



CERT Troubleshooting Guide

Version: 2020.3.0

Copyright AppViewX, Inc.

Copyright © 2022 AppViewX, Inc. All Rights Reserved.

This document may not be copied, disclosed, transferred, or modified without the prior written consent of AppViewX, Inc. While all content is believed to be correct at the time of publication, it is provided as general-purpose information. The content is subject to change without notice and is provided “as is” and with no expressed or implied warranties whatsoever, including, but not limited to, a warranty for accuracy made by AppViewX. The software described in this document is provided under written license only, contains valuable trade secrets and proprietary information, and is protected by the copyright laws of the United States and other countries. Unauthorized use of software or its documentation can result in civil damages and criminal prosecution.

Trademarks

The trademarks, logos, and service marks displayed in this manual are the property of AppViewX or other third parties. Users are not permitted to use these marks without the prior written consent of AppViewX or such third party which may own the mark.

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).

All other trademarks mentioned in this document are the property of their respective owners.

Contact Information

AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: info@appviewx.com

Web: www.appviewx.com

Contents

Preface.....	6
Revision History.....	6
About this Guide.....	6
Audience.....	6
Text Conventions.....	6
Chapter 1. Troubleshooting CA.....	7
Overview.....	7
Troubleshooting Amazon CA.....	7
Troubleshooting Custom CA.....	16
Troubleshooting DigiCert CA.....	21
Troubleshooting EJBCA CA.....	28
Troubleshooting Entrust MPKI.....	41
Troubleshooting GlobalSign CA.....	47
Troubleshooting GoDaddy CA.....	55
Troubleshooting Google Private CA.....	67
Troubleshooting InCommon CA.....	78
Troubleshooting LetsEncrypt CA.....	91
Troubleshooting Microsoft Enterprise CA.....	97
Troubleshooting Microsoft Standalone CA.....	123
Troubleshooting Sectigo CA.....	144
Troubleshooting Symantec CA.....	157
Troubleshooting Trustwave CA	163
Windows Agent Setup.....	169
Chapter 2. Troubleshooting General.....	184
Overview.....	184
Troubleshooting Certificate Group.....	184
Troubleshooting Certificate Policy.....	187

Troubleshooting Certificate Reports Configuration.....	188
Troubleshooting Configuration of Workflow.....	190
Chapter 3. Troubleshooting Protocols.....	191
Overview.....	191
Troubleshooting Auto-Enrolment ACME.....	191
Troubleshooting Auto-Enrolment EST.....	195
Troubleshooting Auto-enrolment of MsIntune SCEP.....	202
Troubleshooting Auto-enrolment of SCEP.....	205
Chapter 4. Troubleshooting AWS, CLOUD.....	209
Overview.....	209
Troubleshooting of AWS - CLOUD (ACM and IAM).....	209
Troubleshooting AWS CLOUD CloudFront.....	217
Troubleshooting AWS CLOUD ELB.....	221
Troubleshooting Azure CLOUD.....	226
Troubleshooting CLOUD - Common Functionality.....	243
Chapter 5. Troubleshooting Server, Firewalls, WAF, and Rapid SB Connectors	255
Overview.....	255
Troubleshooting Apache Linux.....	256
Troubleshooting Barracuda WAF.....	268
Troubleshooting Cisco ASA Firewall.....	272
Troubleshooting Cisco CallManager.....	277
Troubleshooting Common Functionality of Servers.....	282
Troubleshooting Data Power Server.....	289
Troubleshooting F5 WAF.....	297
Troubleshooting Fortigate Firewall.....	303
Troubleshooting HP ILO.....	308
Troubleshooting IBMClient Linux.....	314
Troubleshooting IBMClient Windows.....	321
Troubleshooting Imperva WAF.....	330

Troubleshooting Linux JBoss Server.....	336
Troubleshooting Microsoft Enterprise CA.....	354
Troubleshooting Microsoft Tomcat.....	380
Troubleshooting MQServer Linux.....	393
Troubleshooting MQServer Windows.....	401
Troubleshooting MS SQL Windows.....	406
Troubleshooting Nginx Server.....	413
Troubleshooting NginxPlus ADC.....	419
Troubleshooting Paloalto Firewall.....	424
Troubleshooting Panorama Firewall.....	429
Troubleshooting RabbitMQ Server.....	434
Troubleshooting Rapid SB Server Inventory.....	446
Troubleshooting Rapid SB Linux Server.....	456
Troubleshooting Tomcat Linux.....	476
Troubleshooting Weblogic Linux.....	487
Troubleshooting Websphere Linux.....	498
Troubleshooting Websphere Windows.....	511
Troubleshooting Windows Apache Server.....	519
Troubleshooting Windows JBoss Server.....	526
Troubleshooting Windows Weblogic Server.....	540
Chapter 6. Glossary.....	548

Preface

Revision History

Revision	Description	Date
1.0	Initial release of document for Release 2020.3.0	September 2020

About this Guide

This document helps you troubleshoot the common problems that you might encounter when using CERT + functionalities.

Audience

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

Text Conventions

The following text conventions are used in this document:

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

Chapter 1: Troubleshooting CA

- [Overview](#)

Overview

Overview This section of the troubleshooting guide will help you deal with issues faced while using the different functionalities of various CAs. If the problem still remains unresolved please send a request to Technical Support by opening a case with the AppViewX Technical Services team. You can open a case from helpcenter.appviewx.com or send an email to help@appviewx.com.

- [Troubleshooting Amazon CA](#)
- [Troubleshooting Custom CA](#)
- [Troubleshooting DigiCert CA](#)
- [Troubleshooting EJBCA CA](#)
- [Troubleshooting Entrust MPKI](#)
- [Troubleshooting GlobalSign CA](#)
- [Troubleshooting GoDaddy CA](#)
- [Troubleshooting Google Private CA](#)
- [Troubleshooting InCommon CA](#)
- [Troubleshooting LetsEncrypt CA](#)
- [Troubleshooting Microsoft Enterprise CA](#)
- [Troubleshooting Microsoft Standalone CA](#)
- [Troubleshooting Sectigo CA](#)
- [Troubleshooting Symantec CA](#)
- [Troubleshooting Trustwave CA](#)
- [Windows Agent Setup](#)

Troubleshooting Amazon CA

- [Overview](#)
- [Supported Web Browsers](#)
- [Issues in Amazon CA](#)

Overview

This section will guide you in troubleshooting the common problems that you might encounter when using Amazon CA functionalities like setting addition, enrollment, renewal, regeneration, and revocation.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Amazon CA

- [Issues in Amazon CA setting addition using AppViewX UI](#)
- [Issues in Enrolling Amazon Certificate](#)
- [Issues in Renewing Amazon Certificate](#)
- [Issues in Regenerating Amazon Certificate](#)
- [Issues in Revoking Amazon Certificate](#)

Issues in Amazon CA setting addition using AppViewX UI

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.

The **Server Certificate** page is displayed.

- From the left pane, expand **Administration** and click **Certificate Authority**.

The **Certificate Authority** page is displayed.

- On the **Certificate Authority** page, click **Amazon**.



Note: Currently Amazon does not support Suspend & Reinstate CLM actions.

- Click **Add**.

• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for Amazon already exists in inventory.	Check the CA Setting name, it should be unique.

Error Message	Possible Cause	Possible Solution
Please provide information as required	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.
Connection failed due to incorrect CA settings details : The request signature we calculated does not match the signature you provided. Check your AWS Secret Access Key and signing method	Secret Access Key or Access key is incorrect.	Please check the provided Access key and secret key is valid.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.

Issues in Enrolling Amazon Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server/Client** Tab.
The **Enroll Server Certificate** page is displayed.
5. Select certificate authority as **Amazon**.

Enroll Server Certificate

General Information

Assign Group
Default

CA Details

Certificate Authority
Amazon

Renew Automatically
off

Regenerate Automatically
off

CA Account
amazon-ca

Certificate Type
None

Connector Name
Amazon CA connector

Description

CSR Generation
☒ AppViewX
☐ Upload CSR

CSR Parameters

Common Name

Subject Alternative Name
0 value

Hash Function
SHA160

Key Type
RSA

Bit Length
4096

Attachments

Add
Reset

• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Error while requesting certificate	- Domain validation failed in amazon CA. - Exceeded the limit for new certificates.	- Validate the provided domain is as per standard. - Check whether certificate enrollment has reached the limit in amazon.
Error while fetching cert	Enrollment requests may be in progress on the Amazon side.	Retry the action after some time.

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. Check whether network access is available.
Unable to establish connection, Please ensure Proxy / Internet connectivity.	1. Internet connectivity may be unavailable. 2. Invalid URL provided in CA Settings.	1. Please check Internet connectivity to reach CA. 2. Please Check whether a valid CA URL is provided in CA Settings or Contact Support Team.
Insufficient privilege for the user to create a certificate.	Request accepted but operation is refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges in the Amazon server for creating certificates or Contact Support Team.
Invalid Create Certificate Payload	Missing or invalid input parameters / JSON body in the request.	Please validate the input parameters/ payload provided or Contact the Support Team.
Too many create certificate requests	Too many create certificate requests for Amazon.	Please try to create a certificate request after some time or Contact the Support Team.

Issues in Renewing Amazon Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Renew Certificate** submenu.
4. Click **Server/Client/Code Signing Certificate**.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Select any **Amazon** certificate.
7. From the dropdown Actions in the toolbar at the top of the page, select **Renew Certificate**.

• [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Look for an email from ACM, and then follow the link in that email to validate your domain	Domain validation required	Check for email triggered from ACM to validate the domain.
One or more domain names were not validated before the certificate expired, and ACM did not renew the certificate. You can request a new certificate.	Issue in domain name validation.	Check whether the provided domain is valid.
ACM hasn't started the managed renewal process for this certificate.	ACM has not started the renewal request for the provided certificate.	Retry the request after some time.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Insufficient privilege for the user to create a certificate.	Request accepted but operation is refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges in the Amazon server for creating certificates or Contact Support Team.
Invalid Create Certificate Payload	Missing or invalid input parameters / JSON body in the request.	Please validate the input parameters/payload provided or Contact the Support Team.
Too many create certificate requests	Too many create certificate requests for Amazon.	Please try to create a certificate request after some time or Contact the Support Team.

Issues in Regenerating Amazon Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**.
4. Click **Server/Client/Code Signing Certificate** Tab
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **Amazon certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Regenerate**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Error while requesting certificate	Domain validation failed in amazon CA. Exceeded limit for a new certificate.	Validate the provided domain is as per standard. Check whether certificate enrollment has reached the limit in amazon.
Error while fetching cert	Enrollment requests may be in progress on the Amazon site.	Retry the action after some time.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Insufficient privilege for the user to create a certificate.	Request accepted but operation is refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges in the Amazon server for creating certificates or Contact Support Team.

Error Message	Possible Cause	Possible Solution
Invalid Create Certificate Payload	Missing or invalid input parameters / JSON body in the request.	Please validate the input parameters/ payload provided or Contact the Support Team.
Too many create certificate requests	Too many create certificate requests for Amazon	Please try to create a certificate request after some time or Contact the Support Team.

Issues in Revoking Amazon Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Revoke Certificate** submenu.
4. Click **Server/Client/Code Signing Certificate**.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **Amazon certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Revoke**.

• [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
AWS Premium Support Subscription is required to use this service. This certificate can be revoked by submitting a ticket with AWS support.	Amazon does not support "certificate revoke".	Check with Amazon premium support for getting revoke service.

Troubleshooting Custom CA

- [Overview](#)
- [Supported Web Browsers](#)
- [Issues in Custom CA](#)

Overview

This section will help you troubleshoot the common problems that you might encounter when using Custom CA functionalities like setting addition, enrollment, fetching, renewal, regeneration, and revocation.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Custom CA

- [Issues in Custom CA setting addition and Custom CA fetch CA names](#)
- [Issues in Enrolling Custom CA certificate](#)
- [Issues in Fetching Custom CA certificate](#)

- [Issues in Renewing Custom CA certificate](#)
- [Issues in Regenerating Custom CA certificate](#)
- [Issues in Revoking Custom CA certificate](#)

Issues in Custom CA setting addition and Custom CA fetch CA names

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Certificate Authority**.
The **Certificate Authority** page is displayed.
4. On the **Certificate Authority** page, click **Custom CA**.
5. Click **Add**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Failed to add custom CA details as name already exists	A CA setting with the same name for Custom CA already exists in inventory.	Check the CA Setting name, it should be unique.
1)This field should not be null or empty 2) Mandatory Field(s) - <Field name> is/are empty 3) CA Settings - [<Fields>] mandatory fields cannot be empty.	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.
Upload a valid CA certificate in .pfx format	Upload certificate not in .pfx or .p12 format	Upload the certificate in either of pfx or p12 format
Uploaded CA certificate already exist	Uploaded certificate already exists.	Uploaded a new certificate
Issuer serial number is mandatory on request.	Issuer serial number is missing.	Please provide issuer serial number

Error Message	Possible Cause	Possible Solution
CA certificate details are missing	CA certificate details are missing.	Please provide ca certificate details

Issues in Enrolling Custom CA certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server/Client/Code Signing** Tab.
The **Enroll Server Certificate** page is displayed.
5. Select **Certificate Authority** as **Custom CA**.

• [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid issuer details are specified in the request.	Issuer details are missing	Please provide issuer details
Issuer serial number is mandatory on request.	Issuer serial number is missing	Please provide issuer serial number
CA certificate details are missing	CA certificate details are missing	Please provide ca certificate details
Field cannot be empty.	Mandatory field is missing	Please provide the values for the field
Invalid CSR.	Specified CSR is invalid	Provide a valid CSR

Issues in Fetching Custom CA certificate

Error Message	Possible Cause	Possible Solution
Entered order id is invalid.	Order id is invalid.	Provide valid order id.

Issues in Renewing Custom CA certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Renew Certificate** submenu.
4. Click **Server/Client/Code Signing Certificate** Tab.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Select any **Custom CA certificate**.
7. From the dropdown **Actions** in the toolbar at the top of the page, select **Renew Certificate**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid issuer details are specified in the request.	Issuer details are missing	Please provide issuer details
Issuer serial number is mandatory on request.	Issuer serial number is missing	Please provide issuer serial number
CA certificate details are missing	CA certificate details are missing	Please provide CA certificate details
Field cannot be empty.	Mandatory field is missing	Please provide the values for the mandatory field.
Invalid CSR.	Specified CSR is invalid	Provide a valid CSR

Issues in Regenerating Custom CA certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**.
4. Click **Server/Client/Code Signing Certificate** Tab.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.

5. From the menu bar at the top of the page, click **List**.
6. Click any **Custom CA certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Regenerate**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid issuer details are specified in the request.	Issuer details are missing	Please provide issuer details
Issuer serial number is mandatory on request.	Issuer serial number is missing	Please provide issuer serial number
CA certificate details are missing	CA certificate details are missing	Please provide ca certificate details
Field cannot be empty.	Mandatory field is missing	Please provide the values for the field
Invalid CSR.	Specified CSR is invalid	Provide a valid CSR

Issues in Revoking Custom CA certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Revoke Certificate** submenu.
4. Click **Server/Client/Code Signing Certificate**.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **Custom CA certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Revoke**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Serial number or revocation request is null or empty.	Invalid request or invalid serial number specified.	Provide the valid request.
The certificate cannot be revoked as it does not have CRL distribution point.	Certificate does not have a CRL distribution point.	Invalid serial number provided.
The certificate is already revoked.	Certificate is already revoked.	Already revoked, so I need to revoke again.
Entered revocation reason is invalid.	Invalid reason specified	Specify valid reason to revoke the certificate

Troubleshooting DigiCert CA

- [Overview](#)
- [Supported Web Browsers](#)
- [Issues in DigiCert CA](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using DigiCert CA functionalities like setting addition, certificate enrollment, renewal, revocation, suspension, reinstating, and discovery.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in DigiCert CA

- [Issues in DigiCert CA setting addition using AppViewX UI](#)
- [Issues in Enrolling DigiCert certificate](#)
- [Issues in Renewing DigiCert certificate](#)
- [Issues in Regenerating DigiCert certificate](#)
- [Issues in Revoking DigiCert certificate](#)
- [Issues in Discovering DigiCert certificates](#)

Issues in DigiCert CA setting addition using AppViewX UI

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Certificate Authority**.
The **Certificate Authority** page is displayed.
4. On the **Certificate Authority** page, click **Digicert**.
5. Click **Add**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for Digicert already exists in inventory.	Check the CA Setting name, it should be unique.

Error Message	Possible Cause	Possible Solution
Fetch certificate types action has failed Connection failed due to incorrect CA settings details	Please check the Service URL or API Access key.	Verify the service URL configured: Sample URL:https://www.digicert.com/services/v2/.
Fetch certificate types action has failed Access denied due to missing permission.	Access Key may be wrong or may not have enough authorization.	Verify the Access key and check its API authorization, it should be set as none.
Fetch certificate types action has failed Proxy details is not configured in proxy settings	Proxy details might have not been configured.	Configure valid proxy details.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Unable to establish connection, Please ensure Proxy / Internet connectivity.	1. Invalid proxy details. 2. Internet connectivity may not be available. 3. Invalid URL provided in CA Settings.	1. Please check the proxy details provided. 2. Please check Internet connectivity to reach CA. 3. Please check whether a valid CA URL is provided in CA Settings or Contact the Support Team.

Issues in Enrolling DigiCert certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server/Client/Code Signing** Tab.
The **Enroll Server Certificate** page is displayed.
5. From the **Certificate Authority** list, select **DigiCert**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority.-Invalid organization name provided.	Organization information provided might not be available in the CA account.	Please check the list of organizations available in the CA settings.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.

Issues in Renewing DigiCert certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Renew Certificate** submenu.
4. Click **Server/Client/Code Signing Certificate** Tab.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Select any **DigiCert certificate**.
7. From the dropdown **Actions** in the toolbar at the top of the page, select **Renew Certificate**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Please provide a valid order Id of the certificate.	OrderId may be incorrect to perform CLM action in Digicert	Verify the orderid of the certificate from the Digicert CA account.
You must select a Certificate Authority to issue the certificate from	The CA certificateId may be incorrect.	Provide the valid ID of the intermediate certificate authority (ICA) certificate to select as the issuing certificate.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.

Issues in Regenerating DigiCert certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**.
4. Click **Server/Client/Code Signing Certificate** Tab.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **Digicert certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Regenerate**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority.-Invalid organization name provided.	Organization information provided might not be available in the CA account.	Please check the list of organizations available in the CA settings.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.

Issues in Revoking DigiCert certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Revoke Certificate** submenu.
4. Click **Server/Client/Code Signing Certificate**.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **DigiCert certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Revoke**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Error while revoking certificate-The specified order was not found.	The order id provided in the connector might be wrong.	Check the orderId for the certificate in Digicert CA Portal.
Error while revoking certificate-Order Id not provided to get corresponding certificate Id.	orderid is not provided for the action	Provide a valid order id to proceed with the action.
You must select a Certificate Authority to issue the certificate from	The CA certificateld may be incorrect.	Provide the valid ID of the intermediate certificate authority (ICA) certificate to select as the issuing certificate.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. Check whether network access is available.

Issues in Discovering DigiCert certificates

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery** and select **Discovery**.
4. Click **Certificate Authority Scan**.
The **Discovery: Certificate Authority Scan: Add Discovery** page is displayed.
5. Select **CA** as **DigiCert**.
6. Click **Discover** at the bottom of the page.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Service unavailable, please limit request volume	DigiCert throws Service unavailable, please limit request volume when 1000+ continuous requests fired, So with buffer to enroll certificates, 900 certificate requests only be fired in a batch	AppViewX Cert discovery automatically handles it by introducing a delay of 50 minutes between each 900 requests

Troubleshooting EJBCA CA

- [Overview](#)
- [Supported Web Browsers](#)
- [Issues in EJBCA CA](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using EJBCA CA functionalities like EJBCA CA setting addition, certificate enrollment, renewal, revocation, suspension, reinstatement, and discovery.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA

Browser	Version	Notes
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in EJBCA CA

- [Issues in EJBCA CA setting addition and fetch EEPs](#)
- [Issues in Enrolling EJBCA certificate](#)
- [Issues in Renewing EJBCA certificate](#)
- [Issues in Regenerating EJBCA certificate](#)
- [Issues in Revoking EJBCA certificate](#)
- [Issues in Suspending EJBCA certificate](#)
- [Issues in Reinstating EJBCA certificate](#)
- [Issues in Discovering EJBCA certificates](#)

Issues in EJBCA CA setting addition and fetch EEPs

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Certificate Authority**.
The **Certificate Authority** page is displayed.
4. On the **Certificate Authority** page, click **EJBCA**.
5. Click **Add**.

• [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for EJBCA already exists in inventory.	Check the CA Setting name, it should be unique.
1. This field should not be null or empty. 2. Mandatory Field(s) - <Field name> is/are empty. 3. CA Settings - [<Fields>] mandatory fields cannot be empty.	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.
Please enter valid credentials - Certificate and key, URL	Uploaded client certificate is incorrect or does not have the required permissions.	Please check the uploaded certificate and its permissions. Please ensure that the required permissions are given.
At Least one end entity profile should be added.	CA Setting does not have at least one End entity profile selected and added.	CA Settings should have at least one End entity profile selected and added.
Unable to establish connection with CA.	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Unable to establish connection, Please ensure Proxy / Internet connectivity/EJBCA Server.	Invalid proxy details.	Please check the proxy details provided.

Error Message	Possible Cause	Possible Solution
Unable to establish connection, Please ensure Proxy / Internet connectivity/EJBCA Server.	1. Internet connectivity may not be available. 2. Invalid URL provided in CA Settings.	1. Please check Internet connectivity to reach CA." 2. Please check whether a valid URL is provided in CA Settings or Contact Support Team.

Issues in Enrolling EJBCA certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server/Client/Code Signing** Tab.
The **Enroll Server Certificate** page is displayed.
5. Select **Certificate Authority** as **EJBCA**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority - Subject DN field <FieldName> must exist.	FieldName may be set as mandatory in the selected End entity profile in EJBCA portal.	1. Set the FieldName as optional in the selected End entity profile in EJBCA portal. 2. Add a value for the failed field in the certificate enrollment page (If the field is Organization, Organization unit, Locality, Country, State). 3. If the field is not listed on the enrollment page, add the field in the End entity profile, then pass the value via the enrollment page.

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority - Wrong number of <FieldName> fields in Subject Alternative Name.	No. of values sent and no. of values configured for the field do not match.	1. Send the exact no of values for the fields configured in the EJBCA portal. 2. Change the field count in EJBCA portal to match the sending value count.
Unable to submit the CSR request to certificate authority - Couldn't find certificate profile (<ProfileId>,) among available certificate profiles.	Certificate profiles may not be configured in the selected End entity profile.	Configure the selected certificate profile in the selected End entity profile.
Unable to submit the CSR request to certificate authority - End Entity data contains a CA, <CA ID>, which the Certificate Profile, <ProfileId>, isn't authorized to use.	Configuration of the selected Issuer is not done in the selected certificate profile.	Configure the selected Issuer name in the selected certificate profile.
Unable to establish connection with CA	1. Incorrect configuration of CA details. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Unable to establish connection, Please ensure Proxy / Internet connectivity/ EJBCA Server.	Invalid proxy details.	Please check the proxy details provided.
Unable to establish connection, Please ensure Proxy / Internet connectivity/ EJBCA Server.	1. Internet connectivity may not be available. 2. Invalid URL provided in CA Settings.	1. Please check Internet connectivity to reach CA. 2. Please check whether a valid CA URL is provided in CA Settings or Contact Support Team.

Error Message	Possible Cause	Possible Solution
Insufficient privilege for the user to create a certificate.	Request accepted but operation refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges in EJBCA server for creating certificates or Contact the Support Team.
Invalid Create Certificate Payload	Missing or invalid input parameters / JSON body in the request.	Please validate the input parameters/payload provided or Contact the Support Team.
Too many create certificate requests	Too many create certificate requests for EJBCA.	Please try to create a certificate request after some time or Contact the Support Team.

Issues in Renewing EJBCA certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Renew Certificate** submenu.
4. Click **Server/Client/Code Signing Certificate**.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Select any **EJBCA certificate**.
7. From the dropdown **Actions** in the toolbar at the top of the page., select **Renew Certificate**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Error while renewing certificate. - Subject DN field <FieldName>must exist.	FieldName may set as mandatory in the selected End entity profile in EJBCA portal	1. Set the FieldName as optional in the selected End entity profile in EJBCA portal. 2. Add a value for the failed field in the certificate enrollment

Error Message	Possible Cause	Possible Solution
		page (If the field is Organization, Organization unit, Locality, Country, State). 3. If the field is not listed on the enrollment page, add the field in the End entity profile, then pass the value via the enrollment page.
Error while renewing certificate. - Wrong number of <FieldName> fields in Subject Alternative Name.	No. of values sent and no. of values configured for the field do not match.	1. Send the exact no of values for the fields configured in the EJBCA portal. 2. Change the field count in EJBCA portal as sending value count.
Error while renewing certificate. - Couldn't find certificate profile (<ProfileId>,) among available certificate profiles	Certificate profile selected may not be configured in the selected End entity profile	Configure the selected certificate profile in the selected End entity profile
Error while renewing certificate. - End Entity data contains a CA, <CA ID>, which the Certificate Profile, <ProfileId>, isn't authorized to use.	Configuration of the selected Issuer is not done in the selected certificate profile.	Configure the selected issuer name in the selected certificate profile.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Unable to establish connection, Please ensure Proxy / Internet connectivity/EJBCA Server.	Invalid proxy details.	Please check the proxy details provided.

Error Message	Possible Cause	Possible Solution
Unable to establish connection, Please ensure Proxy / Internet connectivity/EJBCA Server.	1. Internet connectivity may not be available. 2. Invalid URL provided in CA Settings.	1. Please check Internet connectivity to reach CA. 2. Please check whether a valid CA URL is provided in CA Settings or Contact Support Team.
Insufficient privilege for the user to create a certificate.	Request accepted but the operation is refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges, disabled features in EJBCA server for creating certificates, or Contact the Support Team.
Invalid Create Certificate Payload	Missing or invalid input parameters / JSON body in the request.	Please validate the input parameters/payload provided or Contact the Support Team.
Too many create certificate requests	Too many create certificate requests for EJBCA.	Please try to create a certificate request after some time or Contact the Support Team.
CSR or private key is not available. Use the regenerate option.	CSR or private key may not be available	Use regenerate or upload the private key and perform renew action.

Issues in Regenerating EJBCA certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**.
4. Click **Server/Client/Code Signing Certificate** Tab.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **EJBCA certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Regenerate**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority - Subject DN field <FieldName> must exist.	FieldName may set as mandatory in the selected End entity profile in EJBCA portal	1. Set the FieldName as optional in the selected End entity profile in EJBCA portal. 2. Add a value for the failed field in the certificate enrollment page (If the field is Organization, Organization unit, Locality, Country, State). 3. If the field is not listed on the enrollment page, add the field in the End entity profile, then pass the value via the enrollment page.
Unable to submit the CSR request to certificate authority - Wrong number of <FieldName> fields in Subject Alternative Name.	No of values sent and no of values configured for the field do not match.	1. Send the exact no of values for the fields configured in the EJBCA portal. 2. Change the field count in EJBCA portal as sending value count.
Unable to submit the CSR request to certificate authority - Couldn't find certificate profile (<ProfileId>,) among available certificate profiles	Certificate profiles may not be configured in the selected End entity profile.	Configure the selected certificate profile in the selected End entity profile
Unable to submit the CSR request to certificate authority - End Entity data contains a CA, <CA ID>, which the Certificate Profile, <ProfileId>, isn't authorized to use.	Configuration of the selected Issuer is not done in the selected certificate profile.	Configure the selected issuer name in the selected certificate profile.

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Insufficient privilege for the user to create a certificate.	Request accepted but the operation is refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges, disabled features in EJBCA server for creating certificates, or Contact the Support Team.
Invalid Create Certificate Payload	Missing or invalid input parameters / JSON body in the request.	Please validate the input parameters/payload provided or Contact the Support Team.
Too many create certificate requests	Too many create certificate requests for EJBCA	Please try to create a certificate request after some time or Contact the Support Team.

Issues in Revoking EJBCA certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Revoke Certificate** submenu.
4. Click **Server/Client/Code Signing Certificate**.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **EJBCA certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Revoke**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Error while revoking certificate- Could not find end entity certificate.	The issuer name in the connector may be wrong	Set the actual issuer name in the connector then perform revoke action
Missing issuer details in the request.	Issuer details may be missing.	Provide Issuer details
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.

Issues in Suspending EJBCA certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and Click **Server/Client/Code Signing Certificate**.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
4. From the menu bar at the top of the page, click **List**.
5. Click any **EJBCA certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
6. From the dropdown menu next to the **Certificate**, click **Suspend**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Error while suspending certificate- Could not find end entity certificate.	The issuer name in the connector may be wrong	Set the actual issuer name in the connector then perform revoke action
Missing issuer details in the request.	Issuer details may be missing.	Provide Issuer details
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.

Issues in Reinstating EJBCA certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and Click **Server/Client/Code Signing Certificate**.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
4. From the menu bar at the top of the page, click **List**.
5. Click any suspended **EJBCA certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
6. From the dropdown menu next to the **Certificate**, click **Reinstate**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Error while reinstating certificate- Could not find end entity certificate.	The issuer name in the connector may be wrong.	Set the actual issuer name in the connector then perform revoke action.

Error Message	Possible Cause	Possible Solution
Missing issuer details in the request.	Issuer details may be missing.	Provide Issuer details.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.

Issues in Discovering EJBCA certificates

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery** and select **Discovery**.
4. Click **Certificate Authority Scan**.
The **Discovery: Certificate Authority Scan: Add Discovery** page is displayed.
5. Select **CA** as **EJBCA**.
6. Click **Discover** at the bottom of the page.

• [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Expiry Days need to be configured to discover certificates	Expiry days not configured in the selected EJBCA CA Settings.	Set the expiry days in the selected CA Settings

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.

Troubleshooting Entrust MPKI

- [Overview](#)
- [Supported Web Browsers](#)
- [Issues in Entrust MPKI](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using Entrust MPKI functionalities like setting addition, certificate enrollment, renewal, revocation, suspension, reinstating, and discovery.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher

Device	OS	Resolution
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Entrust MPKI

- [Issues in Entrust MPKI setting addition using AppViewX UI](#)
- [Issues in Enrolling Entrust MPKI certificate](#)
- [Issues in Renewing Entrust MPKI certificate](#)
- [Issues in Regenerating Entrust MPKI certificate](#)
- [Issues in Revoking Entrust MPKI certificate](#)
- [Issues in Discovering Entrust MPKI certificates](#)

Issues in Entrust MPKI setting addition using AppViewX UI

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the menu and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Certificate Authority**.
The **Certificate Authority** page is displayed.
4. On the **Certificate Authority** page, click **Entrust**.
The **Entrust** page is displayed.
5. On the **Entrust** page, click the **Entrust MPKI** tab.
6. Click **Add**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for Entrust MPKI already exists in inventory.	Check the CA Setting name, it should be unique.

Error Message	Possible Cause	Possible Solution
Fetch certificate types action has failed Proxy details is not configured in proxy settings	Proxy details might have not been configured.	Configure valid proxy details.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Unable to establish connection, Please ensure Proxy / Internet connectivity.	1. Invalid proxy details. 2. Internet connectivity may not be available. 3. Invalid URL provided in CA Settings.	1. Please check the proxy details provided. 2. Please check Internet connectivity to reach CA. 3. Please check whether a valid CA URL is provided in CA Settings or Contact the Support Team.

Issues in Enrolling Entrust MPKI certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the menu and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server/Client/Code Signing** Tab.
The **Enroll Server Certificate** page is displayed.
5. From the **Certificate Authority** list, select **Entrust MPKI**.

• [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority.-Invalid organization name provided.	Organization information provided might not be available in the CA account.	Please check the list of organizations available in the CA settings.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.

Issues in Renewing Entrust MPKI certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the menu and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Renew Certificate** submenu.
4. Click **Server/Client/Code Signing Certificate** Tab.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Select any **Entrust MPKI** certificate.
7. From the **Actions** dropdown in the toolbar at the top of the page, select **Renew Certificate**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
You must select a Certificate Authority to issue the certificate from	The CA certificateId may be incorrect.	Provide the valid ID of the intermediate certificate authority (ICA) certificate to select as the issuing certificate.

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.

Issues in Regenerating Entrust MPKI certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the menu and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**.
4. Click **Server/Client/Code Signing Certificate** Tab.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **Entrust MPKI certificate**.
A holistic view of **Server Certificate** with the **Certificate number** is displayed.
7. From the dropdown menu next to the **Certificate**, click **Regenerate**.

• [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.

Issues in Revoking Entrust MPKI certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the menu and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Revoke Certificate** submenu.
4. Click **Server/Client/Code Signing Certificate**.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **Entrust MPKI certificate**. A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Revoke**.

• [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
You must select a Certificate Authority to issue the certificate from	The CA certificateId may be incorrect.	Provide the valid ID of the intermediate certificate authority (ICA) certificate to select as the issuing certificate.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. Check whether network access is available.

Issues in Discovering Entrust MPKI certificates

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the menu and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery** and select **Discovery**.

4. Click **Certificate Authority Scan**.

The **Discovery: Certificate Authority Scan: Add Discovery** page is displayed.

5. Select **CA** as **Entrust MPKI**.

6. Click **Discover** at the bottom of the page.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.

Troubleshooting GlobalSign CA

- [Overview](#)
- [Supported Web Browsers](#)
- [GlobalSign CA Issues](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using GlobalSign CA functionalities like setting addition, connectivity, certificate enrollment, renewal, reissue, revocation, and discovery.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA

Browser	Version	Notes
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

GlobalSign CA Issues

- [Issue in GlobalSign CA Settings Addition](#)
- [Issue in Enrolling certificate using GlobalSign CA](#)
- [Issues in Renewing certificate using GlobalSign CA](#)
- [Issues in Revoking certificate using GlobalSign CA](#)
- [Issues in Discovering GlobalSign certificates](#)
- [Issues in GlobalSign CA Connectivity Check](#)
- [Issues in Reissue certificate using GlobalSign CA](#)

Issue in GlobalSign CA Settings Addition

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Certificate Authority**.
The **Certificate Authority** page is displayed.
4. On the **Certificate Authority** page, click **GlobalSign**.
The **Certificate Authority GlobalSign** Page is displayed.
5. Click **Add** or **Configure Now**.

The screenshot displays the AppViewX web interface for configuring a Certificate Authority (CA). The left-hand navigation menu includes sections for Alerts & Logs, Groups & Policies, and Administration. The main content area is titled 'Certificate Authority' and shows the configuration for a 'GlobalSign' CA. The 'General Information' section contains fields for 'CA Account name' (GlobalSignCA), 'Purpose/Usage' (Server), and 'Proxy Required' (checkbox). A note indicates that the AppViewX CA agent must be restarted if proxy settings are changed. The 'Data Center' is set to 'absecon'. The 'CA Configuration' section shows the 'SSL URL' as 'https://test-gcc.globalsign.com'. 'Update' and 'Cancel' buttons are located at the bottom of the configuration form.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for GlobalSign already exists in inventory.	Check the CA Setting name, it should be unique.
This field should not be null or empty	Some of the mandatory fields might be missing or invalid.	Add all the valid information in the mandatory section.
Mandatory Field(s) - <Field name> is/are empty		
CA Settings - [<Fields>] mandatory fields cannot be empty.		
CA Settings name already exists.	A CA setting with the same name for GlobalSign already exists in inventory.	Check the CA Setting name, it should be unique.
Invalid URL	vendorSpecificSettings.url is not valid.	Provide valid input for vendorSpecificSettings.url.

Error Message	Possible Cause	Possible Solution
Login should not be blank	vendorSpecificSettings.login is not valid.	Provide valid input for vendorSpecificSettings.login.
Password should not be blank	vendorSpecificSettings.password is not valid.	Provide valid input for vendorSpecificSettings.password.

Issue in Enrolling certificate using GlobalSign CA

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab.
The **Enroll Server Certificate** page is displayed.
5. Select **Certificate Authority** as **GlobalSign**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority.	1. Invalid credentials. 2. Invalid Global Sign URL. 3. Ip is not whitelisted by GlobalSign firewall 4. Invalid CSR parameters.	1. Check the credentials provided. 2. Check the provided URL. 3. Make sure your public IP is whitelisted by global Sign. 4. Validate the CSR parameters.
Host endpoint cannot be null or empty.	Endpoint URL of the given CA setting is null or empty.	Provide valid endpoint URL during CA setting addition.
Proxy details is not configured in proxy settings	Proxy settings are not available.	Configure proxy settings in settings>general.

