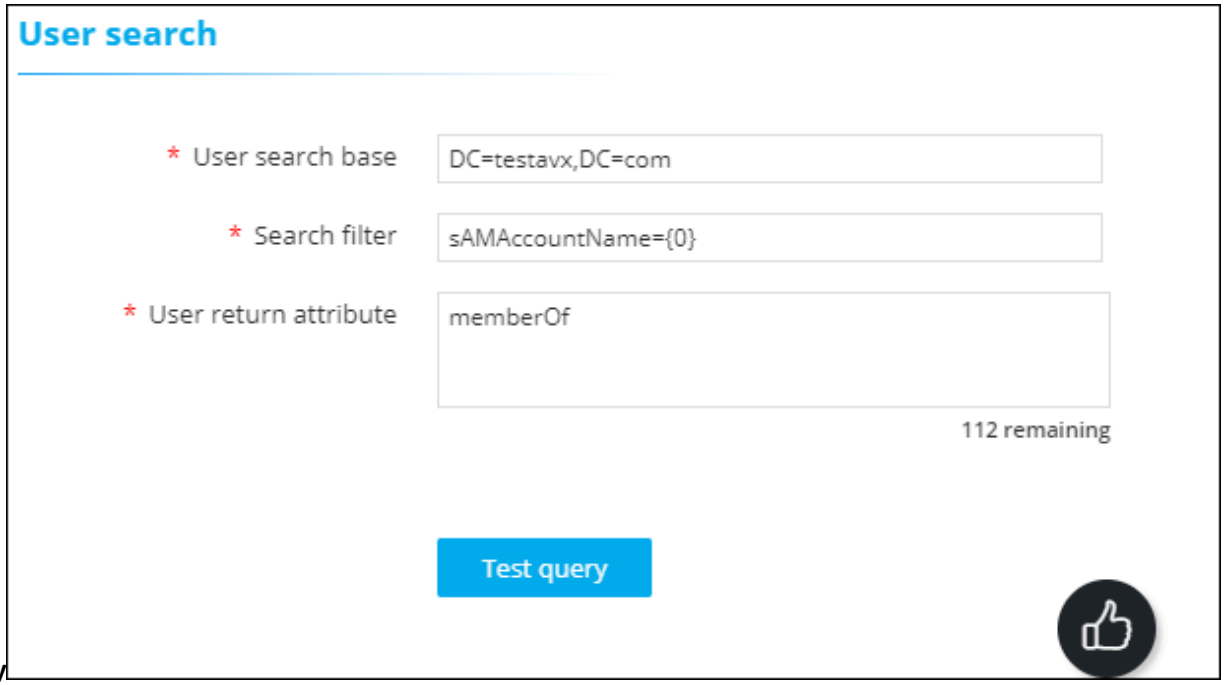
9. After entering the above connection details, to test if the host is reachable and the port is valid for establishing an LDAP/LDAPS connection, click Test Connection.

> **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.

10. 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. **Note:** This field is enabled only when Authorization (in the General Information section) is enabled. **Note:** You can specify only User return attribute.

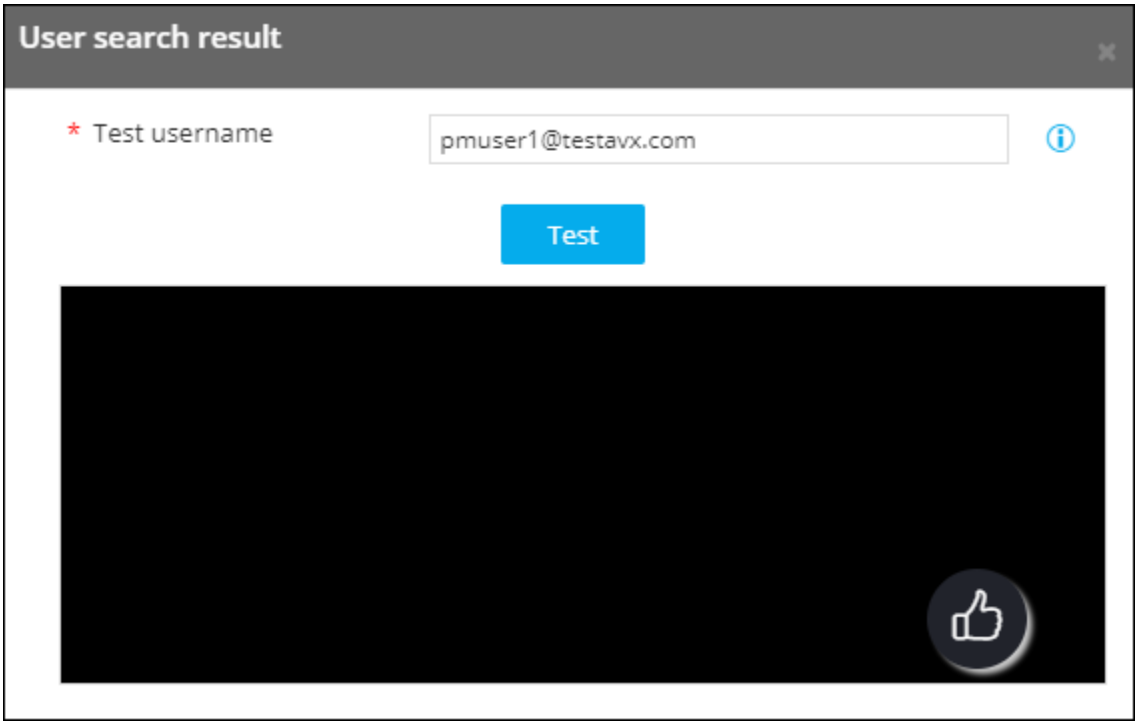
***:**



Mandatory

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

12. 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.

13. To test which user group the user belongs to (and, in the Group search section, enter the following details:

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

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

***: 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.

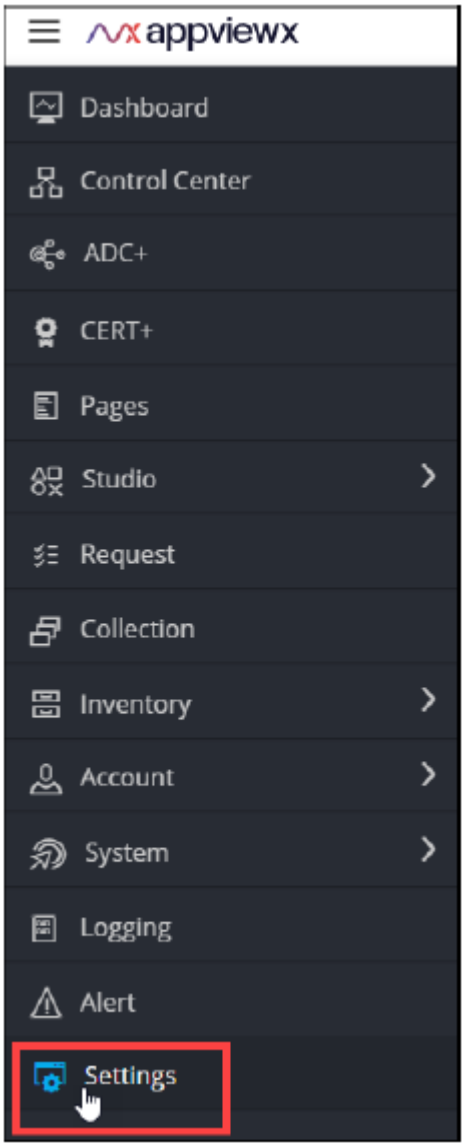
Note: In the case of multiple LDAP servers, to define/update the order in which the servers will be authenticated, drag and drop the entries in this table.

• Deleting a LDAP Configuration

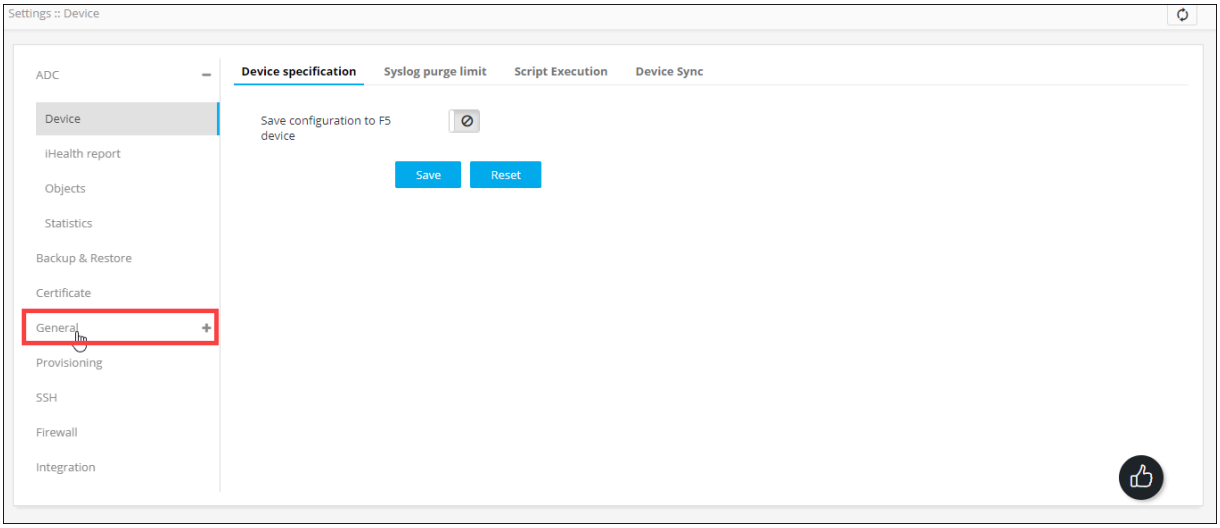
Deleting a LDAP Configuration

To delete a LDAP configuration:

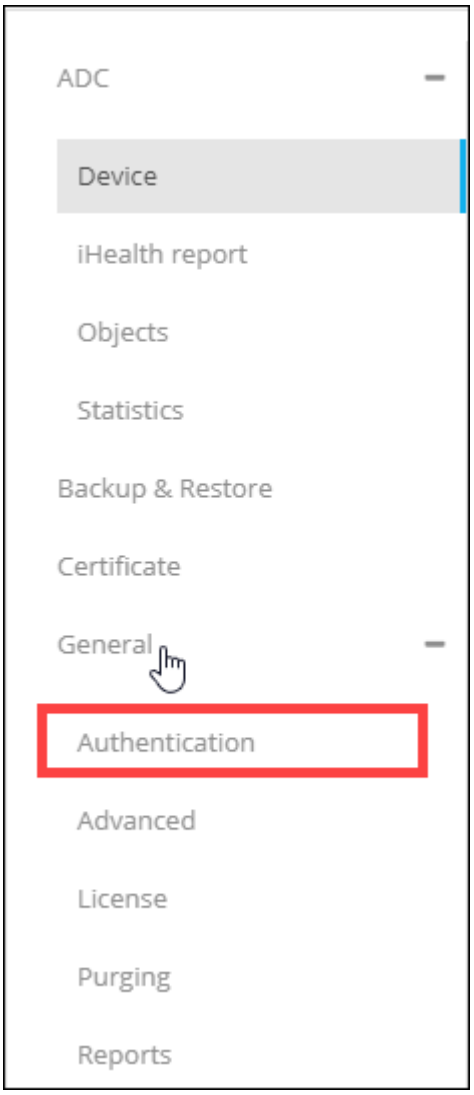
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Settings.



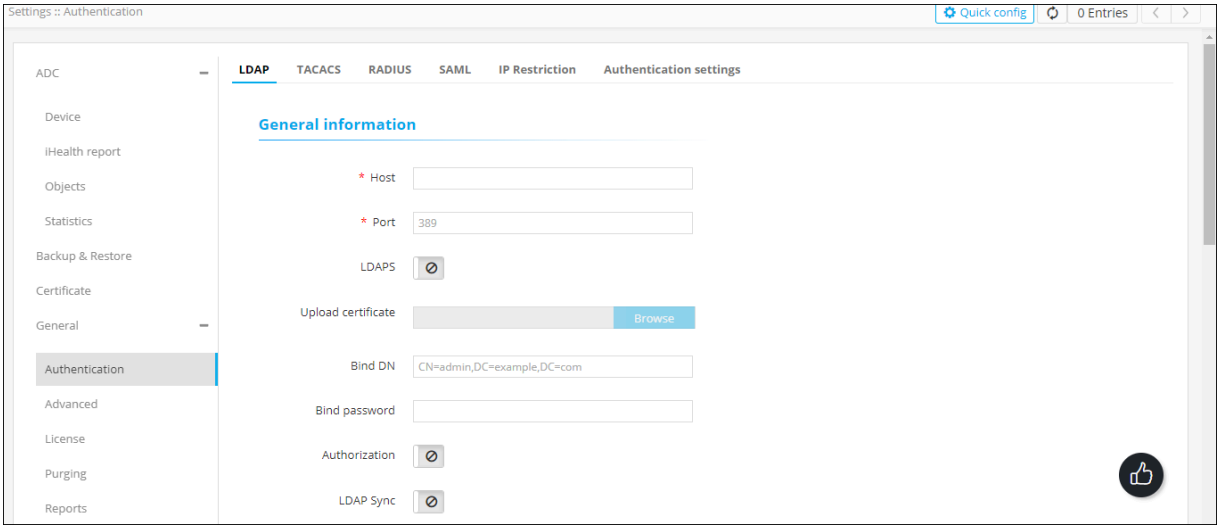
3. On the Settings page, from the navigation pane on the left, click General.



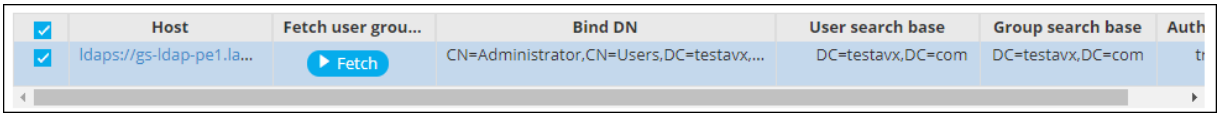
4. Under General settings, click Authentication.



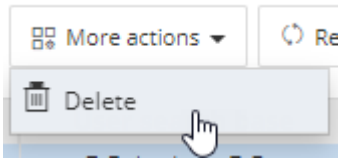
5. The Settings :: Authentication page is displayed, with the LDAP tab open by default.



6. From the top-right corner of the screen, click Quick Config. The RBAC Journey :: Authentication page is displayed.
7. From the table of LDAP configurations, to delete a LDAP configuration, select the check box corresponding to that entry.



8. From the More Actions drop-down menu, click Delete.

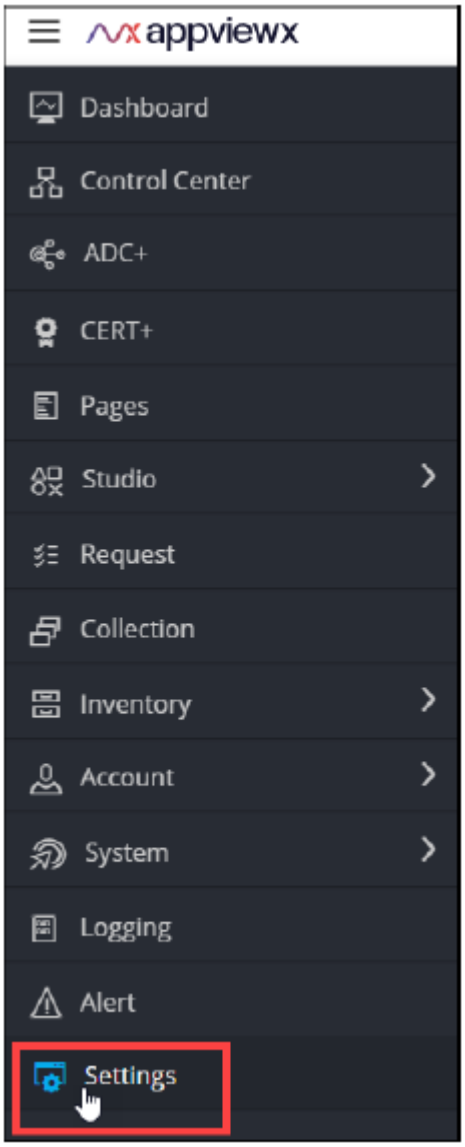


9. In the Confirmation dialog box, click Delete. The selected configuration is deleted.

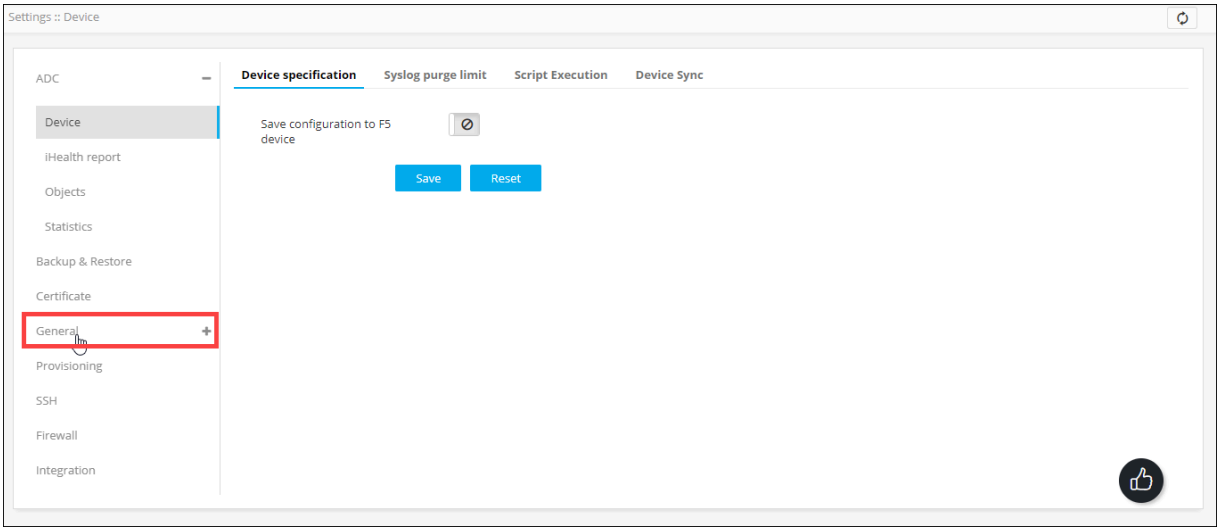
Configuring Role-Based Access Control for TACACS

To configure RBAC for TACACS authentication:

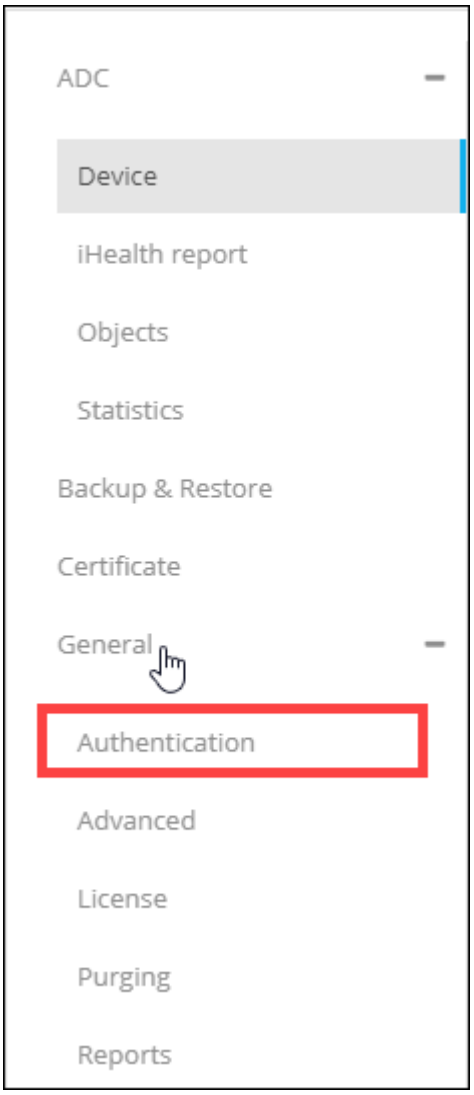
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Settings.



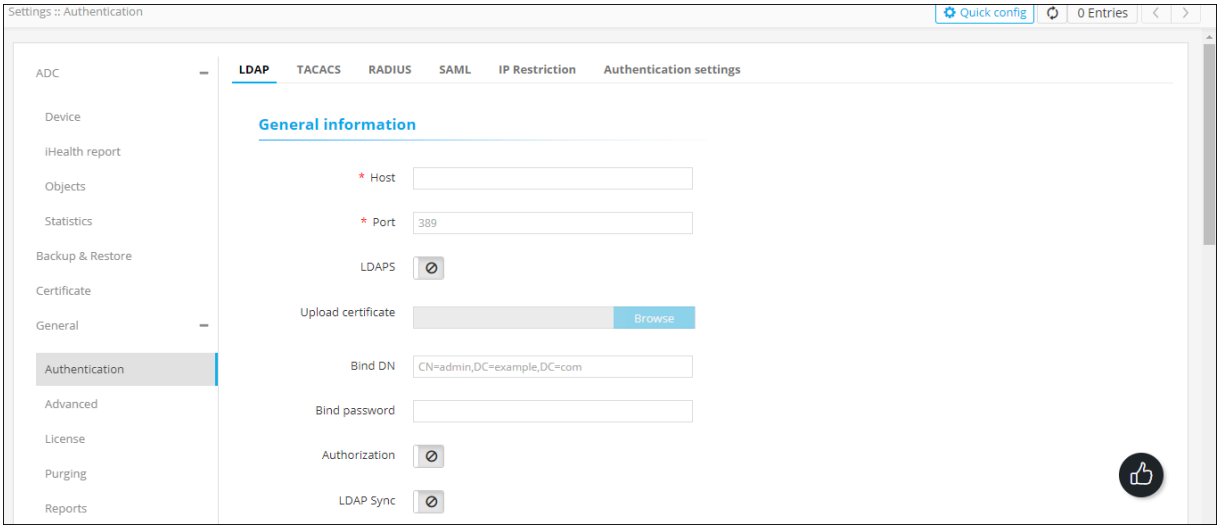
3. On the Settings page, from the navigation pane on the left, click General.



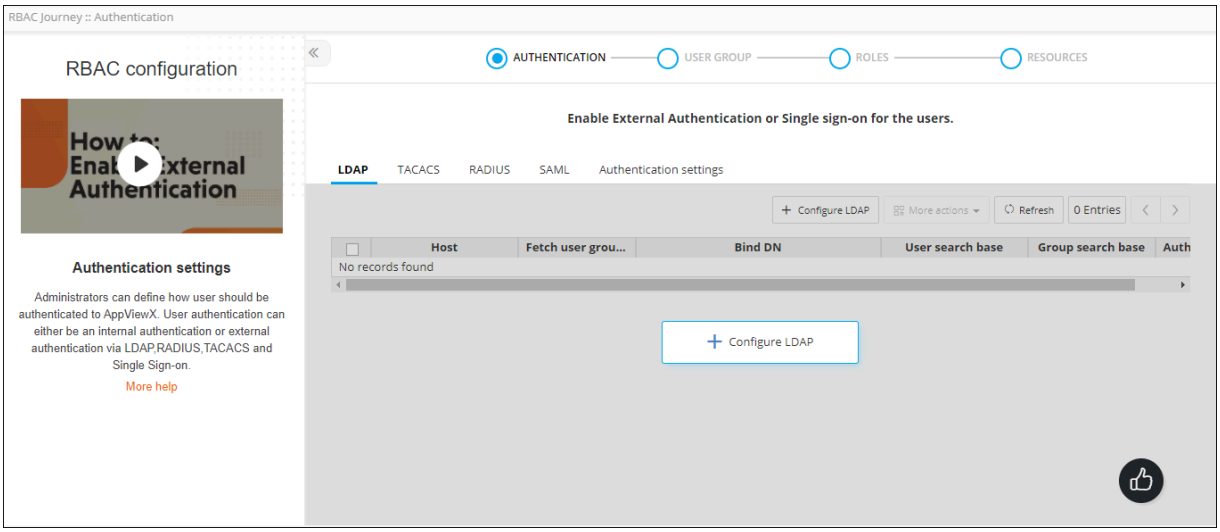
4. Under General settings, click Authentication.



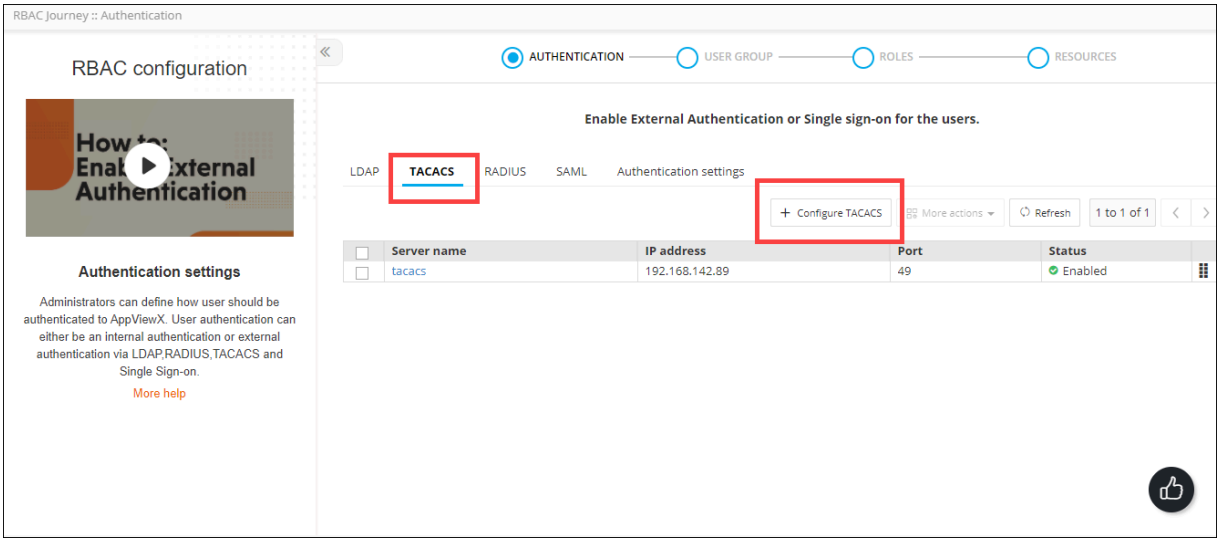
5. The Settings :: Authentication page is displayed, with the LDAP tab open by default.



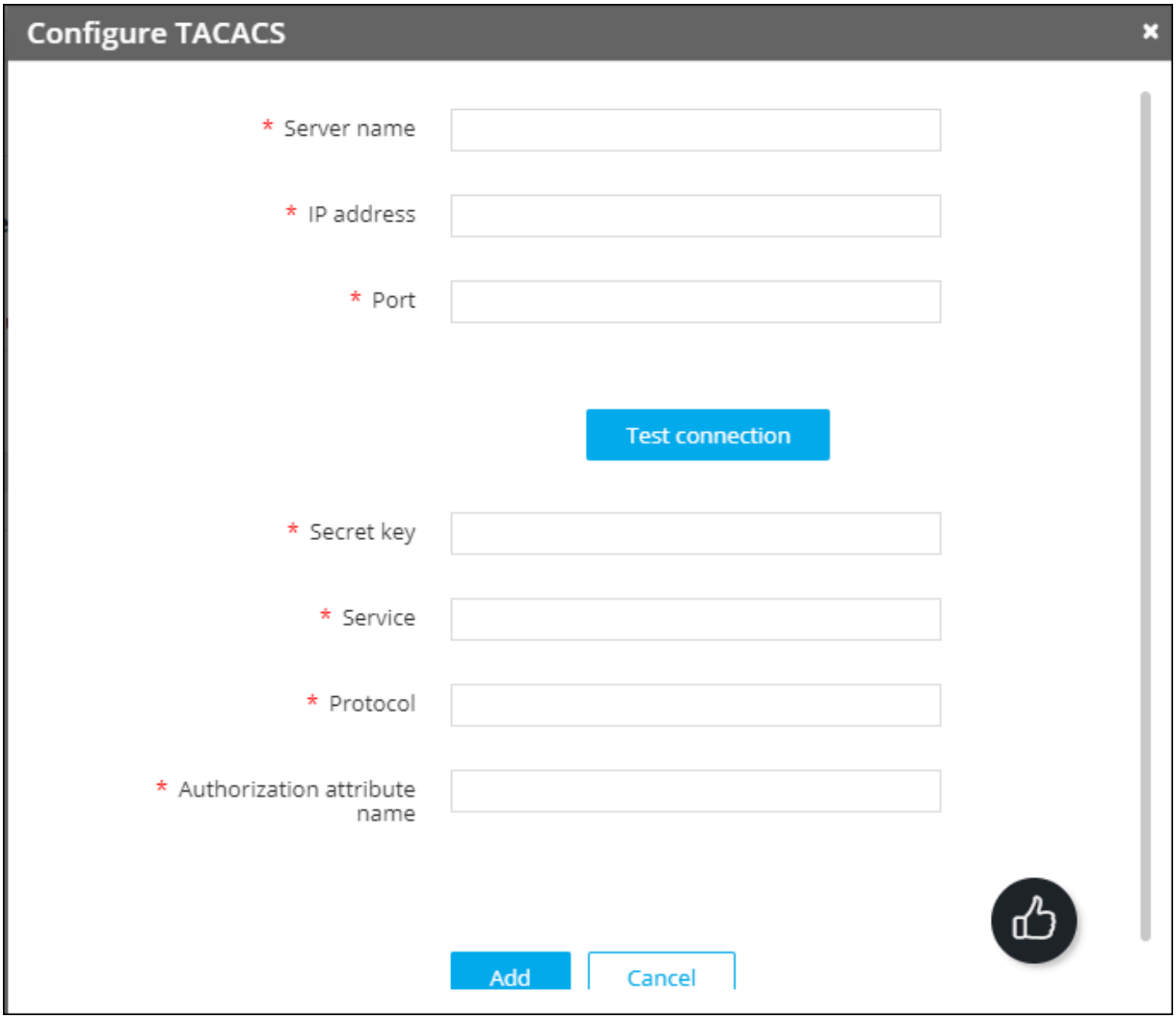
6. From the top-right corner of the screen, click Quick Config.
7. The RBAC Journey :: Authentication page is displayed.



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

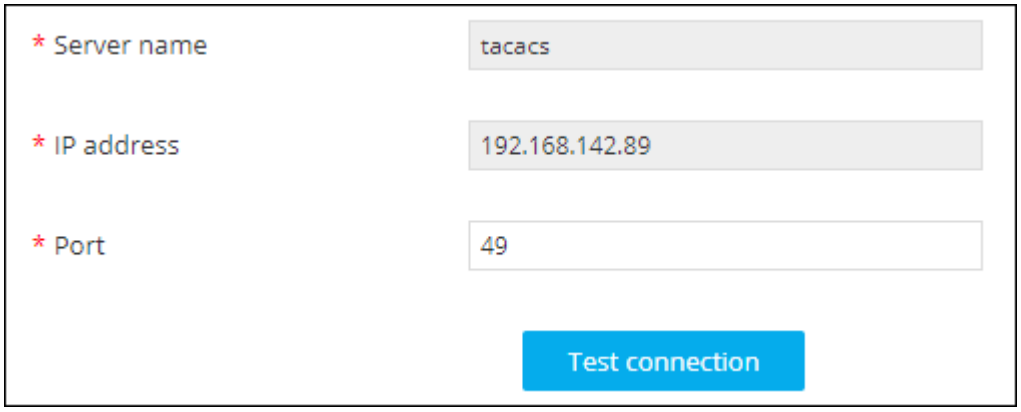


9. The Configure TACACS action pane is displayed.



10. 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

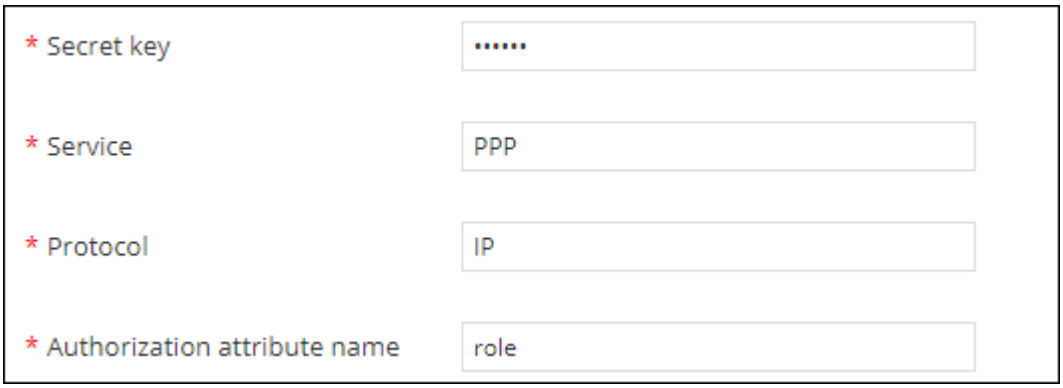


***:Mandatory**

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

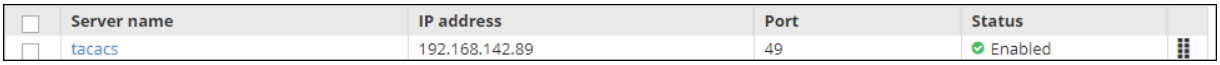
Field	Description
Secret key*	A unique key for authentication between the App-ViewX server and the TACACS server
Service*	Name of the service used by the user requested to be authorized Specifying the service name is mandatory be-cause it enables the TACACS+ server to behave according to the type of each authorization re-quest. 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 associ-

Field	Description
	ated 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



***Mandatory**

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



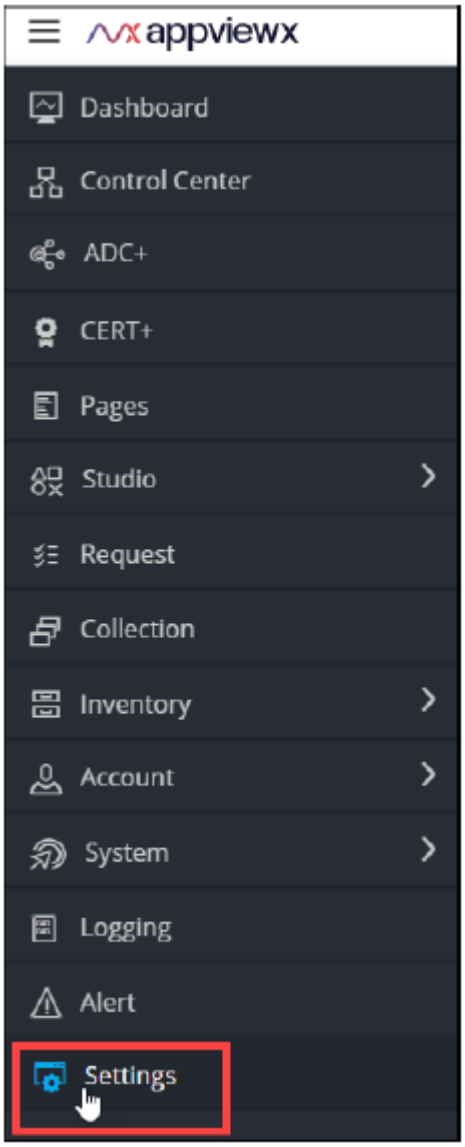
Note: In the case of multiple TACACS servers, to define/update the order in which the servers will be authenticated, drag and drop the entries in this table.

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

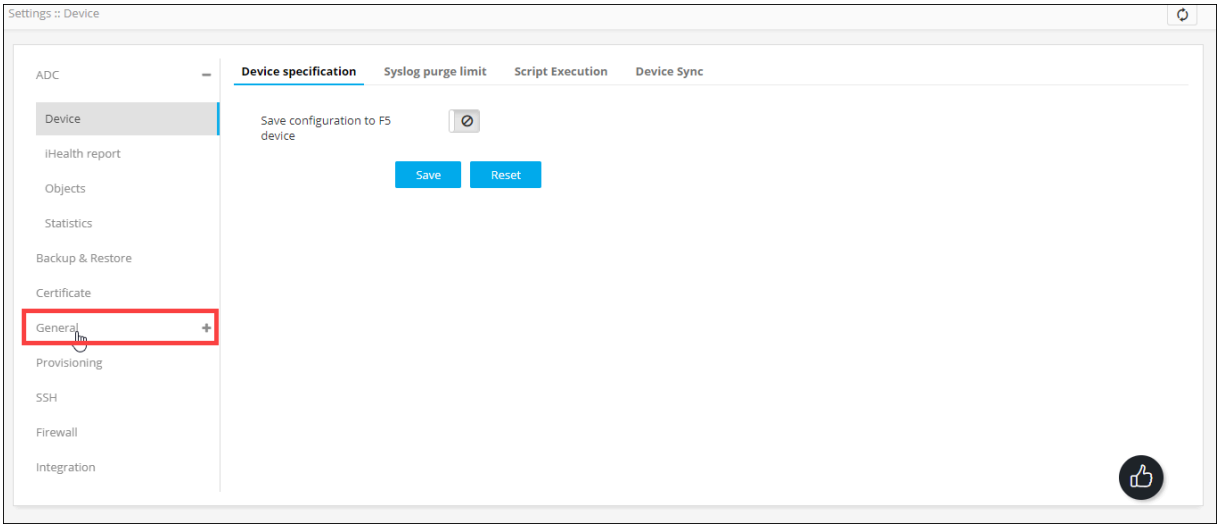
Deleting a TACACS Configuration

To delete a TACACS configuration:

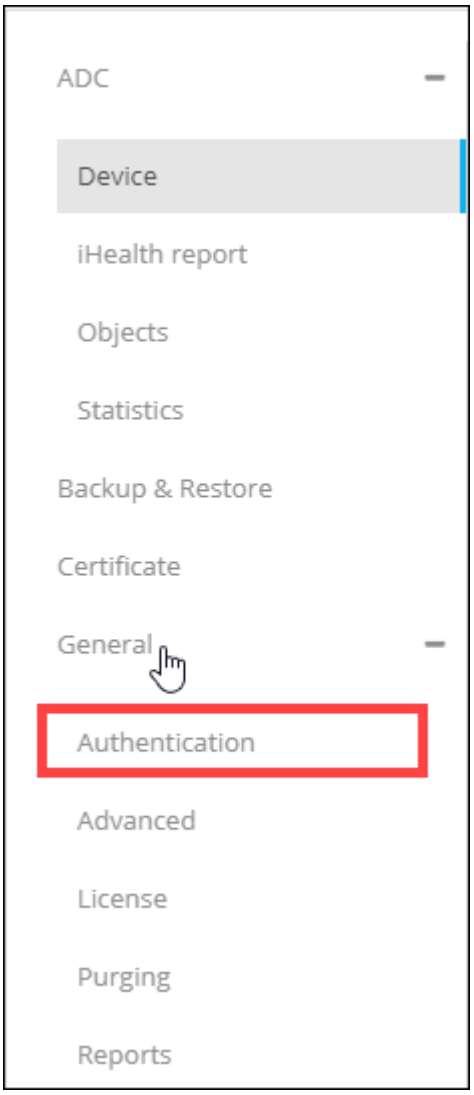
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Settings.



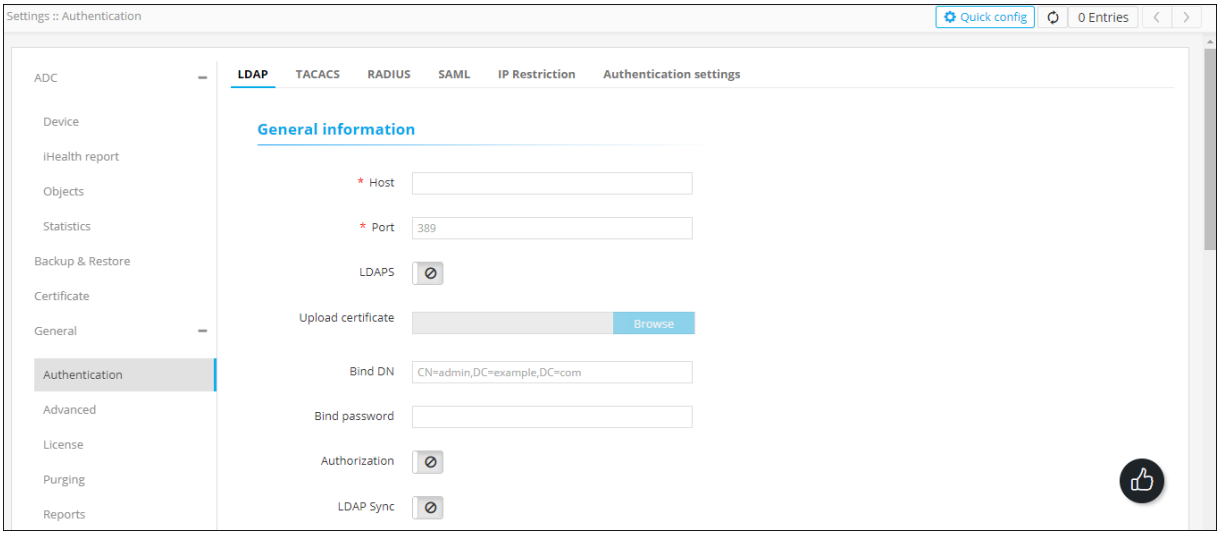
3. On the Settings page, from the navigation pane on the left, click General.



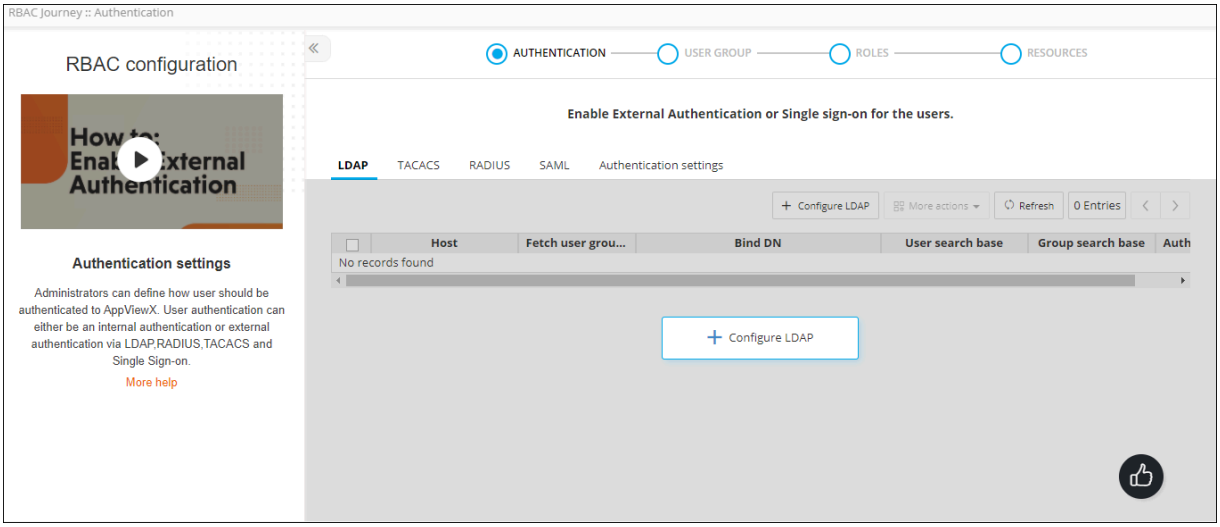
4. Under General settings, click Authentication.



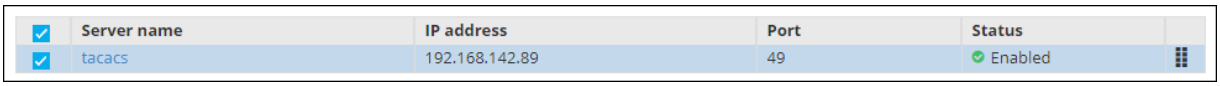
5. The Settings :: Authentication page is displayed, with the LDAP tab open by default.



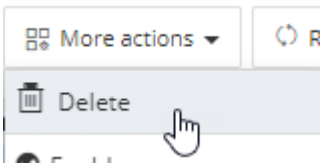
6. From the top-right corner of the screen, click Quick Config.
7. The RBAC Journey :: Authentication page is displayed.



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



10. From the More Actions drop-down menu, click Delete.

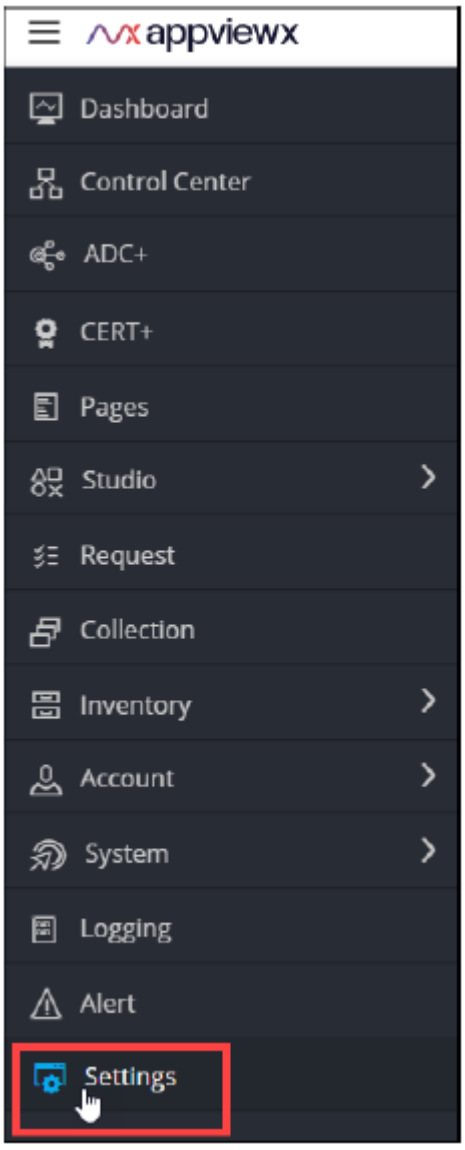


11. In the Confirmation message dialog box, click Proceed. The selected configuration is deleted.

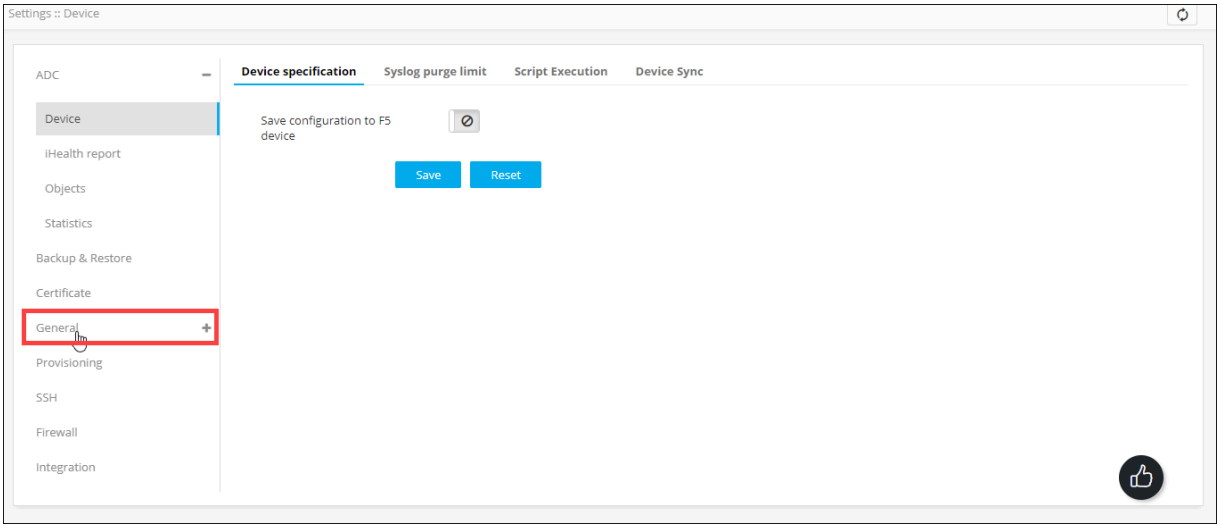
Disabling a TACACS Configuration

To disable a TACACS configuration:

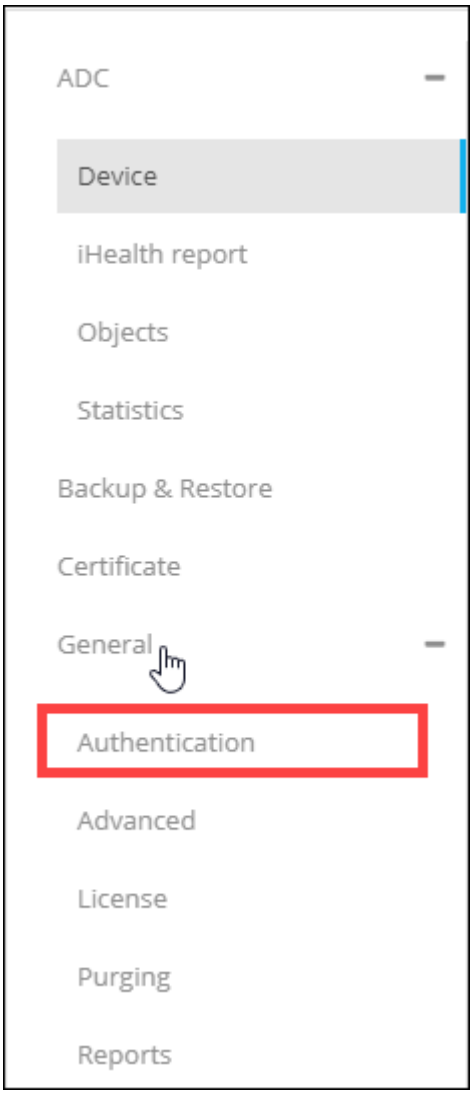
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Settings.



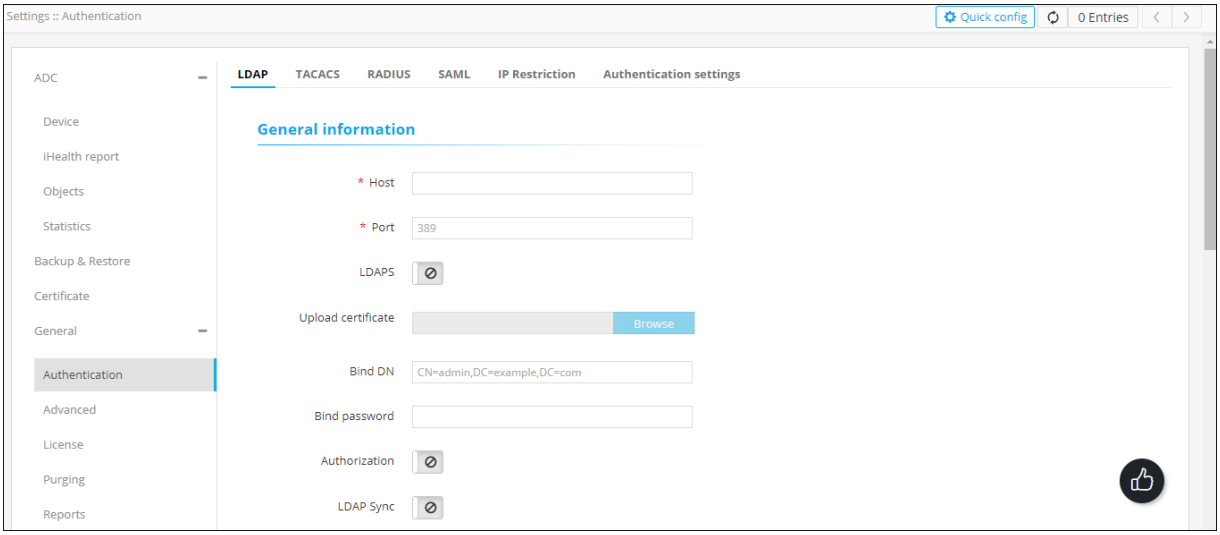
3. On the Settings page, from the navigation pane on the left, click General.



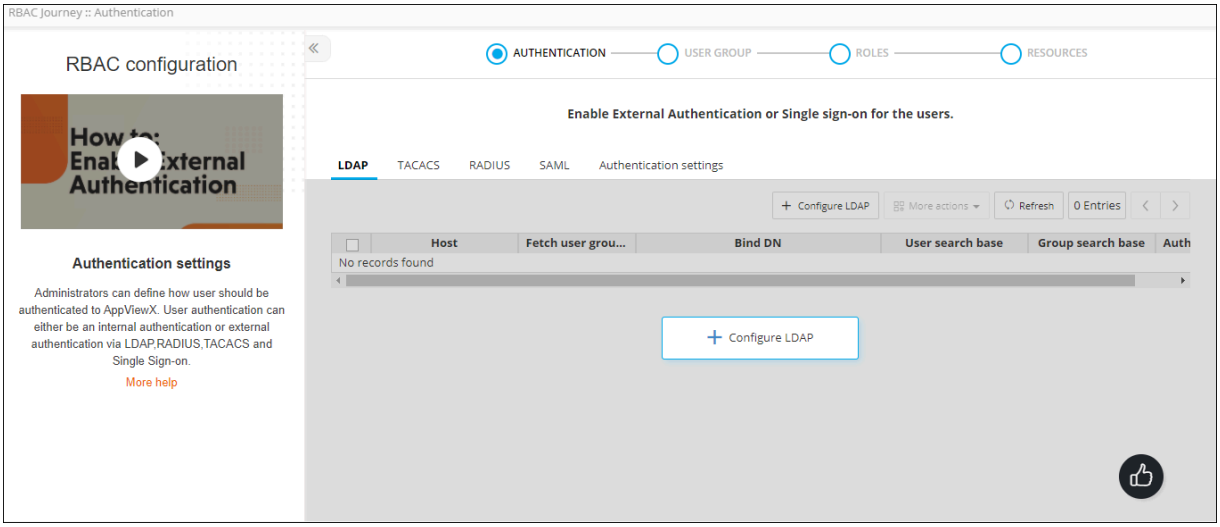
4. Under General settings, click Authentication.



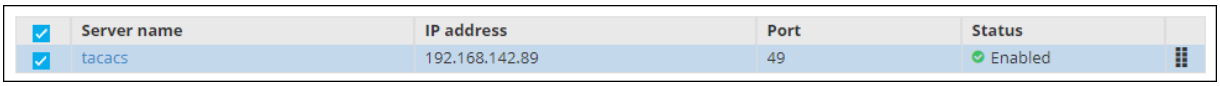
5. The Settings :: Authentication page is displayed, with the LDAP tab open by default.

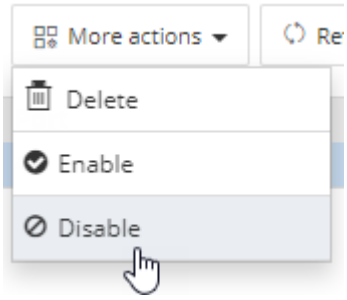


6. From the top-right corner of the screen, click Quick Config. The RBAC Journey :: Authentication page is displayed.



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



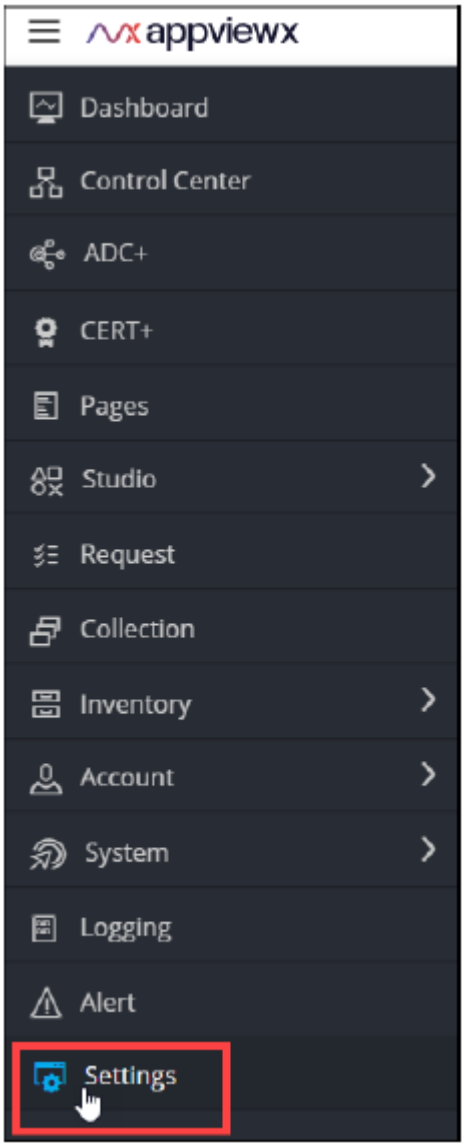


9. From the More Actions drop-down menu, click Disable.
10. In the Confirmation message dialog box, click Proceed. The selected configuration is disable.

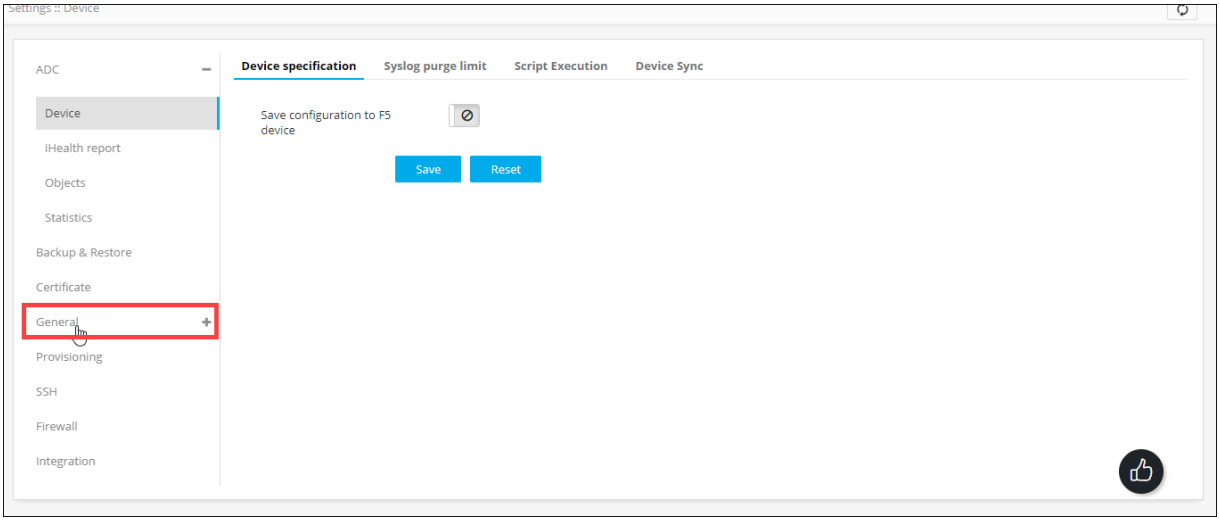
Enabling a TACACS Configuration

To enable a TACACS configuration:

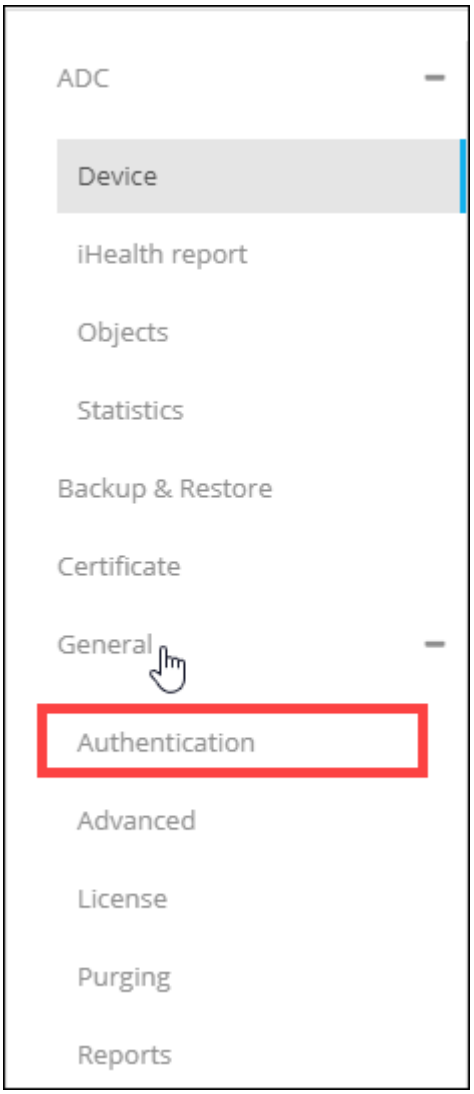
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Settings.



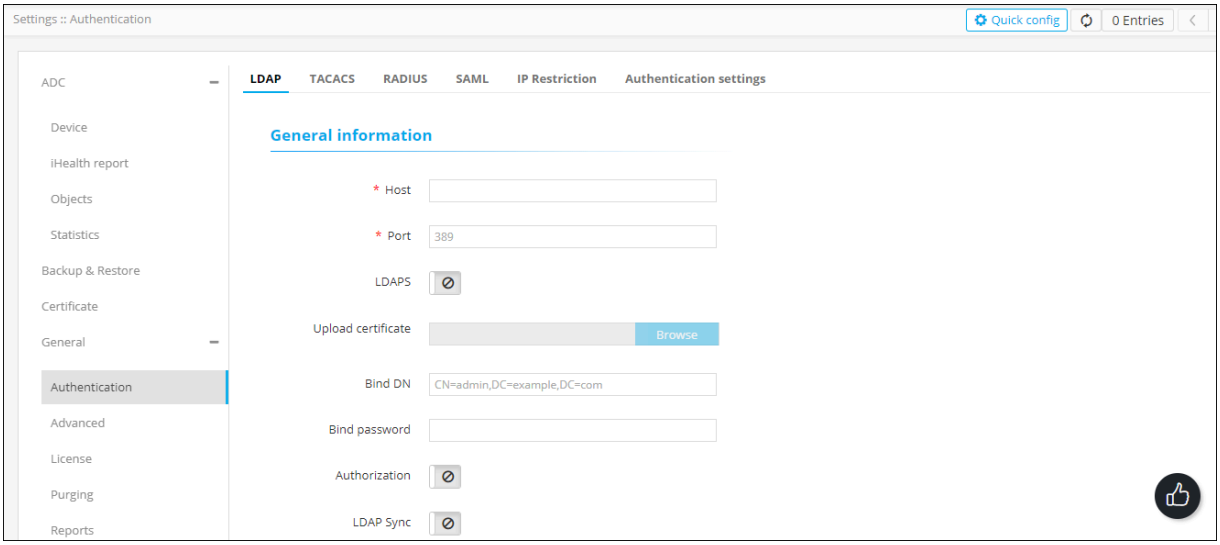
3. On the Settings page, from the navigation pane on the left, click General.



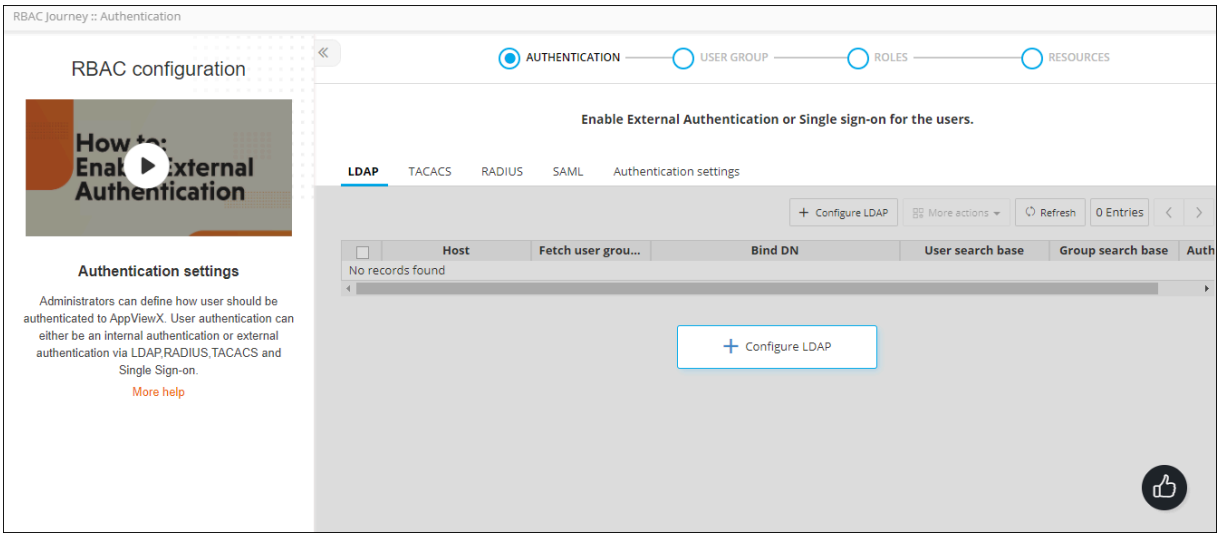
4. Under General settings, click Authentication.



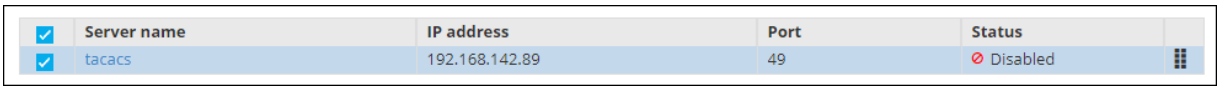
5. The Settings :: Authentication page is displayed, with the LDAP tab open by default.

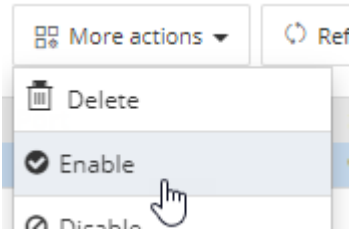


6. From the top-right corner of the screen, click Quick Config. The RBAC Journey :: Authentication page is displayed.



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



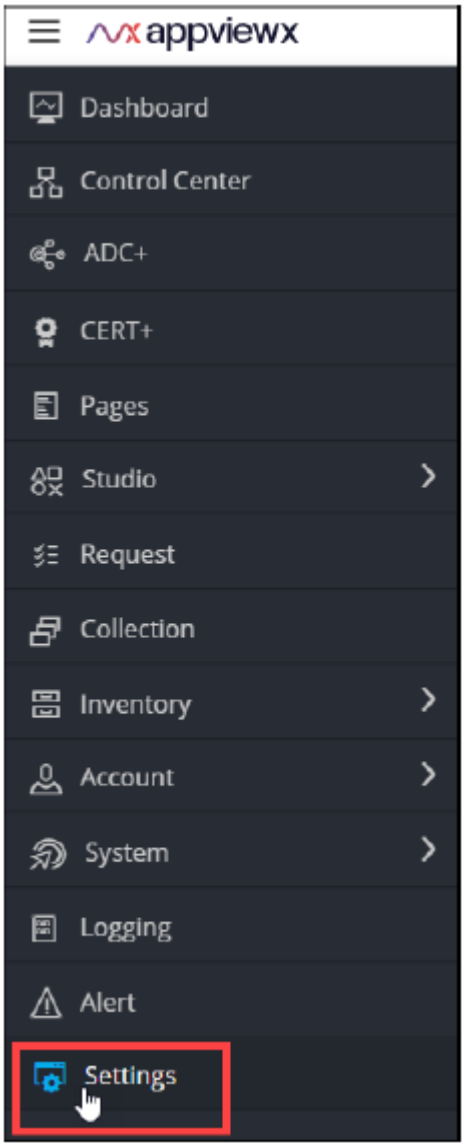
9. From the More Actions drop-down menu, click Enable. 

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

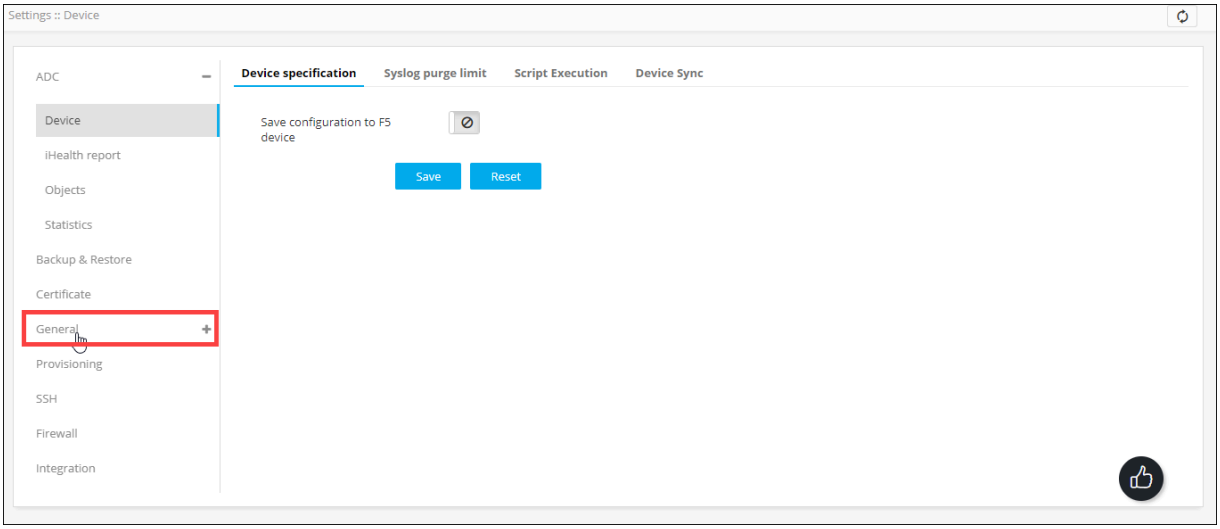
Configuring Role-Based Access Control for RADIUS

To configure RBAC for RADIUS authentication:

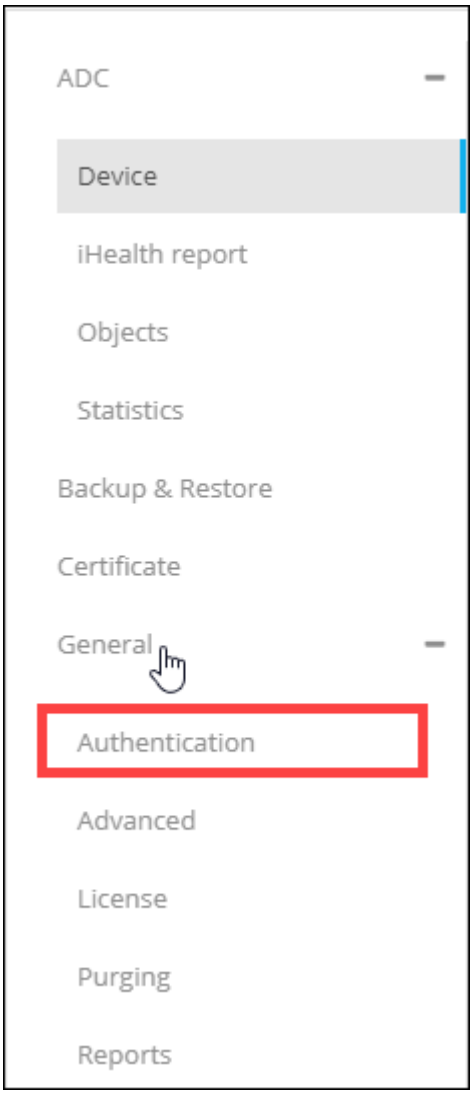
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Settings.



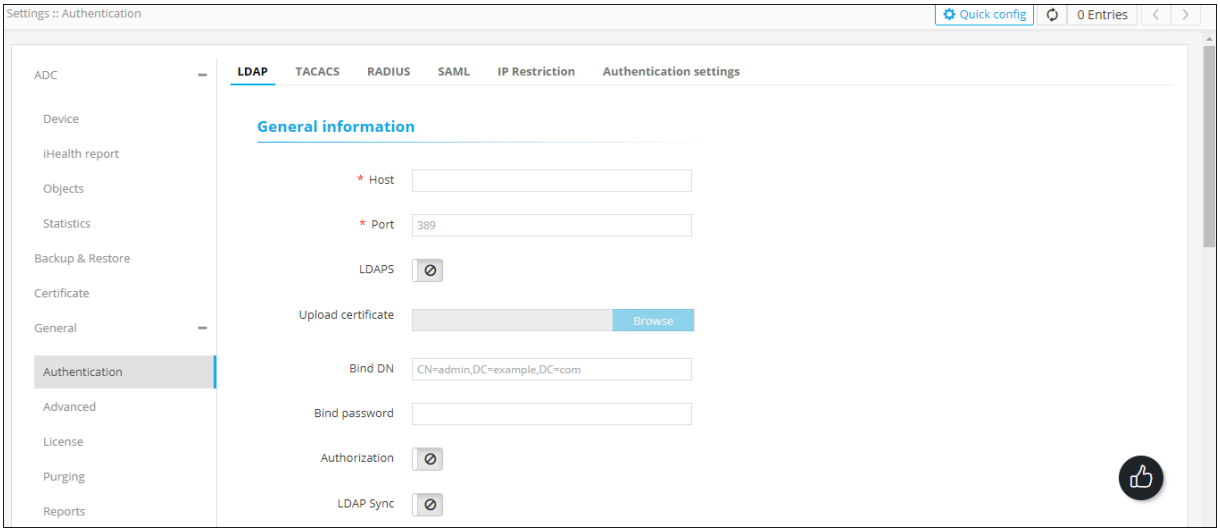
3. On the Settings page, from the navigation pane on the left, click General.



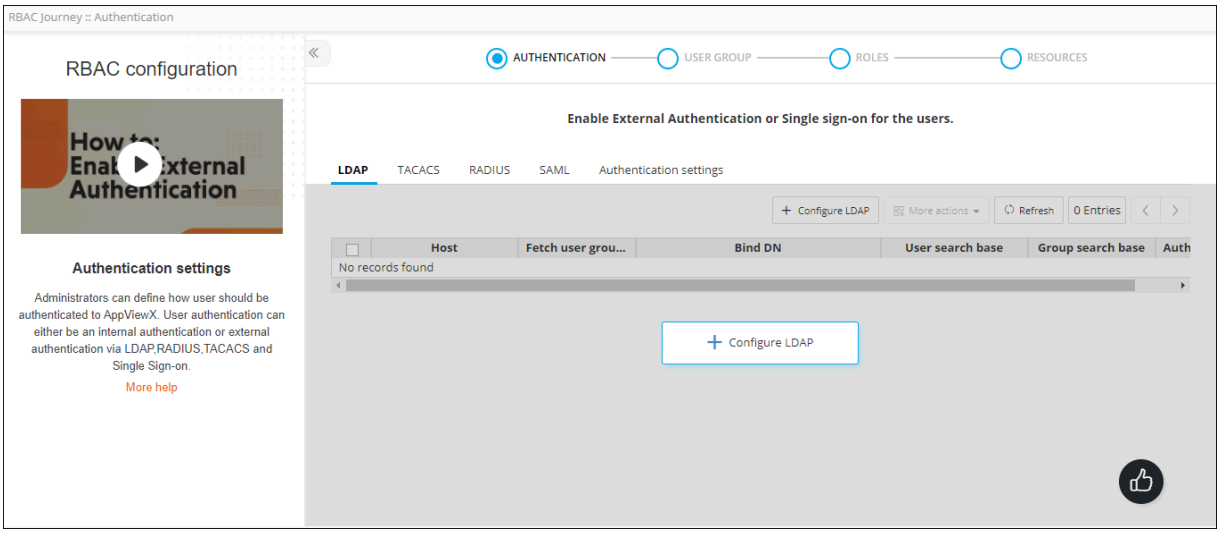
4. Under General settings, click Authentication.



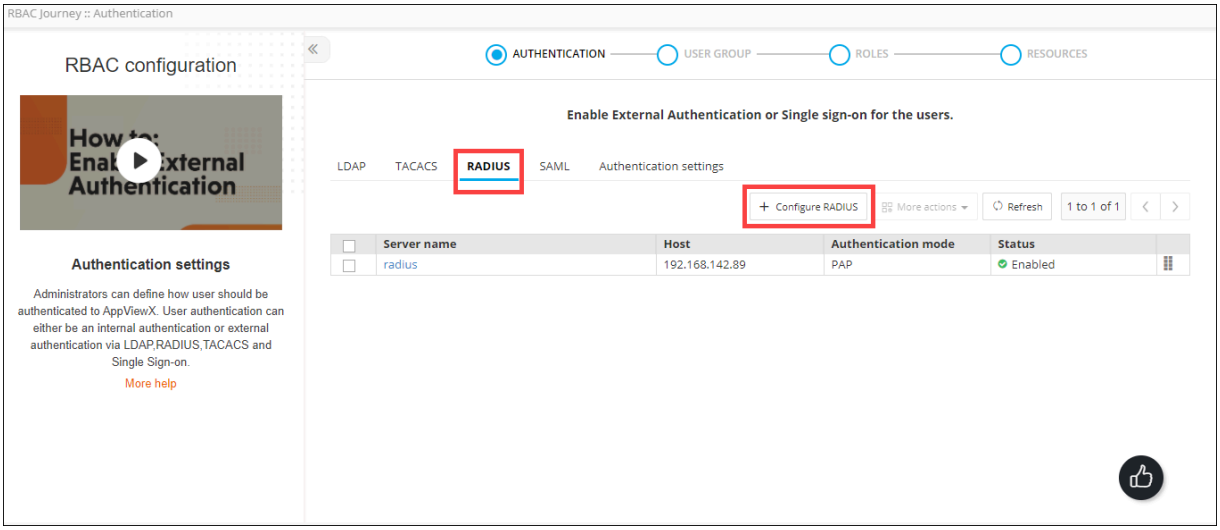
5. The Settings :: Authentication page is displayed, with the LDAP tab open by default.



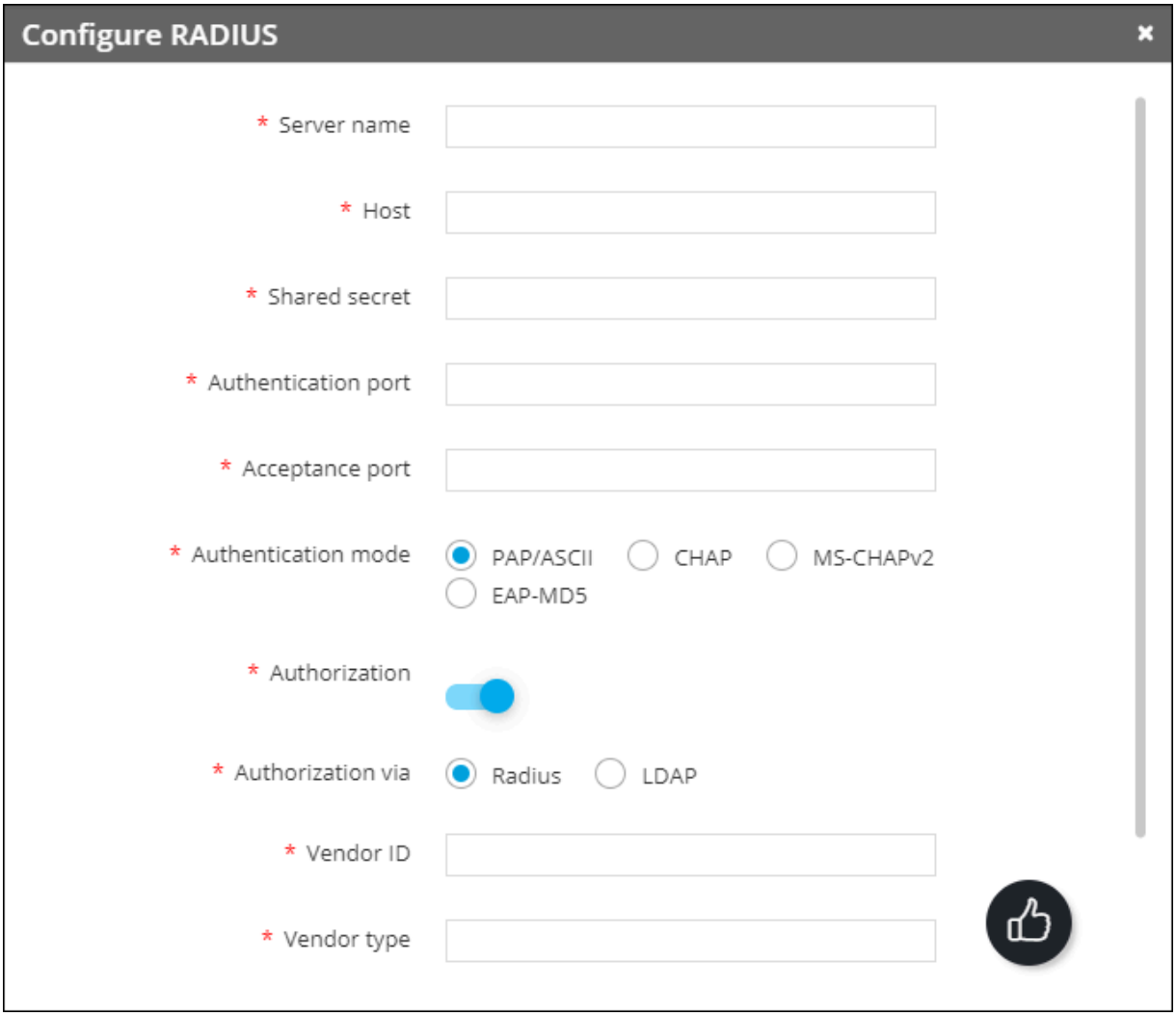
6. From the top-right corner of the screen, click Quick Config. The RBAC Journey:: Authentication page is displayed.



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



8. The Configure RADIUS action is displayed.

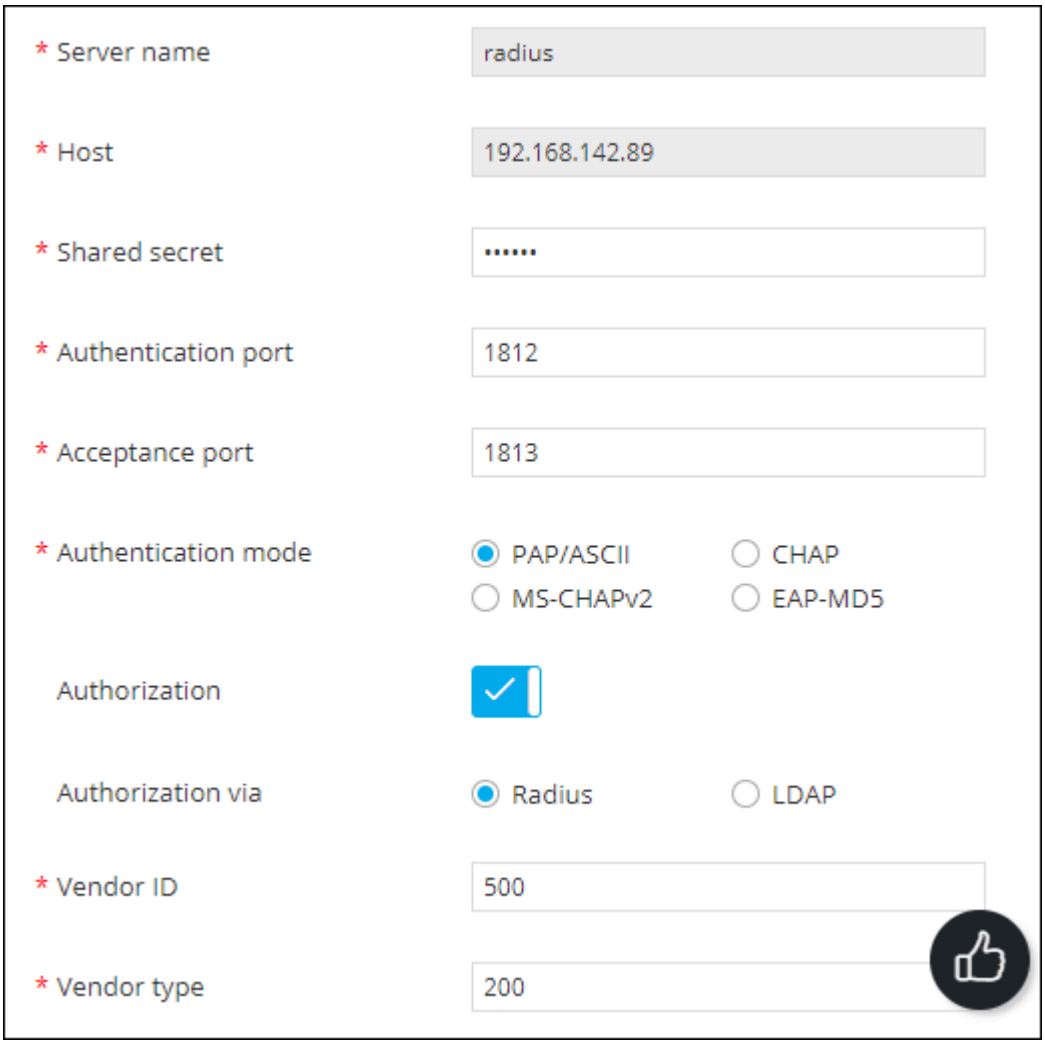


9. Enter the following details (sample values are shown in the image below the table):

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 **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.

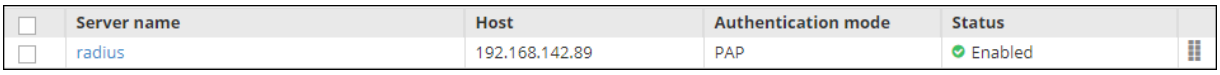
Field	Description
	To enable authorization along with authentication, select this check box. **Note:** If Authorization is not enabled, AppViewX will only carry out RADIUS authentication for the given user.
Authorization via	This field is enabled only when Authorization  is enabled. Select from one of the following authorization modes: • RADIUS • LDAP
Vendor ID*	This field is enabled only when Authorization  is enabled and authorization is done via the RADIUS server. 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.
Vendor type*	This field is enabled only when Authorization  is enabled and authorization is done via the RADIUS server. Enter the vendor type.

Field	Description
	Note: AppViewX does not have a unique vendor type. We use a free vendor ID: 200. Ensure that this is configured as part of the RADIUS server settings.
LDAP*	This field is enabled only when Authorization is enabled and authorization is done via the LDAP server. From the drop-down menu, select the LDAP server to be used for the authorization.



***Mandatory**

10. 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:



Server name	Host	Authentication mode	Status
radius	192.168.142.89	PAP	Enabled

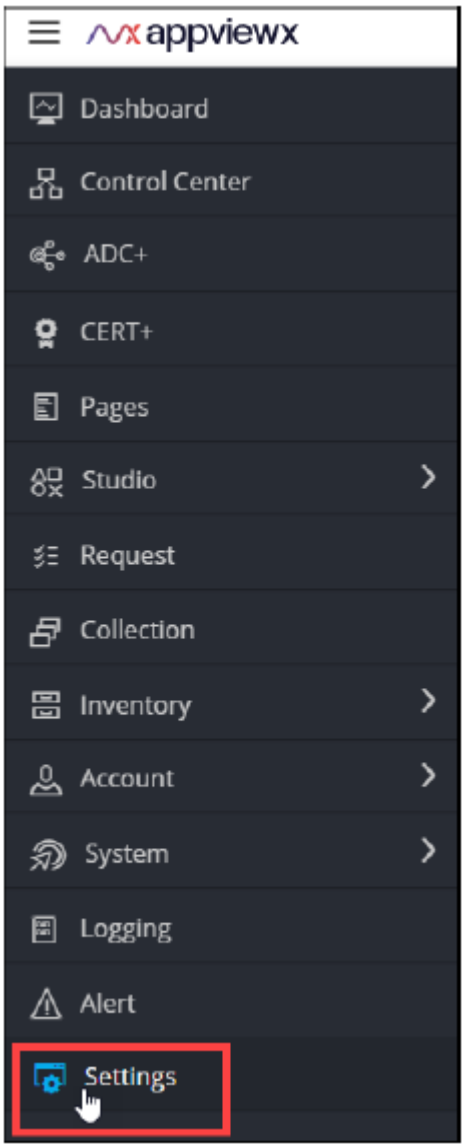
Note: In the case of multiple RADIUS servers, to define/update the order in which the servers will be authenticated, drag and drop the entries in this table.

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

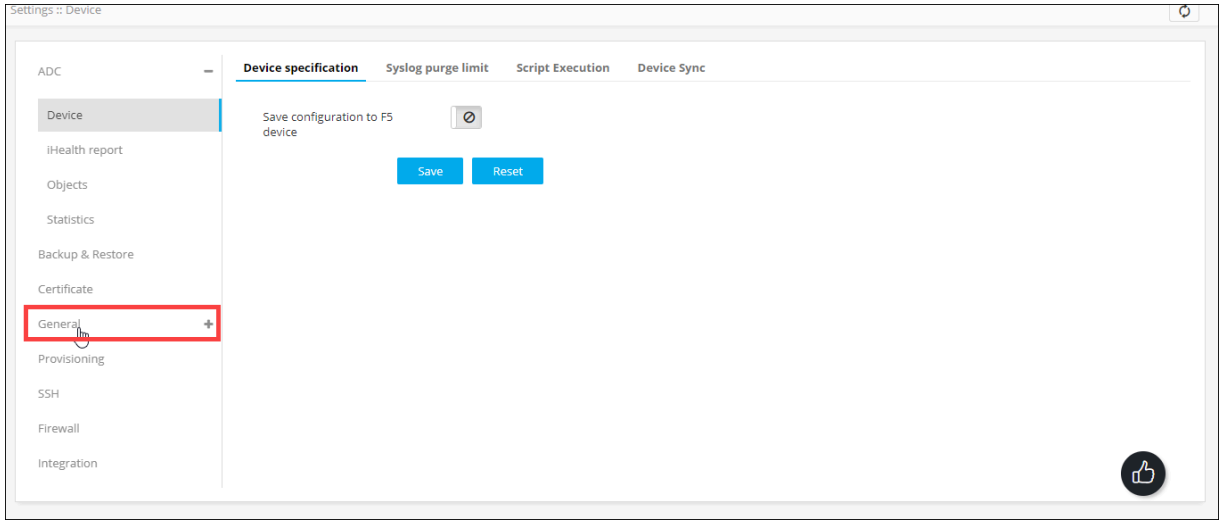
Deleting a RADIUS Configuration

To delete a RADIUS configuration:

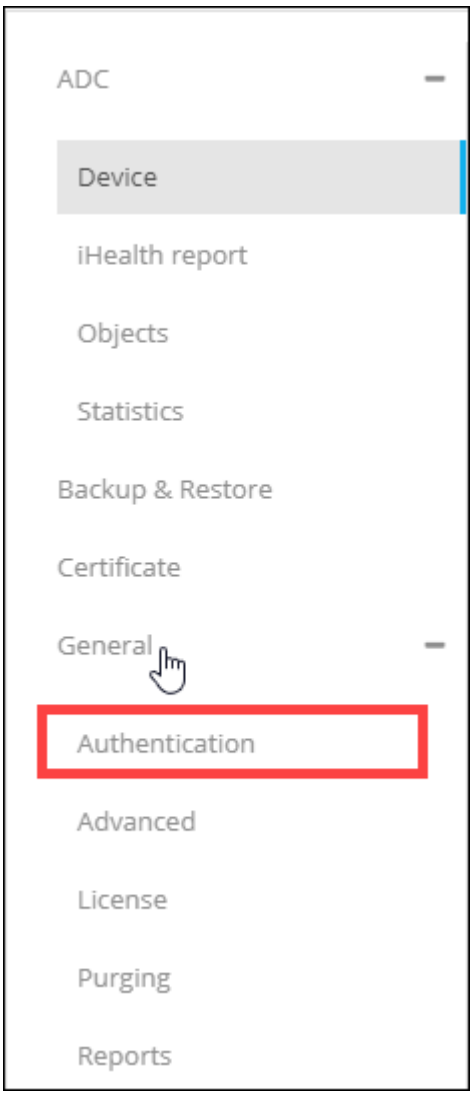
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Settings.



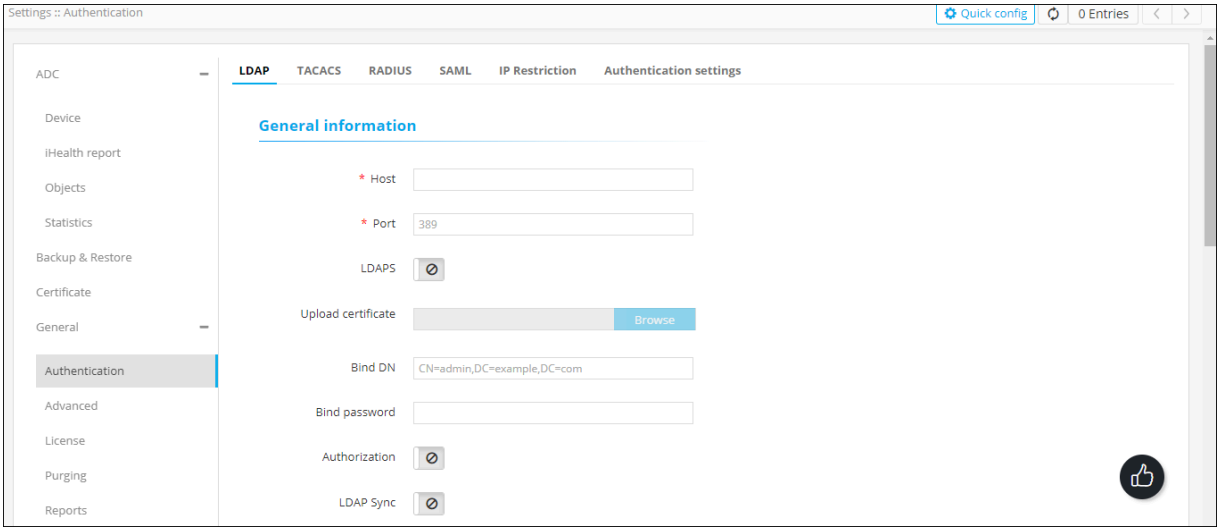
3. On the Settings page, from the navigation pane on the left, click General.



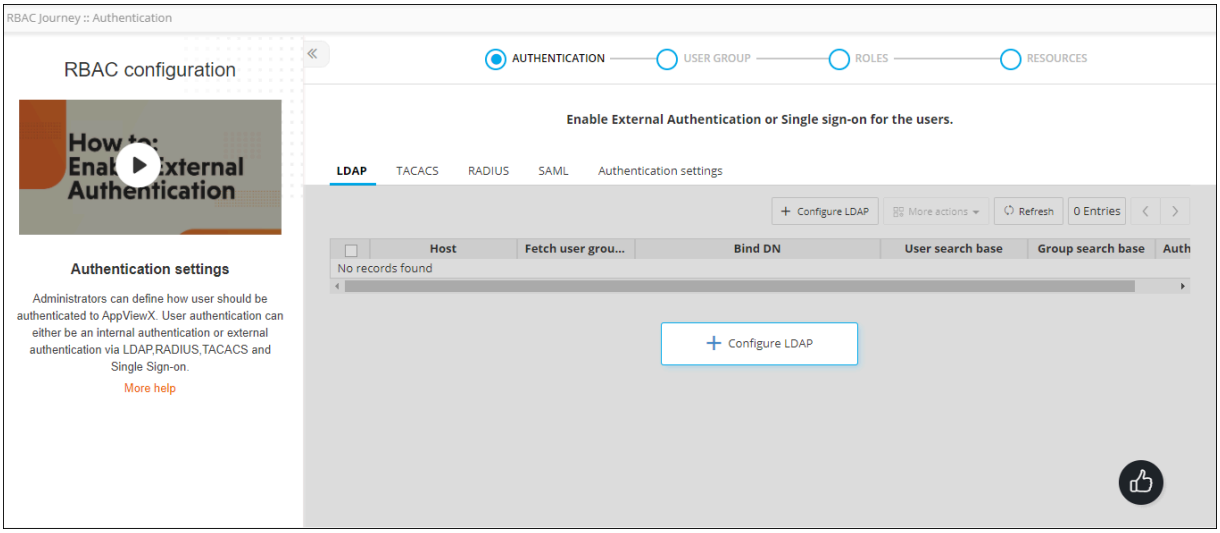
4. Under General settings, click Authentication.



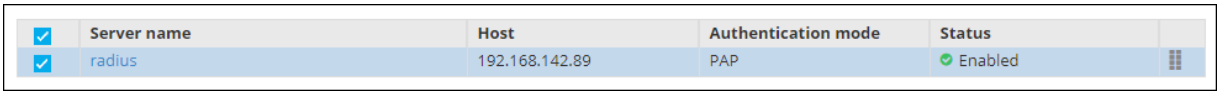
5. The Settings :: Authentication page is displayed, with the LDAP tab open by default.



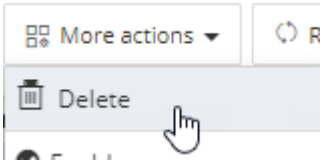
6. From the top-right corner of the screen, click Quick Config. The RBAC Journey :: Authentication page is displayed.



7. On the RBAC Journey :: Authentication page, click the RADIUS tab.
8. From the table of RADIUS configurations, for the configuration you want to delete, select the check box corresponding to that entry.



9. From the More Actions drop-down menu, click Delete.

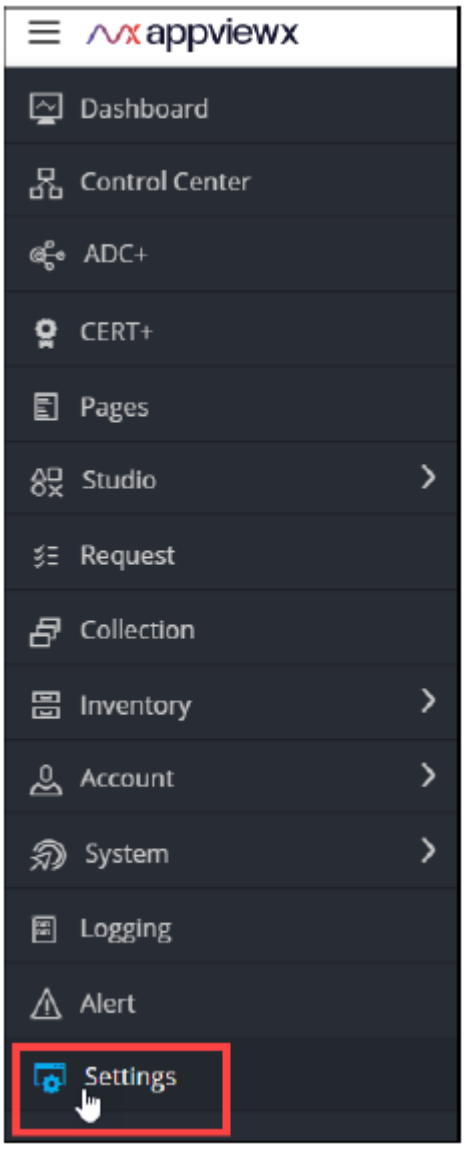


10. In the Confirmation message dialog box, click Proceed. The selected configuration is disabled.

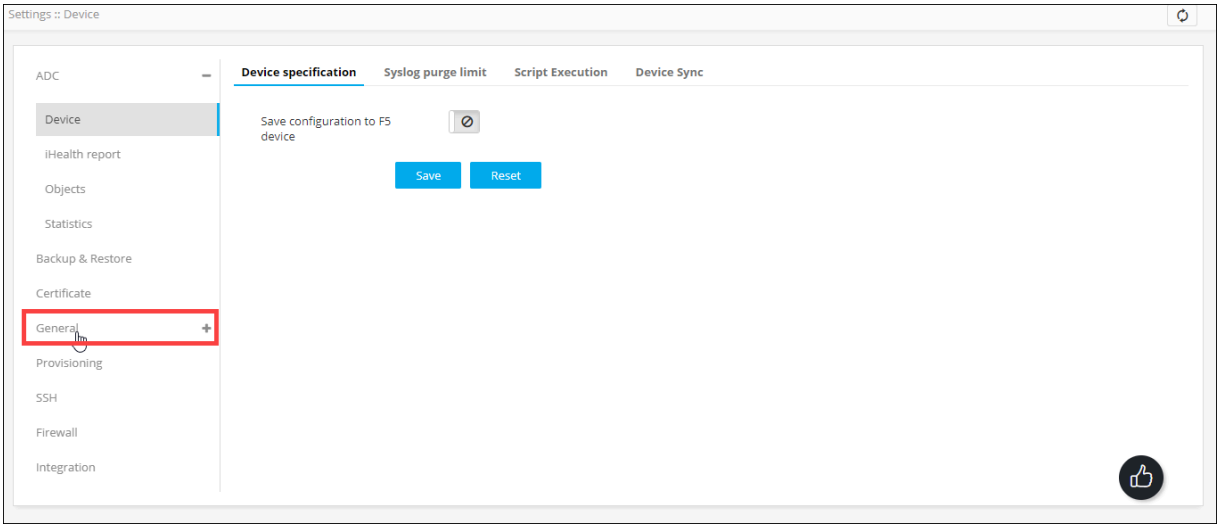
Disabling a RADIUS Configuration

To disable a RADIUS configuration:

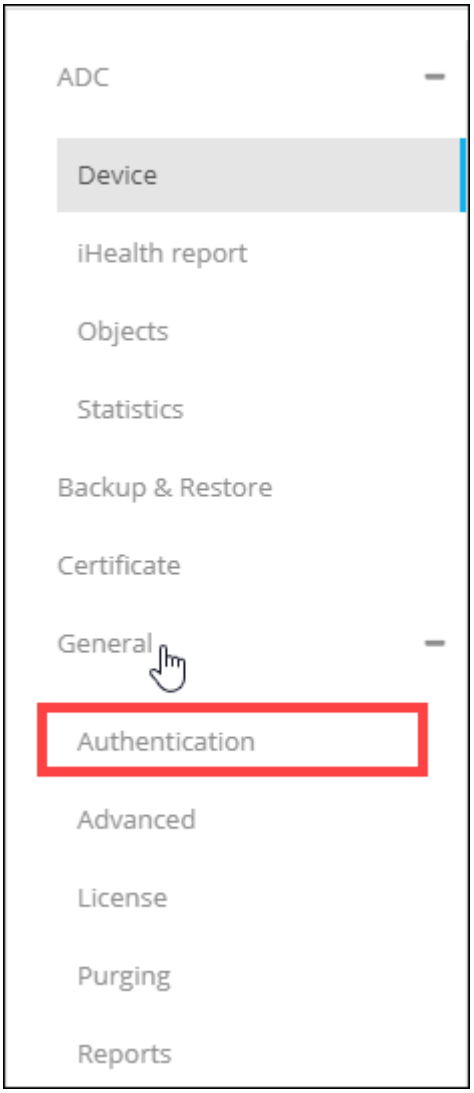
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Settings.



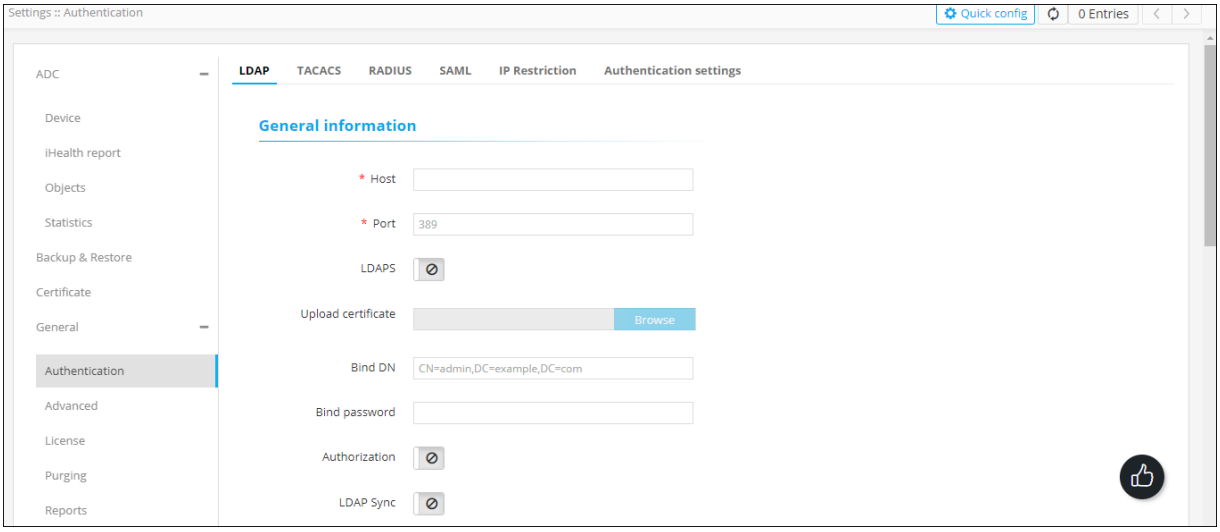
3. On the Settings page, from the navigation pane on the left, click General.



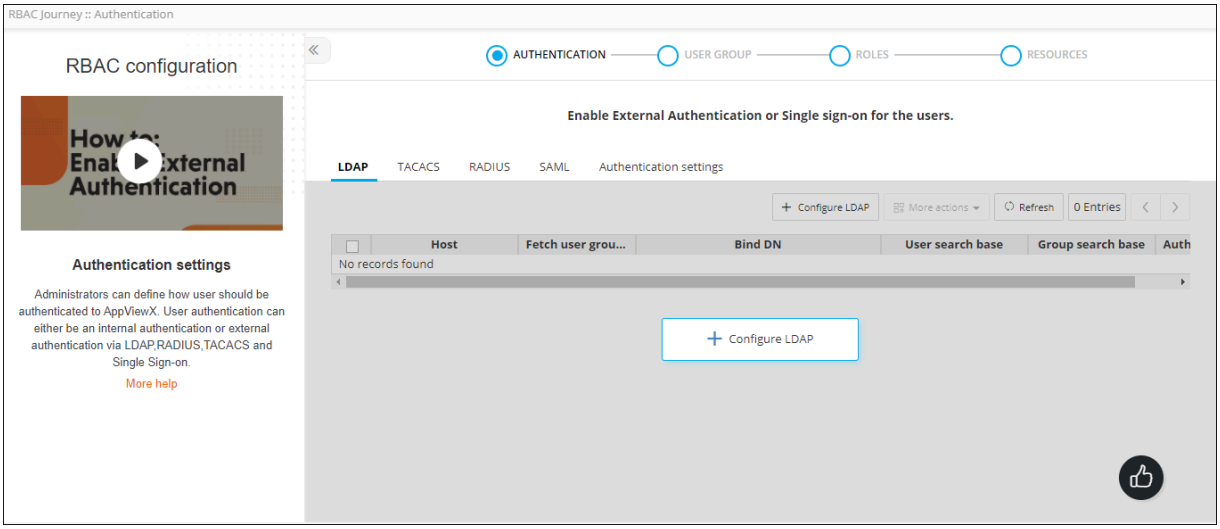
4. Under General settings, click Authentication.



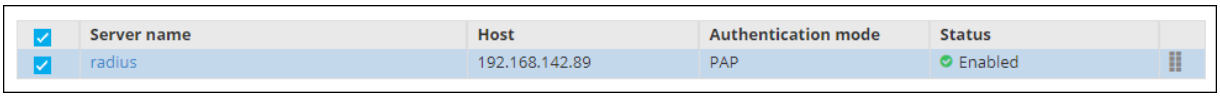
5. The Settings :: Authentication page is displayed, with the LDAP tab open by default.



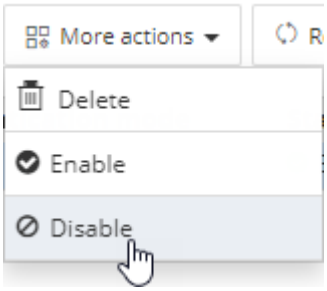
6. From the top-right corner of the screen, click Quick Config. The RBAC Journey :: Authentication page is displayed.



7. On the RBAC Journey :: Authentication page, click the RADIUS tab.
8. From the table of RADIUS configurations, for the configuration you want to disable, select the check box corresponding to that entry.



9. From the More Actions drop-down menu, click Disable.

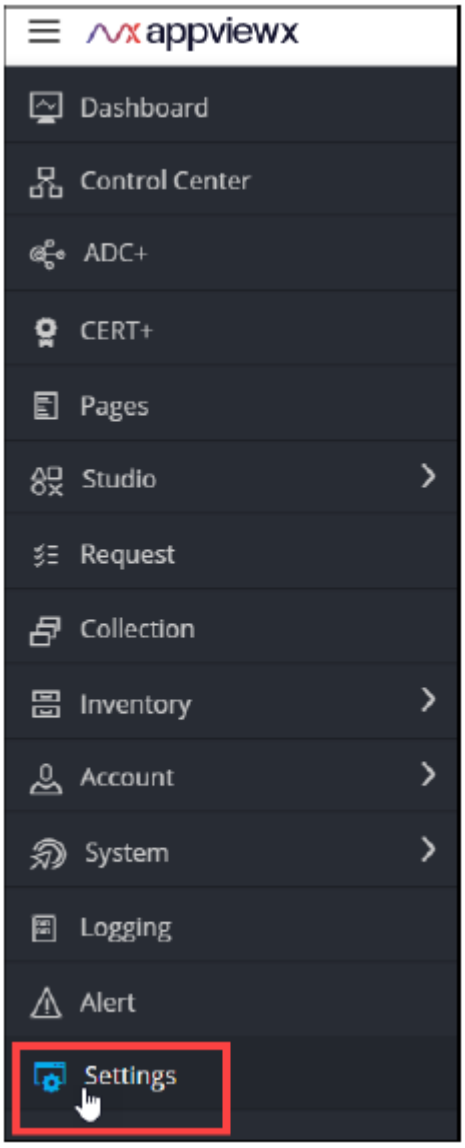


10. In the Confirmation message dialog box, click Proceed. The selected configuration is disabled.

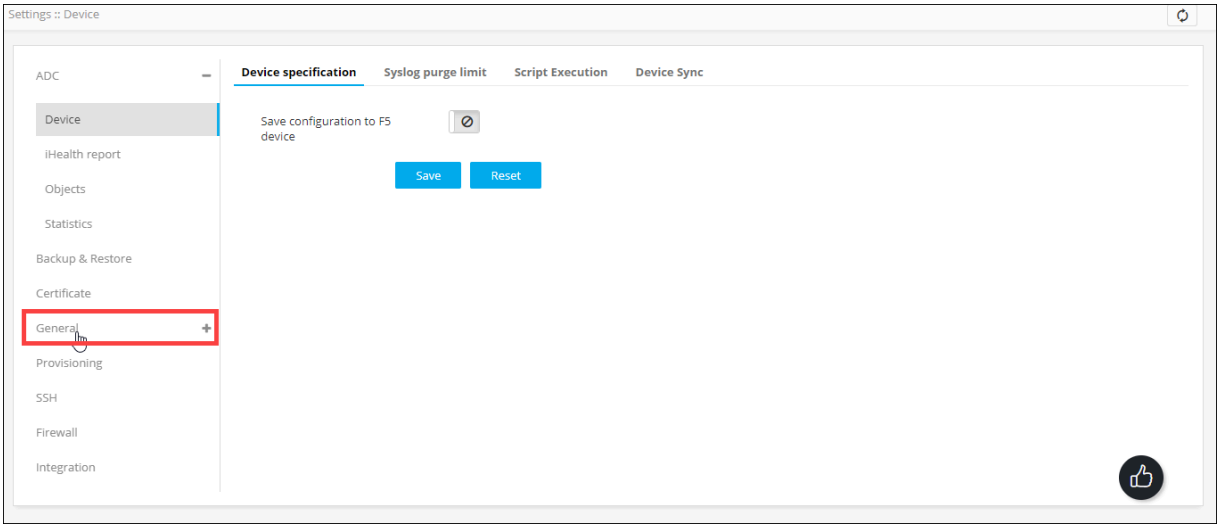
Enabling a RADIUS Configuration

To enable a RADIUS configuration:

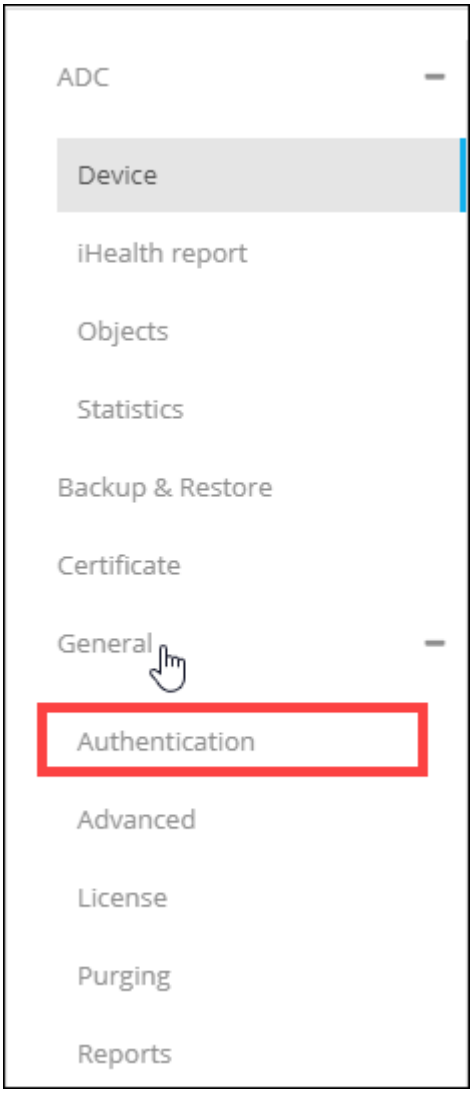
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Settings.



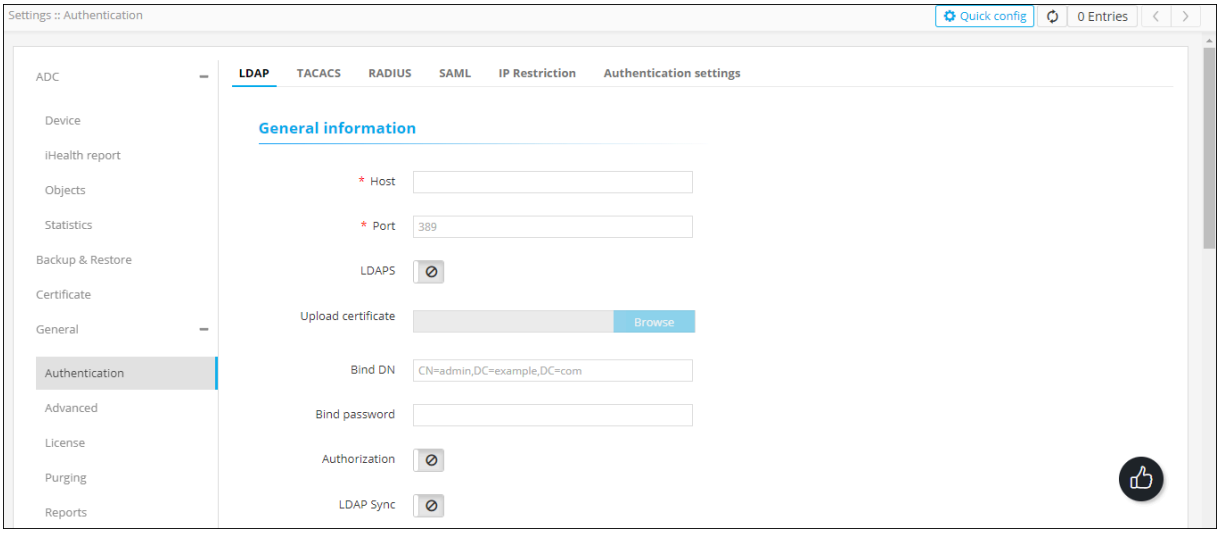
3. On the Settings page, from the navigation pane on the left, click General.



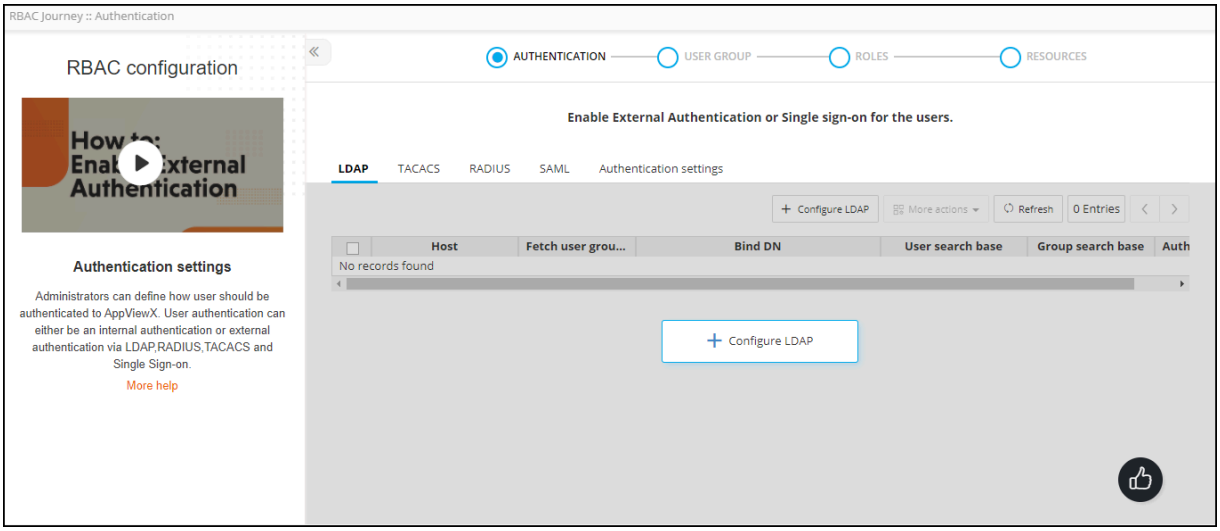
4. Under General settings, click Authentication.



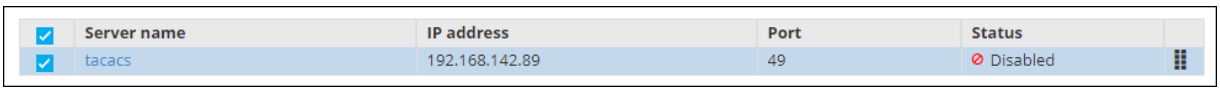
5. The Settings :: Authentication page is displayed, with the LDAP tab open by default.

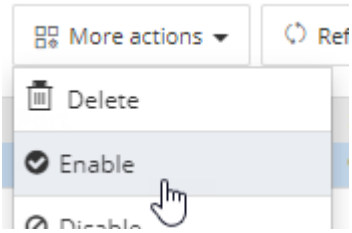


6. From the top-right corner of the screen, click Quick Config. The RBAC Journey :: Authentication page is displayed.



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



9. From the More Actions drop-down menu, click Enable. 

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

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.

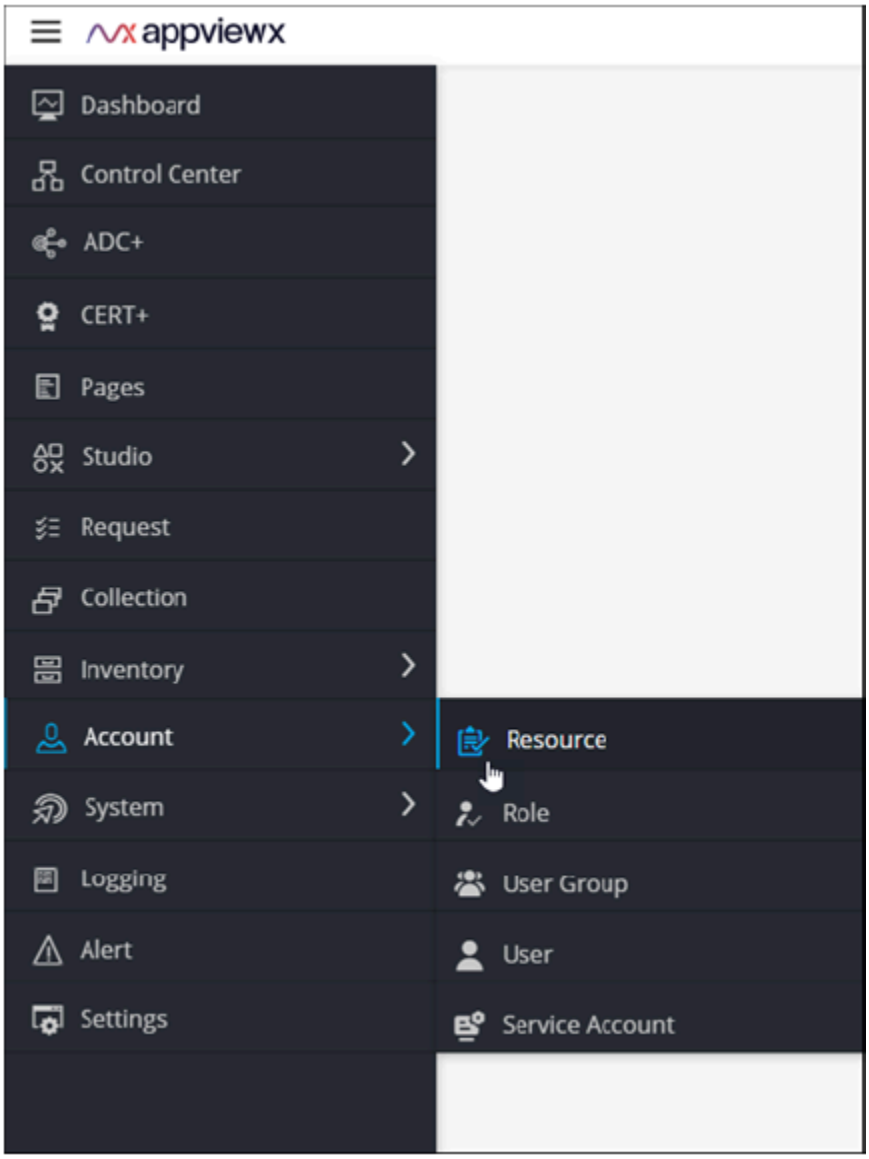
- Create an RBAC Rule to Tag ADC Objects Using a Query
- Configuring a Variable as a Filter Condition Value based on Patterns
- Configuring the Resource Name
- Configuring the Certificate Group Name

- Configuring the Resource Name Based on Patterns
- Create an RBAC Rule to Tag ADC Objects/Certificates using a Script
- 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

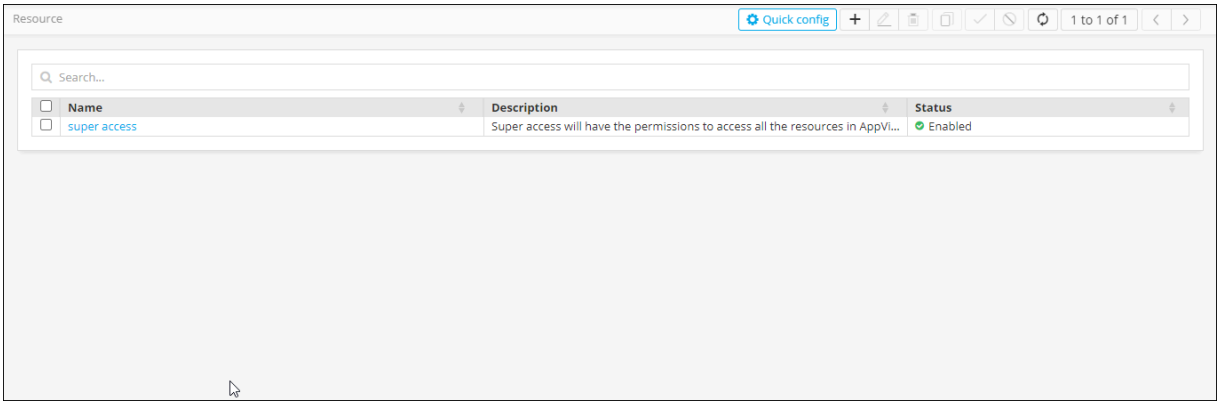
Create an RBAC Rule to Tag ADC Objects Using a Query

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

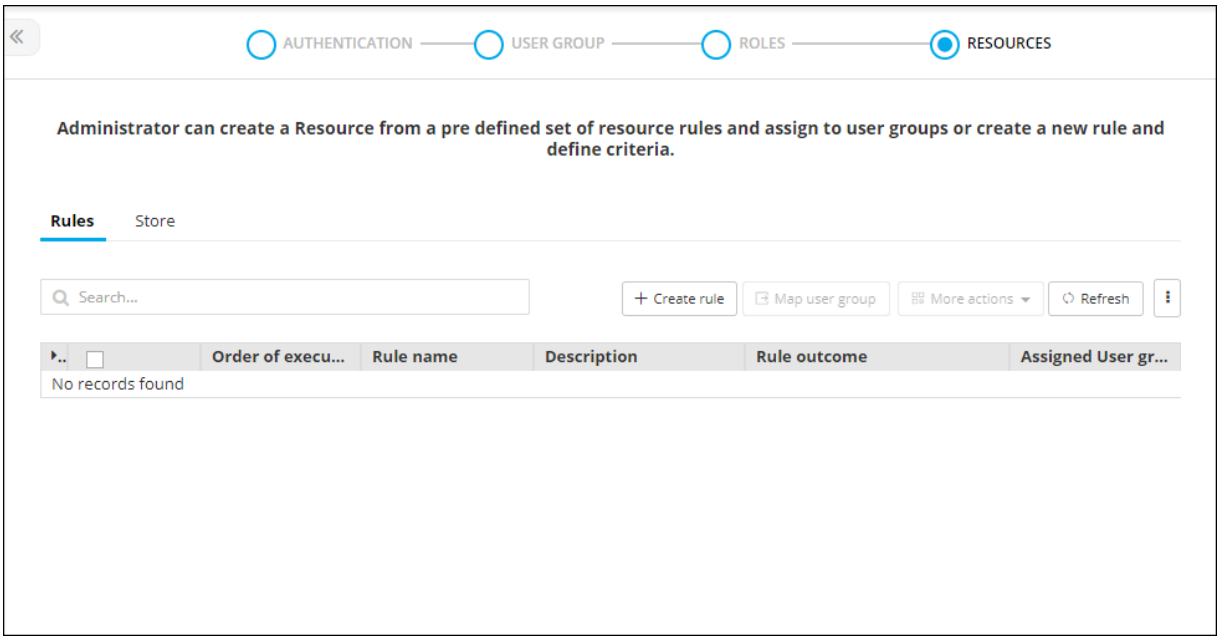
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Account > Resource.



3. The Resource page is displayed.

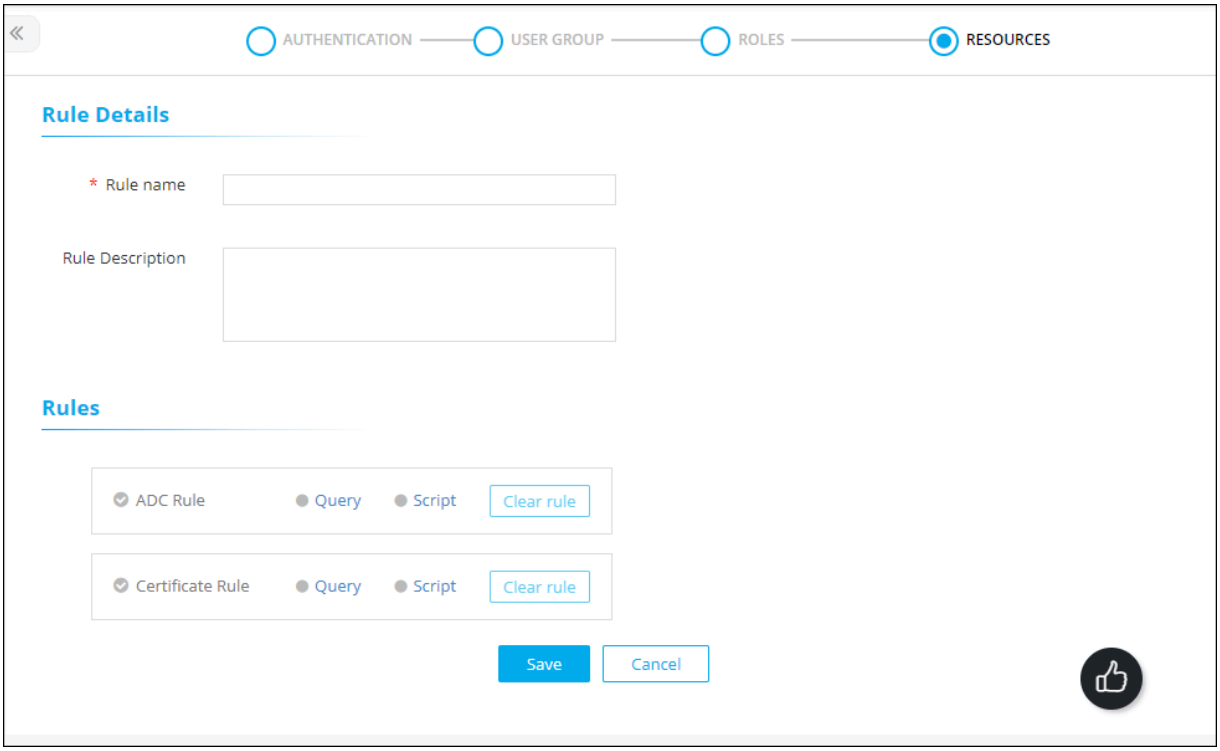


4. From the top-right corner of the screen, click Quick Config. The RBAC Journey :: Authentication page is displayed.
5. Navigate to the Resource stage as part of the wizard flow to add roles into AppViewX, with the Rules tab displayed by default.



6. Click + Create rule .

7. The Rules :: Create screen is displayed.



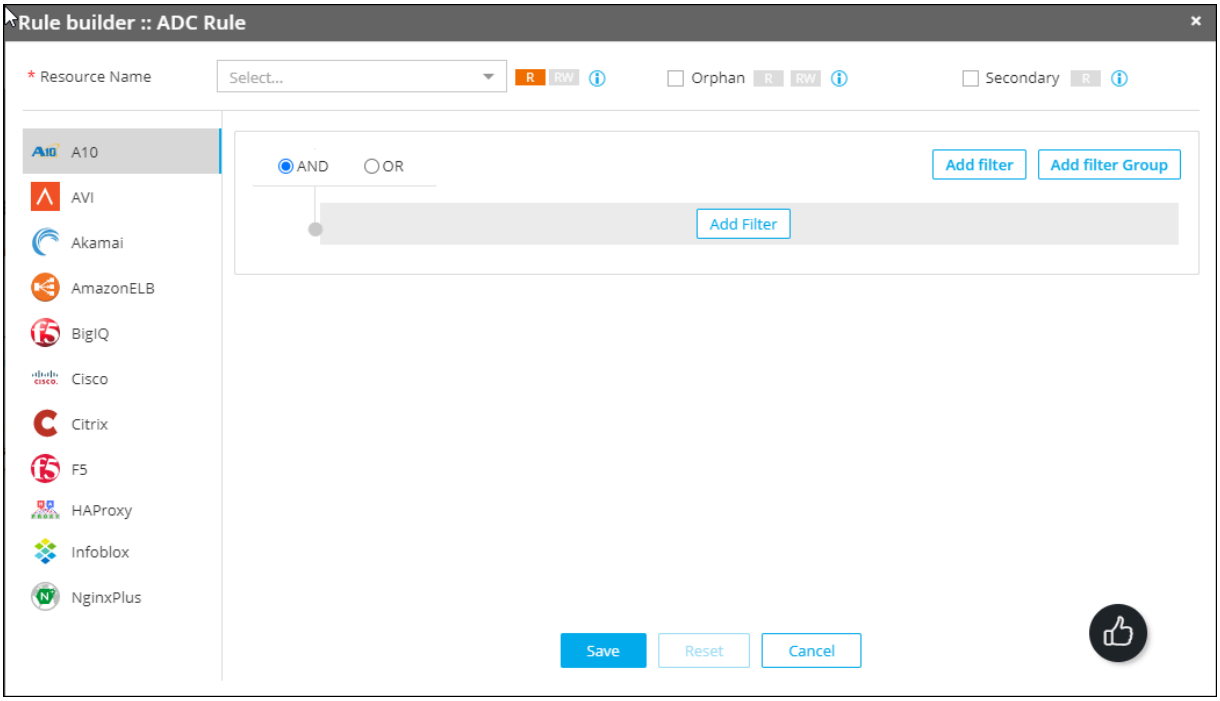
8. In the Rule Details section, enter the following details:

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

***Mandatory**

9. To configure a rule to dynamically tag ADC objects using Query, in the Rules section, for the ADCRule, click Query.

10. The Rule builder :: Rule action pane is displayed.



11. On the Rule builder :: ADC Rule action pane, click Add Filter.
12. 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.

Configuring the Certificate Group Name

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

1. Provide the certificate group name of an existing resource by choosing the certificate group name from the drop-down menu.
2. Provide a Static Name to the certificate group name. [When Rule matches the Resource Name would be created on Demand].
3. Provide a Pattern for the certificate group name. [Provide the variable pattern defined in the Query as the Resource Name].

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

Configuring the Resource Name Based on Patterns

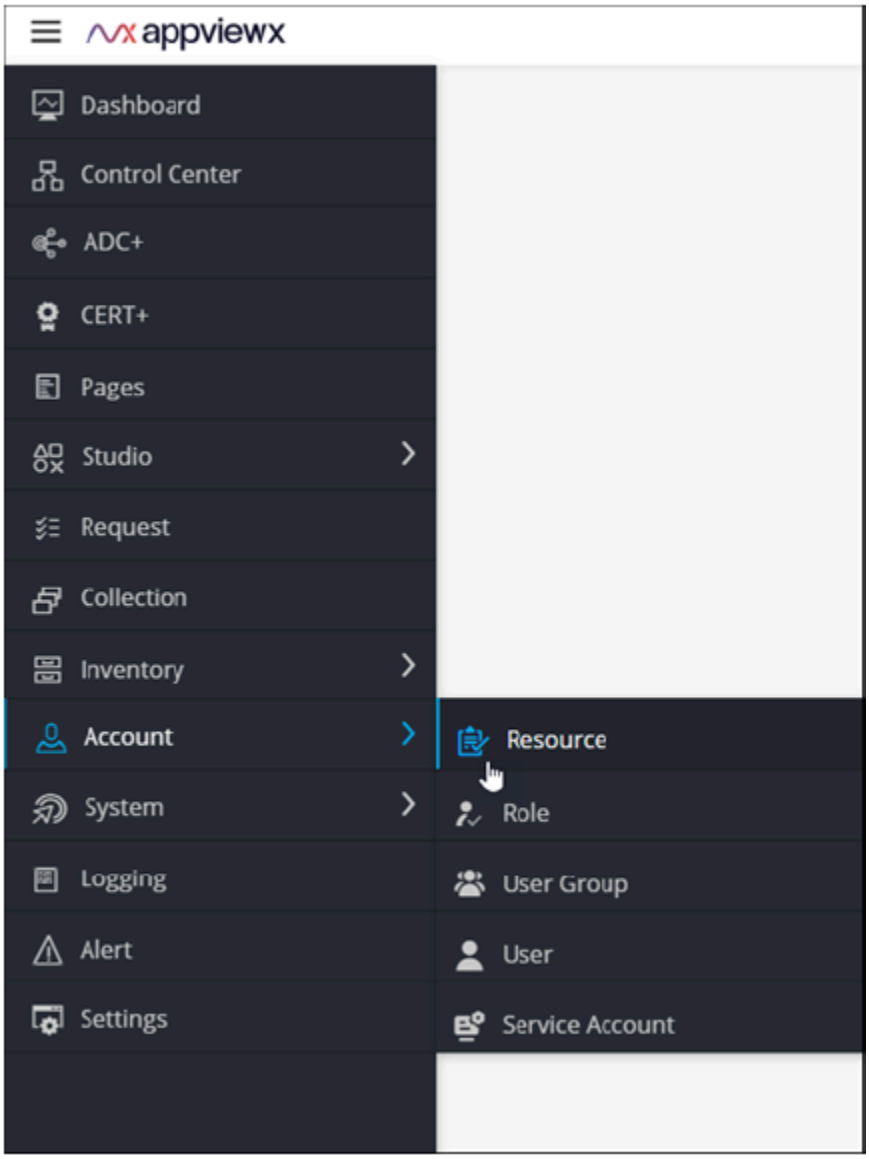
To create resources dynamically based on patterns, the resource name can be configured in the below ways:

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

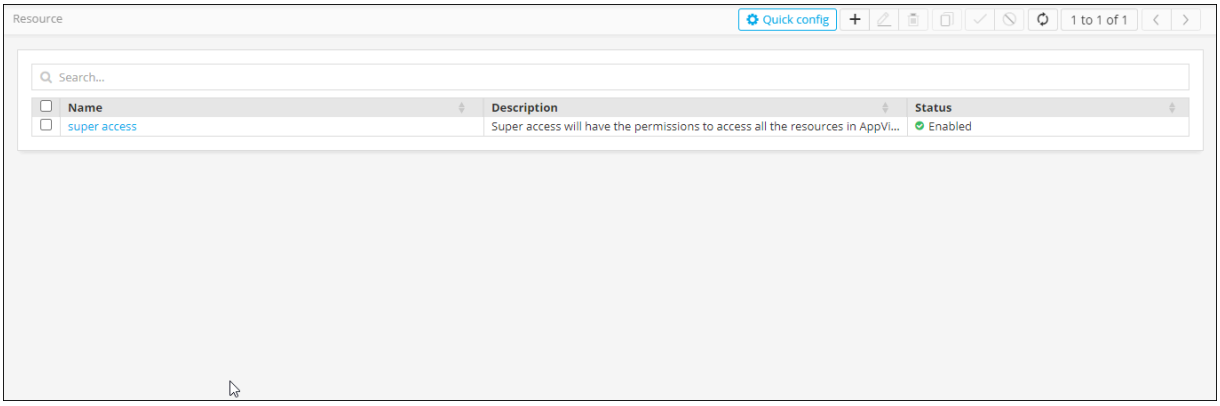
Create an RBAC Rule to Tag ADC Objects/Certificates using a Script

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

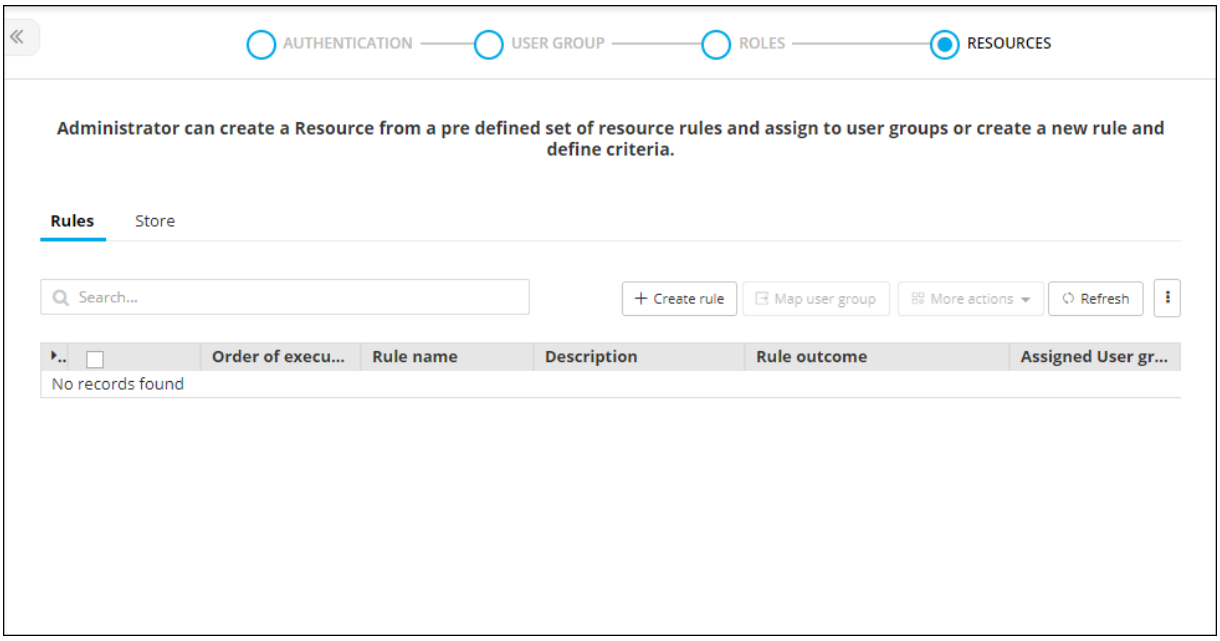
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Account > Resource.



3. The Resource page is displayed.

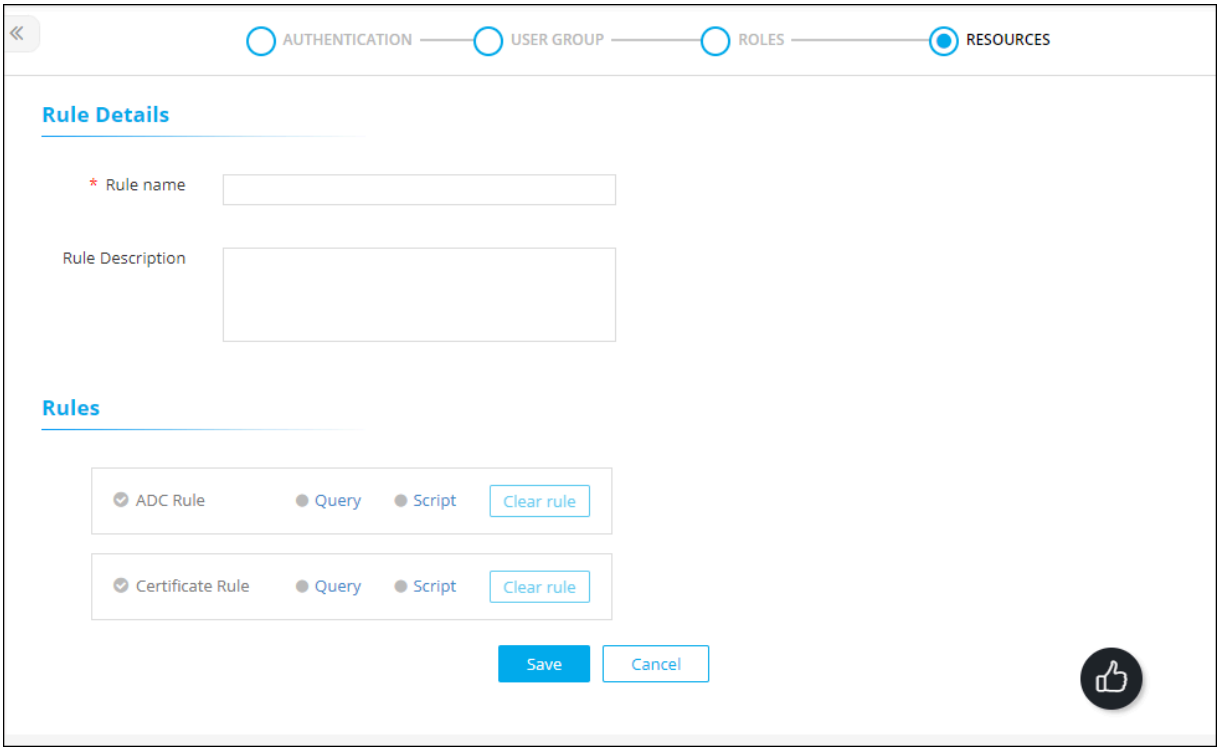


4. From the top-right corner of the screen, click Quick Config. The RBAC Journey :: Authentication page is displayed.
5. Navigate to the Resource stage as part of the wizard flow to add roles into AppViewX, with the Rules tab displayed by default.