Error Message	Possible Cause	Possible Solution
Invalid Common Name, Please provide valid commonname.	Common name provided in CSR is invalid.	Provide a valid common name in CSR parameters.
Empty response received from the portal, Check with Proxy / CA Setting configurations.	1. Error in provided CA details. 2. Check if the CA portal is accessible from AppViewX.	1. Check the given CA details. 2. Check for internet/ proxy settings.
Invalid Validity Period	Validity period provided is invalid.	Check with CA for the supported validity period and update accordingly.

Issues in Renewing certificate using GlobalSign CA

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Renew Certificate** submenu.
4. Click **Server**.
The **Server Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Select any **GlobalSign certificate**.
7. From the dropdown **Actions** in the toolbar at the top of the page, select **Renew Certificate**.

• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Host endpoint cannot be null or empty.	Endpoint URL of the given CA setting is null or empty.	Provide valid endpoint URL during CA setting addition.
Proxy details is not configured in proxy settings	Proxy settings are not available.	Configure proxy settings in settings>general.

Error Message	Possible Cause	Possible Solution
Invalid Common Name, Please provide valid commonname.	Common name provided in CSR is invalid.	Provide a valid common name in CSR parameters.
Empty response received from the portal, Check with Proxy / CA Setting configurations.	1. Error in provided CA details. 2. Check if the CA portal is accessible from AppViewX.	1. Check the given CA details. 2. Check for internet/ proxy settings.
Invalid Validity Period	Validity period provided is invalid.	Check with CA for the supported validity period and update accordingly.

Issues in Revoking certificate using GlobalSign CA

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Revoke Certificate** submenu.
4. Click **Server**.
The **Server Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **GlobalSign** certificate.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Revoke**.

• [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Order Id not provided to get corresponding certificate Id.	Order id is empty in the revoke request.	Check and provide a valid order id.
Host endpoint cannot be null or empty.	Endpoint URL of the given CA setting is null or empty.	Provide valid endpoint URL during CA setting addition.

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy settings are not available.	Configure proxy settings in settings>general.

Issues in Discovering GlobalSign certificates

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery** and select **Discovery**.
4. Click **Certificate Authority Scan**.
The **Discovery: Certificate Authority Scan: Add Discovery** page is displayed.
5. Select **CA** as **GlobalSign**.
6. Click **Discover** at the bottom of the page.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to perform Discovery, Please check settings.	1. Invalid credentials. 2. Invalid Global Sign URL. 3. Ip is not whitelisted by GlobalSign firewall. 4. Invalid CSR parameters.	1. Check the credentials provided. 2. Check the provided URL. 3. Make sure your public IP is whitelisted by global Sign. 4. Validate the CSR parameters.
Host endpoint cannot be null or empty.	Endpoint URL of the given CA setting is null or empty.	Provide valid endpoint URL during CA setting addition.
Proxy details is not configured in proxy settings	Proxy settings are not available.	Configure proxy settings in settings>general.

Issues in GlobalSign CA Connectivity Check

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.

The **Server Certificate** page is displayed.

- From the left pane, expand **Administration** and click **Certificate Authority**.

The **Certificate Authority** page is displayed.

- On the **Certificate Authority** page, click **GlobalSign**.

The **Certificate Authority GlobalSign** Page is displayed.

- To check connectivity with the **CA**, click **Check** in **Connection Status**.

• [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid Global Sign Credentials.	Proxy details provided might be incorrect.	Provide valid proxy details.
	Invalid credentials	Please check the credentials provided.
	Invalid GlobalSign URL.	Please check the provided URL.
	Ip is not whitelisted by GlobalSign firewall.	Please make sure your public IP is whitelisted by GlobalSign.
Connection failed due to incorrect CA settings details Access denied due to invalid permissions.	Invalid credentials	Please check the credentials provided.

Issues in Reissue certificate using GlobalSign CA

- Log in to **AppViewX** application with valid credentials.

- From the left pane, expand the **menu** and click **Cert+**.

The **Server Certificate** page is displayed.

- From the left pane, expand **Certificate Action** and select **Reissue Certificate** submenu.

- Click **Server**.

The **Server Certificate** page is displayed.

5. From the menu bar at the top of the page, click **List**.

6. Click any **GlobalSign certificate**.

A holistic view of **Server Certificate** with the **Certificate number** is displayed.

7. From the dropdown menu next to the **Certificate**, click **Reissue**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Host endpoint cannot be null or empty.	Endpoint URL of the given CA setting is null or empty.	Provide valid endpoint URL during CA setting addition.
Proxy details is not configured in proxy settings	Proxy settings are not available.	Configure proxy settings in settings>general.

Troubleshooting GoDaddy CA

- [Overview](#)
- [Supported Web Browsers](#)
- [Issues in GoDaddy CA](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using GoDaddy CA functionalities like setting addition, certificate enrollment, renewal, revocation, suspension, reinstating, and discovery.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7,	From AppViewX Version 11.1

Browser	Version	Notes
	macOS - Version 13.1.2)	
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in GoDaddy CA

- [Issues in GoDaddy CA setting addition](#)
- [Issues in Enrolling GoDaddy certificate](#)
- [Issues in Renewing GoDaddy certificate](#)
- [Issues in Regenerating GoDaddy certificate](#)
- [Issues in Revoking GoDaddy certificate](#)
- [Issues in Discovering GoDaddy certificates](#)

Issues in GoDaddy CA setting addition

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Certificate Authority**.
The **Certificate Authority** page is displayed.
4. On the **Certificate Authority** page, click **GoDaddy**.
5. Click **Add**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for GoDaddy already exists in inventory.	Check the CA Setting name, it should be unique.
1. This field should not be null or empty 2. Mandatory Field(s) - <Field name> is/are empty 3. CA Settings - [<Fields>] mandatory fields cannot be empty.	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.
Please enter valid credentials – URL	URL entered might be wrong and not in proper URL format	Please check the URL entered
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Unable to establish connection, Please ensure Proxy / Internet connectivity/GoDaddy Server.	Invalid proxy details.	Please check the proxy details provided.
Unable to establish connection, Please ensure Proxy / Internet connectivity/GoDaddy Server.	1. Internet connectivity may not be available. 2. Invalid URL provided in CA Settings.	1. Please check Internet connectivity to reach CA. 2. Please check whether a valid CA URL is provided in CA Settings or Contact Support Team.

Issues in Enrolling GoDaddy certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server/Code Signing** Tab.
The **Enroll Server Certificate** page is displayed.
5. Select **Certificate Authority** as **GoDaddy**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority - No available units for the selected product type	Units may not be available for the product type selected in the GoDaddy account.	Purchase a valid unit for the product type in the GoDaddy account.
Unable to submit the CSR request to certificate authority - No available units for the selected product type	Units may be available for the product type selected in the GoDaddy account but the selected certificate validity may be incorrect for the product purchased.	Edit the CA connector and change the Validity in CSR parameters as purchased in the product.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Unable to establish connection, Please ensure Proxy / Internet connectivity/ GoDaddy Server.	Invalid proxy details.	Please check the proxy details provided.

Error Message	Possible Cause	Possible Solution
Unable to establish connection, Please ensure Proxy / Internet connectivity/ GoDaddy Server.	1. Internet connectivity may not be available. 2. Invalid URL provided in CA Settings.	1. Please check Internet connectivity to reach CA. 2. Please check whether a valid CA URL is provided in CA Settings or Contact Support Team.
Insufficient privilege for the user to create a certificate.	Request accepted but operation is refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges in GoDaddy server for creating certificates or Contact Support Team.
Invalid Create Certificate Payload	Most likely missing or invalid input parameters / JSON body in the request.	Please validate the input parameters/payload provided or Contact the Support Team.
Too many create certificate requests	Too many create certificate requests for GoDaddy.	Please try to create a certificate request after some time or Contact the Support Team.

Issues in Renewing GoDaddy certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Renew Certificate** submenu.
4. Click **Server/Code Signing Certificate**.
The **Server Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Select any **GoDaddy certificate**.
7. From the dropdown **Actions** in the toolbar at the top of the page, select **Renew Certificate**.

- [Error Messages](#)
- [Screenshots to get the certificate id \(order id\) from Go Daddy portal](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority - No available units for the selected product type	Units may not be available for the product type selected in the GoDaddy account.	Purchase a valid unit for the product type in the GoDaddy account.
Unable to submit the CSR request to certificate authority - No available units for the selected product type	Units may be available for the product type selected in the GoDaddy account but the selected certificate validity may be incorrect for the product purchased.	Edit the CA connector and change the Validity in CSR parameters as purchased in the product.
Unable to submit the CSR request to certificate authority - No orderId available	There might not be any order id i.e certificate id available for the certificate in ca connector information.	• Update the order id manually by copying it from the GoDaddy portal as shown in the screenshot. • Or do the following: 1. Download and have a backup of the certificate. 2. Delete the certificate from the inventory. 3. Do a GoDaddy discovery to get back the certificate id or order id.
Unable to renew the certificate	There might not be an available product to renew the certificate.	Purchase the product type separately for renewing the certificate.

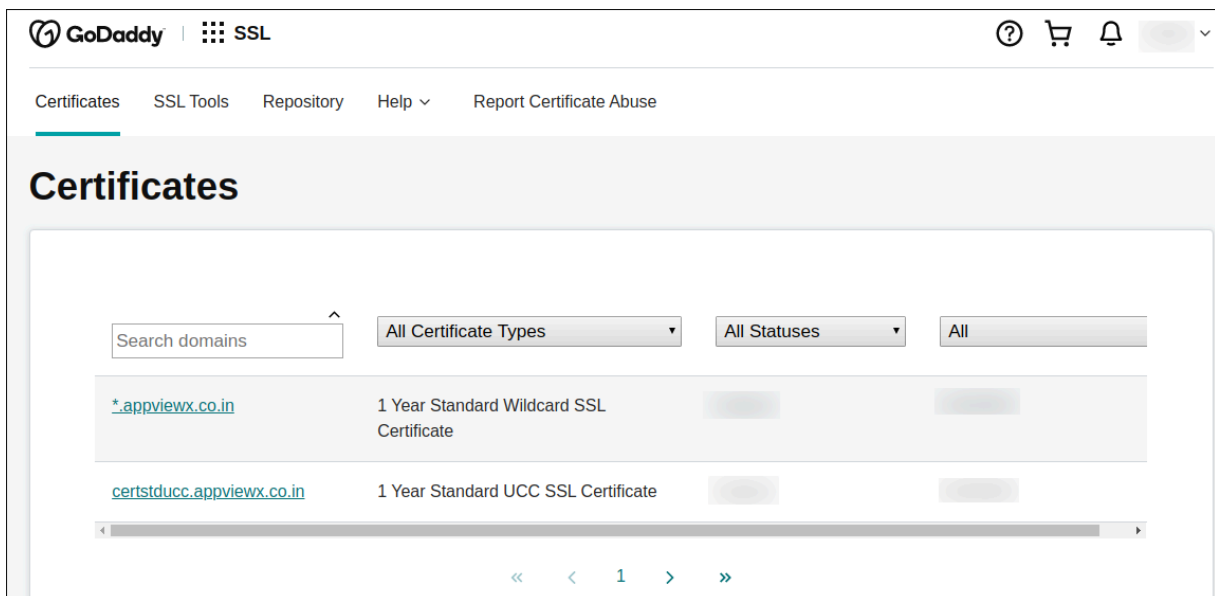
Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Unable to establish connection, Please ensure Proxy / Internet connectivity/ GoDaddy Server.	Invalid proxy details.	Please check the proxy details provided.
Unable to establish connection, Please ensure Proxy / Internet connectivity/ GoDaddy Server.	1. Internet connectivity may not be available. 2. Invalid URL provided in CA Settings.	1. Please check Internet connectivity to reach CA. 2. Please Check whether a valid CA URL is provided in CA Settings or Contact Support Team.
Insufficient privilege for the user to create a certificate.	Request accepted but operation is refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges in GoDaddy server for creating certificates or Contact Support Team.
Invalid Create Certificate Payload	Most likely missing or invalid input parameters / JSON body in the request.	Please validate the input parameters/payload provided or Contact the Support Team.
Too many create certificate requests	Too many create certificate requests for GoDaddy	Please try to create a certificate request after some time or Contact the Support Team.

Screenshots to get the certificate id (order id) from Go Daddy portal

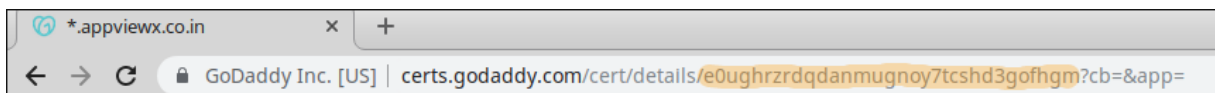
The order id (or) certificate id for a particular certificate can be obtained in GoDaddy URL by following the steps mentioned below:

1. Login to GoDaddy account.
2. Navigate to My Account -> SSL Certificates.

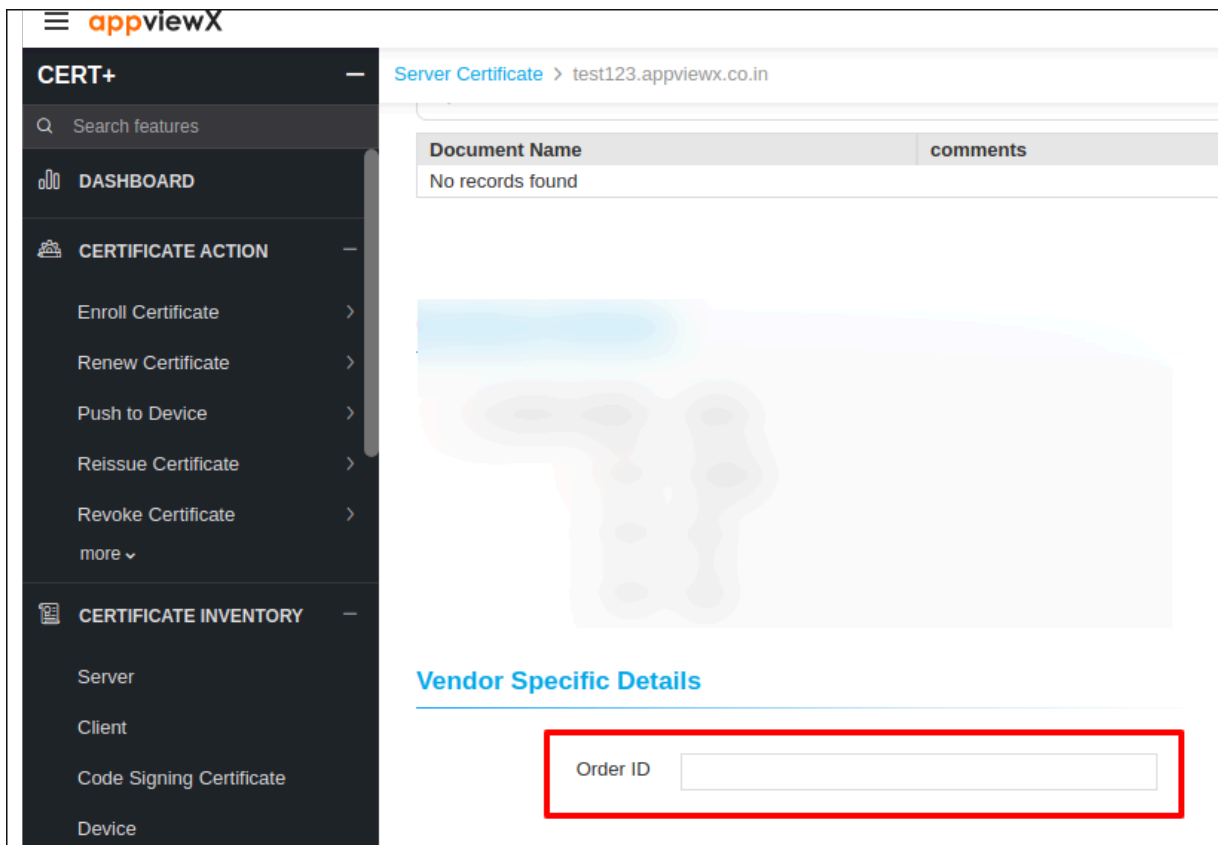
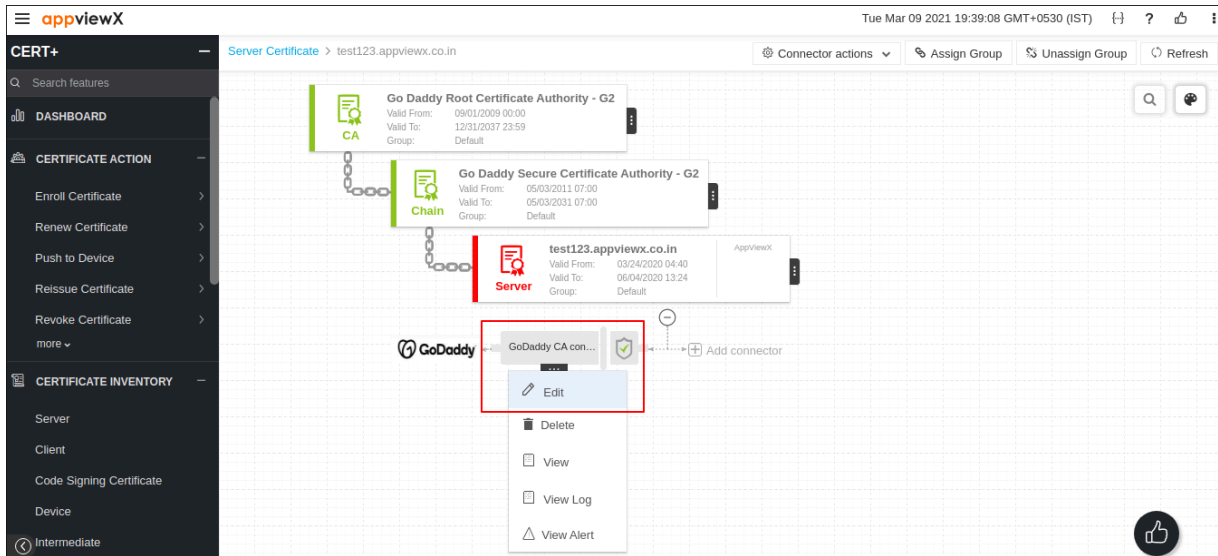
Here you can see the list of certificates created via this GoDaddy account.



3. Click on the certificate for which you require the order id.
- In the URL framed you can see the order id.



4. Use this order id in our AppViewX CA connector as shown below:
 - a. Click on edit in CA connector options.
 - b. Find for Order Id in vendor specific fields.
 - c. Input the order id obtained from CA portal and update the connector.
 - d. Resubmit the failed request.



Issues in Regenerating GoDaddy certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**.
4. Click **Server/Code Signing Certificate**.
The **Server Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **GoDaddy certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Regenerate**.

• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority - No available units for the selected product type	There might not be available units for the product type selected in the GoDaddy account.	Purchase a valid unit for the product type in the GoDaddy account.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Insufficient privilege for the user to create a certificate.	Request accepted but operation is refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges, disabled features in GoDaddy server for creating certificates or Contact Support Team.
Invalid Create Certificate Payload	Missing or invalid input parameters / JSON body in the request.	Please validate the input parameters/ payload provided or Contact the Support Team.

Error Message	Possible Cause	Possible Solution
Too many create certificate requests	Too many create certificate requests for GoDaddy	Please try to create a certificate request after some time or Contact the Support Team.

Issues in Revoking GoDaddy certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Revoke Certificate** submenu.
4. Click **Server/Code Signing Certificate**.
The **Server Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **GoDaddy certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Revoke**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority - No orderId available	There might not be an order id i.e certificate id available for the certificate in ca connector information.	• Update the order id manually by copying it from the GoDaddy portal as shown in the screenshot. • Or do the following:

Error Message	Possible Cause	Possible Solution
		1. Download and have a backup of the certificate. 2. Delete the certificate from the inventory. 3. Do a GoDaddy discovery to get back the certificate id or order id.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.

Issues in Discovering GoDaddy certificates

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery** and select **Discovery**.
4. Click **Certificate Authority Scan**.
The **Discovery: Certificate Authority Scan: Add Discovery** page is displayed.
5. Select **CA** as **GoDaddy**.
6. Click **Discover** at the bottom of the page.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured in the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Unable to establish connection, Please ensure Proxy / Internet connectivity/ GoDaddy Server.	Invalid proxy details.	Please check the proxy details provided.
Unable to establish connection, Please ensure Proxy / Internet connectivity/ GoDaddy Server.	1. Internet connectivity may not be available. 2. Invalid URL provided in CA Settings.	1. Please check Internet connectivity to reach CA. 2. Please Check whether a valid CA URL is provided in CA Settings or Contact Support Team.
Insufficient privilege for the user to create a certificate.	Request accepted but operation is refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges, disabled features in GoDaddy server for creating certificates, or Contact the Support Team.

Troubleshooting Google Private CA

- [Overview](#)
- [Supported Web Browsers](#)
- [Issues in Google Private CA](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using Google private CA functionalities like setting addition, certificate enrollment, renewal, regeneration, revocation, suspension, and discovery.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Google Private CA

- [Issue in Google private CA setting addition and Google fetch CA names](#)
- [Issues in Enrolling Google private certificate](#)
- [Issues in Renewing Google private certificate](#)
- [Issues in Regenerating Google private certificate](#)
- [Issues in Revoking Google private certificate](#)
- [Issues in Suspending Google private certificate](#)
- [Issues in Reinstating Google private certificate](#)
- [Issues in Discovering Google certificates](#)

Issue in Google private CA setting addition and Google fetch CA names

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.

3. From the left pane, expand **Administration** and click **Certificate Authority**.

The **Certificate Authority** page is displayed.

4. On the **Certificate Authority** page, click **Google**.

5. Click **Add**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for Google private already exists in inventory.	Check the CA Setting name, it should be unique.
1) This field should not be null or empty 2) Mandatory Field(s) - <Field name> is/are empty 3) CA Settings - [<Fields>] mandatory fields cannot be empty.	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.
Proxy details not configured	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Failed to generate the authentication token	1. Please check whether the uploaded certificate or json is valid. 2. This URL https://www.googleapis.com may not be reachable.	1. Invalid client certificate or invalid client Json uploaded. 2. Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Empty response received from the CA.	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.

Error Message	Possible Cause	Possible Solution
Permission '<Operation>' denied on '<Resource>'	Permission may not be available for the <operation> for the resource.	Please give permission to the user for the specific operation for the resource.

Issues in Enrolling Google private certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server/Client/Code Signing** Tab.
The **Enroll Server Certificate** page is displayed.
5. Select **Certificate Authority** as **Google**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Requested entity already exists	certificateId value may be already used to issue a certificate.	Please change the certificateId value to the CA connector. It should be unique.
error parsing CSR: generic::invalid_argument: invalid signature: x509: cannot verify signature: algorithm unimplemented	Unsupported keytype or curve details may be used.	Please check the key type and curve and use valid types.
Certificate authority is not enabled.	Certificate authority may not be enabled in Google portal.	Please enable the selected certificate authority.
Proxy details not configured	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.

Error Message	Possible Cause	Possible Solution
Failed to generate the authentication token	1. Please check whether the uploaded certificate or json is valid. 2. This URL https://www.googleapis.com may not be reachable.	1. Invalid client certificate or invalid client Json uploaded. 2. Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Empty response received from the CA.	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Permission '<Operation>' denied on '<Resource>'	Permission may not be available for the <operation> for the resource.	Please give permission to the user for the specific operation for the resource.

Issues in Renewing Google private certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Renew Certificate** submenu.
4. Click **Server/Client/Code Signing Certificate**.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Select any **Google certificate**.
7. From the dropdown **Actions** in the toolbar at the top of the page, select **Renew Certificate**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Requested entity already exists	certificateId value may be already used to issue a certificate.	Please change the certificateId value to the CA connector. It should be unique.
error parsing CSR: generic::invalid_argument: invalid signature: x509: cannot verify signature: algorithm unimplemented	Unsupported key type or curve details may be used.	Please check the key type and curve and use valid types.
Certificate authority is not enabled.	Certificate authority may not be enabled in Google portal.	Please enable the selected certificate authority.
Proxy details not configured	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Failed to generate the authentication token	1. Please check whether the uploaded certificate or json is valid. 2. This URL https://www.googleapis.com may not be reachable.	1. Invalid client certificate or invalid client Json uploaded. 2. Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Empty response received from the CA.	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Permission '<Operation>' denied on '<Resource>'	Permission may not be available for the <operation> for the resource.	Please give permission to the user for the specific operation for the resource.
CSR or private key is not available. Use the regenerate option.	CSR or private key may not be available.	Use regenerate or upload the private key and perform renew.

Issues in Regenerating Google private certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**.
4. Click **Server/Client/Code Signing Certificate** Tab.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **Google certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the Certificate click **Regenerate**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Requested entity already exists	certificateId value may be already used to issue a certificate.	Please change the certificateId value to the CA connector. It should be unique.
error parsing CSR: generic::invalid_argument: invalid signature: x509: cannot verify signature: algorithm unimplemented	Unsupported keytype or curve details may be used.	Please check the key type and curve and use valid types.
Certificate authority is not enabled.	Certificate authority may not be enabled in Google portal.	Please enable the selected certificate authority.
Proxy details not configured	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.

Error Message	Possible Cause	Possible Solution
Failed to generate the authentication token	1. Please check whether the uploaded certificate or json is valid. 2. This URL https://www.googleapis.com may not be reachable.	1. Invalid client certificate or invalid client Json uploaded. 2. Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Empty response received from the CA.	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Permission '<Operation>' denied on '<Resource>'	Permission may not be available for the <operation> for the resource.	Please give permission to the user for the specific operation for the resource.

Issues in Revoking Google private certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Revoke Certificate** submenu.
4. Click **Server/Client/Code Signing Certificate**.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **Google certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the Certificate, click **Revoke**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Revocation reason may not be supported by CA.	Please provide the correct reason.
The requested action is not supported by the issuing CA of the certificate	Selected CA may be in Devops tier.	Please select an Enterprise tier.
Proxy details not configured	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Failed to generate the authentication token	1. Please check whether the uploaded certificate or json is valid. 2. This URL https://www.googleapis.com may not be reachable.	1. Invalid client certificate or invalid client Json uploaded. 2. Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Empty response received from the CA.	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Permission '<Operation>' denied on '<Resource>'	Permission may not be available for the <operation> for the resource.	Please give permission to the user for the specific operation for the resource.

Issues in Suspending Google private certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and Click **Server/Client/Code Signing Certificate**.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
4. From the menu bar at the top of the page, click **List**.
5. Click any **Google certificate**.

A holistic view of **Server Certificate** with the **Certificate number** will be displayed.

6. From the dropdown menu next to the **Certificate**, click **Suspend**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Revocation reasons may not be supported by CA.	Please provide the correct reason.
The requested action is not supported by the issuing CA of the certificate	Selected CA may be in Devops tier.	Please select an Enterprise tier.
Proxy details not configured	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Failed to generate the authentication token	1. Please check whether the uploaded certificate or json is valid. 2. This URL https://www.googleapis.com may not be reachable.	1. Invalid client certificate or invalid client Json uploaded. 2. Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Empty response received from the CA.	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Permission '<Operation>' denied on '<Resource>'	Permission may not be available for the <operation> for the resource.	Please give permission to the user for the specific operation for the resource.

Issues in Reinstating Google private certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.

The **Server Certificate** page is displayed.

3. From the left pane, expand **Certificate Action** and Click **Server/Client/Code Signing Certificate**.

The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.

4. From the menu bar at the top of the page, click **List**.

5. Click any suspended **Google certificate**.

A holistic view of **Server Certificate** with the **Certificate number** will be displayed.

6. From the dropdown menu next to the **Certificate**, click **Reinstate**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Revocation reasons may not be supported by CA.	Please provide the correct reason.
The requested action is not supported by the issuing CA of the certificate	Selected CA may be in Devops tier.	Please select an Enterprise tier.
Proxy details not configured	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Failed to generate the authentication token	1. Please check whether the uploaded certificate or json is valid. 2. This URL https://www.googleapis.com may not be reachable.	1. Invalid client certificate or invalid client Json uploaded. 2. Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Empty response received from the CA.	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Permission '<Operation>' denied on '<Resource>'	Permission may not be available for the <operation> for the resource.	Please give permission to the user for the specific operation for the resource.

Issues in Discovering Google certificates

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery** and select **Discovery**.
4. Click **Certificate Authority Scan**.
The **Discovery: Certificate Authority Scan: Add Discovery** page is displayed.
5. Select **CA** as **Google**.
6. Click **Discover** at the bottom of the page.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Proxy details not configured	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Failed to generate the authentication token	1. Please check whether the uploaded certificate or json is valid. 2. This URL https://www.googleapis.com may not be reachable.	1. Invalid client certificate or invalid client Json uploaded. 2. Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Empty response received from the CA.	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.

Troubleshooting InCommon CA

- [Overview](#)
- [Issues in InCommon CA](#)

Overview

This section helps you troubleshoot the common problems that you might encounter while using functionalities like configuration, setting addition, CLM actions and discovery associated with InCommon Certificate Authority.

Issues in InCommon CA

- [Issues in InCommon CA Configuration](#)
- [Issues in InCommon CA setting validation](#)
- [Issues in Enrolling InCommon Certificate](#)
- [Issues in Regenerating InCommon Certificate](#)
- [Issues in Renewing InCommon Certificate](#)
- [Issues in Reissuing InCommon Certificate](#)
- [Issues in Revoking InCommon Certificate](#)
- [Issues in Discovering InCommon Certificates](#)

Issues in InCommon CA Configuration

1. Log in to **AppViewX** application with valid credentials.
 2. From the left pane, expand the **Menu** and click **Cert+**.
The **Server Certificate** page is displayed.
 3. From the left pane, expand **Administration** and click **Certificate Authority**.
The **Certificate Authority** page is displayed.
 4. On the **Certificate Authority** page, click **InCommon**.
The **InCommon** page is displayed.
 5. Click **Add** or **Configure Now**.
 6. Configure the **General Information** and **CA Configuration** details.
 7. Click **Fetch Certificate Types**.
- [Error Messages](#)

Error Messages

The Certificate types available for the CA account will be fetched from the Certificate Authority.

Following errors may occur during this -

Error Message	Possible Cause	Possible Solution
Fetch certificate types action has failed Unknown user	Username or password may be incorrect.	Check and correct the username and password.
Fetch certificate types action has failed Invalid auth data	URI may be invalid.	Check and correct the URI. For example: <a href="https://cert-manager.com/customer/<customer_uri>/ssl">https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Fetch certificate types action has failed Wrong url specified or the url is not reachable	Base URL may be invalid.	Validate and correct the base URL.
Fetch certificate types action has failed Invalid CA settings details	Proxy details could be wrong.	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings of the general

Issues in InCommon CA setting validation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Certificate Authority**.
The **Certificate Authority** page is displayed.
4. On **Certificate Authority** page, click **InCommon**.
The **Certificate Authority InCommon** Page is displayed.
5. To validate the **CA setting**, Click **Check** in **Connection Status**.

• Error Messages

Error Messages

CA Settings will be validated and the Connection Status will be shown as either Success or Failure.

Possible error scenarios could be -

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password.
Invalid auth data	URI may be invalid	Check and correct the URI. For example: <a href="https://cert-manager.com/customer/<customer_uri>/ssl">https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Connection failed due to incorrect CA settings details : Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL.
Connection failed due to incorrect CA settings details : Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the general settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in general settings.

Issues in Enrolling InCommon Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server/Client** Tab.
The **Enroll Server Certificate** page is displayed.
5. Select **Certificate Authority** as **InCommon** and proceed with certificate enrollment.

• Error Messages

Error Messages

Common reasons and possible Remedies for the failure are mentioned in the table below.

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting. For example: <a href="https://cert-manager.com/customer/<customer_uri>/ssl">https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.
You cannot order certificates for the following or additional domains: testcert.test.net. Please double-check correctness of entered information or navigate to "Domains" subtab of "Settings" tab to request/activate/ delegate them or enable this type of certificate for them in terms of the selected organization.	Domain part of the common name specified in the request is not supported by Certificate Authority	Validate the configured domains or activate the domain in the CA portal, as specified in the error message.
The validity period (term) is invalid for this certificate type.	The validity period (term) is	Please specify the validity period (term)

Error Message	Possible Cause	Possible Solution
	invalid for this certificate type.	that is supported by the chosen cert type in the CA connector and resubmit the request.
Certificate Profile does not support Key Type 'EC - brainpoolP160r1'.	EC key type with the specified curve is not supported for the chosen certificate type.	Please specify the key type that is supported by the chosen cert type in the CA connector and resubmit the request.

Issues in Regenerating InCommon Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.

The **Server Certificate** page is displayed.

3. From the left pane, expand **Certificate Inventory**.
4. Click **Server/Client** Tab.

The **Server Certificate/Client Certificate** page is displayed.

5. From the menu bar at the top of the page, click **List**.
6. Click any **InCommon certificate**.

A holistic view of **Server Certificate** with the **Certificate number** will be displayed.

7. From the dropdown menu next to the **Certificate**, click **Regenerate**.

• [Error Messages](#)

Error Messages

If the request has failed, then the failure status shall be displayed in the holistic view. Click on the **link** above the failure message to know the reason for the workflow failure.

Common reasons for the failure are mentioned in the table below. Please follow the given remediation steps for the respective error message and resubmit the request.

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting. For example: <a href="https://cert-manager.com/customer/<customer_uri>/ssl">https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.
You cannot order certificates for the following or additional domains: testcert.test.net. Please double-check correctness of entered information or navigate to "Domains" subtab of "Settings" tab to request/activate/ delegate them or enable this type of certificate for them in terms of the selected organization.	Domain part of the common name specified in the request is not supported by Certificate Authority	Validate the configured domains or activate the domain in the CA portal, as specified in the error message.
The validity period (term) is invalid for this certificate type.	The validity period (term) is	Please specify the validity period (term)

Error Message	Possible Cause	Possible Solution
	invalid for this certificate type.	that is supported by the chosen cert type in the CA connector and resubmit the request.
Certificate Profile does not support Key Type 'EC - brainpoolP160r1'.	EC key type with the specified curve is not supported for the chosen certificate type.	Please specify the key type that is supported by the chosen cert type in the CA connector and resubmit the request.

Issues in Renewing InCommon Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**.
4. Click **Server/Client** Tab.
The **Server Certificate/Client Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **InCommon certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Renew**.

• [Error Messages](#)

Error Messages

If the request has failed, then the failure status will be shown in the holistic view. Click on the **link** above the failure message to know the reason for the workflow failure.

Common reasons for the failure are mentioned in the table below. Please follow the given remediation steps for the respective error message and resubmit the request.

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting. For example: <a href="https://cert-manager.com/customer/<customer_uri>/ssl">https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.
You cannot order certificates for the following or additional domains: testcert.test.net. Please double-check correctness of entered information or navigate to "Domains" subtab of "Settings" tab to request/activate/ delegate them or enable this type of certificate for them in terms of the selected organization.	Domain part of the common name specified in the request is not supported by Certificate Authority	Validate the configured domains or activate the domain in the CA portal, as specified in the error message.
The validity period (term) is invalid for this certificate type.	The validity period (term) is	Please specify the validity period (term)

Error Message	Possible Cause	Possible Solution
	invalid for this certificate type.	that is supported by the chosen cert type in the CA connector and resubmit the request.

Issues in Reissuing InCommon Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**.
The **Server Certificate** page is displayed.
4. Click **Server/Client** Tab.
The Server **Certificate/Client Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **InCommon certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Reissue**.

- [Error Messages](#)

Error Messages

If the request has failed, then the failure status will be shown in the holistic view. Click on the link above the failure message to know the reason for the workflow failure.

Common reasons for the failure are mentioned in the table below. Please follow the given remediation steps for the respective error message and resubmit the request.

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting.