6. Click + Create rule .

7. The Rules :: Create screen is displayed.



8. 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

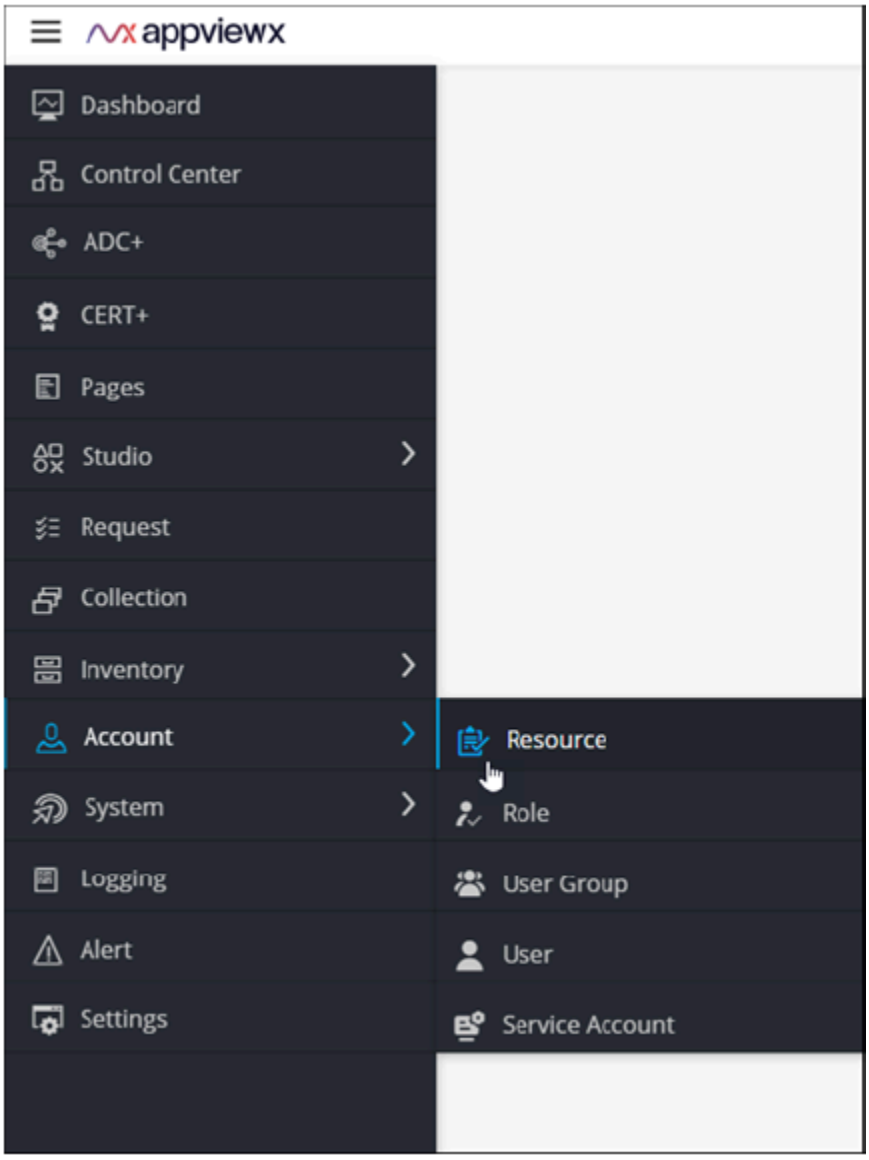
***:Mandatory**

9. To configure a rule to dynamically tag ADC objects/certificates using Script, in the Rules section, for the ADC Rule/Certificate Rule, click Script.
10. 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.
11. Click Save.
12. Saved rules will be displayed in the Rules tab.
13. 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.
14. Enable the rule by clicking on the respective status icon for the rule to be actively running.

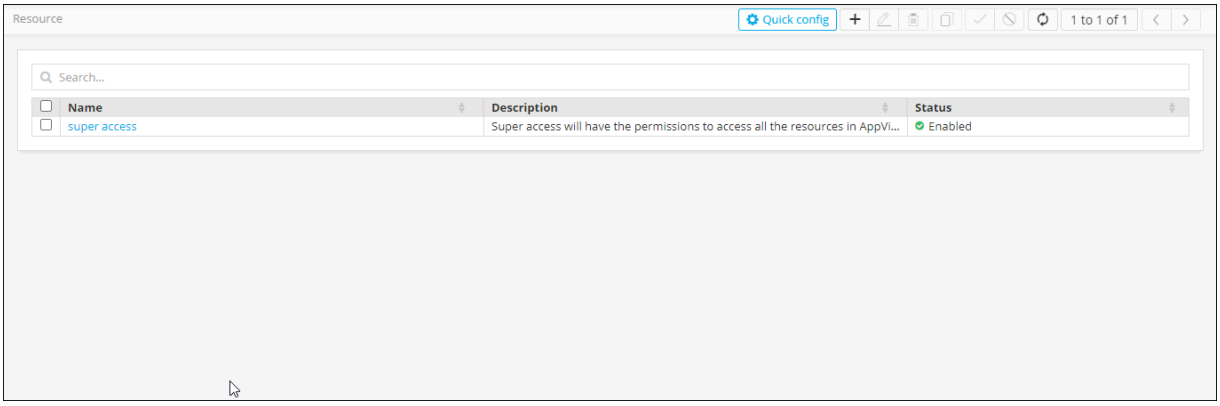
Clone a Rule

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.



3. The Resource page is displayed.

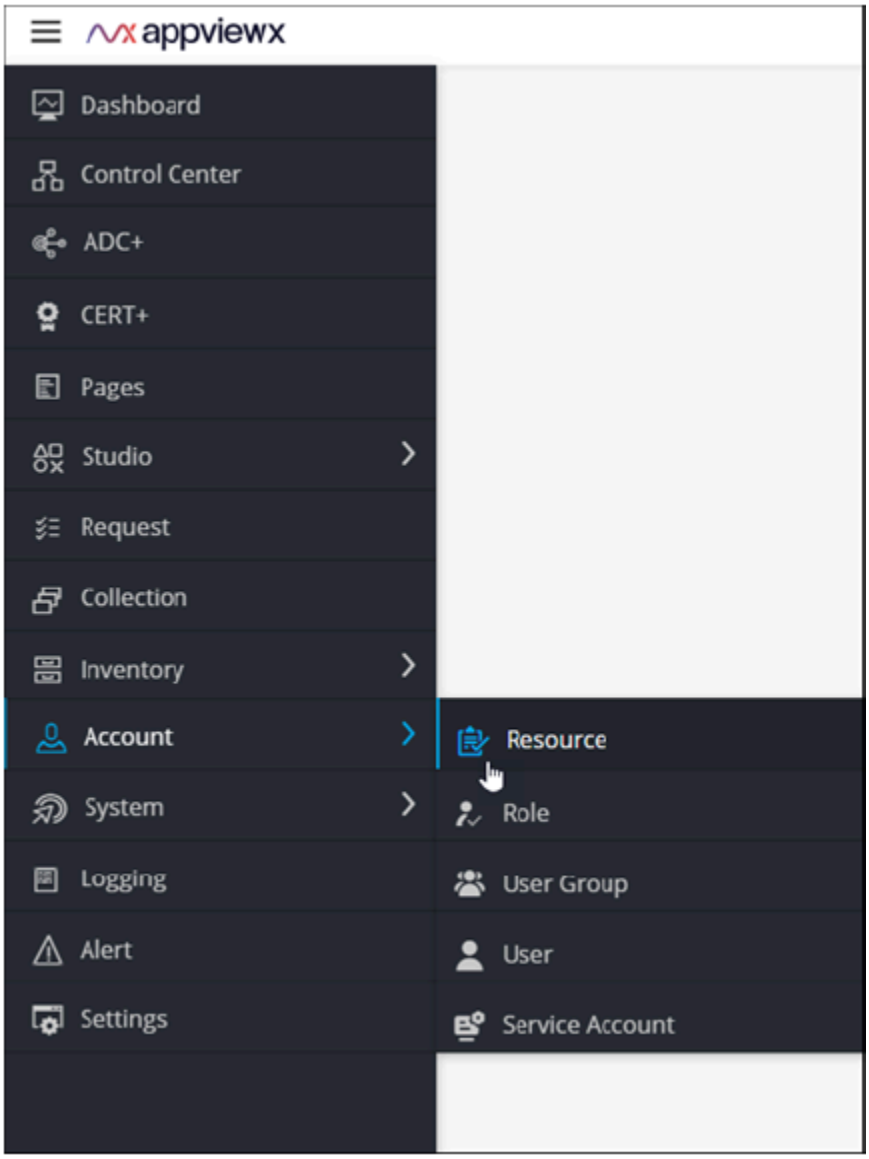


4. From the top-right corner of the screen, click Quick Config. The RBAC Journey :: Authentication page is displayed.
5. Navigate to the Resource stage as part of the wizard flow to add roles into AppViewX, with the Rules tab displayed by default.
6. For the resource you want to clone, select the check box against that resource.
7. From the More Actions drop-down menu, click Clone.
8. 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.
9. 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.

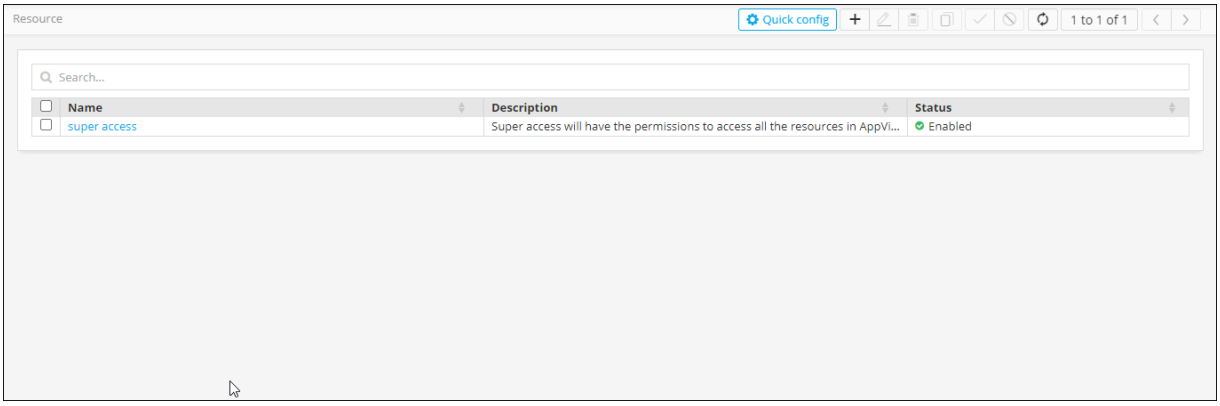
Delete a Rule

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.



3. The Resource page is displayed.

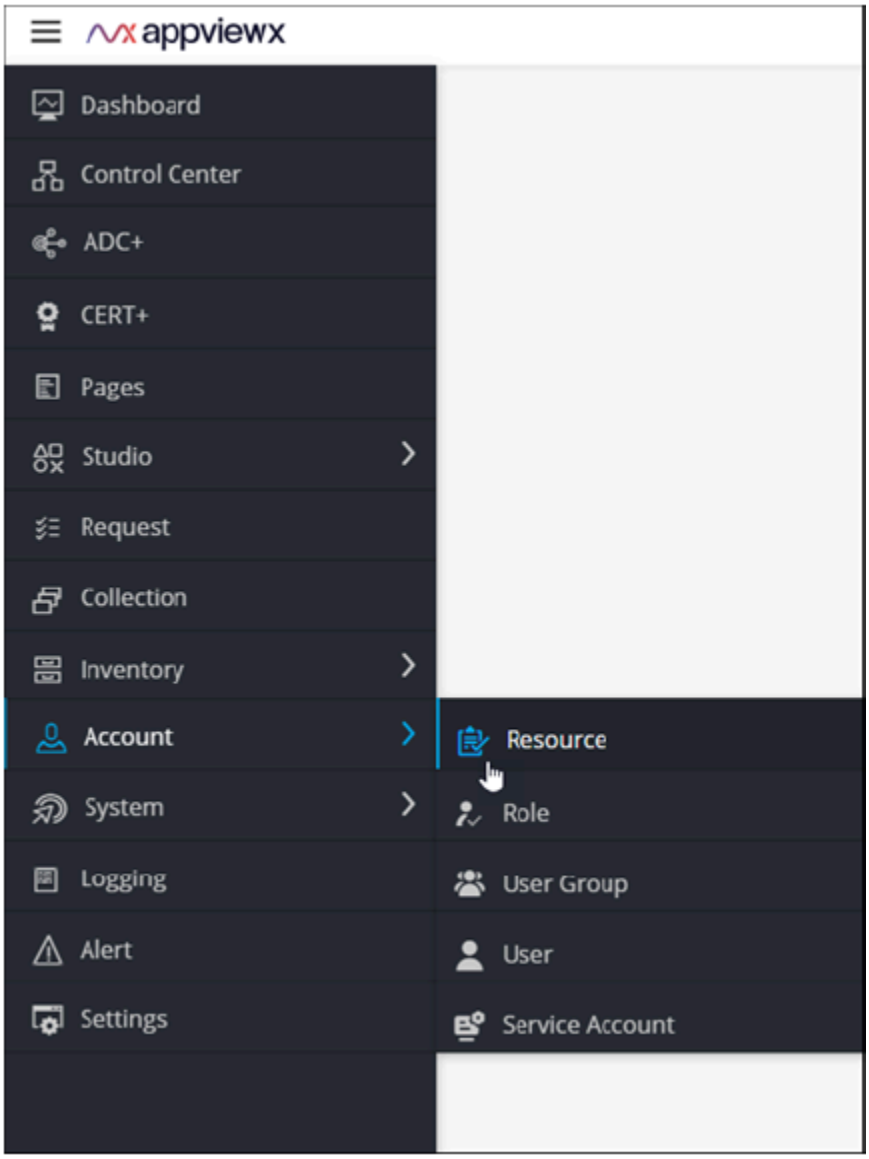


4. From the top-right corner of the screen, click Quick Config. The RBAC Journey :: Authentication page is displayed.
5. Navigate to the Resource stage as part of the wizard flow to add roles into AppViewX, with the Rules tab displayed by default.
6. For the resource you want to delete, select the check box against that resource.
7. From the More Actions drop-down menu, click Delete. In the Confirmation dialog box, click Yes.

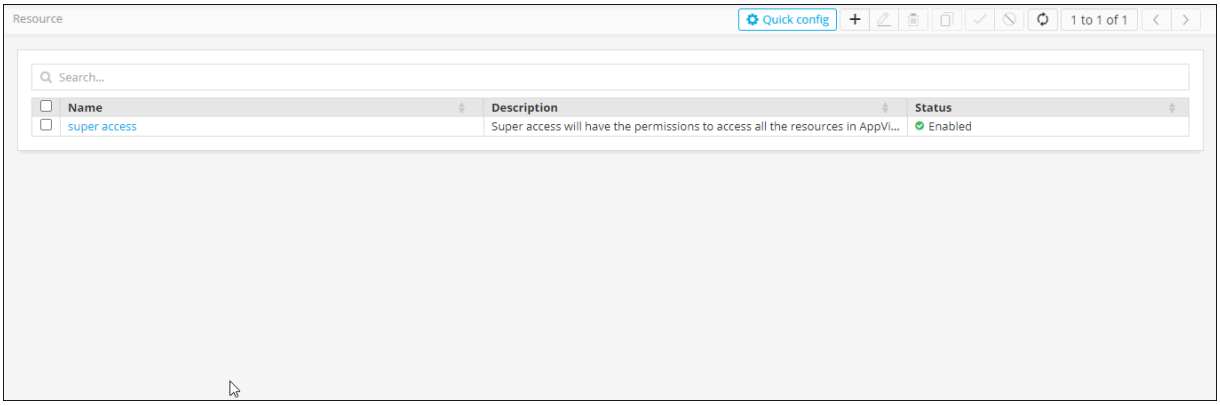
RBAC Rule Mapping to User Groups to Dynamically Provide Access for Resources to User Groups

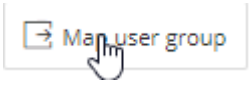
To create a RBAC rule to dynamically provide access for resources to user groups:

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.



3. The Resource page is displayed.



4. From the top-right corner of the screen, click Quick Config. The RBAC Journey :: Authentication page is displayed.
5. Navigate to the Resource stage as part of the wizard flow to add roles into AppViewX, with the Rules tab displayed by default.
6. For the resource you want to map to user groups, select the check box against that resource.
7. Click 

.
8. In the Map user group action pane, select the user groups the resource will be mapped to.
9. Click Save.

Managing Order of Execution and Short Circuit Configuration for Rules

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

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

Key points for consideration:

1. 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.
2. 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.

3. 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:

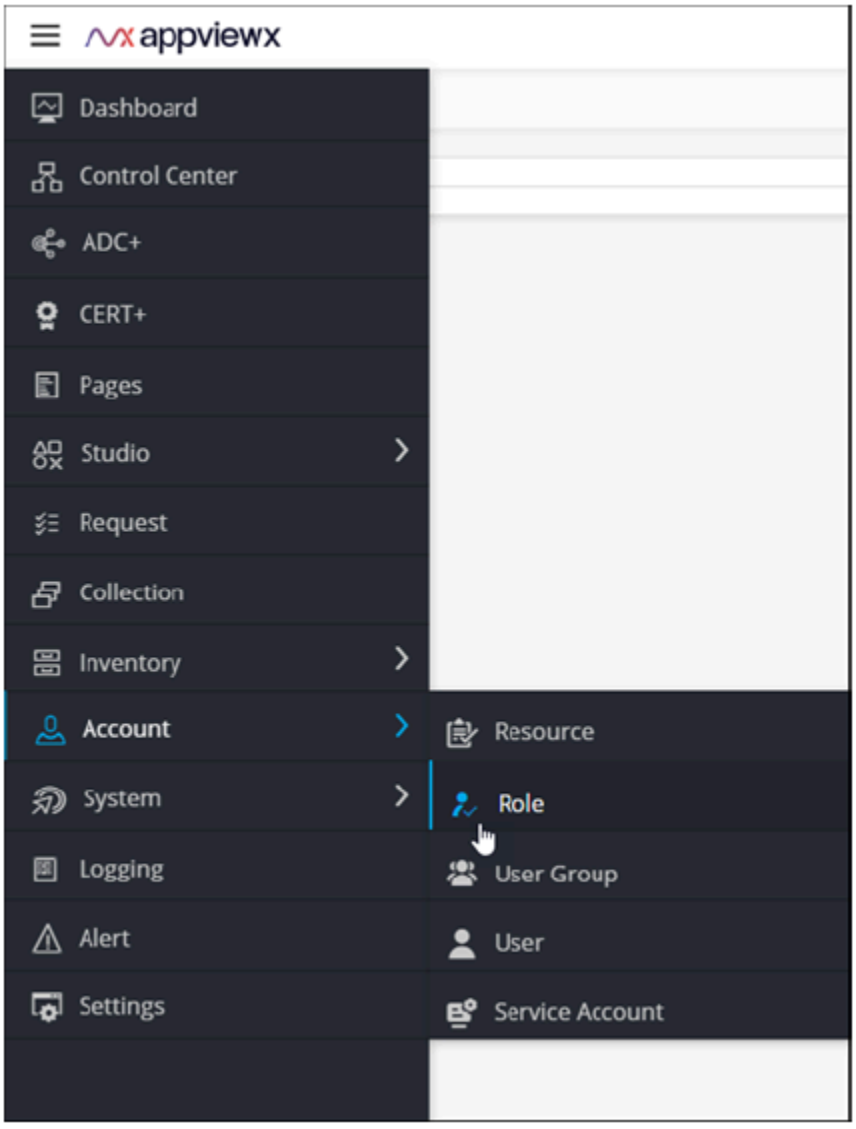
- Out of the Box (OOB) roles are available for ADC, Certificates, Security, and Automation modules.
- OOB roles can be cloned, enabled, and disabled. OOB roles can't be updated/deleted.
- Administrators can also create custom roles. Custom roles can be updated, deleted, enabled and disabled.
- Users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

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

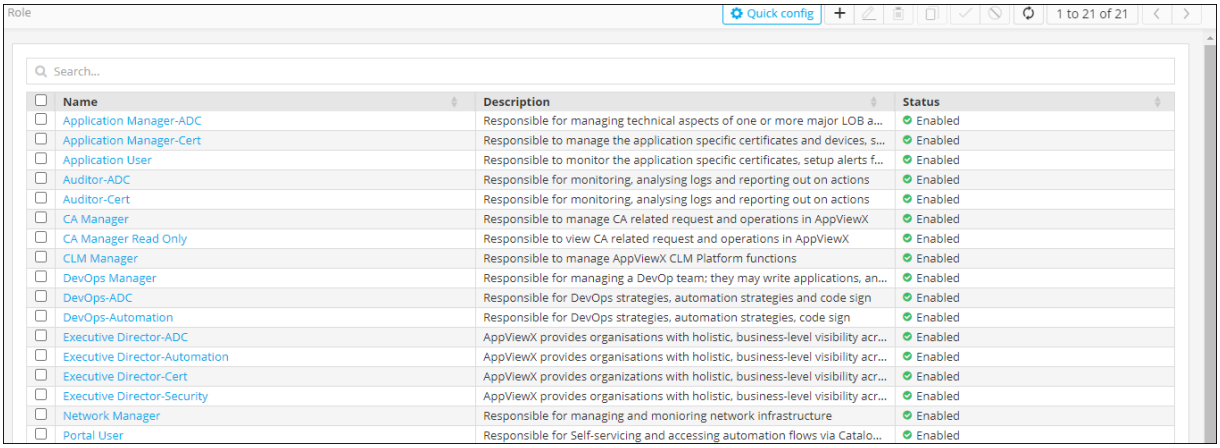
Creating a Custom Role

To create a custom role:

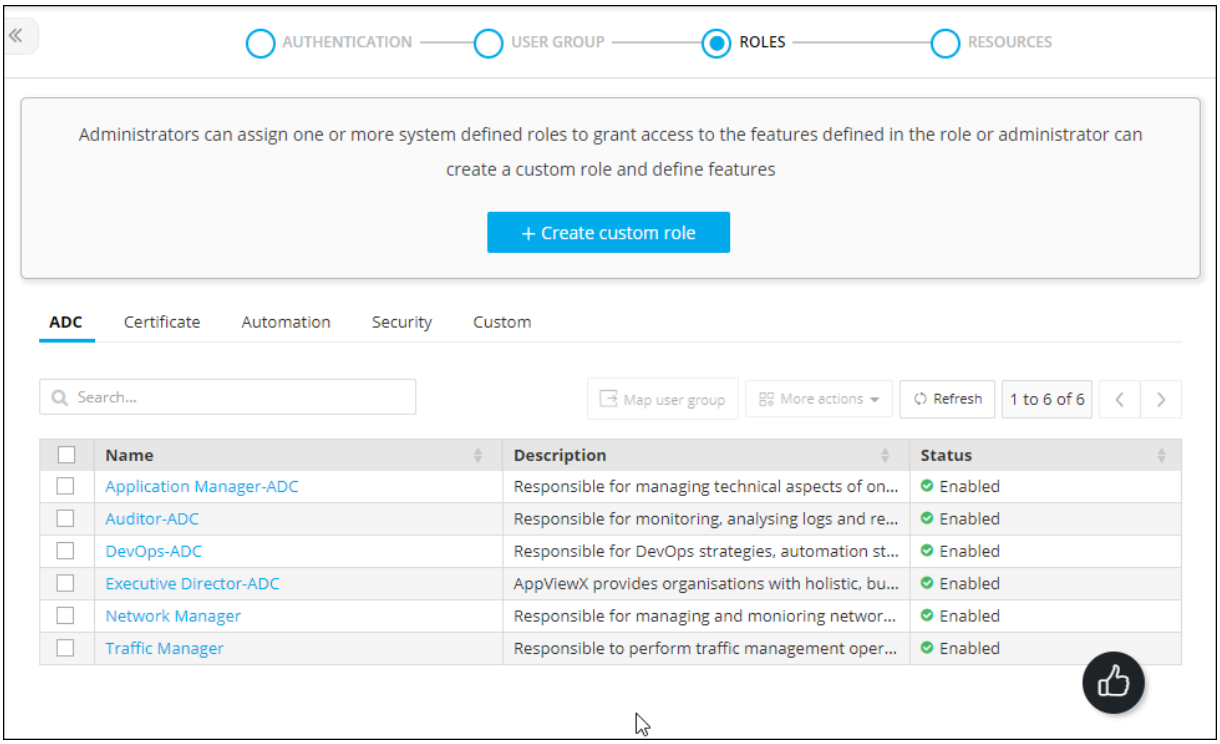
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Account > Role.



3. The Role page is displayed.



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



6. Click + Create custom role.
7. The Create custom role action pane is displayed. Under the Information tab, enter the following details:

Field	Description
Name*	Role name

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

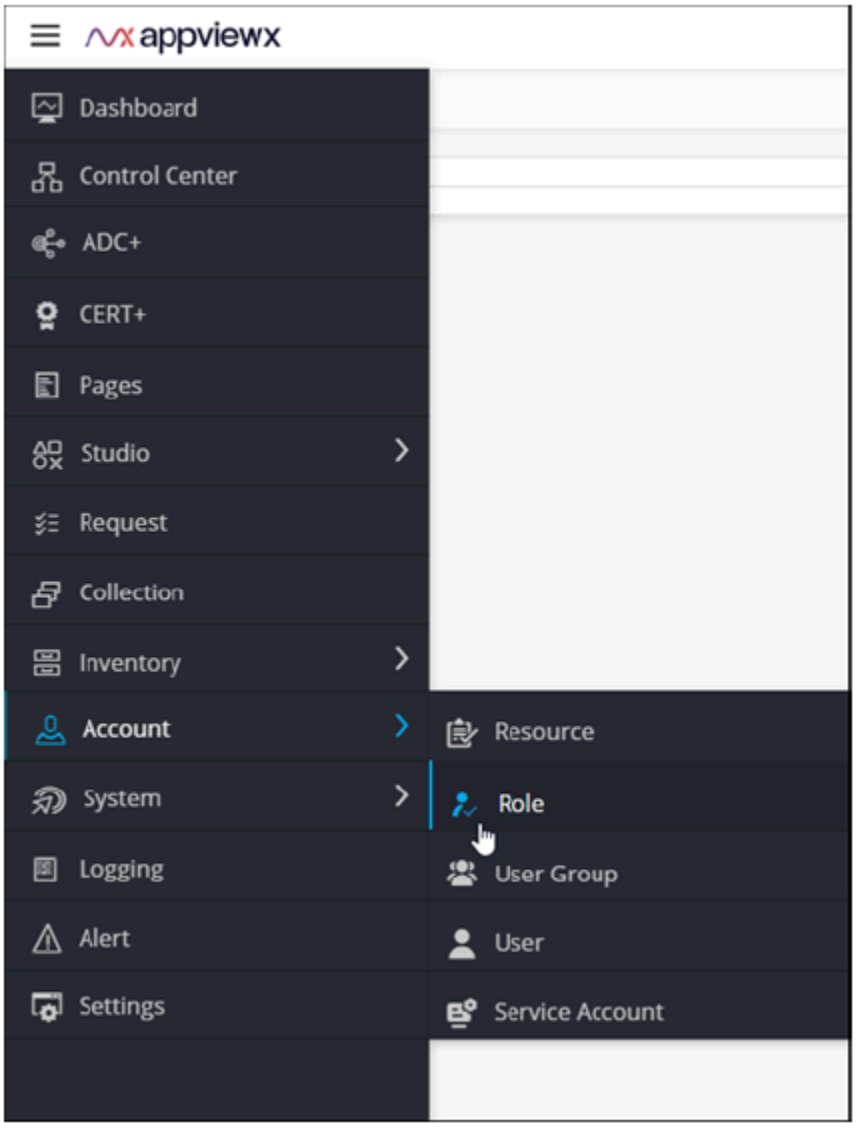
***:Mandatory**

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

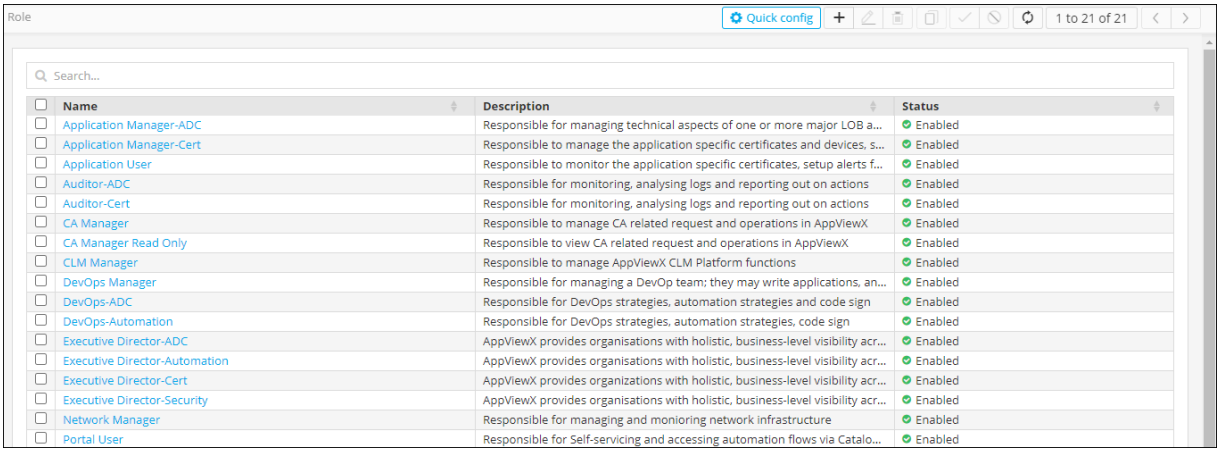
Modifying a Role

To modify a custom role:

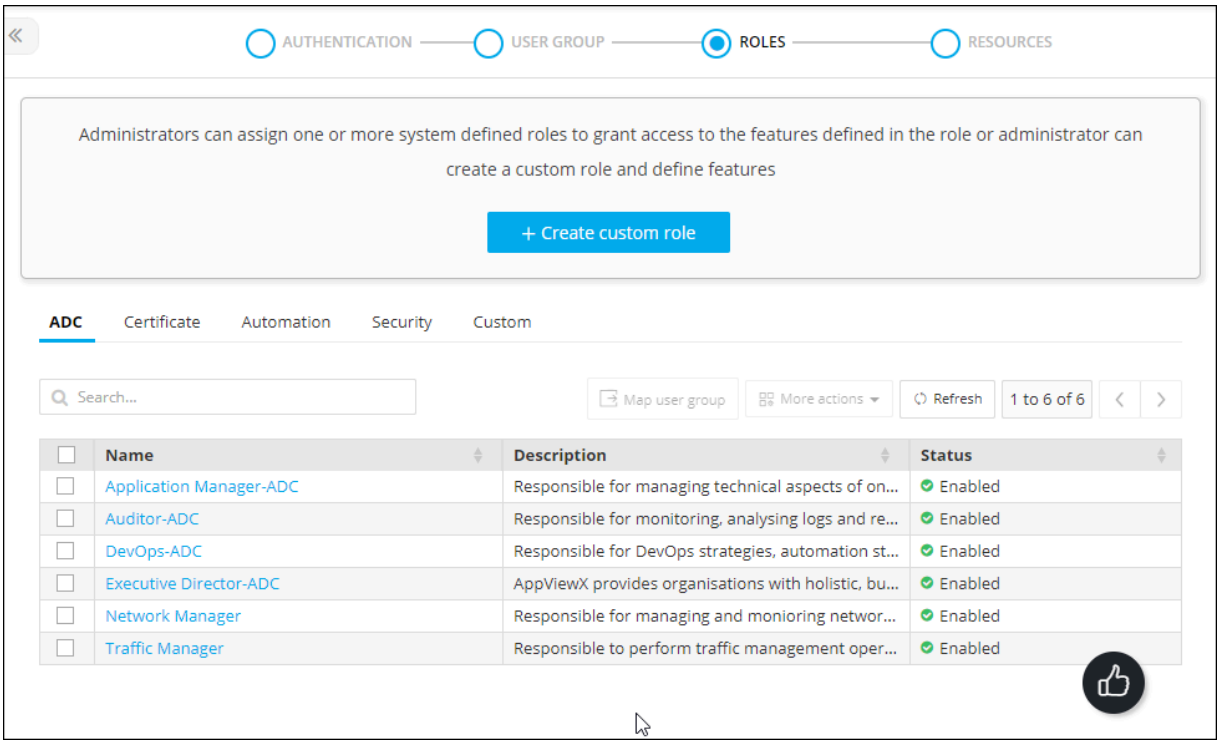
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Account > Role.



3. The Role page is displayed.



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



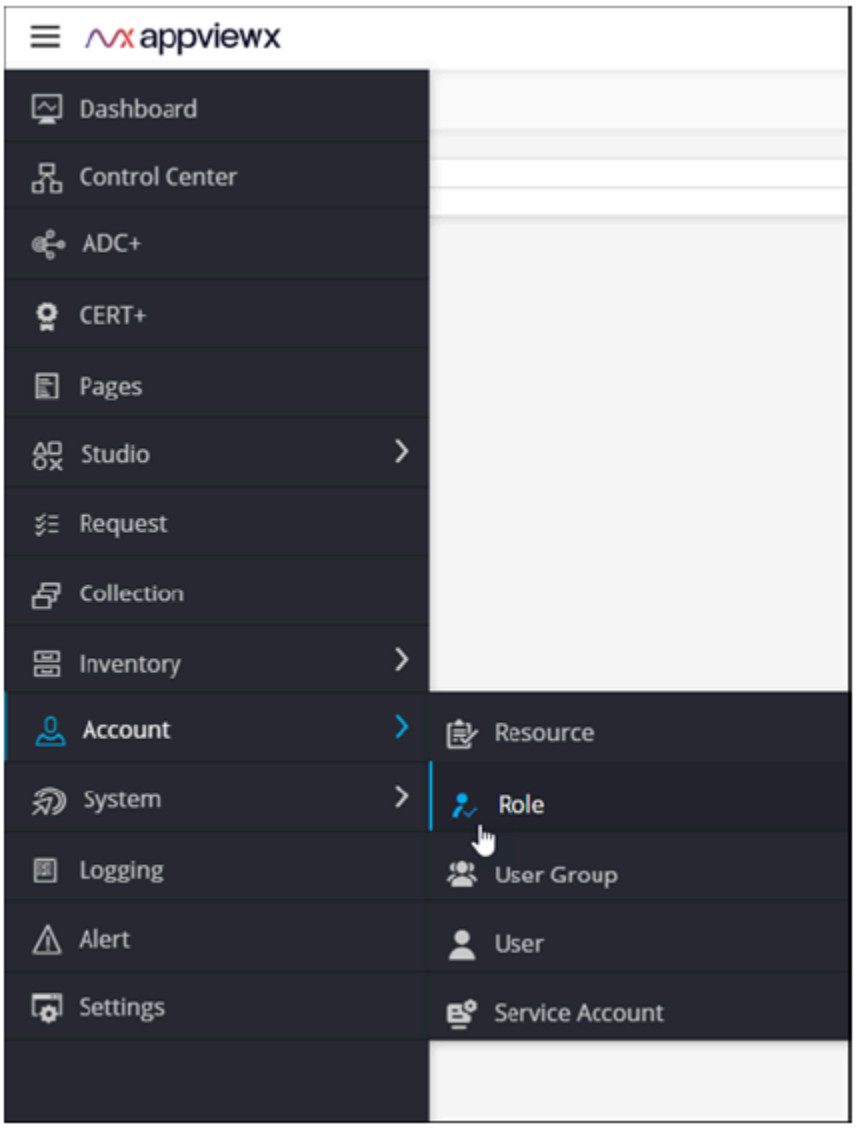
6. Click the role name you want to modify.
7. The Edit role action pane is displayed for the selected role.
8. Modify the details in the Information and Authorized functions as required.
9. Click Save.

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

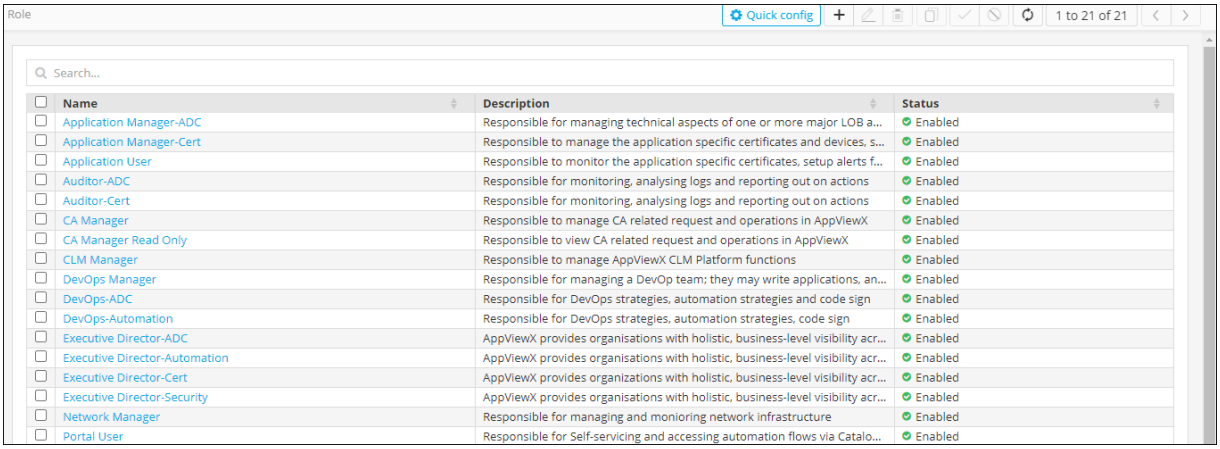
Enabling a Role

To enable a user:

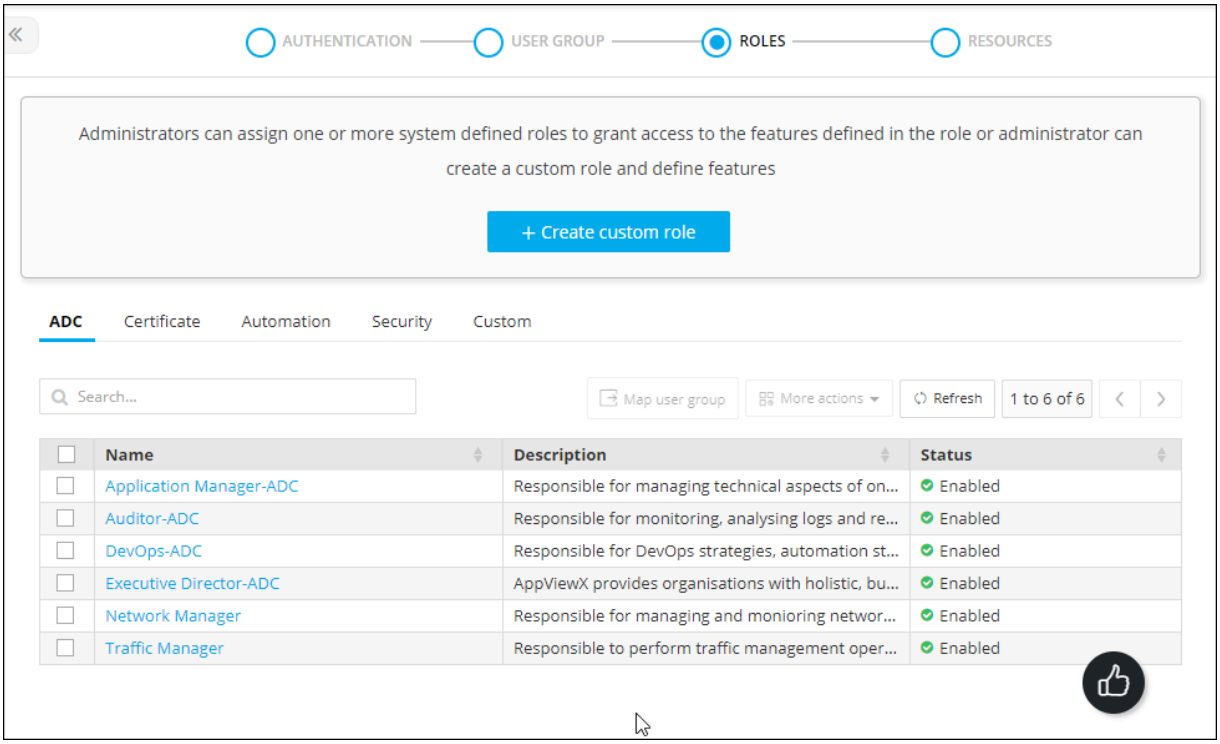
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Account > Role.



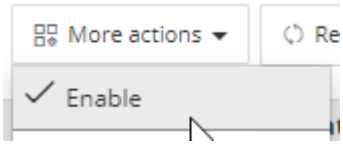
3. The Role page is displayed.



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



6. To enable a role, select the check box against that role.
7. From the More Actions drop-down menu, select Enable.



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

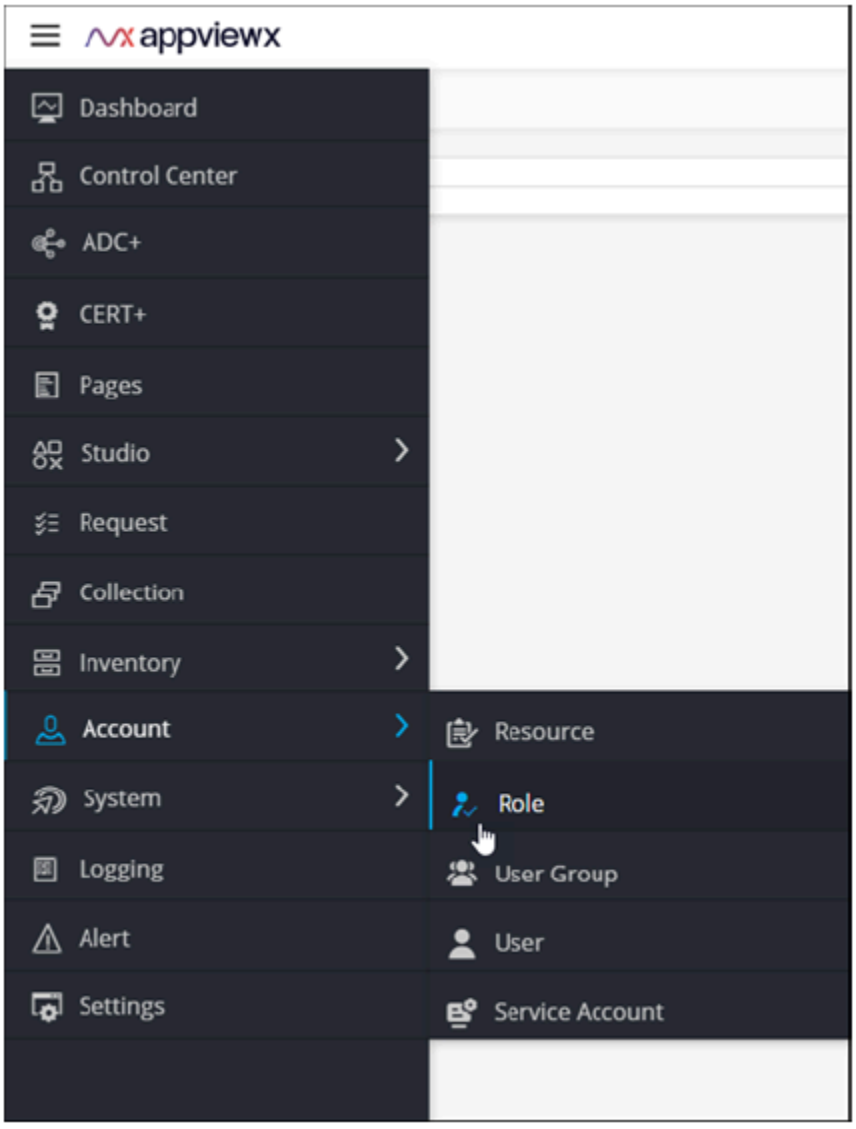
Disabling a Role

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

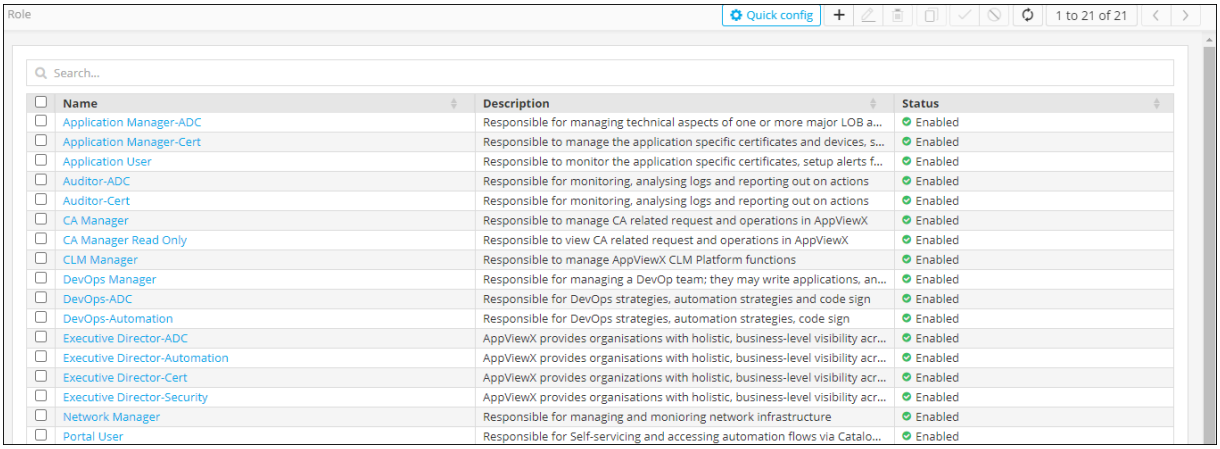
Note: The users associated with a disabled role through a user group will not be allowed to log in to AppViewX.

To disable a role:

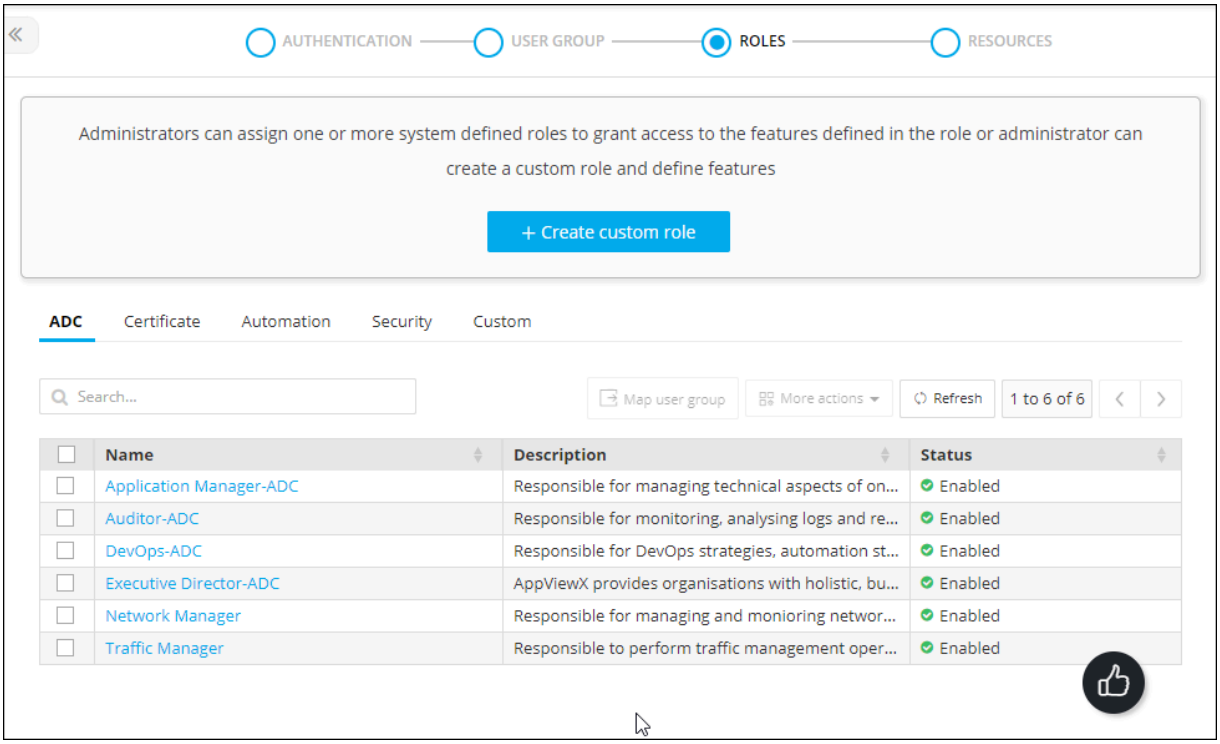
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Account > Role.

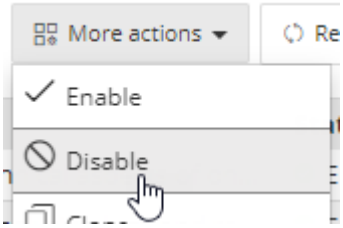


3. The Role page is displayed.



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



6. To disable a role, select the check box against that role. From the More Actions drop-down menu, select Disable. 

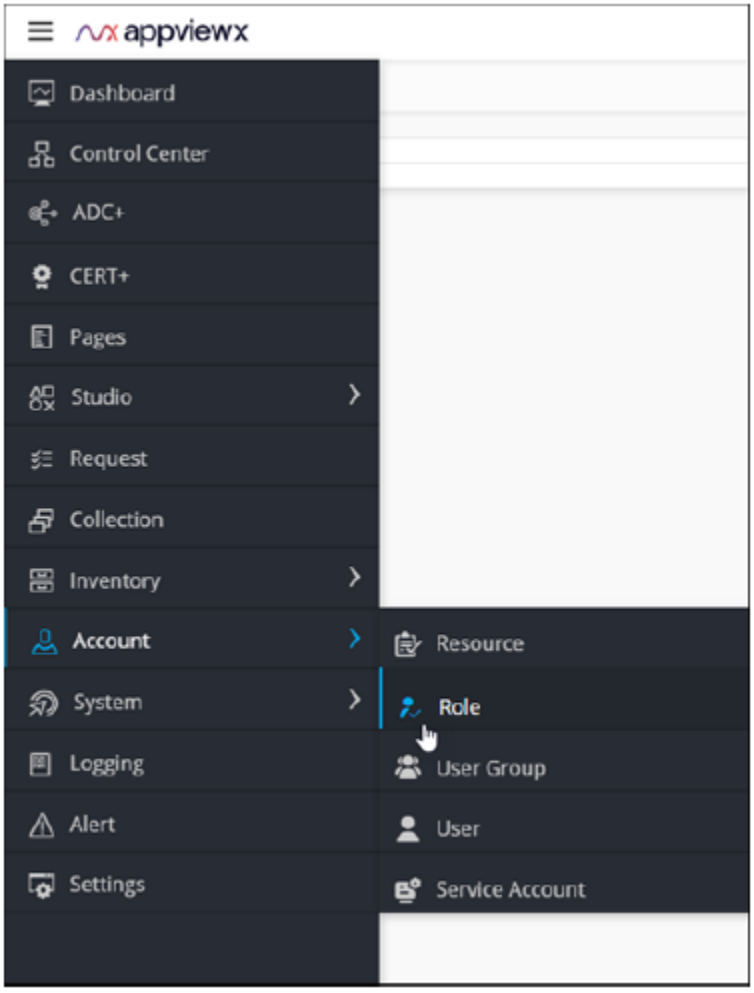
7. In the Disable role(s) dialog box, click Yes.

Cloning a Role

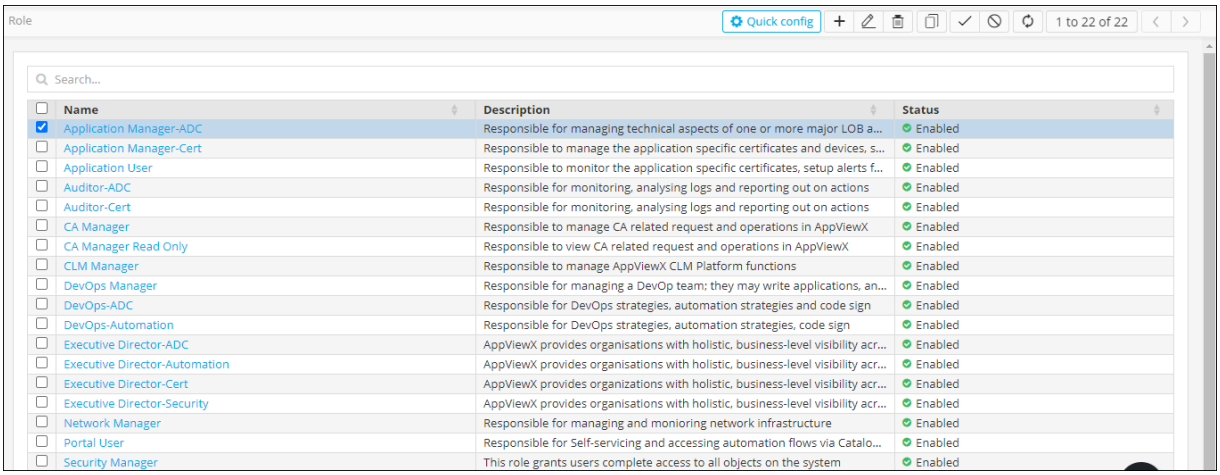
Cloning lets you create a copy of an existing role with a different name. You can modify the permissions and tasks that can be performed while cloning a role.

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.

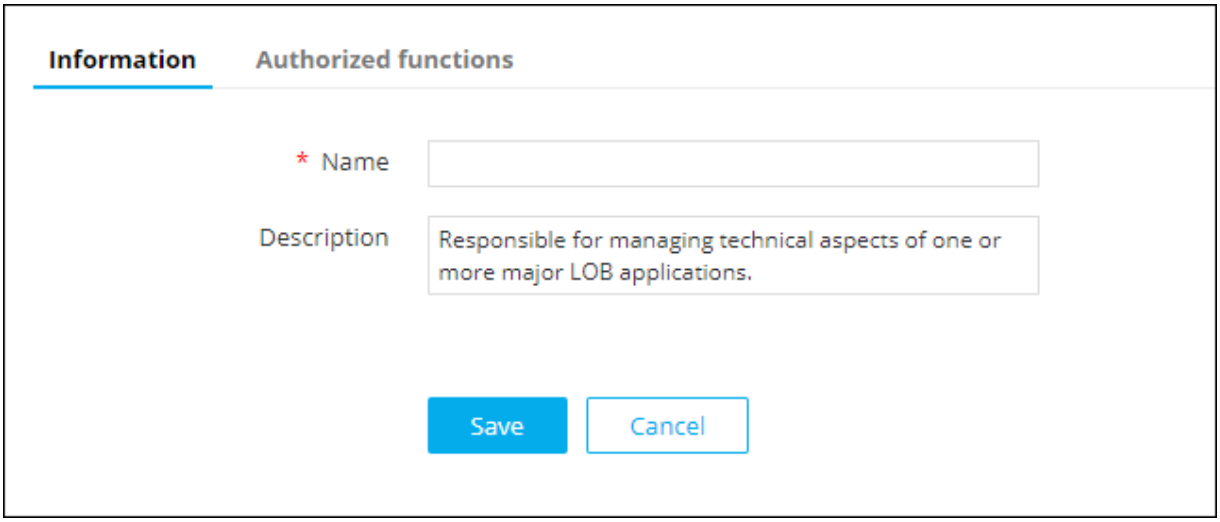


3. The Role page is displayed.



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

6. In the Information section, enter a new name for the role.

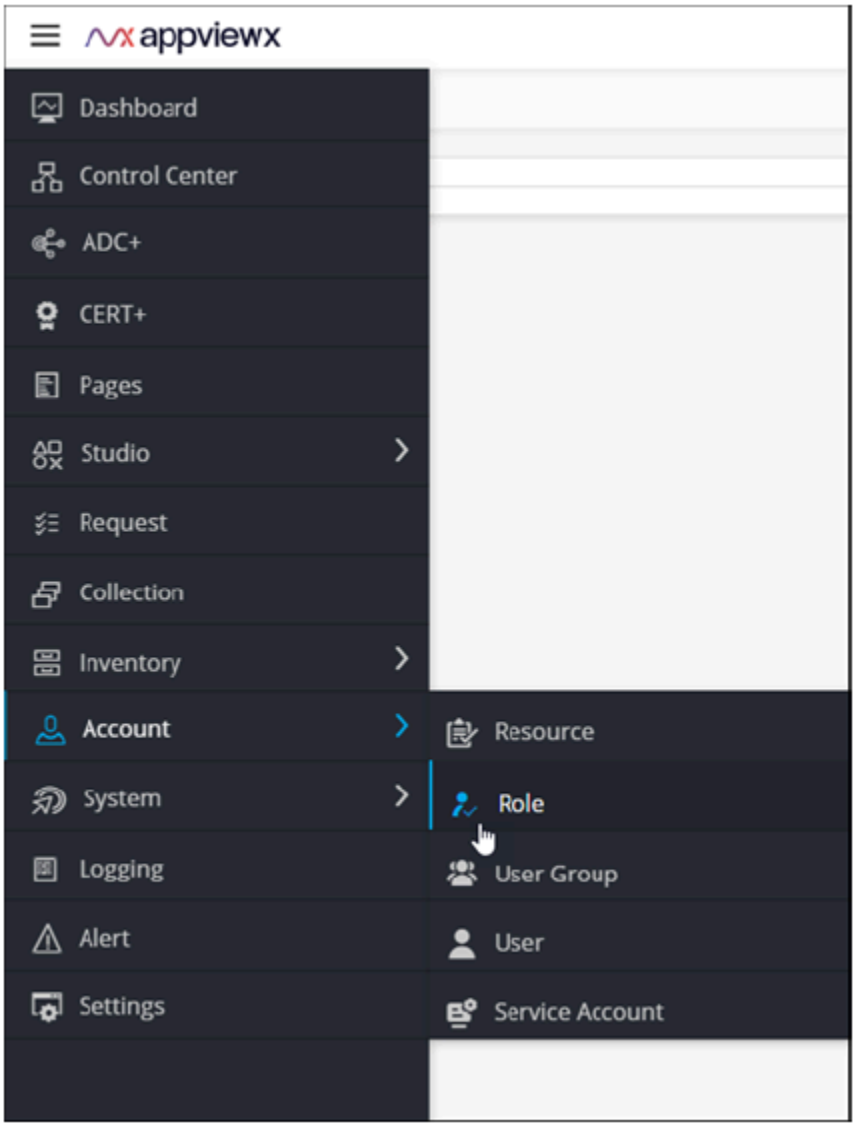


7. Click Save.

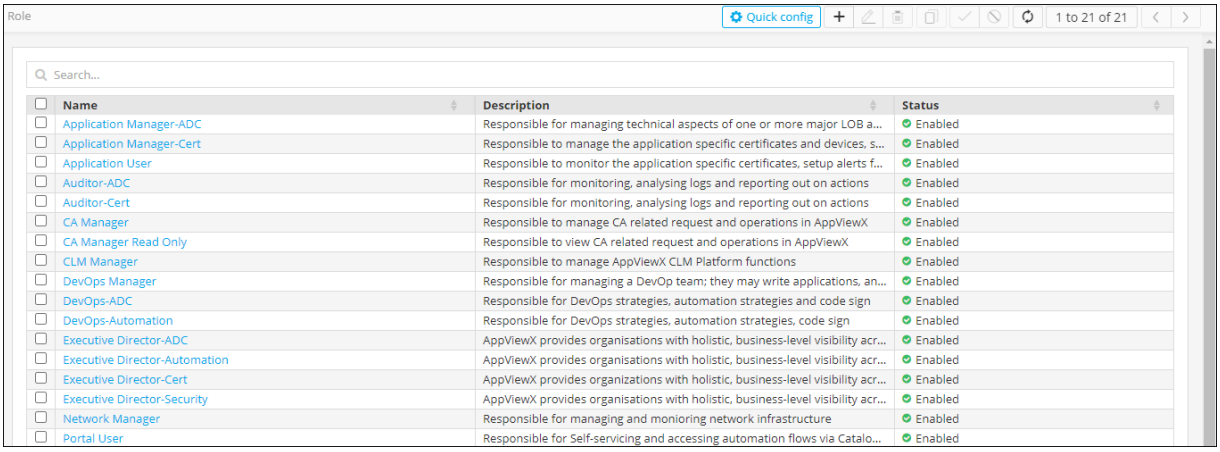
Mapping Role to User Groups

To map roles to user groups:

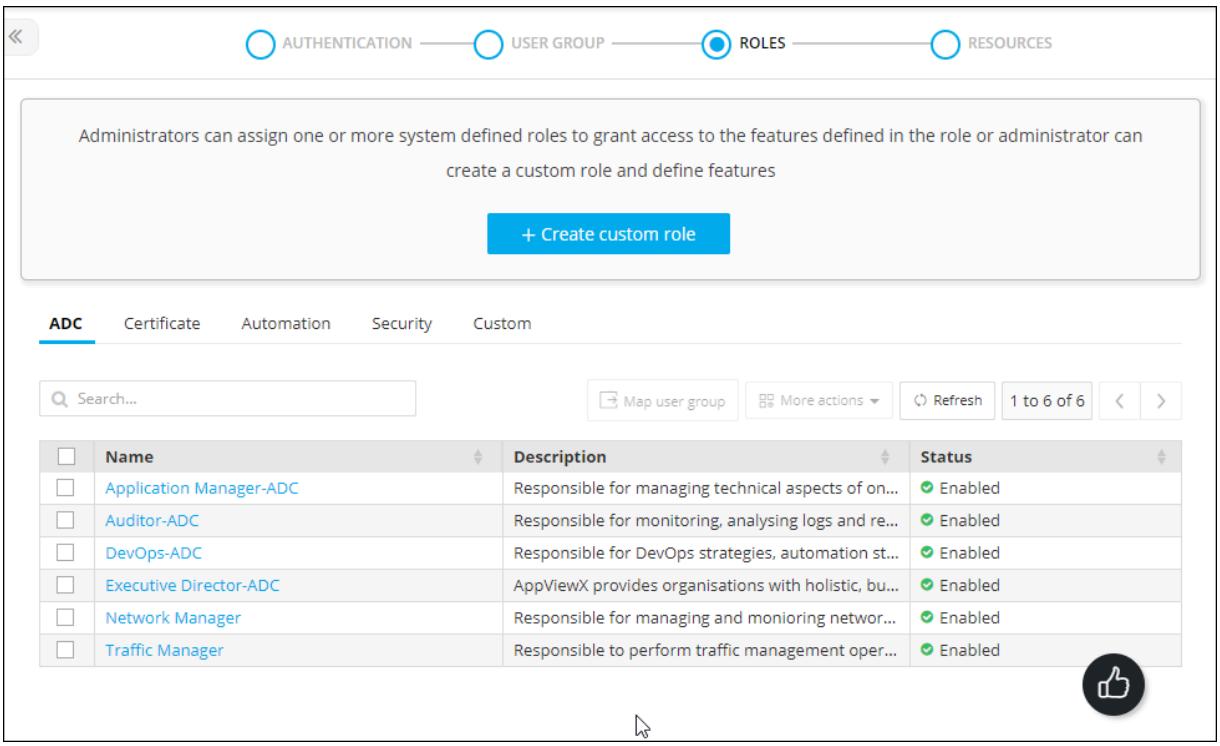
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Account > Role.



3. The Role page is displayed.



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



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

.
8. In the Mapping user group action pane, select the user groups the role will be mapped to.
9. Click Save. The saved list of user groups will be displayed as a hyperlink in the rule inventory for each group.

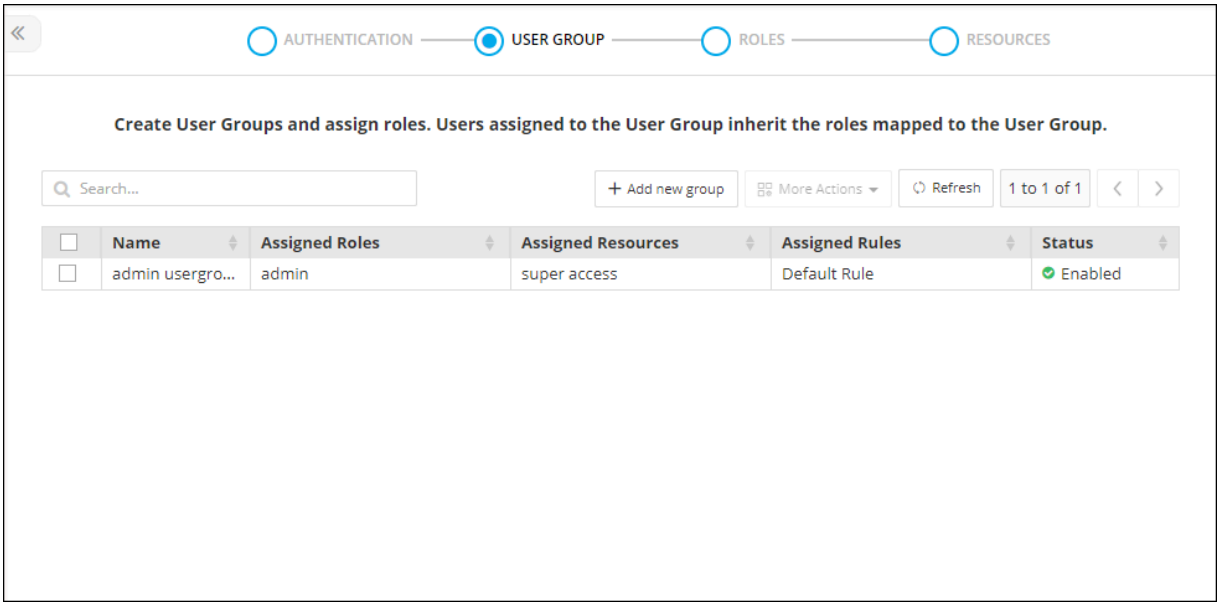
User Group

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.

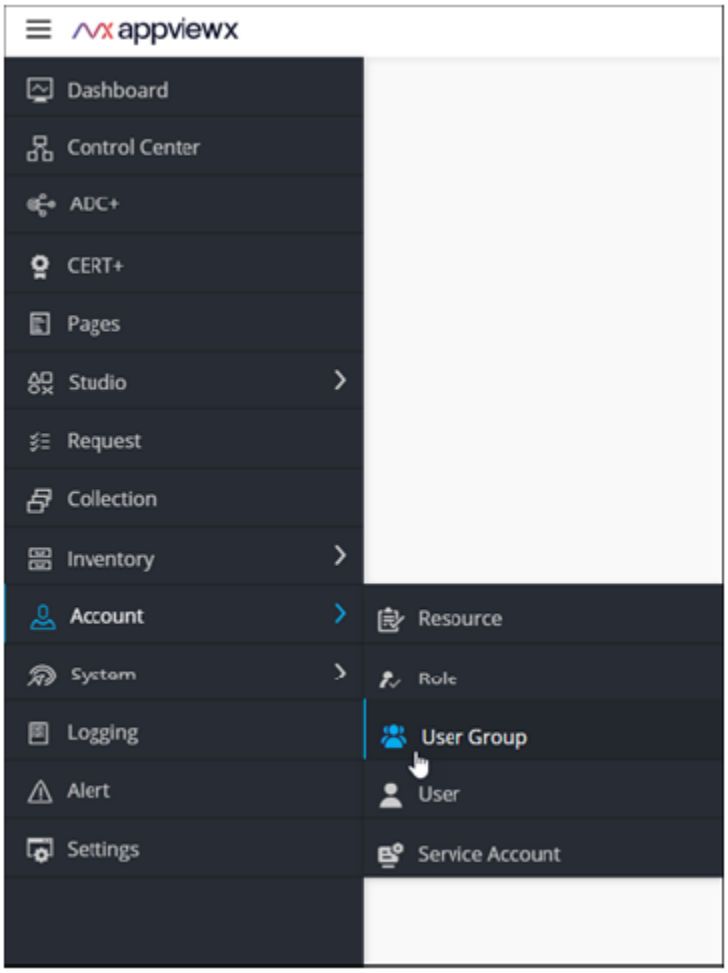
- Adding a New User Group by Syncing Groups from LDAP
- Adding a New User Group using the TACACS/RADIUS/SAML/AppViewX Option
- Add New User Group by Bulk Import
- Disabling a User Group
- Enabling a User Group

- Cloning a User Group
- Deleting a User Group

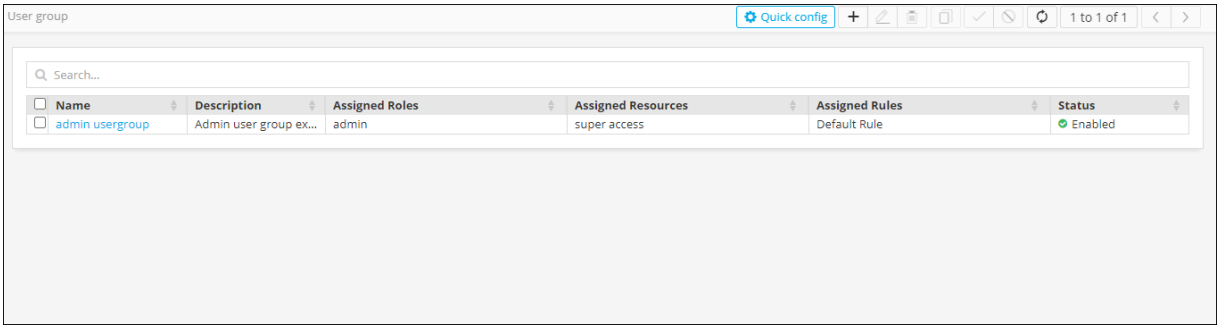
Adding a New User Group by Syncing Groups from LDAP

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

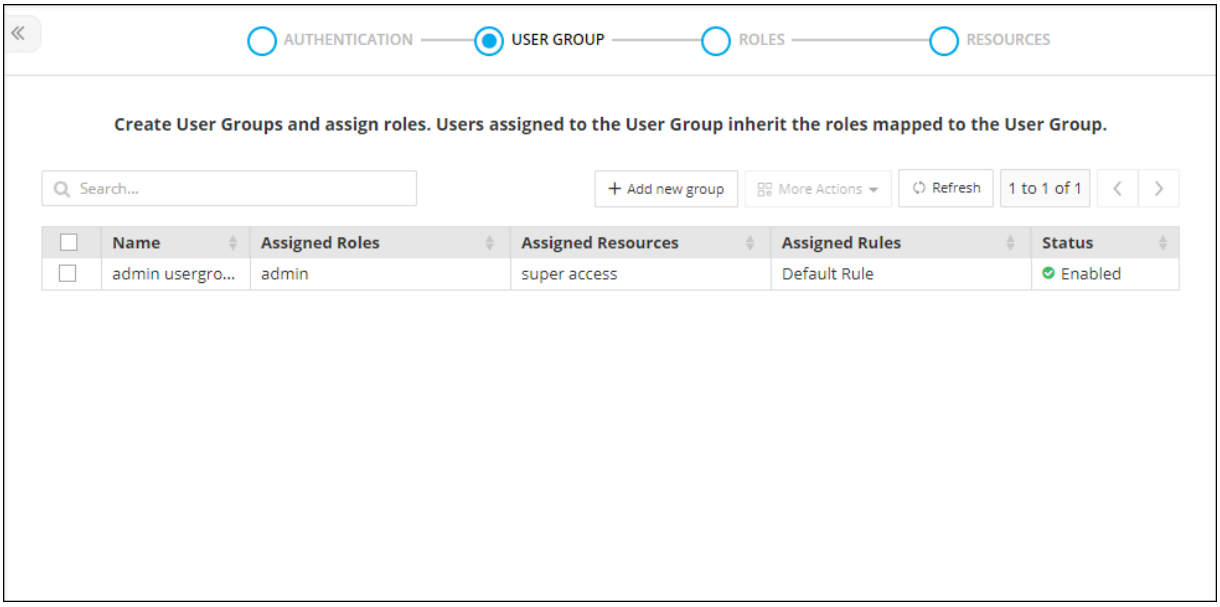
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Account > User Group.