Error Message	Possible Cause	Possible Solution
		For example: <a href="https://cert-manager.com/customer/<customer_uri>/ssl">https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.
You cannot order certificates for the following or additional domains: testcert.test.net. Please double-check correctness of entered information or navigate to "Domains" subtab of "Settings" tab to request/activate/ delegate them or enable this type of certificate for them in terms of the selected organization.	Domain part of the common name specified in the request is not supported by Certificate Authority	Validate the configured domains or activate the domain in the CA portal, as specified in the error message.
The validity period (term) is invalid for this certificate type.	The validity period (term) is invalid for this certificate type.	Please specify the validity period (term) that is supported by the chosen cert type in the CA connector and resubmit the request.
Certificate Profile does not support Key Type 'EC - brainpoolP160r1'.	EC key type with the specified curve is not	Please specify the key type that is supported by the chosen cert type

Error Message	Possible Cause	Possible Solution
	supported for the chosen certificate type.	in the CA connector and resubmit the request.

Issues in Revoking InCommon Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.

The **Server Certificate** page is displayed.

3. From the left pane, expand **Certificate Inventory**.
4. Click **Server/Client** Tab.

The **Server Certificate/Client Certificate** page is displayed.

5. From the menu bar at the top of the page, click **List**.
6. Click any **InCommon certificate**.

A holistic view of **Server Certificate** with the **Certificate number** will be displayed.

7. From the dropdown menu next to the **Certificate**, click **Revoke**.

- [Error Messages](#)

Error Messages

If the request has failed, then the failure status will be shown in the holistic view. Click on the **link** above the failure message to know the reason for the workflow failure.

Common reasons for the failure are mentioned in the table below. Please follow the given remediation steps for the respective error message and resubmit the request.

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting. For example: <a href="https://cert-manager.com/customer/<customer_uri>/ssl">https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.

Error Message	Possible Cause	Possible Solution
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.

Issues in Discovering InCommon Certificates

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery** and select **Discovery**.
4. Click **Certificate Authority Scan**.
The **Discovery: Certificate Authority Scan: Add Discovery** page is displayed.
5. Select **CA** as **InCommon** and provide the necessary information.
6. Click **Discover** at the bottom of the page.

• Error Messages

Error Messages

If the discovery status is Failed, the reason for failure will be available in the Discovery Batch Summary pop, which can be launched by clicking the icon next to the discovery status.

Common reasons for the failure are mentioned in the table below. Please follow the given remediation steps for the respective error message and resubmit the request.

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting.

Error Message	Possible Cause	Possible Solution
		For example: <a href="https://cert-manager.com/customer/<customer_uri>/ssl">https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA Settings.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.

Troubleshooting LetsEncrypt CA

- [Overview](#)
- [Supported Web Browsers](#)
- [LetsEncrypt CA Issues](#)

Overview

This section helps you troubleshoot the common problems that you might encounter while using functionalities like setting addition, connectivity, certificate enrollment, renewal, revocation, and other actions associated with LetsEncrypt.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1

Browser	Version	Notes
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

LetsEncrypt CA Issues

- [Issues in LetsEncrypt CA Settings Addition](#)
- [Issues in Enrolling certificate using LetsEncrypt CA](#)
- [Issues in Renewing certificate using LetsEncrypt CA](#)
- [Issues in Revoking certificate using LetsEncrypt CA](#)
- [Issues in LetsEncrypt CA Connectivity Check](#)
- [Issues in sending Rest requests to LetsEncrypt CA](#)

Issues in LetsEncrypt CA Settings Addition

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Certificate Authority**.
The **Certificate Authority** page is displayed.
4. On the **Certificate Authority** page, click **LetsEncrypt**.
5. Click **Add**.

• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to save CA settings. CA settings name already exists.	A CA setting with the same name for LetsEncrypt already exists in inventory.	Check the CA Setting name, it should be unique.
Please validate given information	Invalid URL given.	Please check the URL.
	LetsEncrypt portal might be down.	Please check any problem in the LetsEncrypt portal.
	Proxy might be required.	Please check the proxy required for this environment. Proxy details may not be configured in proxy settings.
This field should not be null or empty.	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.
Mandatory Field(s) - <Field name> is/are empty		

Error Message	Possible Cause	Possible Solution
CA Settings - [<Fields>] mandatory fields cannot be empty.		
Invalid Email Id	Email ID given while account creation is invalid.	Provide valid email ID.

Issues in Enrolling certificate using LetsEncrypt CA

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server/Client/Code Signing** Tab.
The **Enroll Server Certificate** page is displayed.
5. Select **Certificate Authority** as **LetsEncrypt**.

• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid proxy details specified.	Proxy detail is not configured in proxy settings or is invalid.	Provide valid proxy details.
Invalid Authorization	Authorization failed while fetching the challenge.	Provide valid CSR details in the request to receive valid order details in the CA response.
Challenge Not Found	Challenge not received from CA.	Provide valid CSR details in the request to receive valid order details in the CA response.
Error during calculating thumbprint	Invalid public key or publicjsonweb key.	Provide valid details while adding the LetsEncrypt account.
Timeout while Validating Challenge	Challenge verification was not completed within the time limit.	Verify the challenge within the time limit or generate a new challenge and verify.

Error Message	Possible Cause	Possible Solution
Challenge Verification Failed	Challenge verification returned status as Invalid from CA.	Check if the internet or proxy is enabled. Check if the TXT record has been added correctly.

Issues in Renewing certificate using LetsEncrypt CA

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Renew Certificate** submenu.
4. Click **Server/Client/Code Signing Certificate**.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Select any **LetsEncrypt certificate**.
7. From the dropdown **Actions** in the toolbar at the top of the page, select **Renew Certificate**.

• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid proxy details specified.	Proxy detail is not configured in proxy settings or is invalid.	Provide valid proxy details.

Issues in Revoking certificate using LetsEncrypt CA

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Revoke Certificate** submenu.
4. Click **Server/Client/Code Signing Certificate**.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **LetsEncrypt certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Revoke**.

• [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid proxy details specified.	Proxy detail is not configured in proxy settings or is valid.	Provide valid proxy details.
Content Extraction Failed	Unable to get encoded X509 certificate using its content.	Provide valid certificate content for the certificate to be revoked.

Issues in LetsEncrypt CA Connectivity Check

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Certificate Authority**.
The **Certificate Authority** page is displayed.
4. On the **Certificate Authority** page, click **LetsEncrypt**.
The **Certificate Authority LetsEncrypt Page** is displayed.
5. To check connectivity with the **CA**, click **Check** in **Connection Status**.

Lets Encrypt				
Name	Purpose/Usage	Connection Status	Account ID	
LetsEncryptCA	Server	New Check	https://acme-v02.api.letsencrypt.org/acme/acct/115123...	

• [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Communication with CA failed.	Proxy details provided may be incorrect.	Provide valid proxy details.

Error Message	Possible Cause	Possible Solution
	Invalid LetsEncrypt Account Id.	Provide valid credentials associated with a valid account.

Issues in sending Rest requests to LetsEncrypt CA

Error Message	Possible Cause	Possible Solution
In getKeyStore(), While getting instance for the keystore and loading the store file	Unable to read keystore file "avx_client_cert_keystore" from security path, i.e. \${JAVA_HOME}/lib/security/	Internal error. Possibly a deployment issue. Contact support team.
In createStore(), While traversing to java security folder	Java security directory is missing or is corrupted.	Internal error. Possibly a deployment issue. Contact support team.
In createStore(), While getting the instance for the keystore	Unable to get Keystore instance.	Internal error. Possibly a deployment issue. Contact support team.
In createStore(), While loading the key store	Unable to load keystore.	Internal error. Possibly a deployment issue. Contact support team.

Troubleshooting Microsoft Enterprise CA

- [Overview](#)
- [Supported Web Browsers](#)
- [Issues in Microsoft Enterprise CA](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using functionalities like setting addition, certificate enrollment, renewal, revocation, suspension, reinstatement, discovery, and other actions associated with Microsoft Enterprise.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Microsoft Enterprise CA

- [Issues in Microsoft Enterprise CA setting addition and fetch CAs](#)
- [Issues in Enrolling, Fetching, Renewing, Regenerating Microsoft Enterprise certificate](#)
- [Issues in Revoking Microsoft Enterprise certificate](#)
- [Issues in Suspending Microsoft Enterprise certificate](#)
- [Issues in Reinstating Microsoft Enterprise certificate](#)
- [Issues in Discovering Microsoft Enterprise certificates](#)

Issues in Microsoft Enterprise CA setting addition and fetch CAs

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Certificate Authority**.
The **Certificate Authority** page is displayed.

4. On the **Certificate Authority** page, click **Microsoft**, select **Enterprise**.
5. Click **Add**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for Microsoft Enterprise already exists in inventory.	Check the CA Setting name, it should be unique.
1) This field should not be null or empty 2) Mandatory Field(s) - <Field name> is/are empty 3) CA Settings - [<Fields>] mandatory fields cannot be empty.	Some of the mandatory fields might be missing or invalid.	Add all the valid information in the mandatory section.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.

Error Message	Possible Cause	Possible Solution
767cf2b6-bfc3-45a0-9490-a95cf841e693: Connecting to remote server <SERVER> failed with the following error message : WinRM cannot process the request. The following error occurred while using Kerberos authentication: The computer <SERVER> is unknown to Kerberos. Verify that the computer exists on the network, that the name provided is spelled correctly, and that the Kerberos configuration for accessing the computer is correct. The most common Kerberos configuration issue is that an SPN with the format HTTP/<SERVER> is not configured for the target. If Kerberos is not required, specify the Negotiate authentication mechanism and resubmit the operation. For more information, see the about_Remote_Troubleshooting Help topic	Kerberos configuration is not configured for the target machine. The most common Kerberos configuration issue is that an SPN with the format HTTP/<SERVER> is not configured for the target.	The issue occurs with Powershell Remoting since it uses Kerberos Authentication. • In Agent Machine start command prompt as Administrator and execute the following command • setspn -s http/machinename domain\username. • Please note this will work in environments where Kerberos Authentication is set up and there is an AD Domain Setup • If no kerberos authentication is set up then we need to communicate via WMI. • Verify that the computer exists on the network, that the name provided is spelled correctly, and that the Kerberos configuration for accessing the computer is correct. • If Kerberos is not required, specify the Negotiate authentication mechanism and resubmit the operation. For more information, see the about_Remote_Troubleshooting Help topic.
PowerShell ScriptExecution Error: Access is denied. 0x80070005 (WIN32: 5) OR Error Code 0x80070005 - Access is denied	Access is denied.	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should

Error Message	Possible Cause	Possible Solution
		be part of Local Administrator group. 3. Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group.
The WinRM client received an HTTP status code of 502 from the remote WS-Management service. For more information, see the about_Remote_Troubleshooting Help topic	Powershell remoting not configured.	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force". 4. Execute "netsh winhttp show proxy" and if a proxy is configured then we need to reset it via "netsh winhttp reset proxy". 5. For more information, see the about_Remote_Troubleshooting Help topic.
41783361-015b-453f-b321-e31709b1850c: Connecting to remote server <SERVER> failed with the following error message : Access is denied. For more information, see the about_Remote_Troubleshooting Help topic.	Access is denied.	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group. 3. Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group.

Error Message	Possible Cause	Possible Solution
		4. Check if WinRM service is running. 5. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 6. Execute "Enable-PSRemoting -force". 7. For more information, see the about_Remote_Troubleshooting Help topic.
The client cannot connect to the destination specified in the request. Verify that the service on the destination is running and is accepting requests. Consult the logs and documentation for the WS-Management service running on the destination, most commonly IIS or WinRM. If the destination is the WinRM service, run the following command on the destination to analyze and configure the WinRM service: "winrm quickconfig"	Powershell remoting is not configured.	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force". 4. Verify that the service on the destination is running and is accepting requests. 5. Consult the logs and documentation for the WS-Management service running on the destination, most commonly IIS or WinRM. 6. If the destination is the WinRM service, run the following command on the destination to analyze and configure the WinRM service: "winrm quickconfig".
d4f98a6a-41ef-4864-9848-03a07e113d75: CCertRequest::Submit: The RPC server	The Remote Procedure Call Service	Navigate to the target machine and start RPC service if it has stopped.

Error Message	Possible Cause	Possible Solution
is unavailable. 0x800706ba (WIN32: 1722 RPC_S_SERVER_UNAVAILABLE)	is not responding.	
727838ed-151e-46bf-883c-07ccb3a3989f: Connecting to remote server ptpld005 failed with the following error message : The user name or password is incorrect. For more information, see the about_Remote_Troubleshooting Help topic.	The username or password is incorrect.	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group. 3. Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group. 4. Check if WinRM service is running. 5. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 6. Execute "Enable-PSRemoting -force". 7. For more information, see the about_Remote_Troubleshooting Help topic.
fd3812f9-030a-421c-81e7-0e0510ce49e0: Access to the path <PATH> is denied.	The username or password is incorrect.	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group.

Error Message	Possible Cause	Possible Solution
		3. Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group.
This site can't be reached	This site can't be reached.	1. Windows Gateway is not reachable from AppViewX. 2. Windows Gateway service is down.
Html response : Access is denied	Access is denied.	1. In Target machine's Local Computer certificate store, Trusted Root Certification Authorities should have Root CA certificates and Intermediate Certification Authorities should have intermediate certificates only. 2. Client certificate used in AppViewX is not imported in Target machine's Local computer store.
More than 5 connections are not allowed	Powershell configuration has restricted access for concurrent script executions.	Run Powershell as Administrator 1. Check existing config winrm get winrm/config. 2. Change the settings to increase the maxshellsperUser to 100 on the Remote machine wherein this issue is occurring winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}' winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}'

Error Message	Possible Cause	Possible Solution
		<pre>winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'</pre> .
Connecting to the remote server failed with the following error message : The WS-Management service cannot process the request. This user is allowed a maximum number of 4 concurrent shells, which has been exceeded. Close existing shells or raise the quota for this user.	Powershell configuration has restricted access for concurrent script executions.	Run Powershell as Administrator 1. Check existing config winrm get winrm/config. 2. Change the settings to increase the maxshellsperUser to 100 on the Remote machine wherein this issue is occurring <pre>winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}'</pre> <pre>winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}'</pre> <pre>winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'</pre> .
Client Certificate gives Permission Denied 403 error. This can happen in certain environment and its intermittent	CA Store mismatch or invalid client certificate used.	1. Check if the Client certificate is installed correctly by checking the chain in the Personal Store. 2. Root of the client certificate should be available in the Trusted Root Certification Store of the Server. 3. Intermediate of the client certificate can be available in the Intermediate Certification authorities of the Server. 4. If all the above looks good then go to the agent server and do the following steps

Error Message	Possible Cause	Possible Solution
		a. MMC. b. Add "Add/Remove SnapIn. c. select certificates. d. select "LocalMachine". e. Navigate to the Personal Store and click on the client certificate. f. Navigate to Chain. g. Export the Root certificate and save it as Root.cer in a location. h. Import the "Root.cer" into trusted Root back again. i. If the issue still remains unsolved, then check if the Trusted root contains and non-root certificates. j. Click on the "Trusted Root" store and check if there are certificates that have different IssuedTo and IssuedBy. k. Take a backup of such certificates and move it to respective stores. l. If the issue remains unsolved, then add the root certificate to "Client Certificate Issuers".
the permission on the certificate template do not allow the current user to enroll for this type of certificate	User does not have access to the certificate template	1. Navigate to CA Server. 2. open Certificate Authority. 3. Select the CA Server. 4. Right click on properties. 5. Click on Security Tab.

Error Message	Possible Cause	Possible Solution
	used for enrollment.	6. Check if the user used in Agent has necessary permissions to read, issue and manage certificates and request certificates. 7. If a user is part of a group then please ensure that the group has permissions. 8. Click on Certificate Templates and right-click to manage templates. 9. Right-click on the template which has the issue and navigate to security. 10. Add permission to the user or group.
An attempt was made to open a Certification Authority database session, but there are already too many active sessions" on a request using CERTADMINLib.IenumCERTVIEWROW.Next().	The Certification Authority database has too many active sessions.	In CA server navigate to registry via regedit command and set the following: 1. HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBSessionCount to 64 hex (100 Dec). 2. HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBMaxReadSessionCount is also set to 64 hex (100 Dec).
803f4314-3a11-486a-87e5-367b8c5c6f9f: The user name or password is incorrect.\r\n	The user name or password is incorrect.	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be

Error Message	Possible Cause	Possible Solution
		part of the Local Administrator group. 3. Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group
42abe1ef-2bff-40e8-82e2-c97c5707a0c1: Connecting to remote server avxstca failed with the following error message : The user name or password is incorrect. For more information, see the about_Remote_Troubleshooting Help topic.	The user name or password is incorrect.	Check if the credentials are valid.
Connecting to remote server ptpld334 failed with the following error message : WinRM cannot complete the operation. Verify that the specified computer name is valid, that the computer is accessible over the network, and that a firewall exception for the WinRM service is enabled and allows access from this computer. By default, the WinRM firewall exception for public profiles limits access to remote computers within the same local subnet. For more information, see the about_Remote_Troubleshooting Help topic.	Powershell remoting is not configured.	1. C:\Windows\system32>WinRM quickconfig 2. WinRM service is already running on this machine. 3. WinRM is not set up to allow remote access to this machine for management. 4. The following changes must be made: • Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine. • Make these changes [y/n]? y • WinRM has been updated for remote management. • Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.
1. There is not enough space on the disk	There is not enough	Ensure that your hard disk has enough free space.

Error Message	Possible Cause	Possible Solution
2. The WSMAN service could not launch a host process to process the given request. Make sure the WSMAN provider host server and proxy are properly registered. For more information, see the about_Remote_Troubleshooting Help topic. 3. Execute process failed Machinename mspwvadsnybcc01.csc.nycnet, ProcessName Powershell -NoProfile - ExecutionPolicy Bypass -Command C:\\Windows\\Temp\\1jmtip3g.sjl\\1jmtip3g.sjl.ps1, Error is, Stack trace Management Connect to remote machine mspwvadsnybcc01.csc.nycnet as user failed with the following error Value does not fall within the expected range.	space on the disk.	
Management Connect to remote machine VMEUSWPCA021.us.int.safelite.net as user failed with the following error User credentials cannot be used for local connections	User credentials cannot be used for local connections.	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of the Local Administrator group. 3. Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group. 4. or configure the credentials in AppViewX.CertPlus.Service Logon option.
Device Communication failed while using Native option to connect to CA remotely	Local System Account doesn't have access to	1. Navigate to agent machine.. 2. Open services.msc using Start>>Run command on the windows machine.

Error Message	Possible Cause	Possible Solution
	CA. Please change the logon credentials in service.	3. Find the service "AppViewXCertPlus". 4. Right-click and view properties. 5. Click "log on" tab. 6. Change the option to this account and enter the user account and password information. 7. Click on "Apply" and a message will pop up to add an account as "Log on as service". Click "OK" and save the changes. 8. Click on restart the service 9. Remove the username and password from AppViewX.

Issues in Enrolling, Fetching, Renewing, Regenerating Microsoft Enterprise certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**.
4. Click **Server/Client/Code Signing Certificate** Tab.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **Microsoft Enterprise certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Regenerate**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	Check the CA details configured on the CA settings page. Check whether proxy details are configured in proxy settings. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.
The account configured in Application pool identity don't have access to the requested Template	User doesn't have access to the template.	Please give access to the user.
DATA is invalid log message	Invalid header for CSR.	Replace (----BEGIN NEW CERTIFICATE REQUEST----) with (----BEGIN CERTIFICATE REQUEST----) and Replace (----END NEW CERTIFICATE

Error Message	Possible Cause	Possible Solution
		REQUEST----) with (----END CERTIFICATE REQUEST----)
Error Code 0x80070005 - Access is denied	Access not available.	1. Agent and CA Should be under the same domain. 2. ApplicationPoolIdentity of IIS Agent site should be a Custom account with admin credentials. 3. To verify template name, Go to CA portal, Right. Click on Certificate templates, Select Manage, Select the template, right-click on it, and select properties, In General Tab, you can find Template name which needs to be used in AppViewX. 4. To check Template permission, Go to the CA portal, Right. Click on Certificate templates, Select Manage, Select the template, right-click on it and select properties, in the security tab check all permissions given for the user.
Retrieving the COM class factory for remote component with CLSID	Unable to connect to certificate authority.	1. The Component used for accessing CA (certadm.dll) is not installed or has permission issues. 2. Check if dll is available in C:\Windows\System32 folder else install Microsoft Remote Server Administration Tools

Error Message	Possible Cause	Possible Solution
		(RSAT) for the respective OS. EX: for Windows 10 https://www.microsoft.com/en-in/download/details.aspx?id=45520
PowerShell ScriptExecution Error: Access is denied. 0x80070005 (WIN32: 5) OR Error Code 0x80070005 - Access is denied	Access is denied.	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group 3. Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group.
the permission on the certificate template do not allow the current user to enroll for this type of certificate	User does not have access to the certificate template used for enrollment.	1. Navigate to CA Server. 2. Open Certificate Authority. 3. Select the CA Server. 4. Right-click on properties. 5. Click on Security Tab. 6. Check if the user used in Agent has the necessary permissions to read, issue and manage certificates and request certificates. 7. If a user is part of a group then please ensure that the group has permissions. 8. Click on Certificate Templates and right-click to manage templates.

Error Message	Possible Cause	Possible Solution
		9. Right-click on the template which has the issue and navigate to security. 10. Add permission to the user or group.
An attempt was made to open a Certification Authority database session, but there are already too many active sessions" on a request using CERTADMINLib.IenumCERTVIEWROW.Next().	The Certification Authority database has too many active sessions.	In CA server navigate to registry via regedit command and set the following: 1. HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBSessionCount to 64 hex (100 Dec). 2. HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBMaxReadSessionCount is also set to 64 hex (100 Dec).
The WinRM client received an HTTP status code of 502 from the remote WS-Management service. For more information, see the about_Remote_Troubleshooting Help topic	Powershell remoting not configured.	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force". 4. Execute "netsh winhttp show proxy" and if a proxy is configured then we need to reset it via "netsh winhttp reset proxy".

Error Message	Possible Cause	Possible Solution
The client cannot connect to the destination specified in the request. Verify that the service on the destination is running and is accepting requests. Consult the logs and documentation for the WS-Management service running on the destination, most commonly IIS or WinRM. If the destination is the WinRM service, run the following command on the destination to analyze and configure the WinRM service: "winrm quickconfig"	Powershell remoting is not configured.	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force".
More than 5 connections are not allowed	Powershell configuration has restricted access for concurrent script executions.	Run Powershell as Administrator 1. Check existing config 2. winrm get winrm/config. 3. Change the settings to increase the maxshellsperUser to 100 on the Remote machine wherein this issue is occurring: • winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}' • winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}' • winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'.
Connecting to the remote server failed with the following error message : The WS-Management service cannot process the request. This user is allowed a maximum number of 4 concurrent shells, which has been exceeded. Close existing shells or raise the quota for this user.	Powershell configuration has restricted access for concurrent script executions	Run Powershell as Administrator 1. Check existing config 2. winrm get winrm/config. 3. Change the settings to increase the maxshellsperUser to 100 on

Error Message	Possible Cause	Possible Solution
		the Remote machine wherein this issue is occurring: • winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}' • winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}' • winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'.
Client Certificate gives Permission Denied 403 error. This can happen in certain environment and its intermittent	1. Certificate store mismatch. 2. Invalid client certificate specified.	1. Check if the Client certificate is installed correctly by checking the chain in the Personal Store. 2. Root of the client certificate should be available in the Trusted Root Certification Store of the Server. 3. Intermediate of the client certificate can be available in the Intermediate Certification authorities of the Server. 4. If all the above looks good then go to the agent server and do the following steps: a. MMC. b. Add "Add/Remove SnapIn. c. select certificates. d. select "LocalMachine". e. Navigate to the Personal Store and click on the client certificate. f. Navigate to Chain. g. Export the Root certificate and save it as Root.cer in a location.

Error Message	Possible Cause	Possible Solution
		h. Import the "Root.cer" into trusted Root back again. i. If this also doesn't solve the issue then check if the Trusted root contains and non-root certificates. j. Click on the "Trusted Root" store and check if there are certificates that have different IssuedTo and IssuedBy. k. Take a backup of such certificates and move it to respective stores. l. Even after this if it doesn't solve then add the root certificate to "Client Certificate Issuers".
Certificate Request (CSR) is using different account to request certificate from CA as compared to account configured in AppViewX		1. Navigate to the agent machine. 2. Open services.msc using Start>>Run command on the windows machine. 3. Find service "AppViewXCertPlus" 4. Right-click and view properties. 5. Click on "log on" tab 6. Change the option to this account and enter the user account and password information. 7. Click on "Apply" and a popup message will appear and ask you to add an account as "Log

Error Message	Possible Cause	Possible Solution
		on as service". Click "OK" and save the changes. 8. Click on restart the service. 9. Remove the username and password from AppViewX.
CSR Parameters invalid error	CSR Parameters supplied mismatch with Selected template/CA's Policy.	Supply valid CSR values accepted by template or CA policy.
Denied by Policy Module 0x80094800, The request was for a certificate template that is not supported by the Active Directory Certificate Services policy: WebServer1.	Incorrect certificate template used.	Use template name instead of the template display name.
Connecting to remote server ptpld334 failed with the following error message : WinRM cannot complete the operation. Verify that the specified computer name is valid, that the computer is accessible over the network, and that a firewall exception for the WinRM service is enabled and allows access from this computer. By default, the WinRM firewall exception for public profiles limits access to remote computers within the same local subnet. For more information, see the about_Remote_Troubleshooting Help topic.	Powershell remoting is not configured.	C:\Windows\system32>WinRM quickconfig WinRM service is already running on this machine. WinRM is not set up to allow remote access to this machine for management. The following changes must be made: • Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine. • Make these changes [y/n]? y • WinRM has been updated for remote management.

Error Message	Possible Cause	Possible Solution
		Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.

Issues in Revoking Microsoft Enterprise certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Revoke Certificate** submenu.
4. Click **Server/Client/Code Signing Certificate**.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **Microsoft Enterprise certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Revoke**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Invalid reason specified for revocation	Please use the correct reason supported by the CA.

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether client certificate is valid.

Issues in Suspending Microsoft Enterprise certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and Click **Server/Client/Code Signing Certificate**.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
4. From the menu bar at the top of the page, click **List**.
5. Click any **Microsoft Enterprise certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
6. From the dropdown menu next to the **Certificate**, click **Suspend**.

• [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Invalid reason specified for suspension.	Please use the correct reason supported by the CA.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured in the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether client certificate is valid.

Issues in Reinstating Microsoft Enterprise certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and Click **Server/Client/Code Signing Certificate**.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
4. From the menu bar at the top of the page, click **List**.
5. Click any suspended **Microsoft Enterprise certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
6. From the dropdown menu next to the **Certificate**, click **Reinstate**.

• [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Invalid reason specified for reinstatement.	Please use the correct reason supported by the CA.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured in the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.

Issues in Discovering Microsoft Enterprise certificates

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery** and select **Discovery**.
4. Click **Certificate Authority Scan**.
The **Discovery: Certificate Authority Scan: Add Discovery** page is displayed.

5. Select **CA** as **Microsoft Enterprise**.
6. Click **Discover** at the bottom of the page.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.

Troubleshooting Microsoft Standalone CA

- [Overview](#)
- [Supported Web Browsers](#)
- [Issues in Microsoft Standalone CA](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using functionalities like setting addition, certificate enrollment, renewal, revocation, suspension, reinstatement, discovery, and other actions associated with Microsoft Standalone.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Microsoft Standalone CA

- [Issues in Microsoft Standalone CA setting addition and fetch CAs](#)
- [Issues in Enrolling, Fetching, Renewing, Regenerating Microsoft Standalone certificate](#)
- [Issues in Revoking Microsoft Standalone certificate](#)
- [Issues in Suspending Microsoft Standalone certificate](#)
- [Issues in Reinstating Microsoft Standalone certificate](#)
- [Issues in Discovering Microsoft Standalone certificates](#)

Issues in Microsoft Standalone CA setting addition and fetch CAs

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Certificate Authority**.
The **Certificate Authority** page is displayed.
4. On the **Certificate Authority** page, click **Microsoft**.
5. Click **Standalone**.
6. Click **Add**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for Microsoft Enterprise already exists in inventory.	Check the CA Setting name, it should be unique.
1) This field should not be null or empty 2) Mandatory Field(s) - <Field name> is/are empty 3) CA Settings - [<Fields>] mandatory fields cannot be empty.	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.
Unable to establish connection with CA	1. The configured CA details may be incorrect.	1. Check the CA details configured in the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.

Error Message	Possible Cause	Possible Solution
	2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	
767cf2b6-bfc3-45a0-9490-a95cf841e693: Connecting to remote server <SERVER> failed with the following error message : WinRM cannot process the request. The following error occurred while using Kerberos authentication: The computer <SERVER> is unknown to Kerberos. Verify that the computer exists on the network, that the name provided is spelled correctly, and that the Kerberos configuration for accessing the computer is correct. The most common Kerberos configuration issue is that an SPN with the format HTTP/<SERVER> is not configured for the target. If Kerberos is not required, specify the Negotiate authentication mechanism and resubmit the operation. For more information, see the about_Remote_Troubleshooting Help topic	Kerberos configuration is not configured for target machine	The issue occurs with “Powershell Remoting” since it uses Kerberos Authentication 1. In Agent Machine start command prompt as Administrator and execute the following command. 2. <code>setspn -s http/machinename domain \username.</code> 3. Please note this will work in environments where Kerberos Authentication is setup and there is an AD Domain Setup. 4. If no kerberos authentication is set up then we need to communicate via WMI.
PowerShell ScriptExecution Error: Access is denied. 0x80070005 (WIN32: 5) OR Error Code 0x80070005 - Access is denied	Access is denied	1. The username should be configured as "Username@Domain" 2. The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group

Error Message	Possible Cause	Possible Solution
		3. Navigate to local Users and Groups and access "Administrators". Check if the configured username is part of administrator group
The WinRM client received an HTTP status code of 502 from the remote WS-Management service. For more information, see the about_Remote_Troubleshooting Help topic	Powershell remoting not configured	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force". Execute "netsh winhttp show proxy" and if a proxy is configured then we need to reset it via "netsh winhttp reset proxy".
41783361-015b-453f-b321-e31709b1850c: Connecting to remote server <SERVER> failed with the following error message : Access is denied. For more information, see the about_Remote_Troubleshooting Help topic.	Access is denied	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of the Local Administrator group. 3. Navigate to local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group. 4. Check if WinRM service is running. 5. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 6. Execute "Enable-PSRemoting -force".
The client cannot connect to the destination specified in the request. Verify that the service on the dest	Powershell remoting is not configured	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force".

Error Message	Possible Cause	Possible Solution
ination is running and is accepting requests. Consult the logs and documentation for the WS-Management service running on the destination, most commonly IIS or WinRM. If the destination is the WinRM service, run the following command on the destination to analyze and configure the WinRM service: "winrm quickconfig"		
d4f98a6a-41ef-4864-9848-03a07e113d75: CCertRequest::Submit: The RPC server is unavailable. 0x800706ba (WIN32: 1722 RPC_S_SERVER_UNAVAILABLE)	Remote Procedure Call Service is not responding	Navigate to the target machine and start RPC service if it has stopped.
727838ed-151e-46bf-883c-07ccb3a3989f: Connecting to remote server ptpld005 failed with the following error message : The user name or password is incorrect. For more information, see the about_Remote_Troubleshooting Help topic.	The username or password is incorrect.	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of the Local Administrator group. 3. Navigate to local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group. 4. Check if WinRM service is running. 5. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 6. Execute "Enable-PSRemoting -force".
fd3812f9-030a-421c-81e7-0e0510ce49e0: Access to the path <PATH> is denied.	The username or password is incorrect	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target

Error Message	Possible Cause	Possible Solution
		Machine) or should be part of the Local Administrator group. 3. Navigate to local Users and Groups and access "Administrators". 4. Check if the configured username is part of the administrator group.
This site can't be reached	This site can't be reached	1. Windows Gateway is not reachable from AppViewX. 2. Windows Gateway service is down.
Html response : Access is denied	Access is denied	1. In Target machine's Local Computer certificate store, Trusted Root Certification Authorities should have Root CA certificates and Intermediate Certification Authorities should have intermediate certificates only. 2. Client certificates used in AppViewX are not imported in Target machine's Local computer store.
More than 5 connections are not allowed	Powershell configuration has restricted access for concurrent script executions	Run Powershell as Administrator. 1. Check existing config. 2. winrm get winrm/config. 3. Change the settings to increase the maxshellsperUser to 100 on the Remote machine wherein this issue is occurring. • winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}'. • winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}'. • winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'.

Error Message	Possible Cause	Possible Solution
Connecting to the remote server failed with the following error message : The WS-Management service cannot process the request. This user is allowed a maximum number of 4 concurrent shells, which has been exceeded. Close existing shells or raise the quota for this user.	Powershell configuration has restricted access for concurrent script executions	Run Powershell as Administrator 1. Check existing config. 2. winrm get winrm/config. 3. Change the settings to increase the maxshellsperUser to 100 on the Remote machine wherein this issue is occurring. • winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}'. • winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}'. • winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'.
Client Certificate gives Permission Denied 403 error. This can happen in certain environment and its intermittent	CA Store mismatch or invalid client certificate used	1. Check if the Client certificate is installed correctly by checking the chain in the Personal Store. 2. Root of the client certificate should be available in the Trusted Root Certification Store of the Server. 3. Intermediate of the client certificate can be available in the Intermediate Certification authorities of the Server. 4. If all the above looks good then go to agent server and do following steps a. MMC. b. Add "Add/Remove SnapIn. c. select certificates. d. select "LocalMachine" e. Navigate to the Personal Store and click on the client certificate. f. Navigate to Chain. g. Export the Root certificate and save as Root.cer in a location.

Error Message	Possible Cause	Possible Solution
		h. Import the "Root.cer" into trusted Root back again. i. If this also doesn't solve the issue then check if the Trusted root contains and non-root certificates. j. Click on "Trusted Root" store and check if there are any certificates which have different IssuedTo and IssuedBy. k. Take backup of such certificates and move it to respective stores. l. Even after this if it doesn't solve then add the root certificate to "Client Certificate Issuers".
An attempt was made to open a Certification Authority database session, but there are already too many active sessions" on a request using CERTADMINLib.IenumCERTVIEWROW.Next().	Certification Authority database has too many active sessions	In CA server navigate to registry via regedit command and set the following 1. HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBSessionCount to 64 hex (100 Dec) 2. HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBMaxReadSessionCount is also set to 64 hex (100 Dec)
803f4314-3a11-486a-87e5-367b8c5c6f9f: The user name or password is incorrect.\r\n	The username or password is incorrect	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of the Local Administrator group. 3. Navigate to local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group.

Error Message	Possible Cause	Possible Solution
42abe1ef-2bff-40e8-82e2-c97c5707a0c1: Connecting to remote server avxstca failed with the following error message : The user name or password is incorrect. For more information, see the about_Remote_Troubleshooting Help topic.	The username or password is incorrect	The username or password is incorrect.
Connecting to remote server ptpld334 failed with the following error message : WinRM cannot complete the operation. Verify that the specified computer name is valid, that the computer is accessible over the network, and that a firewall exception for the WinRM service is enabled and allows access from this computer. By default, the WinRM firewall exception for public profiles limits access to remote computers within the same local subnet. For more information, see the about_Remote_Troubleshooting Help topic.	Powershell remoting is not configured	C:\Windows\system32>WinRM quickconfig WinRM service is already running on this machine. WinRM is not set up to allow remote access to this machine for management. The following changes must be made: • Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine. • Make these changes [y/n]? y • WinRM has been updated for remote management. • Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.
1. There is not enough space on the disk 2. The WSMAN service could not launch a host process to process the given request. Make sure the WSMAN provider host server and proxy are properly registered. For more information, see the about_Remote_Troubleshooting Help topic. 3. Execute process failed Machinename mspwvadsnybcc01.csc.nycnet, ProcessName Powershell -NoProfile - ExecutionPolicy	There is not enough space on the disk	Ensure that your hard disk has enough free space.