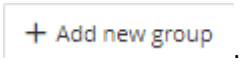


3. The User group page is displayed.

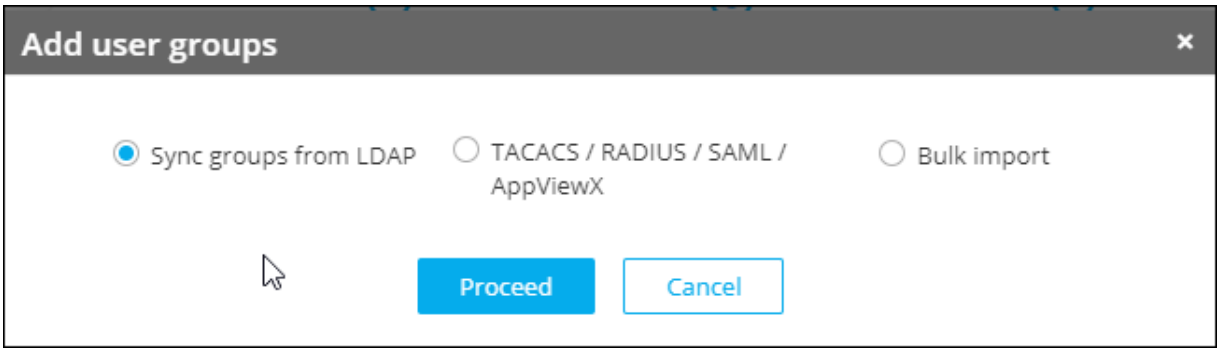


4. From the top-right corner of the screen, click Quick Config. The RBAC Journey :: Authentication page is displayed.
5. Navigate to the User Group stage as part of the wizard flow to add user groups into AppViewX.



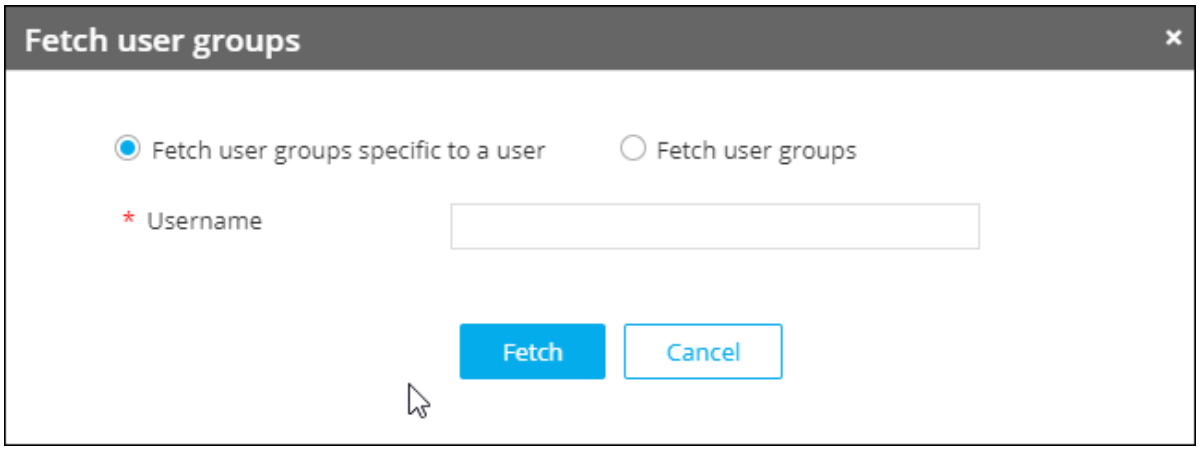
6. Click 

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



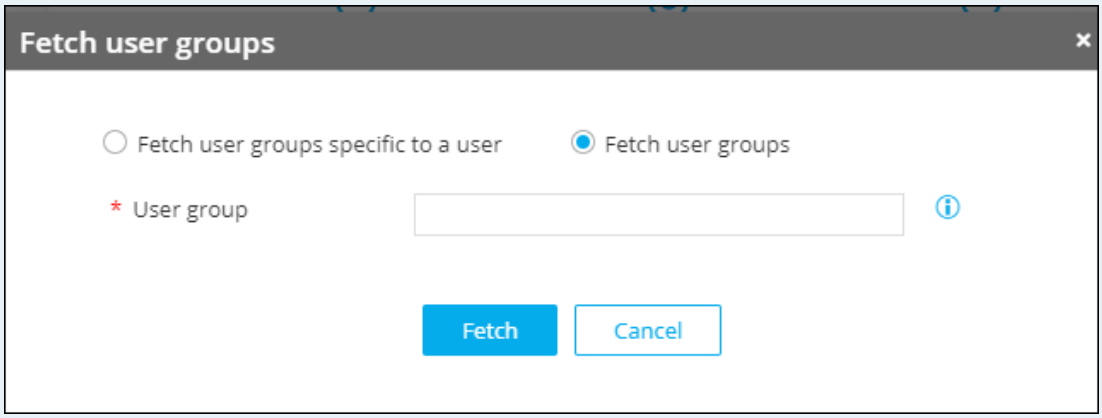
8. The LDAP inventory table is displayed.

9. 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 .
10. 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.



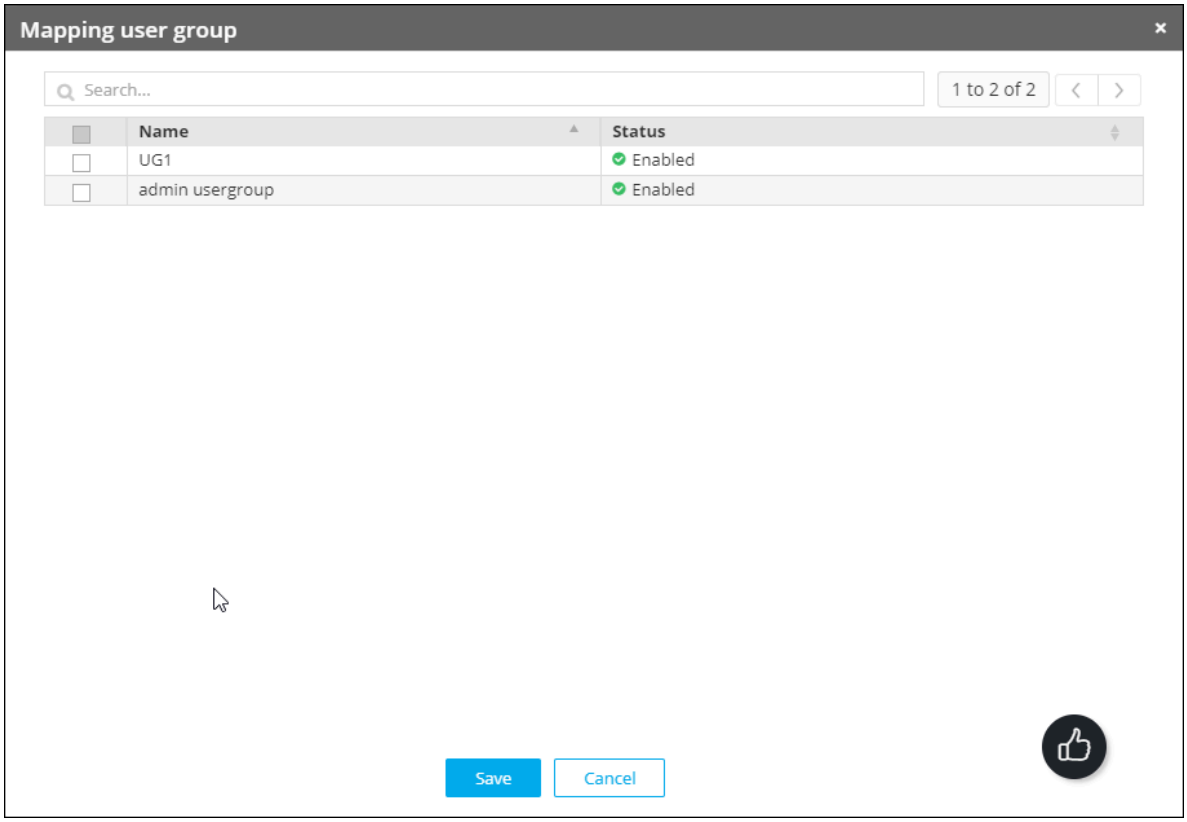
    - To fetch user groups by a specific name, select Fetch user groups and type the enter the User group name from the AD.

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



11. Click Fetch. A table containing the AD group names and their corresponding AppViewX user group names is displayed.
12. Select the AD user group(s) that must be created with the same name in AppViewX and click Save to Appviewx .
13. 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.

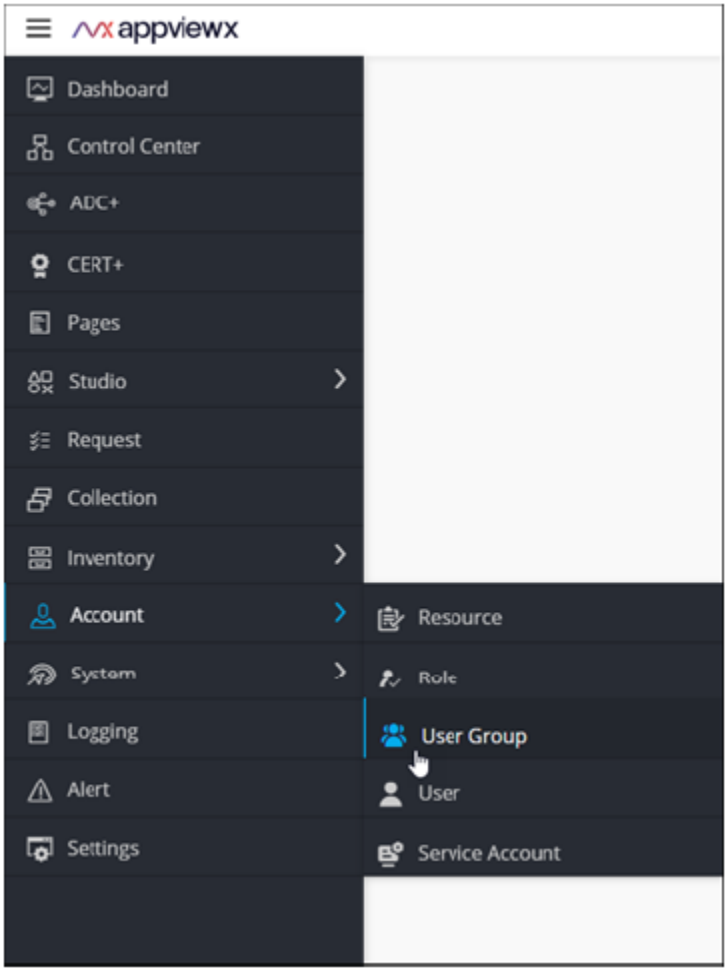
Selected AD user group(s) will be now mapped to the existing AppViewX user group and the same mapping will reflect in the AD group names table.

14. 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.

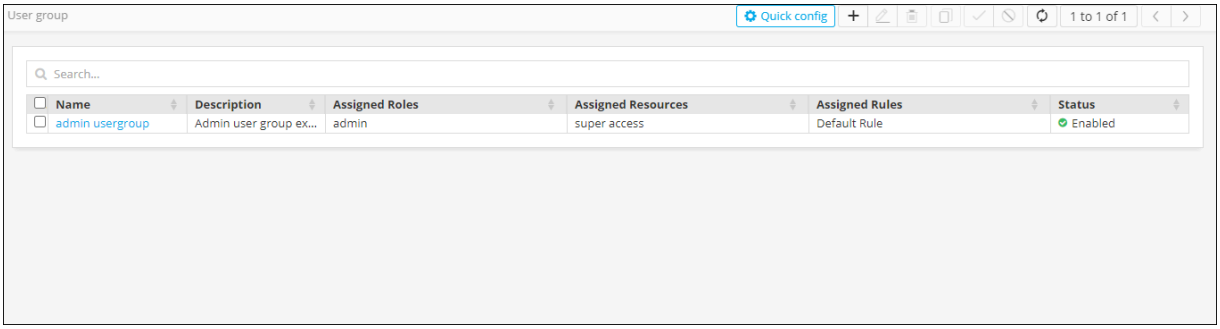
Adding a New User Group using the TACACS/RADIUS/SAML/AppViewX Option

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 > User Group.

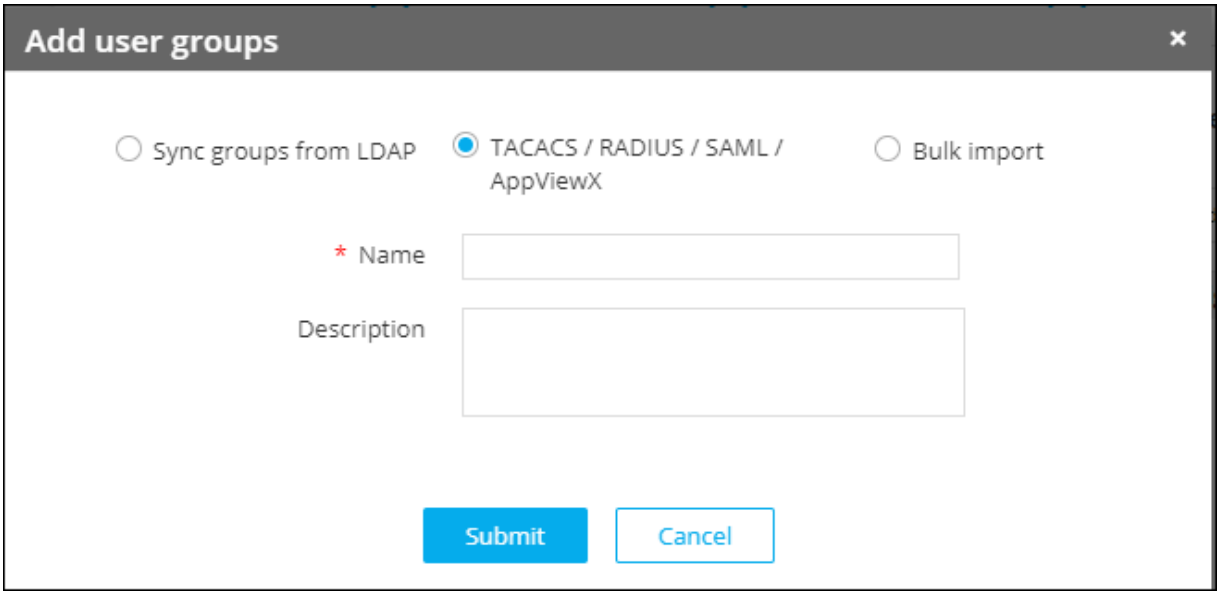


3. The User group page is displayed.



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

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

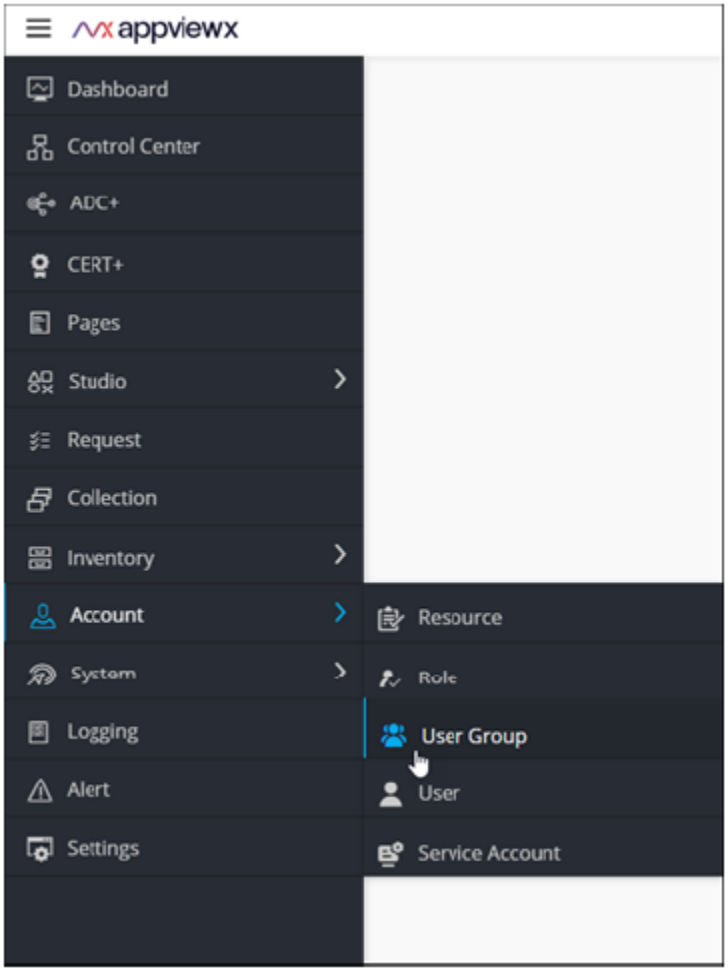


9. Click Submit.

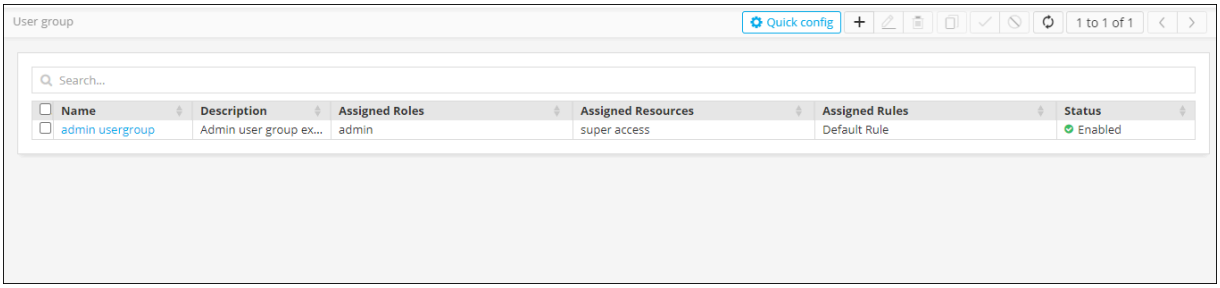
Add New User Group by Bulk Import

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.

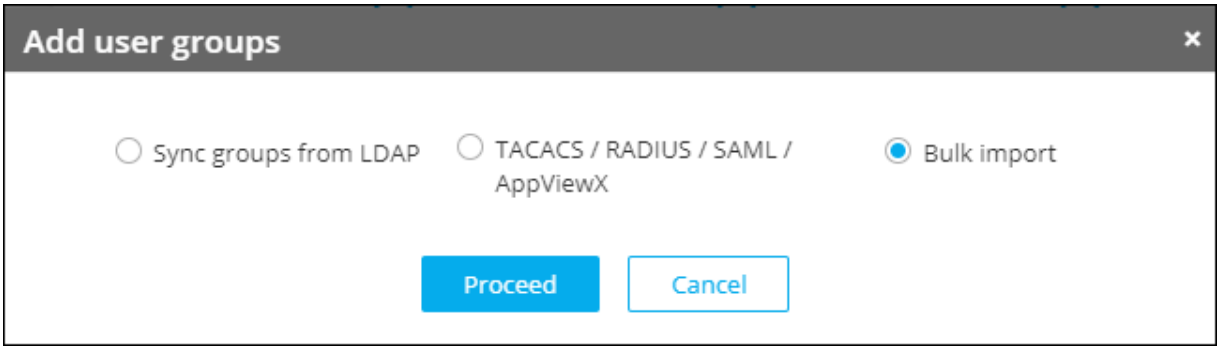


3. The User group page is displayed.



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

7. From the Add user groups dialog box, select Bulk import.



8. Click Browse.
9. 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 .

10. 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).

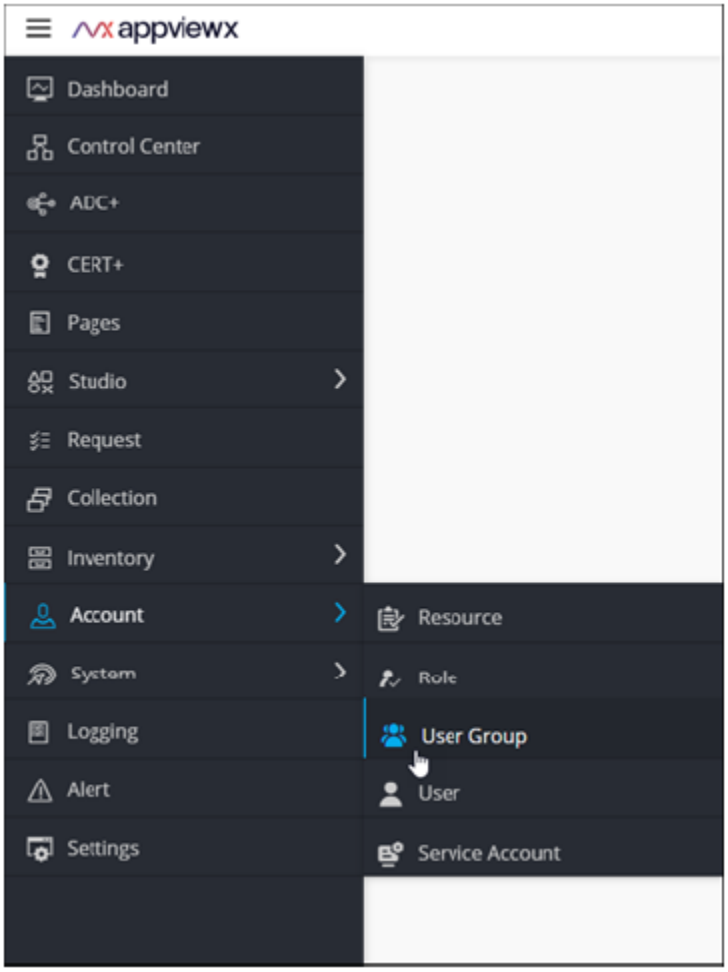
11. To save the user groups, select the list of user groups and click . All user groups with the valid status will be saved into AppViewX.

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

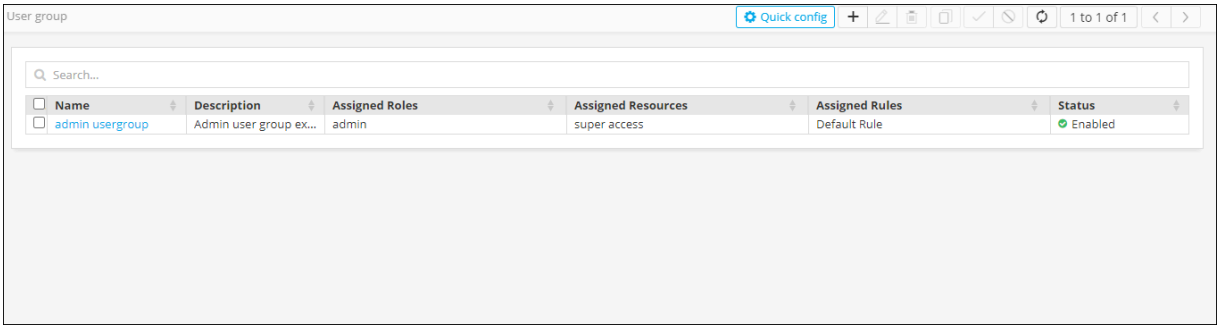
Disabling a User Group

To disable a user group:

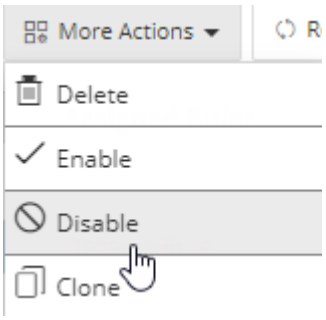
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Account > User Group.



3. The User group page is displayed.



4. From the top-right corner of the screen, click Quick Config. The RBAC Journey :: Authentication page is displayed.
5. Navigate to the User Group stage as part of the wizard flow to add user groups into AppViewX.
6. From the inventory table, select the user group to be disabled.

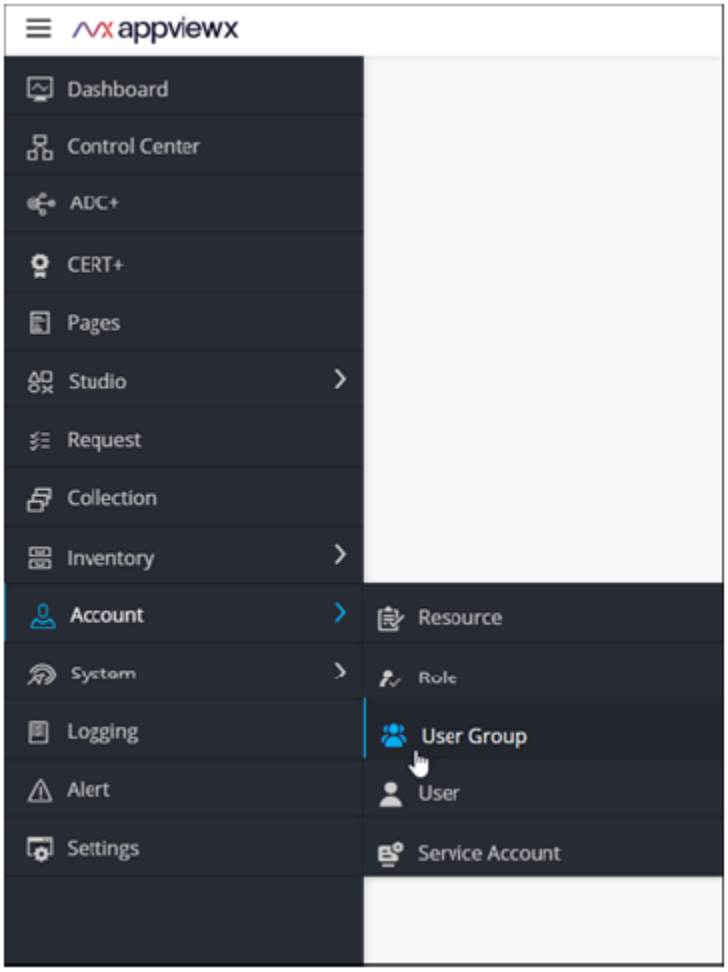


7. From the More Action drop-down menu, select Disable.
8. From the Disable user group dialog box, click Yes.

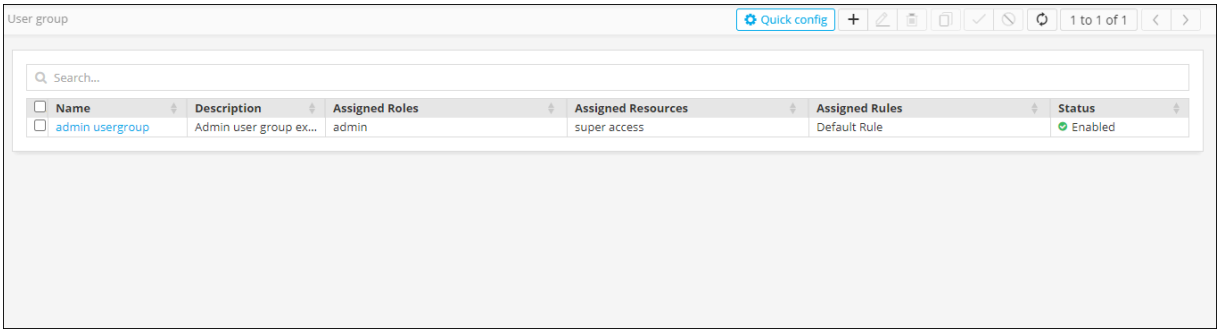
Enabling a User Group

To enable a user group:

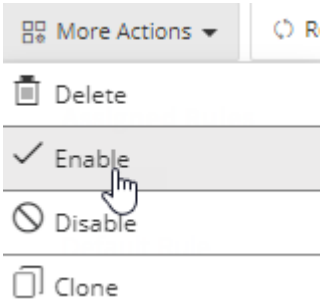
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Account > User Group.



3. The User group page is displayed.



4. From the top-right corner of the screen, click Quick Config. The RBAC Journey :: Authentication page is displayed.
5. Navigate to the User Group stage as part of the wizard flow to add user groups into AppViewX.
6. From the inventory table, select the user group to be enabled.

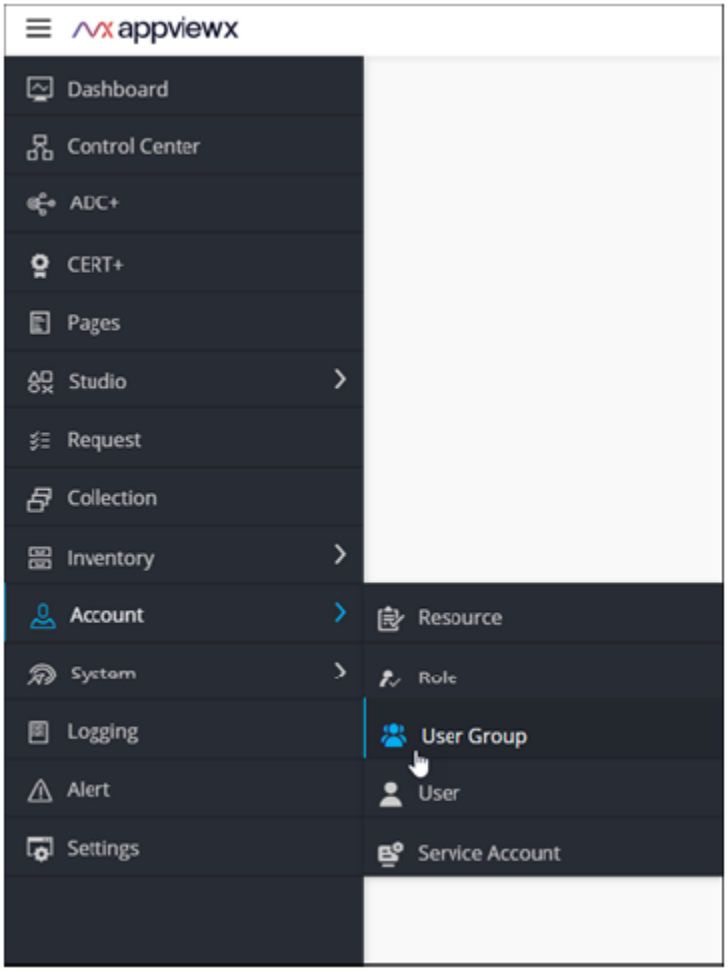


7. From the More Action drop-down menu, select Enable.
8. From the Enable user group dialog box, click Yes.

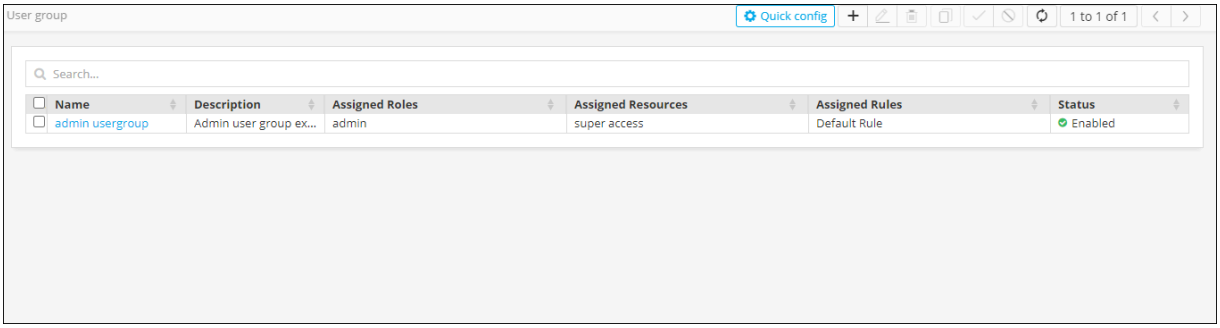
Cloning a User Group

To clone a user group:

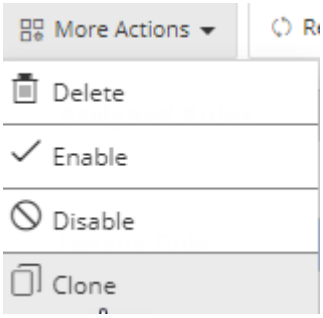
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Account > User Group.



3. The User group page is displayed.



4. From the top-right corner of the screen, click Quick Config. The RBAC Journey :: Authentication page is displayed.
5. Navigate to the User Group stage as part of the wizard flow to add user groups into AppViewX.
6. From the inventory table, select the user group to be cloned.

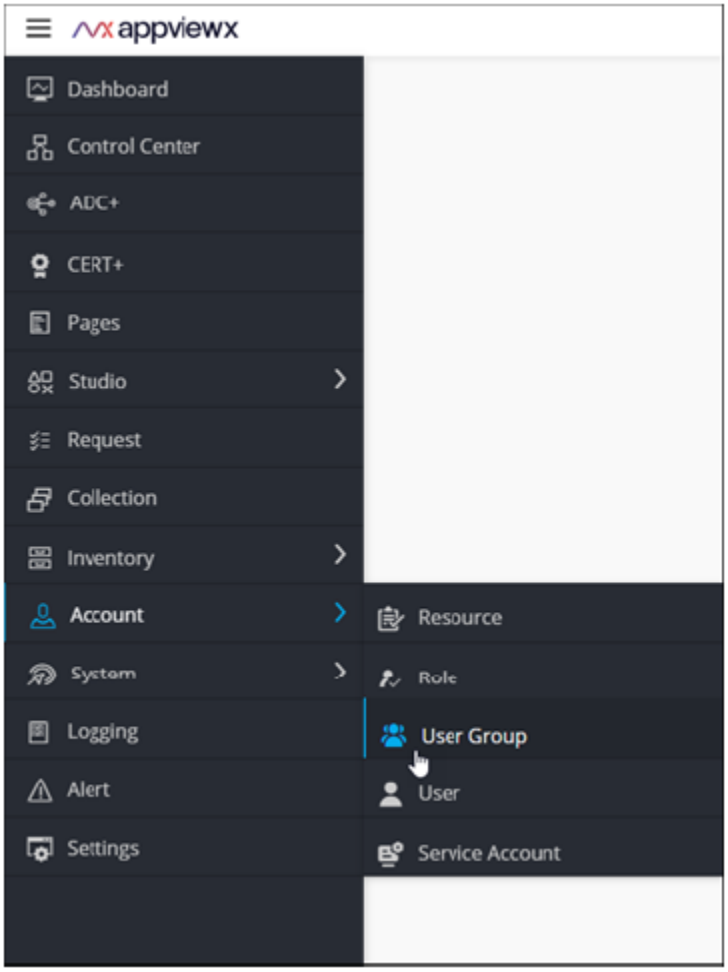


7. From the More Action drop-down menu, select Clone.
8. In the Clone dialog box, enter a name for the cloned user group and update the description, if required.
9. Click Save.

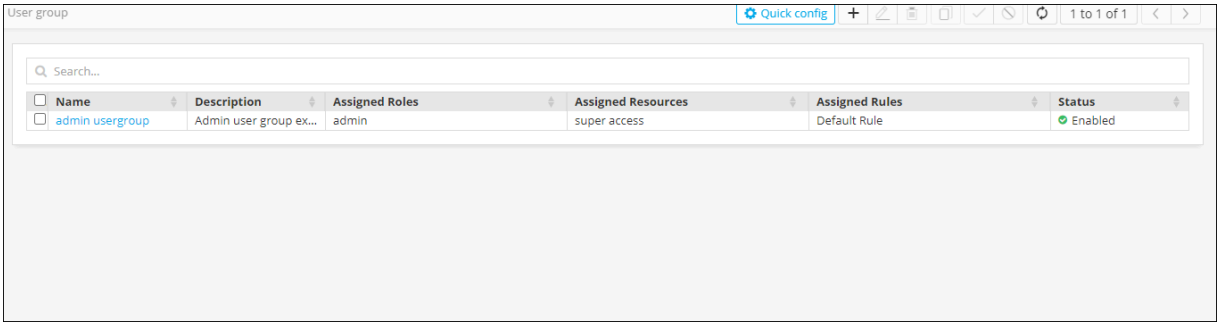
Deleting a User Group

To delete a user group:

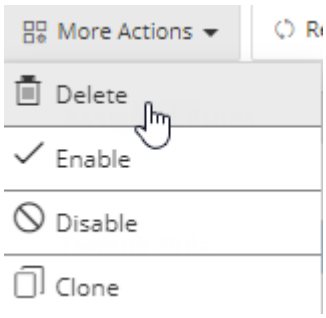
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Account > User Group.



3. The User group page is displayed.



4. From the top-right corner of the screen, click Quick Config. The RBAC Journey :: Authentication page is displayed.
5. Navigate to the User Group stage as part of the wizard flow to add user groups into AppViewX.
6. From the inventory table, select the record to be deleted.



7. From the More Action drop-down menu, select Delete.
8. From the Delete user group dialog box, click Yes.

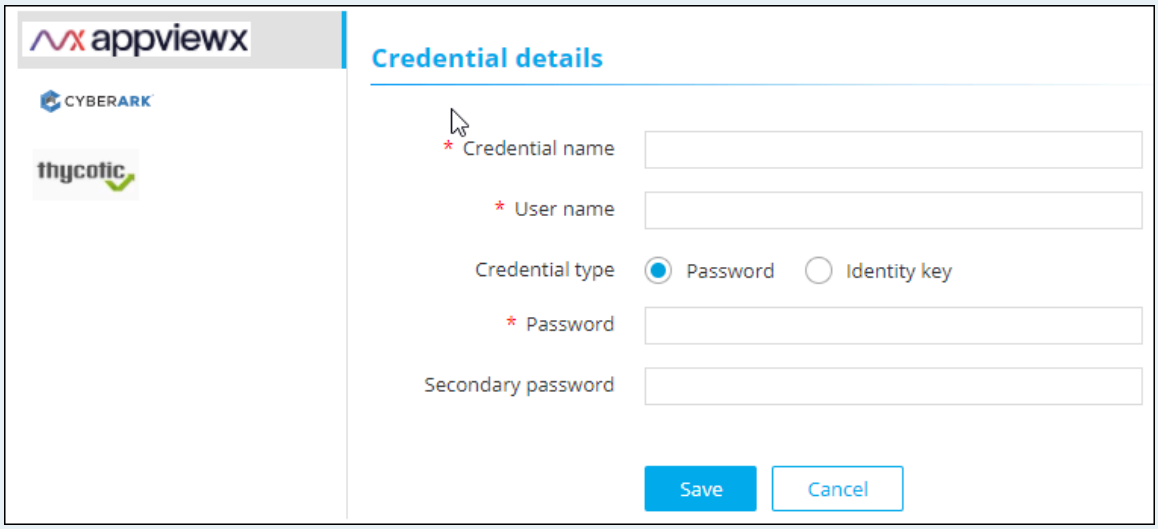
Chapter 4: Configuring Privileged Access Management

- AppViewX
- CyberArk
- Thycotic Secret

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.

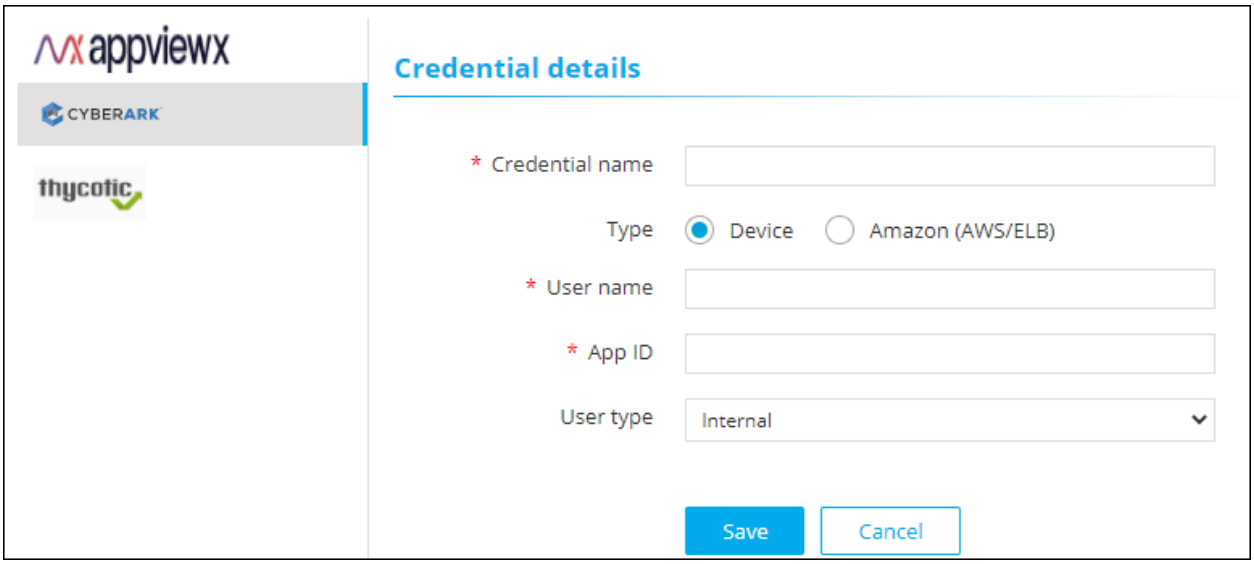


To configure credential details for the AppViewX vault, enter the following details:

Field	Description
Credential name*	Name for the credential for the users to identify it
User name*	User name used for device onboarding
Credential type	Select the type of authentication from one of the following:

Field	Description
	• Password • Identity key
Password*	**Note:** This field is displayed for the Password credential type Password configured at the time of device onboarding.
Secondary password	**Note:** This field is displayed for the Password credential type. Additional password enabled by vendors for specific operations.
Identity key*	**Note:** This field is displayed for the Identity key credential type. Credentials (private key in the .pem or the .txt format) for enabling device communication via SSH.
Passphrase	**Note:** This field is displayed for the Identity key credential type. Key to protect the private key files.

CyberArk

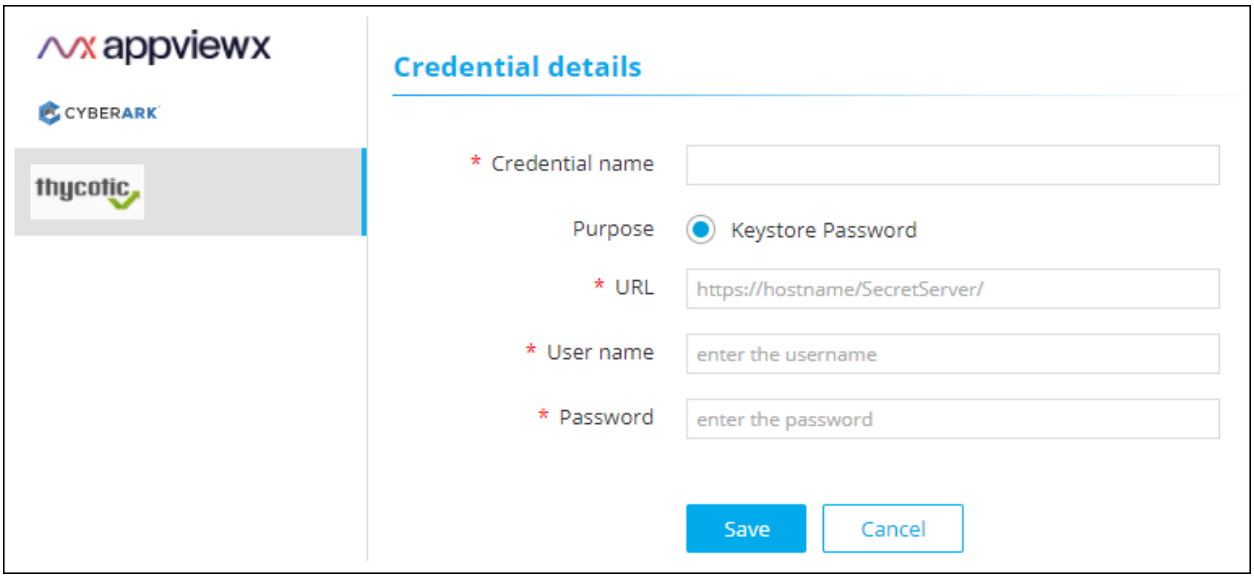


To configure credential details for the CyberArk vault, enter the following details:

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

Field	Description
	Note: This field is displayed when the Device type is selected.
User type	From the drop-down menu, select one of the following: • Internal (user created directly in the device) • External (user created in the Active Directory) **Note:** 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

Thycotic Secret



To configure credential details for the Thycotic vault:

1. Enter the following details:

Field	Description
Credential name*	Unique name for the credential for the users to identify it
Purpose	Enable/Disable the Keystore Password.
URL*	URL of the Thycotic Secret server
User name*	Username for accessing the Thycotic Secret server
Password*	Password for accessing the Thycotic Secret server

2. To save the credential details in the credential inventory, click Save.

Chapter 5: Configuring General Settings

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

Configuring the SMTP Settings

• Configuring the SMTP Settings for Google

• Configuring the SMTP Settings for Microsoft

Configuring the SMTP Settings for Google

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

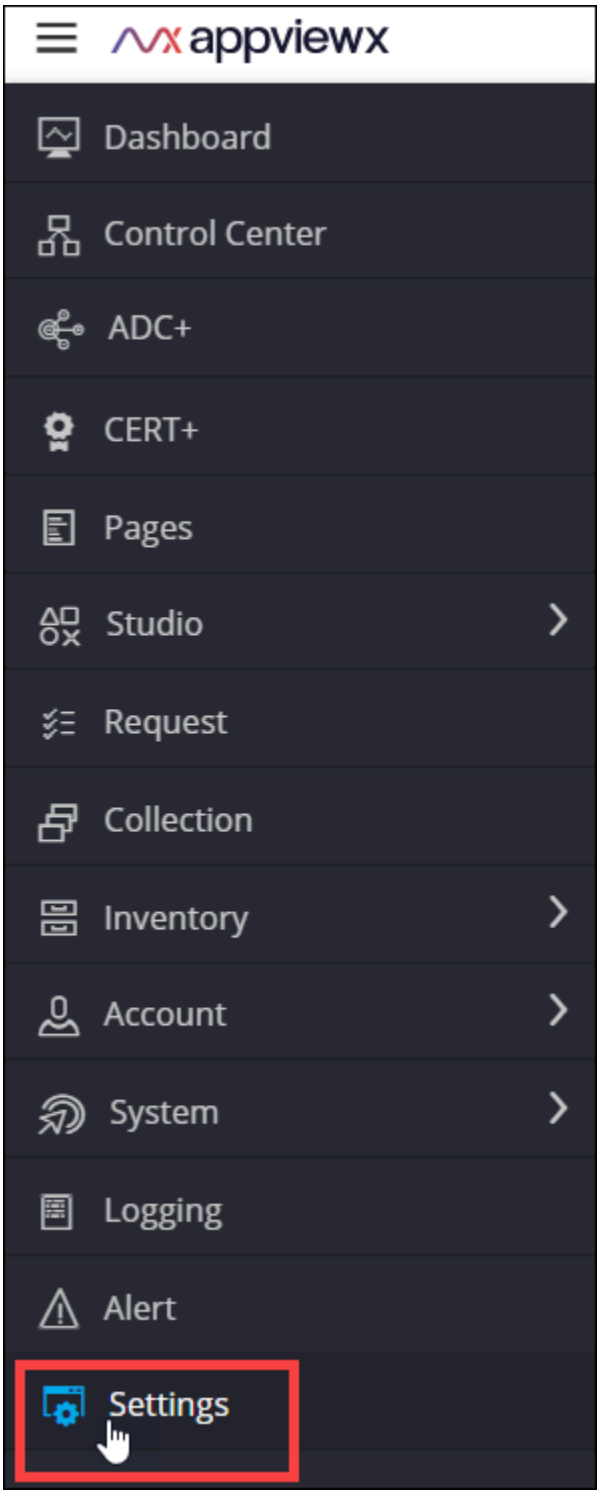
The SMTP oAuth uses an access token instead of a password to send email. The access token works as a temporary password with fixed validity and has permissions delegated by the user.

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

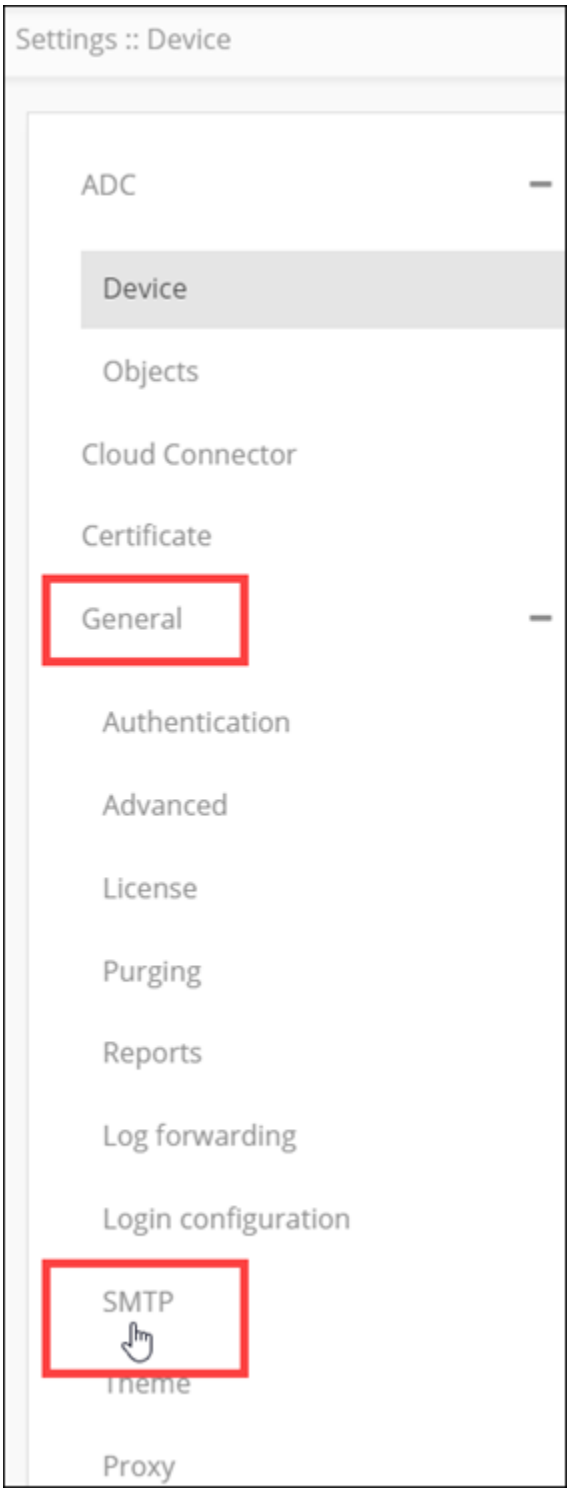
The Auth code is exchanged with the access token and refresh token in the backend and saved in DB.

To configure the SMTP server:

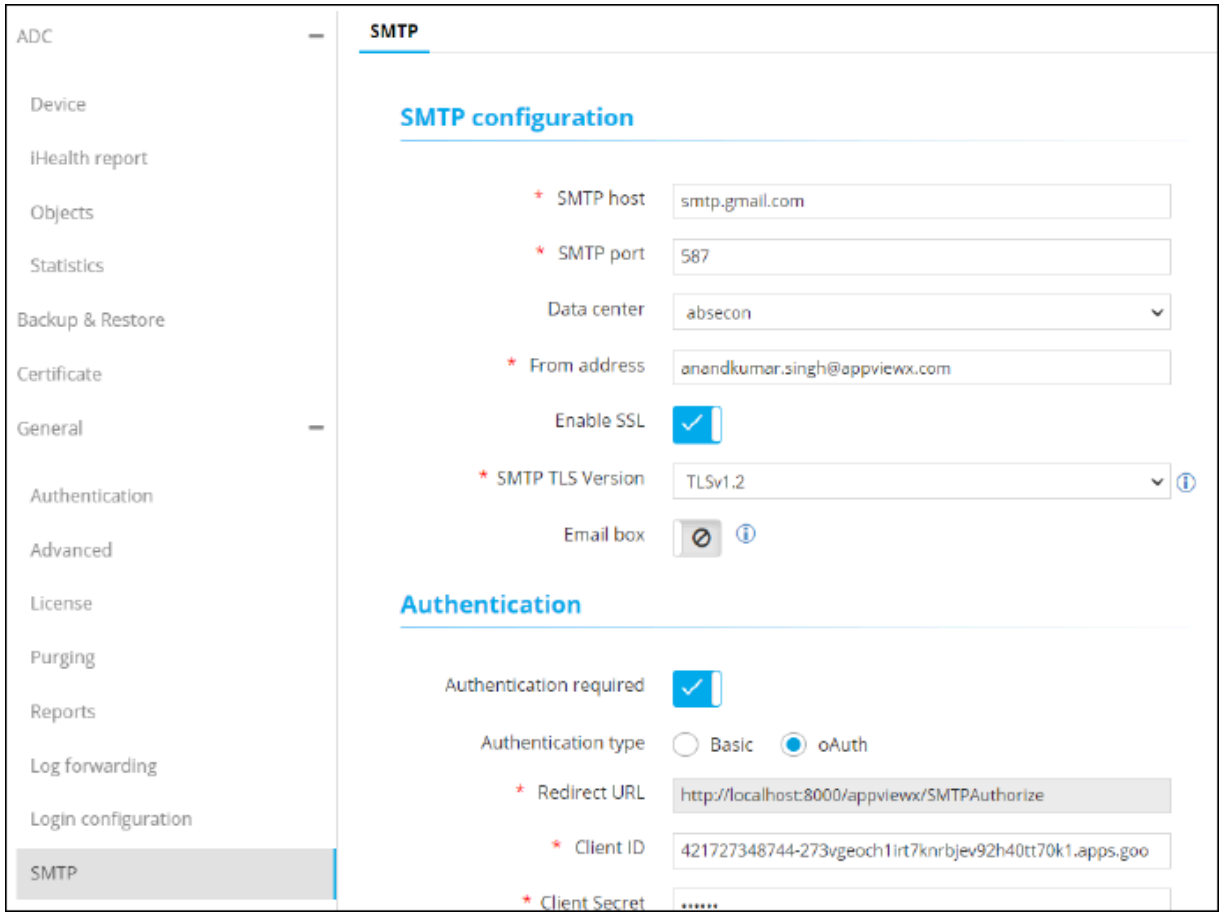
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Settings**.



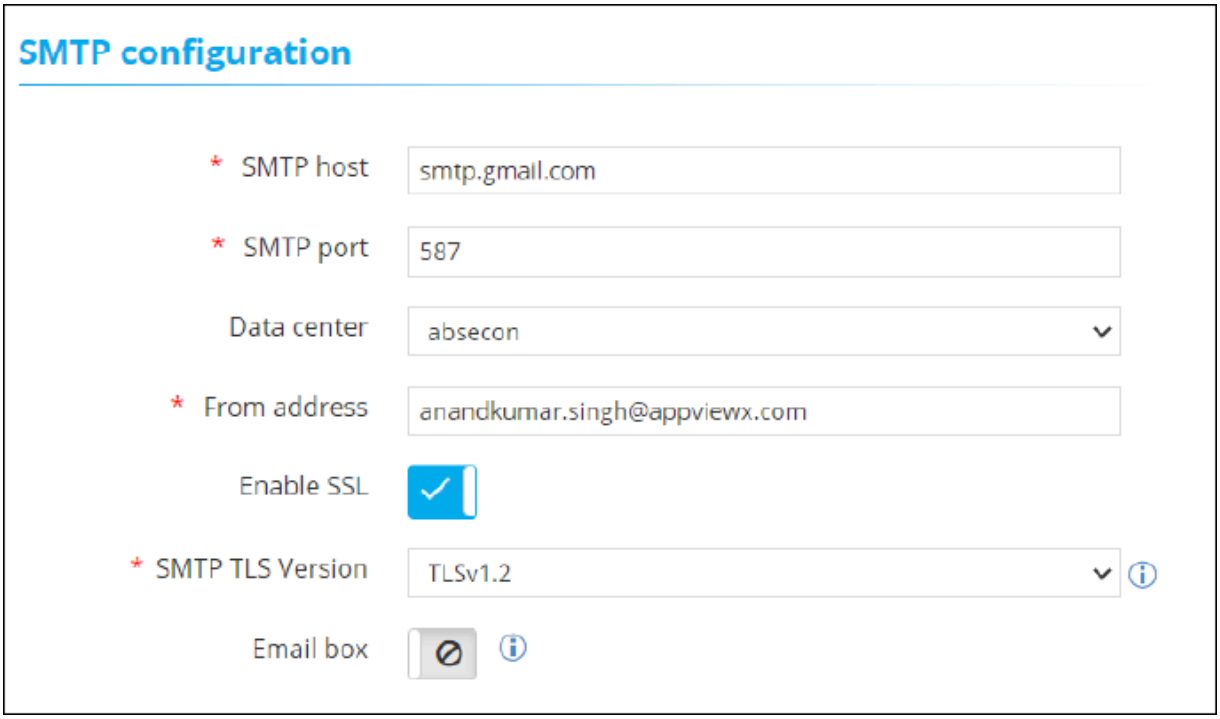
3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **SMTP**.



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



5. In the **SMTP configuration** section, enter the required field information.

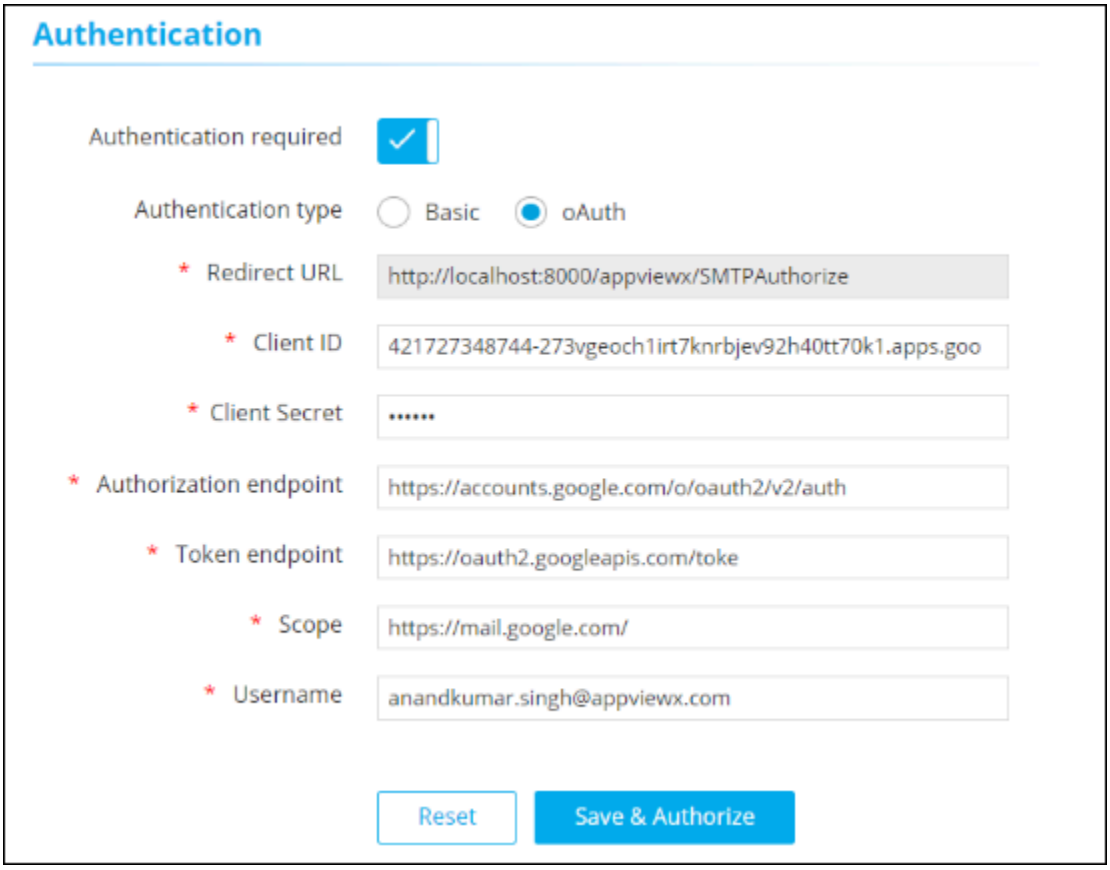


The following table describes the fields in this section:

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

Field	Description
	Note: This field is displayed only if the **Email box** key is enabled.
***Password**	Password of the IMAP server used for the mailbox feature. **Note:** This field is displayed only if the **Email box** key is enabled.
***Host name**	Host name of the IMAP server used for the mailbox feature. **Note:** This field is displayed only if the **Email box** key is enabled.
***Port**	Enter the Port number. **Note:** This field is displayed only if the **Email box** key is enabled.
All * marked fields are mandatory.	

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



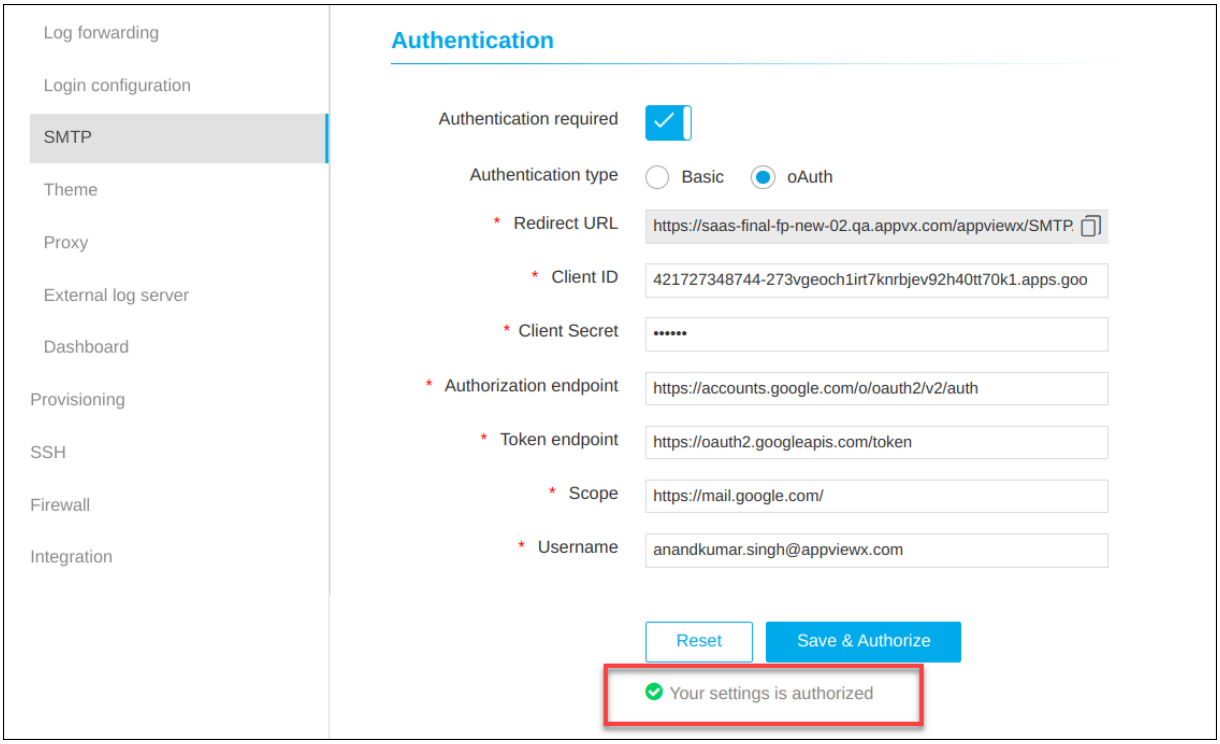
This table describes the fields in this section:

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

Field	Description
	For more information on steps for Google, click here. For more information on steps for Microsoft click here.
***Client Secret**	Enter the Client Secret that is generated in the oAuth server when the oAuth client is created.
***Authorization endpoint**	Enter the authorization endpoint where the user authorizes and gives permission to the oAuth client to send email on behalf of the user.
***Token endpoint**	Enter the token endpoint to get Access Token and Refresh Token. You can get the endpoint by providing Client ID, Secret, and other relevant values based on oAuth 2.0 specifications.
***Scope**	The permission required to send email. **Note:** For Google, enter **https://mail.google.com/**.
***Username**	**Note:** This field is enabled only if the **Authentication required** key is enabled. Username for the authenticated mail server
All * marked fields are mandatory.	

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

9. Displays confirmation of SMTP Settings Authorized.



A new tab opens asking for sign-in.

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

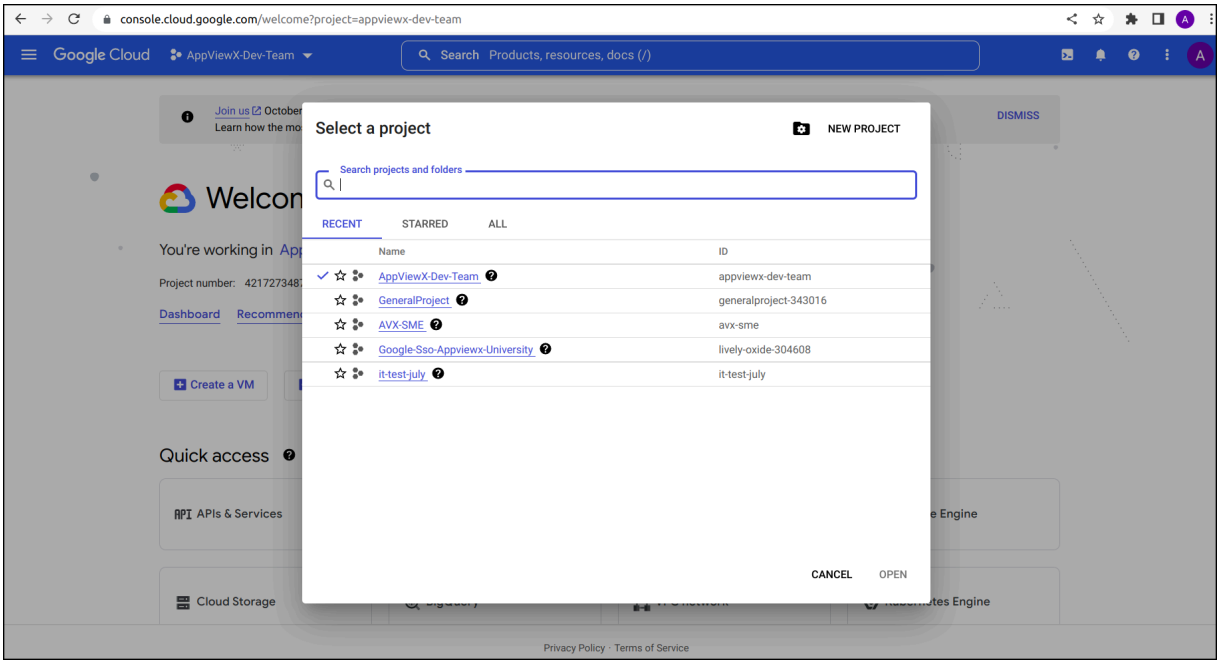
- Authentication for Google SMTP Settings

Authentication for Google SMTP Settings

Create authorization credentials

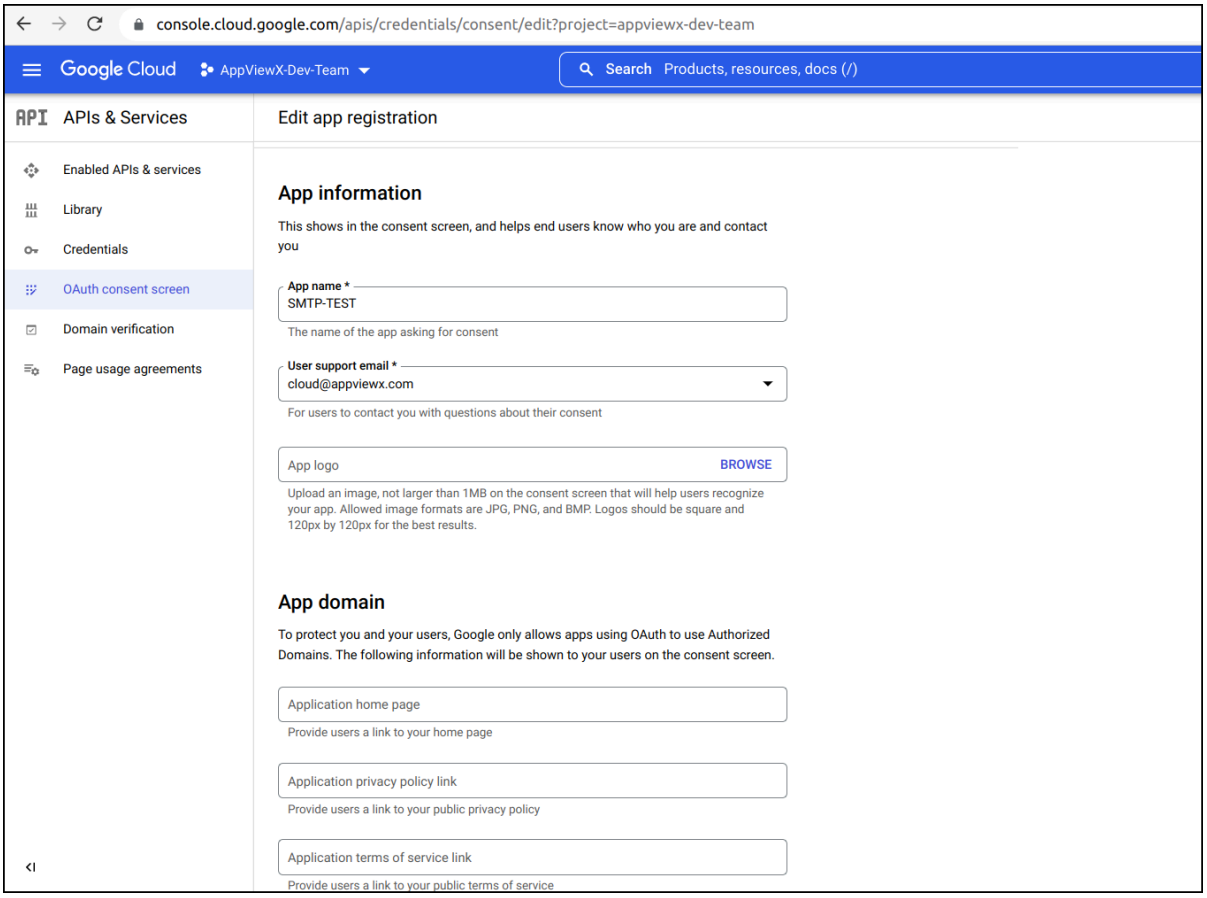
Any application that uses OAuth 2.0 to access Google APIs must have authorization credentials that identify the application to Google's OAuth 2.0 server. The following steps explain how to create credentials for your project. Your applications can then use the credentials to access APIs that you have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

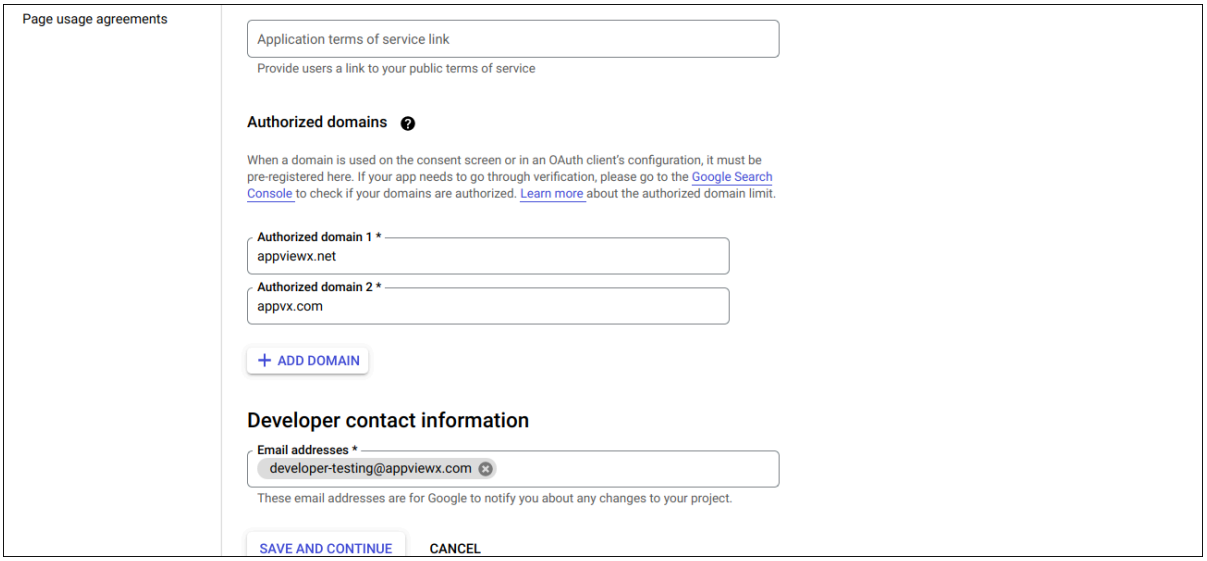
1. Google **App Registration** URL: https://console.cloud.google.com/.