Error Message	Possible Cause	Possible Solution
Bypass -Command C:\\Windows\\Temp\\1jmtip3g.sjl\\1jmtip3g.sjl.ps1, Error is, Stack trace Management Connect to remote machine mspwvadsnybcc01.csc.nycnet as user failed with the following error Value does not fail within the expected range.		
Management Connect to remote machine VMEUSWPCA021.us.int.safelite.net as user failed with the following error User credentials cannot be used for local connections	User credentials cannot be used for local connections	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of the Local Administrator group. 3. Navigate to local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group.or configure the credentials in AppViewX.CertPlus.Service Logon option.
Device Communication failed while using Native option to connect to CA remotely	Local System Account doesn't have access to CA. Please change the logon credentials in service.	1. Navigate to the agent machine. 2. Open services.msc using Start>>Run command on the windows machine. 3. Find the service "AppViewXCertPlus". 4. Right click and view properties. 5. Click on "log on" tab. 6. Change the option to this account and enter the user account and password information. 7. Click on "Apply" and a message will popup to add an account as "Log on as service". Click "OK" and save the changes.

Error Message	Possible Cause	Possible Solution
		8. Click on restart the service. 9. Remove the username and password from AppViewX.

Issues in Enrolling, Fetching, Renewing, Regenerating Microsoft Standalone certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**.
4. Click **Server/Client/Code Signing Certificate** Tab.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **Microsoft Standalone certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Regenerate**.

• [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured.	1. Check the CA details configured in the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.

Error Message	Possible Cause	Possible Solution
	3. AppViewX may not be able to reach CA	
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.
DATA is invalid log message	Invalid header for CSR	Replace (----BEGIN NEW CERTIFICATE REQUEST----) with (----BEGIN CERTIFICATE REQUEST----) and Replace (----END NEW CERTIFICATE REQUEST----) with (----END CERTIFICATE REQUEST----)
Error Code 0x80070005 - Access is denied	Access not available	1. Agent and CA Should be under the same domain. 2. ApplicationPoolIdentity of IIS Agent site should be a Custom account with admin credentials.
Retrieving the COM class factory for remote component with CLSID	Unable to connect to certificate authority	1. The Component used for accessing CA (certadm.dll) is not installed or has permission issues. 2. Check if DLL is available in C:\Windows\System32 folder else install Microsoft Remote Server Administration Tools (RSAT) for

Error Message	Possible Cause	Possible Solution
		respective OS. EX: for Windows 10 https://www.microsoft.com/en-in/download/details.aspx?id=45520 .
PowerShell ScriptExecution Error: Access is denied. 0x80070005 (WIN32: 5) OR Error Code 0x80070005 - Access is denied	Access is denied	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of the Local Administrator group. 3. Navigate to local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group.
An attempt was made to open a Certification Authority database session, but there are already too many active sessions" on a request using CERTADMINLib.IenumCERTVIEWROW.Next().	Certification Authority database has too many active sessions	In CA server navigate to registry via regedit command and set the following 1) HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBSessionCount to 64 hex (100 Dec) 2) HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBMaxReadSessionCount is also set to 64 hex (100 Dec)
The WinRM client received an HTTP status code of 502 from the remote WS-Management service. For more information, see the about_Remote_Troubleshooting Help topic	Powershell remoting not configured	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force". 4. Execute "netsh winhttp show proxy" and if a proxy is configured then we need to reset it via "netsh winhttp reset proxy".

Error Message	Possible Cause	Possible Solution
The client cannot connect to the destination specified in the request. Verify that the service on the destination is running and is accepting requests. Consult the logs and documentation for the WS-Management service running on the destination, most commonly IIS or WinRM. If the destination is the WinRM service, run the following command on the destination to analyze and configure the WinRM service: "winrm quickconfig"	Powershell remoting is not configured.	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force".
More than 5 connections are not allowed	Powershell configuration has restricted access for concurrent script executions.	Run Powershell as Administrator 1. Check existing config 2. winrm get winrm/config. 3. Change the settings to increase the maxshellsperUser to 100 on the Remote machine wherein this issue is occurring. • winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}' • winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}' • winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'
Connecting to the remote server failed with the following error message : The WS-Management service cannot process the request. This user is allowed a maximum number of 4 concurrent shells, which has been exceeded. Close existing shells or raise the quota for this user.	Powershell configuration has restricted access for concurrent script executions.	Run Powershell as Administrator 1. Check existing config 2. winrm get winrm/config. 3. Change the settings to increase the maxshellsperUser to 100 on the Remote machine wherein this issue is occurring.

Error Message	Possible Cause	Possible Solution
		• winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}' • winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}' • winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'
Client Certificate gives Permission Denied 403 error. This can happen in certain environment and its intermittent	1. Certificate store mismatch. 2. Invalid client certificate specified.	1. Check if the Client certificate is installed correctly by checking the chain in the Personal Store. 2. Root of the client certificate should be available in the Trusted Root Certification Store of the Server. 3. Intermediate of the client certificate can be available in the Intermediate Certification authorities of the Server. 4. If all the above looks good then go to agent server and do following steps: a. MMC . b. Add "Add/Remove SnapIn c. select certificates. d. select "LocalMachine". e. Navigate to the Personal Store and click on the client certificate. f. Navigate to Chain. g. Export the Root certificate and save as Root.cer in a location. h. Import the "Root.cer" into trusted Root back again. i. If this also doesn't solve the issue then check if the Trusted root contains and non-root certificates. j. Click on "Trusted Root" store and check if there are any certificates which have different IssuedTo and IssuedBy.

Error Message	Possible Cause	Possible Solution
		k. Take backup of such certificates and move it to respective stores. l. Even after this if it doesn't solve then add the root certificate to "Client Certificate Issuers"
Certificate Request (CSR) is using different account to request certificate from CA as compared to account configured in AppViewX		1. Navigate to the agent machine. 2. Open services.msc using Start>>Run command on the windows machine. 3. Find the service "AppViewXCertPlus". 4. Right click and view properties. 5. Click on the "log on" tab. 6. Change the option to this account and enter the user account and password information. 7. Click on "Apply" and a message will popup to add an account as "Log on as service". Click "OK" and save the changes. 8. Click on restart the service. 9. Remove the username and password from AppViewX.
Connecting to remote server ptpld334 failed with the following error message : WinRM cannot complete the operation. Verify that the specified computer name is valid, that the computer is accessible over the network, and that a firewall exception for the WinRM service is enabled and allows access from this computer. By default, the WinRM firewall exception for public profiles limits access to remote computers within the same local	Powershell remoting is not configured	1. C:\Windows\system32>WinRM quickconfig. 2. WinRM service is already running on this machine. 3. WinRM is not set up to allow remote access to this machine for management. 4. The following changes must be made:

Error Message	Possible Cause	Possible Solution
subnet. For more information, see the about_Remote_Troubleshooting Help topic.		• Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine. • Make these changes [y/n]? y • WinRM has been updated for remote management. • Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.

Issues in Revoking Microsoft Standalone certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Revoke Certificate** submenu.
4. Click **Server/Client/Code Signing Certificate**.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **Microsoft Standalone certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Revoke**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Invalid reason specified for revocation	Please use the correct reason which is supported by the CA

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured in the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.

Issues in Suspending Microsoft Standalone certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and Click **Server/Client/Code Signing Certificate**.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
4. From the menu bar at the top of the page, click **List**.
5. Click any **Microsoft Standalone certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
6. From the dropdown menu next to the **Certificate**, click **Suspend**.

• [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Invalid reason specified for suspension	Please use the correct reason which is supported by the CA
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured in the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.

Issues in Reinstating Microsoft Standalone certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and Click **Server/Client/Code Signing Certificate**.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
4. From the menu bar at the top of the page, click **List**.
5. Click any suspended **Microsoft Standalone certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
6. From the dropdown menu next to the **Certificate**, click **Reinstate**.

• [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Invalid reason specified for reinstatement	Please use the correct reason which is supported by the CA
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured in the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.

Issues in Discovering Microsoft Standalone certificates

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery** and select **Discovery**.
4. Click **Certificate Authority Scan**.
The **Discovery: Certificate Authority Scan: Add Discovery** page is displayed.

5. Select **CA** as **Microsoft Standalone**.
6. Click **Discover** at the bottom of the page.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether client certificate is valid

Troubleshooting Sectigo CA

- [Overview](#)
- [Issues in Sectigo CA](#)

Overview

This section helps you troubleshoot the common problems that you might encounter while using functionalities like setting addition, certificate enrollment, renewal, revocation, discovery, and other actions associated with Sectigo Certificate Authority.

Issues in Sectigo CA

- [Issues in Sectigo CA Configuration](#)
- [Issues in Sectigo CA setting validation](#)
- [Issues in Enrolling Sectigo Certificate](#)
- [Issues in Regenerating Sectigo Certificate](#)
- [Issues in Renewing Sectigo Certificate](#)
- [Issues in Reissuing Sectigo Certificate](#)
- [Issues in Revoking Sectigo Certificate](#)
- [Issues in Discovering Sectigo Certificates](#)

Issues in Sectigo CA Configuration

1. Log in to **AppViewX** application with valid credentials.
 2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
 3. From the left pane, expand **Administration** and click **Certificate Authority**.
The **Certificate Authority** page is displayed.
 4. On the **Certificate Authority** page, click **Sectigo**.
The **Sectigo** page is displayed.
 5. Click **Add** or **Configure Now**.
 6. Configure the **General Information** and **CA Configuration** details.
 7. Click **Fetch Certificate Types**.
The Certificate types available for the CA account will be fetched from the **Certificate Authority**.
- [Error Messages](#)

Error Messages

Following errors may occur in this step -

Error Message	Possible Cause	Possible Solution
Fetch certificate types action has failed Unknown user	Username or password may be invalid	Check and correct the username and password.
Fetch certificate types action has failed Invalid auth data	URI may be invalid	Check and correct the URI. For example: <a href="https://cert-manager.com/customer/<customer_uri>/ssl">https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Fetch certificate types action has failed Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL.
Fetch certificate types action has failed Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the general settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA settings but proxy details are not configured in proxy settings.	Configure the proxy details in general settings.

Issues in Sectigo CA setting validation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Certificate Authority**.
The **Certificate Authority** page is displayed.
4. On the **Certificate Authority** page, click **Sectigo**.
The **Sectigo** Page is displayed.
5. To validate the **CA setting**, click **Check** in **Connection Status**.
CA settings will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.

• Error Messages

Error Messages

Possible error scenarios could be as follows:

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be in valid	Check and correct the username and password.
Invalid auth data	URI may be invalid	Check and correct the URI. For example: <a href="https://cert-manager.com/customer/<customer_uri>/ssl">https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Connection failed due to incorrect CA settings details : Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL.
Connection failed due to incorrect CA settings details : Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the general settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA settings but proxy details are not configured in proxy settings.	Configure the proxy details in general settings.

Issues in Enrolling Sectigo Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server/Client** Tab.
The **Enroll Certificate** page is displayed.
5. Select **Certificate Authority** as **Sectigo** and proceed with **Certificate Enrollment**.

• Error Messages

Error Messages

Common reasons for the failure are mentioned in the table below. Please follow the respective remediation steps and resubmit the request.

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting. For example: <a href="https://cert-manager.com/customer/<customer_uri>/ssl">https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.
You cannot order certificates for the following or additional domains: testcert.test.net. Please double-check correctness of entered information or navigate to "Domains" subtab of "Settings" tab to request/activate/ delegate them or enable this type of certificate for them in terms of the selected organization.	Domain part of the common name specified in the request is not supported by Certificate Authority	Validate the configured domains or activate the domain in the CA portal, as specified in the error message.
The validity period (term) is invalid for this certificate type.	The validity period (term) is	Please specify the validity period (term)

Error Message	Possible Cause	Possible Solution
	invalid for this certificate type.	that is supported by the chosen cert type in the CA connector and resubmit the request.
Certificate Profile does not support Key Type 'EC - brainpoolP160r1'.	EC key type with the specified curve is not supported for the chosen certificate type.	Please specify the key type that is supported by the chosen cert type in the CA connector and resubmit the request.

Issues in Regenerating Sectigo Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.

The **Server Certificate** page is displayed.

3. From the left pane, expand **Certificate Inventory**.
4. Click **Server/Client** Tab.

The **Server Certificate/Client Certificate** page is displayed.

5. From the menu bar at the top of the page, click **List**.
6. Click any **Sectigo certificate**.

A holistic view of **Server Certificate** with the **Certificate number** will be displayed.

7. From the dropdown menu next to the **Certificate**, click **Regenerate**.

- [Error Messages](#)

Error Messages

If the request has failed, then the failure status will be shown in the holistic view. Click on the link above the failure message to know the reason for the workflow failure.

Common reasons for the failure are mentioned in the table below. Please follow the respective remediation steps and resubmit the request.

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting. For example: <a href="https://cert-manager.com/customer/<customer_uri>/ssl">https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.
You cannot order certificates for the following or additional domains: testcert.test.net. Please double-check correctness of entered information or navigate to "Domains" subtab of "Settings" tab to request/activate/ delegate them or enable this type of certificate for them in terms of the selected organization.	Domain part of the common name specified in the request is not supported by Certificate Authority	Validate the configured domains or activate the domain in the CA portal, as specified in the error message.
The validity period (term) is invalid for this certificate type.	The validity period (term) is	Please specify the validity period (term)

Error Message	Possible Cause	Possible Solution
	invalid for this certificate type.	that is supported by the chosen cert type in the CA connector and resubmit the request.
Certificate Profile does not support Key Type 'EC - brainpoolP160r1'.	EC key type with the specified curve is not supported for the chosen certificate type.	Please specify the key type that is supported by the chosen cert type in the CA connector and resubmit the request.

Issues in Renewing Sectigo Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**.
4. Click **Server/Client** Tab.
The **Server Certificate/Client Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **Sectigo certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Renew**.

• [Error Messages](#)

Error Messages

If the request has failed, then the failure status will be shown in the holistic view. Click on the link above the failure message to know the reason for the workflow failure.

Common reasons for the failure are mentioned in the table below. Please follow the respective remediation steps and resubmit the request.

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting. For example: <a href="https://cert-manager.com/customer/<customer_uri>/ssl">https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.
You cannot order certificates for the following or additional domains: testcert.test.net. Please double-check correctness of entered information or navigate to "Domains" subtab of "Settings" tab to request/activate/ delegate them or enable this type of certificate for them in terms of the selected organization.	Domain part of the common name specified in the request is not supported by Certificate Authority	Validate the configured domains or activate the domain in the CA portal, as specified in the error message.
The validity period (term) is invalid for this certificate type.	The validity period (term) is	Please specify the validity period (term)

Error Message	Possible Cause	Possible Solution
	invalid for this certificate type.	that is supported by the chosen cert type in the CA connector and resubmit the request.

Issues in Reissuing Sectigo Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.

The **Server Certificate** page is displayed.

3. From the left pane, expand **Certificate Inventory**.
4. Click **Server/Client** Tab.

The **Server Certificate/Client Certificate** page is displayed.

5. From the menu bar at the top of the page., click **List**.
6. Click any **Sectigo certificate**.

A holistic view of **Server Certificate** with the **Certificate number** will be displayed.

7. From the dropdown menu next to the **Certificate**, click **Reissue**.

• [Error Messages](#)

Error Messages

If the request has failed, then the failure status will be shown in the holistic view. Click on the link above the failure message to know the reason for the workflow failure.

Common reasons for the failure are mentioned in the table below. Please follow the respective remediation steps and resubmit the request.

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting.

Error Message	Possible Cause	Possible Solution
		For example: <a href="https://cert-manager.com/customer/<customer_uri>ssl">https://cert-manager.com/customer/<customer_uri>ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.
You cannot order certificates for the following or additional domains: testcert.test.net. Please double-check correctness of entered information or navigate to "Domains" subtab of "Settings" tab to request/activate/ delegate them or enable this type of certificate for them in terms of the selected organization.	Domain part of the common name specified in the request is not supported by Certificate Authority	Validate the configured domains or activate the domain in the CA portal, as specified in the error message.
The validity period (term) is invalid for this certificate type.	The validity period (term) is invalid for this certificate type.	Please specify the validity period (term) that is supported by the chosen cert type in the CA connector and resubmit the request.
Certificate Profile does not support Key Type 'EC - brainpoolP160r1'.	EC key type with the specified curve is not	Please specify the key type that is supported by the chosen cert type

Error Message	Possible Cause	Possible Solution
	supported for the chosen certificate type.	in the CA connector and resubmit the request.

Issues in Revoking Sectigo Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.

The **Server Certificate** page is displayed.

3. From the left pane, expand **Certificate Inventory**.
4. Click **Server/Client** Tab.

The **Server Certificate/Client Certificate** page is displayed.

5. From the menu bar at the top of the page, click **List**.
6. Click any **Sectigo certificate**.

A holistic view of **Server Certificate** with the **Certificate number** will be displayed.

7. From the dropdown menu next to the **Certificate**, click **Revoke**.

- [Error Messages](#)

Error Messages

If the request has failed, then the failure status will be shown in the holistic view. Click on the **link** above the failure message to know the reason for the workflow failure.

Common reasons for the failure are mentioned in the table below. Please follow the respective remediation steps and resubmit the request.

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting. For example: <a href="https://cert-manager.com/customer/<customer_uri>/ssl">https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.

Error Message	Possible Cause	Possible Solution
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.

Issues in Discovering Sectigo Certificates

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery** and select **Discovery**.
4. Click **Certificate Authority Scan**.
The **Discovery: Certificate Authority Scan: Add Discovery** page is displayed.
5. Select **CA** as **Sectigo** and provide the necessary information.
6. Click **Discover** at the bottom of the page.

• Error Messages

Error Messages

If the discovery status is Failed, the reason for failure will be available in the Discovery Batch Summary pop, which can be launched by clicking the icon next to the discovery status.

Common reasons for the failure are mentioned in the table below. Please follow the respective remediation steps and rerun the discovery.

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting.

Error Message	Possible Cause	Possible Solution
		For example: <a href="https://cert-manager.com/customer/<customer_uri>/ssl">https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA Settings.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.

Troubleshooting Symantec CA

- [Overview](#)
- [Supported Web Browsers](#)
- [Issues in Symantec CA](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using functionalities like setting addition, certificate enrollment, renewal, regeneration, revocation, reissue, and other actions associated with Symantec CA.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1

Browser	Version	Notes
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Symantec CA

- [Issues in Symantec CA setting addition and fetch custom attributes](#)
- [Issues in Enrolling Symantec certificate](#)
- [Issues in Fetching Symantec certificate](#)
- [Issues in Renewing Symantec certificate](#)
- [Issues in Regenerating Symantec certificate](#)
- [Issues in Revoking Symantec certificate](#)
- [Issues in Reissuing Symantec certificate](#)

Issues in Symantec CA setting addition and fetch custom attributes

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Certificate Authority**.
The **Certificate Authority** page is displayed.
4. On the **Certificate Authority** page, click **Symantec**.
5. Click **Add**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for Symantec already exists in inventory.	Check the CA Setting name, it should be unique.
1) This field should not be null or empty 2) Mandatory Field(s) - <Field name> is/are empty 3) CA Settings - [<Fields>] mandatory fields cannot be empty.	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.
<Field> should not be blank	Mandatory field <Field> may be missing	Please add the field <Field> and proceed
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
The SSL certificate error	Used certificate may be invalid	Use the valid certificate

Issues in Enrolling Symantec certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server/Client/Code Signing** Tab.
The **Enroll Server Certificate** page is displayed.
5. Select **Certificate Authority** as **Symantec**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
The SSL certificate error	Used certificate may be invalid.	Use the valid certificate.

Issues in Fetching Symantec certificate

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings.	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
The SSL certificate error	Used certificate may be invalid.	Use the valid certificate.

Issues in Renewing Symantec certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Renew Certificate** submenu.
4. Click **Server/Client/Code Signing Certificate**.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Select any **Symantec certificate**.
7. From the dropdown **Actions** in the toolbar at the top of the page, select **Renew Certificate**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX	Please configure proxy details in AppViewX
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
The SSL certificate error	Used certificate may be invalid.	Use the valid certificate
CSR or private key is not available. Use the regenerate option.	CSR or private key may not be available	Use regenerate or upload the private key and perform renew.

Issues in Regenerating Symantec certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**.
4. Click **Server/Client/Code Signing Certificate** Tab.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. Click **List** From the menu bar at the top of the page.
6. Click any **Symantec certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Regenerate**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.

Error Message	Possible Cause	Possible Solution
The SSL certificate error	Used certificate may be invalid.	Use the valid certificate.

Issues in Revoking Symantec certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Revoke Certificate** submenu.
4. Click **Server**.
The **Server Certificate** page is displayed.
5. From the menu bar at the top of the page , click **List**.
6. Click any **Symantec certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Revoke**.

• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
The SSL certificate error	Used certificate may be invalid.	Use the valid certificate.

Issues in Reissuing Symantec certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and and select **Reissue Certificate** submenu.
4. Click **Server**.
The **Server Certificate** page is displayed.

5. From the menu bar at the top of the page, click **List**.

6. Click any **Symantec certificate**.

A holistic view of **Server Certificate** with the **Certificate number** will be displayed.

7. From the dropdown menu next to the **Certificate**, click **Reissue**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
The SSL certificate error	Used certificate may be invalid.	Use the valid certificate.

Troubleshooting Trustwave CA

- [Overview](#)
- [Supported Web Browsers](#)
- [Issues in Trustwave CA](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using functionalities like setting addition, certificate enrollment, renewal, regeneration, revocation, reissue, and other actions associated with Trustwave CA.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post AppViewX Version 11.0

Browser	Version	Notes
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Trustwave CA

- [Issues in Trustwave CA setting addition](#)
- [Issues in Enrolling Trustwave certificate](#)
- [Issues in Fetching Trustwave certificate](#)
- [Issues in Renewing Trustwave certificate](#)
- [Issues in Regenerating Trustwave certificate](#)
- [Issues in Revoking Trustwave certificate](#)
- [Issues in Reissuing Trustwave certificate](#)

Issues in Trustwave CA setting addition

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Certificate Authority**.
The **Certificate Authority** page is displayed.
4. On the **Certificate Authority** page, click **Trustwave**.
5. Click **Add**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for Trustwave already exists in inventory.	Check the CA Setting name, it should be unique.
1) This field should not be null or empty 2) Mandatory Field(s) - <Field name> is/are empty 3) CA Settings - [<Fields>] mandatory fields cannot be empty.	Some of the mandatory fields might be missing or invalid.	Add all the valid information in the mandatory section.
<Field> should not be blank	Mandatory field <Field> may be missing.	Please add the field <Field> and proceed.
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
Authentication failed for user <user>	Username or password may be wrong	Please provide the valid username and password
Authorization failed	Incorrect reseller id provided	Please provide valid reseller id.
You don't have permission to access <url> on this server.	Invalid URL specified.	Please provide a valid URL.

Issues in Enrolling Trustwave certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server/Client/Code Signing** Tab.
The **Enroll Server Certificate** page is displayed.
5. Select **Certificate Authority** as **Trustwave**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
Unsupported certificate type {certType} with validity year : {year}	Certificate type selected may be invalid.	Please select the valid certificate type.
The following name(s) do not end with a top level domain registered in IANA's Root Zone Database: <commonName>	Specified common name is invalid , it should end with a domain name.	Please provide a valid common name.

Issues in Fetching Trustwave certificate

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
Certificate is not issued	Certificate polling may be in progress.	Certificate polling will happen and retrieve once the certificate is issued.

Issues in Renewing Trustwave certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Renew Certificate** submenu.
4. Click **Server/Client/Code Signing Certificate**.

The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.

5. From the menu bar at the top of the page, click **List**.
6. Select any **Trustwave certificate**.
7. From the dropdown **Actions** in the toolbar at the top of the page, select **Renew Certificate**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
Order Id not provided to get corresponding certificate Id.	Order id may not be available in the CA connector.	Please update the order id in the CA connector and proceed.
CSR or private key is not available. Use the regenerate option.	CSR or private key may not be available.	Use regenerate or upload the private key and re- perform renew.

Issues in Regenerating Trustwave certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**.
4. Click **Server/Client/Code Signing Certificate** Tab.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **Trustwave certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Regenerate**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX
Unsupported certificate type {certType} with validity year : {year}	Certificate type selected may be invalid.	Please select the valid certificate type.
The following name(s) do not end with a top level domain registered in IANA's Root Zone Database: <commonName>	Invalid common name specified, it should end with a domain name.	Please provide a valid common name.

Issues in Revoking Trustwave certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Revoke Certificate** submenu.
4. Click **Server/Client/Code Signing Certificate**.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **Trustwave certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Revoke**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.

Error Message	Possible Cause	Possible Solution
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
Order Id not provided to get corresponding certificate Id.	Order id may not be available in the CA connector.	Please update the order id in the CA connector and proceed.

Issues in Reissuing Trustwave certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Reissue Certificate** submenu.
4. Click **Server/Client/Code Signing Certificate** Tab.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **Trustwave certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Reissue**.

• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Proxy details are not configured in proxy settings.	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
Order Id not provided to get corresponding certificate Id.	Order id may not be available in the CA connector.	Please update the order id in the CA connector and proceed.
CSR content is empty	CSR may not be available for the certificate to reissue.	Either CSR or private key should be available in the certificate.

Windows Agent Setup

- [Overview](#)
- [Installing a Validator:](#)
- [Windows Gateway Errors and Solutions](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using Windows Agent Setup. Effective troubleshooting documents depend on the availability of useful, detailed information. This guide will give more troubleshooting processes on Windows Agent Setup. It helps you understand the importance of installing a validator and the method to do so.

Installing a Validator:

Validator analyzes an Agent and validates all the prerequisites before installing an agent. It is also used to troubleshoot any issue that occurs in the managed machines that run on a network. Before installing AppViewX gateway and the certificates, make sure you have downloaded the validator to either the Downloads folder or to the Desktop in your local environment.

1. Click the AppViewX.CertPlus.Validator.exe file to open the application for validation.
2. In the AppViewX CertPlus Validator screen that opens enter all the mandatory fields in the Basic Information section to proceed.
3. Select the Agent, Certificate Authority, IIS, and Non-IIS checkbox depending on what you want to validate and manage in the target machine.

- Based on the checkboxes you selected, the fields that are mandatory will be highlighted in Red color.
- The CA Name is required only if the Certificate Authority check box is selected.

Click Submit and the results are displayed as shown in the following image:

- AppViewX CertPlus Compatibility Checker is used for troubleshooting or validating the prerequisites as part of Windows Agent Installation. It comprises the following fields:

Name	Description	Condition
Machine Name	The name of the target machine must be validated. It is a hostname.	Mandatory field
CA Name	The name of the CA in the CA config.	Mandatory only when a CA is selected
User Name	User Name to be used for validating the target machine. It is in the format "username@domainname".	Mandatory field
Password	The password corresponding to the provided user name.	Mandatory field

Options

- User can select single or multiple options based on the installation/ troubleshooting criteria:
- Agent: Select this option if we need to install an agent in the target machine which is configured in the "Machine Name". It will validate the prerequisites which are required for Agent Installation
- Certificate Authority: Select this option if we need to validate the Certificate Authority related functionality. The CA Name is mandatory only in this case. Use the certutil -dump command to get the

CA Name. In the output of certutil command use-value in the "Server" as the Machine Name and use "Name" as the CA Name.

- Based on the example below the machine Name is win3.avxdevlab.net and CA Name is avxdevlab-WIN3-CA-no-space.
- IIS: Select this option if we need to validate the IIS sites related functionality.

Validations

Validate	Agent	CA	IIS	Keystore
User	Yes	Yes	Yes	Yes
.Net framework	Yes	Yes	Yes	Yes
Powershell	Yes	Yes	Yes	Yes
CertUtil	Yes	Yes	No	No
Certadm.dll	Yes	Yes	No	No
netsh	Yes	No	No	No
RPC	Yes	Yes	Yes	Yes
WinRM	Yes	Yes	Yes	Yes
WMI	Yes	Yes	Yes	Yes
IIS	No	No	Yes	No

- **KeyStore:** Select this option if you need to add to validate only the Microsoft Certificate Store related functionality

```

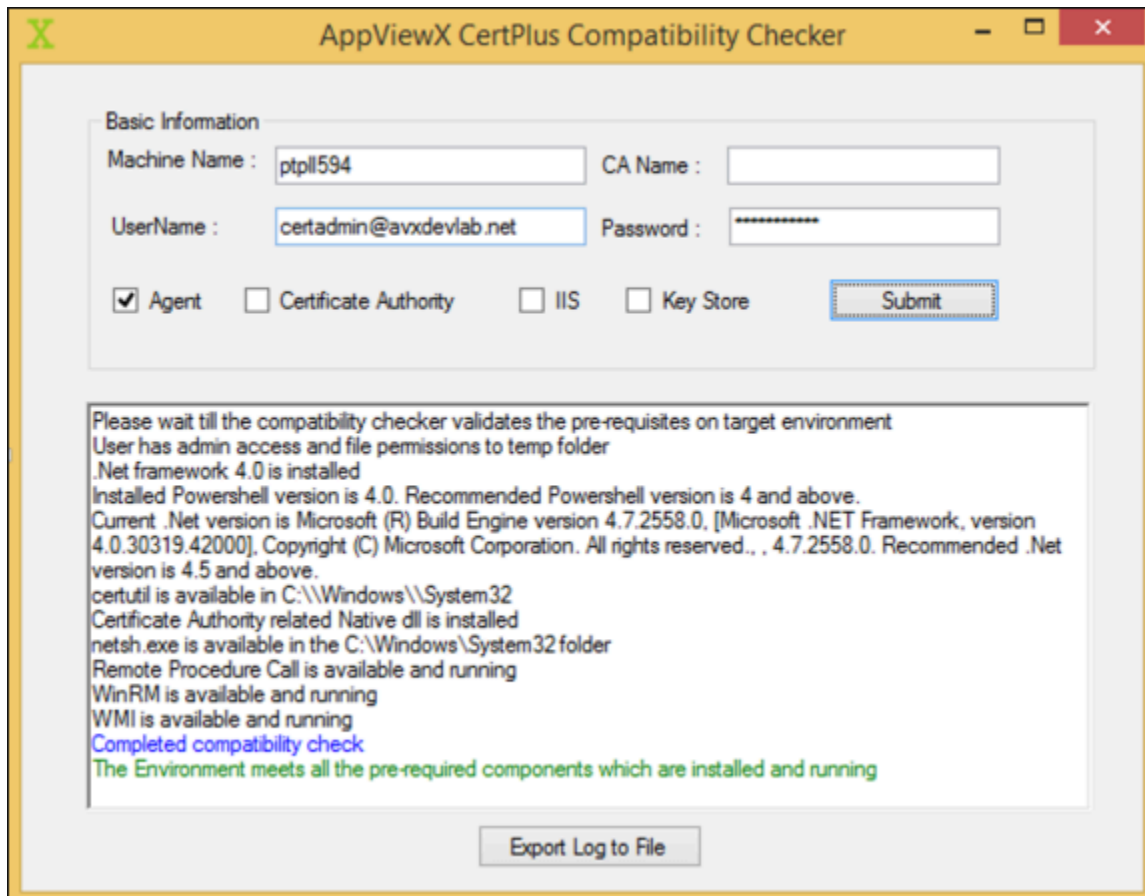
Entry 5:
Name: 'avxdevlab-WIN3-CA-no-space'
Organizational Unit: ''
Organization: ''
Locality: ''
State: ''
Country/region: ''
Config: 'win3.avxdevlab.net\avxdevlab-WIN3-CA-no-space'
Exchange Certificate: ''
Signature Certificate: ''
Description: ''
Server: 'win3.avxdevlab.net'
Authority: 'avxdevlab-WIN3-CA-no-space'
Sanitized Name: 'avxdevlab-WIN3-CA-no-space'
Short Name: 'avxdevlab-WIN3-CA-no-space'
Sanitized Short Name: 'avxdevlab-WIN3-CA-no-space'
Flags: '1'
Web Enrollment Servers: ''
CertUtil: -dump command completed successfully.

```


1. User Access: It will validate by connecting to the target machine with the specified username and password and check if it has admin access.
2. .Net Framework: It will check if .Net framework 4.5+ is installed and will display the current .Net framework version.
3. Powershell version: It will check if Powershell is installed and will display the current Powershell version
4. CertUtil: It will check if certutil component is available. This is used to get the CA name and the corresponding templates.
5. CertAdm.dll: This is the native component used to access the CA and will check if this component is available in the C:WindowsSystem32 folder. Sometimes, while trying to access this component during the verification it will return an error and hence, a manual check must be performed.
6. netsh.exe: This is used to bind the certificate to the installed agent port (8999).
7. RPC service: The remote procedure call service must be running to perform all the remote operations and it will validate if the service is installed and running on the target machine.
8. WinRM service: Windows Remote Management service is required for the Powershell execution and it will validate if the service is installed and running on the target machine.
9. WMI service: Windows Management Instrumentation service is required for WMI and Powershell execution and it will validate if the service is installed and running on the target machine.
10. IIS: It will check if the IIS server is installed and identify the current IIS version.

Color Codes during the Execution

- **Black:** Success information and output
- **Red:** An error or warning, must take corrective action based on the prerequisite document in case of any issues
- **Blue:** Completion of the validation process
- **Green:** Complete process is successful



Export Log to File: This is used for exporting the validation summary into a log file.

Steps to test gateway installation:

To test the installation, go to the following URL:

<https://localhost:8999/appviewx/>

<https://<IP/Hostname>:<Port>/appviewx/rest/help> (Needs the certificate to be on the store/ browser)

For example, <https://xx.xx.xx.xx:8999/appviewx/rest/help>

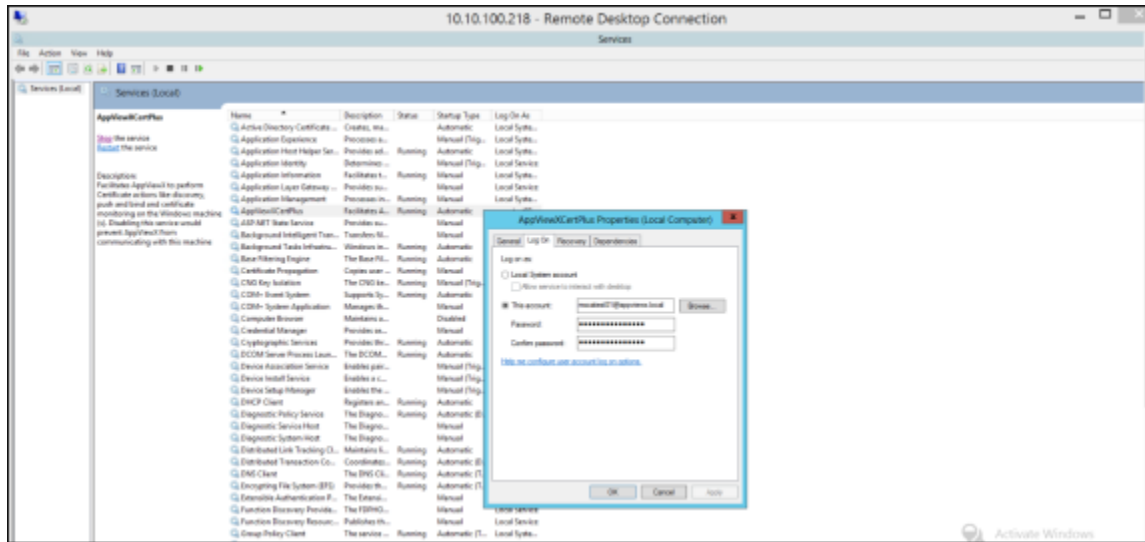
Operations at https://10.10.100.218:8999/appviewx/rest		
This page describes the service operations at this endpoint.		
URL	Method	Description
ReadCertificateTolite	POST	Service at https://10.10.100.218:8999/appviewx/rest/ReadCertificateTolite
ReadPushCertificates	POST	Service at https://10.10.100.218:8999/appviewx/rest/ReadPushCertificates
CreateAndSubmitRequest	POST	Service at https://10.10.100.218:8999/appviewx/rest/CreateAndSubmitRequest
DiscoverCertificates	GET	Service at https://10.10.100.218:8999/appviewx/rest/DiscoverCertificates?SourceName={SOURCE_NAME}&Mode={MODE}&IncludeBinaryData={INCLUDE_BINARY_DATA}&Start={START}&Limit={LIMIT}&FilterColumn={FILTER_COLUMN}&FilterCondition={FILTER_CONDITION}&FilterValue={FILTER_VALUE}
ExecuteCommand	POST	Service at https://10.10.100.218:8999/appviewx/rest/ExecuteCommand
ExecuteScriptInPowerShell	POST	Service at https://10.10.100.218:8999/appviewx/rest/ExecuteScriptInPowerShell
ExportCertificate	GET	Service at https://10.10.100.218:8999/appviewx/rest/ExportCertificate?RequestID={REQUEST_ID}&CACongigURL={CACONFIGURL}&ExportDateofWebServiceURL={EXPORTMENTWEBSEVERURL}&UseHttps={USEHTTPS}
FTPHead	POST	Service at https://10.10.100.218:8999/appviewx/rest/FTPHead
FTPWrite	POST	Service at https://10.10.100.218:8999/appviewx/rest/FTPWrite
GetConfig	GET	Service at https://10.10.100.218:8999/appviewx/rest/GetConfig
GetSites	GET	Service at https://10.10.100.218:8999/appviewx/rest/GetSites?TargetMachineName={TARGETMACHINE_NAME}
GetWebsiteInfo	GET	Service at https://10.10.100.218:8999/appviewx/rest/GetWebsiteInfo?TargetMachineName={TARGETMACHINE_NAME}&WebsiteName={WEBSITE_NAME}
PushAndReadCertificate	POST	Service at https://10.10.100.218:8999/appviewx/rest/PushAndReadCertificate
PushCertificate	POST	Service at https://10.10.100.218:8999/appviewx/rest/PushCertificate
PushMultipleCertificates	POST	Service at https://10.10.100.218:8999/appviewx/rest/PushMultipleCertificates
ReadFile	POST	Service at https://10.10.100.218:8999/appviewx/rest/ReadFile
ReadMultipleFiles	POST	Service at https://10.10.100.218:8999/appviewx/rest/ReadMultipleFiles
RevokeCertificate	POST	Service at https://10.10.100.218:8999/appviewx/rest/RevokeCertificate
Validation	POST	Service at https://10.10.100.218:8999/appviewx/rest/Validation
WriteFile	POST	Service at https://10.10.100.218:8999/appviewx/rest/WriteFile

- The above page confirms the accessibility and installation of the service.
- In case, a different client authentication certificate is being used, ensure that the CRL mentioned in the certificate is reachable from the AppViewX Windows gateway hosting server.
- Go to **AppViewX>> Settings>> Certificate** to register the gateway with AppViewX.
- Register the gateway with the URL format as follows: `https://<IP/Hostname>:<Port>/appviewx`

For example, <https://xx.xx.xx.xx:8999/appviewx>

Modify Agent services with the service Account The Windows gateway agent can be installed using a service account or an admin account.

- If the customer has a policy that states that the service account cannot be part of the administrator group or that the service account is only a part of the user group, then:
 - The gateway agent service is installed using an admin account.
 - The installed agent service is updated with the service account details in services.msc. Add the account in the properties of the AppViewXCert Plus service.
 - Services.msc -> AppViewXCert Plus -> Right click (Properties) -> LogOn .> Update the user account in the format of username@domainname.
 - Refer to the following image.



- In this case, the following command has to be executed from the PowerShell:

Netsh http add urlacl url=https://+:8999/appviewx/user=appviewx.localmstest01

- In the above command, the value for user = <domainserviceaccount> and the URL must be changed respectively.
- Once this is done, stop and start the AppViewXCertPlus Service in services.msc.

Windows Gateway Errors and Solutions

Error	Solution
767cf2b6-bfc3-45a0-9490-a95cf841e693: Connecting to remote server <machine name> failed with the following error message : WinRM cannot process the request. The following error occurred while using Kerberos authentication: The computer <name> is unknown to Kerberos. Verify that the computer exists on the network, that the name provided	• This issue occurs with Powershell remoting as it uses Kerberos authentication. • In the agent machine, start the command prompt as an administrator and execute the command <code>setspn -s http/machinename domainusername</code>. • This will work in the environments where Kerberos authentication and an AD domain are set up. • If no kerberos authentication is set up, then the communication must be done through WMI.

Error	Solution
is spelled correctly, and that the Kerberos configuration for accessing the computer is correct. The most common Kerberos configuration issue is that an SPN with the format HTTP/<machine name> is not configured for the target. If Kerberos is not required, specify the Negotiate authentication mechanism and resubmit the operation. For more information, see the about_Remote_Troubleshooting Help topic.	
Retrieving the COM class factory for remote component with CLSID	• The component used for accessing CA (certadm.dll) is not installed or has permission issues. • Check if the DLL is available in C:\Windows\System32 folder or else, install Microsoft Remote Server Administration Tools (RSAT) for the respective OS. For example, for Windows 10 https://www.microsoft.com/en-in/download/details.aspx?id=45520.
PowerShell ScriptExecution Error: Access is denied. 0x80070005 (WIN32: 5) OR Error Code 0x80070005 - Access is denied	• The username must be configured as "Username@Domain". • The user must have admin access to the remote/target machine or must be part of the local administrator group. • Go to the Local Users and Groups and access "Administrators". Check if the configured username is a part of the administrator group.
Connecting to remote server <machine name> failed with the following error message: WinRM cannot process the request. The following error with error code 0x80090322 occurred while using	• This issue occurs with Powershell remoting as it uses Kerberos authentication. • In the agent machine, start the command prompt as an administrator and execute the command <code>setspn -s http/machinename domainusername</code>.

Error	Solution
Negotiate authentication: An unknown security error occurred.	• This will work in the environments where Kerberos authentication and an AD domain are set up. • If no kerberos authentication is set up, then the communication must be done through WMI.
The WinRM client received an HTTP status code of 502 from the remote WS-Management service. For more information, see the about_Remote_Troubleshooting Help topic	• Check if the WinRM service is running. • Go to the Powershell on the target machine and run the command <code>WinRM QuickConfig</code>. • Execute the command <code>Enable-PSRemoting -force</code>. • Execute the command <code>netsh winhttp show proxy</code> and if a proxy is configured, it must be reset using the command <code>netsh winhttp reset proxy</code>.
41783361-015b-453f-b321-e31709b1850c: Connecting to remote server <machine name> failed with the following error message : Access is denied. For more information, see the about_Remote_Troubleshooting Help topic.	• The username must be configured as "Username@Domain". • The user must have admin access to the remote/target machine or must be a part of the local administrator group. • Go to the Local Users and Groups and access "Administrators" and check if the configured username is part of the administrator group. • Check if the WinRM service is running. • Go to Powershell on the target machine and execute the command <code>WinRM QuickConfig</code>. • Execute the command <code>Enable-PSRemoting -force</code>.
The client cannot connect to the destination specified in the request. Verify that the service on the destination is running and is accepting requests. Consult the logs and documentation for the WS-Management service running on the destination, most commonly IIS or WinRM. If the destination is the WinRM service, run the following command on the destination to analyze and configure the WinRM service: "winrm quickconfig"	• Check if the WinRM service is running. • Go to Powershell on the target machine and execute the command <code>WinRM QuickConfig</code>. • Execute the command <code>Enable-PSRemoting -force</code>.

Error	Solution
d4f98a6a-41ef-4864-9848-03a07e113d75: CCertRequest::Submit: The RPC server is unavailable. 0x800706ba (WIN32: 1722 RPC_S_SERVER_UNAVAILABLE)	Go to the target machine and start the RPC service if it is stopped.
727838ed-151e-46bf-883c-07ccb3a3989f: Connecting to remote server <machine name> failed with the following error message : The user name or password is incorrect. For more information, see the about_Remote_Troubleshooting Help topic.	• The username must be configured as "Username@Domain". • The user must have admin access to the remote/target machine or must be a part of the local administrator group. • Go to the Local Users and Groups and access "Administrators" and check if the configured username is part of the administrator group. • Check if the WinRM service is running. • Go to Powershell on the target machine and execute the command <code>WinRM QuickConfig</code>. • Execute the command <code>Enable-PSRemoting -force</code>.
fd3812f9-030a-421c-81e7-0e0510ce49e0: Access to the path '\\<machine name>\C\$\Windows\Temp\lqgwwkqi3.fff' is denied.	• The username must be configured as "Username@Domain". • The user must have admin access to the remote/target machine or must be part of the local administrator group. • Go to the Local Users and Groups and access "Administrators". Check if the configured username is a part of the administrator group.
More than 5 connections are not allowed	• Run Powershell as an administrator. • Check existing config <code>winrm get winrm/config</code>. • Change the settings to increase the maxshellsperUser to 100 on the remote machine where this issue is concurring. • <code>winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}'</code> • <code>winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}'</code> • <code>winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'</code>
Connecting to remote server failed with the following error message: The WS-Management service cannot process the	• Run Powershell as an administrator. • Check existing config <code>winrm get winrm/config</code>. • Change the settings to increase the maxshellsperUser to 100 on the remote machine where this issue is concurring.

Error	Solution
request. This user is allowed a maximum number of 4 concurrent shells, which has been exceeded. Close existing shells or raise the quota for this user.	• winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}' • winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}' • winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'
Client Certificate gives Permission Denied 403 errors. This can happen in a certain environment and it's intermittent	• Check if the client certificate is installed correctly by validating the chain in the Personal Store. • The root of the client certificate must be available in the Trusted Root Certification Store of the server. • The intermediate of the client certificate must be available in the Intermediate Certification authorities of the server. • If all of the above are fine, go to the agent server and complete the following steps: 1. MMC 2. Add/Remove SnapIn 3. Select certificate 4. Select LocalMachine 5. Go to Personal Store and click on client certificate 6. Go to chain 7. Export the root certificate and save as Root.cer in a location 8. Import the Root.cer into trusted root back again 9. If this does not solve the issue, then check if the trusted root contains and non- root certificates 10. Click on "Trusted Root" store and check if there any certificate which has IssuedTo and IssuedBy different 11. Take a backup of such certificates and move it to respective stores 12. If it does not solve the issue, then add the root certificate to the "Client Certificate Issuers"
The permission on the certificate template do not allow the current user to enroll for this type of certificate	1. Go to the CA server. 2. Open Certificate Authority and select the CA Server. 3. Right-click on properties and select the Security tab. 4. Check if the user used in Agent has the necessary permissions to read, issue, manage, and request certificate(s).

Error	Solution
	5. If the user is a part of a group, then ensure that the group has the required permissions. 6. Click on the Certificate Templates and right-click to manage the template. 7. Right-click on the template which has the issue and navigates to security. 8. Add permission to the user or group.
An attempt was made to open a Certification Authority database session, but there are already too many active sessions" on a request using CERTADMINLib.IenumCERTVIEWROW.Next().	In the CA server, navigate to the registry through the regedit command and set the following: 1. HKLMSYSTEMCurrentControlSetServicesCertSvc ConfigurationDBSessionCount to 64 hex (100 Dec) 2. HKLMSYSTEMCurrentControlSetServicesCertSvc ConfigurationDBMaxReadSessionCount is also set to 64 hex (100 Dec)
803f4314-3a11-486a-87e5-367b8c5c6f9f: The user name or password is incorrect.rn	• The username must be configured as "Username@Domain". • The user must have admin access to the remote/target machine or must be part of the local administrator group. • Go to the Local Users and Groups and access "Administrators". Check if the configured username is a part of the administrator group.
42abe1ef-2bff-40e8-82e2-c97c5707a0c1: Connecting to remote server <machine name> failed with the following error message : The user name or password is incorrect. For more information, see the about_Remote_Troubleshooting Help topic.	The user name or password is incorrect.
Connecting to remote server <machine name> failed with the following error message: WinRM cannot complete the operation. Verify that the	• WinRM service is already running on the following location of the machine: C:Windowssystem32>WinRM quickconfig • If WinRM is not set up to allow remote access to this machine for management, the following changes must be made:

Error	Solution
specified computer name is valid, that the computer is accessible over the network, and that a firewall exception for the WinRM service is enabled and allows access from this computer. By default, the WinRM firewall exception for public profiles limits accesses to remote computers within the same local subnet. For more information, see the about_Remote_Troubleshooting Help topic.	• Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine. • Make these changes [y/n]? y
There is not enough space on the disk	Ensure that your hard disk has enough free space.
Management Connect to remote machine <machine name> as user failed with the following error User credentials cannot be used for local connections	• The username must be configured as "Username@Domain". • The user must have admin access to the remote/target machine or must be part of the local administrator group. • Go to the Local Users and Groups and access "Administrators". Check if the configured username is a part of the administrator group. • Configure the credentials in AppViewX.CertPlus.Service Logon option.
Denied by Policy Module 0x80094800, The request was for a certificate template that is not supported by the Active Directory Certificate Services policy: WebServer1.	Use template name instead of the template display name.
Device Communication failed while using Native option to connect to CA remotely	1. Go to the agent machine. 2. Open <code>services.msc</code> using Start > Run command on the Windows machine. 3. Find the service "AppViewXCertPlus". 4. Right-click and view properties.

Error	Solution
	- Click on the "log on" tab. - Change the option to this account and enter the user account and password information. - Click on "Apply" and a message will pop up to add the account as "Log on as service". Click "OK" and save changes. - Click on restart the service. - Remove the username and password from AppViewX.
Certificate Request (CSR) is using a different account to request a certificate from CA as compared to account configured in AppViewX	- Go to the agent machine. - Open <code>services.msc</code> using Start > Run command on the Windows machine. - Find the service "AppViewXCertPlus". - Right-click and view properties. - Click on the "log on" tab. - Change the option to this account and enter the user account and password information. - Click on "Apply" and a message will pop up to add the account as "Log on as service". Click "OK" and save changes. - Click on restart the service. - Remove the username and password from AppViewX.

Chapter 2: Troubleshooting General

- [Overview](#)

Overview

This section of the guide will help you address the general issues faced during various processes related to Certificates like Group, Policy, Reports, and workflow. If the problem still remains unresolved please send a request to Technical Support by opening a case with the AppViewX Technical Services team. You can open a case from helpcenter.appviewx.com or send an email to help@appviewx.com.

- [Troubleshooting Certificate Group](#)
- [Troubleshooting Certificate Policy](#)
- [Troubleshooting Certificate Reports Configuration](#)
- [Troubleshooting Configuration of Workflow](#)

Troubleshooting Certificate Group

- [Overview of Certificate Group Troubleshooting](#)
- [Issues in Certificate Group](#)

Overview of Certificate Group Troubleshooting

This section guides you in troubleshooting problems that you might encounter while dealing with Certificate Group like creating or updating, deleting, assigning/ unassigning certificates to a group.

Issues in Certificate Group

- [Issues in Group create/update](#)
- [Issues in group delete](#)
- [Issues in assign/unassign certificate to a group](#)

Issues in Group create/update

Error Message	Possible Cause	Possible Solution
Given parent group is not present in AppViewX.	The parent group provided by the user does not exist in AppViewX.	Check if the group exists in the given parent group name.
Group already exists with the given name	Another group with the same name already exists.	Group name should be unique.
Missing user information.	User information is not available in the request.	Provide valid user information in the request.
Permission restricted to this group to edit/delete.	Given group has only read permission.	Change the group permission as RW to update the group.
Parent name and group name should not be same. Kindly change the parent name.	Parent group name and group name are the same in the given request.	Change the group name in the request.
You don't have access to this group.	Users do not have permission for a given group.	Change the group permission as RW to update the group.
Failed to update certificate group.	AppViewX is not able to update the group details.	DB may not be accessible during that time.
Given child group is not present in AppViewX.	The Child group provided by the user is not available in AppViewX.	Check if the group is available in the given child group name.
Certificate policy updation failed while updating certificate group.	AppViewX is not able to update the group details in policy.	DB may not be accessible during that time.

Issues in group delete

Error Message	Possible Cause	Possible Solution
Default group cannot be deleted.	The user is trying to delete the default group provided by AppViewX.	AppViewX allows users to delete only user-defined groups.

Error Message	Possible Cause	Possible Solution
Permission restricted to this group to edit/delete.	Given group has only read permission.	Change the group permission as RW to update the group.
Given parent group is not present in AppViewX.	The parent group provided by the user is not available in AppViewX.	Check if the group is available in the given parent group name.
You don't have access to this group.	Users do not have permission for a given group.	Change the group permission as RW to update the group.
Given child group is not present in AppViewX.	The child group provided by the user is not available in AppViewX.	Check if the group is available in the given child group name.
Failed to delete certificate groups since it is not available. Those groups are <GroupNames>	Given groups are not available in AppViewX.	Check and provide a valid group name to delete.

Issues in assign/unassign certificate to a group

Error Message	Possible Cause	Possible Solution
You don't have access to this group.	Users do not have permission for a given group.	Change the group permission as RW to update the group.
The operation cannot be completed as <count> selected certificate(s) are in Read-Only access groups	Some of the selected certificates are in groups that have "read-only" permission for the user.	Remove the certificates that have "read-only" permission or Change the group permissions to "RW".
Group name cannot be empty.	Group is given as empty in the request.	Groupname should not be empty. Give a valid group name.
Certificate uuid either empty/invalid.	Certificate UUID is not given in the request.	Provide a valid certificate UUIDs to perform the action.

Troubleshooting Certificate Policy

- [Overview](#)
- [Issues in Certificate Policy](#)

Overview

This section of the guide will help you troubleshoot the common problems that you might encounter while dealing with Certificate Policy actions like creating or updating or deleting.

Issues in Certificate Policy

- [Issues in policy create/update](#)
- [Issues in policy delete](#)

Issues in policy create/update

Error Message	Possible Cause	Possible Solution
[group] Groups are already assigned to another policy or doesn't exist	The group may be associated with some other policy. Group may not be available in AppViewX.	Check if the group is associated with some other policy. Check if the group is available in AppViewX.
At least one ECDSA curve should be selected for each EC bitlength	ECDSA curve details are not provided in the request.	It is mandatory to give at least one ECDSA curve for each EC bit length.
Failed to fetch the policy.	AppViewX is not able to fetch policy details from DB.	DB may not be accessible during that time. Please retry the operation.
Policy already exists with the given name.	Policy name already exists in the inventory.	Policy names should be unique.
Failed to update certificate policy information.	AppViewX is not able to update policy details from DB.	DB may not be accessible during that time. Please retry the operation.

Error Message	Possible Cause	Possible Solution
Given child group is not present in AppViewX.	The Child group provided by the user is not available in AppViewX.	Check if the group is available in the given child group name.
Certificate policy updation failed while updating certificate group.	AppViewX is not able to update the group details in policy.	DB may not be accessible during that time.

Issues in policy delete

Error Message	Possible Cause	Possible Solution
Default policy cannot be deleted.	The user is trying to delete the default policy provided by AppViewX.	AppViewX allows users to delete only user-defined policies.
Mandatory field is missing or invalid - policyNames	The field policyNames is not provided with any values in the request.	Check if the policyNames field is available and has values in the request.
Failed to delete certificate policy information.	AppViewX is not able to delete the policy.	DB may not be accessible during that time. Please retry the operation.

Troubleshooting Certificate Reports Configuration

- [Overview](#)
- [Issues in Configuring Reports](#)

Overview

This section of the guide helps you troubleshoot the common problems that you might encounter while configuring various certificate reports like validation status reports, summary reports, count by issuer reports.

Issues in Configuring Reports

- [Issues in configuring Validation Status Report](#)
- [Issues in configuring Certificate Summary Report](#)
- [Issues in configuring Count by Issuer Report](#)

Issues in configuring Validation Status Report

Error Message	Possible Cause	Possible Solution
FQDN cannot be null or empty.	The FQDN value provided is either null or empty.	Provide a valid FQDN value.
Certificate network discovery plugin may not be enabled. Contact AppViewX support team.	The plugin <code>avx_vendor_cert_network_discovery</code> is not enabled.	Enable <code>avx_vendor_cert_network_discovery</code> plugin.
Certificate network discovery plugin may be in not running state.	The plugin <code>avx_vendor_cert_network_discovery</code> may be in the "Not Running" state.	Start <code>avx_vendor_cert_network_discovery</code> plugin and try again.
IP <ipPort> is invalid	Given IP port is not valid.	Check and provide a valid IP port.
Invalid FQDN.	AppViewX is not able to access the given FQDN.	Check if the FQDN is valid and whether AppViewX has access to the FQDN.
Missing user information.	User information is not available in the request.	Provide a valid session-id or username and password in the request.

Issues in configuring Certificate Summary Report

Error Message	Possible Cause	Possible Solution
Cert report settings name already exists, Please verify.	The report settings name provided is already taken.	Report settings name should be unique.
Unable to schedule report generation, skipping to add/update the settings.	AppViewX is not able to add/update the scheduler job in crontab.	1. Provide valid cron settings.

Error Message	Possible Cause	Possible Solution
		2. DB may not be reachable, try after some time.

Issues in configuring Count by Issuer Report

Error Message	Possible Cause	Possible Solution
Cert report settings name already exists, Please verify.	The report settings name provided is already taken.	Report settings name should be unique.
Unable to schedule report generation, skipping to add/update the settings.	AppViewX is not able to add/update the scheduler job in crontab.	1. Provide a valid cron setting. 2. DB may not be reachable, try after some time.

Troubleshooting Configuration of Workflow

- [Overview](#)
- [Issues in configuring workflow](#)

Overview

This section of the guide helps you troubleshoot the problems encountered while configuring workflow.

Issues in configuring workflow

Error Message	Possible Cause	Possible Solution
Csr submission failed. User is not authorized.	No permission for the workflow related to that action.	Check if the user has permission for the action workflow in Accounts>Resources.
Certificate <action>failed. User is not authorized.	No permission for the workflow related to that action.	Check if the user has permission for the action workflow in Accounts>Resources.

Chapter 3: Troubleshooting Protocols

- [Overview](#)

Overview

This section of the guide helps you to troubleshoot the various issues encountered by you while using different protocol functionalities. The different protocols covered are ACME, EST, MsIntune SCEP, and SCEP. If the problem still remains unresolved please send a request to Technical Support by opening a case with the AppViewX Technical Services team. You can open a case from helpcenter.appviewx.com or send an email to help@appviewx.com.

- [Troubleshooting Auto-Enrolment ACME](#)
- [Troubleshooting Auto-Enrolment EST](#)
- [Troubleshooting Auto-enrolment of MsIntune SCEP](#)
- [Troubleshooting Auto-enrolment of SCEP](#)

Troubleshooting Auto-Enrolment ACME

- [Overview](#)
- [Supported Web Browsers](#)
- [Supported ACME Client](#)
- [Issues in ACME](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using ACME functionalities like setting addition, checking communication, enrollment, and revocation.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0

Browser	Version	Notes
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Supported ACME Client

- Certbot
- Cert manager

Issues in ACME

- [Issues in ACME setting addition and check the settings](#)
- [Issues in Auto Enrolling Certificate via ACME](#)

Issues in ACME setting addition and check the settings

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration**, select **Auto Enrollment**.
4. Click **ACME**.
The **Auto Enrollment ACME** page is displayed.
5. Click **Add**.
6. After settings are added, click **Check** to see the validity.

• [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Agent name already added. Please enter a different name..	An ACME setting with the same name already exists in ACME Page.	Check the ACME Setting name, it should be unique.
1) This field should not be null or empty 2) Mandatory Field(s) - <Field name> is/are empty	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.
ACME setting is invalid - Agent ip is not reachable	The ACME agent IP and port provided might not be accessible from the AppViewX node.	Please check the IP port provided so that it can be pingable from the AppViewX node.
ACME setting is invalid - Policy is not associated to the provided group	The policy selected might be associated with some other group that is not selected.	Please check whether the selected policy and group are associated with one another.

Issues in Auto Enrolling Certificate via ACME



Note: From the client machine hit the auto-enroll call using AppViewX ACME server URL which is displayed on the ACME setting page.

Error Message	Possible Cause	Possible Solution
No agent settings found for the provided agent ip address (OR) Agent settings is not found	The provided agent IP or agent name is not found in the ACME settings.	Check for the agent IP and agent name in the client machine.

Error Message	Possible Cause	Possible Solution
Unable to perform ACME account creation/updation operation	ACME is already present or the account is not proper in the client machine.	1. Check whether the account is proper in the client machine. 2. Delete the acme accounts in the client machine and retry.
Unable to perform ACME challenge creation operation	Challenge verification failed before enrolling the certificate.	1. Check for the option selected in the ACME setting if it's HTTP or DNS. 2. Check for the reachability of URL for HTTP challenge verification.
HTTP authentication failed due to invalid parameters provided.	The HTTP authentication parameters provided must be invalid	1. Check for passwords in BASIC authentication. 2. Check for the nonce and other parameters in DIGACME parameters.
Unable to perform ACME order finalize operation	This phase is used to obtain the CSR and submit it.	1. Check for the input CSR in the request. 2. Check whether the CSR submission is successful in AppViewX.
Unable to obtain the enrolled certificate	The certificate might not be present for the provided transaction id.	Check if the certificate is enrolled or not in AppViewX inventory.
Unable to establish connection with ACME server.	There might be an issue with reaching the AppViewX ACME agent IP from the client.	Check whether the ACME agent IP is reachable from the client machine. Check whether the ACME agent IP is open and can be accessible.
Group policy does not have the given hash function	The requACMEed hash function in the CSR parameters may not be available in the selected policy.	1. Navigate to the policy page. 2. Select the CA used in the ACME setting. 3. In the hash function field include the "requACMEed" and missing hash functions. 4. Save the CA details and update the policy.

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority	Failure due to specific CA functionality.	Check in the logs and failed Work order for the reason of submission failure.
Unable to submit the CSR request to certificate authority - For MSCA	There might be an error in work order log - “Denied due to policy module”	Check for the bit length in the CSR parameters, if it's lesser than or equal to 1024 then increase that in the CSR.
CSR parameters already exists	There might be another CSR already present in the inventory for which certificates would not have been issued.	1. Delete the previous CSR present in inventory and try enrolling. 2. Connect database and update the entry as below: <pre>db.cert_metadata.update({"_id" : "DO_CSR_PARAMS_UNIQUENESS_CHECK"}, {"\$set":{"constant":"no"}})</pre>  Note: This would allow multiple CSR's with the same parameters in the certificate inventory.

Troubleshooting Auto-Enrolment EST

- [Overview](#)
- [Supported Web Browsers](#)
- [Supported EST Client](#)
- [Issues in EST](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using EST functionalities of CA like setting addition, enrollment, obtaining, and re-enrollment.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Supported EST Client

- Cisco Routers
- Libest client

Issues in EST

- [Issues in EST setting addition and check the settings](#)
- [Issues in auto-enrolling certificate via EST](#)
- [Issues in obtaining CA certificate via EST](#)
- [Issues in auto re-enrolling certificate via EST](#)

Issues in EST setting addition and check the settings

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.

The **Server Certificate** page is displayed.

3. From the left pane, expand **Administration**, select **Auto Enrollment**.

4. Click **EST**.

The **Auto Enrollment EST** page is displayed.

5. Click **Add**.

6. After settings are added, click **Check** to see the validity.

• [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Agent name already added. Please enter a different name..	An EST setting with the same name already exists on EST Page.	Check the EST Setting name, it should be unique.
1) This field should not be null or empty 2) Mandatory Field(s) - <Field name> is/are empty	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.
EST setting is invalid - Agent ip is not reachable	The EST agent IP and port provided might not be accessible from the AppViewX node.	Please check the IP port provided so that it can be pingable from the AppViewX node.
EST setting is invalid - Certificate does not belong to the selected CA.	The issuer certificate provided does not belong to the CA which is selected.	Please check whether the selected issuer certificate belongs to the CA which was selected earlier.

Issues in auto-enrolling certificate via EST



Note: From the client machine hit the auto-enroll call using AppViewX EST server URL which is displayed on the EST setting page.

Error Message	Possible Cause	Possible Solution
No agent settings found for the provided agent ip address (OR) Agent settings is not found	The provided agent IP or agent name is not found in the EST settings.	Check for the agent IP and agent name in the client machine.
Client certificate authentication failed since no client certificate content is obtained	The client certificate is not set in the enroll request from the client machine	1. Check whether the client certificate and key are set in the enroll certificate request. 2. If the provided certificate is pfx or pkcs12 certificate check whether the provided password is correct.
Provided client certificate is not valid.	The provided client certificate might be Expired or Revoked.	Provide a Valid certificate in the enrollment request.
HTTP authentication failed due to invalid parameters provided.	The HTTP authentication parameters provided must be invalid.	1. Check for password in BASIC authentication. 2. Check for nonce and other parameters in DIGEST parameters.
CA certificate is not found	The issuer certificate of the selected "server certificate" might have been deleted or the server certificate has been deleted.	Check for the issuer certificate and its issuer certificate available in the inventory.
Unable to establish connection with EST server.	There might be an issue with reaching the AppViewX EST agent IP from the client.	Check whether the EST agent IP is reachable from the client machine. Check whether the EST agent IP is open and can be accessible.
Group policy does not have the given hash function	The requested hash function in the CSR parameters may not be available in the selected policy.	1. Navigate to the policy page. 2. Select the CA used in the EST setting. 3. In the hash function field include the requested and missing hash functions. 4. Save the CA details and update the policy.

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority	Failure due to specific CA functionality.	Check in the logs and failed Work order for the reason of submission failure.
Unable to submit the CSR request to certificate authority - For MSCA	There might be an error in the work order log - "Denied due to policy module".	Check for the bit length in the CSR parameters, if it is lesser than or equal to 1024 then increase that in the CSR.
CSR parameters already exists	There might be another CSR already present in the inventory for which certificates would not have been issued.	1. Delete the previous CSR present in inventory and try enrolling again. 2. Connect database and update the entry as given below: <pre>db.cert_metadata.update({"_id" : "DO_CSR_PARAMS_UNIQUENESS_CHECK"}, {"\$set":{"constant":"no"}})</pre>  Note: This would allow multiple CSR's with the same parameters in the certificate inventory.

Issues in obtaining CA certificate via EST



Note: From the client machine hit the get ca certificate call using AppViewX EST server URL which is displayed on the EST setting page.

Error Message	Possible Cause	Possible Solution
No agent settings found for the provided agent ip address (OR) Agent settings is not found	The provided agent IP or agent name is not found in the EST settings.	Check for the agent IP and agent name in the client machine.

Error Message	Possible Cause	Possible Solution
Client certificate authentication failed since no client certificate content is obtained	The client certificate is not set in the get ca request from the client machine.	1. Check whether the client certificate and key are set in the "get ca certificate request". 2. If the provided certificate is pfx or pkcs12 certificate check whether the provided password is correct.
Provided client certificate is not valid.	The provided client certificate might be Expired or Revoked.	Provide a Valid certificate in the "get ca cert request".
HTTP authentication failed due to invalid parameters provided.	The HTTP authentication parameters provided must be invalid.	1. Check for password in BASIC authentication. 2. Check for nonce and other parameters in DIGEST parameters.
CA certificate is not found	The issuer certificate of the selected "server certificate" might have been deleted or the server certificate has been deleted.	Check for the issuer certificate and its issuer certificate available in the inventory.
Unable to establish connection with EST server.	There might be an issue with reaching the AppViewX EST agent IP from the client.	Check whether the EST agent IP is reachable from the client machine. Check whether the EST agent IP is open and can be accessible.

Issues in auto re-enrolling certificate via EST



Note: Note: From the client machine hit the auto re-enroll call using AppViewX EST server URL which is displayed on the EST setting page.

Error Message	Possible Cause	Possible Solution
No agent settings found for the provided agent ip address (OR) Agent settings is not found	The provided agent IP or agent name is not found in the EST settings.	Check for the agent IP and agent name in the client machine.
Client certificate authentication failed since no client certificate content is obtained	The client certificate is not set in the re-enroll request from the client machine	1. Check whether the client certificate and key is set in the re-enroll certificate request. 2. If the provided certificate is pfx or pkcs12 certificate check whether the provided password is correct.
Provided client certificate is not valid.	The provided client certificate might be Expired or Revoked.	Provide a Valid certificate in the re-enroll request.
HTTP authentication failed due to invalid parameters provided.	The HTTP authentication parameters provided must be invalid.	1. Check for password in BASIC authentication. 2. Check for nonce and other parameters in DIGEST parameters.
CA certificate is not found	The issuer certificate of the selected "server certificate" might have been deleted or the server certificate has been deleted.	Check for the issuer certificate and its issuer certificate available in the inventory.
Unable to establish connection with EST server.	There might be an issue with reaching the AppViewX EST agent IP from the client.	Check whether the EST agent IP is reachable from the client machine. Check whether the EST agent IP is open and can be accessible.
Group policy does not have the given hash function	The requested hash function in the CSR parameters may not be available in the selected policy.	1. Navigate to the policy page. 2. Select the CA used in the EST setting. 3. In the hash function field include the requested and missing hash functions. 4. Save the CA details and update the policy.

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority	Failure due to specific CA functionality.	Check in logs and in failed Work order for the reason why submission got failed.
Unable to submit the CSR request to certificate authority - For MSCA	There might be an error in the work order log - "Denied due to policy module" .	Check for the bit length in the CSR parameters, if its lesser than or equal to 1024 then increase that in the CSR.
CSR parameters already exists	There might be another CSR already present in the inventory for which certificates would not have been issued.	1. Delete the previous CSR present in inventory and try enrolling. 2. Connect database and update the entry as mentioned below: <pre>"db.cert_metadata.update({"_id" : "DO_CSR_PARAMS_UNIQUENESS_CHECK"}, {"\$set":{"constant":"no"}})"</pre>  Note: This would allow multiple CSR's with the same parameters in the certificate inventory.
Enrolled Certificate is not found	While renewing the enrolled certificate, the enrolled certificate might not be present in certificate inventory.	1. Check if the enrolled cert is present in certificate inventory. 2. Check if the enrolled certificate provided in "renew request" is a valid one and is enrolled already in AppViewX. 3. If the enrolled certificate is not present in inventory, check if the authentication cert is in cert inventory.

Troubleshooting Auto-enrolment of MsIntune SCEP

- [Overview](#)
- [Issues in MSIntune SCEP](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using MSIntune SCEP functionalities like setting addition and certificate enrollment.

Issues in MSIntune SCEP

- [Issues in MSIntune SCEP setting addition and validating the settings](#)
- [Issues in auto enrolling certificate via MS Intune SCEP](#)

Issues in MSIntune SCEP setting addition and validating the settings

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration**, select **Auto Enrollment**.
4. Click **MsIntune**.
The **Auto Enrollment MsIntune** page is displayed.
5. Click **Add**.
6. After settings are added, click **Check** to see the validity.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Agent ip is not reachable	The MS Intune SCEP agent IP and specified port may not be reachable from the AppViewX node.	Validate and ensure that the agent IP/Port is reachable.
Certificate does not belong to the selected CA.	The server certificate provided in the agent setting does not belong to the CA which is selected.	Please check whether the selected server certificate belongs to the CA which was selected earlier.
CA setting connection is in Failed status	The connection status of the chosen CA setting chosen in the agent setting failed.	Check the specified CA setting and make necessary changes to make it valid.

Issues in auto enrolling certificate via MS Intune SCEP



Note:

1. From the client machine, enroll for the certificate using Company Portal application.
2. Newly enrolled certificate should be available in the AppViewX CERT+ Inventory. If the new certificate is not available in the AppViewX CERT+ Inventory, even after 5 minutes from triggering the request from the device, then logon to the CLI and verify the logs for avx_vendor_cert_intune_agent plugin.

Following errors may appear in the logs -

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority	Request might have failed due to a specific error from CA	Verify the vendor logs to see if there is any CA specific error.
CSR parameters already exists	There might be another CSR already present in the inventory for which certificates would not have been issued.	1. Delete the previous CSR present in inventory and try enrolling. 2. Connect database and update the entry given below: <pre>"db.cert_metadata.update({"_id" : "DO_CSR_PARAMS_UNIQUENESS_CHECK"},{\$set: {"constant":"no"}})"</pre> Note: This would allow multiple CSR's with the same parameters in the certificate inventory.
Challenge in PKCS#10 request (Transaction ID: <<transactionID>>) is not valid. Certificate enrollment will not be processed.	Challenge password validation with Microsoft Intune has failed. Possible reasons -	1. Validate the internet access in the AppViewX server. 2. Check and correct the Intune Client Id/Tenant Id/Client Secret configured in the MS Intune agent setting.

Error Message	Possible Cause	Possible Solution
	1. Connectivity issue with Microsoft Intune. 2. Intune credentials configured in agent settings might be incorrect.	
No error message but enrollment request does not get triggered after the getCACert call from the client device.	A mismatch between the CA certificate configured in the MS Intune Agent setting and that configured in the Intune portal.	Verify and ensure that the root and intermediate CA certificates of the Server certificate available in the AppViewX MS Intune agent setting match with the Root and Intermediate certificates configured in the MS Intune portal (Azure) SCEP profile.