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

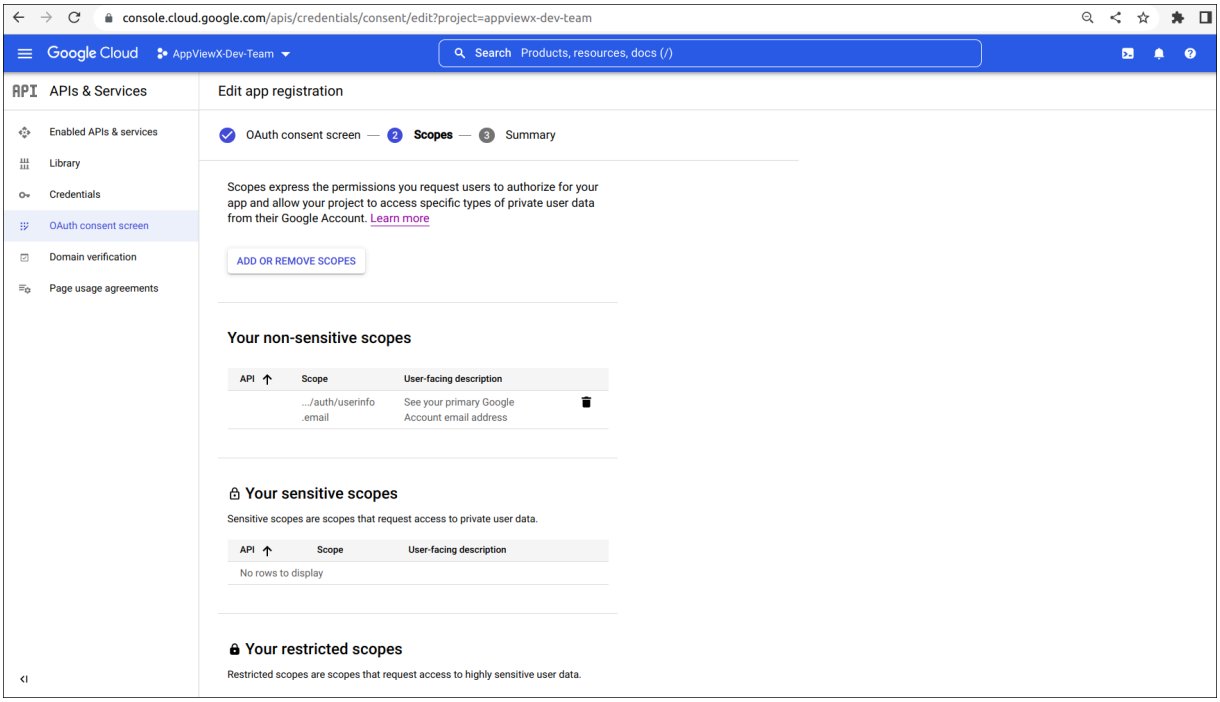
The **OAuth consent screen:: App information** page is displayed.





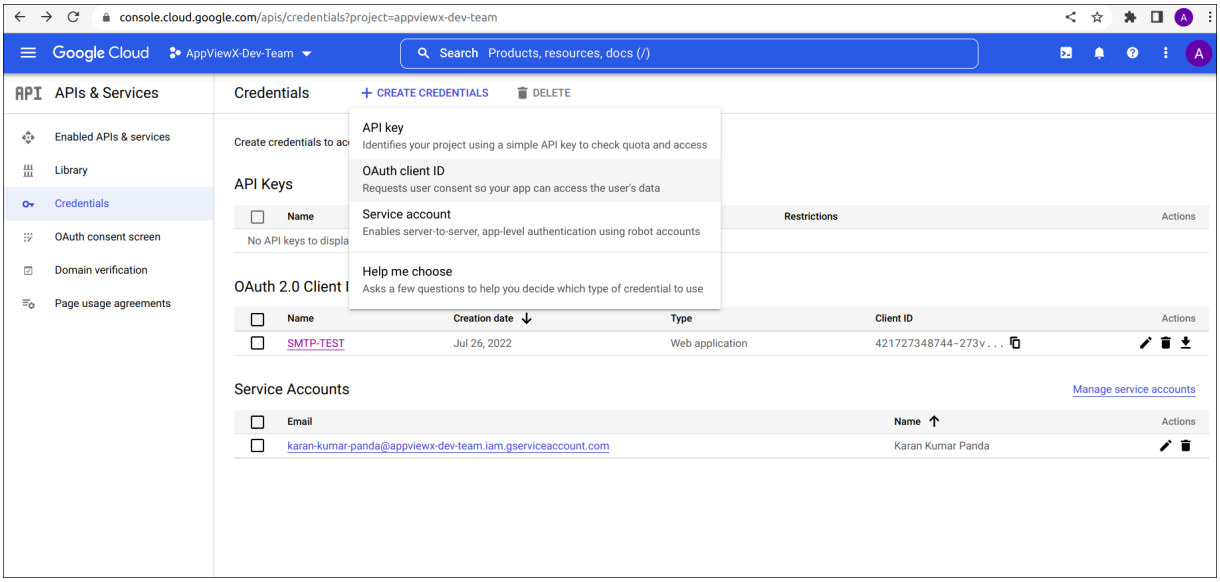
4. In the **App information** section, enter the required field information. **App name***, **User support email***, **Authorized domains**, **and Developer contact information**, then click **Save & Continue**.

The **Save & Continue :: Scopes** page is displayed.



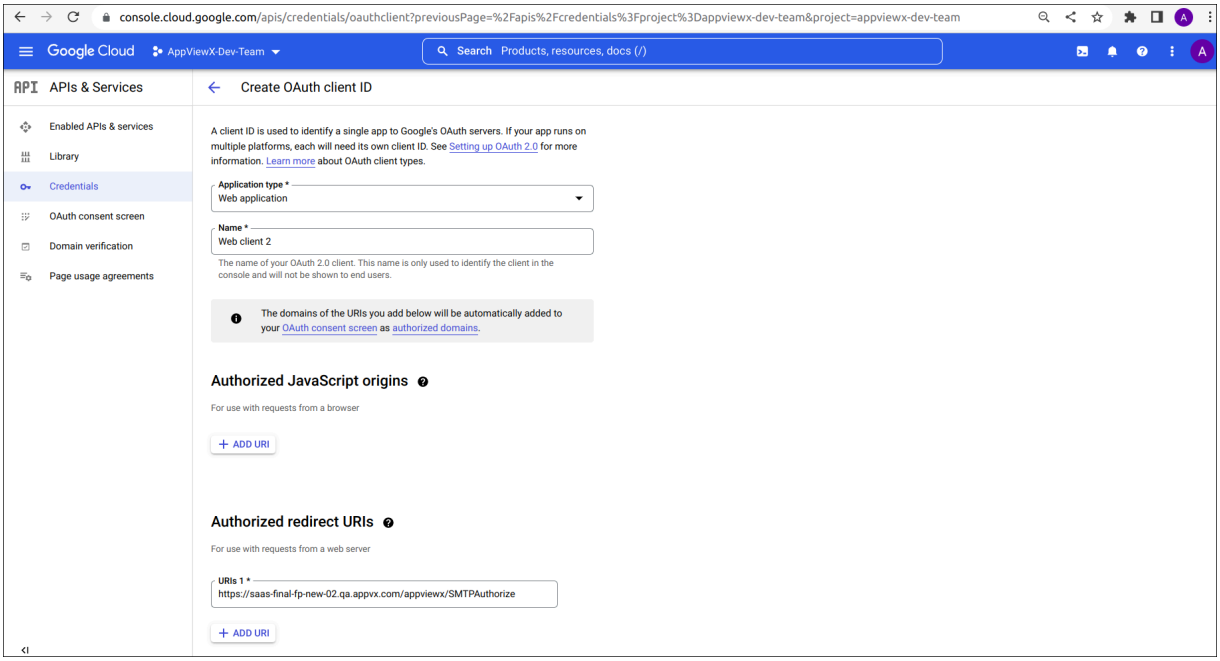
5. Under **Scopes** section, **ADD SCOPES** required information.
6. In the sidebar hover the mouse pointer over the "APIs & Services", click **Credentials**.

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

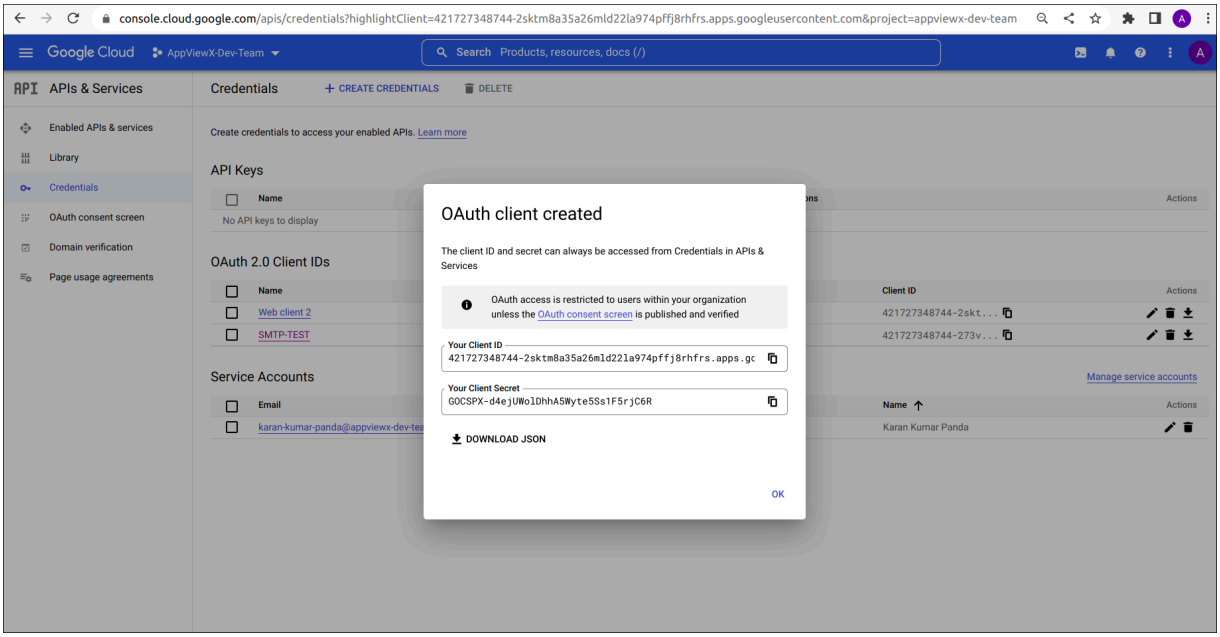


7. In the **Credentials** tab, click the **+CREATE CREDENTIALS,** from the drop-down list, choose **OAuth client ID**.

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



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



10. Copy the **Client ID** and **Client Secret** for Authentication of SMTP Server Settings.
11. Authorization endpoint URL: https://accounts.google.com/o/oauth2/v2/auth.
12. Token endpoint URL: https://oauth2.googleapis.com/token.

Configuring the SMTP Settings for Microsoft

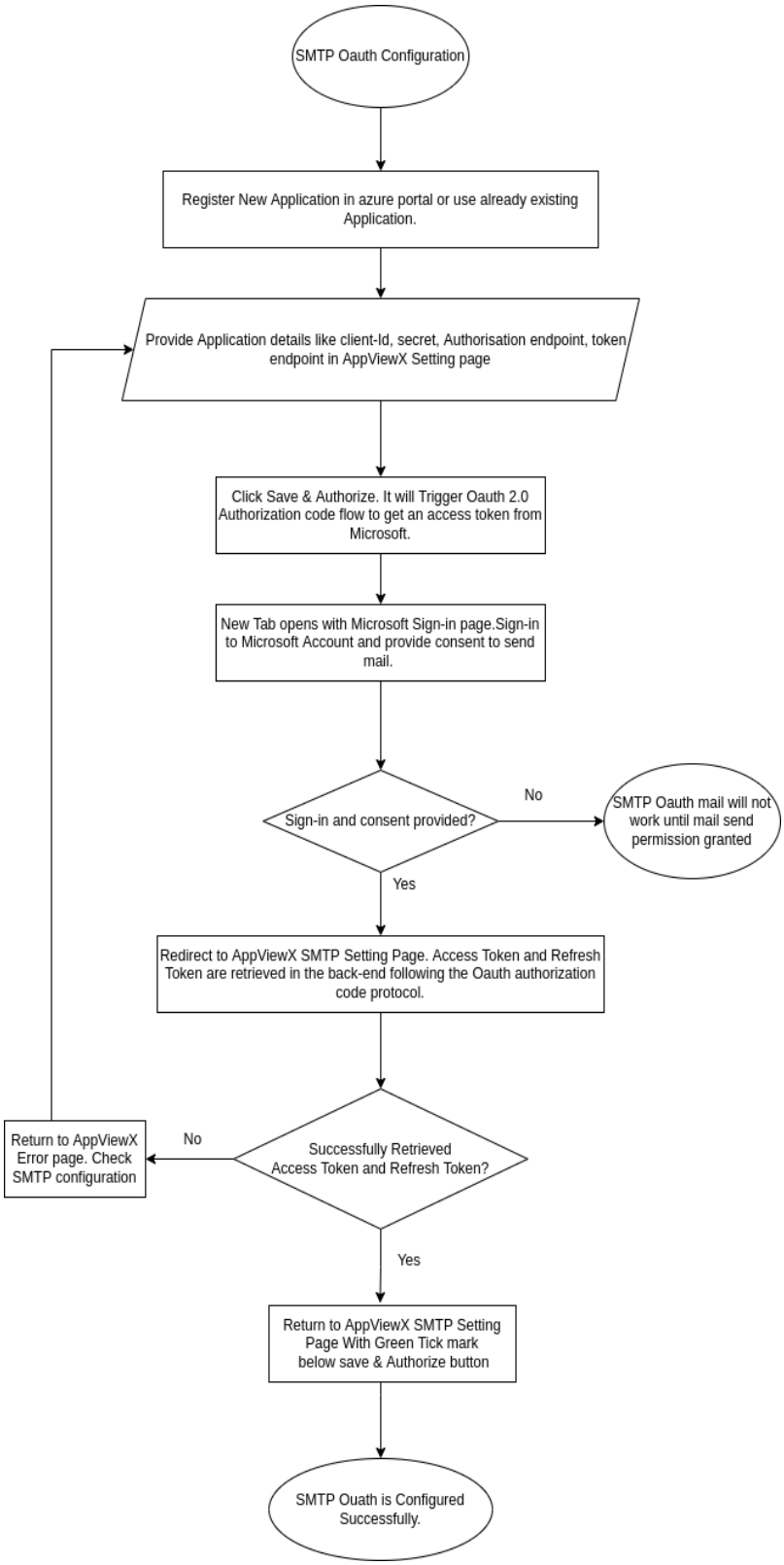
The SMTP configuration is required for AppViewX to be able to send logs and alerts via email and for other email related activities such as sending and receiving notifications and so on.

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

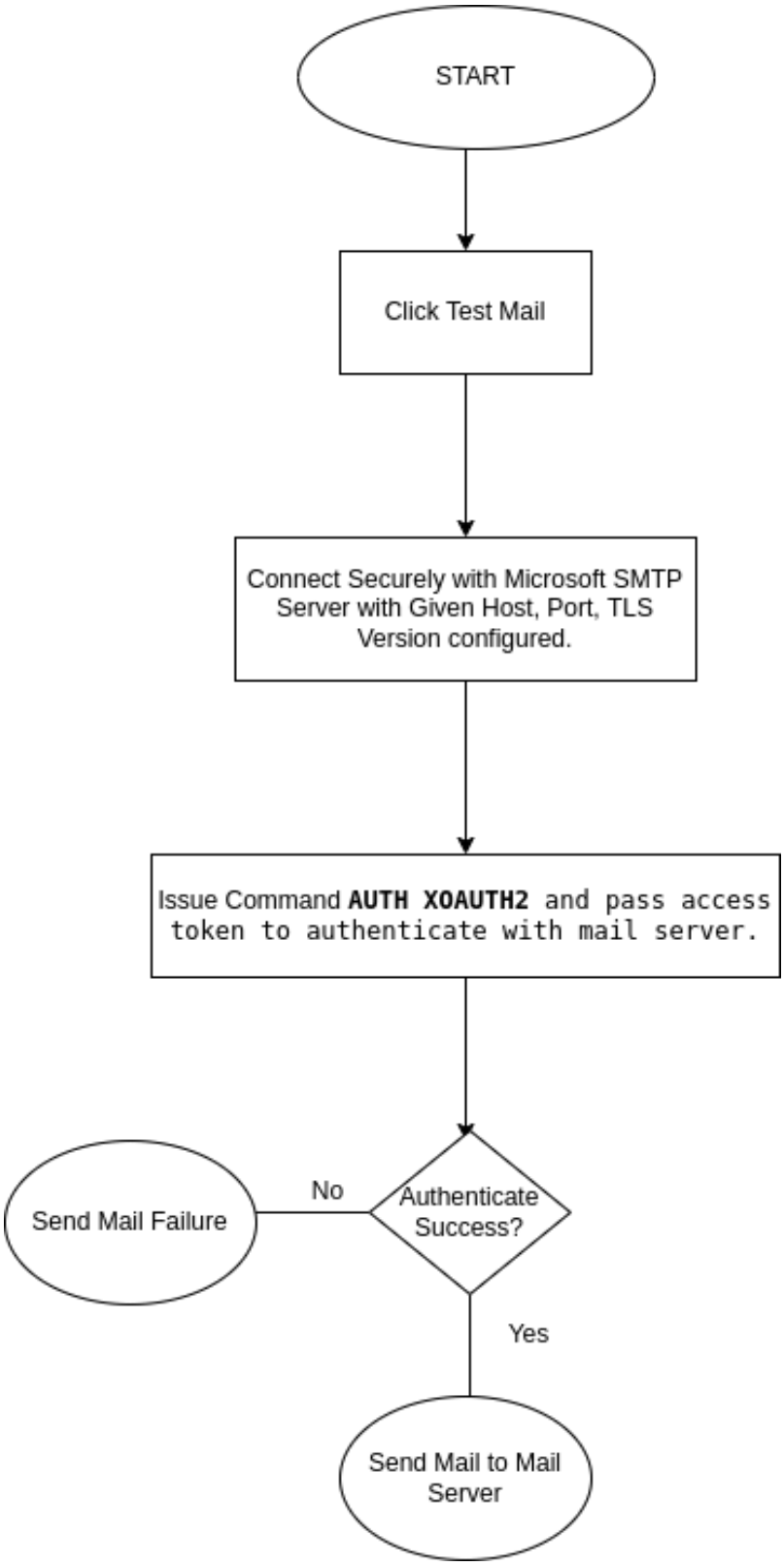
To get the access token you must provide details such as username, client-id, secret, Authorization endpoint, token Endpoint and scope. Once these details are submitted, you will be redirected to the oAuth server login page. Once the user authorization is done here, the oAuth server returns the Auth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

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

Flow Chart for SMTP Oauth Configuration.

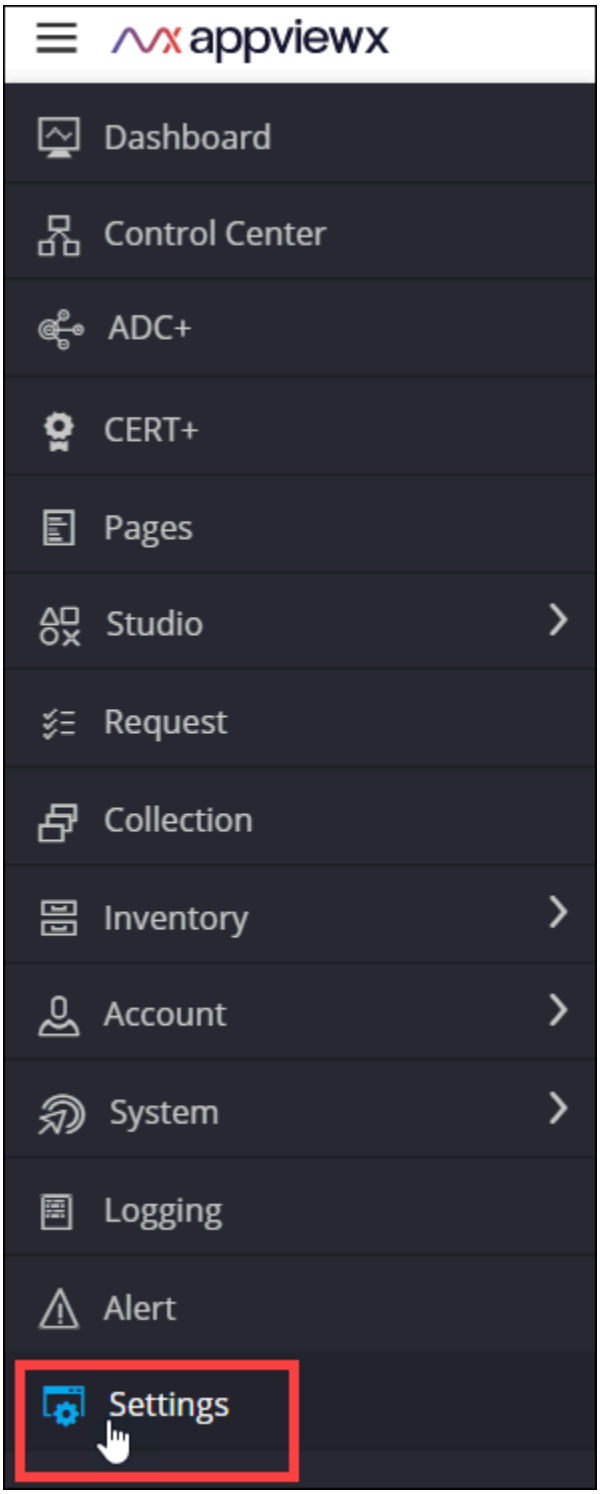


Flow Chart for Test Mail.

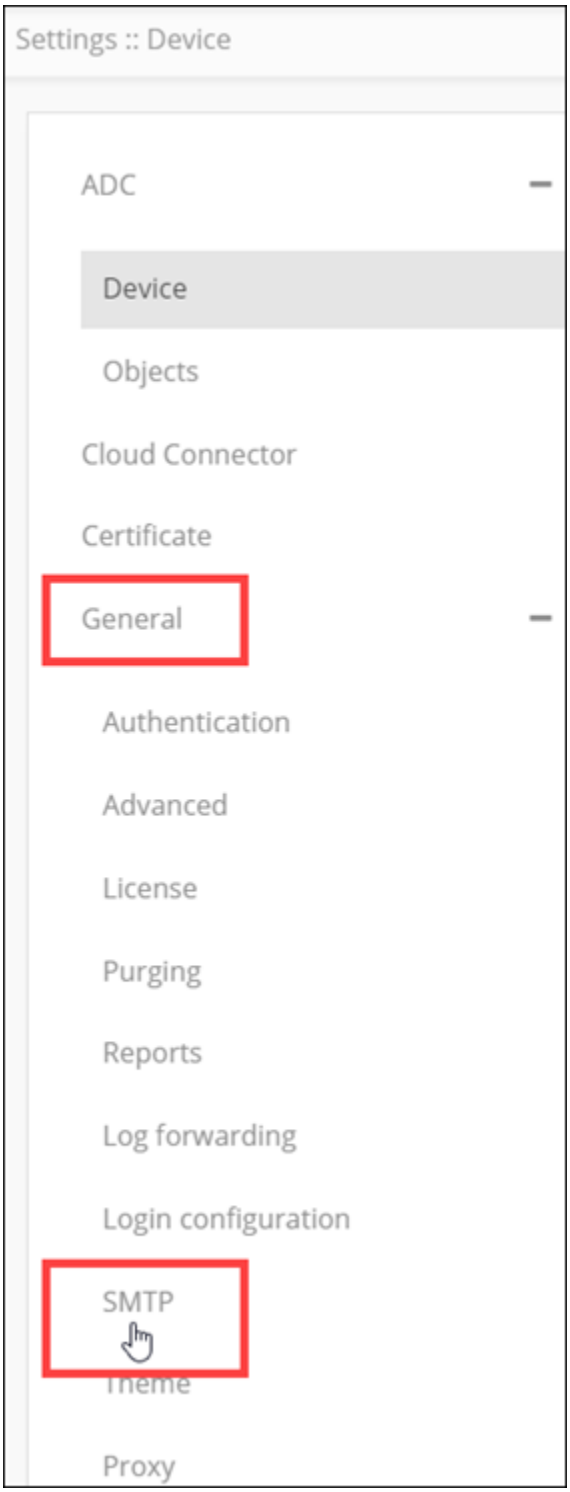


To configure the SMTP server:

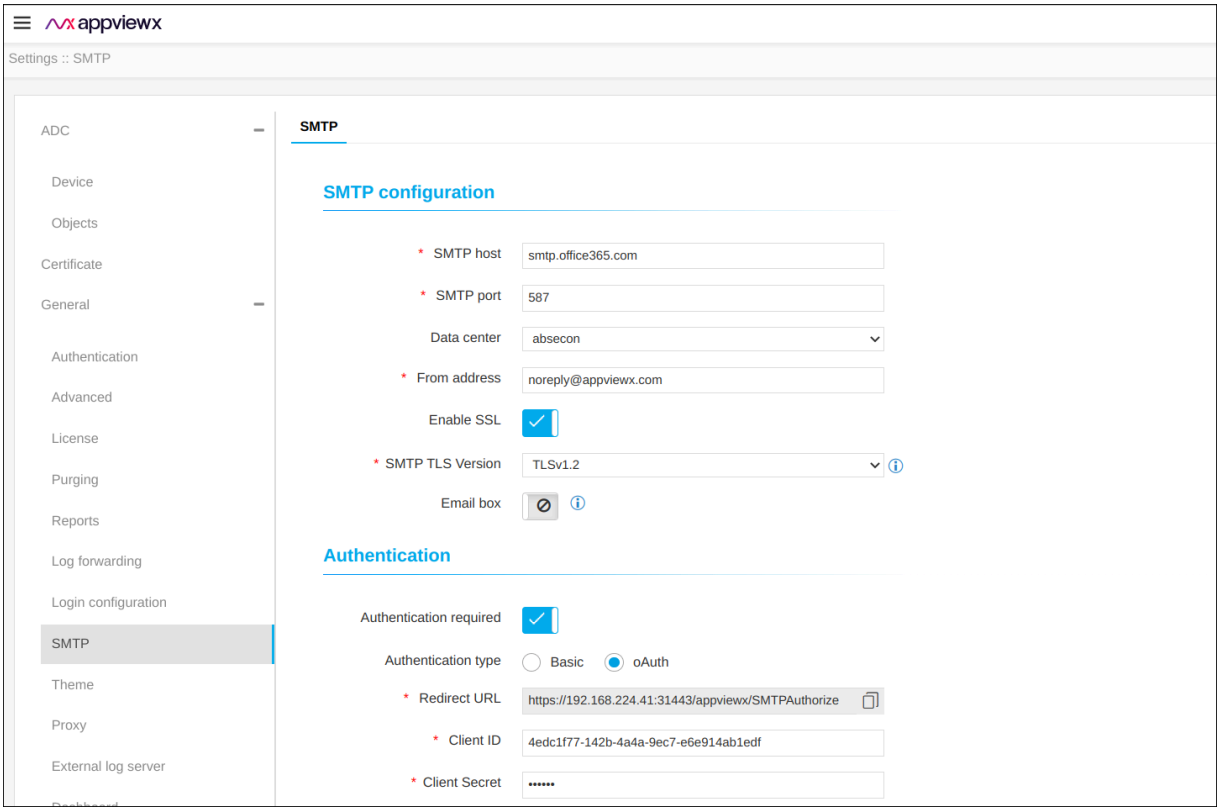
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click **Settings**.



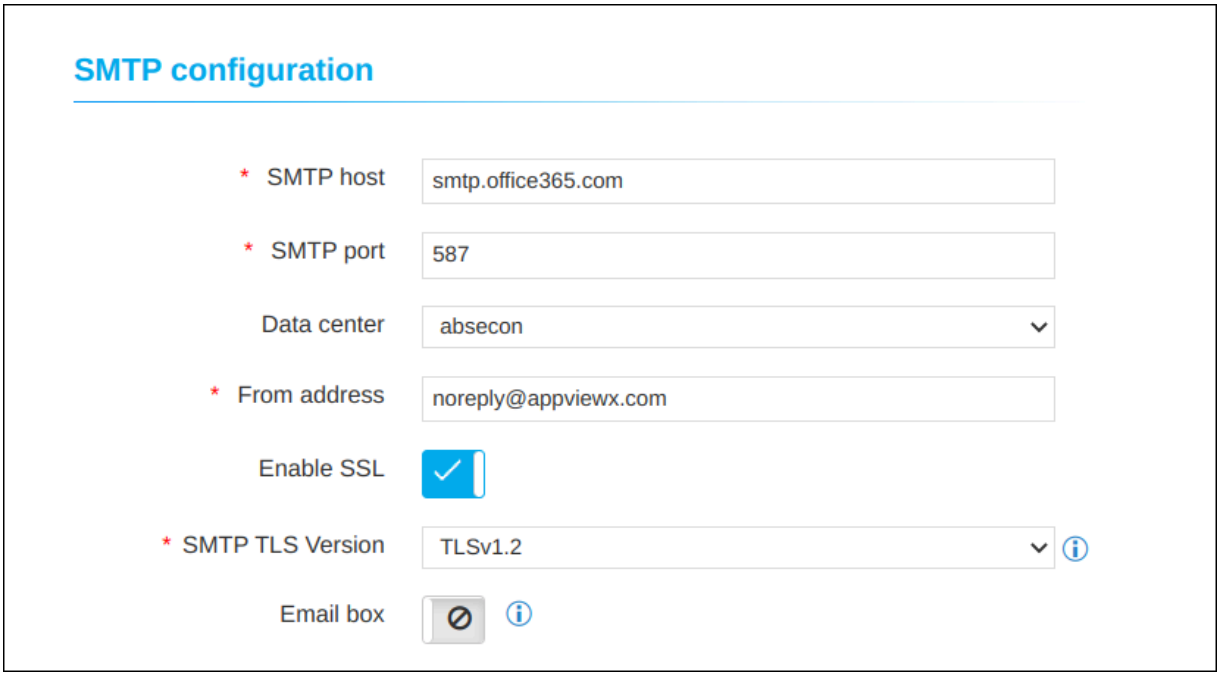
3. On the **Settings** page, from the navigation pane on the left, click **General**.
4. Under **General** settings, click **SMTP**.



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



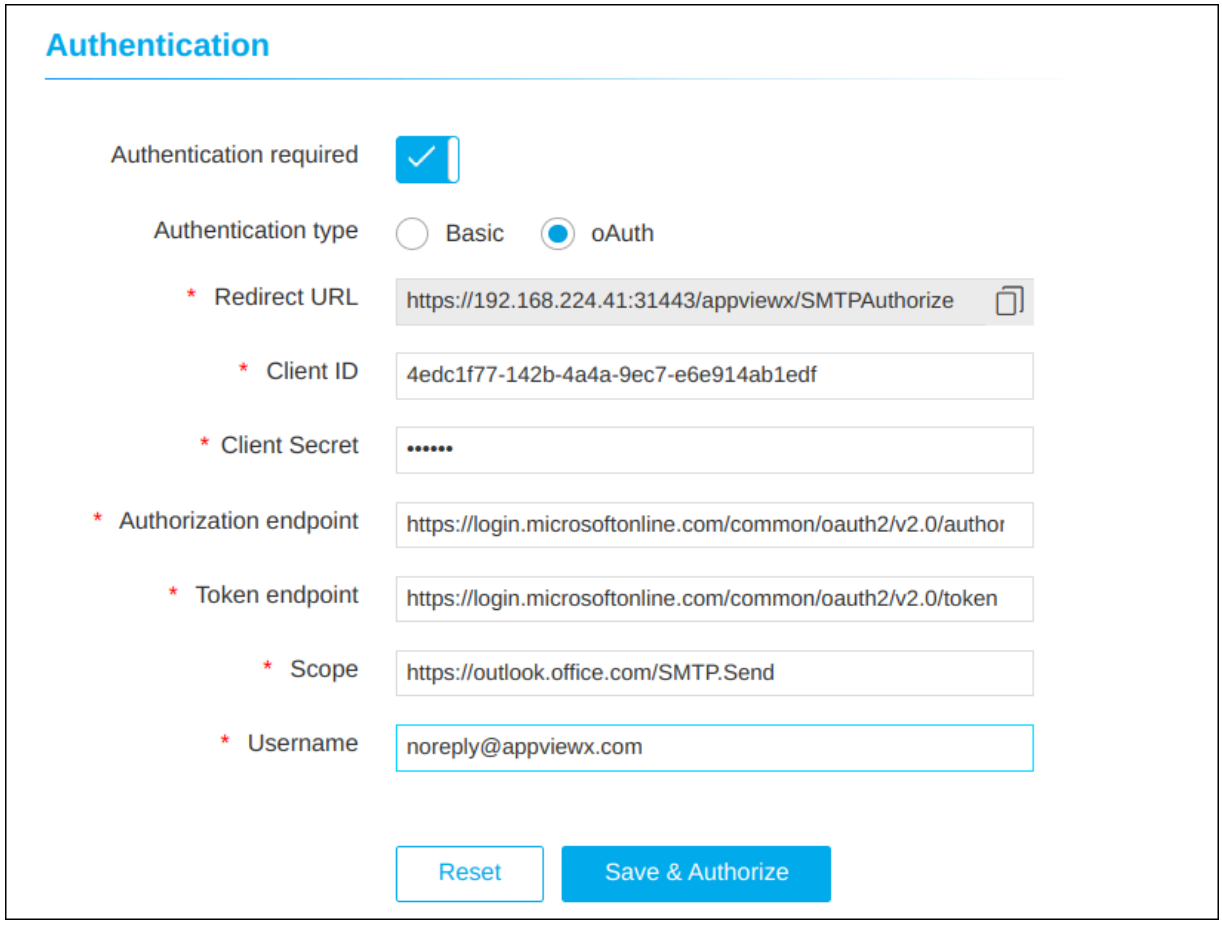
5. In the **SMTP configuration** section, enter the required field information.



The following table describes the fields in this section:

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

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



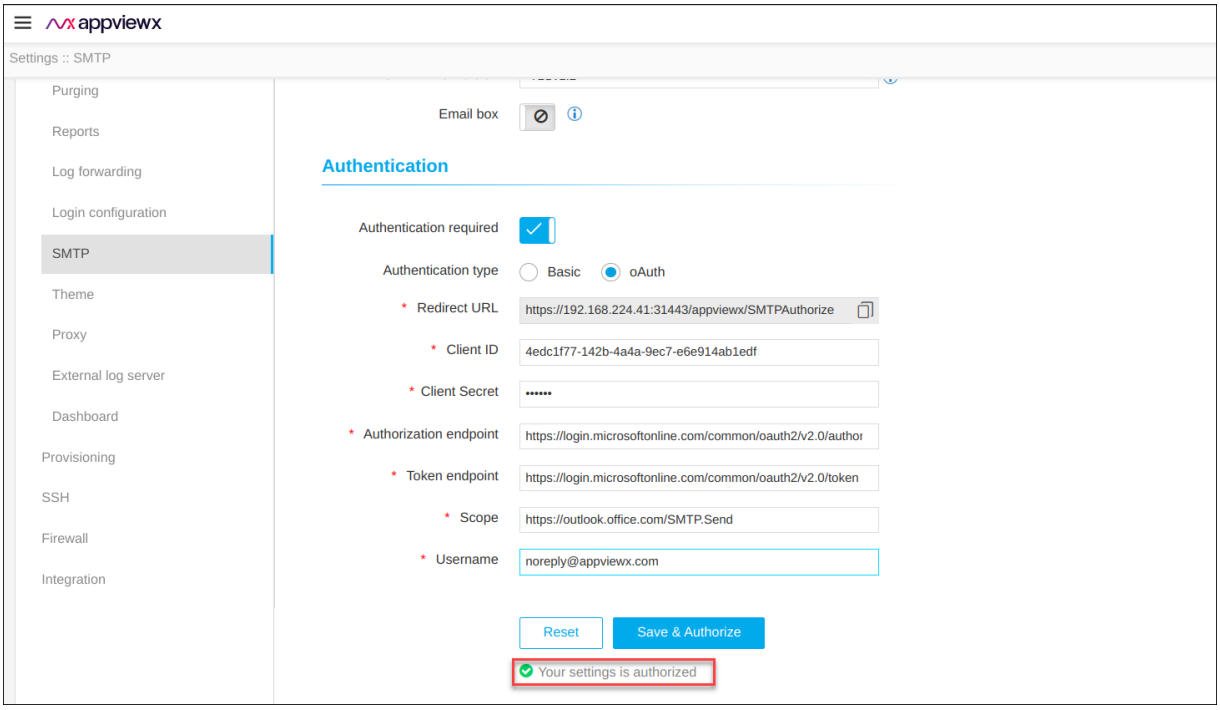
This table describes the fields in this section:

Field	Description
Authentication required	To enable authenticated mail server communication, enable this toggle.
Authentication type	Select the Authentication type as oAuth. **Note:** Selecting oAuth displays the fields that are described below. SMTP oAuth method to send email, we can't use a different address in From field. The sending address must be the same with the authenticated account.
***Redirect URL**	This field is auto-populated from the address bar of the browser.
***Client ID**	Enter the Client ID that is generated in the oAuth server when the oAuth client is created.

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

7. In the **Test email** section, enter the email address to which a test email should be sent and click **Test**.
8. To save the SMTP configuration settings, click **Save & Authorize**.
9. New Tab is opened for Single Sign On (SSO) with microsoft.
10. Provide your login credentials and submit your consent for the mentioned permissions. The login credential should be the same as the username configured in the SMTP Authentication.

11. Displays confirmation of SMTP Settings Authorized.



12. AppViewX can send an Email on behalf of the authorized user as the user has given the consent to send Email on his behalf during Authentication.

    A new tab opens asking for sign-in.

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

- Authentication for Microsoft SMTP Settings
- Frequently Asked Questions

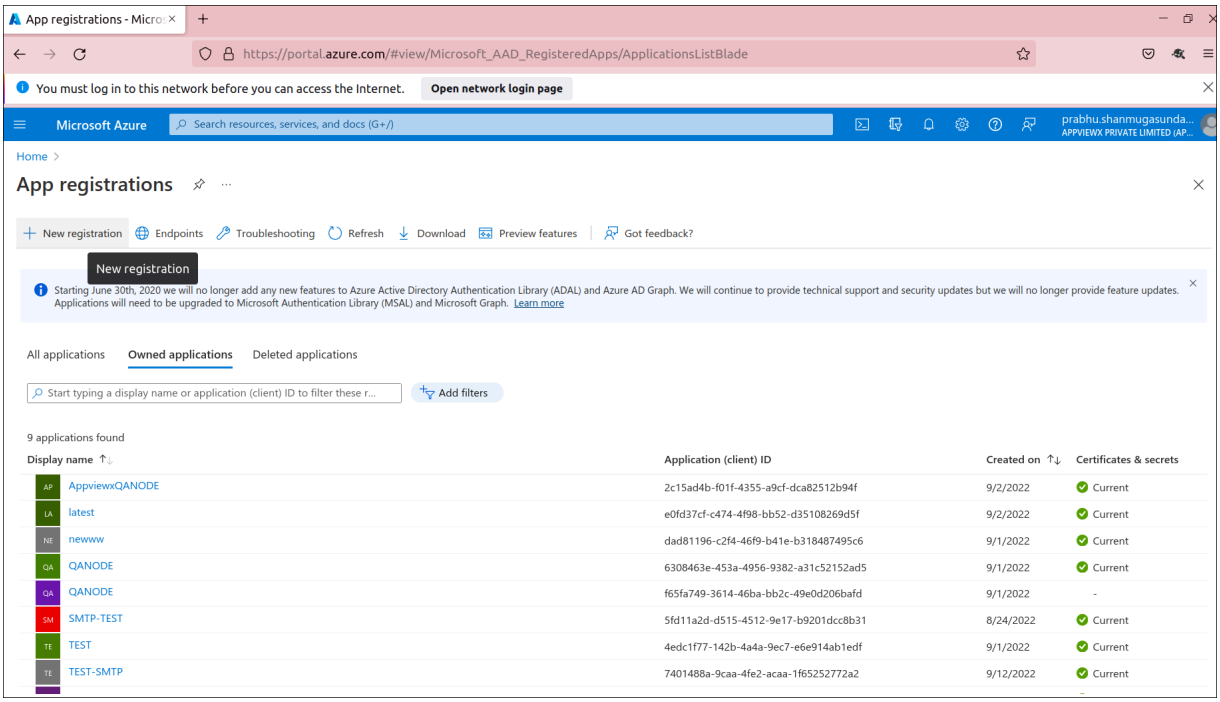
Authentication for Microsoft SMTP Settings

Create authorization credentials

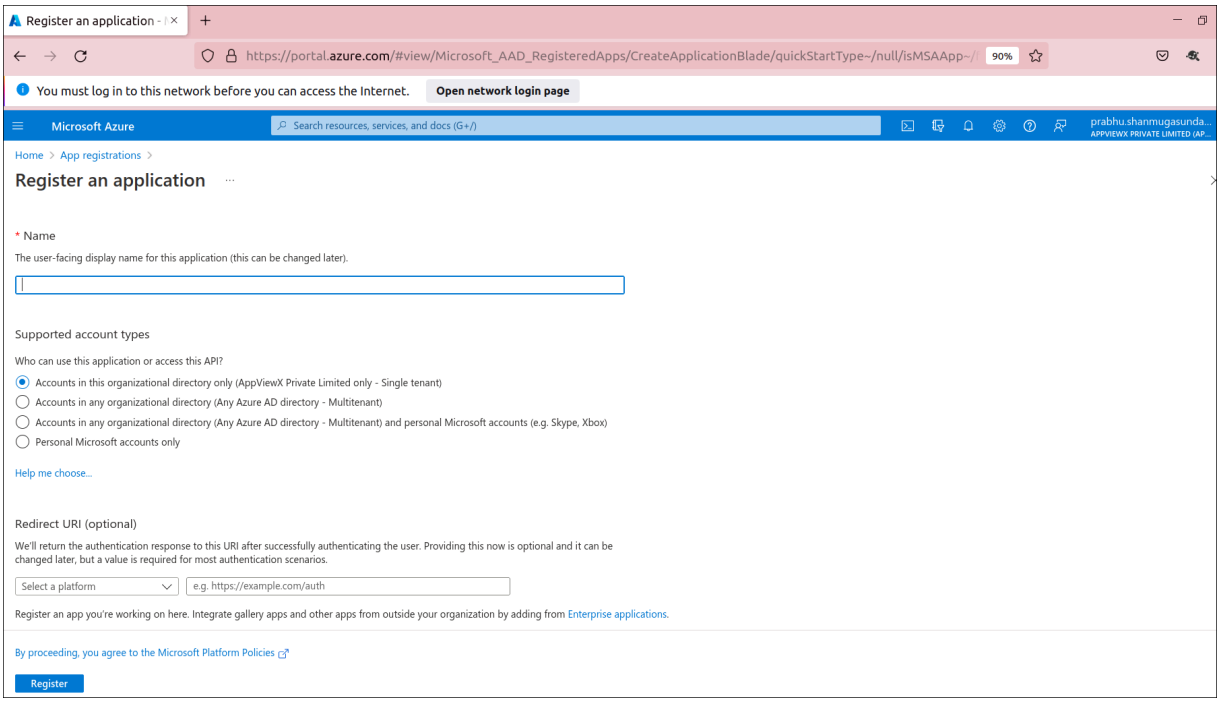
Registering your application establishes a trust relationship between your app and the Microsoft identity platform. The trust is unidirectional: your app trusts the Microsoft identity platform, and not the other way around.

Follow these steps to create the app registration:

1. Microsoft App Registration URL: https://portal.azure.com/.
2. Under **Manage**, click **App registrations** > **New registration**.

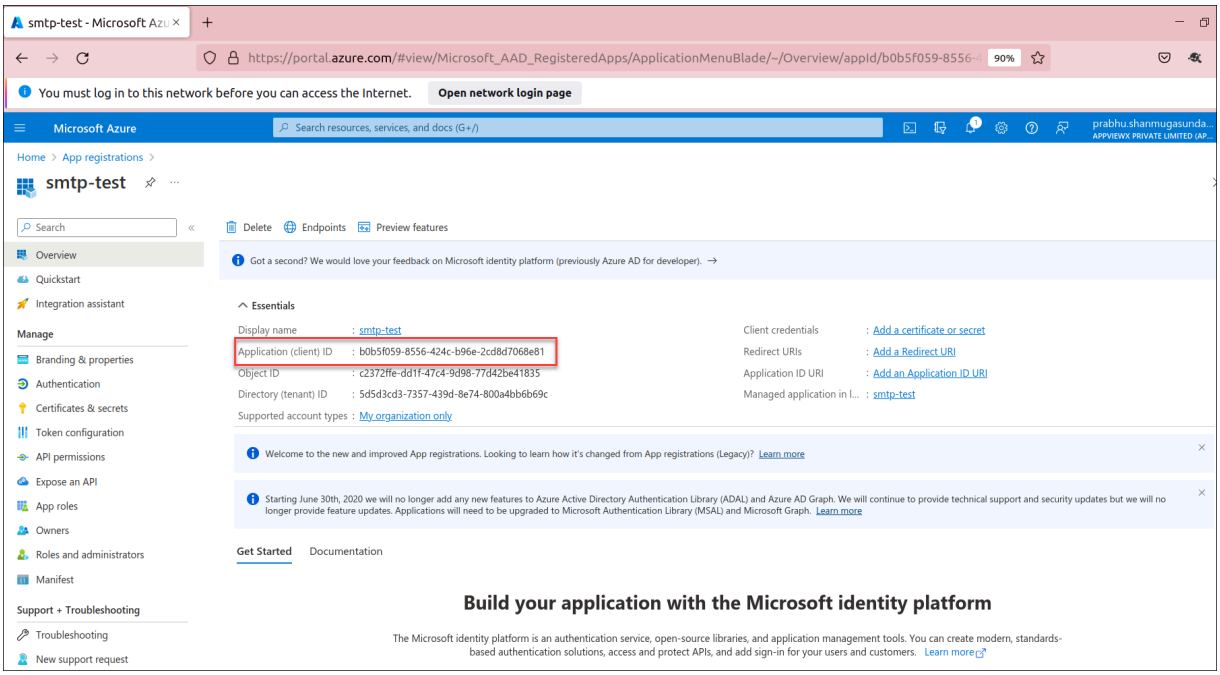


3. In the **Register an Application** section, enter the required field information.

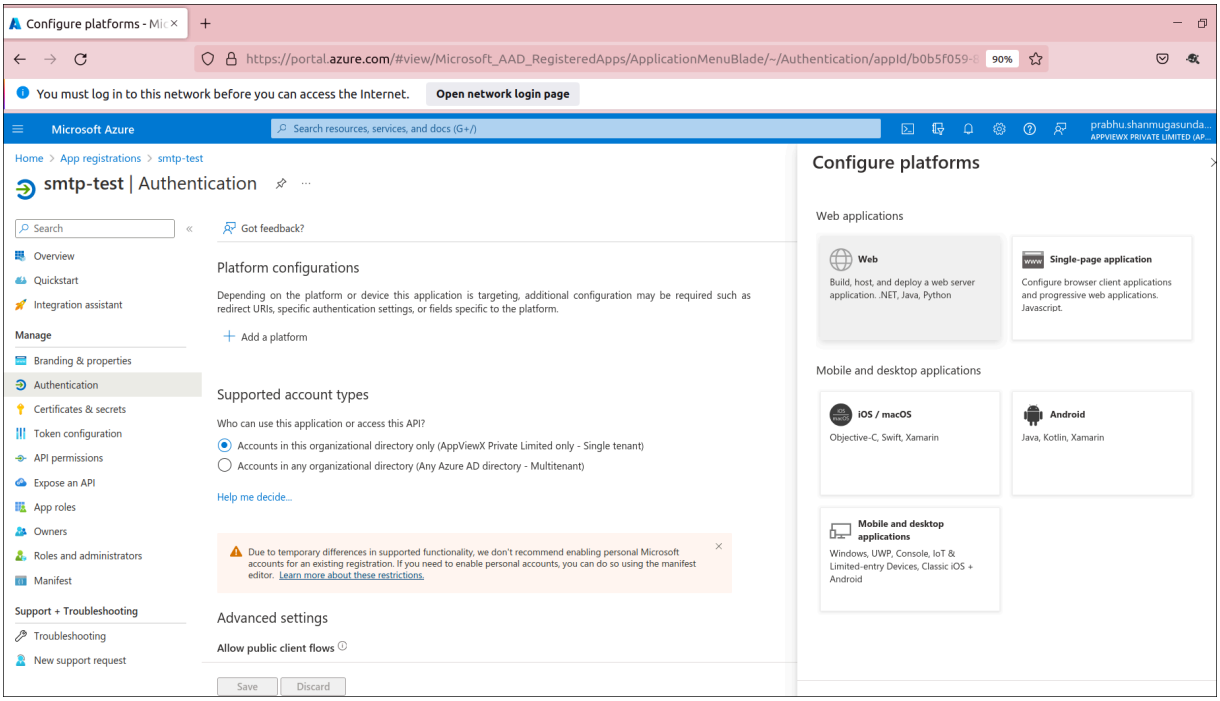


4. Click **Register** to complete the initial app registration.

5. When registration finishes, the Azure portal displays the app registration's Overview pane. You see the **Application (client) ID**.

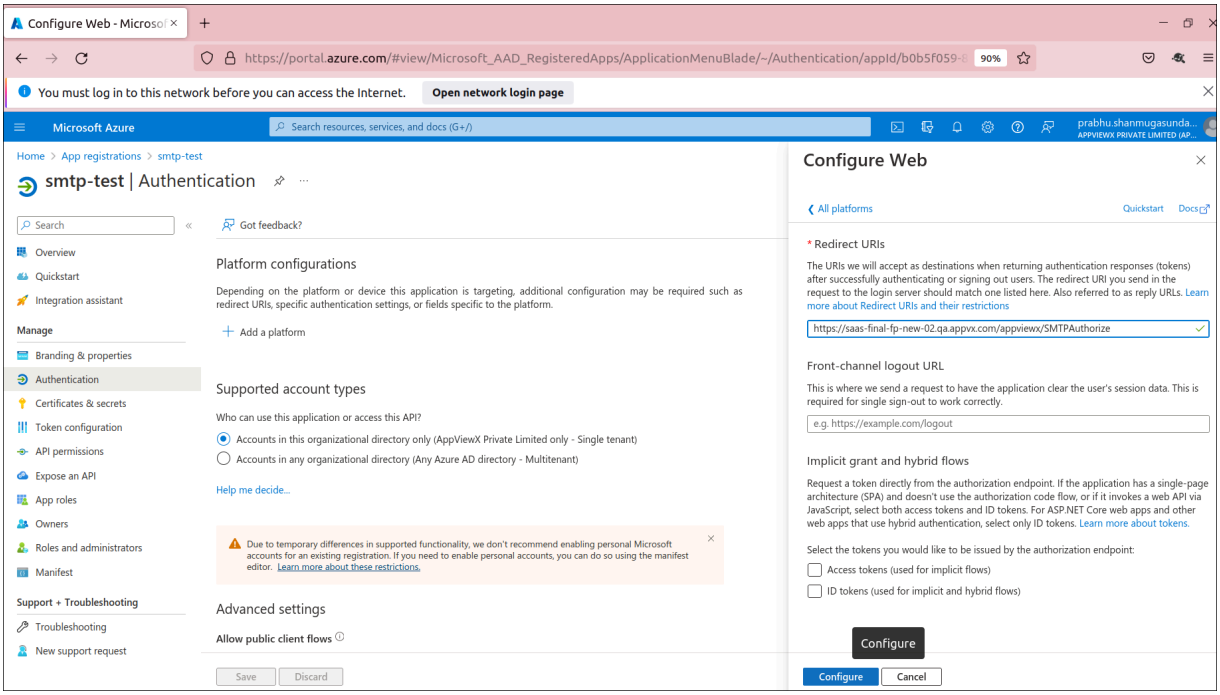


6. Under **Manage**, select **Authentication**.
7. Under **Platform configurations**, select **Add a platform**.

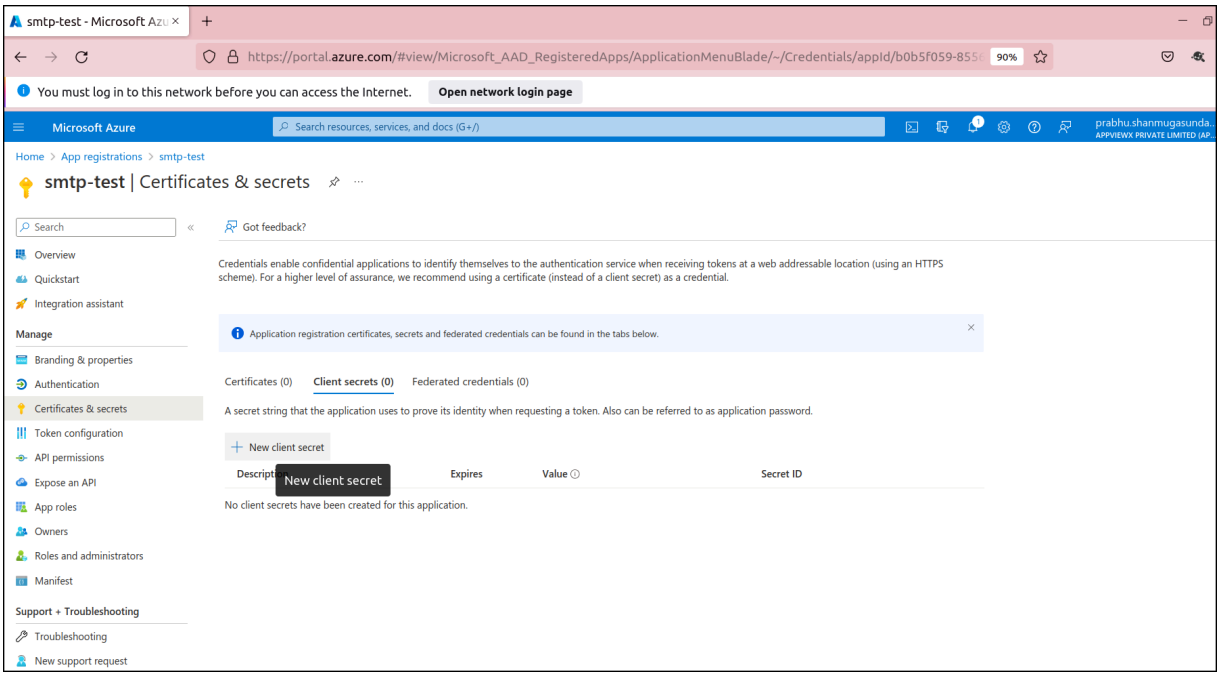


8. Under **Configure platforms**, select **Web** for application type (platform) to configure its settings.

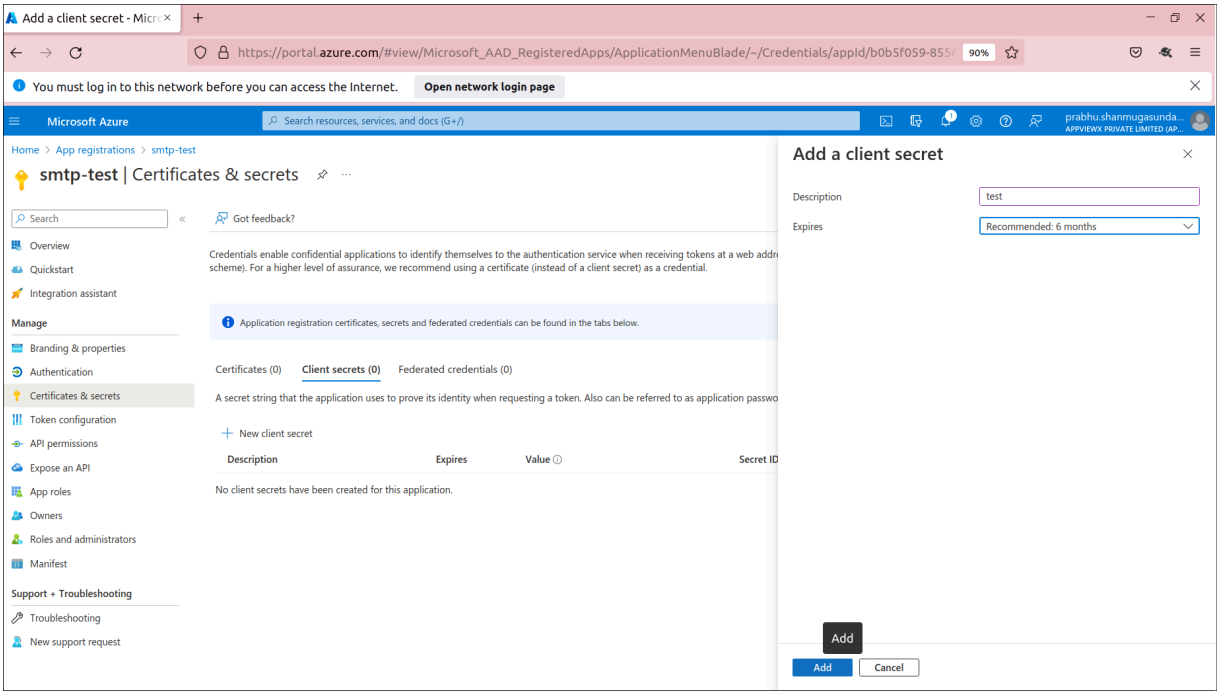
The **Redirect URI :: Configure Web** page is displayed.



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

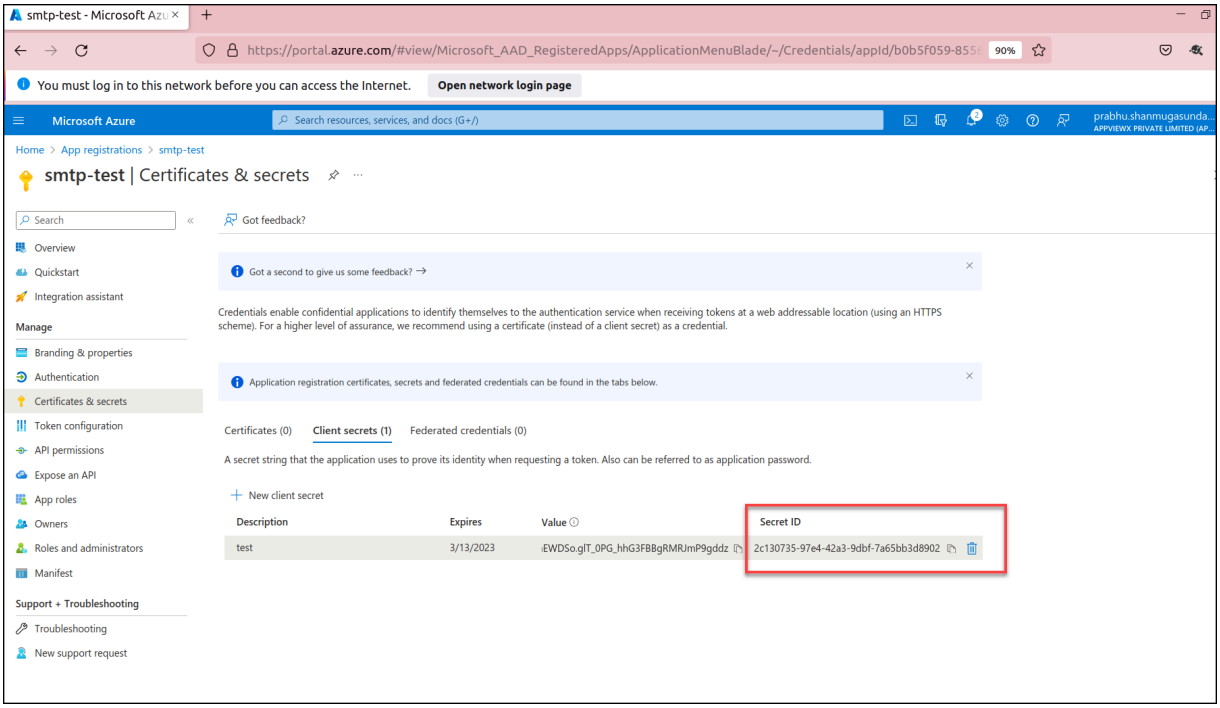


The **New client secret :: Add a client secret** page is displayed.



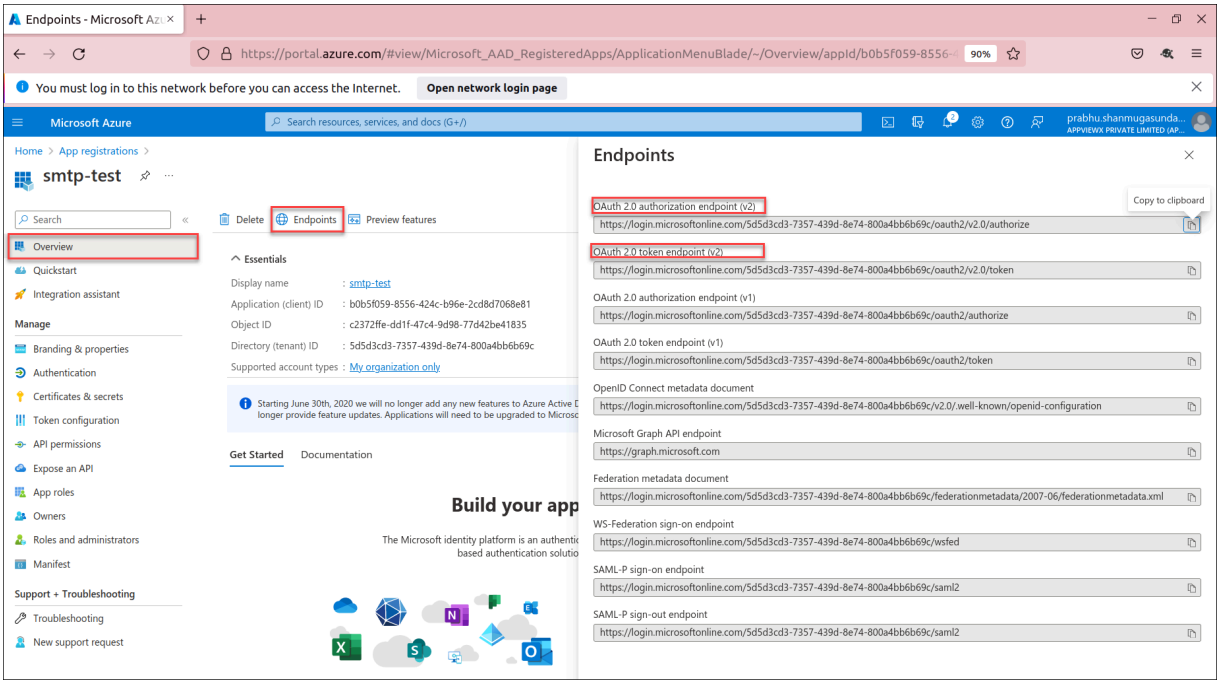
12. Add a **Description** for your client secret.
13. Select an **Expiration** for the secret or specify a custom lifetime.
14. Click **Add**.
15. Record the **Secret value** for use in your client application code.

    This secret value is never displayed again after you leave this page.



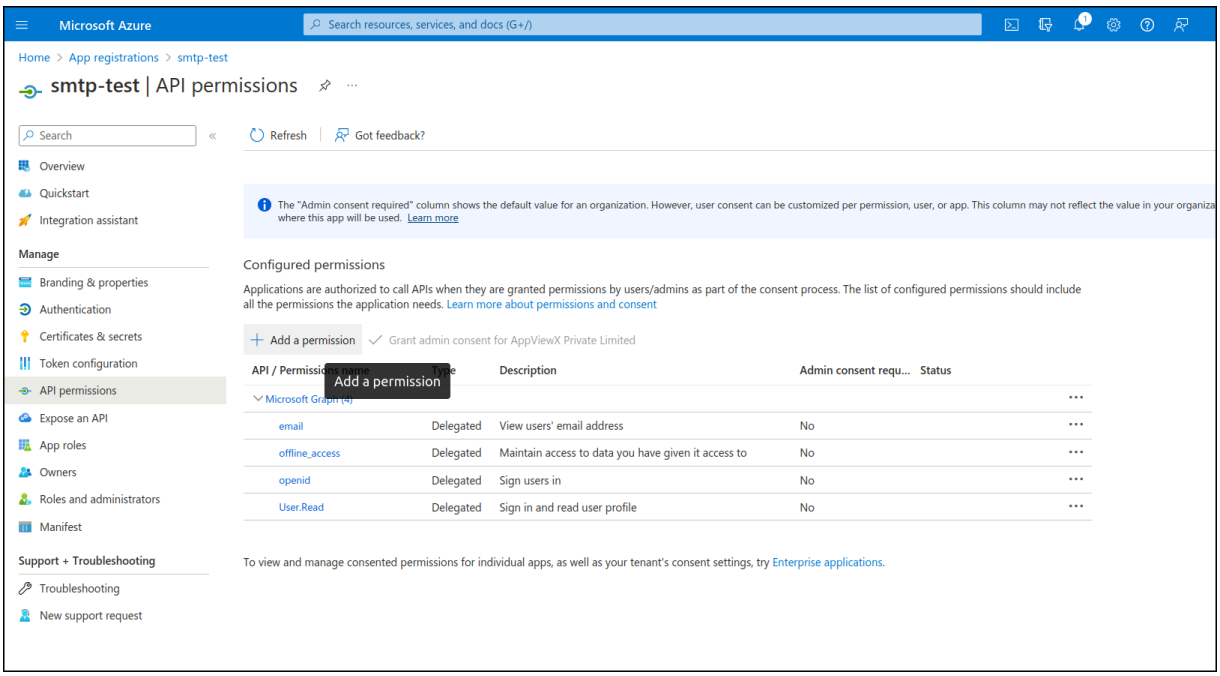
16. Under **App Registration**, Click **Overview**.
17. Click **Endpoints**.

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



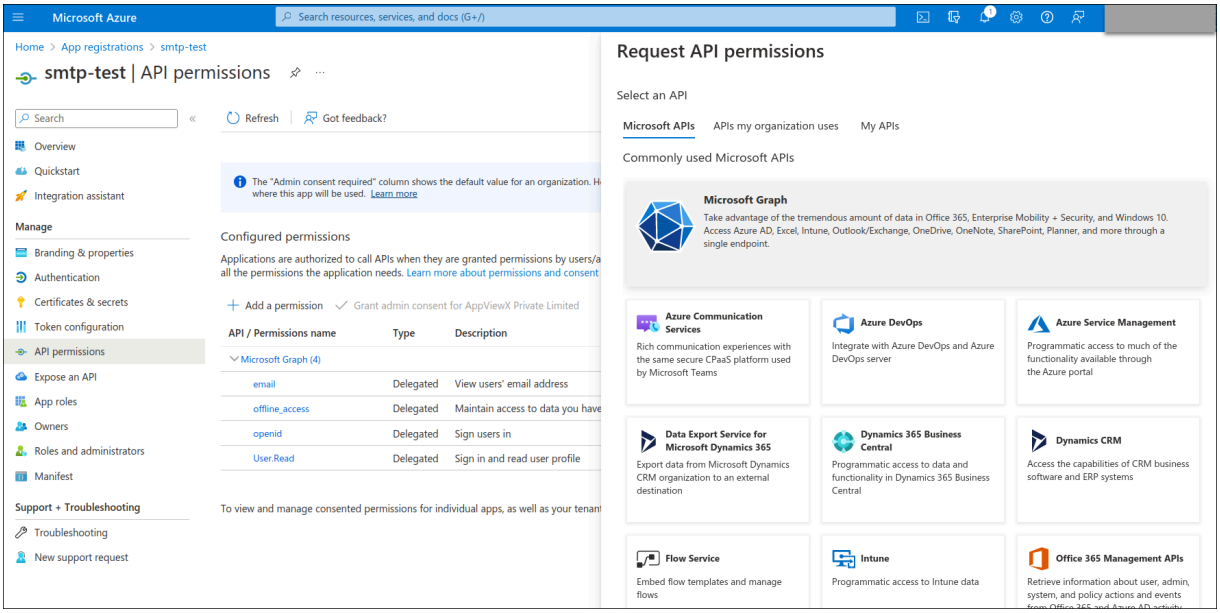
18. Copy **authorization endpoint** and **token endpoint** for Authentication of SMTP Server Settings.
19. Under **Manage**, Click **API permissions**.