Troubleshooting Auto-enrolment of SCEP

- [Overview](#)
- [Supported Web Browsers](#)
- [Supported SCEP Client](#)
- [Issues in SCEP](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using SCEP functionalities like setting addition, enrolment, and obtaining.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7,	From AppViewX Version 11.1

Browser	Version	Notes
	macOS - Version 13.1.2)	
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Supported SCEP Client

- SSCEP client
- Cisco Routers
- Mobileiron Cloud portal

Issues in SCEP

- [Issues in SCEP setting addition and check the settings](#)
- [Issues in Auto Enrolling certificate via SCEP](#)
- [Issues in Obtaining CA certificate via SCEP](#)

Issues in SCEP setting addition and check the settings

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration**, select **Auto Enrollment**.
4. Click **SCEP**.
The **Auto Enrollment SCEP** page is displayed.
5. Click **Add**.
6. After settings are added, click **Check** to see the validity.

• [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Agent name already added. Please enter a different name..	A SCEP setting with the same name already exists on SCEP Page.	Check the SCEP Setting name, it should be unique.
1) This field should not be null or empty 2) Mandatory Field(s) - <Field name> is/are empty	Some of the mandatory fields are missing or invalid.	Add all the valid information in the mandatory section.
SCEP setting is invalid - Agent ip is not reachable	The SCEP agent IP and port provided might not be accessible from the AppViewX node.	Please check the IP port provided so that it can be pingable from the AppViewX node.
SCEP setting is invalid - Certificate does not belong to the selected CA.	The server certificate provided does not belong to the CA which is selected.	Please check whether the selected server certificate belongs to the CA which was selected earlier.

Issues in Auto Enrolling certificate via SCEP



Note: From the client machine hit the auto-enroll call using AppViewX SCEP server URL which is displayed on the SCEP setting page.

Error Message	Possible Cause	Possible Solution
No agent settings found for the provided agent ip address (OR) Agent settings is not found	The provided agent IP or agent name is not found in the SCEP settings.	Check for the agent IP and agent name in the client machine.

Error Message	Possible Cause	Possible Solution
Unable to establish connection with SCEP server.	There might be an issue with reaching the AppViewX SCEP agent IP from the client.	Check whether the SCEP agent IP is reachable from the client machine. Check whether the SCEP agent IP is open and can be accessible.
Group policy does not have the given hash function	The requested hash function in the CSR parameters may not be available in the selected policy.	1. Navigate to the policy page. 2. Select the CA used in the SCEP setting. 3. In the hash function field include the requested and missing hash functions. 4. Save the CA details and update the policy.
Unable to submit the CSR request to certificate authority	Failure due to specific CA functionality.	Check the reason for submission failure in logs and failed Work order.
Unable to submit the CSR request to certificate authority - For MSCA	There might be an error in the work order log - "Denied due to policy module" .	Check for the bit length in the CSR parameters, if it's lesser than or equal to 1024 then increase it in the CSR.
CSR parameters already exists	There might be another CSR already present in the inventory for which certificates would not have been issued.	1. Delete the previous CSR present in inventory and try enrolling again. 2. Connect database and update the entry as mentioned below: <pre> "db.cert_metadata.update({"_id" : "DO_CSR_PARAMS_UNIQUENESS_CHECK"}, {"\$set":{"constant":"no"}})" </pre>  Note: This would allow multiple CSR's with the same parameters in the certificate inventory.

Issues in Obtaining CA certificate via SCEP

Chapter 4: Troubleshooting AWS, CLOUD

- [Overview](#)

Overview

This section of the guide will help you tackle the various issues that arise while using the functionalities of CLOUD services. If the problem still remains unresolved please send a request to Technical Support by opening a case with the AppViewX Technical Services team. You can open a case from helpcenter.AppViewX.com or send an email to help@AppViewX.com.

- [Troubleshooting of AWS - CLOUD \(ACM and IAM\)](#)
- [Troubleshooting AWS CLOUD CloudFront](#)
- [Troubleshooting AWS CLOUD ELB](#)
- [Troubleshooting Azure CLOUD](#)
- [Troubleshooting CLOUD - Common Functionality](#)

Troubleshooting of AWS - CLOUD (ACM and IAM)

- [Overview](#)
- [Supported Web Browsers](#)
- [Issues in ACM Service](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using AWS cloud functionalities for ACM & IAM service like server addition using AppViewX, fetch, certificate discovery & certificate push.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0

Browser	Version	Notes
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in ACM Service

- [Issues in Server Addition using AppViewX UI](#)
- [Issues in Fetch Regions](#)
- [Issues in Discovery in IAM & ACM](#)
- [Issues in Push and Rollback](#)

Issues in Server Addition using AppViewX UI

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Cloud** Tab.
5. From the icon list at the top right corner, click **Add**.
The **Device Addition** page is displayed.
6. From the **Device Details** section on the left, Click **AWS**.
7. Fill in the appropriate details.

Device - Cloud > Add

AWS

Azure

GCP

* Account name

Device description

* Account number

Credentials

* Credential type

* Access key

* Secret key

Key information

* Data center

* Services

* Service region

Provide credentials to fetch region(s)

Select the region(s)

Additional attributes

ACM IAM

Cert sync: ☒ Managed ☐ Monitored ☐ Ignored

appviewX

Mon Mar 08 2021 16:05:36 GMT+0530 (IST)

Device - Cloud

ADC WAF Server DNS Firewall Switch Router Proxy Cloud HSM Others MDM

Search...

Account name	Device description	Vendor	Status	Services
acmTest		AWS	Managed	ACM,IAM

1 to 1 of 1

Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Please provide valid credentials	Provided credential is invalid.	1. Provide valid Access Key. 2. Provide valid Secret Key.

Error Message	Possible Cause	Possible Solution
Provide valid account name	Account name can be duplicate or not as per standard.	1. Provide unique name for account name. 2. Account name can be alphanumeric and can also have period (.) in it.
Details Incorrect	Provide mandatory fields.	Enter mandatory fields like 1. Account Number 2. Access Key 3. Secret Key 4. Data Center 5. Services 6. Regions

Issues in Fetch Regions

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, select **AWS**.
5. Fill in **Access Key** and **Secret Key** in the **Credentials** section.
6. Click **Fetch Regions**.

Credentials

* Credential type

Manual Entry

* Access key

* Secret key

Key information

* Data center

absecon

* Services

Service region

Fetch regions

Provide credentials to fetch region(s)

Select the region(s)

• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Please provide valid credentials	The provided credential is invalid.	1. Provide valid Access Key. 2. Provide a valid Secret key.

Issues in Discovery in IAM & ACM

- Log in to **AppViewX** application with valid credentials.
- From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
- From the left pane, expand **Certificate Discovery** and select **Discovery**.
- Click **Cloud Scan**.
The **Discovery Cloud Scan Add Discovery page** will be displayed.



Note: To discover certificates from Managed devices, the device should be managed under the AppViewX Inventory.

Discovery : Cloud Scan : Add Discovery

Discover Details

* Discovery Run Type ☒ On-demand ☐ Schedule ⓘ

* Discovery Instance Name ⓘ

Description

Discover By

You can either manually enter template details or upload a file.

* Discovery From ⓘ

Cloud device ⓘ 2 [Select All](#)

- ☒ AWS:acmTest
- ☒ ACM
- ☒ IAM

Execute Batches Sequentially ☐ ⓘ

[Discover](#) [Reset](#)

• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	- Discovery name is not given or the length is less than 2 characters. - Interval between batches info. is missing when execution type is sequential.	- Enter a valid name with a minimum of 2 characters. - Provide a time interval between batches in minutes.
Please select a device	No device is selected in the Discover By section.	Select at least one device from which to discover certificates.

Issues in Push and Rollback

Add Connector

General Information

Category
Cloud

Vendor
AWS

Connector Name
AWS connector

Description

2000 remaining

SSL templates

Available devices
ACM

Search...

acmTest:Asia Pacific (Mumbai):ACM
acmTest:Asia Pacific (Seoul):ACM
acmTest:Asia Pacific (Singapore):ACM
acmTest:Asia Pacific (Sydney):ACM
acmTest:Asia Pacific (Tokyo):ACM
acmTest:EU (Frankfurt):ACM
acmTest:EU (Ireland):ACM
acmTest:EU (London):ACM
acmTest:EU (Paris):ACM
acmTest:EU (Stockholm):ACM

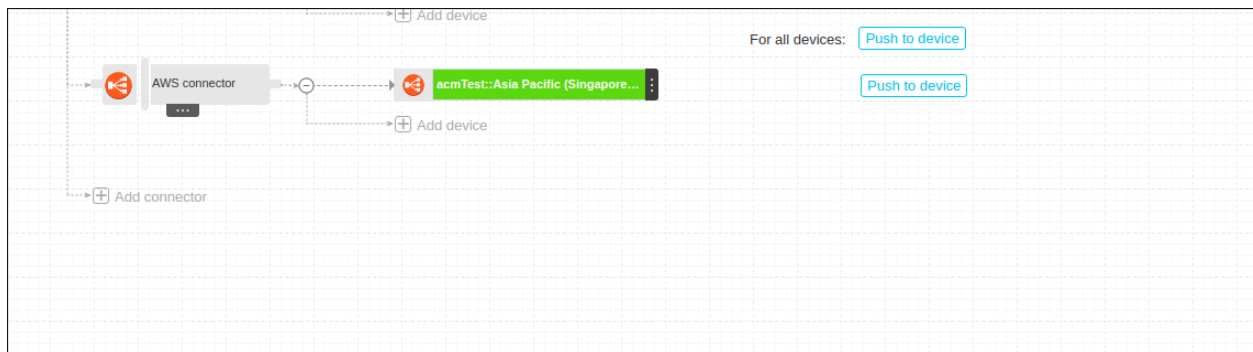
Total records: 15

Selected devices

Search...

acmTest:Canada (Central):ACM

Total records: 1



Error Message	Possible Cause	Possible Solution
Unable to initiate request.	- Pushing to device when certificate is unavailable, such as in a new state. - Previous work order is in progress and not completed. - AppConnector might not be in sync.	- Push to device after certificate has been retrieved from CA. - Initiate push after previous work order is finished. - Synchronize the AppConnector and retry.

Error Message	Possible Cause	Possible Solution
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e., in a new state.	Push to device after certificate has been retrieved from CA.
Provided certificate is not a valid self signed. Please provide either a valid self-signed certificate or certificate chain	Provided certificate is not a valid certificate.	Push a valid certificate.
Push failed as there exists another certificate with commonName	Certificate with same common name is present in certificate manager	Check whether it is a duplicate certificate and remove the invalid one.

Troubleshooting AWS CLOUD CloudFront

- [Overview](#)
- [Supported Web Browsers](#)
- [Issues in CloudFront Service](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using AWS cloud functionalities for CloudFront service. This guide will give more troubleshooting processes on certificate discovery & certificate push.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in CloudFront Service

- [Issues in Discovery in Cloudfront](#)
- [Issues in Push-Bind and Rollback](#)

Issues in Discovery in Cloudfront

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery** and select **Discovery**.
4. Click **Cloud Scan**.

The **Discovery Cloud Scan Add Discovery** page will be displayed.



Note: To discover certificates from Managed devices, the device should be managed under the AppViewX Inventory.

Discovery : Cloud Scan : Add Discovery

* Discovery Instance Name
cloudfront-discovery

Description
Description

Discover By

You can either manually enter template details or upload a file.

* Discovery From
Cloud

Cloud device
Search
1
Select All

☒ AWS::aws
☐ ACM
☐ IAM
☒ Cloudfront

Discover
Reset

Issues in Push-Bind and Rollback

Add Connector

Category

ADC

Vendor

AmazonELB

Connector Name

AmazonELB connector

Description

SSL templates

Available devices

Q Search...

aws_422350247734
aws_422350247734:US East (N. Virginia):acmdemo:HTTPS:443
aws_422350247734:US East (N. Virginia):acmdemo:HTTPS:8086
aws_422350247734:US West (Oregon):app-lb-001:HTTPS:443
aws_422350247734:Asia Pacific (Mumbai):trv-appviewx:HTTPS:443

Selected devices

Q Search...

No records found

Save

Cancel

For all devices: [Push to device](#)

[Rollback](#) or [Push to device](#)

[Add connector](#)

[Add device](#)

[R43](#)
Push - Completed

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	- Pushing to device when certificate is unavailable, i.e, in a new state. - Previous work order is in progress and not completed. - AppConnector might not be in sync.	- Push to device after certificate has been retrieved from CA. - Initiate push after previous work order is finished. - Synchronize the AppConnector and retry.

Copyright © 2022 AppViewX, Inc. All Rights Reserved.

219

Error Message	Possible Cause	Possible Solution
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private Key is required to push certificate to ACM inventory	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Provided certificate is not a valid self signed. Please provide either a valid self-signed certificate or certificate chain	Provided certificate is not a valid certificate.	Push a valid certificate.
Push failed as there exists another certificate with commonName	Certificate with the same common name is present in certificate manager	Check whether it is a duplicate certificate and remove the invalid one.
Cert Association failed with profile	Modify access may not be available on the selected resource	Provide "Modify" access for the resource and retry.

Error Message	Possible Cause	Possible Solution
Association failed with profile-<PROFILE_NAME>as no such profile available	Profile may not be available on the cloud account	Perform config fetch on the device from ADC module and retry association of cert.
Certificate cannot be pushed as selected Amazon CA certificate is in <SOURCE_REGION> region and region you tried is <DESTINATION_REGION>	Selected certificate is in ACM in a different region than the region to be pushed	Use certificates available in the <DESTINATION_REGION> (or) Push a new certificate to the <DESTINATION_REGION>

Troubleshooting AWS CLOUD ELB

- [Overview](#)
- [Supported Web Browsers](#)
- [Issues in ELB Service](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using AWS cloud functionalities for ELB service. This guide will give more troubleshooting processes on certificate discovery & certificate push.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher

Device	OS	Resolution
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in ELB Service

- [Issues in Discovery in ELB](#)
- [Issues in Push-Bind and Rollback](#)

Issues in Discovery in ELB

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery** and select **Discovery**.
4. Click **Cloud Scan**.

The **Discovery Cloud Scan Add Discovery** page will be displayed.



Note: To discover certificates from Managed devices, the device should be managed under the AppViewX Inventory.

Discovery : Managed Devices Scan : Add Discovery

* Discovery Run Type
☒ On-demand
☐ Schedule

* Discovery Instance Name

Description

Discover By

You can either manually enter template details or upload a file.

* Discovery From

☐ Select all

All
Selected
Unselected
Count: 1

☒ AmazonELB::aws_422350247734

Favorites

No records found

• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.

Issues in Push-Bind and Rollback

Add Connector

Category

ADC

Vendor

AmazonELB

Connector Name

AmazonELB connector

Description

SSL templates

Available devices

Search...

aws_422350247734

aws_422350247734:US East (N. Virginia):acmdemo:HTTPS:443

aws_422350247734:US East (N. Virginia):acmdemo:HTTPS:8086

aws_422350247734:US West (Oregon):app-lb-001:HTTPS:443

aws_422350247734:Asia Pacific (Mumbai):trv-appviewx:HTTPS:443

Selected devices

Search...

No records found

Save

Cancel

For all devices: [Push to device](#)

AmazonELB conn... → aws_422350247734:US East (N. V... **R43**
Push - Completed [Rollback](#) or [Push to device](#)

[Add connector](#) [Add device](#)

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	- Pushing to device when certificate is unavailable, i.e, in a new state. - Previous work order is in progress and not completed. - AppConnector might not be in sync.	- Push to device after certificate has been retrieved from CA. - Initiate push after previous work order is finished. - Synchronize the AppConnector and retry.

Copyright © 2022 AppViewX, Inc. All Rights Reserved.

224

Error Message	Possible Cause	Possible Solution
Unable to initiate request, template is in disabled state	Given workflow is not in an enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
1 validation error detected: Value at 'privateKey' failed to satisfy constraint.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because the push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to the device when certificate is unavailable, i.e, in a new state.	Push to the device after certificate has been retrieved from CA.
Provided certificate is not a valid self signed. Please provide either a valid self-signed certificate or certificate chain	The provided certificate is not a valid certificate.	Push a valid certificate.
Push failed as there exists another certificate with commonName	Certificate with the same common name is present in certificate manager	Check whether it is a duplicate certificate and remove the invalid one.
Cert Association failed with profile	Modify access may not be available on the selected resource	Provide Modify access for the resource and retry

Error Message	Possible Cause	Possible Solution
Association failed with profile-<PROFILE_NAME>as no such profile available	Profile may not be available on the cloud account	Perform config fetch on the device from ADC module and retry association of cert.

Troubleshooting Azure CLOUD

- [Overview](#)
- [Supported Web Browsers](#)
- [Issues in Azure Cloud](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using certificate functionalities. This guide will give more troubleshooting processes on cloud addition, deletion, push, bind, rollback, and other actions associated with Azure cloud.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

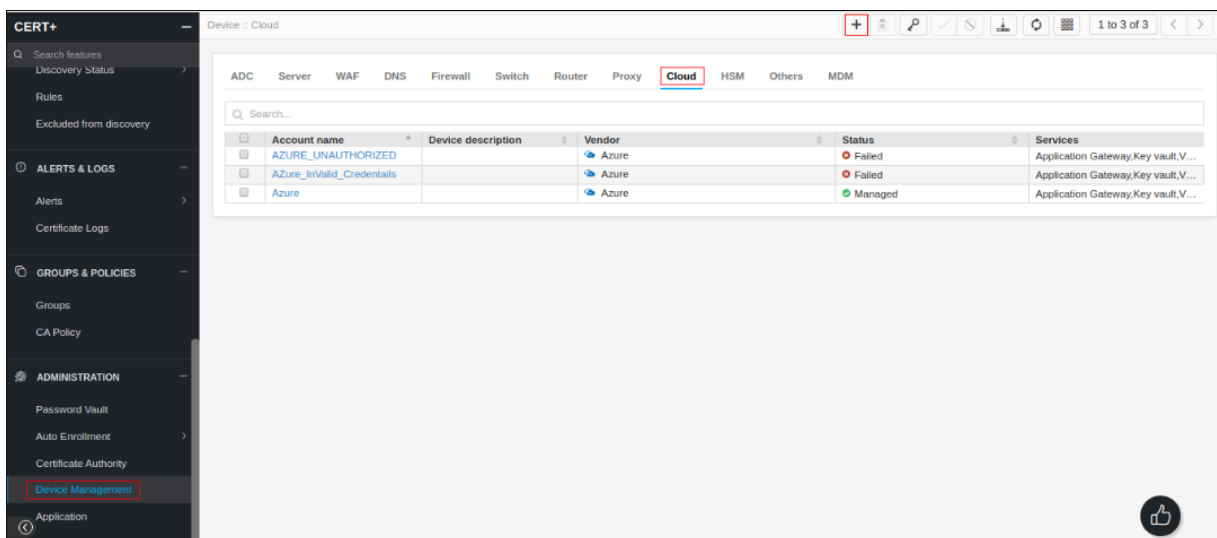
Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Azure Cloud

- Issues in Azure Cloud Addition using AppViewX UI
- Issues in Communicating to Azure Cloud
- Issues in Accessing Azure Cloud
- Issues in Managed Cloud
- Issues in Unmanaged Cloud
- Issues in Fetch Config
- Issues in Certificate Discovery
- Issues in Certificate Import

Issues in Azure Cloud Addition using AppViewX UI

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Cloud** Tab.
5. From the icon list at the top right corner, click **Add**.
The **Device Addition** page is displayed.
6. On the **Device Addition** page, select **Azure** from the **Vendors details section**.



The screenshot shows the CERT+ application interface. On the left is a dark sidebar with a search bar and navigation links: 'Discovery Status', 'Rules', 'Excluded from discovery', 'ALERTS & LOGS' (with sub-links for Alerts and Certificate Logs), 'GROUPS & POLICIES' (with sub-links for Groups and CA Policy), 'ADMINISTRATION' (with sub-links for Password Vault, Auto Enrollment, Certificate Authority, and Device Management), and 'Application' (with a 'more' dropdown). The main content area is titled 'Device :: Cloud > Add'. It features a 'Device details' section with a 'Vendors' list containing 'AWS', 'Azure' (selected), and 'GCP'. To the right of the vendors list are several form sections: 'Basic information' with 'Account name' and 'Description' fields; 'Key information' with 'Subscription ID', 'Tenant ID', 'Client ID', 'Client secret' fields, and a 'Services' dropdown menu containing 'Application Gateway', 'Key vault', and 'Virtual machines'; and 'Additional attributes'.

• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Cloud account already exists.	A Cloud Account with the same name exists in inventory.	Check the Account name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Communicating to Azure Cloud

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.

4. On the **Device Management** page, click **Cloud** Tab.
5. Select the **Device**, click **Status**.

The **Device Status** is displayed.

Device - Cloud

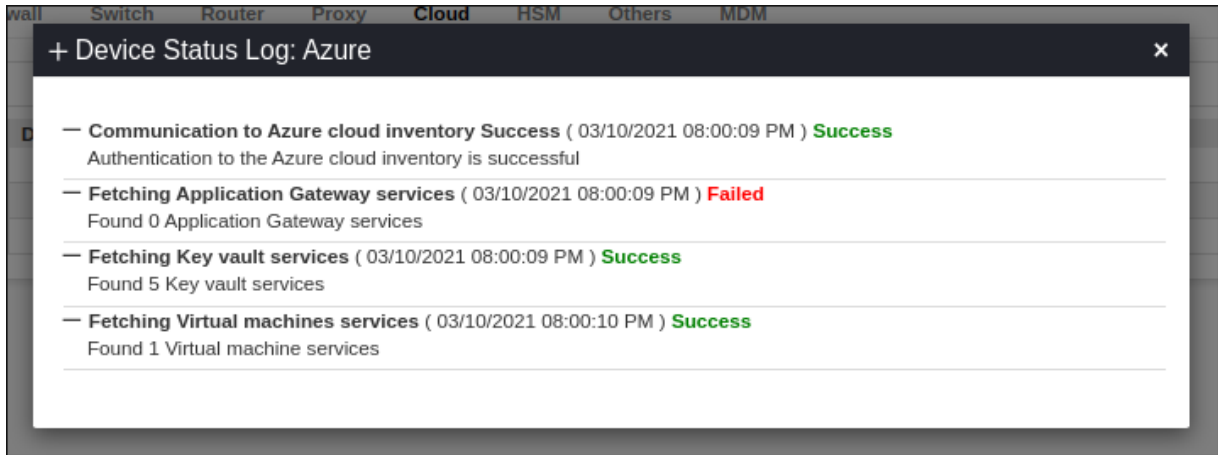
Account name	Device description	Vendor	Status	Services
Azure_UNAUTHORIZED		Azure	Failed	Application Gateway,Key vault,Virtual ...
Azure_Invalid_Credentials		Azure	Failed	Application Gateway,Key vault,Virtual ...
Azure		Azure	Managed	Application Gateway,Key vault,Virtual ...

+ Device Status Log: Azure_Invalid_Credentials

- Communication to Azure cloud inventory Failed (03/10/2021 08:00:59 PM) **Failed**
Authentication to the Azure cloud inventory is Failed

- Device Status Log: AZURE_UNAUTHORIZED

- Communication to Azure cloud inventory Success (03/10/2021 08:08:20 PM) **Success**
Authentication to the Azure cloud inventory is successful
- Fetching Application Gateway services (03/10/2021 08:08:21 PM) **Failed**
Found 0 Application Gateway services
- Fetching Key vault services (03/10/2021 08:08:21 PM) **Failed**
Found 0 Key vault services
- Fetching Virtual machines services (03/10/2021 08:08:22 PM) **Failed**
Found 0 Virtual machine services



- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-', '_', ':', '*', ' ', '!' and spaces.
Authentication to the Azure cloud inventory is Failed	Subscription ID, Tenant ID Client ID and Client secret of the Azure cloud account are incorrect. Check each of the provided ID is valid and active.	Login to Azure portal and get all the valid IDs.
Found 0 Key vault services	No Keyvault instances running for the provided Subscription ID.	Login to Azure portal and check if the Subscription ID has required permission to access the Keyvault instances.
Found 0 Application Gateway services	No Application Gateway instances running for the provided Subscription ID.	Login to Azure portal and check if the Subscription ID has required permission to access the Application Gateway instances.

Error Message	Possible Cause	Possible Solution
Found 0 Virtual machine services	No Virtual Machine instances running for the provided Subscription ID.	Login to Azure portal and check if the Subscription ID has required permission to access the Virtual machine instances.

Issues in Accessing Azure Cloud

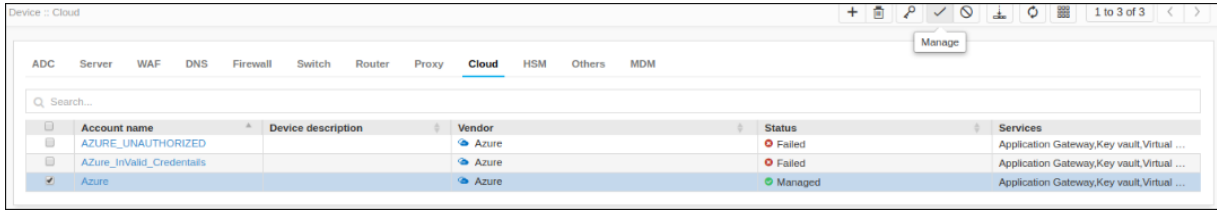
Access Issues might be reproduced when communicating with Azure cloud account, while discovering or fetching the services. These errors can be collected either from logs, API responses, or in the status field for that particular server.

Error Message	Possible Cause	Possible Solution
Connection timeout	Internet / Proxy connection is not provided from the AppViewX node. Firewall settings blocking the REST API request.	Login to AppViewX portal and provide proxy details in Menu->Settings->General->Proxy and Check Firewall settings.
No Keyvault instances are discovered	Subscription ID doesn't have an appropriate role to access the Azure services.	Check if the following role is assigned for the provided subscription ID in Azure cloud account. <pre>{ "properties": { "roleName": "AppViewX_KeyVault_Role", "description": "", "assignableScopes": ["/subscriptions/f2689969-42f6-4fb5-b3be-e3a02e33751c"], "permissions": [{ "actions": ["Microsoft.KeyVault/vaults/read"], "notActions": [], "dataActions": [</pre>

Error Message	Possible Cause	Possible Solution
		<pre> "Microsoft.KeyVault/vaults/certificates/import/action", "Microsoft.KeyVault/vaults/certificates/create/action", "Microsoft.KeyVault/vaults/certificates/update/action", "Microsoft.KeyVault/vaults/certificates/read"], "notDataActions": [] }] }} </pre>
No Keyvault instances are discovered	Azure Keyvault doesn't have certificate Get/List permissions in access policies.	Login to Azure portal and navigate to Azure KeyVault -> Access policies and check if the Certificate management Operations has Get and List permissions.
No Keyvault instances are discovered	Azure Keyvault Networking blocking the certificate discovery.	Login to Azure portal and navigate to Azure KeyVault -> Networking and check if the If IP is allowed to access the Keyvault in Firewalls and virtual networks.

Issues in Managed Cloud

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Cloud** Tab.
5. Select the device and click **Manage**.



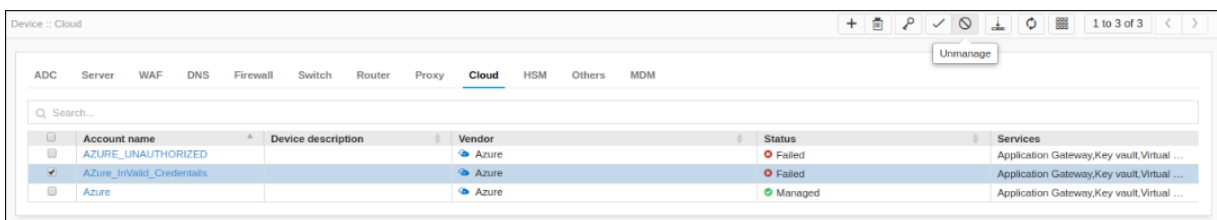
• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
The selected devices are managed. The operation cannot be performed.	Device cannot be managed because it is already in the managed state.	Unmanage the device(s) in the managed state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

Issues in Unmanaged Cloud

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** Page is displayed.
4. On the **Device Management** page, click **Cloud** Tab.
5. Select the device and click **Unmanage**.



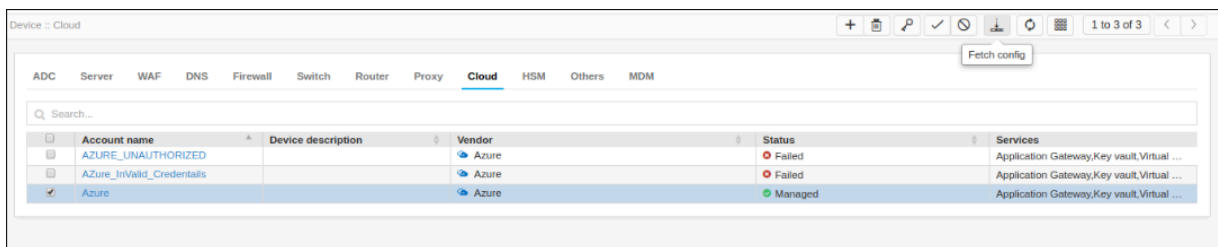
- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
The selected devices are already unmanaged. The operation cannot be performed.	Device cannot be unmanaged because it is already in the unmanaged state.	Manage the device(s) in an unmanaged state before performing action.
Fetch config not allowed for Unmanaged devices	Fetch config operation is only allowed on the devices which are in managed state.	Manage the device(s) in an unmanaged/in-progress state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

Issues in Fetch Config

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Cloud** Tab.
5. Select the **Device**, click **Fetch Config**.



- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Authentication to the Azure cloud inventory is Failed	Subscription ID, Tenant ID Client ID and Client secret of the azure cloud account is incorrect.	Login to Azure portal and get all the valid IDs. Check if each of the provided ID is valid and active.

Issues in Certificate Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Cloud Scan**.



Note: To discover certificates from Managed cloud accounts, the cloud account should be managed under the AppViewX Inventory.

CERT+

Discovery : Cloud Scan : Add Discovery

* Discovery Run Type ☒ On-demand ☐ Schedule ⓘ

* Discovery Instance Name ⓘ

Description

Discover By

You can either manually enter template details or upload a file.

* Discovery From ⓘ

Cloud device 2 [Select All](#)

- ☒ Azure::Azure
 - ☒ Application Gateway
 - ☒ Key vault

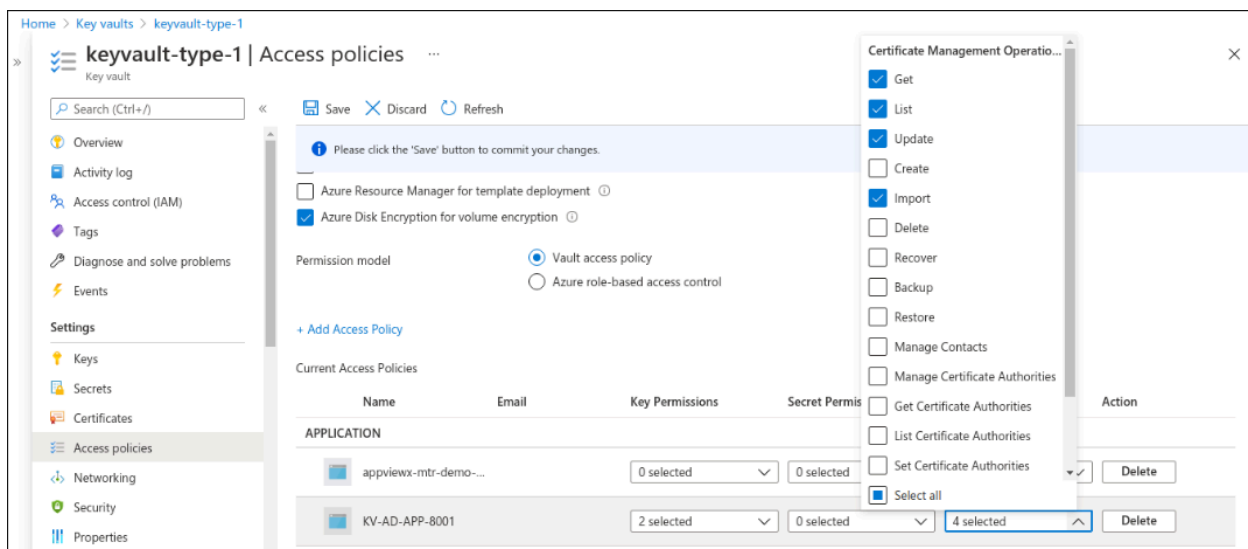
[Discover](#) [Reset](#)

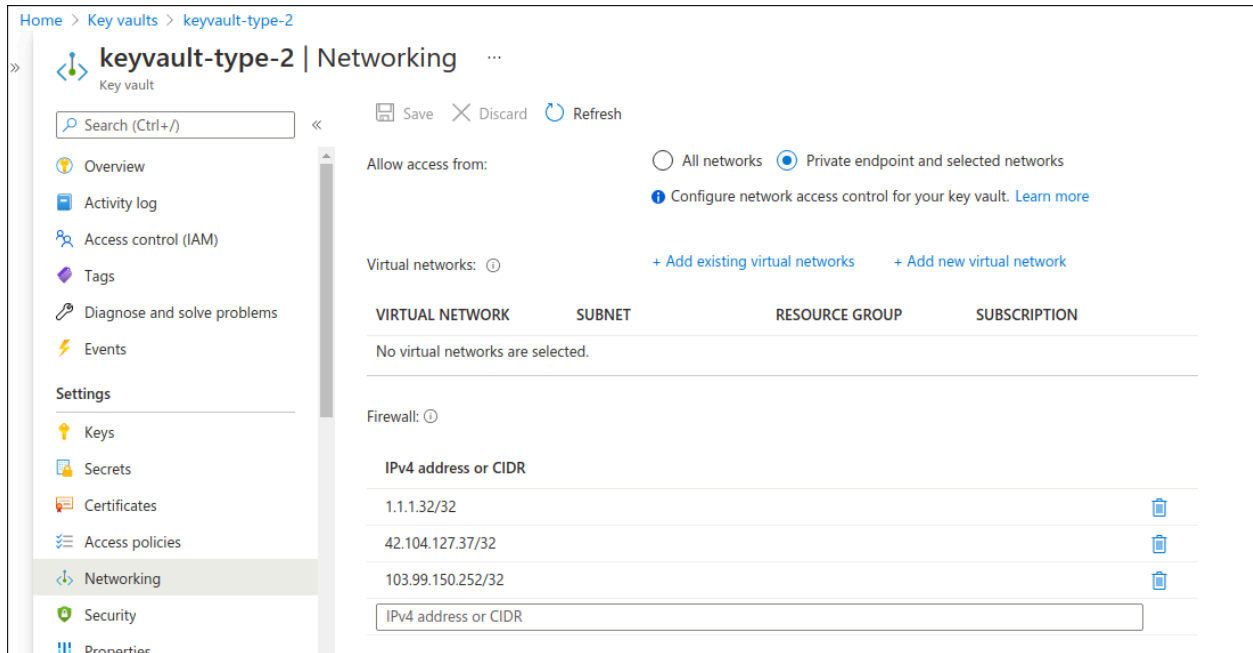
• [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	- Discovery name not given or length is less than 2 characters. - Interval between batches info. is missing when execution type is sequential.	- Enter a valid name with a minimum of 2 characters. - Provide a time interval between batches in minutes.
Please select a devices	No cloud account is selected in the “Discover By” section.	Select at least one device to discover certificates from.

Error Message	Possible Cause	Possible Solution
Discovery Status Failed	Check internet /Proxy connection is provided in AppViewX node.	Login to AppViewX portal and provide proxy details in Menu->Settings->General->Proxy.
No Certificates discovered from Azure KeyVault	Keyvault instance is not discovered from Azure cloud account.	Check device status in device addition page for Azure keyvault, if we have a Keyvault instance discovered count.
No Certificates discovered from Azure KeyVault	Azure Keyvault doesn't have certificate Get/List permissions in access policies	Login to azure portal and navigate to Azure KeyVault -> Access policies and check the Certificate management Operations having Get and List permissions (refer below snapshot)
No Certificates discovered from Azure KeyVault	Azure Keyvault Networking blocking the certificate discovery	Login to Azure portal and navigate to Azure KeyVault -> Networking and check the Firewalls and virtual networks If IP is allowed to access the Keyvault. (refer below snapshot)





Issues in Certificate Import

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**, select **Cloud**.
4. Create an **Application connector** for Azure
5. **Push** the certificate to the device

CERT+

Search features

DASHBOARD

CERTIFICATE ACTION

Enroll Certificate

Renew Certificate

Push to Device

Reissue Certificate

Revoke Certificate

more

CERTIFICATE INVENTORY

Server

Client

Code Signing Certificate

Device

Intermediate

Root

Upload

Download

Server Certificate > Cert23.appviewx.plus > View Work order Status

Request View Workorder View

Search...