    The **API permissions** page is displayed.

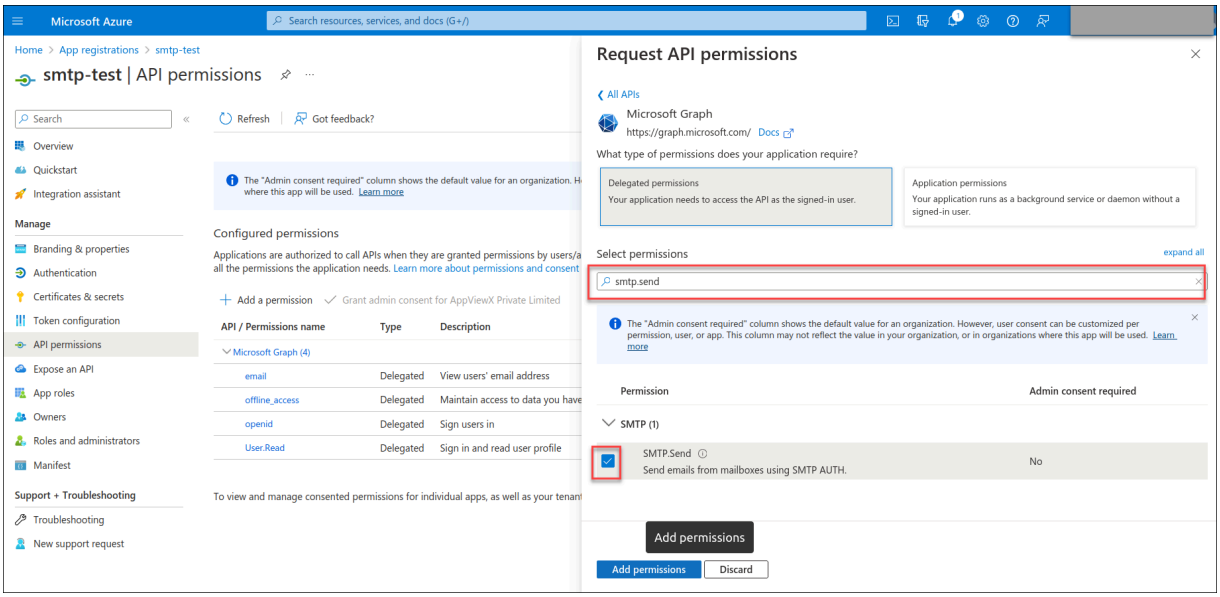


20. To add required permissions, Click on **Add a permission**.

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



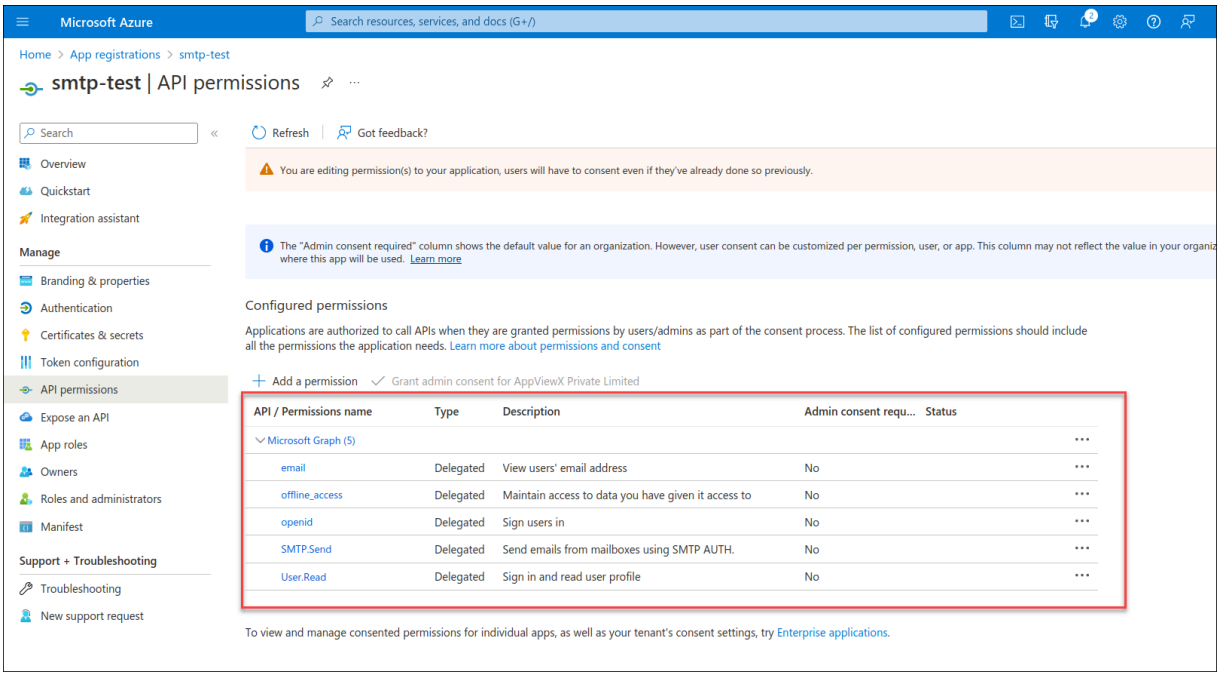
21. Click **Microsoft Graph > Delegated permissions**.



22. Under **Select permissions** search box search for the **smtp.send** and select the **SMTP.Send** from the Dropdown.
23. Similarly Search for **email, offline_access, openid, User.Read** and select the **email, offline_access, openid, User.Read** from the respective Dropdowns.

24. Click **Add permissions**.

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

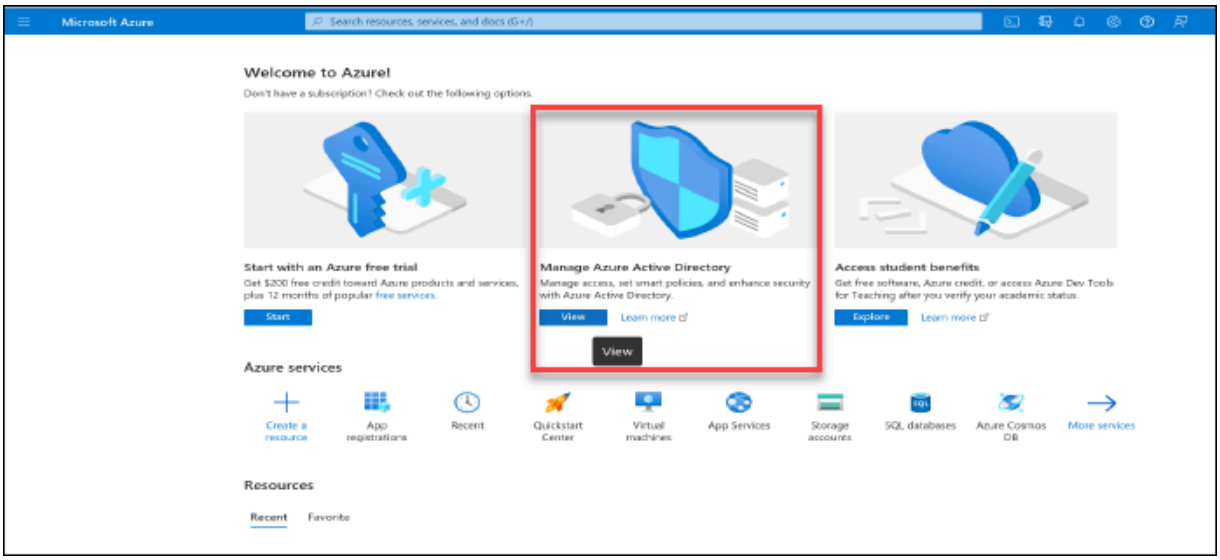


Frequently Asked Questions

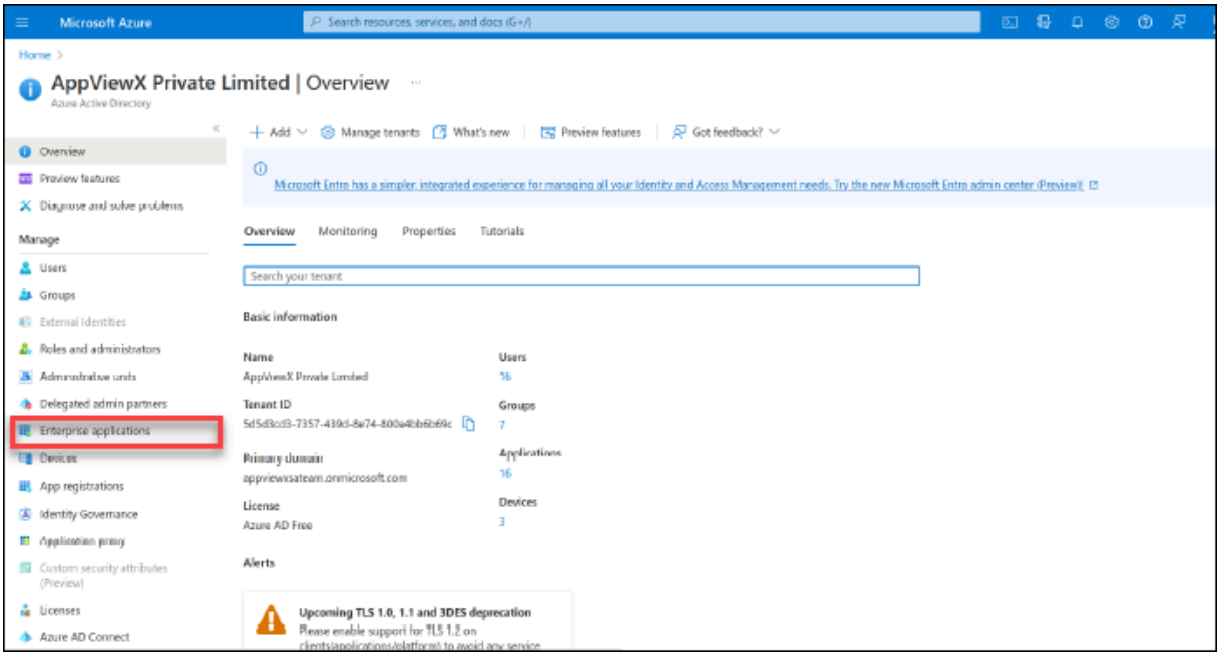
While adding **API permissions** Owner Consent Error is shown, to avoid this error following changes have to be done.

Follow these steps to overcome Owner Consent Error:

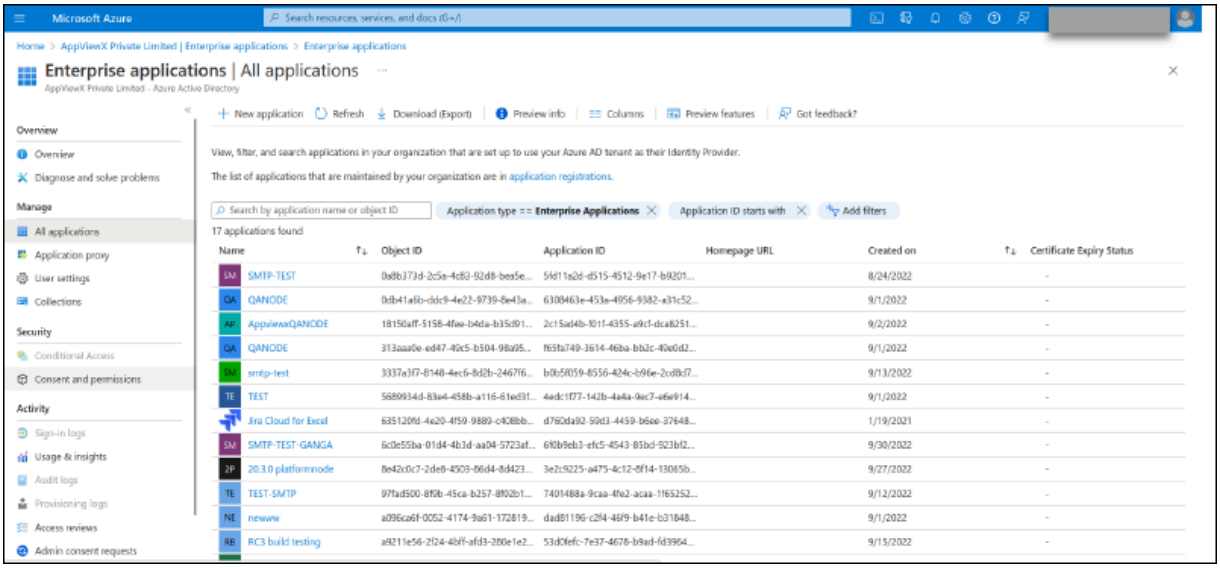
1. Microsoft App Registration URL: https://portal.azure.com/.
2. Click **Manage Azure Active Directory**.



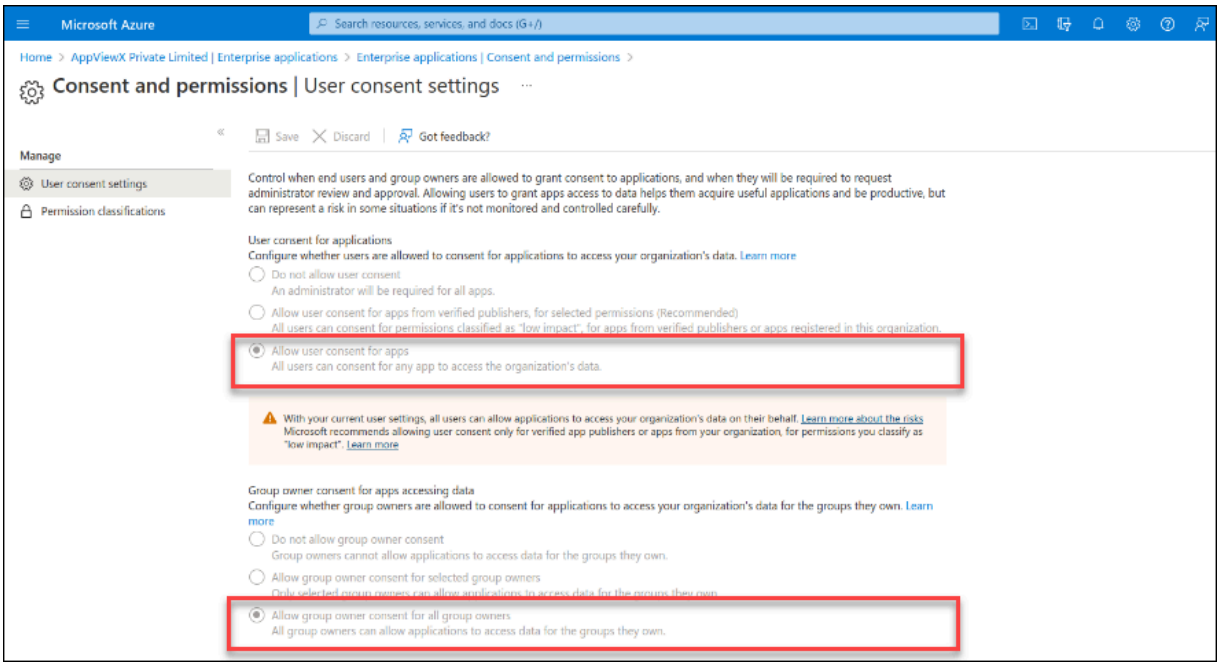
3. Click on **Enterprise applications** in the left menu.



4. Then click on **Consent and permissions** in the left menu.



5. Change the **User Consent Settings** for User consent for applications from **Do not allow user consent** to **Allow user consent for apps**.
6. Also change the **User Consent Settings** for Group Owner Consent for apps accessing data from **Do not allow group owner consent** to **Allow group owner consent for all group owners**.

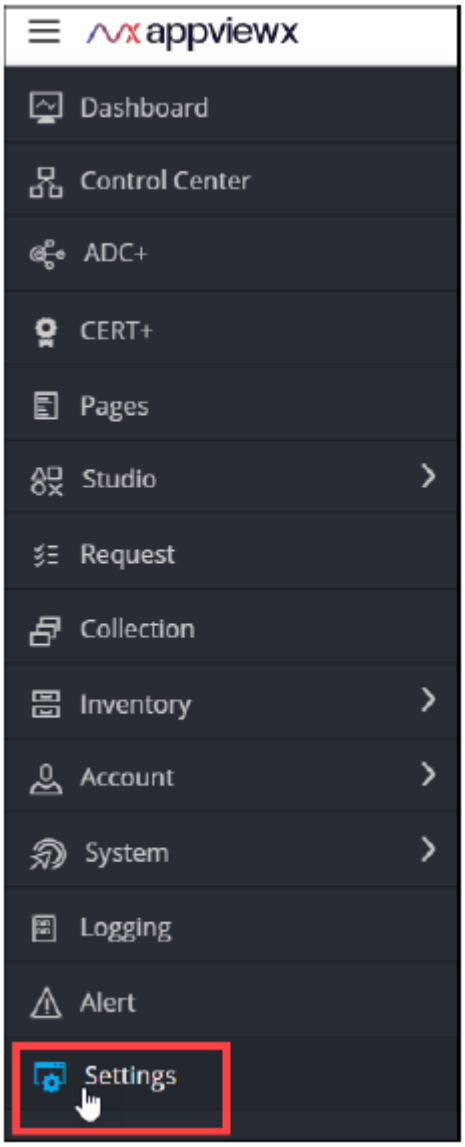


Managing Proxy Settings

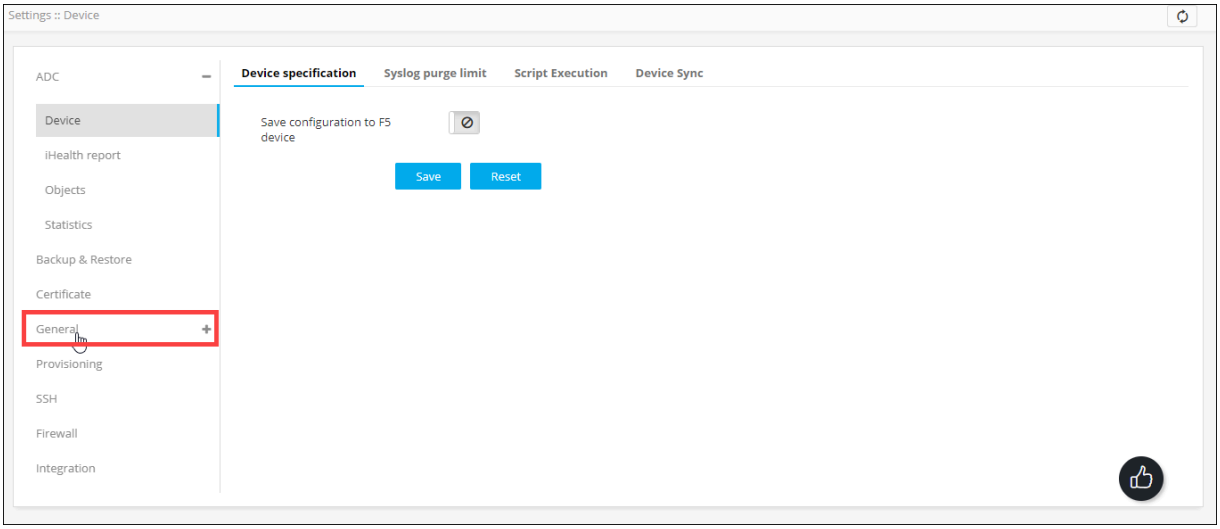
When AppViewX is deployed at a customer's, in order to prevent exposure of the customer's IP address to the internet, AppViewX communicates with the internet using a proxy server.

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 SMTP.

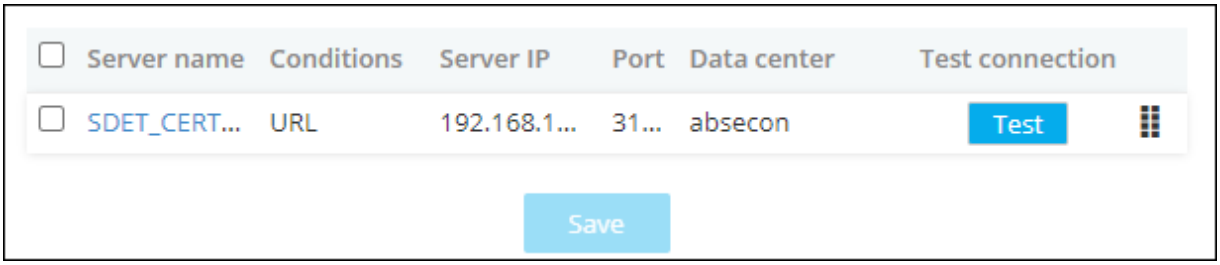
5. The Settings :: Proxy screen is displayed.

6. Enter the following details:

Field	Description
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	**Note:** This field is displayed only when the Advanced check box is selected. From the drop-down menu, select a data center.
URL	**Note:** This field is displayed only when the Advanced check box is selected. From the drop-down menu, select the URL.
Authentication	To enable authentication, select this check box.

Field	Description
Username*	**Note:** This field is displayed only when the Authentication check box is selected. Enter the username.
Password*	**Note:** This field is displayed only when the Authentication check box is selected. This field is displayed only when the Authentication check box is selected.

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



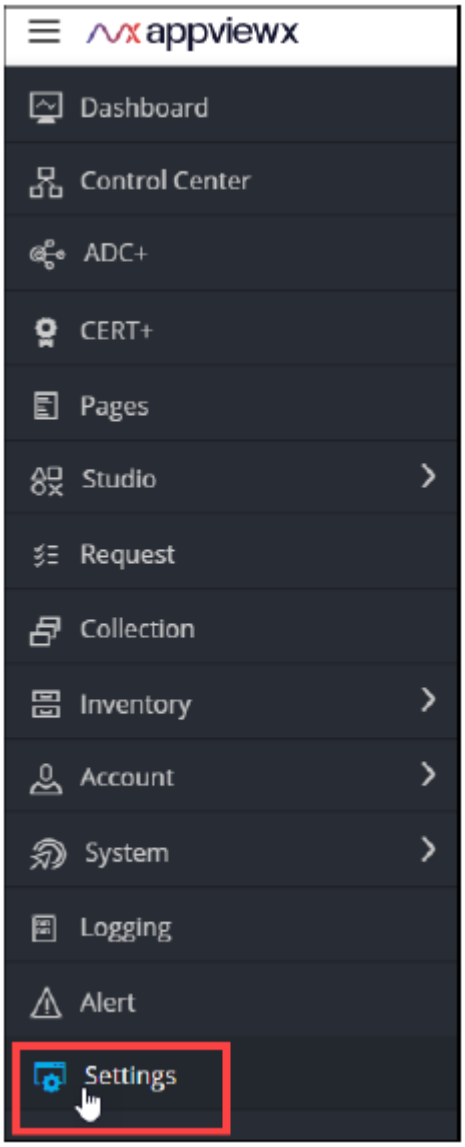
9. To reconfigure the proxy settings, click Reset.

Setting the Cryptographic Policy

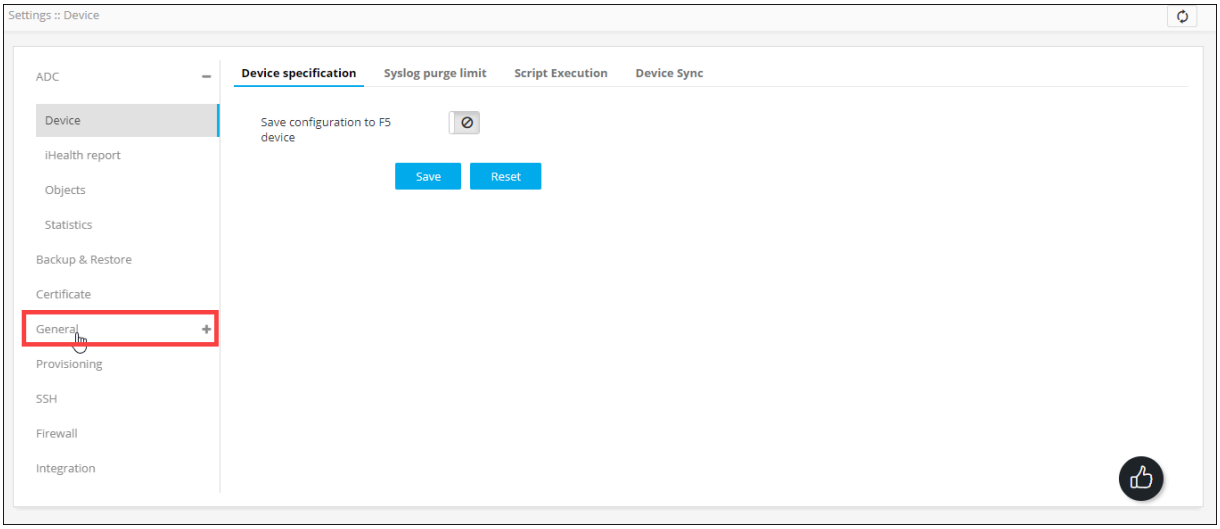
AppViewX enforces a SFTP-based cryptographic policy for protection of sensitive data. Ciphers are used for performing any file operations within AppViewX's functionality and to communicate with devices added in AppViewX.

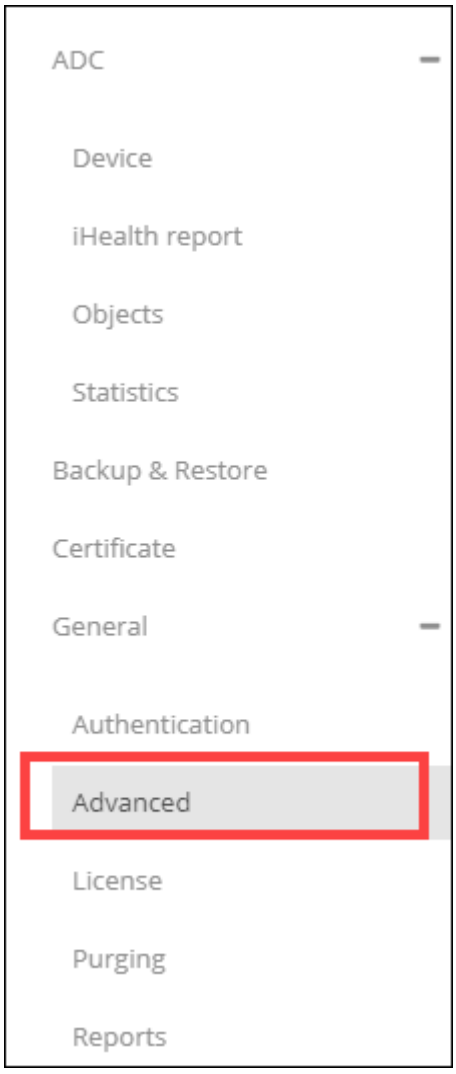
To set the cryptographic policy:

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.
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

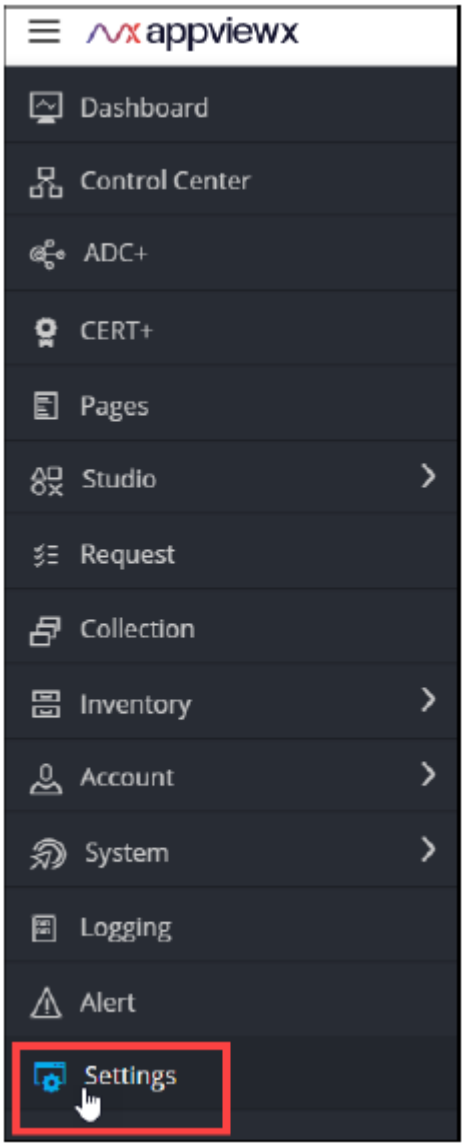
6. Click Save.

Enabling Dashboard View for the User

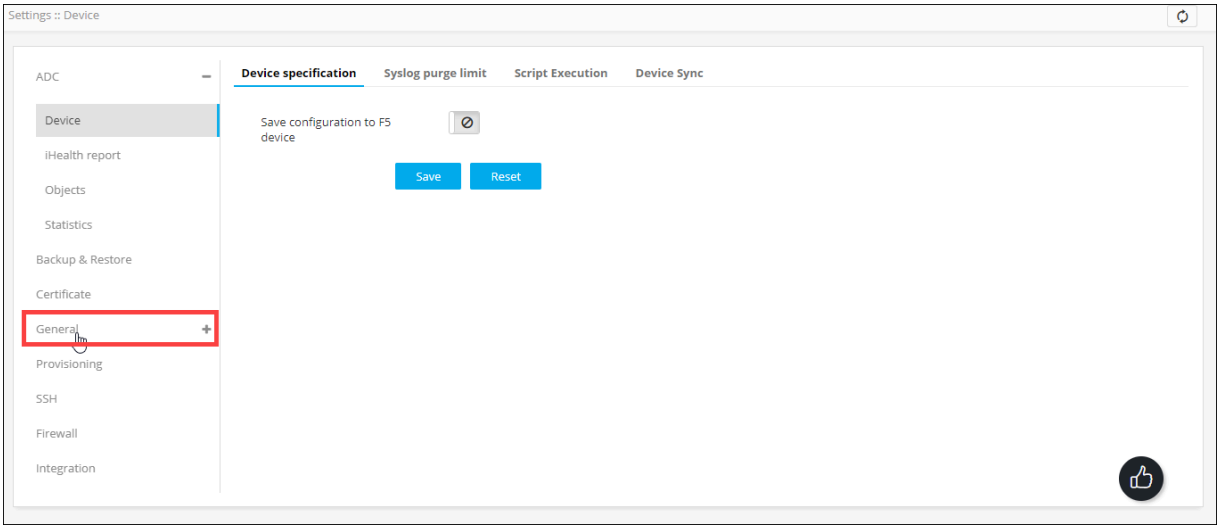
To prevent loss of control over organizational data in the event that a resource leaves the organization, AppViewX lets the admin user have default access to all user dashboard, private as well as public.

To enable default admin access to all dashboards:

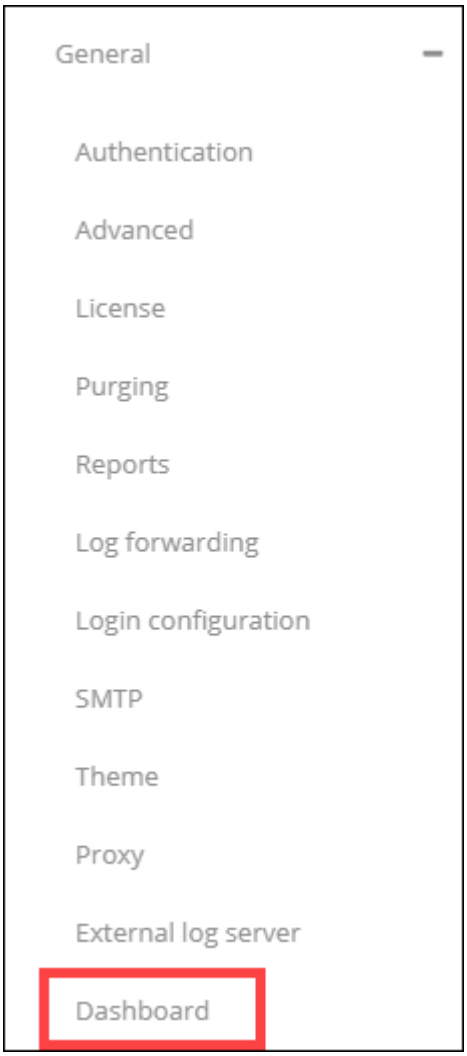
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Settings.



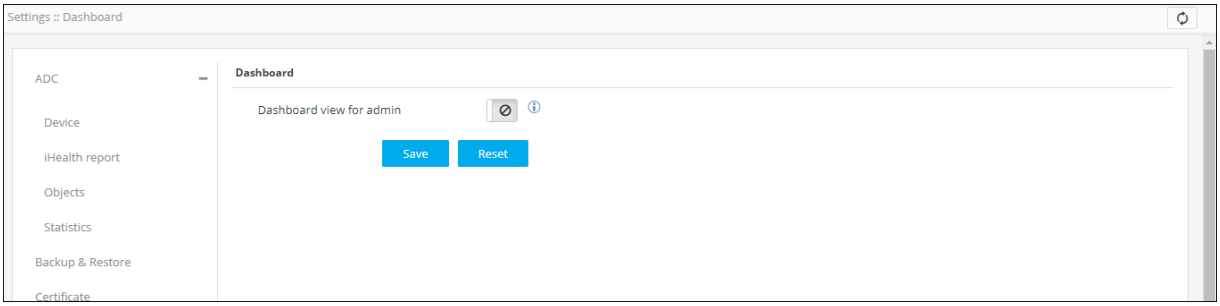
3. On the Settings page, from the navigation pane on the left, click General.



4. Under General settings, click Dashboard.



5. The Settings :: Dashboard page is displayed.



6. Enable the Dashboard view for admin toggle key and click Save.

Managing the Login Configuration

Managing User Inactivity

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

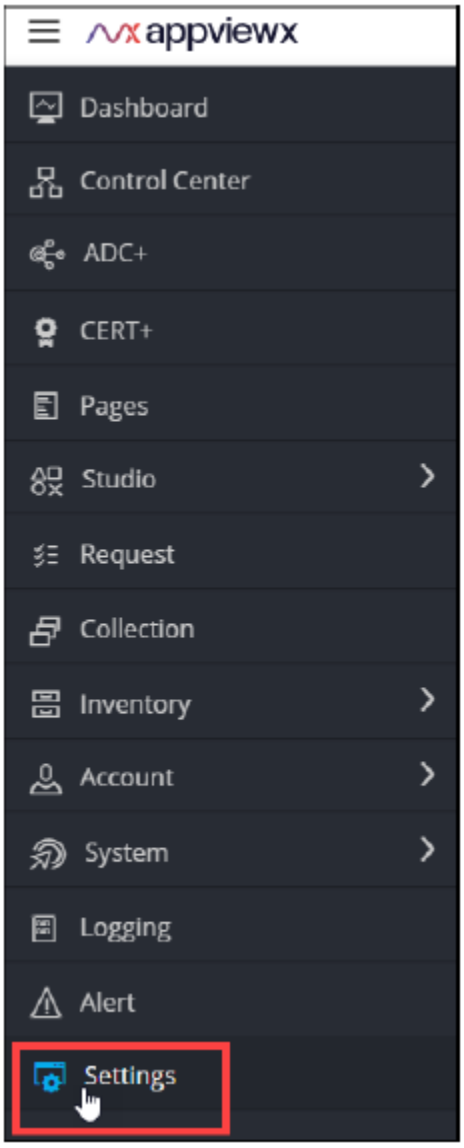
1. In the User inactivity section, enable the Restrict user inactivity period toggle key.
2. To set the number of days for which a user can remain inactive, in the Allowed user inactivity days text field, enter the required value (between 0 and 99).
3. To send the user an email when they are deactivated, select the Send deactivation email alert to user check box.
4. An email alert is sent to the user for three consecutive days before deactivation.
5. Click Save.

Restricting Number of User Sessions

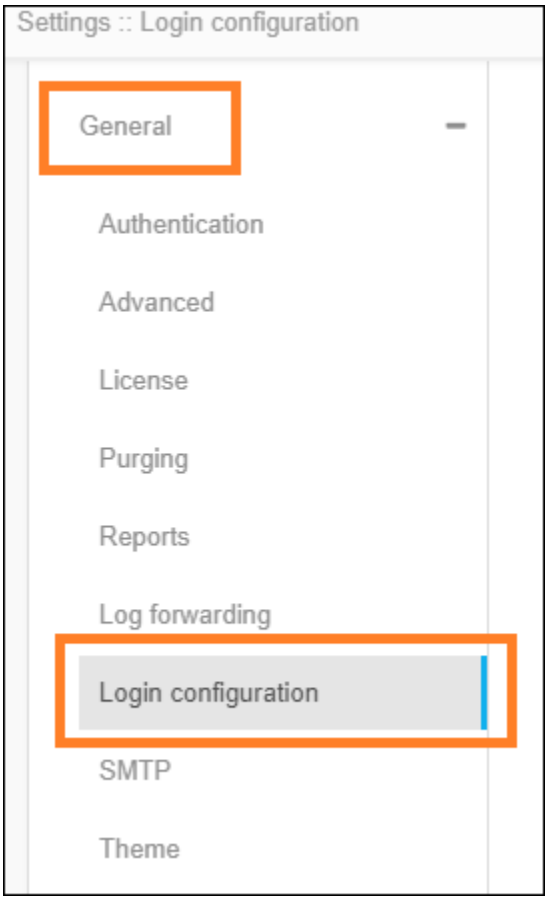
In the **Session** section, enable the **Restrict each user to a single session** toggle key. By default, it is disabled.

In order to enable it, follow the steps mentioned below,

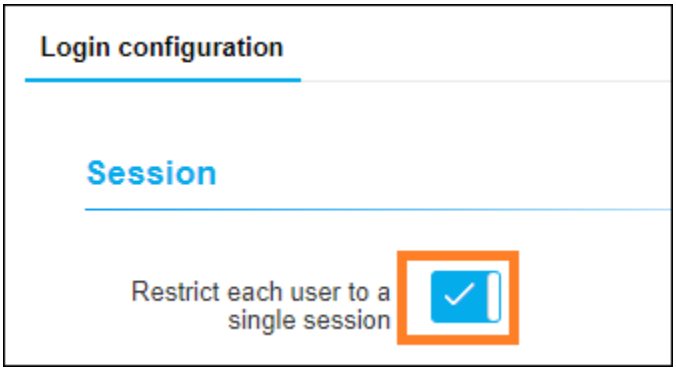
1. Click the menu (☰) icon.
2. Navigate to CERT+ > Settings.



3. On the left menu, navigate to General > Login configuration.

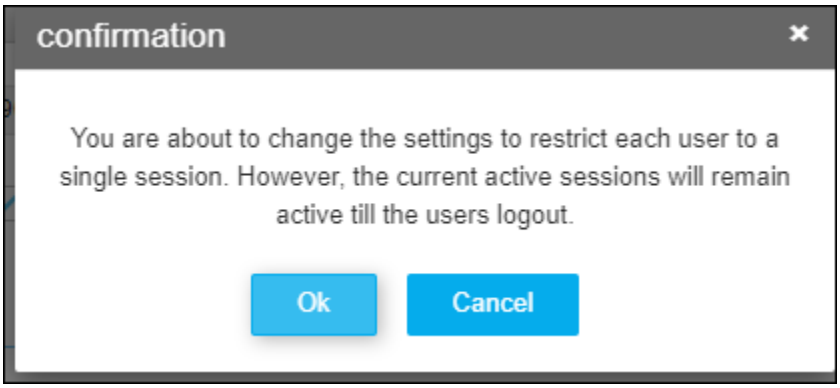


4. In the Session section, enable the Restrict each user to a single session field.



5. Click Save.

6. In the pop-up, click OK.



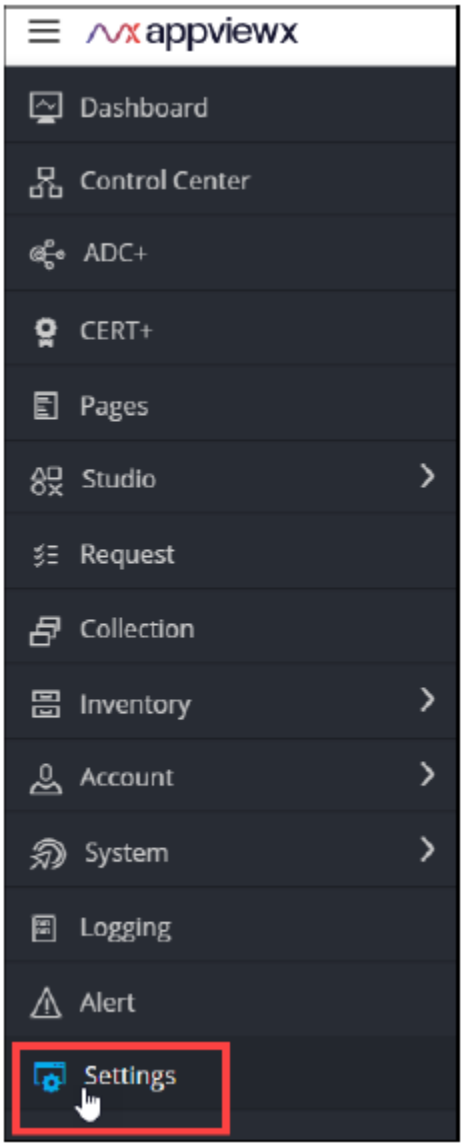
7. The Login setting(s) is modified and it will be applied from next login for internal users.

Restricting the Number of Login Attempts

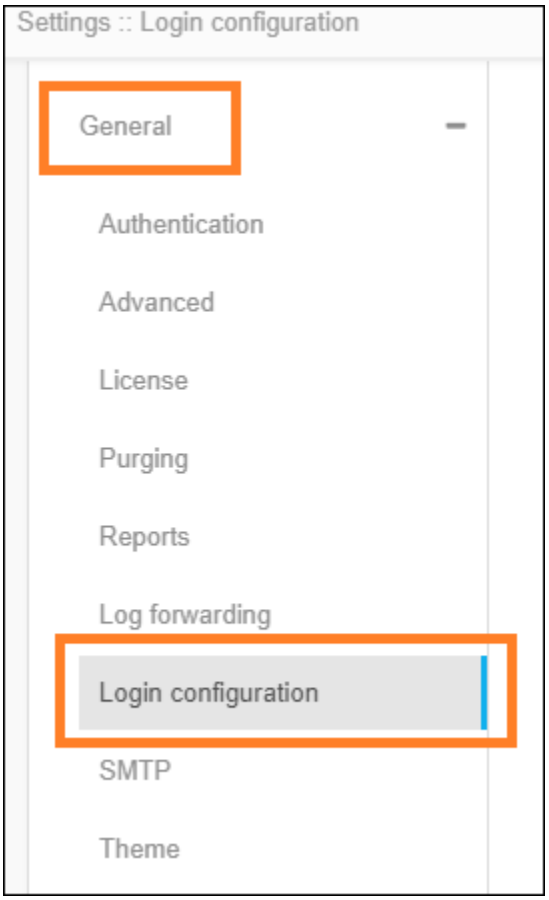
1. In the Login attempts section, enable the Restrict number of login attempts toggle key. It is disabled by default.
2. In the Allow failed login attempts text field, enter the required value (between 0 and 99). By default, it is set to 10.

In order to enable it, follow the steps mentioned below,

1. Click the Menu (☰) icon.
2. Navigate to CERT+ > Settings.



3. On the left menu, navigate to General > Login configuration.



4. In the Login attempts section, enable the Restrict number of login attempts and also provide any number between 0-99 in the Allowed failed login attempts field. By default, it is 10. If the user uses incorrect details more than 10 times, then he/she will get locked out.

5. Click Save.

Managing User Activity

Chapter 6: Managing Logs

- Viewing Logs-Overview
- Setting the Record Count Preference for Logs
- Searching for Logs
- Forwading Logs
- Exporting Logs
- Purging Logs

Viewing Logs-Overview

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

• Viewing ADC Logs

• Viewing AppViewX Logs

• Viewing Audit Logs

• Viewing Certificate Logs

• Viewing Self-Audit Logs

• Viewing SSH Logs

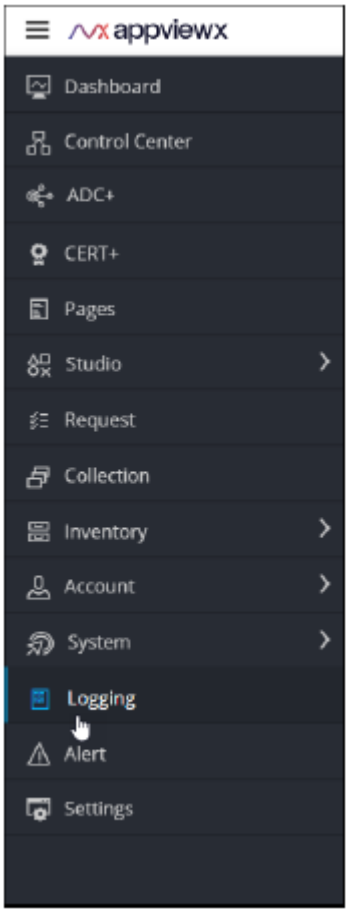
• Viewing Syslog Logs

• Viewing Workflow Logs

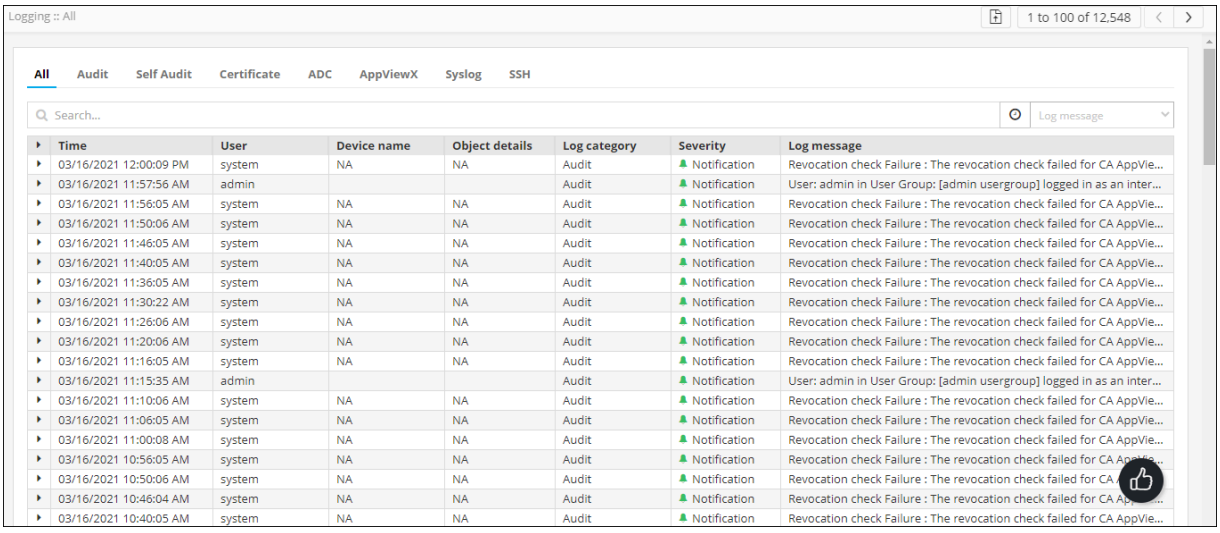
Viewing All Logs

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



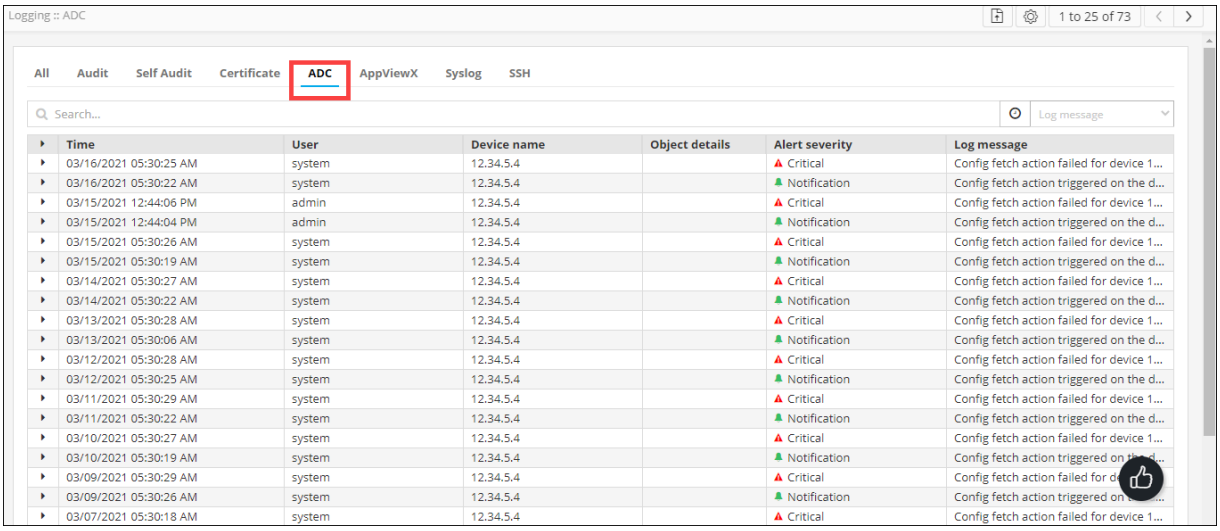
4. For each activity, this page displays the following details:

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 an object-related activity
Log category	The category under which this log record will be filed
Severity	The 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. On the Logging page, click the ADC tab.



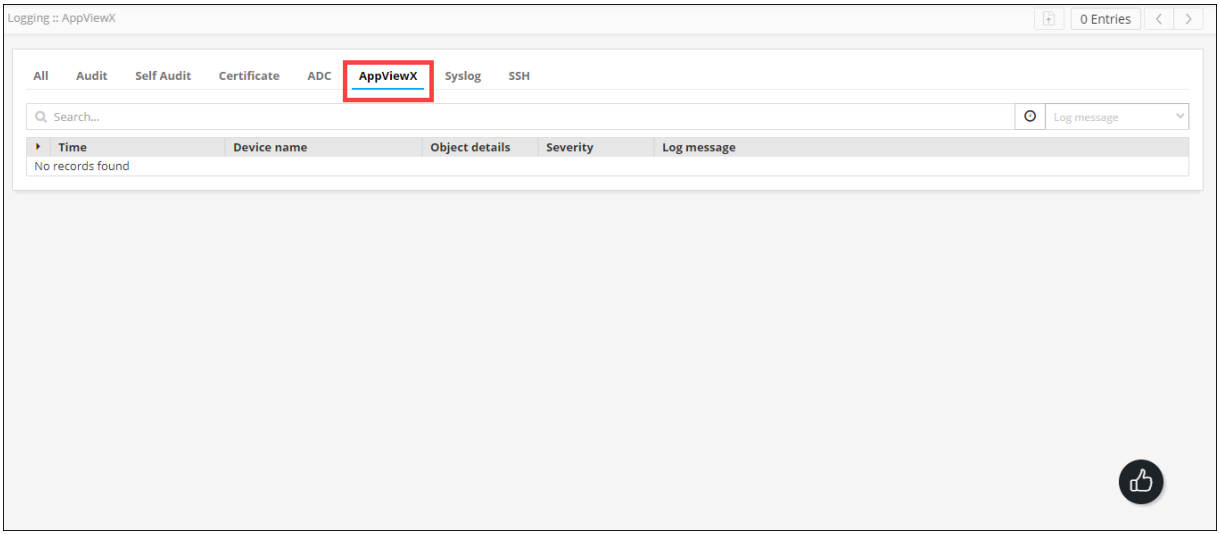
2. The page displays the following details for the ADC logs:

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 an object-related activity
Alert Severity	The 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. On the Logging page, click the AppViewX tab.



2. The page displays the following details for the AppViewX logs:

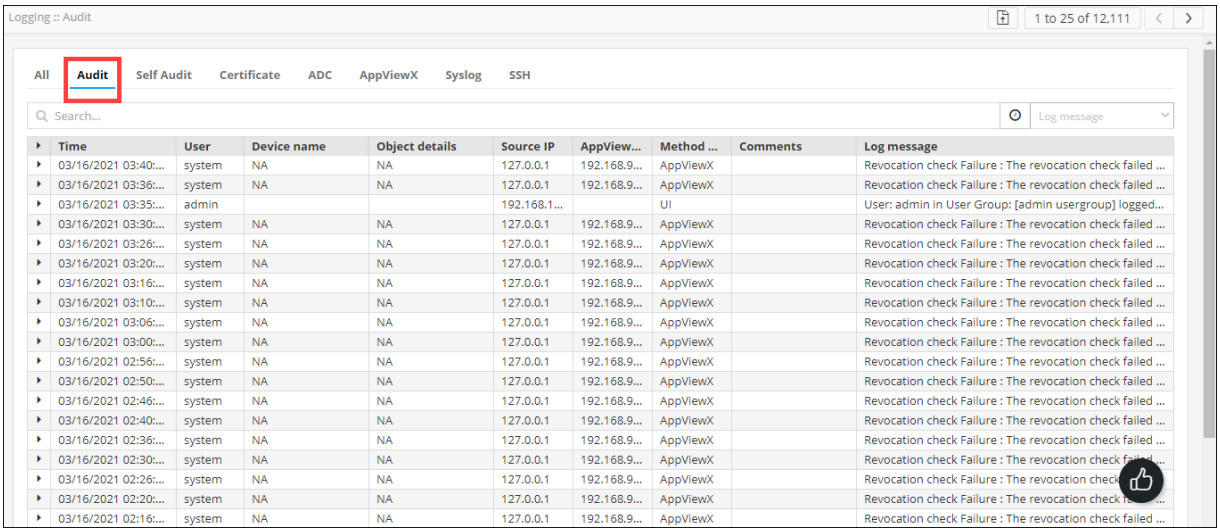
Category	Description
Time	Date and time at which the activity was carried out

Category	Description
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 an object-related activity
Severity	The 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. On the Logging page, click the Audit tab.



2. The page displays the following details for all audit logs:

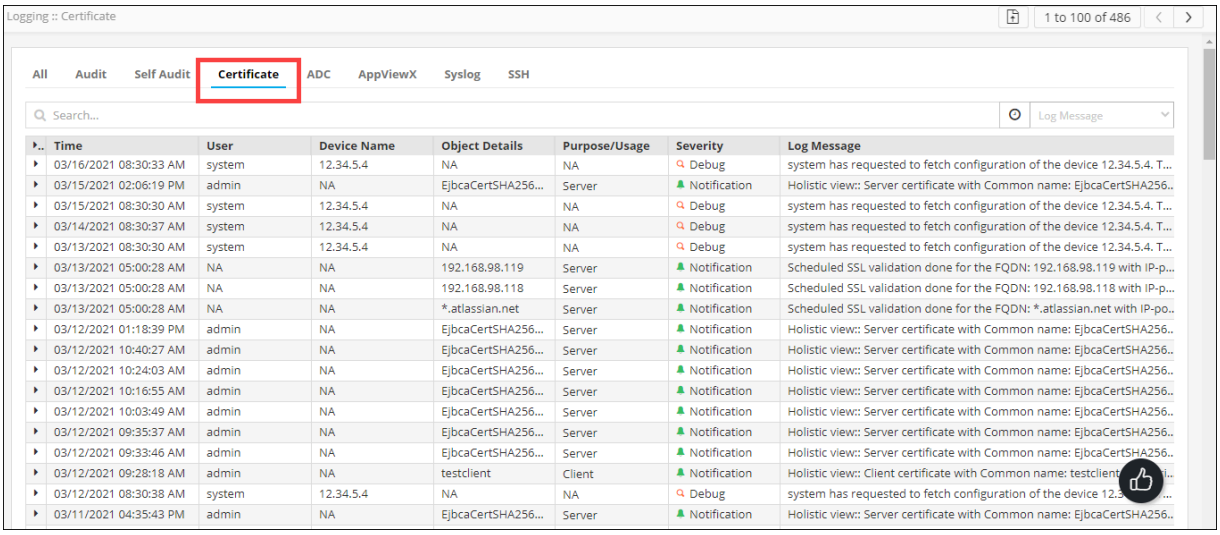
Field	Description
Time	Date and time at which the activity was carried out
User	Username of the user who performed the activity
Device name	Name of the device, if the log is of a device-related activity

Field	Description
Object details	Name of the object, if the log is of an object-related activity
Source IP	The IP address of the system that was the source of the activity
AppViewX node	The 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 Certificate Logs

To view Certificate logs:

1. On the Logging :: All page, click the Certificate tab.



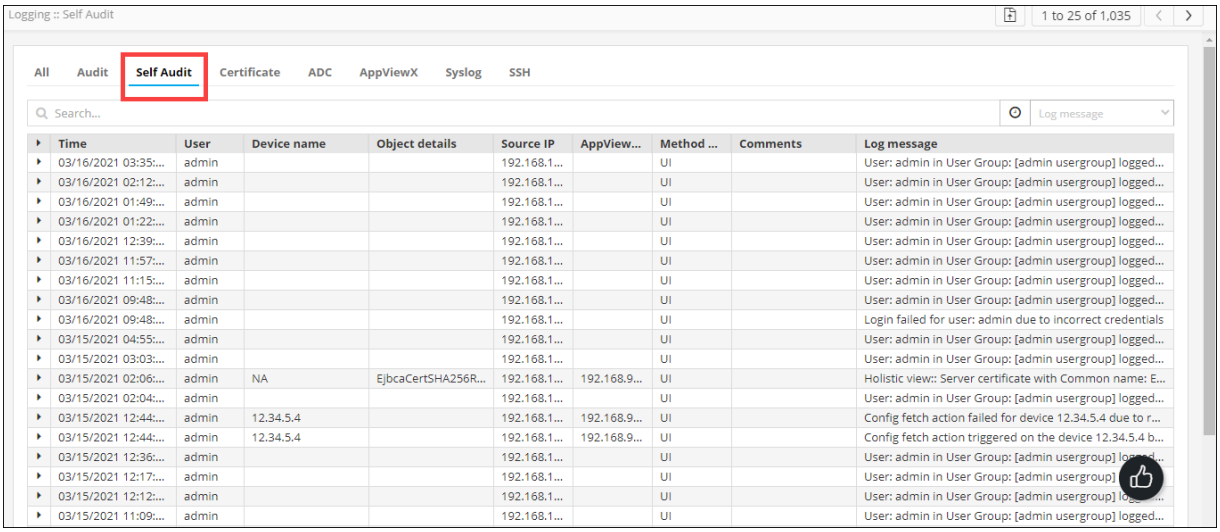
2. The Logging :: Certificate page displays the following details for all certificate-related logs:

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 an object-related activity
Purpose Usage	Certificate type (server, client, device, code signing) associated with the logged activity
Severity	The severity of the activity logged (Notification, Debug, Warn, Error, Fatal, Critical)
Log Message	Description of the activity logged

Viewing Self-Audit Logs

To view Self Audit logs:

1. On the Logging page, click the Self Audit tab.



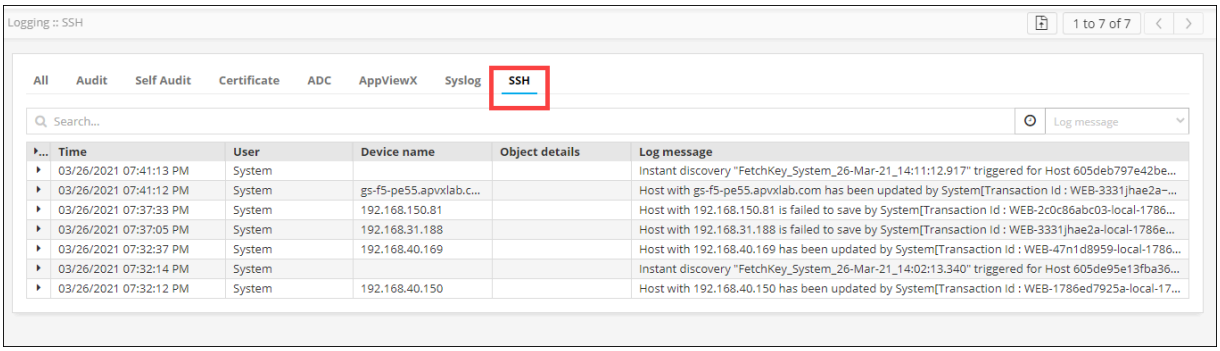
2. The page displays the following details for all self-audit logs:

Field	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 an object-related activity
Source IP	The IP address of the system that was the source of the activity
AppViewX node	The 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 SSH Logs

To view the SSH logs:

1. On the Logging page, click the SSH tab.



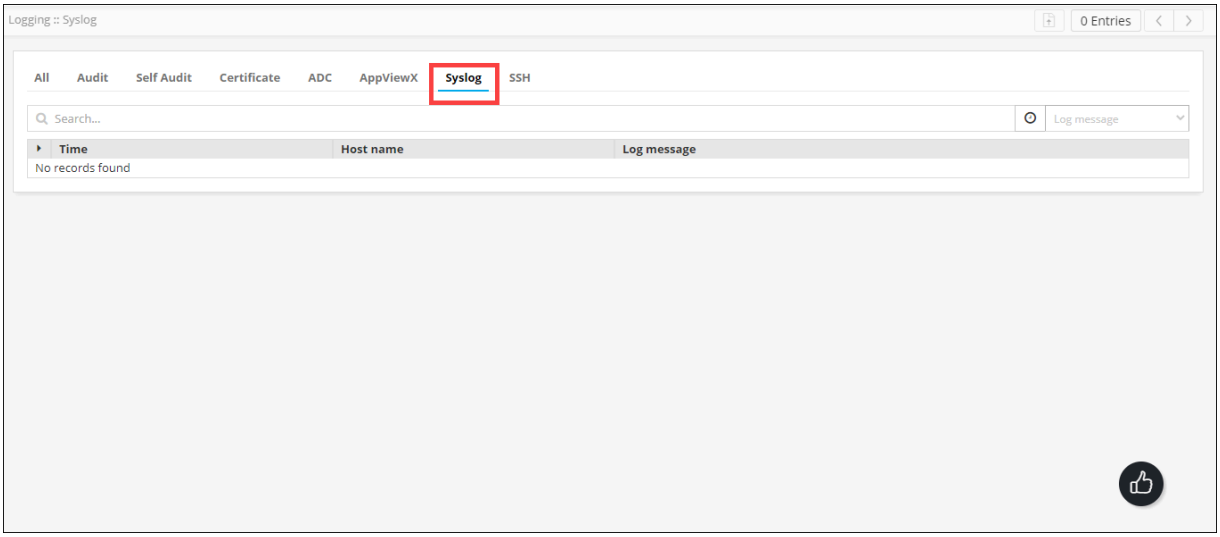
2. The page displays the following details for the SSH logs:

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 an object-related activity
Log Message	Description of the activity logged

Viewing Syslog Logs

To view the Syslog logs:

1. On the Logging page, click the Syslog tab.



2. The page displays the following details for the Syslog logs:

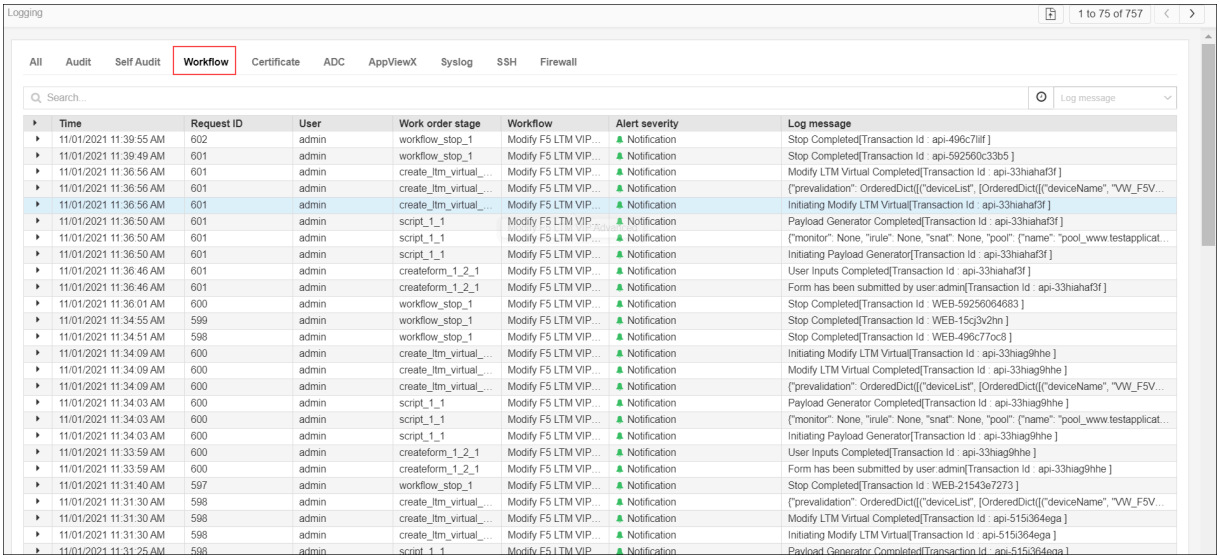
Category	Description
Time	Date and time at which the activity was carried out

Category	Description
Host name	Host name of the Syslog server
Log Message	Description of the activity logged

Viewing Workflow Logs

To view the workflow logs:

1. On the Logging page, click the Workflow tab.



2. The page displays the following details for the Workflow logs:

Field	Description
Time	Date and time at which the activity was carried out
User	Username of the user who performed the activity
Request ID	Workflow request ID
Work order stage	The stage at which an action is performed on the workflow.
Workflow	Name of the workflow
Alert Severity	The severity of the workflow Log message
Log message	Description of the activity logged

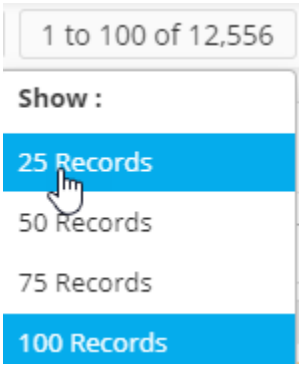
Setting the Record Count Preference for Logs

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.

To set the record count preference:

1. **Note:** By default, 100 records are shown on one page (which is why the control reads 1 to 100).

   On the Logging :: All page, from the top-right corner of the screen, click 1 to 100 of 12,556.
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: 1 to 25 of 12,557

Searching for Logs

AppViewX lets you search for logs in two ways:

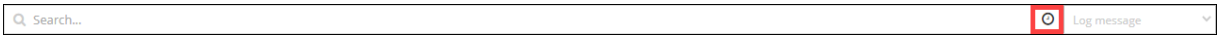
- Based on a timestamp
- Based on the values recorded for each log

- Based on a Timestamp
- Based on the Values Recorded for each Log

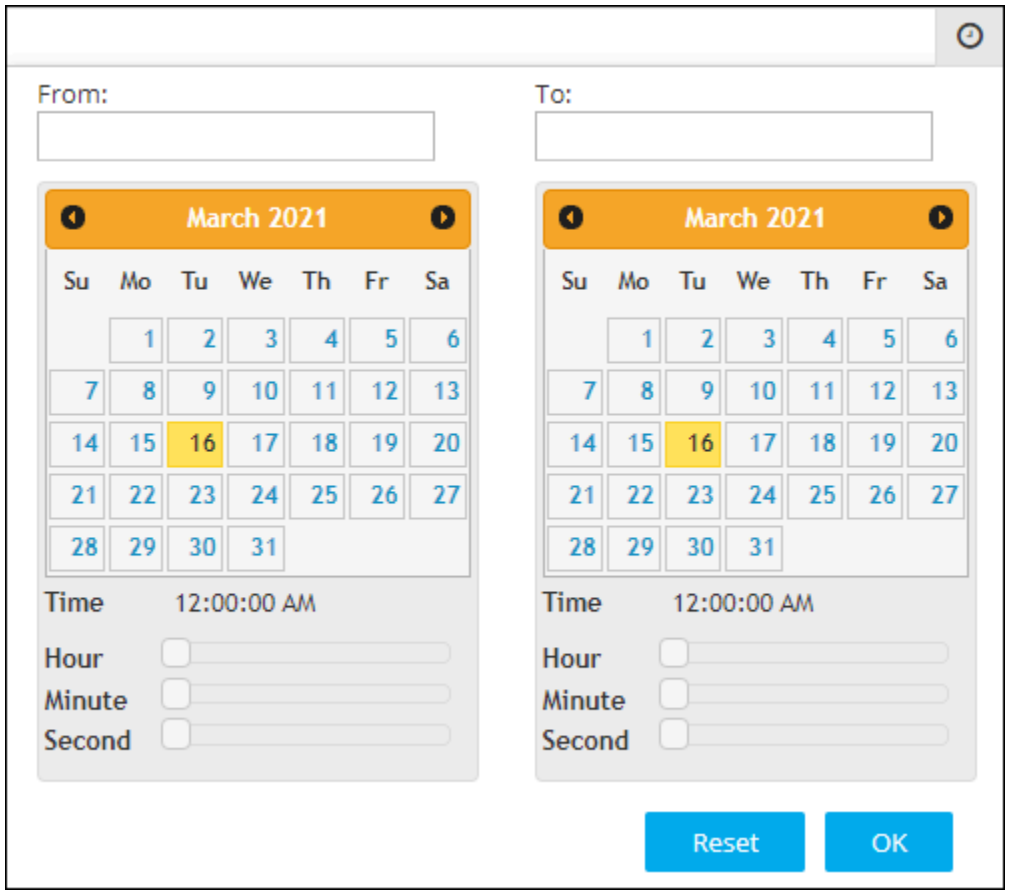
Based on a Timestamp

To search for logs based on a timestamp:

1. From the Search field on the Logging page, click the  icon.



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



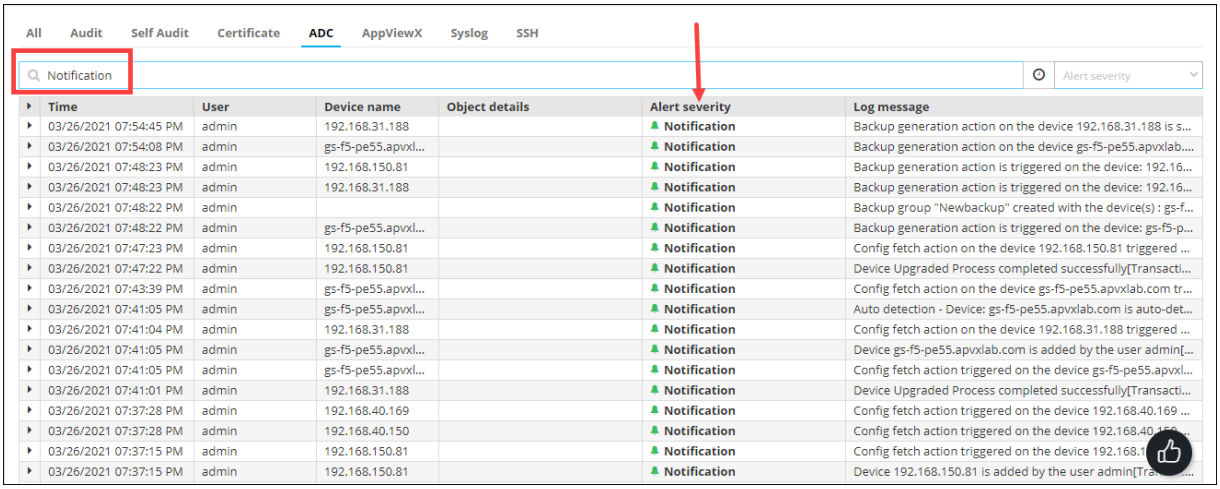
3. To select a date range, in the From and To fields, select the required dates.
4. To set a time, use the Hour, Minute, and Second slider controls.
5. Click OK.
6. The page is updated to display log records from the selected timestamp.

> **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 the category—Alert Severity—for searching the required logs.
3. In the Search field, enter the search value—Notification.
4. 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.

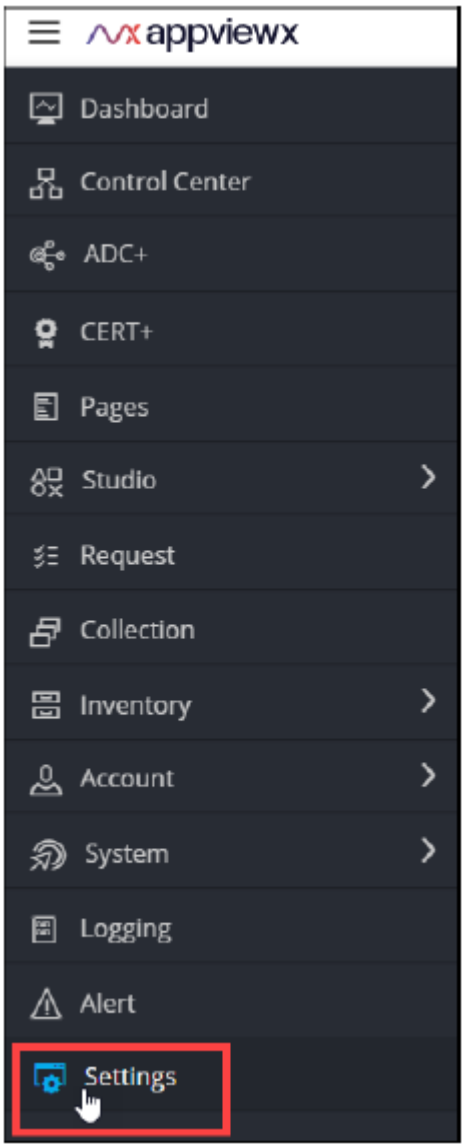
- Configuring Server Inventory Settings
- Deleting Server Inventory Settings
- Disabling Server Inventory Settings
- Enabling Server Inventory Settings
- Configuring Forwarding Settings

Configuring Server Inventory Settings

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

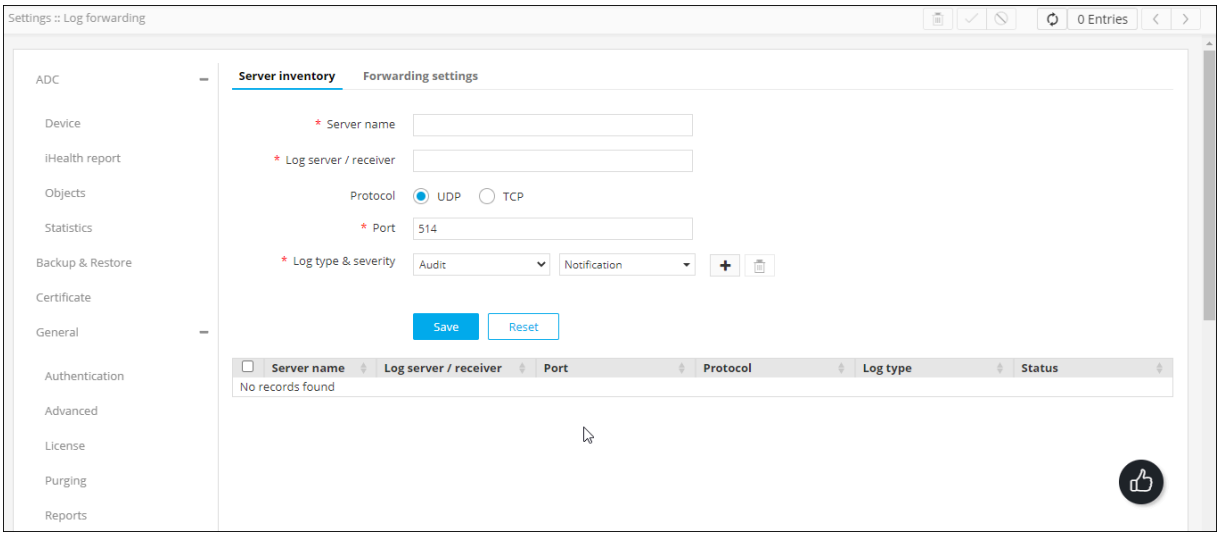
To configure server inventory settings:

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.

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



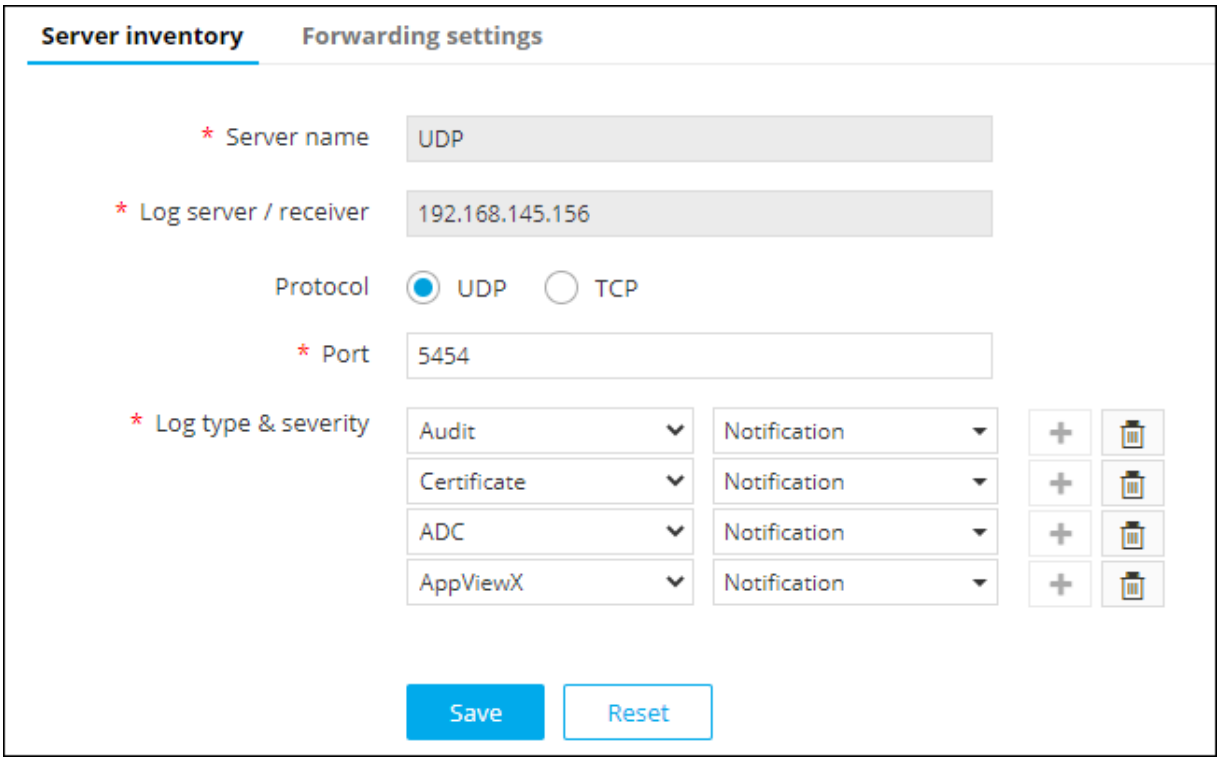
5. In the Server inventory tab, enter the following details (sample values are shown in the image below the table):

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:

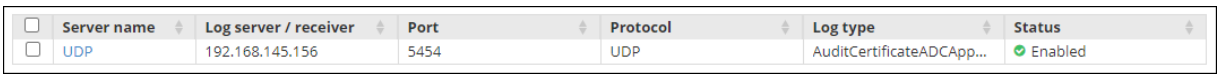
Field	Description
	• UDP (default) • TCP
Port*	The port number on the external server to which the logs will be forwarded
Log type & severity*	You can choose to forward logs of a specific type and a specific severity to an external server. To add a log type and severity entry: a. From the first drop-down 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.

Field	Description
	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.

***:Mandatory**



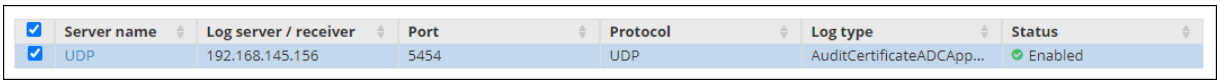
6. To save the server inventory settings, click Save. The settings configured in the fields above are displayed in the table shown at the end of the page.



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.



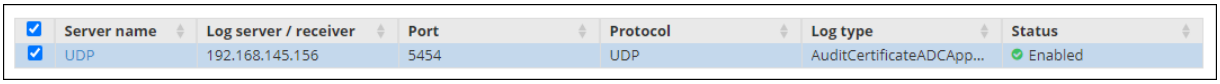
2. From the top right corner of the screen, click  .

> **Note:** You can delete multiple server inventory settings by selecting the check box against all the settings you want to delete.

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.



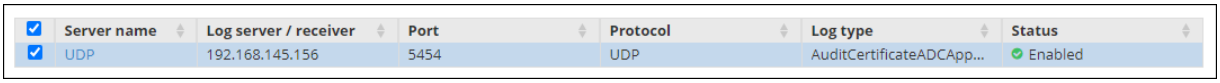
2. From the top right corner of the screen, click  .

> **Note:** You can disable multiple server inventory settings by selecting the check box against all the settings you want to disable.

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.

Configuring Forwarding Settings

To configure the forwarding settings follow the below steps:

1. In 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-down menu, select one of the following options: • Syslog • CEF **Note:** CEF is the most recent industry standard for forwarding logs.
Enable retry	If an attempt to forward logs fails because of server unavailability, AppViewX lets you set a retry interval—the duration after which logs will be forwarded again. To enable this retry, enable the Enable retry toggle key.
Retry interval*	To set a retry interval, from the hour and minutes drop-down menus, select the required values.

***: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:

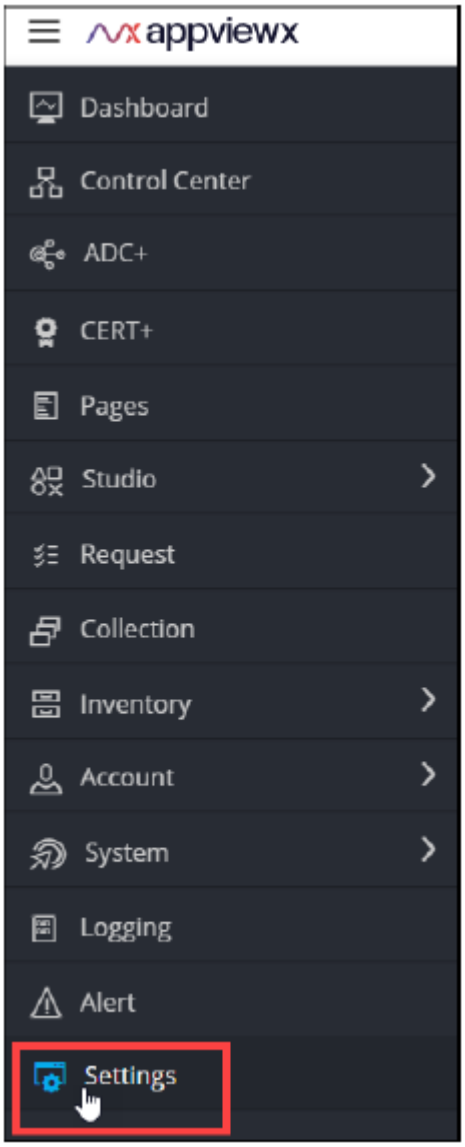
1. Go to the Logging page for the log type (all, audit, self audit, certificate, ADC, AppViewX, Syslog, SSH) you want to export.
2. From the top right corner of the Logging page, click the export icon  .
3. Navigate to the location to save the log file and click Save. All logs of the selected log type are downloaded and saved.

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.

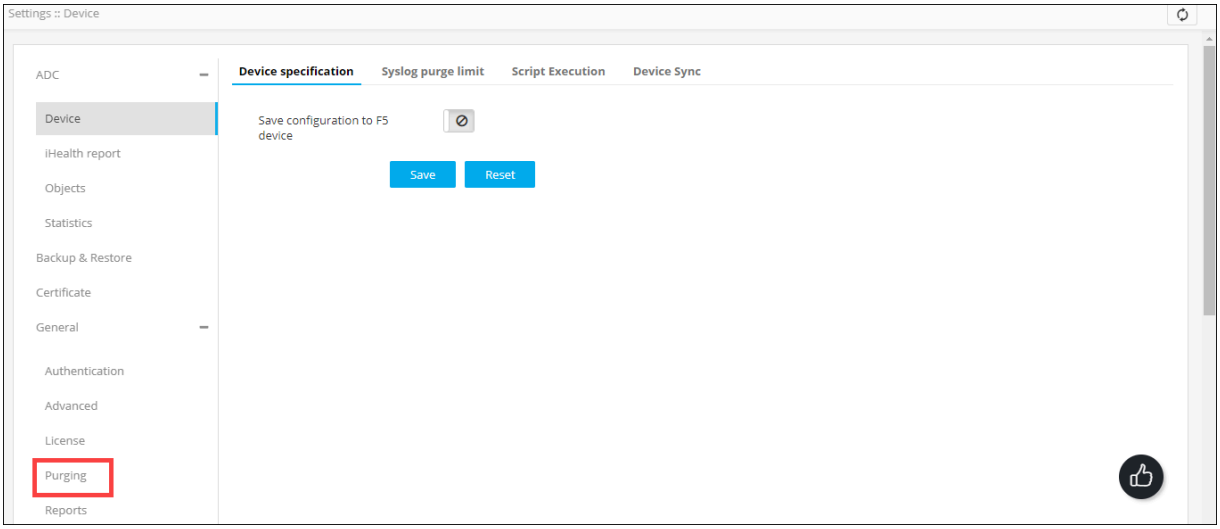
To enable purging of log records:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.

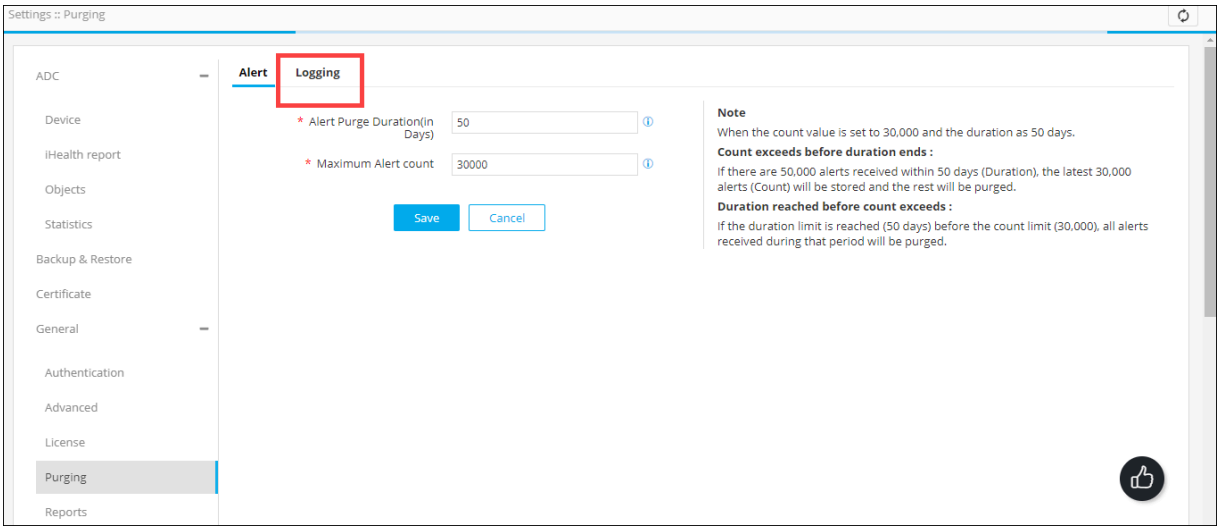


2. From the menu displayed, click Settings.
3. On the Settings page, from the navigation pane on the left, click General.

4. Under General settings, click Purging.



5. The Settings :: Purging screen is displayed.
6. To configure the log purging settings, click the Logging tab.



7. 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.

***:Mandatory**

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

8. Click Save.

Chapter 7: HSM Integration for AppViewX SaaS

- HSM Integration for AppViewX SaaS-Overview
- HSM Architecture for the SaaS Deployment
- Utimaco
- Fortanix
- Thales DPoD
- Thales GPN

HSM Integration for AppViewX SaaS-Overview

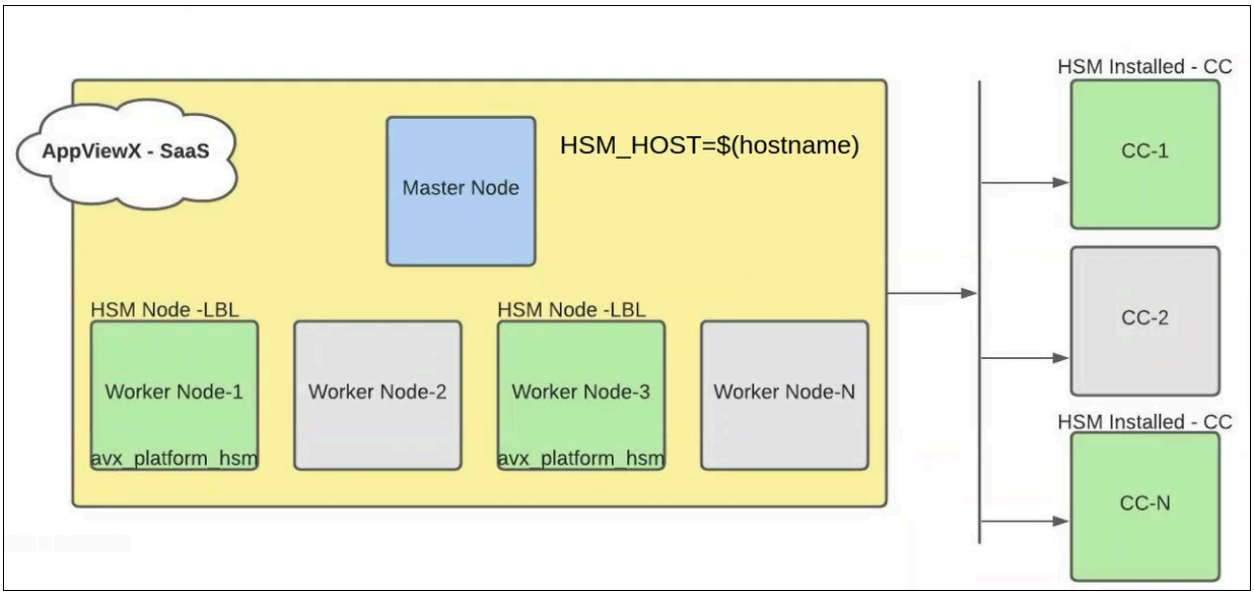
An HSM (Hardware Security Module) is a piece of hardware and associated software or firmware that usually resides in a PC or server and provides at least the minimal cryptographic functions. These functions include (but are not limited to) encryption, decryption, key generation, and hashing. The physical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

- Utimaco
- Fortinax
- Thales - DPoD
- Thales - GPN

HSM Architecture for the SaaS Deployment



For the SaaS deployment, all configuration files to facilitate the integration of and communication with HSM are installed on the AppViewX Cloud Connector

Utimaco

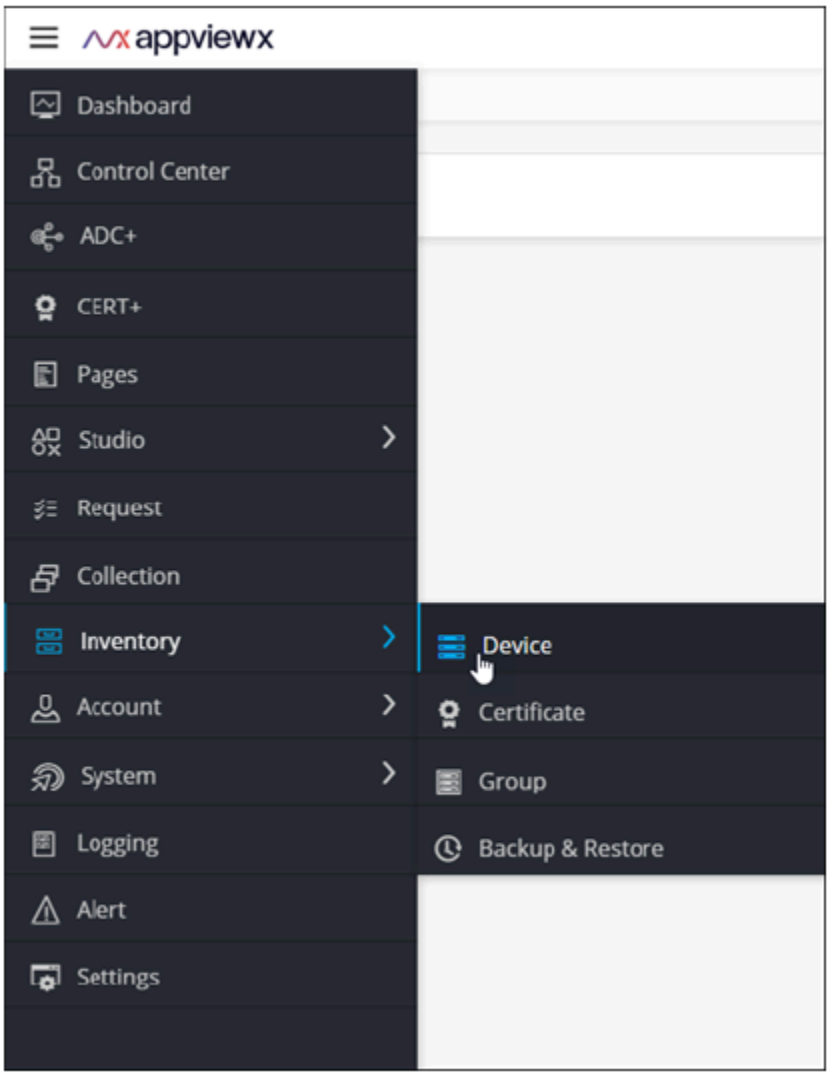
In this section, you will be guided to integrate the Utimaco HSM with the AppViewX SaaS.

- Integrating the Utimaco HSM with the AppViewX SaaS

Integrating the Utimaco HSM with the AppViewX SaaS

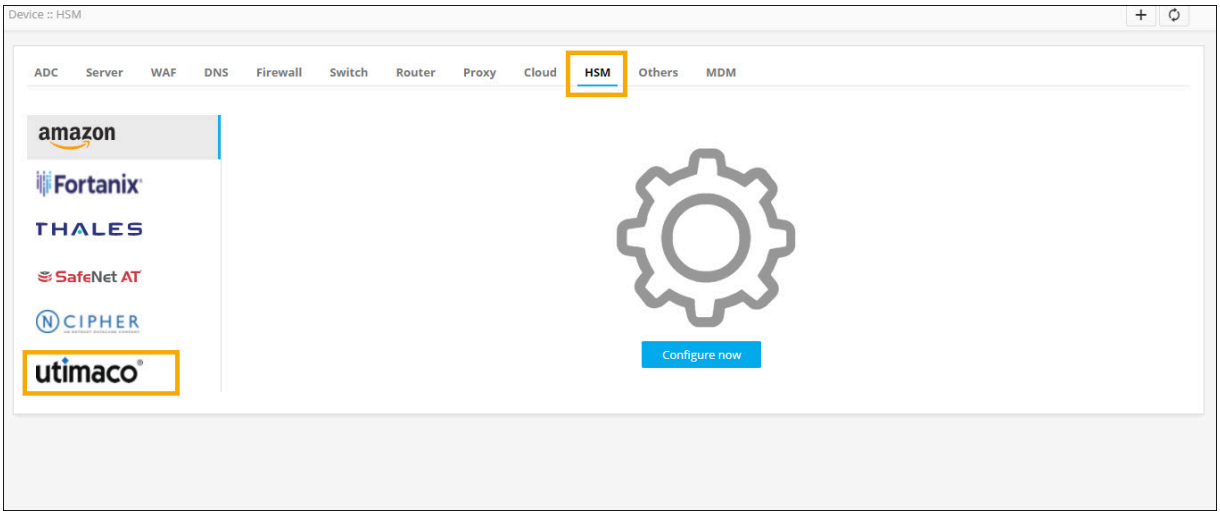
To integrate the Utimaco HSM with the AppViewX SaaS:

1. Login to the AppViewX UI using valid credentials. By default, the **Dashboard** is displayed.
2. From the top-right corner of the **Dashboard**, click ☰.
3. From the menu displayed, select **Inventory** > **Device**.



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

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



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

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	
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.

6. In the Vendor specific details section, enter/select 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
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 location*	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 location*	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.

7. Click Save.
8. 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.
9. If the implementation type is CSR Generation, to generate the CSR, follow the steps given here:

- Server certificate
- Client certificate
- Code signing certificate

Fortanix

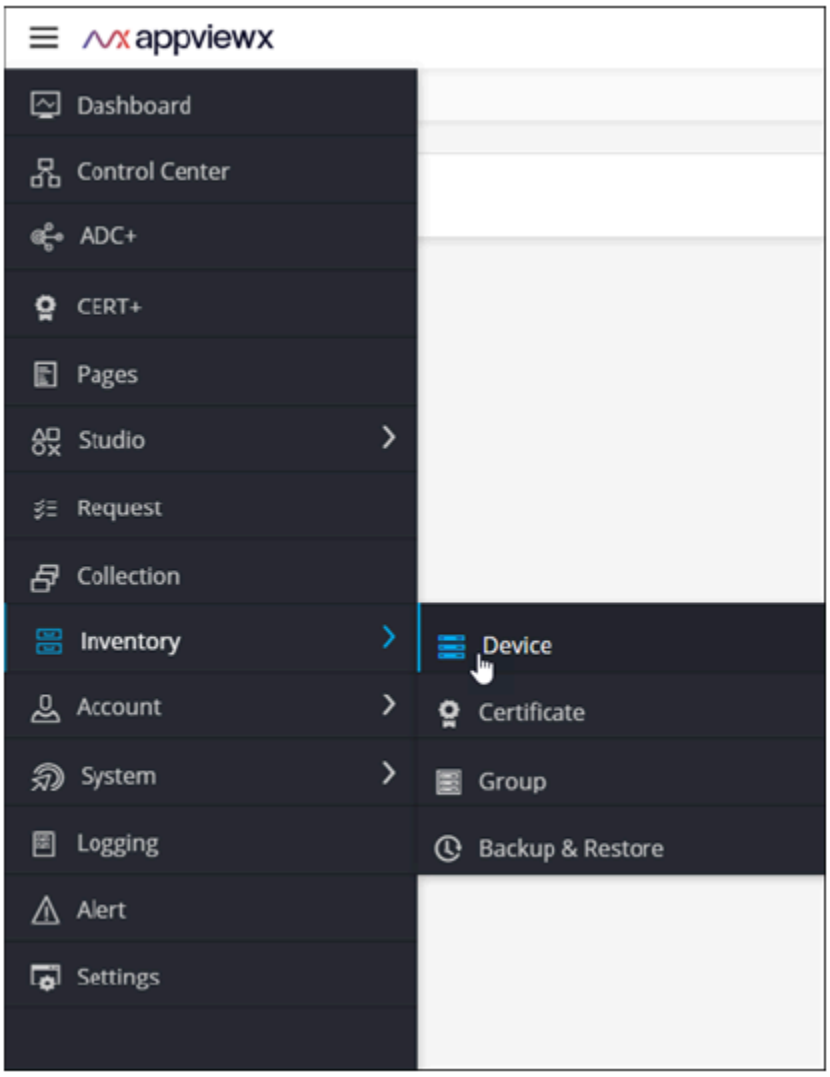
In this section, you will be guided to integrate the Utimaco HSM with the AppViewX SaaS.

• Integrating the Fortanix HSM with the AppViewX SaaS

Integrating the Fortanix HSM with the AppViewX SaaS

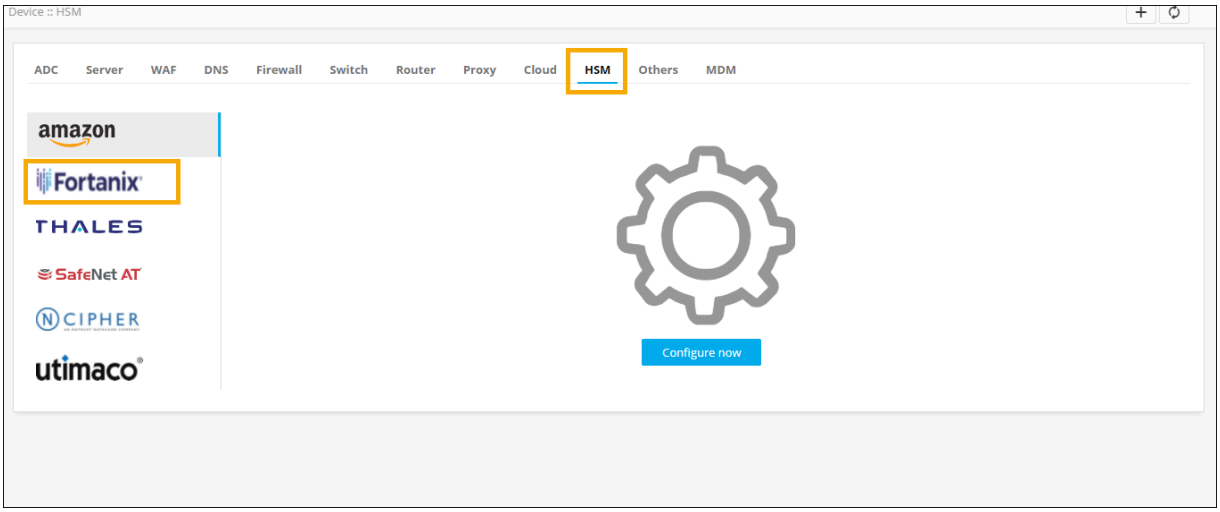
To integrate the Fortanix HSM with the AppViewX SaaS:

1. Login to the AppViewX UI using valid credentials. By default, the **Dashboard** is displayed.
2. From the top-right corner of the **Dashboard**, click ☰.
3. From the menu displayed, select **Inventory** > **Device**.



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

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



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

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	
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.

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

Field	Description
FIPS Mode*	If your Fortanix HSM is running in FIPS mode, Switch On this FIPS mode. Else keep it Off.
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.
So file location*	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 location*	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.

7. Click Save.
8. 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.
9. If the implementation type is CSR Generation, to generate the CSR, follow the steps given here:

- Server certificate
- Client certificate
- Code signing certificate

Thales DPoD

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

• Integrating the Thales DPoD HSM with the AppViewX SaaS

Integrating the Thales DPoD HSM with the AppViewX SaaS

To integrate the Thales DPoD HSM with the AppViewX SaaS:

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:

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

source setenv

export ChrystokiConfigurationPath=/appviewx/dependencies/external_libs/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: {cc_installed_path)_deps/external_lib/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  {CC_INSTALLATION_PATH}/deps/external_libs/hsm/safenet/lunaclient

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

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

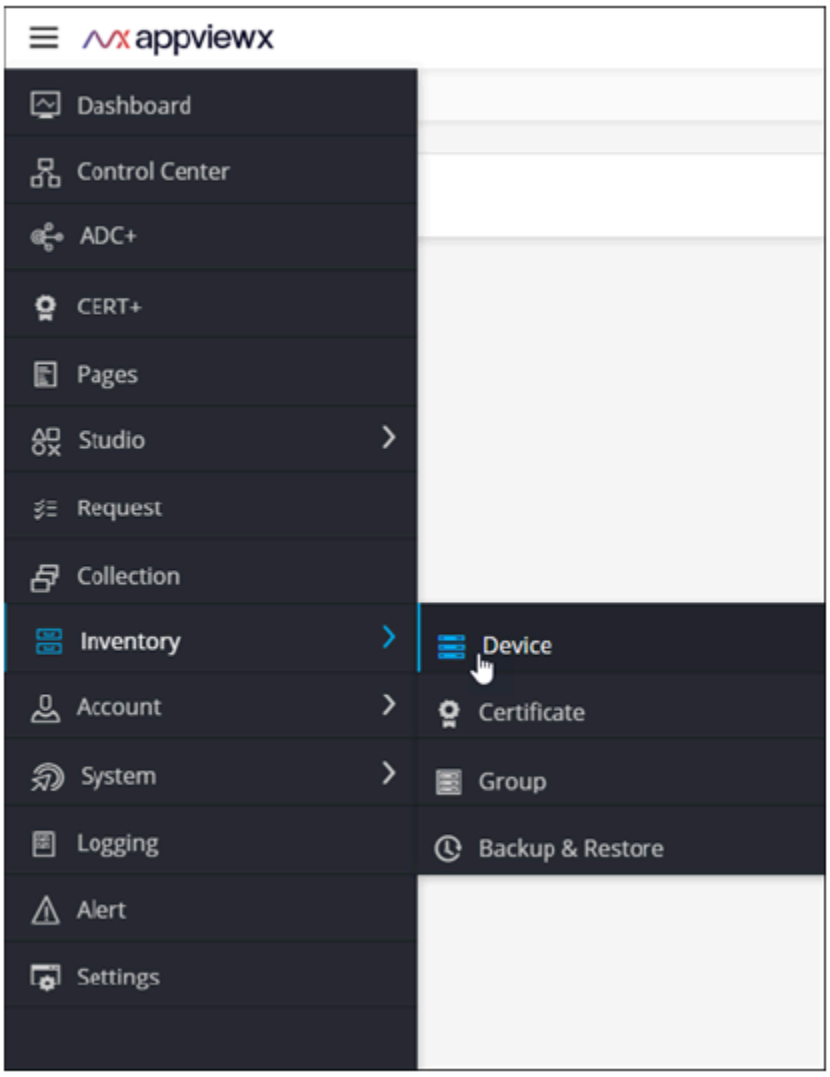
```
cd {CC_INSTALLATION_PATH}/deps/external_libs/hsm/

sudo chmod 755 Chrystoki.conf
```

AppViewX can now communicate with all HSM devices.

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

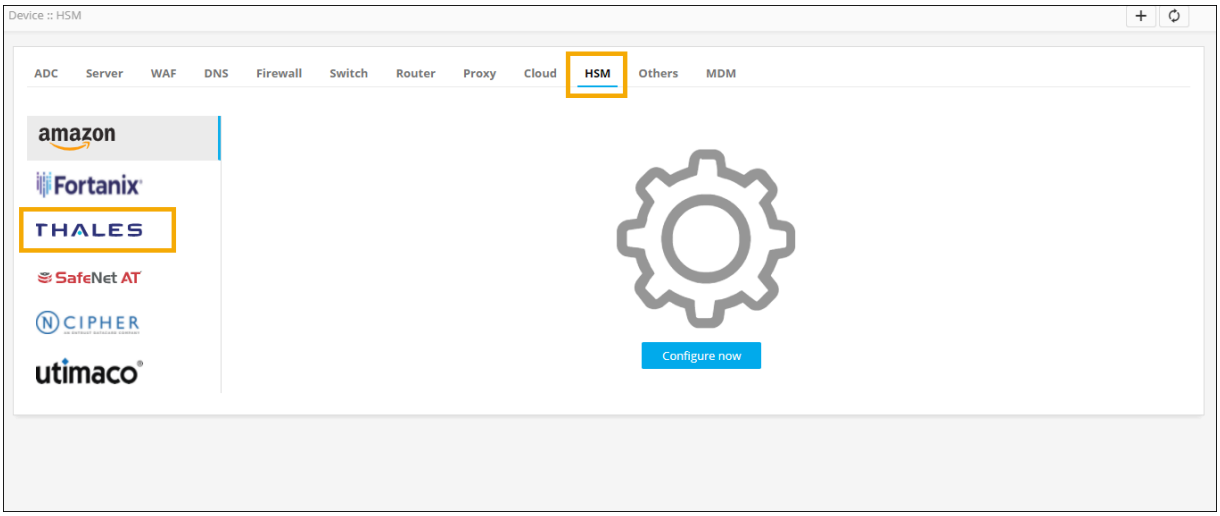
```
list kubectl get pods -n cc

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

13. Login to the AppViewX UI using valid credentials.
14. By default, the Dashboard is displayed. From the top-right corner of the Dashboard, click ☰.
15. From the menu displayed, select Inventory > Device.

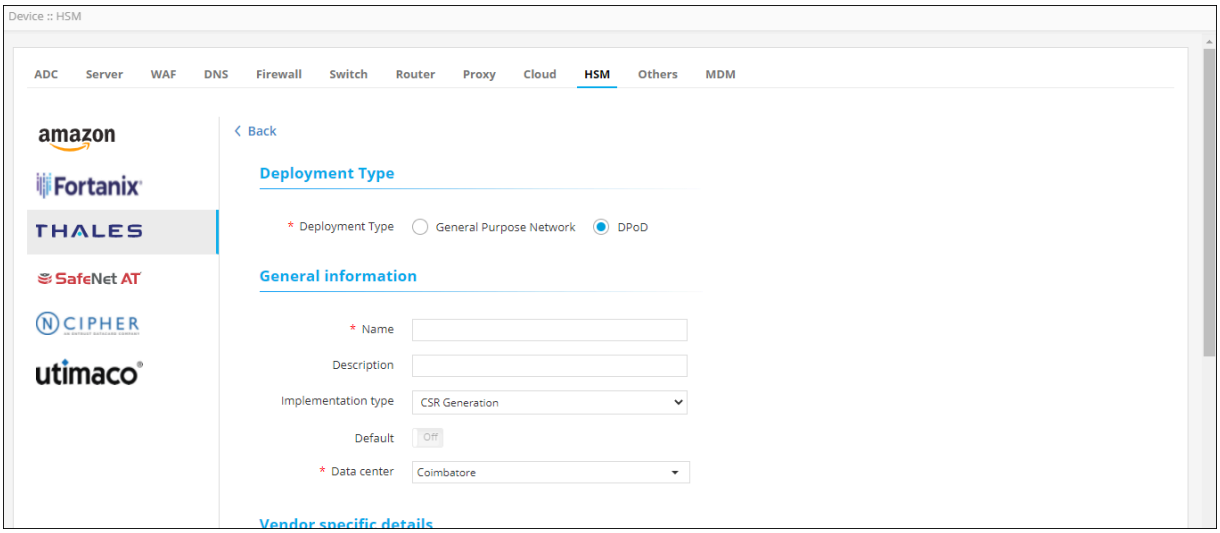


The **Device :: ADC** page is displayed.

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



17. Click Configure Now or from the top right corner of the screen. The Device :: HSM page is updated to display the fields required to integrate Thales-DPoD with the AppViewX SaaS.



18. In the Deployment Type section, for the Deployment Type field, select DPoD.
19. In the General Information section, enter/select the following details:

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	
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.

20. In the **Vendor specific** details section, enter/select 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
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 location*	The SO file is used to facilitate the communication between the HSM and AppViewX. To upload the .so file: a. Click Browse. b. Navigate to the location of the .so file. c. Select the .so file and click Open.

Field	Description
Config file location*	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.

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, to generate the CSR, follow the steps given here:
    - Server certificate
    - Client certificate
    - Code signing certificate

Thales GPN

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

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

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.

• Steps the Configure the Luna Client

Prerequisites

• he 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.

Steps the Configure the Luna Client

Sample values:

• 192.143.161.67: HSM device.
• Ptpll186: Hostname of the server/AppViewX device on which the HSM client is being installed.

1. Copy and paste the HSMDVD to a particular server.
2. Navigate to the location of the install.sh file using the command given below:

```
cd /data/HSMDVD/Software DVD/linux/64
```

3. Execute the chmod command as shown below:

```
sudo chmod 755 install.sh

sudo chmod 755 common
```

4. Run the install.sh file using the command given below:

```
sudo ./install.sh
```

5. When directed, as input for Enter install directory: [/usr], enter the following custom path:
   {CC_INSTALLATION_PATH}/deps/external_libs/hsm
6. When prompted to choose the Luna products to be installed, select Luna SA and enter next (n).
7. When prompted to choose the Luna components to be installed, choose the following packages:

   a. Luna Software Development Kit (SDK)

   b. Luna JSP (Java)

   c. Luna JCProv (Java)

   d. Crypto Command Center Provisioning Client (Not applicable for Luna client v7.2)

8. After installing the Luna client, navigate to the directory in which the Luna client is installed. Path:
   {CC_INSTALLATION_PATH}/deps/external_libs/hsm/safenet/lunaclient/bin
9. Import the server certificate to the Luna client using the following command:

```
sudo scp elabhsm1par58usr@72.138.111.35:server.pem
```

10. Register the HSM server certificate with the client using the following command:

```
sudo ./vtl addServer -n 72.138.111.35 -c server.pem ⇀ >New IP for HSM>
```

11. Create a Client Certificate from the local Linux machine using the following command:

```
sudo ./vtl createCert -n ptpll186
```

12. Export the Client certificate to the node where the HSM is to be configured:

```
sudo scp {CC_INSTALLATION_PATH}/deps/external_libs/hsm/safenet/lunaclient/cert/client/ptpll186.pem elabhsm1par58usr@72.138.111.35:
```

13. Register the Client certificate on the HSM device.

```
client register -client ptpll186 -hostname ptpll186
```

14. Assign the client to a partition using the following command:

```
client assignPartition -client ptpll186 -partition elabhsm1par58
```

Note: Execute this command from the HSM device using the SSH login.

15. Verify the HSM setup on the node on which AppViewX is installed.

```
cd {CC_INSTALLATION_PATH}/deps/external_libs/hsm/safenet/lunaclient/bin

./vtl verify
```

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

```
cd  {CC_INSTALLATION_PATH}/deps/external_libs/hsm/safenet/lunaclient

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

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

```
cd {CC_INSTALLATION_PATH}/deps/external_libs/hsm/

sudo chmod 755 Chrystoki.conf
```

20. AppViewX can now communicate with all HSM devices.

Integrating the Thales GPN HSM with the AppViewX SaaS

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 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: **{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: {cc_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  {CC_INSTALLATION_PATH}/deps/external_libs/hsm/safenet/lunaclient

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

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

```
cd {CC_INSTALLATION_PATH}/deps/external_libs/hsm/

sudo chmod 755 Chrystoki.conf
```

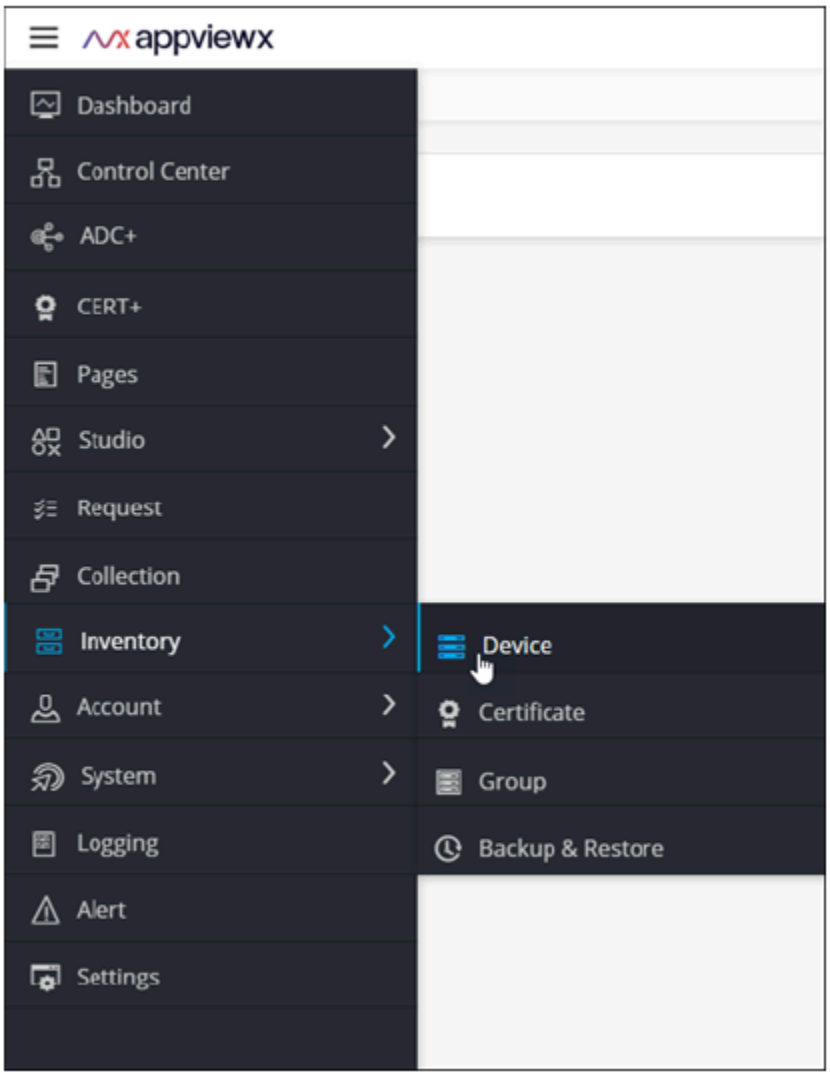
AppViewX can now communicate with all HSM devices.

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

```
list kubectl get pods -n cc

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

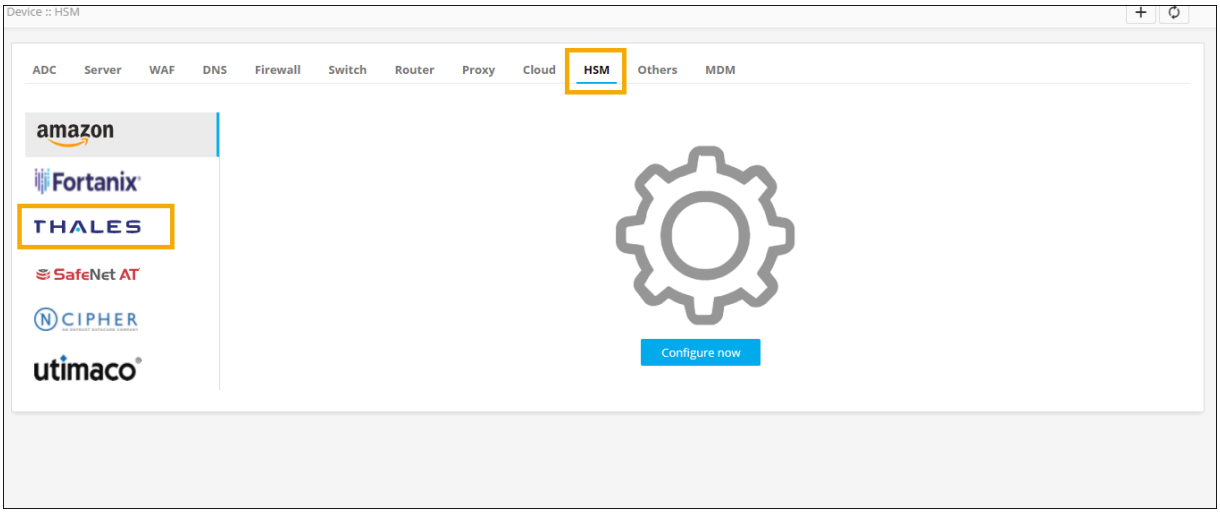
12. Copy the jcprov jar from the location {CC_INSTALLATION_PATH}/deps/external_libs/hsm/safenet/lunaclient/jcprov/lib/jcprov.jar to the location {CC_INSTALLATION_PATH}/deps/external_libs/hsm/.

13. Login to the AppViewX UI using valid credentials. By default, the Dashboard is displayed.
14. From the top-right corner of the Dashboard, click ☰.
15. From the menu displayed, select Inventory > Device.

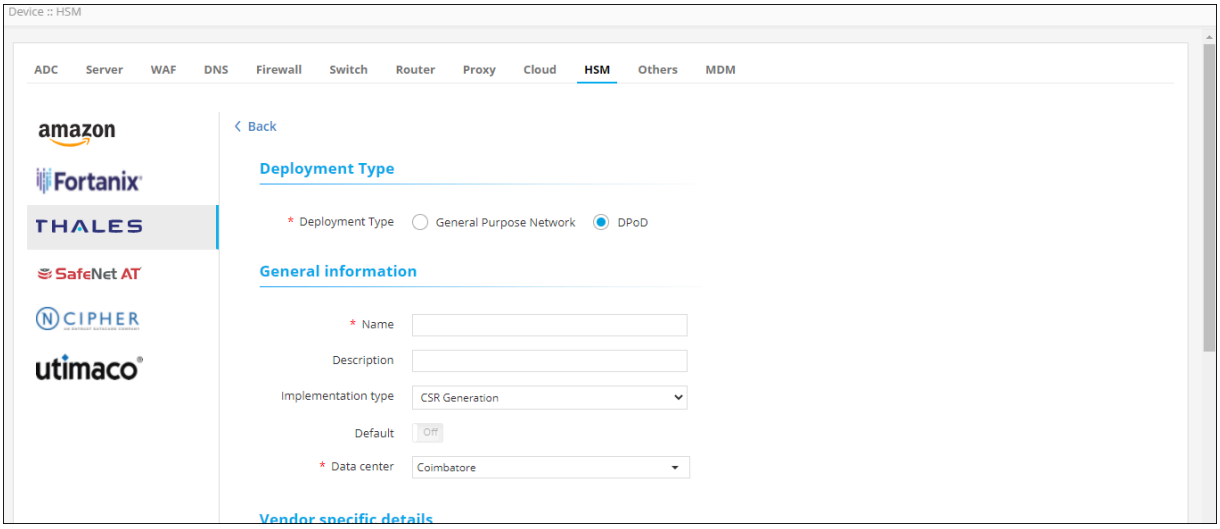


The **Device :: ADC** page is displayed.

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



17. Click Configure Now or from the top right corner of the screen. The Device :: HSM page is updated to display the fields required to integrate Thales-DPoD with the AppViewX SaaS.



18. In the Deployment Type section, for the Deployment Type field, select General Purpose Network.
19. In the General Information section, enter/select the following details:

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	NA
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.

20. In the **Vendor specific** details section, enter/select 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.
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.
SO file location*	The SO file is used to facilitate the communication between the HSM and AppViewX. Enter the relative path of the **.so** file.
Config file location*	The Config file is used to facilitate the communication between the HSM and AppViewX. Enter the relative path of the **.conf** file.

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:

    a. Check the installation path for the HSM.

    b. Ensure that all required permissions have been enabled.

23. If the implementation type is CSR Generation, to generate the CSR, follow the steps given here:

    a. Server certificate

    b. Client certificate

    c. Code signing certificate

Chapter 8: Managing Alerts

- Viewing Existing Alerts
- Setting the Record Count Preference for Viewing Alerts
- Configuring Alerts
- Editing Alerts
- Deleting Alerts
- Searching for Alerts
- Purging Alerts

Viewing Existing Alerts

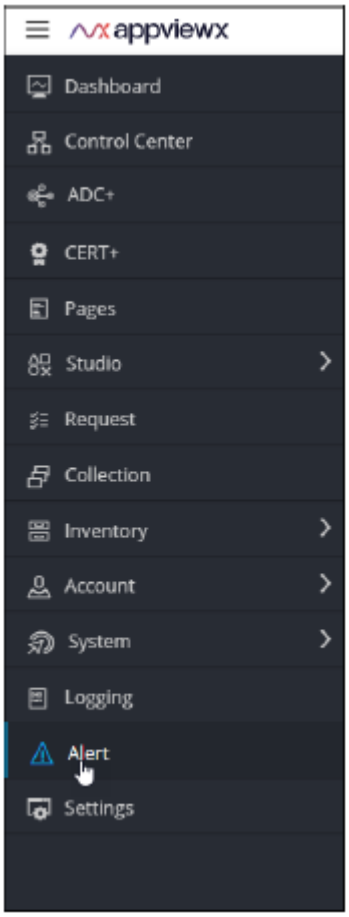
AppViewX lets you view all alerts in one place as well as groups them under the above mentioned categories for a segregated viewing.

- Viewing All Alerts
- Viewing AppViewX Alerts
- Viewing Certificate Alerts
- Viewing SSH Alerts
- Viewing Syslog Alerts

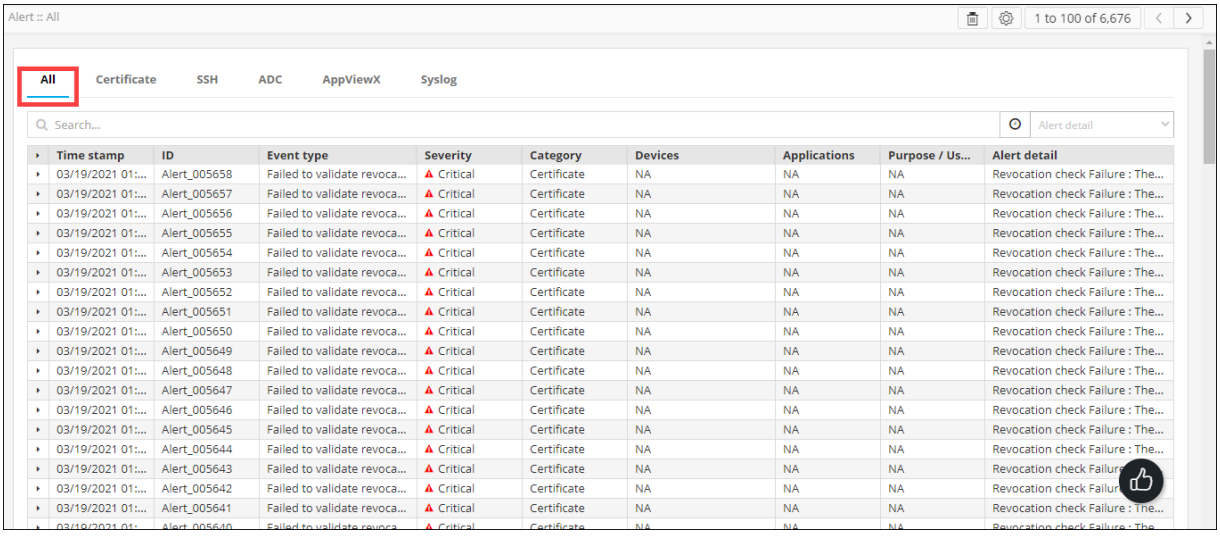
Viewing All Alerts

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



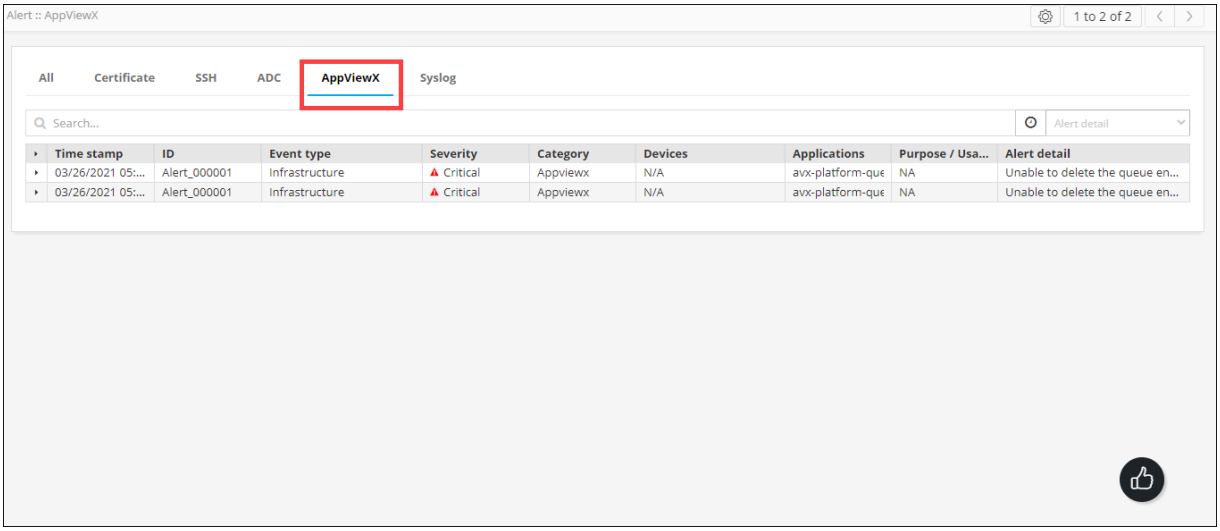
4. For each alert, this page displays the following details:

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	The purpose or usage of the alert.
Alert detail	Description of the alert.

Viewing AppViewX Alerts

To view the AppViewX alerts:

1. On the Alert page, click the AppViewX tab.



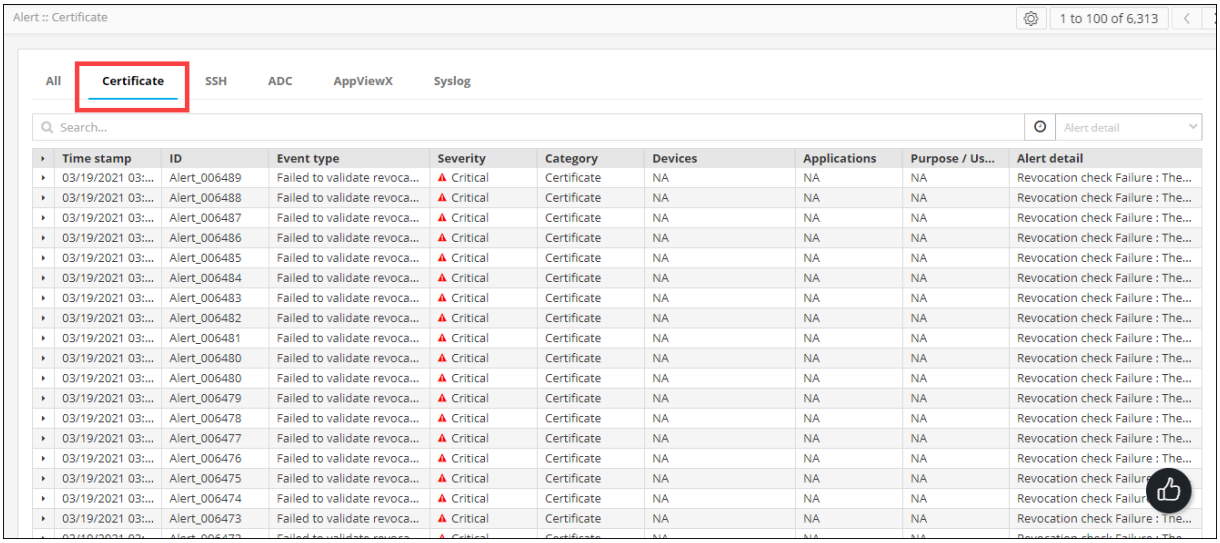
2. For the AppViewX alerts, the page displays the following details:

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	The purpose or usage of the alert.
Alert detail	Description of the alert.

Viewing Certificate Alerts

To view the Certificate alerts:

1. On the Alert page, click the Certificate tab.



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

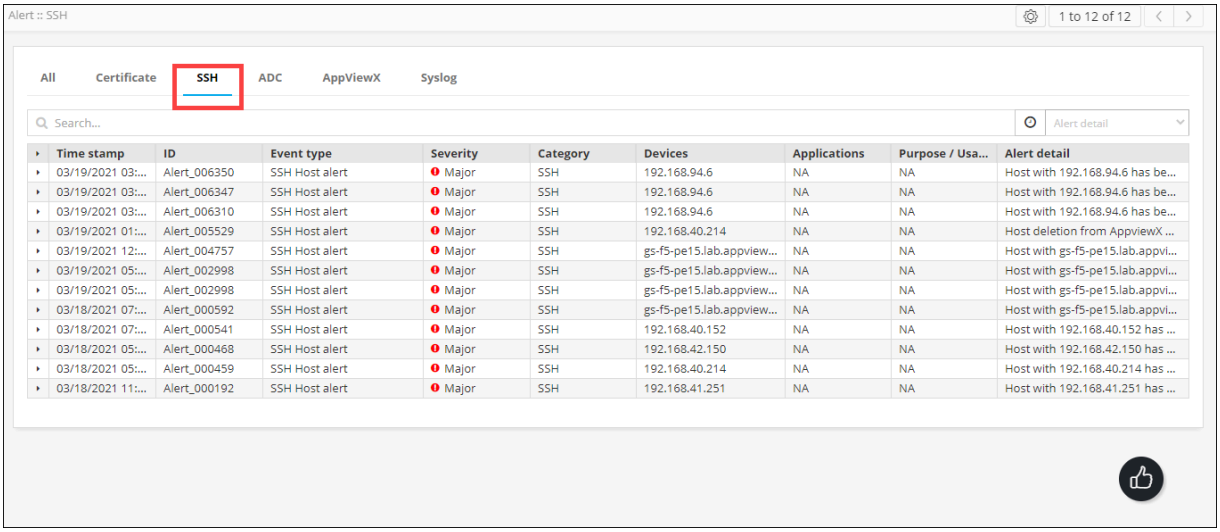
Field	Description
Timestamp	Date and time at which the event, which triggered the alert, occurred
ID	Alert ID
Event type	Type of the event that triggered the alert
Severity	Alert severity. AppViewX identifies the following severity levels (as described above): • Critical • Fatal • Major • Minor
Category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

Field	Description
Applications	Application that triggered the alert.
Purpose/Usage	The purpose or usage of the alert.
Alert detail	Description of the alert.

Viewing SSH Alerts

To view the SSH alerts:

1. On the Alert page, click the SSH tab.



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

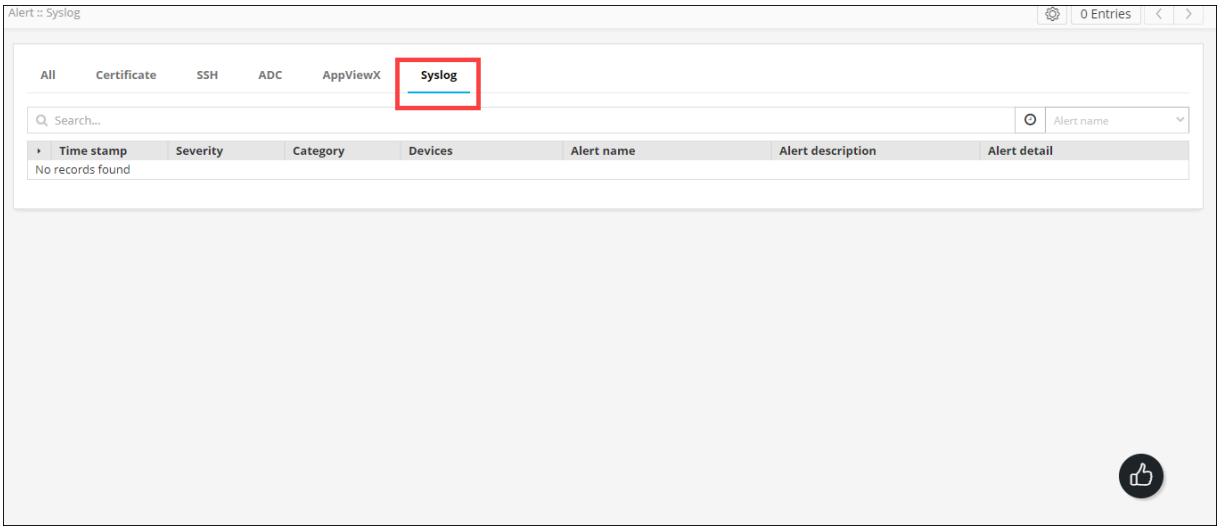
Field	Description
Time stamp	Date and time at which the event, which triggered the alert, occurred
ID	Alert ID
Event type	Type of the event that triggered the alert
Severity	Alert severity. AppViewX identifies the following severity levels (as described above): • Critical • Fatal

Field	Description
	• 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	The purpose or usage of the alert.
Alert detail	Description of the alert.

Viewing Syslog Alerts

To view the Syslog alerts:

1. On the Alert page, click the Syslog tab.



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

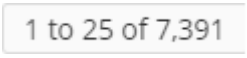
Field	Description
Timestamp	Date and time at which the event, which triggered the alert, occurred
ID	Alert ID
Event type	Type of the event that triggered the alert

Field	Description
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	The purpose or usage 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.

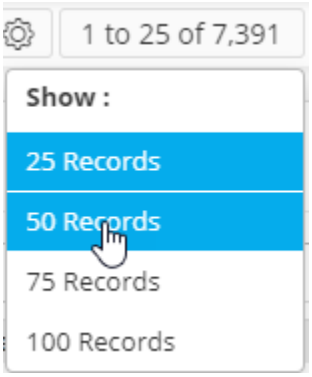
To set the record count preference:

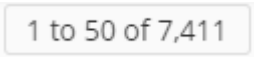
1. On the Alert :: All page, from the top-right corner of the screen, click 

.

> **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:

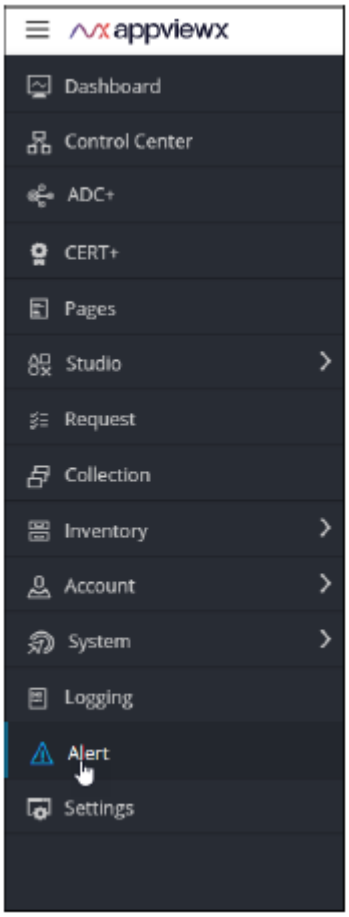
- Certificate
- Syslog
- SSH
- AppViewX
- ADC

- Configuring ADC Alerts
- Configuring AppViewX Alerts
- Configuring Certificate Alerts
- Configuring SSH Alerts
- Configuring Syslog Alerts

Configuring ADC Alerts

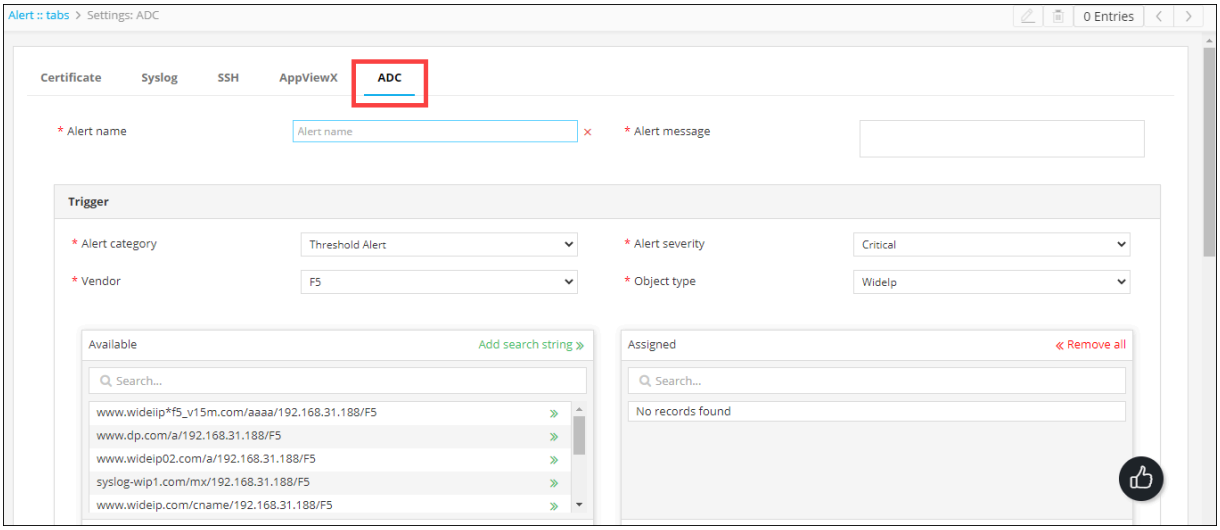
To configure ADC alerts:

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.
3. The Alert :: All page is displayed (by default).
4. From the top-right corner of the screen, click the ⚙ icon.
5. The Settings :: Certificate page is displayed.
6. To configure Syslog alerts, click ADC.

7. The Settings :: ADC page is displayed.



8. 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.

***:Mandatory**

9. 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

Field	Description
Vendor	From the drop-down menu, select the vendor whose device or devices you want to set an alert for.
Object type	From the drop-down menu, select the vendor object that you want to set an alert for. **Note:** The contents of this field will vary depending on the vendor selected.
Detail contains	**Note:** This field is applicable only for the Device Alert category.
Available	Depending on the Object type and Vendor selected, a list of all available ADC objects or devices is displayed here. To add an object/device to the alert, click the icon for that object/device.
Add search string	Instead of adding devices manually, AppViewX lets you automatically assign all existing devices or objects that match your criteria. To do this: a. In the Available section, in the Search field, enter the search criteria. b. Click Add search string. **Note:** The benefit of using a search string rather than selecting devices manually is that the search string continues to work in the background and auto-assigns all new devices that match the search criteria.
Assigned	To add an object to the Assigned column, click the check box corresponding to that object.

***:Mandatory**

10. In the Alert condition section, enter the following details:

Field	Description
Alert interval*	From the drop-down menu, from the following options, select how often you want the system to check for breaches of the threshold levels that you are about to define: • 10 seconds • 20 seconds • 30 seconds • 40 seconds • 50 seconds • 60 seconds
Cool off period*	From the drop-down menu, from the following options, select how much time the system should wait before sending another alert about a continuing threshold breach: • 10 minutes • 20 minutes • 30 minutes

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

11. 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 🗑 .
12. In the Action section, to send the syslog alert as an email, execute the steps for configuring SMTP for email alerting.
13. Enter the following details:

Field	Description
Email configuration	To send the syslog alert as an email, select this check box.

Field	Description
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.

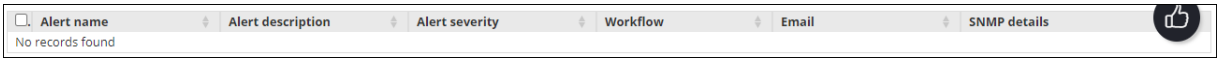
***:Mandatory**

14. 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.

***:Mandatory**

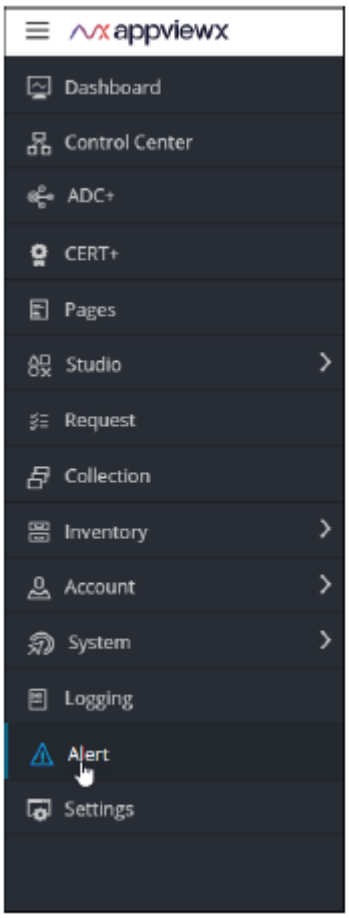
15. To save the ADC alert configure above, click Add. The saved details are displayed in the table shown at the bottom of the screen.



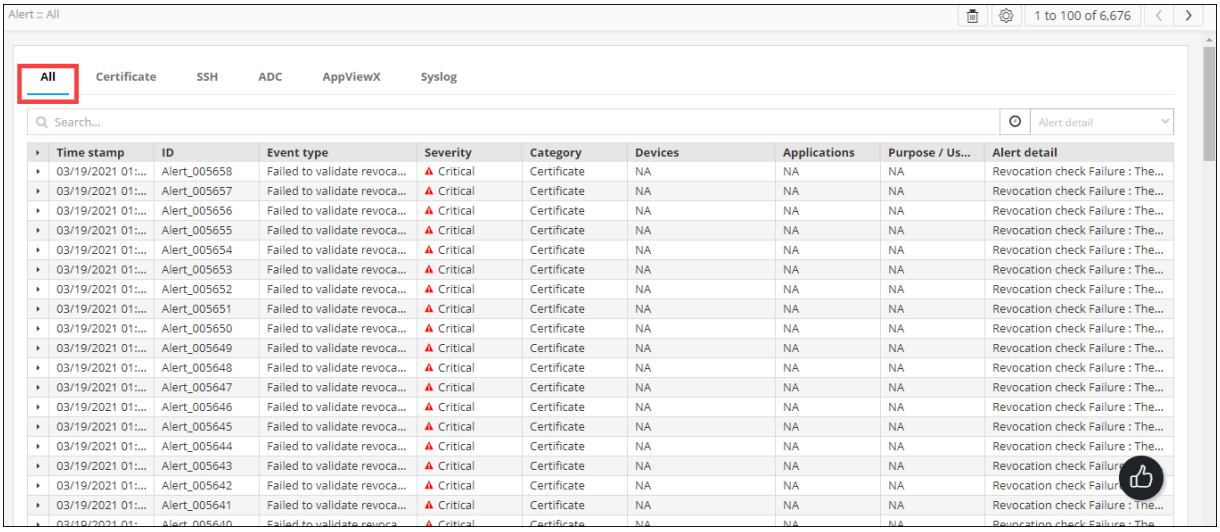
Configuring AppViewX Alerts

To configure AppViewX alerts:

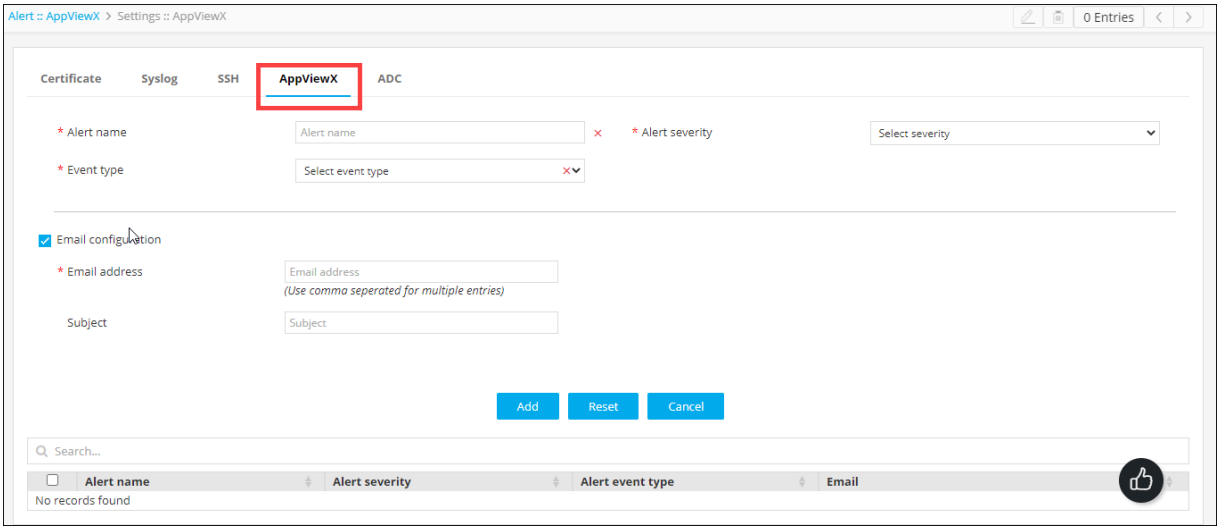
1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.
2. From the menu displayed, click Alert.



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



4. From the top-right corner of the screen, click the  icon.
5. The Settings :: Certificate page is displayed.
6. To configure AppViewX alerts, click the AppViewX tab.
7. The Settings :: AppViewX page is displayed.



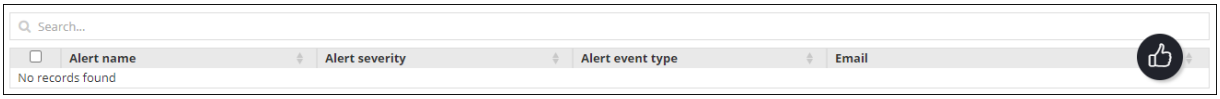
8. Enter the following details:

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

Field	Description
	• Critical • Fatal • Major • Minor • Notification
Event type*	From the drop-down menu, from the following options, select the event type that will trigger this alert: • Infrastructure • Application Discovery
Email configuration	To send the certificate alert as an email, select this check box. **Note:** For AppViewX alerts, this feature is enabled by default.
Email address*	To send the certificate alert as an email, enter the email address to which this specific certificate alert will be sent. **Note:** Separate multiple email addresses with a comma.
Subject	To send the certificate alert as an email, enter a subject line.

***:Mandatory**

9. To save the alert to the AppViewX system, click Add.
10. The saved details are displayed in the table shown at the bottom of the screen.



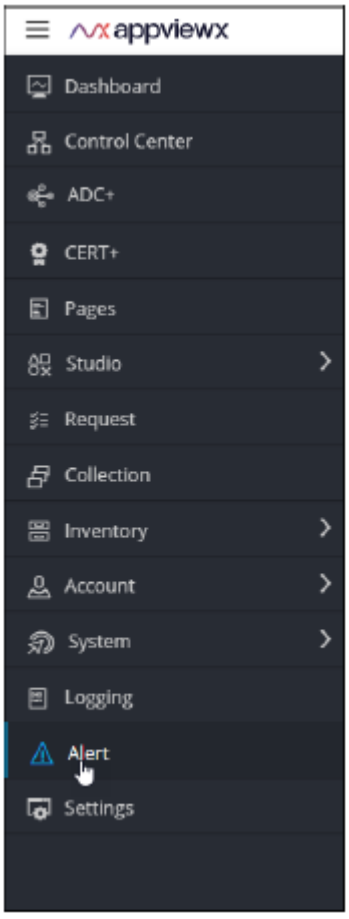
Configuring Certificate Alerts

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

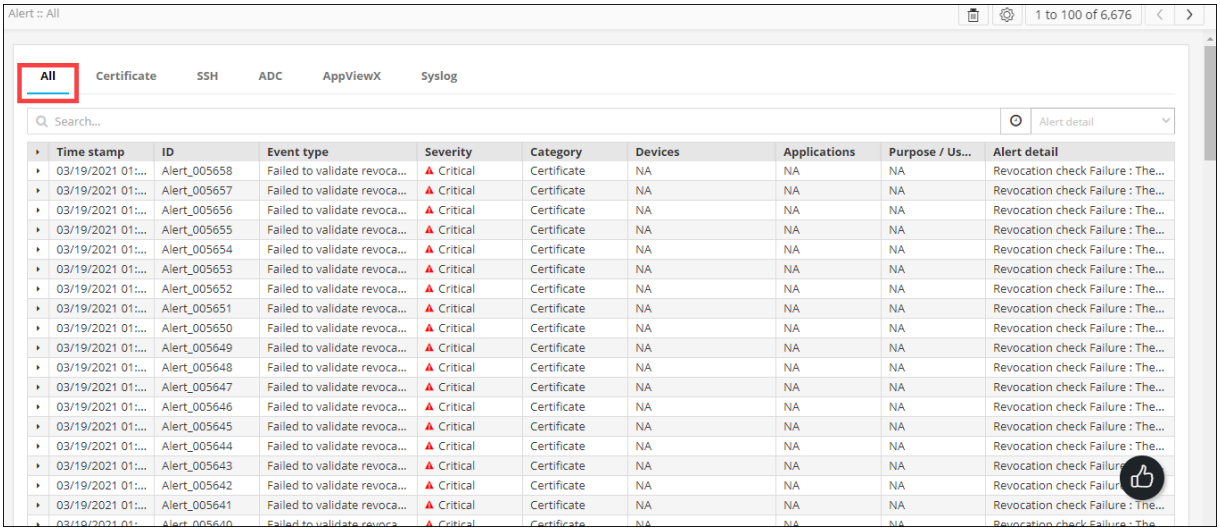
- Certificates need to be validated
- Certificates are set to expire
- Certificates cannot be synchronized

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.



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



4. From the top-right corner of the screen, click the  icon.
5. The Settings :: Certificate page is displayed, with the Certificate tab open by default.
6. 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. **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

Field	Description
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
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.

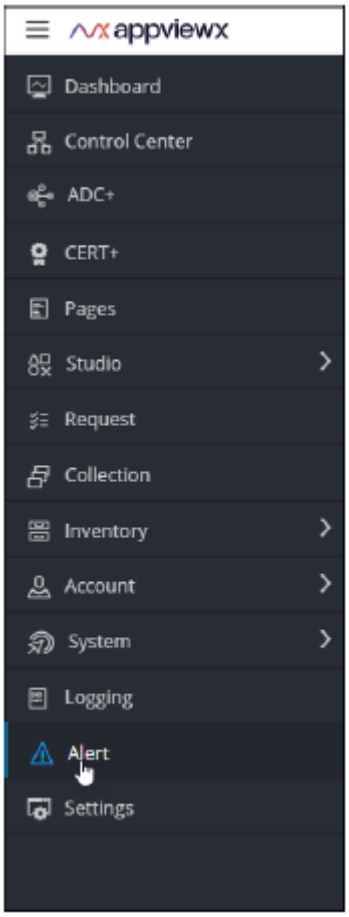
Field	Description
	Note: Separate multiple email addresses with a comma.
Subject	To send the certificate alert as an email, enter a subject line.
SNMP configuration	To use the Simple Network Management Protocol for sending the alert, select this check box.
Destination IP*	Enter the destination IP address 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.

7. 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 SSH Alerts

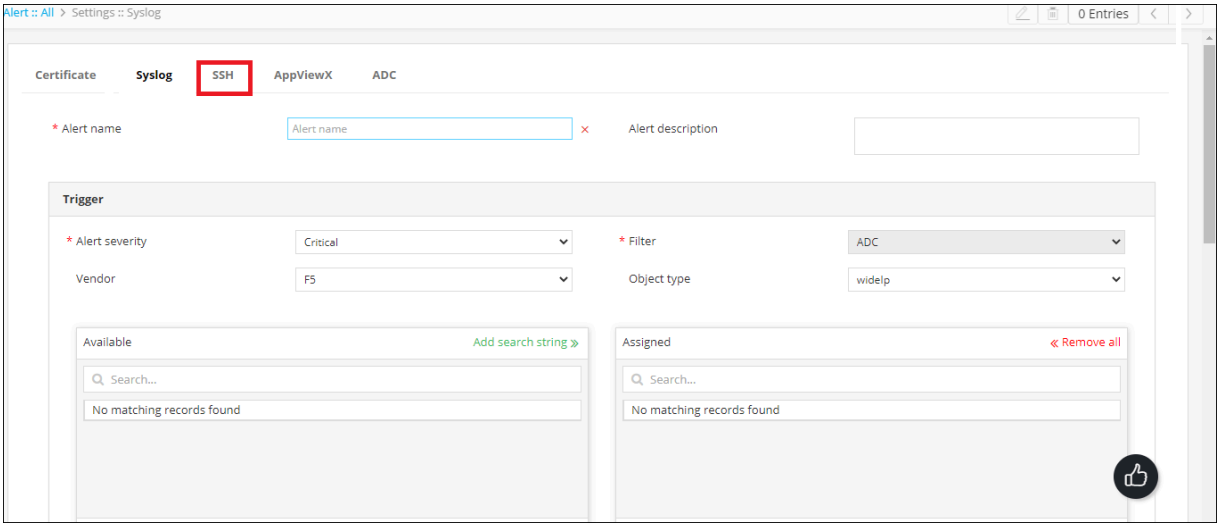
To configure syslog alerts:

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.
3. The Alert :: All page is displayed (by default).
4. From the top-right corner of the screen, click the ⚙ icon.
5. The Settings :: Certificate page is displayed.
6. To configure Syslog alerts, click SSH.

7. The Settings :: SSH page is displayed.



8. 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. **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: • SSH key expiry alert • Compliance alert • SSH key push failure alert • SSH discovery failure alert • SSH key deletion alert • SSH host modify/delete alert

Field	Description
Expires in (days)*	From the drop-down menu, select a severity for the alert from the following options: • Critical • Major • Notification
Key alert criterion*	**Note:** This field is applicable only for the SSH key push failure alert and the SSH key deletion alert. Select the keys you want to include in the alert, from the following options: • Logged in user keys. • All user keys.
SSH keygroup*	**Note:** This field is applicable only for the Compliance alerts, SSH key push failure alert, and SSH key deletion alert. From the drop-down menu, select the key group to be used as the basis for the alert.
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.**
Expires in (days)*	**Note:** This field is applicable only for the SSH key expiry alert. From the drop-down menu, select the number of days until the SSH key expires. The AppView-X system will trigger an alert message when this value is reached.

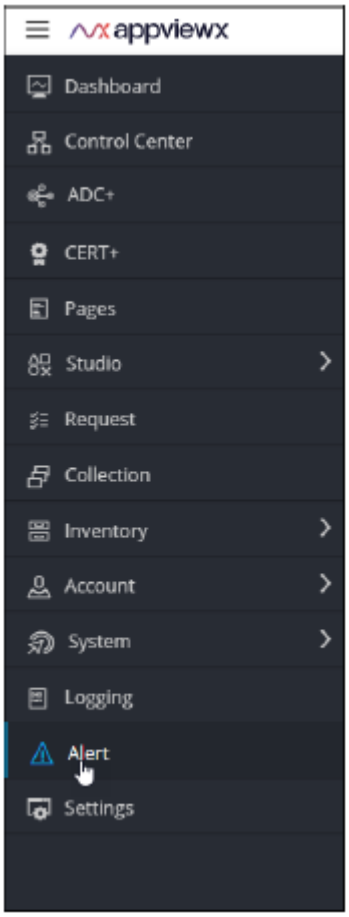
Field	Description
Email configuration	To send the certificate alert as an email, select this check box.
Email address*	To send the certificate alert as an email, enter the email address to which this specific certificate alert will be sent. **Note:** Separate multiple email addresses with a comma.
Subject	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.

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.

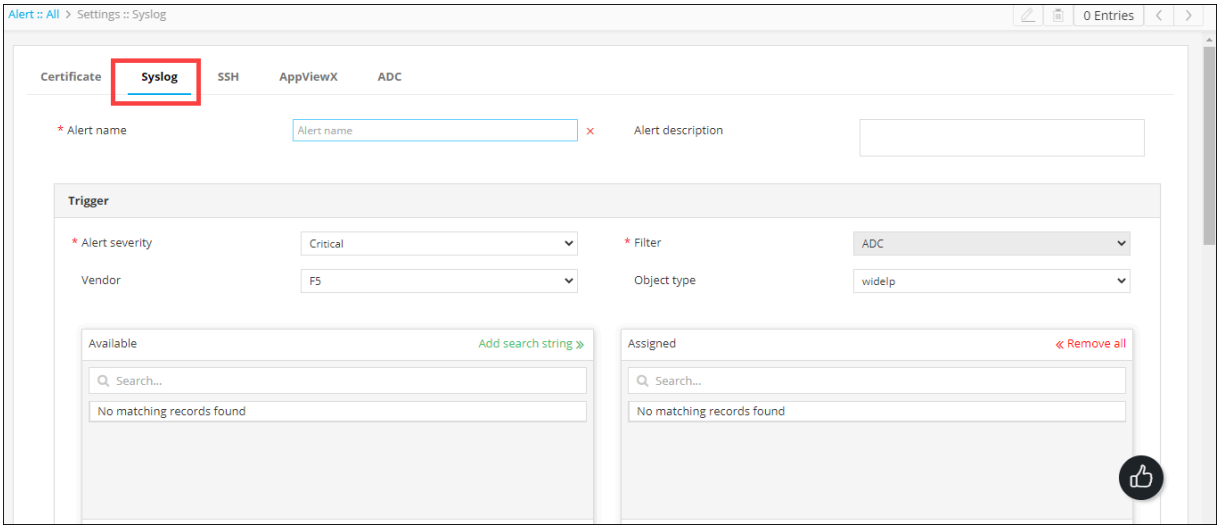
To configure syslog alerts:

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.
3. The Alert :: All page is displayed (by default).
4. From the top-right corner of the screen, click the ⚙ icon.
5. The Settings :: Certificate page is displayed.
6. To configure Syslog alerts, click Syslog.

7. The Settings :: Syslog page is displayed.



8. 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.

9. In the Trigger section, enter the following details:

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)

Field	Description
Object type	Object type for ADC (FQDN, Service IP, Virtual-Service, 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. **Note:** When entering multiple regex patterns/strings, separate the regex strings using commas. The comma works as the BOOLEAN AND operator.

10. In the Action section, enter the following details:

Field	Description
Execute workflow	To select the workflow to trigger:

Field	Description
	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 .

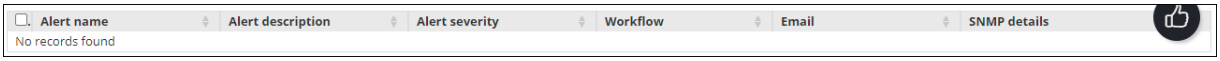
11. To send the syslog alert as an email, execute the steps for configuring SMTP for email alerting.
12. Enter the following details:

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.

13. 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.

14. To save the certificate alerts configuration details, click Add.
15. 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 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. 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:

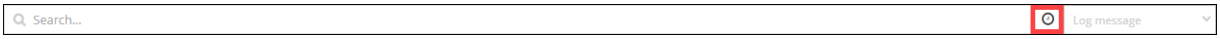
- Based on a timestamp
- Based on the values recorded for each alert

- Based on a Timestamp
- Based on the Values Recorded for each Alert

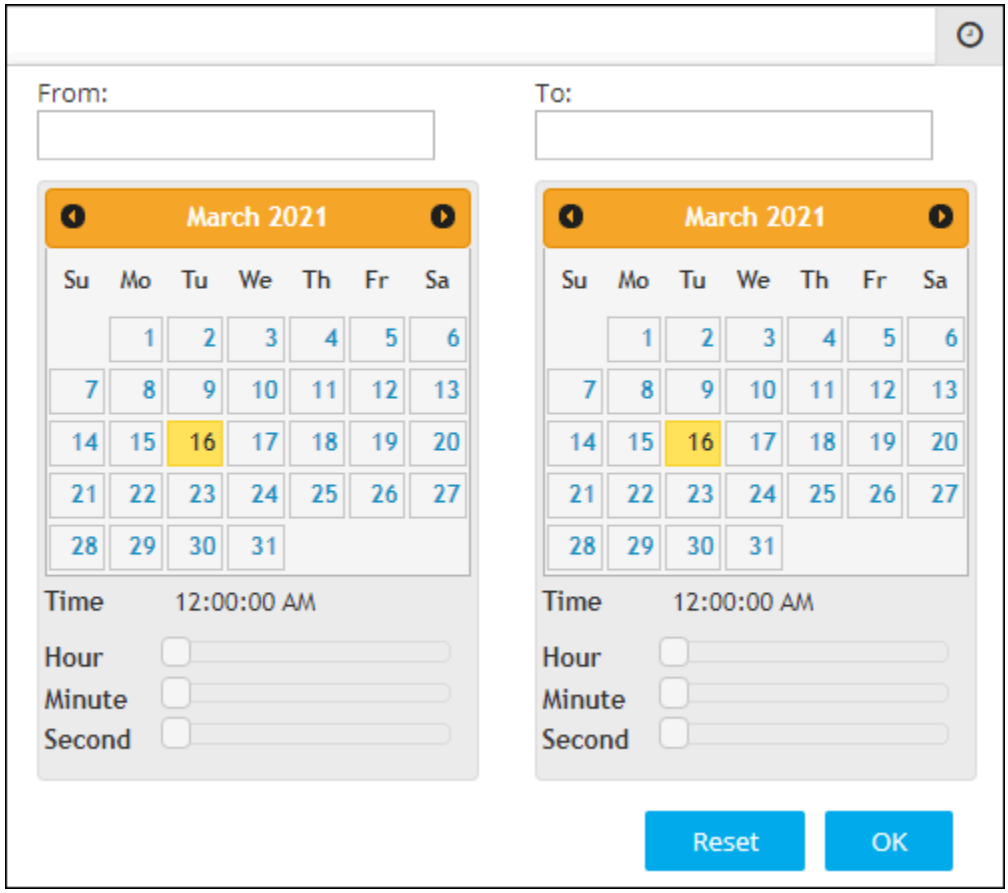
Based on a Timestamp

To search for alerts based on a timestamp:

1. From the Search field on the Alert page, click the  icon.



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

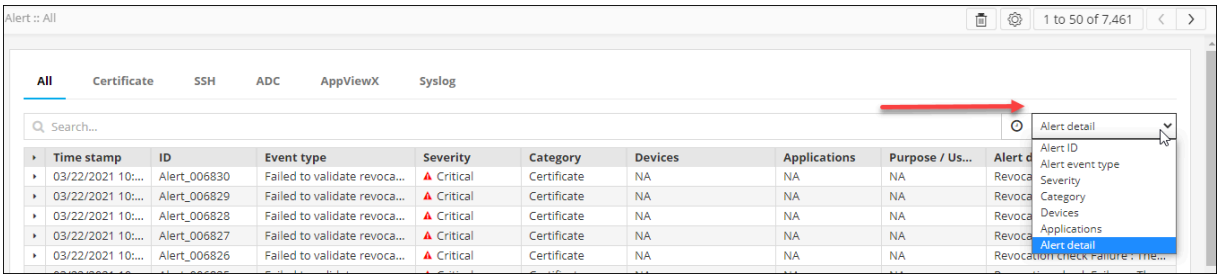


3. To select a date range, in the From and To fields, select the required dates.
4. To set a time, use the Hour, Minute, and Second slider controls.
5. Click OK.
6. The page is updated to display alerts from the selected timestamp.

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.



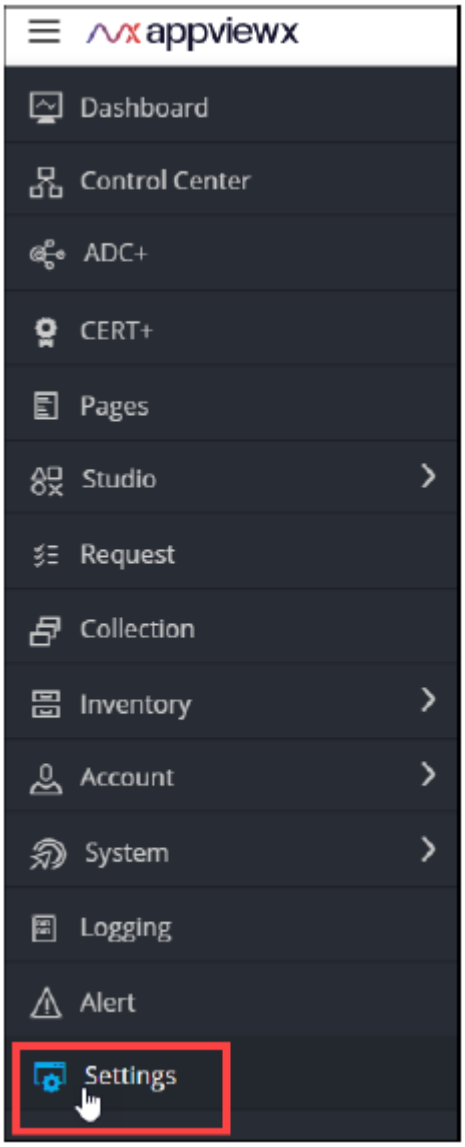
2. In the Search field , enter the search value. For our example, in the Search field, enter the required alert ID. The page is updated to display alerts that fulfil the search criteria.

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.

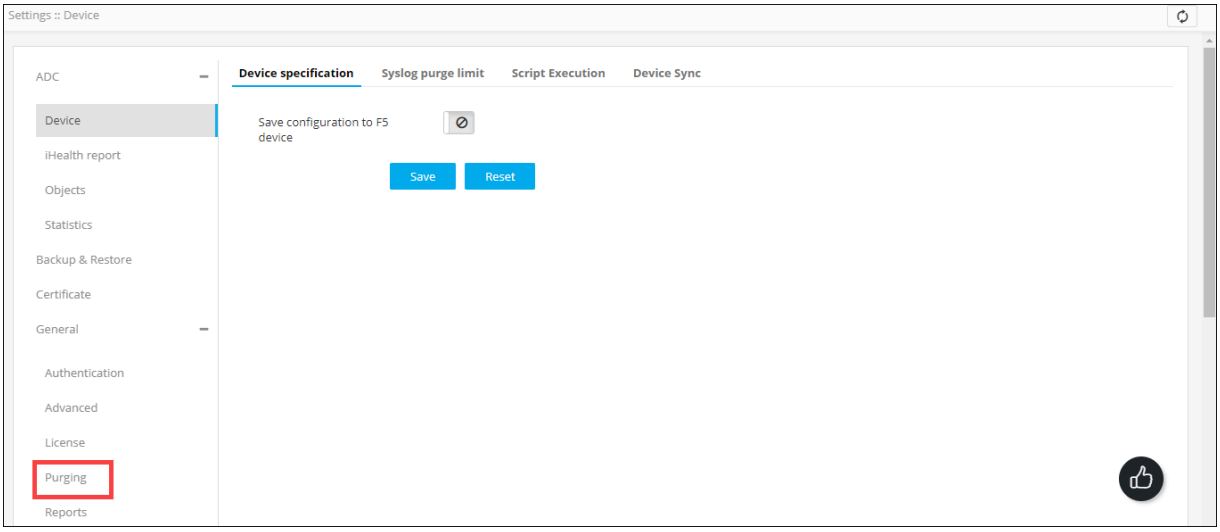
To enable purging of alert records:

1. To access the navigation pane, in the top-left corner of the screen, hover the mouse pointer over the ☰ icon.

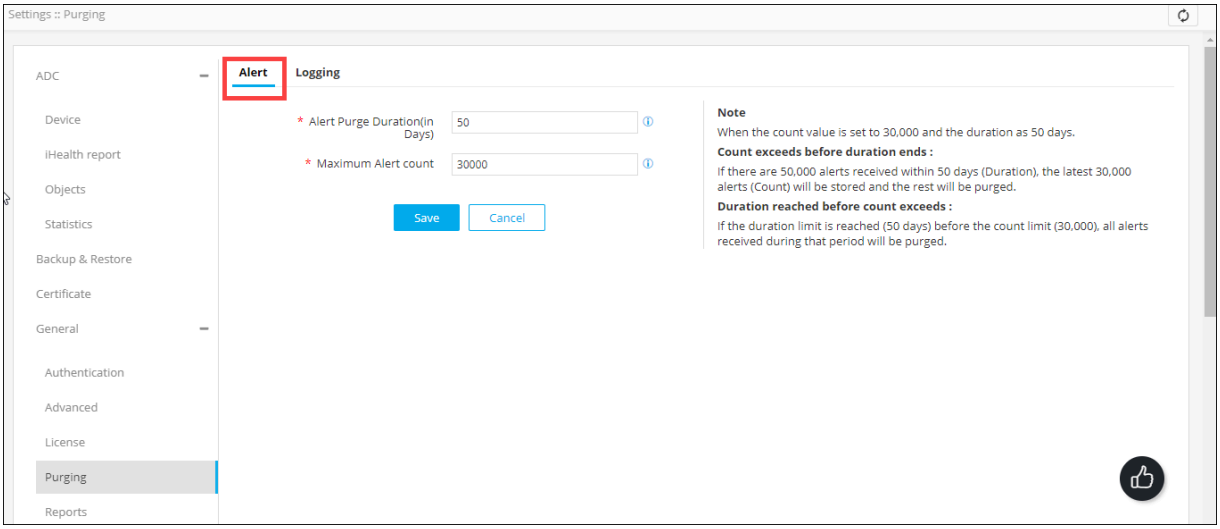


2. From the menu displayed, click Settings.
3. On the Settings page, from the navigation pane on the left, click General.

4. Under General settings, click Purging.



5. The Settings :: Purging screen is displayed.
6. The Alert tab, to configure the alert purging settings is open by default.



7. 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.

***:Mandatory**

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

8. Click Save.

Chapter 9: Managing Licenses

- Getting Started with a Free SaaS Trial
- Viewing License Details
- Upgrading Licenses

Getting Started with a Free SaaS Trial

For users evaluating the AppViewX SaaS solution, which enables turnkey Certificate Lifecycle Management, ADC management and automation, and PKI, AppViewX enables two channels to onboard you for a free trial of the product:

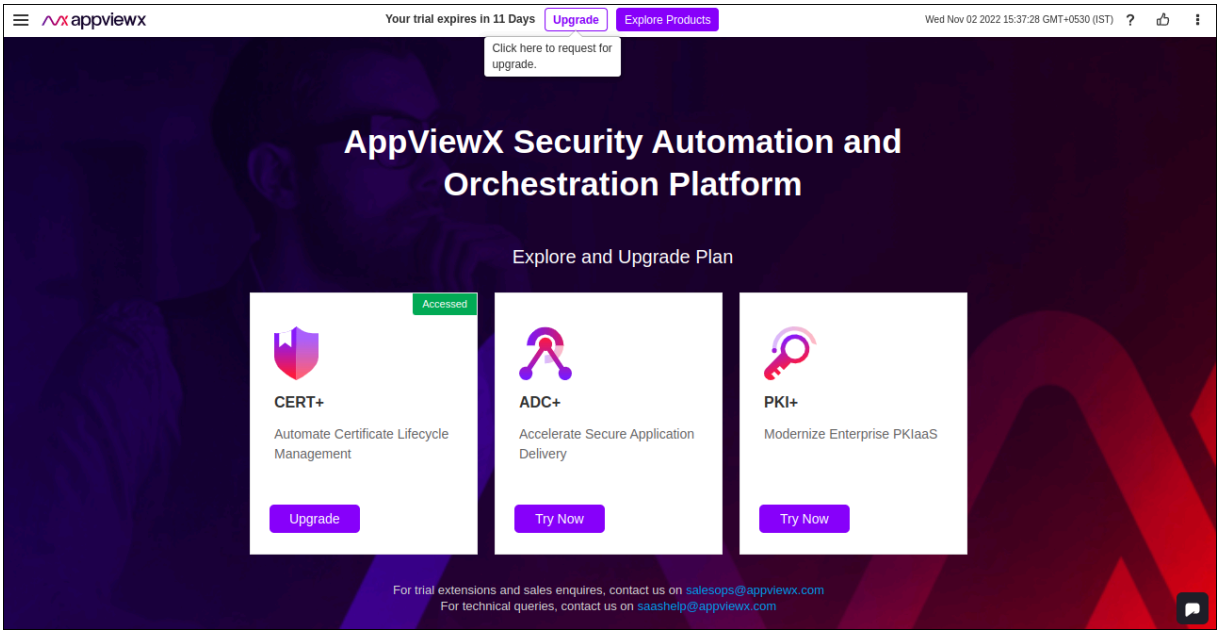
- via the AppViewX website
- via the AWS Marketplace

To get started with the AppViewX SaaS free trial, you can sign up via the AppViewX website and set up the AppViewX SaaS trial, refer to AppViewX SaaS Onboarding and Getting Started Guide.

The following steps explains access to AppViewX SaaS trial:

1. Log in using your user name and the new password.

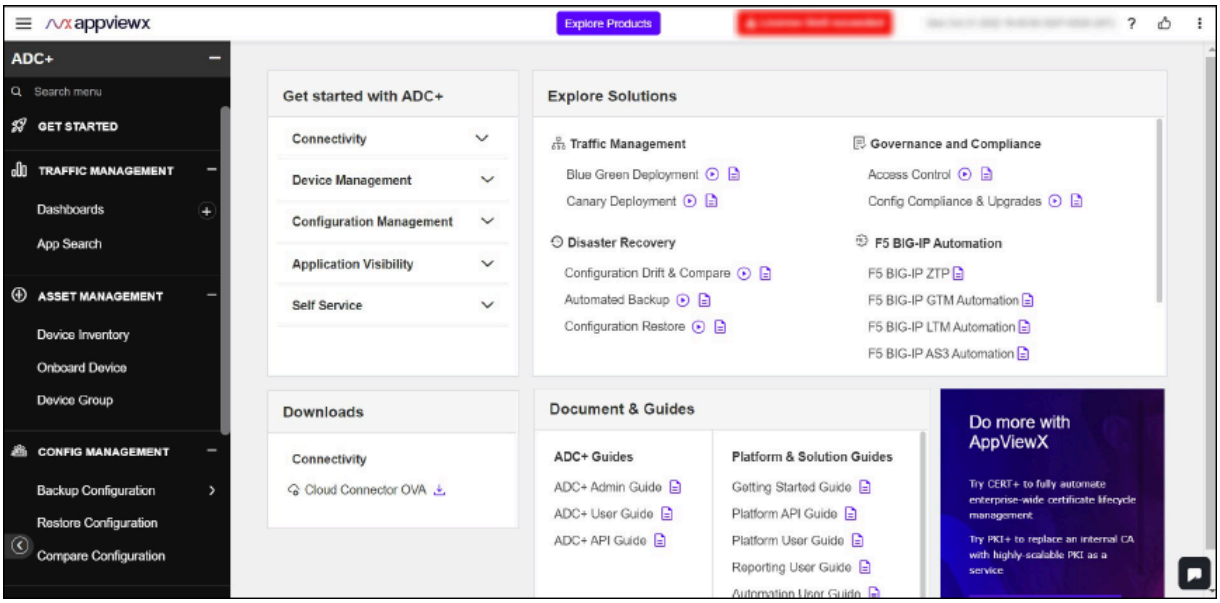
   The **AppViewX SaaS landing page** is displayed.



2. AppViewX SaaS landing page consists of Products, such as **CERT+**, **ADC+** and **PKI+** which allows you to explore and upgrade the plans of the product.

3. To Explore the product details, Click **Try Now** which is provided corresponding to each product.

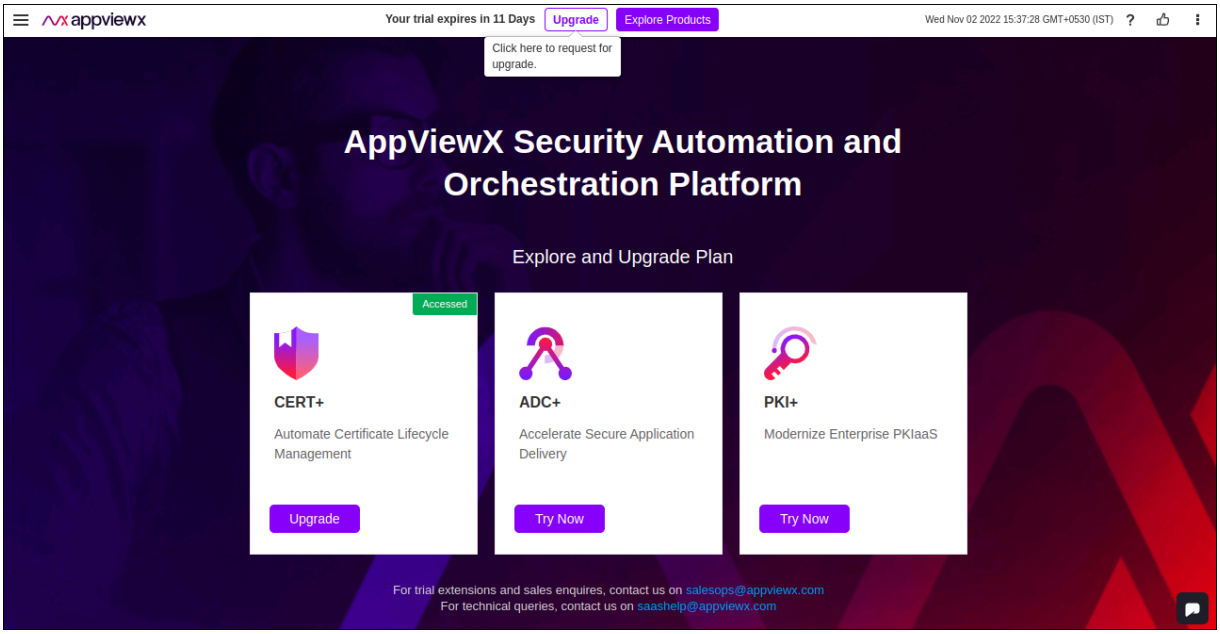
   The corresponding **AppViewX SaaS product landing** page is displayed.



> **Note:** The landing page differs based on a selected AppViewX SaaS product. The following image shows ADC+ landing page.

4. To navigate to the **AppViewX SaaS landing page**, In the screen click on any of the following:
   - AppViewX Logo appviewx
   - Explore Products Explore Products
   - AppViewX Explore Products Explore Products

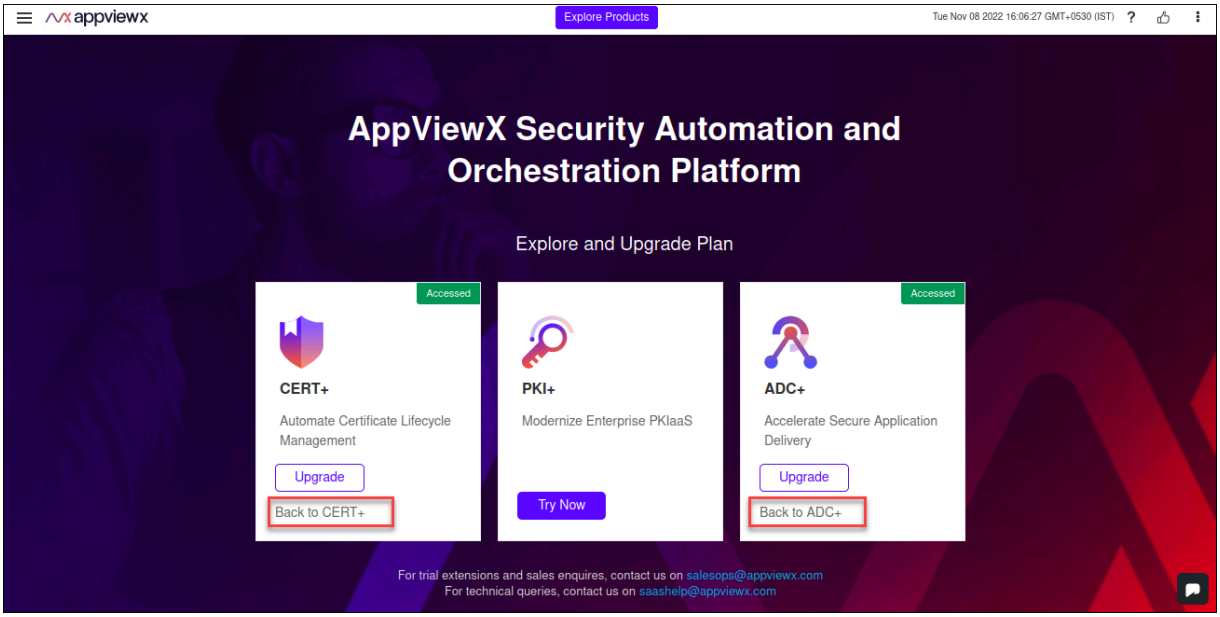
The **AppViewX SaaS landing page** is displayed.



Note: Product can be explored only once as a trial to continue using the product you must upgrade the plan. In the meanwhile, the trial version is accessible up to 30 days. The system alerts the remaining days of the trial period.

5. If once the product is explored by clicking on **Try Now** then it turns into **Upgrade** and an indication of **Accessed** is displayed on the top right corner of the product display.
6. Click **Upgrade** to Upgrade plan.

7. Click the **Back to <product name>** link to be navigated to that product's individual interface.

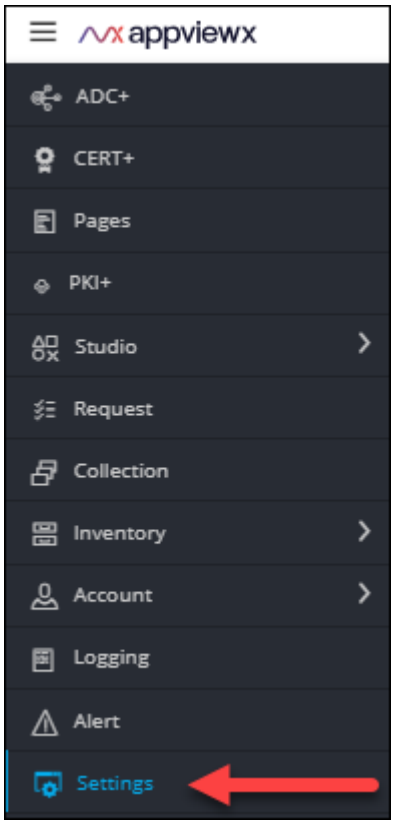


8. **AppViewX SaaS** products can be explored for the trial period of **30 days**.

Viewing License Details

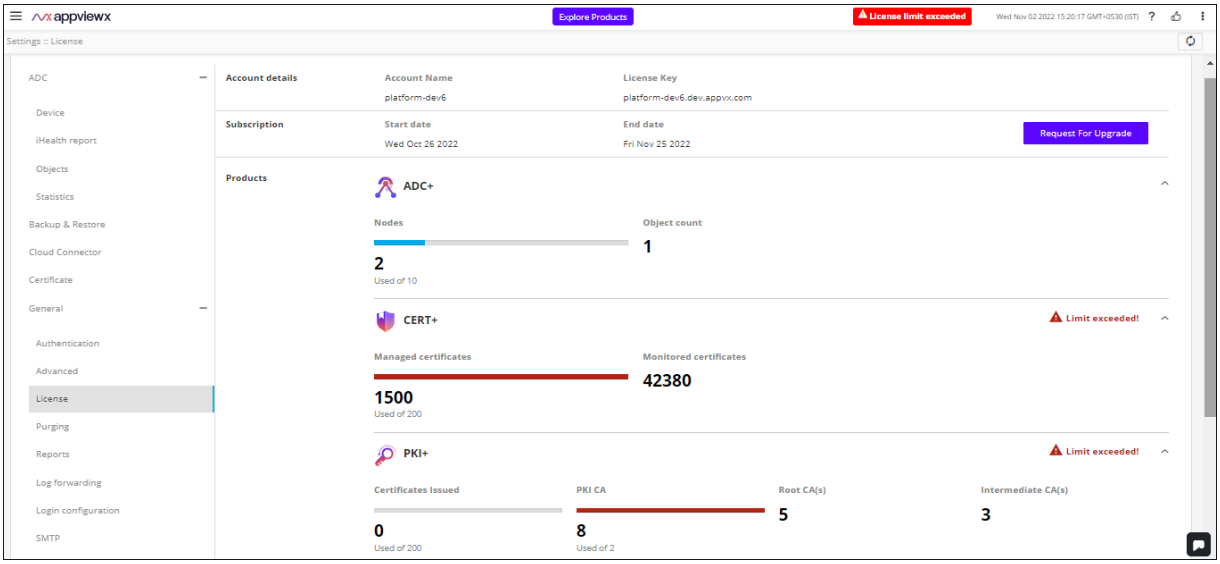
To view the list and details of subscribed licenses:

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.



Note: The License page screen displays details of those license that are purchased or subscribed by the user. The following image shows all products under the **Products** section ADC+, CERT+ and PKI+.

The page shows the following details:

License Detail	Description
Account details	
Account Name	Displays the associated account name.
License Key	The key is generated by the customer perspective. Using which License Key of "16 digit Alphanumeric" value is generated by the sales team. Only License Key generated with installation key can be applied in the respective instance of the product. **Note:** Consider only the license key which is provided by the sales team.
Subscription	
Start date	License Start Date.
End date	Date of expiry of the license.
Products	This includes the details of subscribed licenses of all AppViewX products.
ADC+	
Nodes (SaaS)	All the ADC devices (Independent devices, Controllers, Nodes within controllers) that are onboarded in the inventory.
Object count (SaaS)	All the ADC Applications (Unique GTM WideIPs, LTM VIPs) discovered from the onboarded ADC devices.
CERT+	
Managed certificates	All the certificate instances in the certificate inventory with Managed Status.

License Detail	Description
Monitored certificates	All the certificate instances in the certificate inventory with Monitored Status.
PKI+	
Certificates Issued	Certificates issued are the total number of certificates which includes the number of certificates issued and all CAs created in PKIaaS.
PKI CA	PKI CA is Number of CA's created from AppViewX.

• License Alerts

License Alerts

Following are the system alerts which indicates the product usage limit.

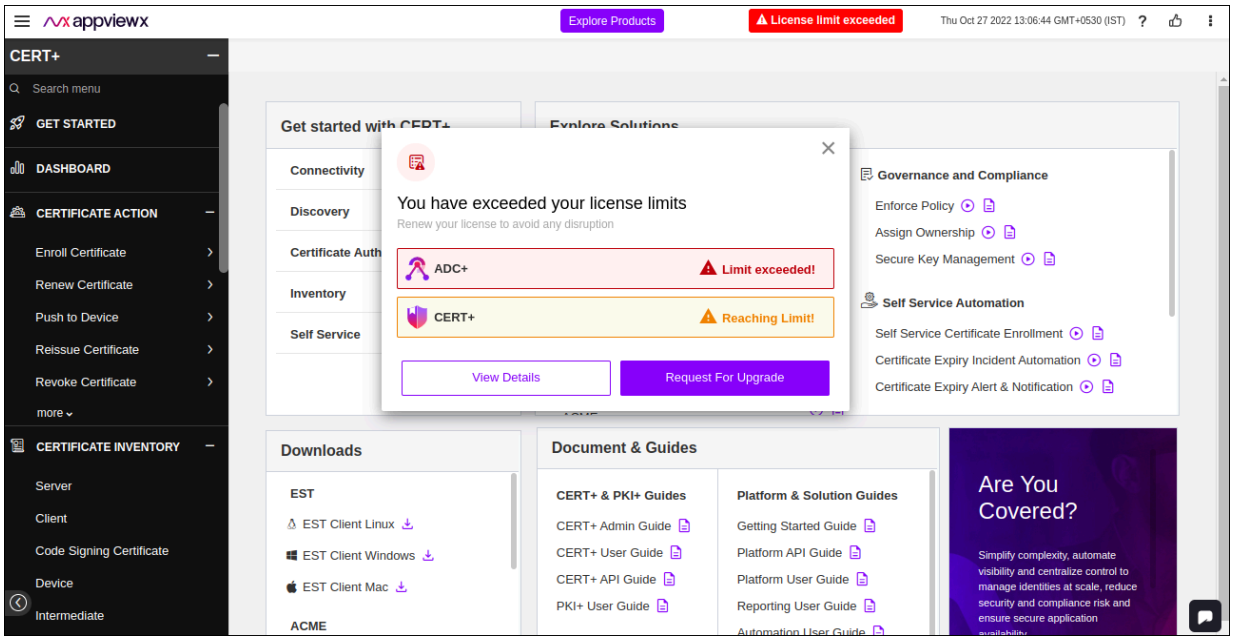
- **Reaching Limit!**

  If the usage reaches 90% of the threshold limit, then **“Reaching Limit!”** alert will be displayed.

- **Limit exceeded!**

If the usage exceeds the threshold limit, then **“Limit exceeded!”** alert will be displayed.

- You will see a header alert message while logging In, if the license limit is exceeded.

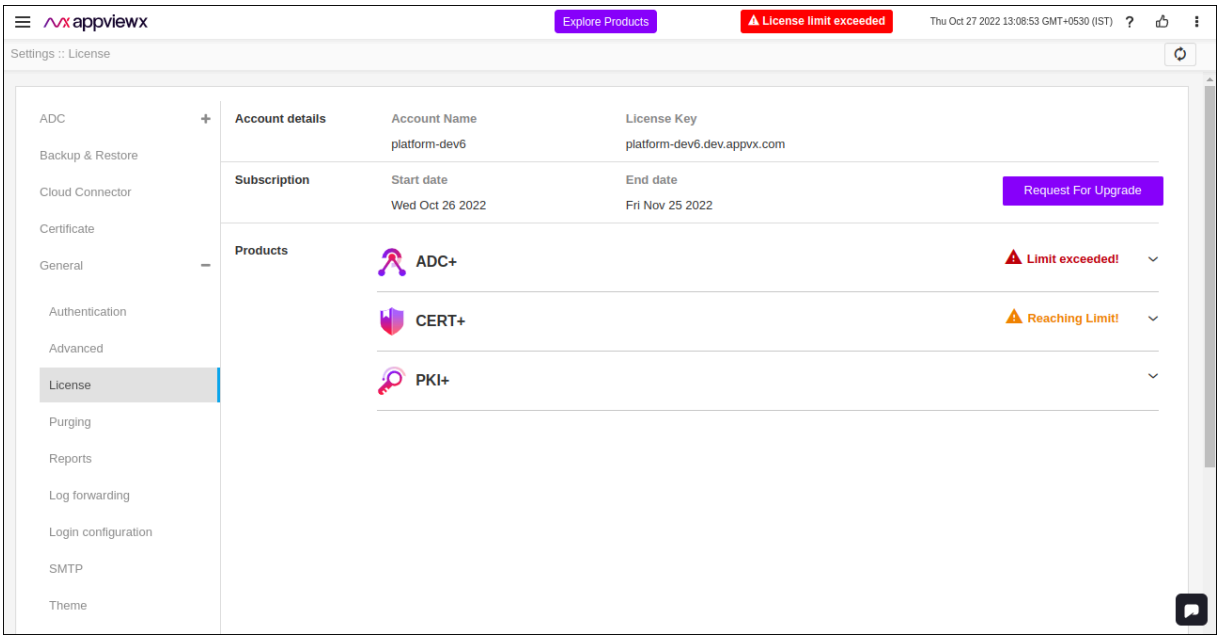


Upgrading Licenses

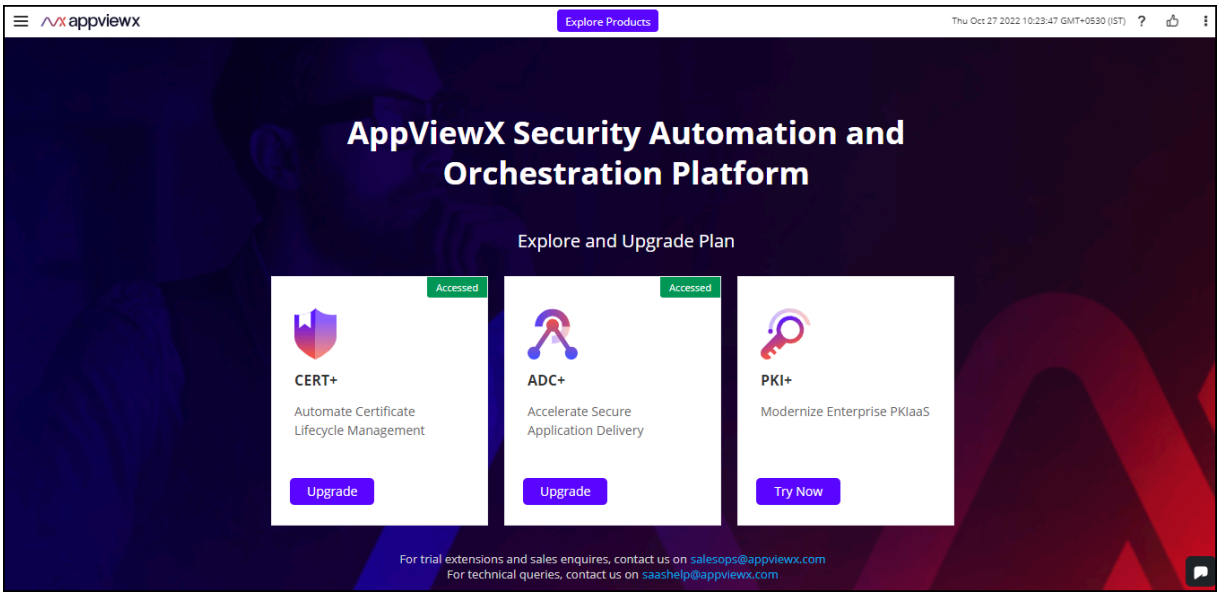
To upgrade a license:

1. On the **Settings :: License** page, from the top right corner of the screen, click **Request For Upgrade**.

> **Note:** This is applicable only for SaaS and SaaS Trial products.

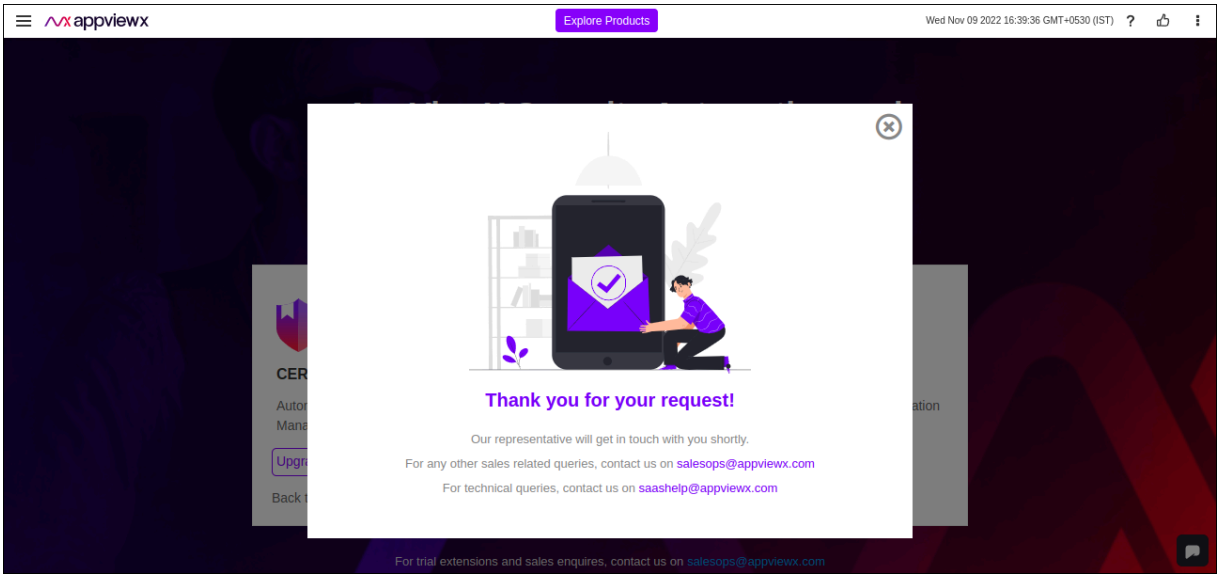


User is navigated back to the **AppViewX SaaS landing page**, where the user can upgrade the product.

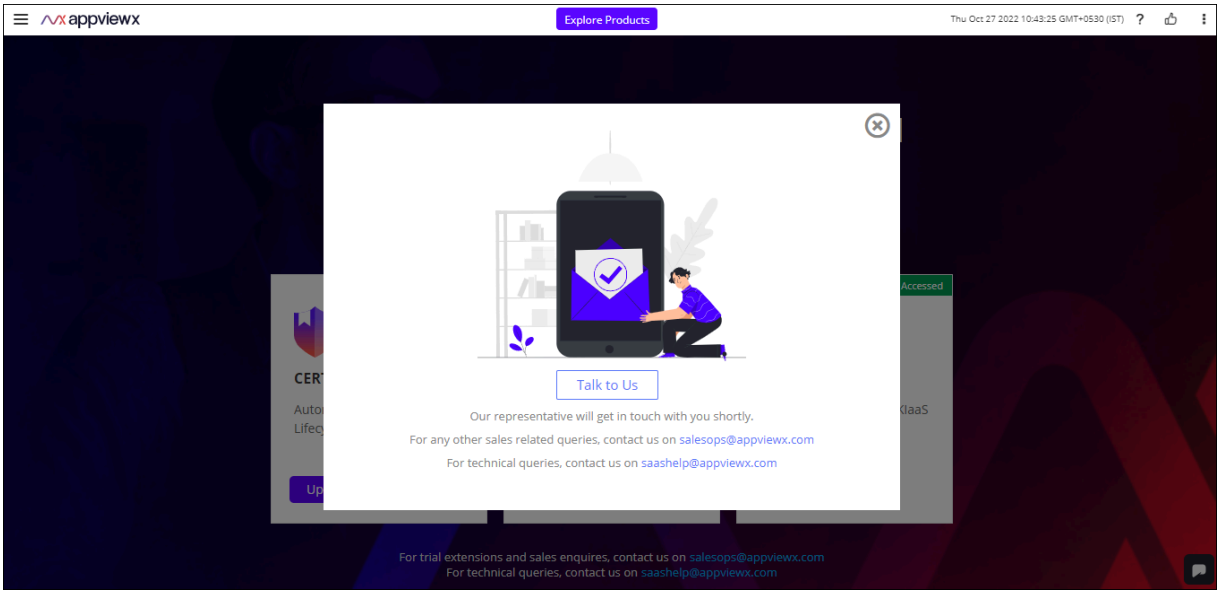


2. Click **Upgrade** on the corresponding product to request for upgrade.

If the request has successfully reached us, **“Thank you for your request!”** dialog box is displayed.



3. If the request failed to reach us, then the **“Talk to us”** page will be displayed. You can click that and submit the upgrade request. Our representative will get in touch with you shortly.



4. Click **Try Now** to Explore other AppViewX Products.

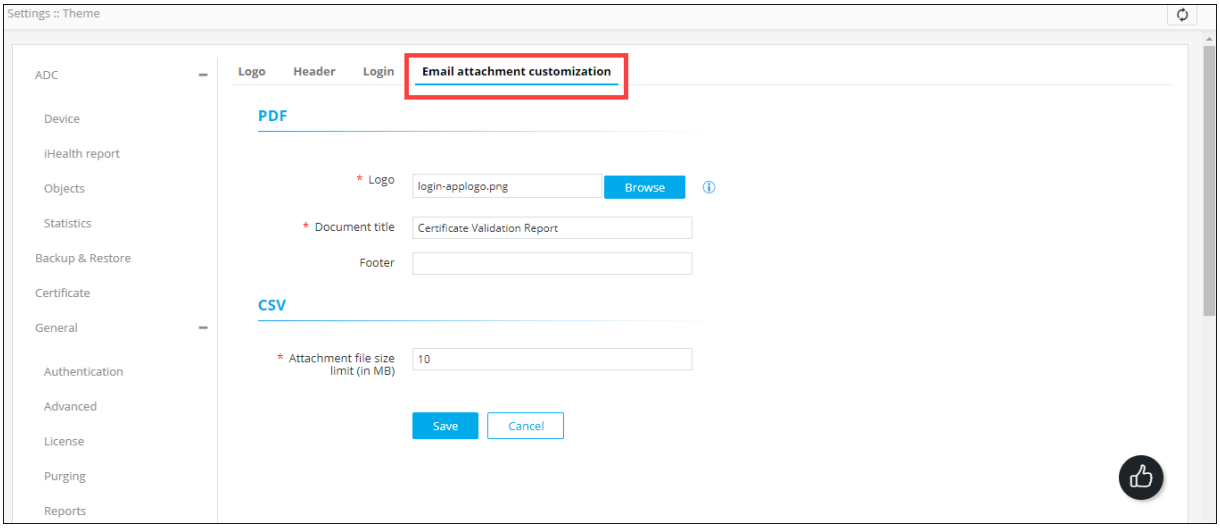
Chapter 10: Customizing the AppViewX User Interface

- Customizing the Email Attachment Representation
- Customizing the Login Screen
- Customizing the Logo
- Customizing the Screen Header

Customizing the Email Attachment Representation

To customize the cosmetics of how email attachments are represented:

1. Navigate to the Settings :: Theme page.
2. Click the Email attachment customization tab.



3. 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.

Field	Description
	Note: The image size must be less than 5 MB.
Document title*	Name to be assigned to the PDF when is it is downloaded
Footer	Footer content to be added to the PDF

4. In the CSV section, enter the following details:

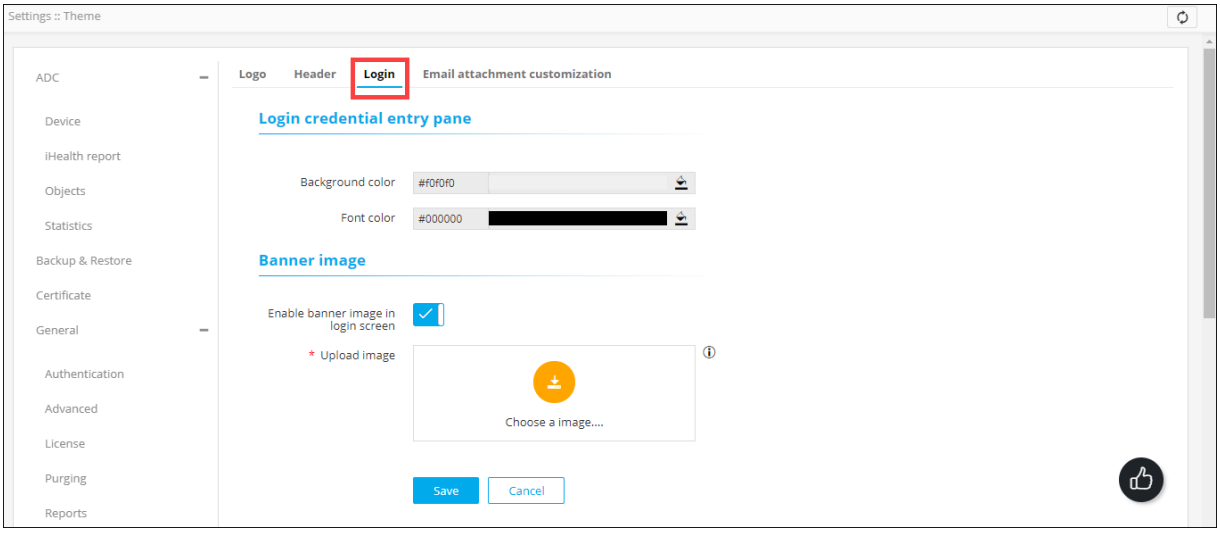
Field	Description
Attachment file size limit (in MB)*	Maximum file size for the attachment

5. To apply the changes configured above, click Save.

Customizing the Login Screen

To customize the login screen:

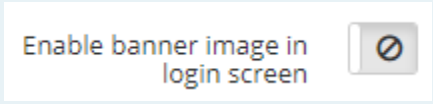
1. Navigate to the Settings :: Theme page.
2. Click the Login tab.



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

Field	Description
Background color	To set a background color for the login screen: Enter the hex code of the required background color (or) To select a color, click 
Font color	To set a font color for the login screen: Enter the hex code of the required font color (or) To select a color, click 

4. In the Banner image section, enter the following details:

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

Field	Description
	• Image formats allowed for upload: .jpg, .jpeg, and .png. • Recommended image resolution: 500 X 500 (width X height). • The image size must not exceed 5 MB. c. In the Confirmation Message dialog box, click Yes.

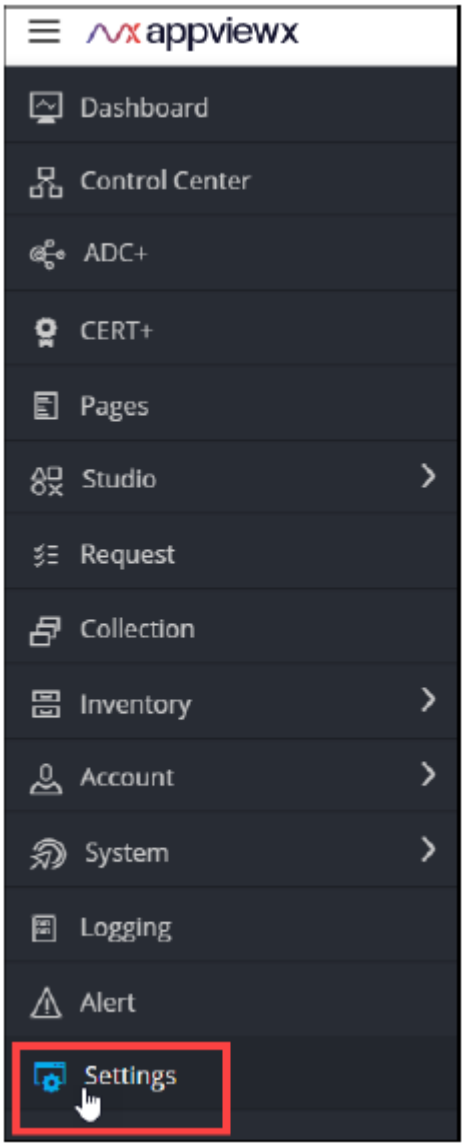
5. In the Preview section, view a preview of your customization for the login screen.
6. To apply the changes, click Save.

Customizing the Logo

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

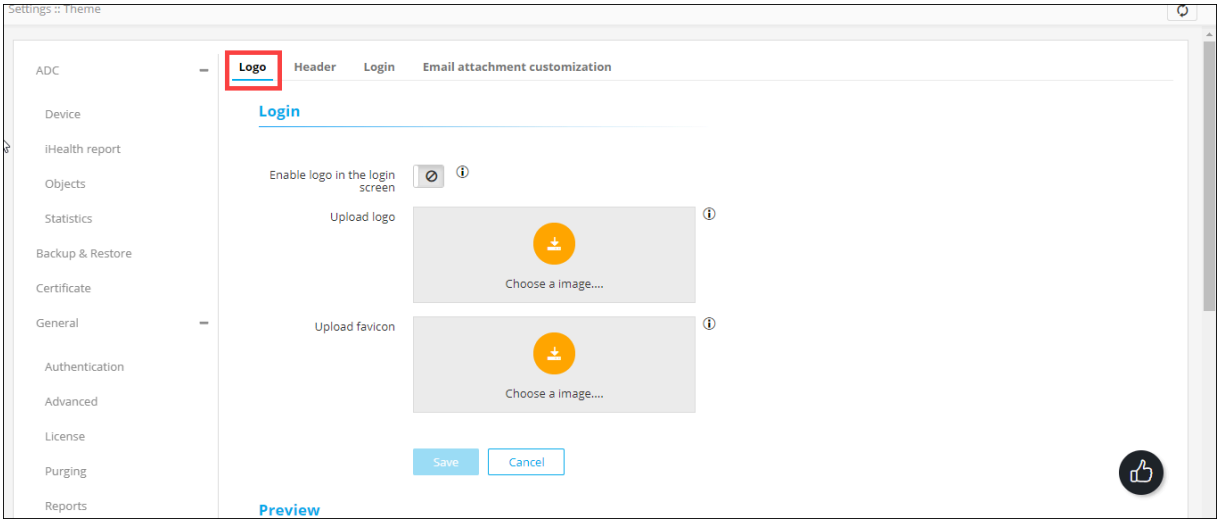
To add a custom logo:

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, click Settings.



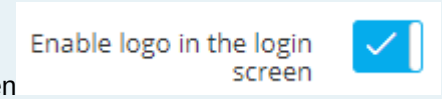
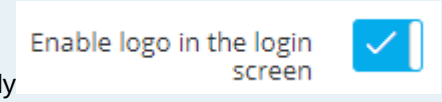
3. On the Settings page, from the navigation pane on the left, click General and select Theme.

4. 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, enable this toggle key. **Note:** If this toggle key is disabled, AppViewX's default theme settings are applied.

Field	Description
Upload logo*	**Note:** This field is enabled only when  is enabled. 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). • Image size should not exceed 5MB. • 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  is enabled. To choose a favicon image:

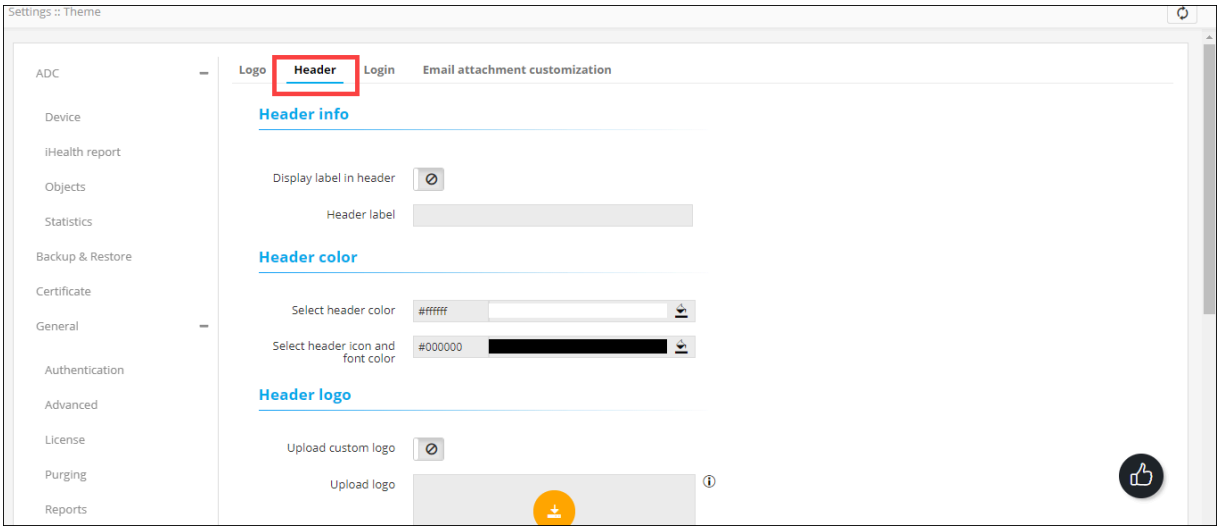
Field	Description
	a. Click  . b. From Windows Explorer, navigate to the location of the logo image, select the image, and click Open. **Note:** • Image formats allowed for upload: .png • Maximum image resolution allowed: 64 X 64 (width X height) • Image size should not exceed 5MB. c. In the Confirmation 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.

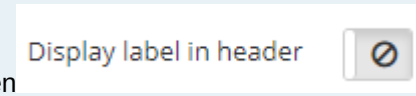
Customizing the Screen Header

To customize the screen header:

1. Navigate to the Settings :: Theme page.
2. To customize the screen header, click the Header tab.



3. In the Header Info section, enter the following details:

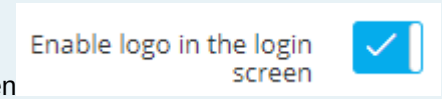
Field	Description
Display label in header	To display custom header text, enable this toggle key.
Header label*	Enter the custom header text. **Note:** This field is enabled only when  is enabled.

4. 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:

Field	Description
	Enter the hex code of the required color (or) To select a color, click  .

5. In the Header logo section, enter the following details:

Field	Description
Update custom logo	To insert a custom logo image in the header, enable this toggle key.
Upload logo*	**Note:** This field is enabled only when  is enabled. 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 should not exceed 5MB. • Recommended image dimensions: 175 X 37 (width X height). c. In the Confirmation Message dialog box, click Yes.

6. In the Preview section, view a preview of your header customization.
7. To apply the changes, click Save.

Chapter 11: 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.

Term	Definition
TACACS	The Terminal Access Controller Access Control System (TACACS) authentication is used to validate users requesting remote access.
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	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.