▶

✓ Push Without Bind Reque...

✓ Review

✓ Implement

✓ Pre Push Script Execution

✗ Push Task

Push Task
Certificate push failed

Logs - Push Task

```

1 03/11/2021 02:17:36 - Initiating Push Task
2 03/11/2021 02:17:39 - Certificate push is failed. Error is, jdk.nashorn.internal.runtime.Undefined
3 03/11/2021 02:17:39 - Push Task Failed
4

```

CERT+

Search features

DASHBOARD

CERTIFICATE ACTION

Enroll Certificate

Renew Certificate

Push to Device

Reissue Certificate

Revoke Certificate

more

CERTIFICATE INVENTORY

Server

Client

Code Signing Certificate

Device

Intermediate

Root

Upload

Download

Server Certificate > AzureMar10 > View Work order Status

Request View Workorder View

Search...

▶

✓ Push Without Bind Reque...

✓ Review

✓ Implement

✓ Pre Push Script Execution

✗ Push Task

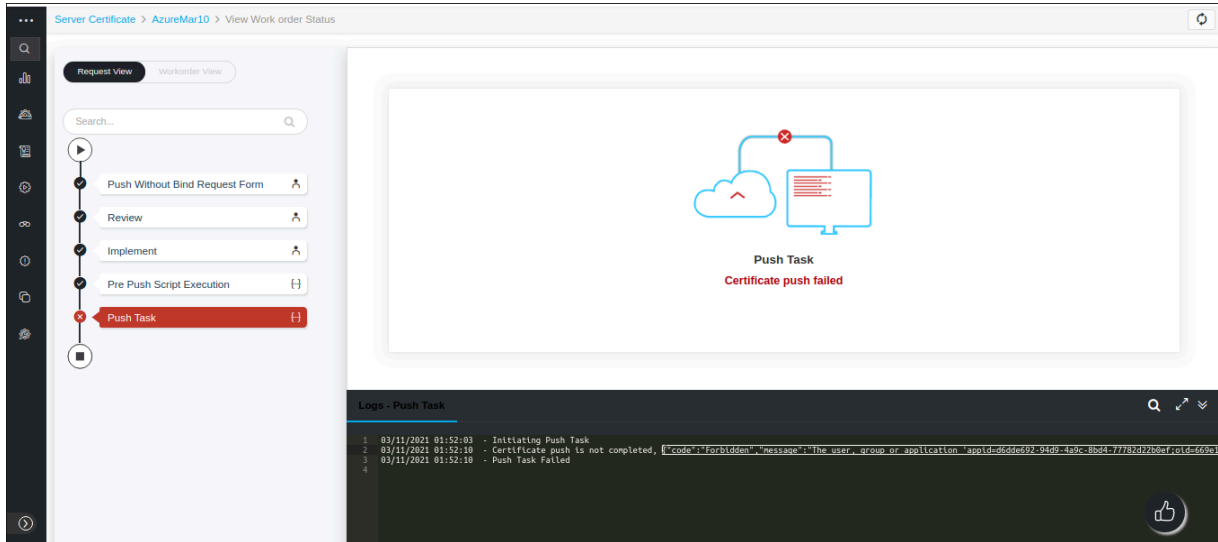
Push Task
Certificate push failed

Logs - Push Task

```

1 03/11/2021 01:44:40 - Initiating Push Task
2 03/11/2021 01:44:50 - Certificate push is not completed, {"code":"Forbidden","message":"Client address is not authorized and caller is not a trusted"}
3 03/11/2021 01:44:51 - Push Task Failed
4

```



• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	- Pushing to device when certificate is unavailable, i.e, in a new state. - Previous work order is in progress and not completed. - AppConnector might not be in sync.	- Push to device after certificate has been retrieved from CA. - Initiate push after previous work order is finished. - Synchronize the AppConnector and retry.

Error Message	Possible Cause	Possible Solution
Unable to initiate request, template is in disabled state	Given workflow is not in the enabled state.	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Certificate push failed. Error is, <code>jdk.nashorn.internal.runtime.Undefined</code>	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.

Error Message	Possible Cause	Possible Solution
Certificate push failed	Check internet /Proxy connection is provided in AppViewX node.	Login to AppViewX portal and provide proxy details in Menu->Settings->General->Proxy.
<code>{"code": "Forbidden", "message": "The user, group or application 'appid=d6dde692-94d9-4a9c-8bd4-77782d22b0ef;oid=669e113f-0651-4bb5-9698-cd4e863e1ee9;numgroups=0;iss=https://sts.windows.net/e5f90d85-3cdf-457d-a611-1aca82b0843b/' does not have Certificates import permission on key vault 'keyvault-type-1;location=eastus'. For help resolving this issue, please see https://go.microsoft.com/fwlink/?linkid=2125287", "innererror": {"code": "ForbiddenByPolicy"}}}</code>	Azure Keyvault instance doesn't have certificate Import permissions in access policies.	Login to Azure portal and navigate to Azure KeyVault -> Access policies and check the Certificate management Operations having Import permission.
<code>{"code": "Forbidden", "message": "Client address is not authorized and caller is not a trusted service.\r\nClient address: 125.21.72.158\r\nCaller: appid=d6dde692-94d9-4a9c-8bd4-77782d22b0ef;oid=669e113f-0651-4bb5-9698-cd4e863e1ee9;iss=https://sts.windows.net/e5f90d85-3cdf-457d-a611-1aca82b0843b\r\nVault: keyvault-type-2;location=eastus", "innererror": {"code": "ForbiddenByFirewall"}}}</code>	Azure Keyvault Network blocking the Certificate Push.	Login to Azure portal and navigate to Azure KeyVault -> Networking and check the Firewalls and virtual networks if IP is allowed to access the Keyvault.

Troubleshooting CLOUD - Common Functionality

- [Overview](#)
- [Supported Web Browsers](#)
- [Issues in Common Functions of CLOUD](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using cloud functionalities. This guide will give more troubleshooting processes on cloud addition, deletion, and other actions available with the cloud module.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	rom AppViewX Version 11.1

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

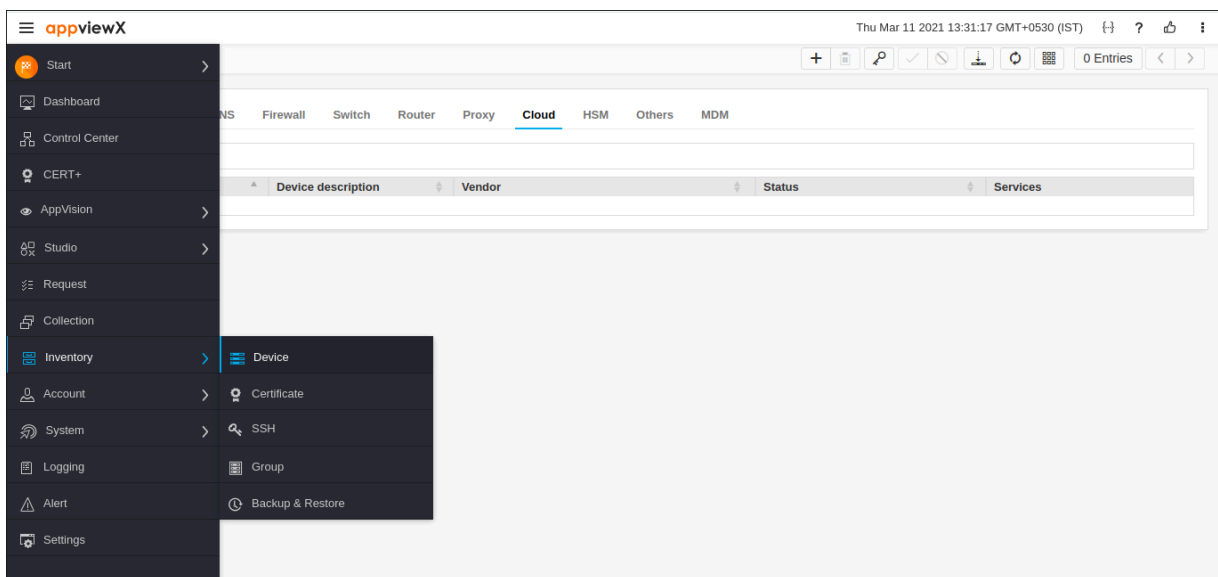
Issues in Common Functions of CLOUD

- [Issues in Cloud Addition using AppViewX UI - AWS](#)
- [Issues in Cloud Addition using AppViewX UI - Azure, GCP](#)
- [Issues in Communicating to Cloud accounts](#)

- [Issues in Managed Cloud Account](#)
- [Issues in Unmanaged Cloud Account](#)
- [Issue in Discovery](#)

Issues in Cloud Addition using AppViewX UI - AWS

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Inventory** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Cloud** Tab.
5. From the icon list at the top right corner, click **Add**.
The **Device Addition** page is displayed.
6. From the **Device Details** Section on the left, Click **AWS**.
7. Fill in the appropriate details.
8. Select services to be managed.
9. Click **Fetch regions**.
10. Fill in additional attributes and click **Save** in the footer.



The screenshot shows the AppViewX application interface. At the top, there's a header with the AppViewX logo and a timestamp. Below the header, a breadcrumb trail indicates 'Device :: Cloud > Add'. The main content area is titled 'Device details' and is divided into two panes. The left pane, labeled 'Vendors', contains a list of cloud providers: AWS, Azure, and GCP. The right pane, labeled 'Basic information', contains several input fields: 'Account name' (with a red asterisk and an info icon), 'Device description', 'Account number' (with a red asterisk), and 'Credential type' (a dropdown menu set to 'Manual Entry'). Below these are fields for 'Access key' and 'Secret key' (both with red asterisks). At the bottom of the right pane is the 'Key information' section with a 'Data center' dropdown menu set to 'absecon'.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Cloud account already exists.	A cloud account with the same Account name already exists in the inventory.	Check the Account name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.
Please provide valid credentials	The credentials provided are invalid/ has no access to fetch regions	Provide valid credentials/ credentials with needed access

Issues in Cloud Addition using AppViewX UI - Azure, GCP

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Inventory** and click **Device**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Cloud** Tab.
5. From the icon list at the top right corner, click **Add**.

The **Device Addition** page is displayed.

6. From the **Device Details Section** on the left, click **Azure/GCP**.
7. Fill in the appropriate details.
8. Select **services** to be managed.
9. Click **Fetch regions**.
10. Fill in additional attributes and click **Save** in the footer.

The screenshot shows the 'Device Addition' page in the AppViewX interface. The left sidebar has a 'Vendors' section with 'AWS', 'Azure', and 'GCP' options. 'Azure' is selected. The main content area is titled 'Basic information' and contains the following fields:

- Account name:** A text input field.
- Description:** A text input field.
- Key information:**
 - Subscription ID:** A text input field.
 - Tenant ID:** A text input field.
 - Client ID:** A text input field.
 - Client secret:** A text input field.
 - Services:** A dropdown menu with three selected options: 'Application Gateway', 'Key vault', and 'Virtual machines'.
- Additional attributes:** A section header for further configuration options.

The screenshot shows the 'Device Addition' page in the AppViewX interface, now with 'GCP' selected in the 'Vendors' sidebar. The main content area is titled 'Basic information' and contains the following fields:

- Account name:** A text input field.
- Device description:** A text input field.
- Key information:**
 - Client email ID:** A text input field.
 - Private key entry by:** Two radio buttons: 'Manual entry' (selected) and 'Key information'.
 - Enter service account key:** A text input field.

At the bottom right of the form, there are two buttons: 'Save' and 'Cancel'.

• [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Cloud account already exists.	A cloud account with the same Account name already exists in inventory.	Check the Account name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

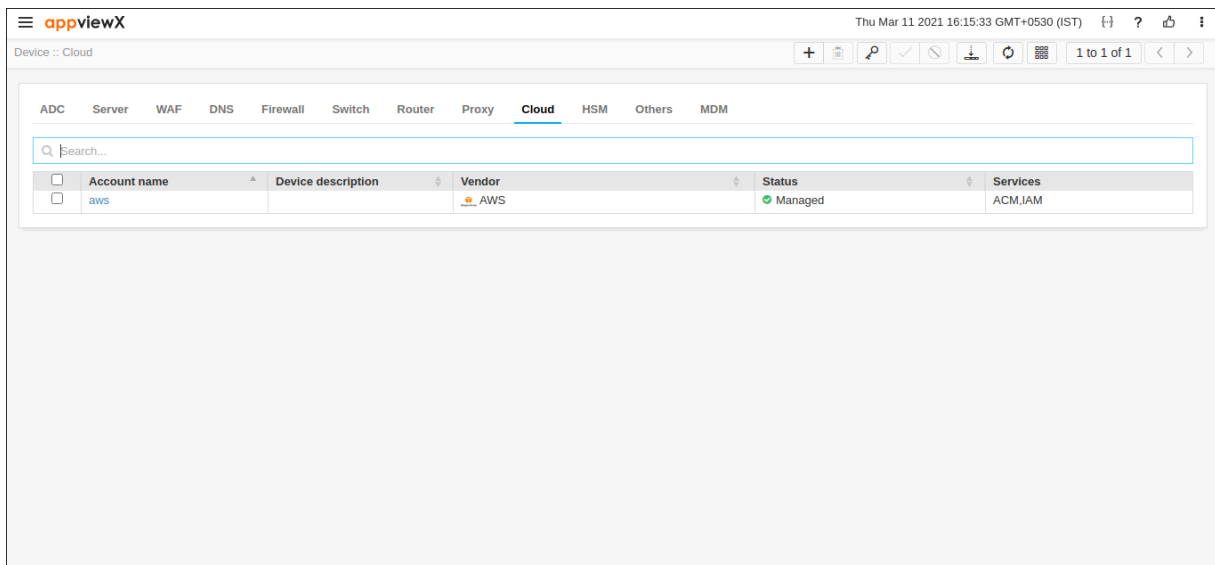
Issues in Communicating to Cloud accounts

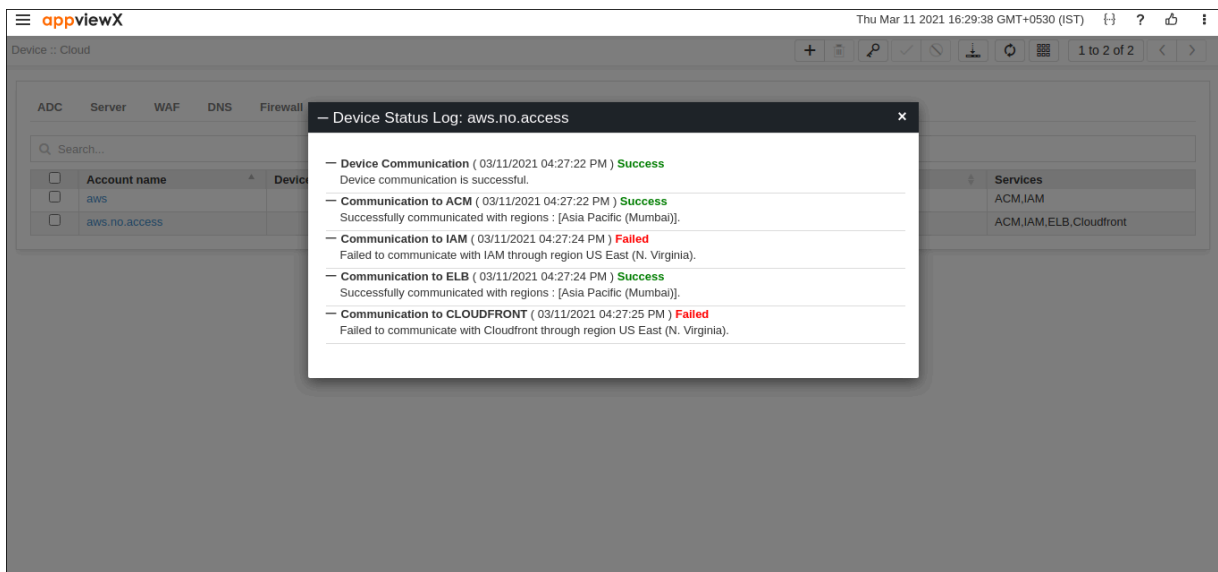
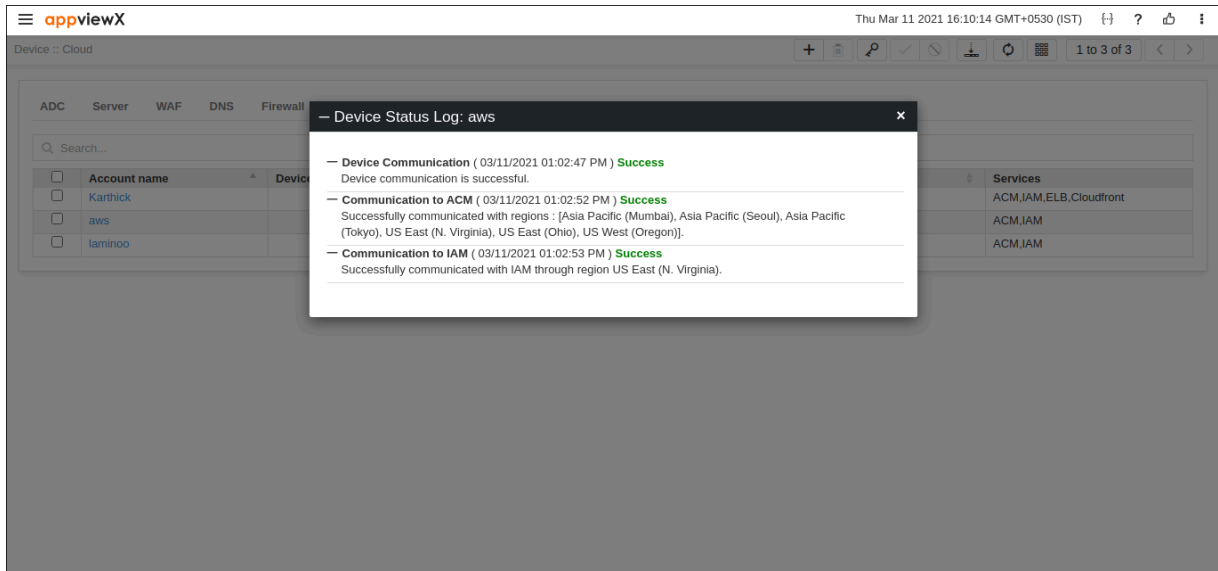
1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Inventory** and click **Device**.

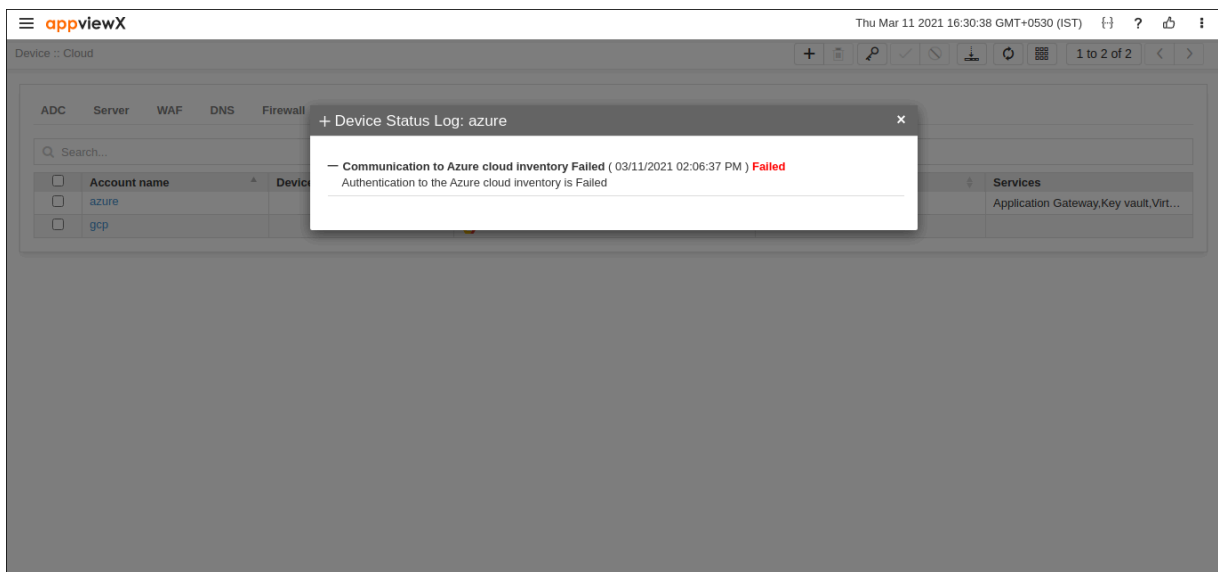
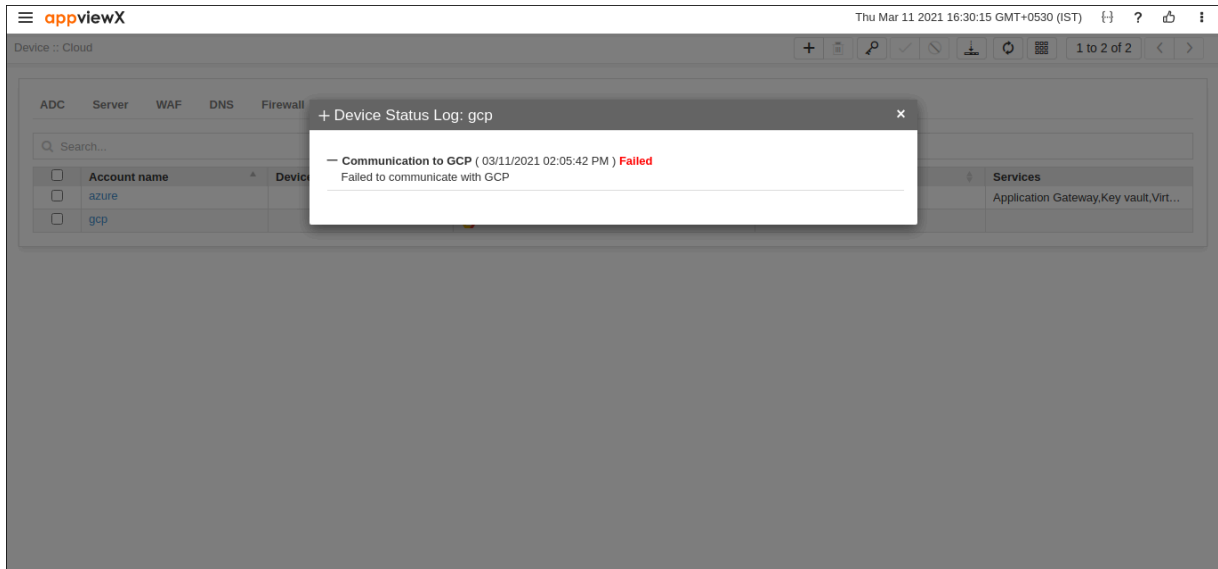
The **Device Management** page is displayed.

4. On the **Device Management** page, click **Cloud** Tab.
5. Select the **Device**, click **Status**.

The **Device Status** is displayed.







• Error Messages

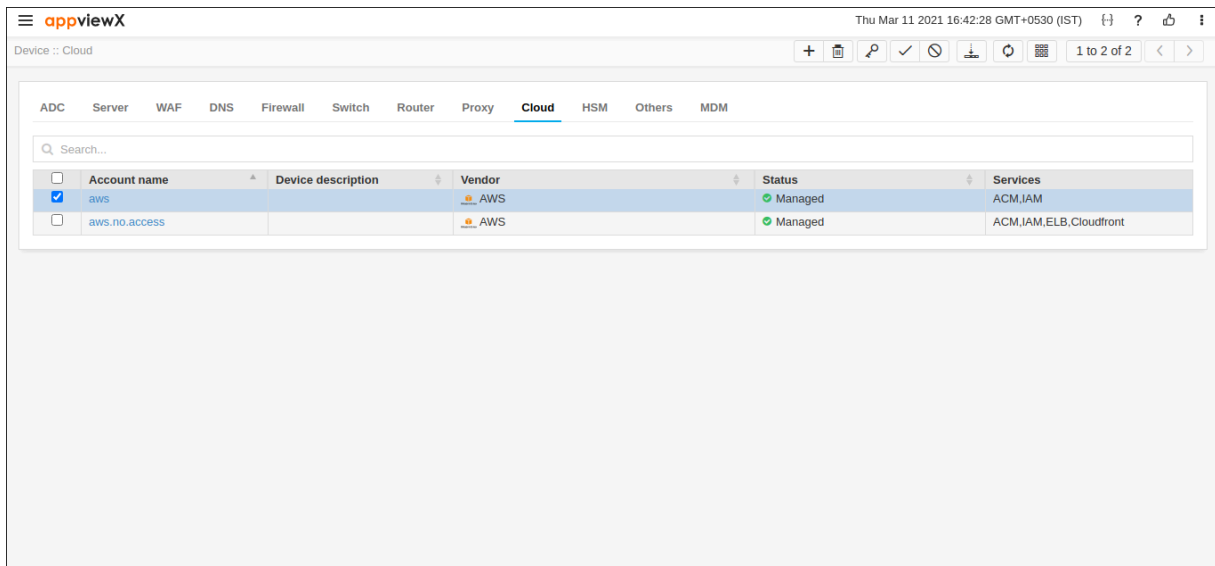
Error Messages

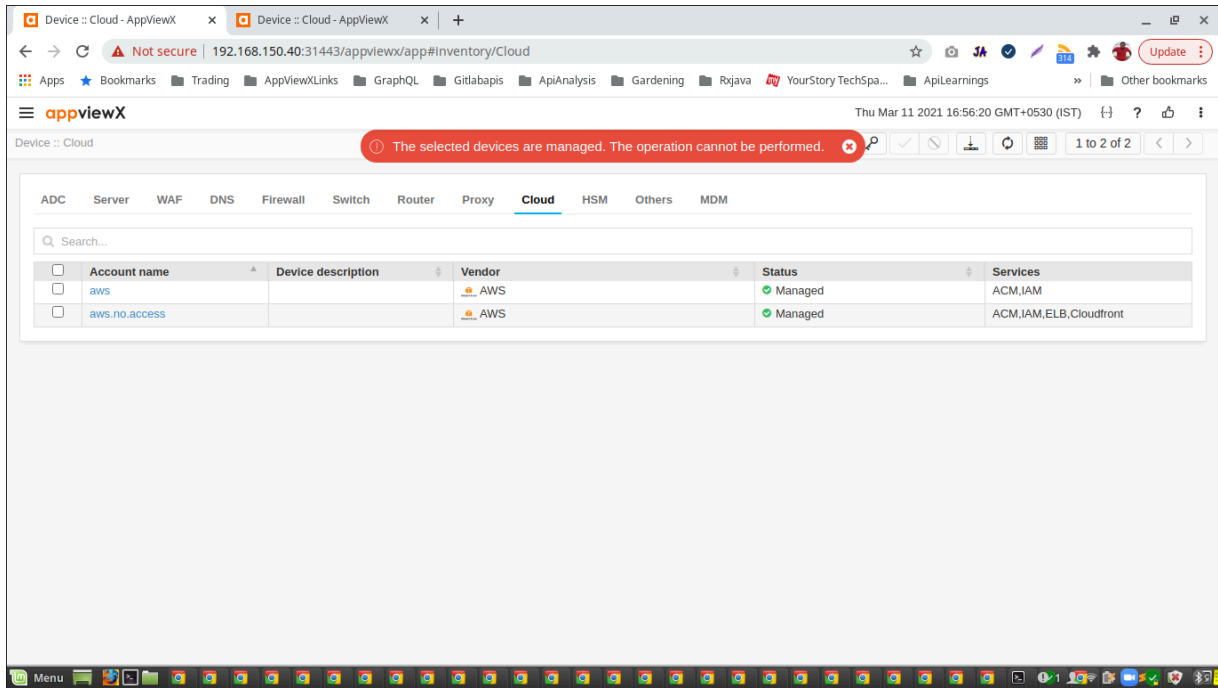
Error Message	Possible Cause	Possible Solution
Authentication to the Azure cloud inventory is Failed	Credentials provided are invalid/ credentials do not have the required access.	Validate the credentials and Check if credentials are provided required access.

Error Message	Possible Cause	Possible Solution
Failed to communicate with GCP	Unable to connect to the endpoint.	Check if the node can reach the endpoint via proxy/internet as configured.
Failed to communicate with <SERVICE> through region <REGIONS>.	Credentials do not have required access	Provide credentials the required access

Issues in Managed Cloud Account

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Inventory** and click **Device**.
The **Device Management** Page is displayed.
4. On the **Device Management** Page, click **Cloud** Tab.
5. Select the device and click **Manage**.





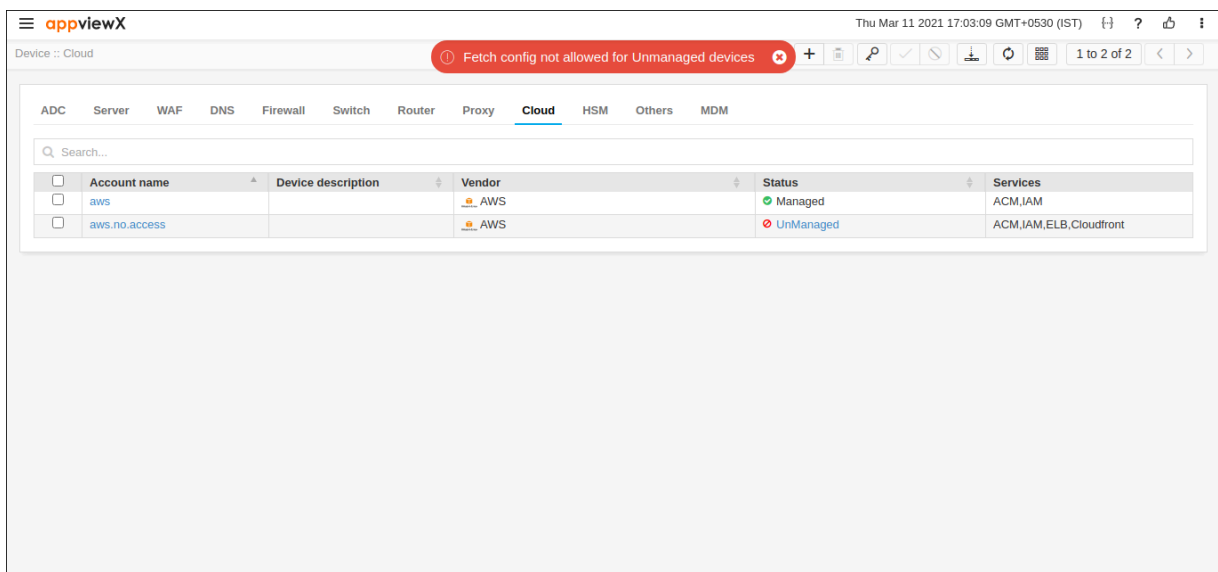
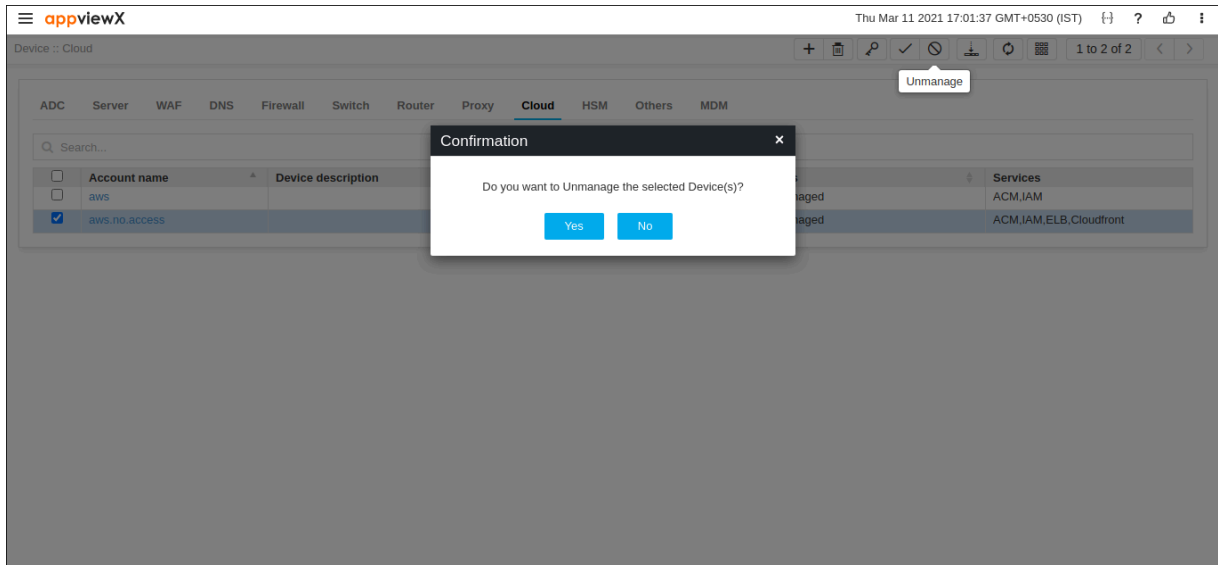
• Error Messages

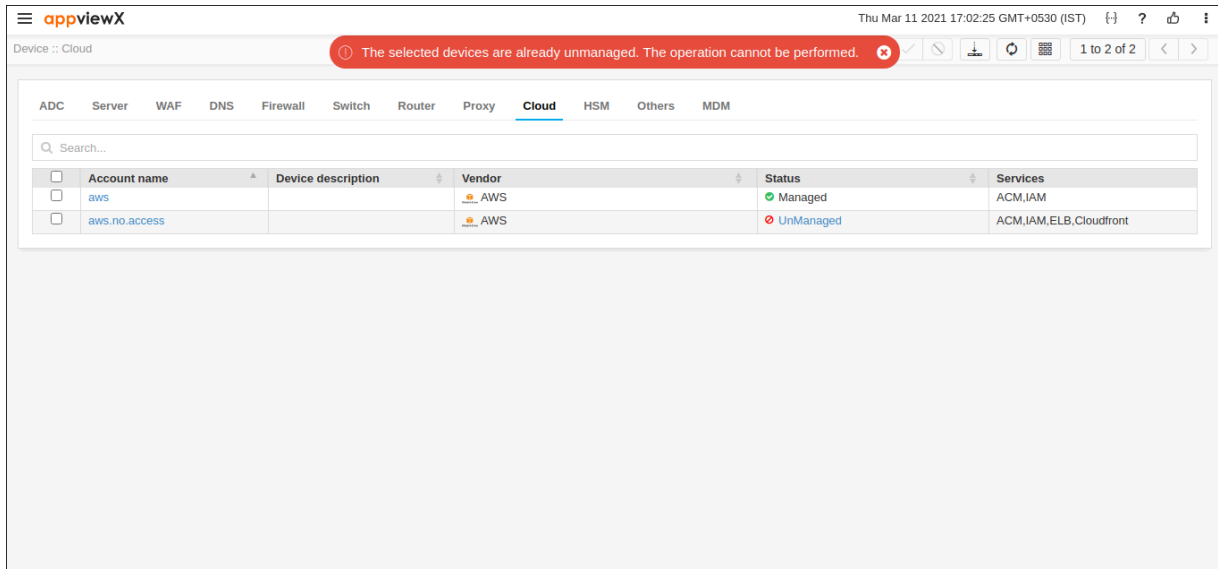
Error Messages

Error Message	Possible Cause	Possible Solution
The selected devices are managed. The operation cannot be performed.	The device cannot be managed because it is already in the managed state.	Unmanage the device(s) before performing the action.

Issues in Unmanaged Cloud Account

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Inventory** and click **Device**.
The **Device Management** Page is displayed.
4. On the **Device Management** Page, click **Cloud** Tab.
5. Select the device and click **Unmanage**.





- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
The selected devices are already unmanaged. The operation cannot be performed.	The device cannot be unmanaged because it is already in the unmanaged state.	Manage the device(s) before performing the action.
Fetch config not allowed for Unmanaged devices	Fetch config operation is only allowed on the devices which are in a managed state.	Manage the device(s) in an unmanaged/in-progress state before performing an action.

Issue in Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Cloud Scan**.



Note: To discover certificates from Managed cloud accounts, the cloud account should be managed under the AppViewX Inventory.

• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. The Discovery name is not given or the length is less than 2 characters. 2. The interval between batches info is missing when the execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates.

Chapter 5: Troubleshooting Server, Firewalls, WAF, and Rapid SB Connectors

- [Overview](#)

Overview

This section of the guide will help you tackle the issues encountered while using the functionalities of servers, firewalls, WAF, and Rapid SB Connectors. It deals with common functionalities of these devices at the beginning of each guide and the rest of the guide deals with functionalities of specific devices. If the problem still remains unresolved please send a request to Technical Support by opening a case with the AppViewX Technical Services team. You can open a case from helpcenter.AppViewX.com or send an email to help@AppViewX.com.

- [Troubleshooting Apache Linux](#)
- [Troubleshooting Barracuda WAF](#)
- [Troubleshooting Cisco ASA Firewall](#)
- [Troubleshooting Cisco CallManager](#)
- [Troubleshooting Common Functionality of Servers](#)
- [Troubleshooting Data Power Server](#)
- [Troubleshooting F5 WAF](#)
- [Troubleshooting Fortigate Firewall](#)
- [Troubleshooting HP ILO](#)
- [Troubleshooting IBMClient Linux](#)
- [Troubleshooting IBMClient Windows](#)
- [Troubleshooting Imperva WAF](#)
- [Troubleshooting Linux JBoss Server](#)
- [Troubleshooting Microsoft Enterprise CA](#)
- [Troubleshooting Microsoft Tomcat](#)
- [Troubleshooting MQServer Linux](#)
- [Troubleshooting MQServer Windows](#)
- [Troubleshooting MS SQL Windows](#)
- [Troubleshooting Nginx Server](#)
- [Troubleshooting NginxPlus ADC](#)

- [Troubleshooting Paloalto Firewall](#)
- [Troubleshooting Panorama Firewall](#)
- [Troubleshooting RabbitMQ Server](#)
- [Troubleshooting Rapid SB Server Inventory](#)
- [Troubleshooting Rapid SB Linux Server](#)
- [Troubleshooting Tomcat Linux](#)
- [Troubleshooting Weblogic Linux](#)
- [Troubleshooting Websphere Linux](#)
- [Troubleshooting Websphere Windows](#)
- [Troubleshooting Windows Apache Server](#)
- [Troubleshooting Windows JBoss Server](#)
- [Troubleshooting Windows Weblogic Server](#)

Troubleshooting Apache Linux

- [Overview](#)
- [Issues in Apache Linux](#)

Overview

This document helps you troubleshoot the common problems that you might encounter when using Apache Linux functionalities. This guide will give more troubleshooting processes on issues related to Apache Linux server. The issues are device addition, communication to the server, CSR generation, access to server, fetch configuration, discovery along with push and rollback.

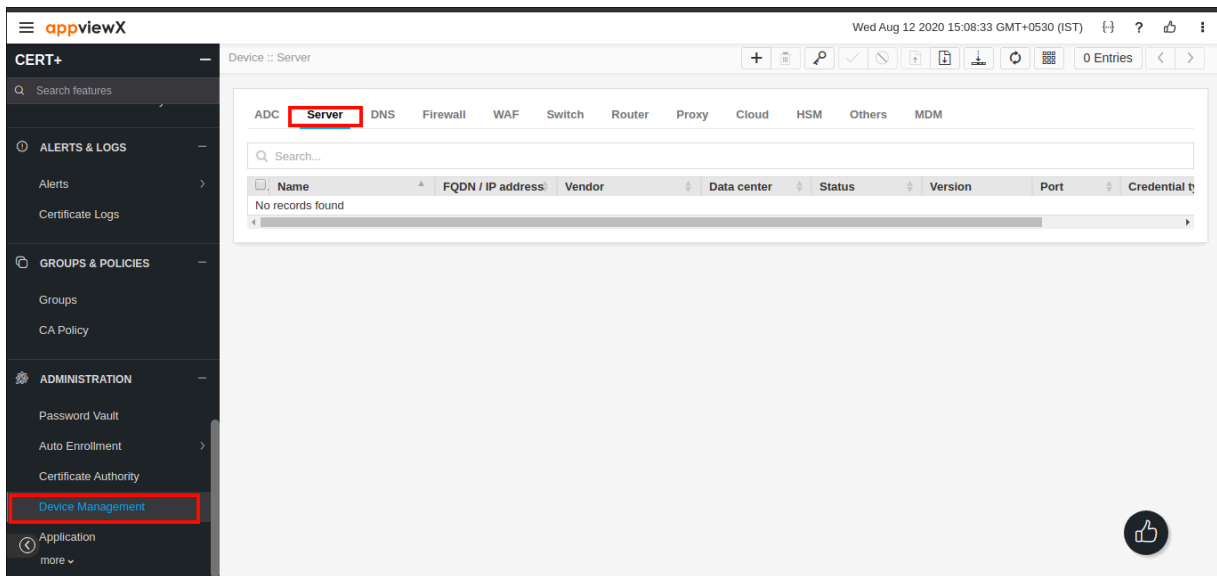
Issues in Apache Linux

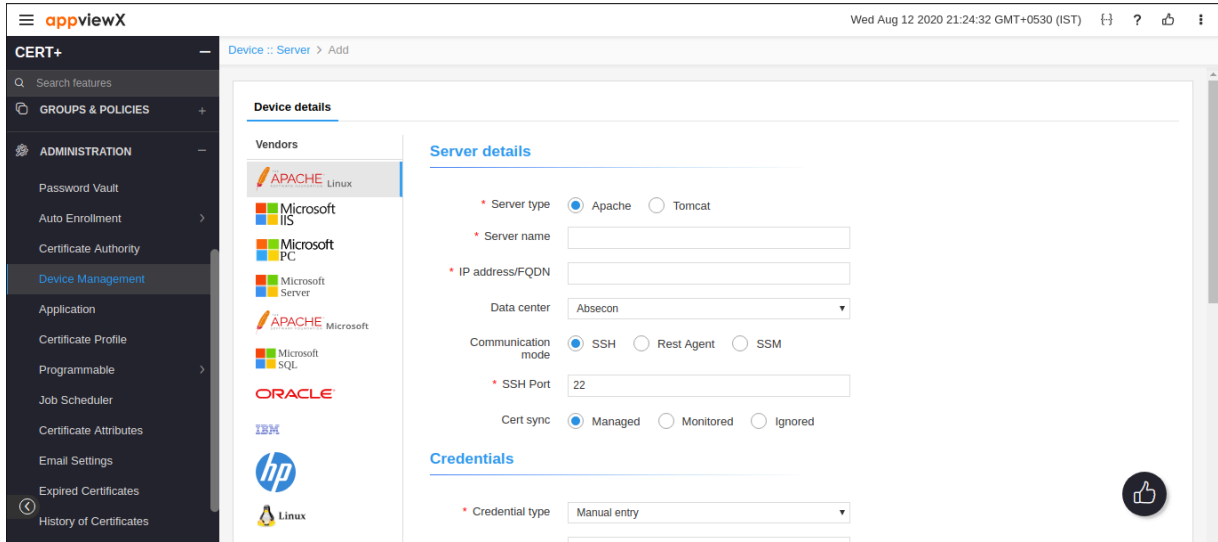
- [Issue in Device Addition using AppViewX UI](#)
- [Issues in Communicating to the server](#)
- [Issues in CSR Generation](#)
- [Issue in Access](#)
- [Issues in Fetch Config](#)

- [Issue in Discovery](#)
- [Issues in Push and Rollback](#)

Issue in Device Addition using AppViewX UI

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the Device Management page, click Server Tab.
5. From the icon list at the top right corner, click **Add**.
The **Device Addition** page is displayed.
6. From the **Device Details** Section on the left, click **Apache Linux**.
7. Click **Server type** as **Apache**.
8. Fill in the appropriate details.
9. Click **Add**.





• Error Messages

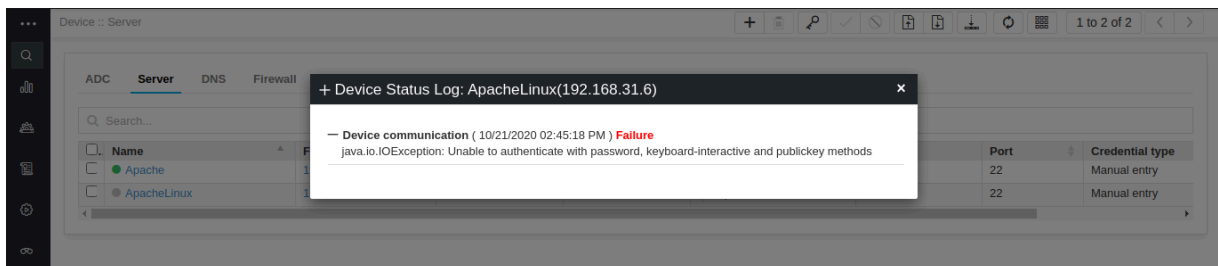
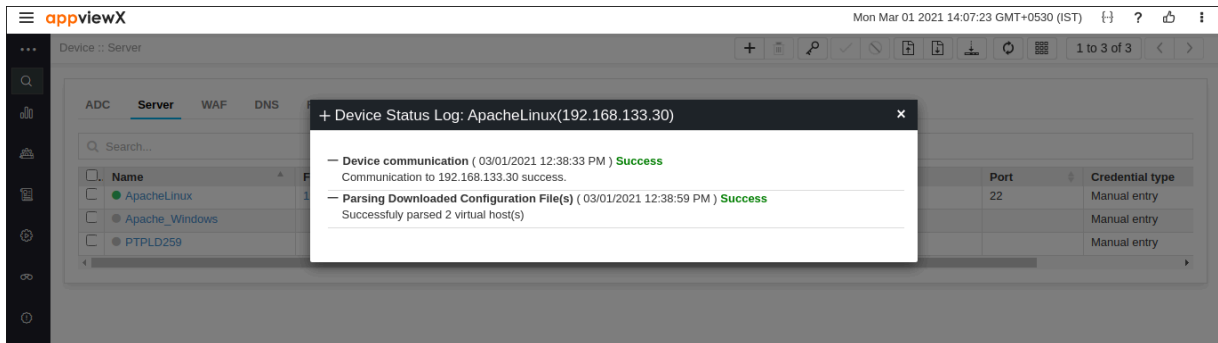
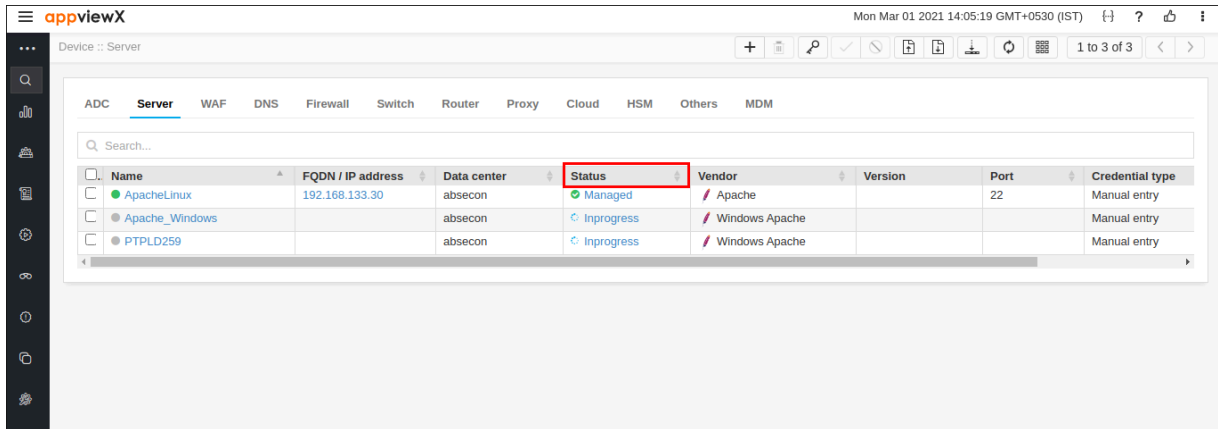
Error Messages

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Communicating to the server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**.
The **Device Communication Status** is displayed.

Troubleshooting Server, Firewalls, WAF, and Rapid SB Connectors



- Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-', '_', '.', '*', ' ', '!' and spaces.
Device IP/FQDN cannot be null or empty.	Device IP/FQDN is empty.	Provide device ip/fqdn as it is a mandatory field.
Invalid device IP/FQDN address.	IP/FQDN address is not valid.	Provide valid IP/FQDN address.
Access list for the device cannot be empty.	Credentials not provided for SSH communication.	Provide valid credentials for SSH communication.
Username cannot be null or empty.	Username is not provided or is empty.	Provide a valid username.
The Password cannot be null or empty.	Password is not provided or is empty.	Provide a valid password.
Key cannot be null or empty.	Key is not provided or is empty.	Provide a valid SSH key.
Ip is not reachable/invalid.	Invalid credentials	Kindly check the credentials provided.
	IP is not reachable	Kindly check if IP is pingable or not and make it up and running.
	IP is blocked by the firewall	Kindly check firewall settings.
Password / key Mismatch or incorrect.	Unable to decrypt the password with the given key.	Provide a valid password that matches the key.
Communication Failed	Username or password may be invalid	Check and provide the correct username and password.

Error Message	Possible Cause	Possible Solution
java.io.IOException: Unable to authenticate with password, keyboard-interactive and publickey methods.	Authentication Failure	Provide correct credentials for authentication. Make sure SSH is enabled on the given server.
Linux rest agent communication failed.	Rest agent running on the destination machine might be down.	Please check the status of the rest agent in the destination machine.

Issues in CSR Generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab.
The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. Click the **Category** from the dropdown.
7. Click the correct **Vendor** from the dropdown.
A list of devices will be generated in the **Devices dropdown**.
8. Select the **Apache** device for generating **CSR**.
9. Click **Add**.

The screenshot shows the 'Enroll Server Certificate' interface in AppViewX. The left navigation pane has 'CERT+' expanded, with 'Enroll Certificate' selected. The main panel contains the following fields:

- CA Account:** AppViewX CA
- Certificate Profile:** Server
- Connector Name:** AppViewX CA connector
- Description:** (empty text area)
- CSR Generation:** Radio buttons for AppViewX, Upload CSR, and HSM. The 'End Point' option is selected under AppViewX.
- Category:** Server
- Vendor:** Apache
- Devices:** ApacheLinux
- CSR Location:** /opt/automation
- CSR file name:** democert .csr
- Key File Name:** demokey .key

At the bottom, there are 'Add' and 'Reset' buttons.

- Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Problem while generating csr on target server	General Failure - SSH/SFTP communication failure	Provide correct credentials and make sure device communication is successful.
Invalid key type specified in the request	Given key type might not be supported by open SSL in the target machine.	Provide valid key type.
Problem while generating csr on the target server.	Location might not have permission.	Check the permission and provide it.
CSR and Private key has been failed	Open SSL configuration might be wrong in the target machine.	Check and correct open SSL configuration in the device.

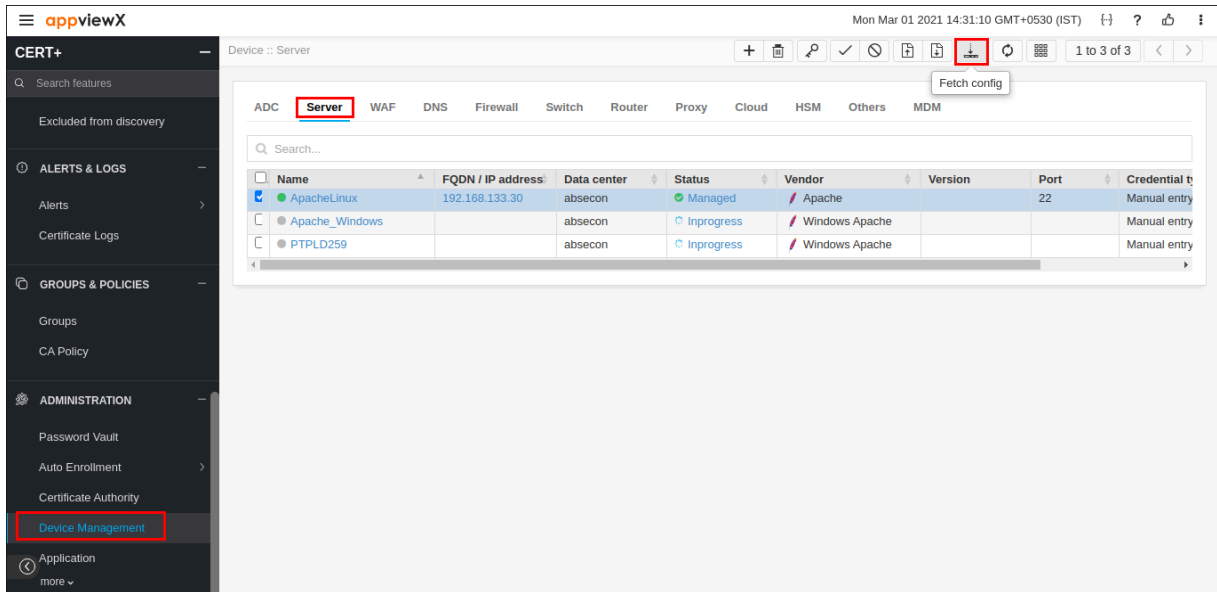
Issue in Access

Access Issues occur while communicating with servers while discovering or fetching configuration files. These errors can be collected either from logs, API responses, or the status field of that server.

Error Message	Possible Cause	Possible Solution
Sudo Access failure	Linux Commands execution with sudo fails.	Verify if the system has the correct sudo setup.
dzdo Access failure	Linux Commands execution with dzdo fails.	Verify if the system has the correct dzdo setup.
Permission denied for file/location.	File might not be present in the avx environment.	Check whether someone deleted the file from AppViewX environment.
	user might not have permission to read in the given source location.	Verify if read permission is given for the location.
	Device communication might not be established when service has started.	Verify the device connection and restart the service.

Issues in Fetch Config

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Fetch Config**.



• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Parsing apache configuration failed.	Configuration file might be corrupted/ empty.	Verify if the configuration file is correct.
	AppViewX is not able to read/ parse the Config files from the server.	Check if the server has proper config files related to Apache Server and AppViewX has proper read permissions.

Issue in Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

The screenshot shows the 'Add Discovery' form in the AppViewX interface. The left sidebar contains navigation options like CERT+, AUTOMATION, CERTIFICATE DISCOVERY, and ALERTS & LOGS. The main form area is titled 'Discovery : Managed Devices Scan : Add Discovery'. It has fields for 'Discovery Run Type' (On-demand is selected), 'Discovery Instance Name' (demoDiscovery), and a 'Description' text area. Under the 'Discover By' section, the 'Discovery From' dropdown is set to 'Managed Servers'. Below this, there is a table with one entry: 'Apache::ApacheLinux'. The 'Discover' button at the bottom is highlighted.

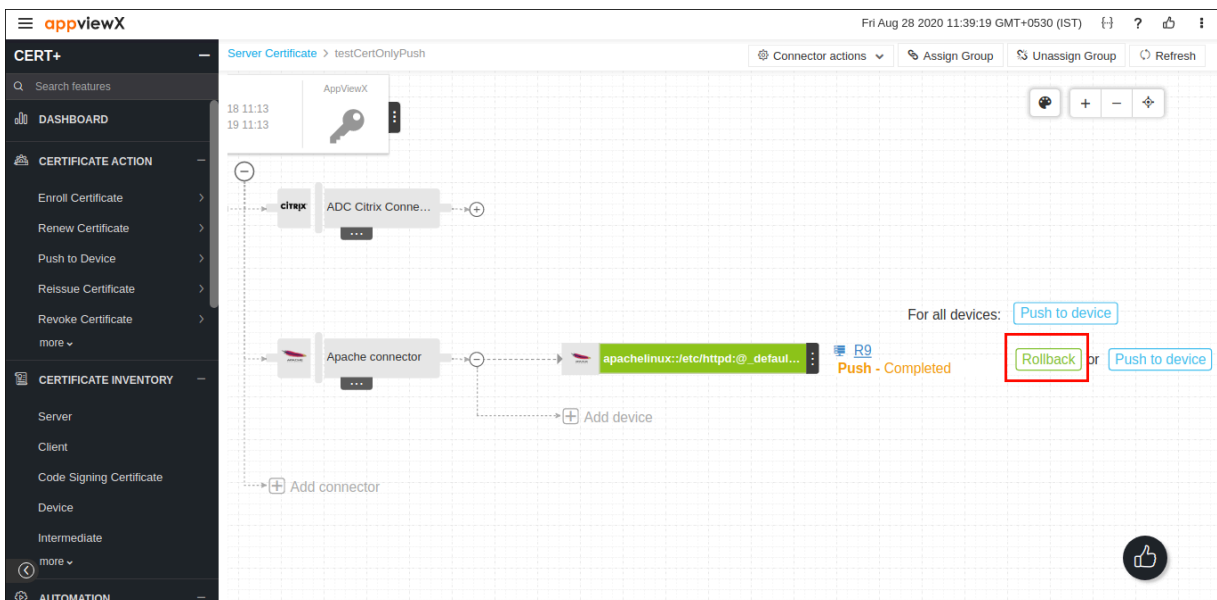
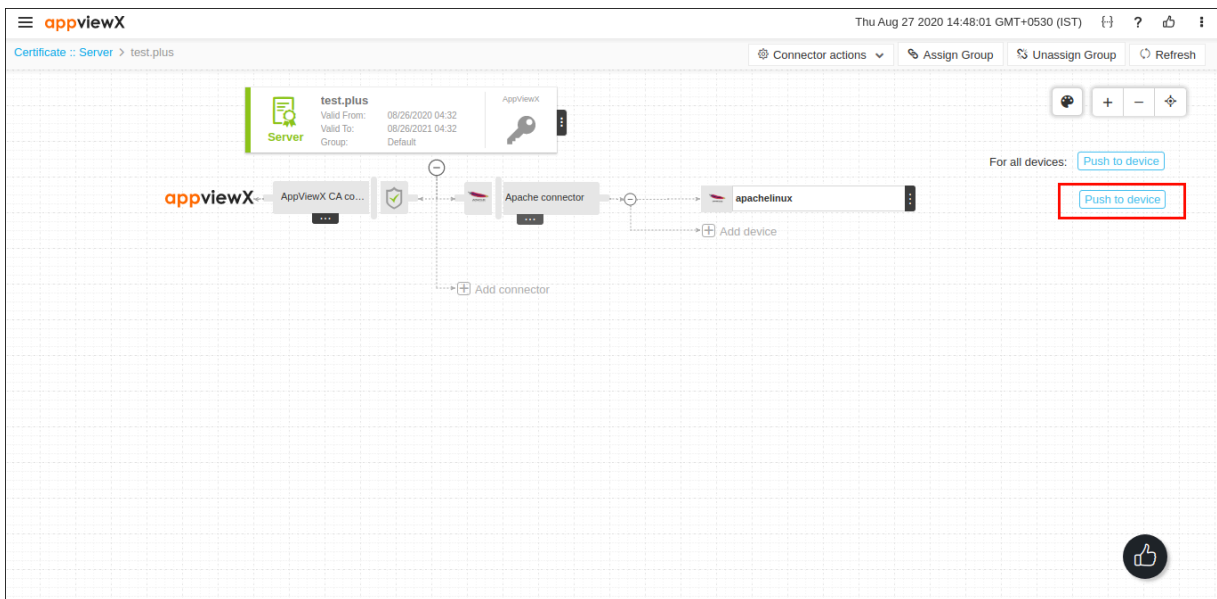
• Error Messages

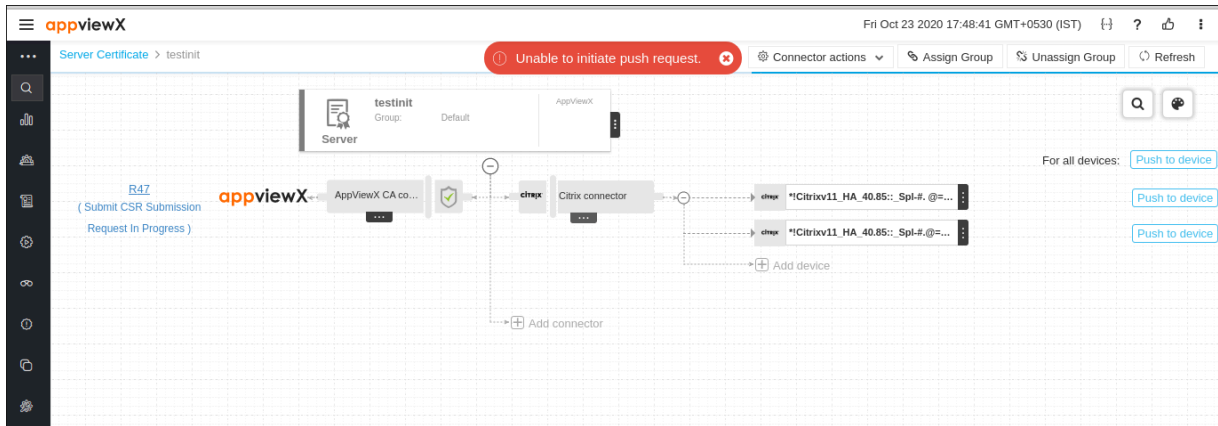
Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	Discovery name is not entered or the length is less than 2 characters.	Enter a valid name with a minimum of 2 characters.
	Interval between batches info. is missing when execution type is sequential.	Provide a time interval between batches in minutes.
Please select a device	No device is selected in the Discover By section.	Select at least one device to discover certificates from.

Issues in Push and Rollback

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**, select **server**.
4. On the top right corner of the page, click **List**.
The **Server Certificate** page is displayed.
5. Click the certificate to be pushed or rolled back.





- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
	Previous work order is in progress and not completed.	Initiate push after previous work order is finished.
	AppConnector might not be in sync.	Synchronize the appConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.

Error Message	Possible Cause	Possible Solution
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.

Troubleshooting Barracuda WAF

- [Overview](#)
- [Issues in Barracuda WAF](#)

Overview

This section helps you deal with the various issues faced by you during the use of Barracuda WAF functionalities.

Issues in Barracuda WAF

- [Issues in Device communication](#)
- [Issue in Discovery](#)
- [Issues in Certificate Push](#)

Issues in Device communication

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.

The **Server Certificate** page is displayed.

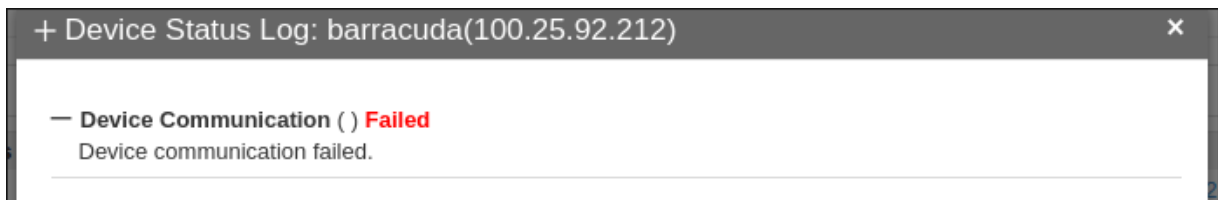
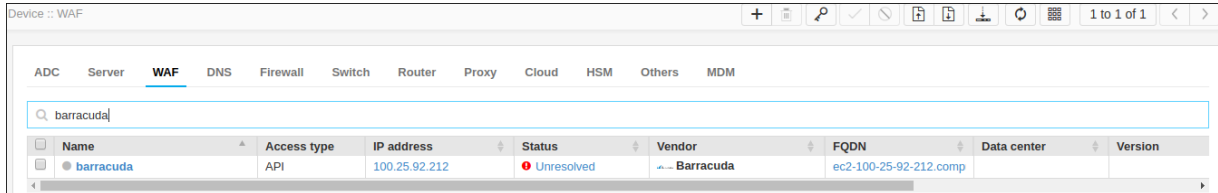
3. From the left pane, expand **Administration** and click **Device Management**.

The **Device Management** page is displayed.

4. On the **Device Management** page, click **WAF** Tab.

5. Select a **Barracuda Device**, click **Status**.

The **Device Communication Status** is displayed.



• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Device communication failed	1. The given credential is incorrect. 2. The given IP/FQDN and Port may be incorrect. 3. Device not reachable.	1. Check and input the correct credential. 2. Check and input the correct IP/FQDN and Port. 3. Ensure the device is up and accessible.

Issue in Discovery

1. Log in to **AppViewX** application with valid credentials.

2. From the left pane, expand the **menu** and click **Cert+**.

The **Server Certificate** page is displayed.

3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.
5. From the dropdown of **Discovery From**, select **Managed WAFs**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

Search...			
Title	Status	Message	Time
Certificate Discovery	Failed	Received failed response for the batch	02/25/2021 18:12:05
OK			

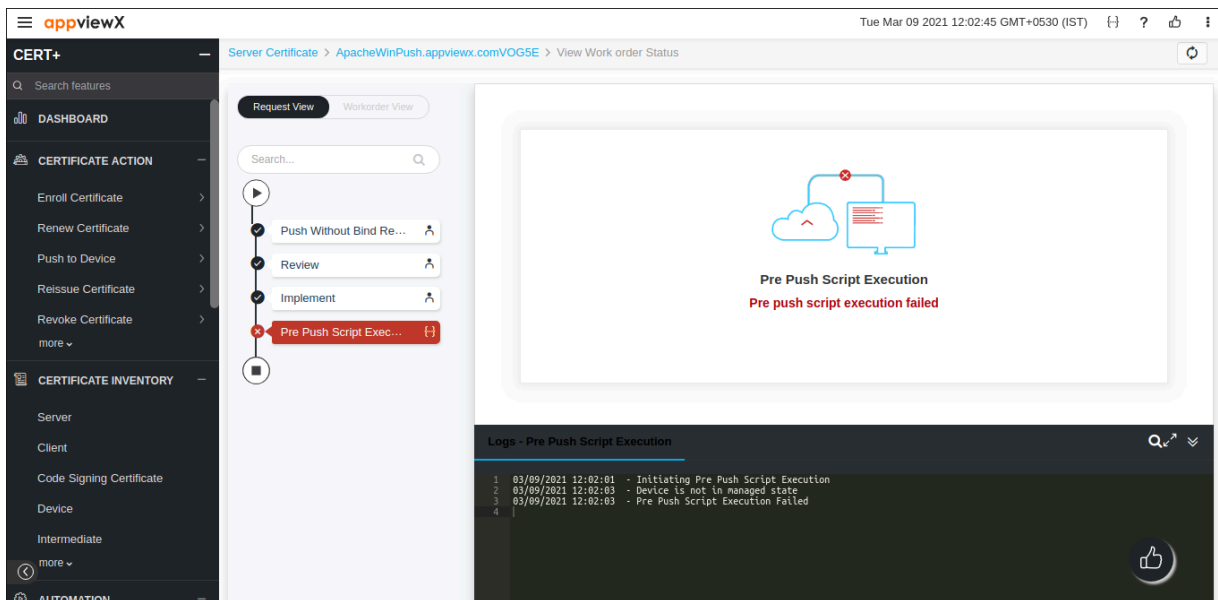
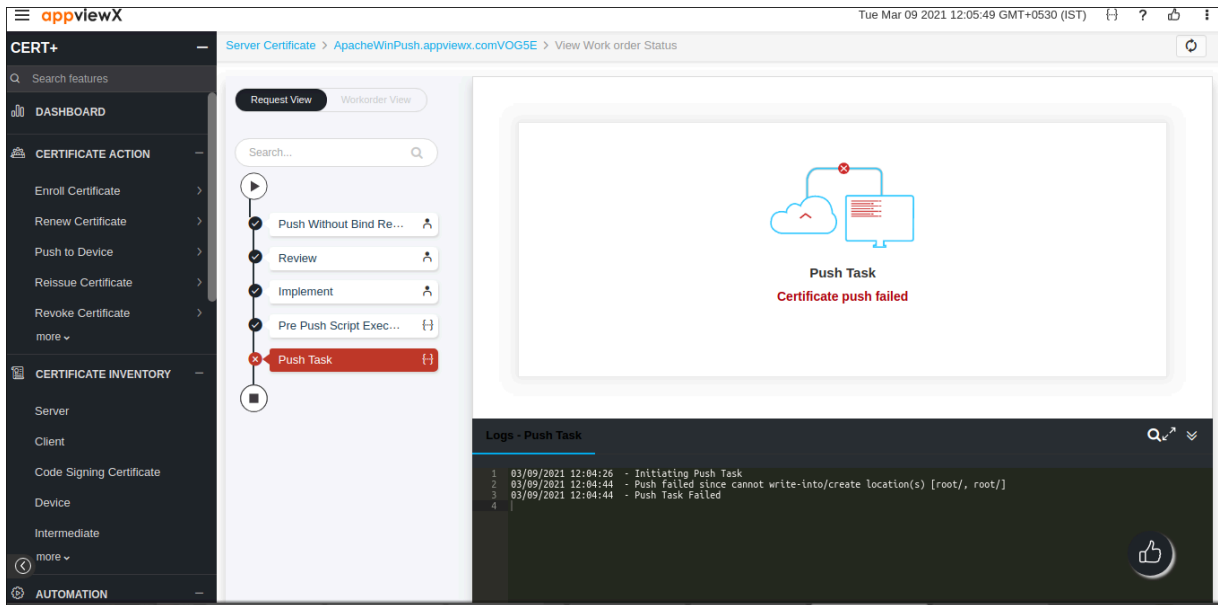
• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Received failed response from batch	1. Device not running or not accessible. 2. No valid certificates available.	1. Ensure target device is up and running. 2. Check the device has valid certificate files.

Issues in Certificate Push

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page will be displayed.
3. From the left pane, expand **Certificate Inventory** menu and select **Server**.
The **Server Certificate** page will be displayed.
4. Select any **Barracuda** server.
A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector actions**, select **Add App Connector**.
6. Push the certificate to the device.



- Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Push failed due to invalid certificate	Push failed when pushing a certificate without key.	Ensure the certificate matches with the key associated in the device on pushing without the key file.
Device is not in managed state	Device is not available in "managed list".	Please check the device status in device inventory.

Troubleshooting Cisco ASA Firewall

- [Overview](#)
- [Issues in Firewall CiscoASA](#)

Overview

This section will guide you to overcome the various issues faced by you during the use of Firewall Cisco ASA and its various functionalities.

Issues in Firewall CiscoASA

- [Issues in Server Addition using AppViewX UI](#)
- [Issues in Device communication](#)
- [Issue in Discovery](#)
- [Issues in Certificate Push](#)
- [Issues in Certificate Bind](#)

Issues in Server Addition using AppViewX UI

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Firewall** Tab.
5. From the icon list at the top right corner, click **Add**.

The **Device Addition** page is displayed.

6. From the **Device Details Section** on the left, click **Cisco**.
7. Fill in the appropriate details.
8. Click **Add**.

- [Error Messages](#)

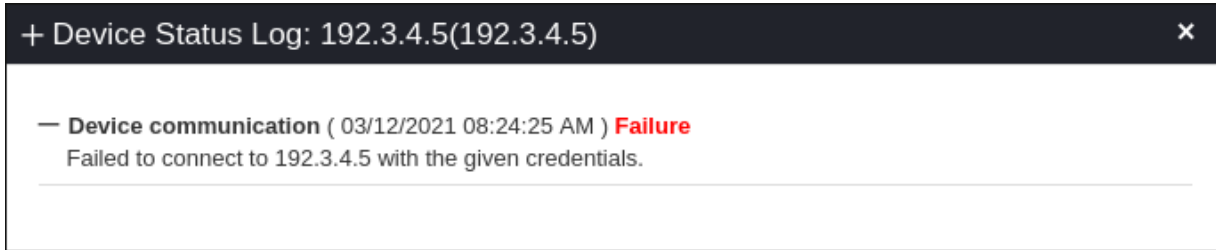
Error Messages

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Device communication

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the Device, click **Status**.
The **Device Communication Status** is displayed.

 ciscoasa	192.168.55.10	gs-cis-pe8.lab.appviewx.r	 Cisco	ASA	9.9(2)	 Managed	9
 192.3.4.5	192.3.4.5	192-3-4-5-host.colocrossl	 Cisco	ASA		 Unresolved	0



- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Failed to connect to <device name> with the given credentials.	1. Device unreachable. 2. Invalid credential. 3. Invalid port.	1. Kindly check if the given IP/FQDN is reachable. 2. Kindly check the credentials provided. 3. Kindly check the port and firewall settings. 4. Kindly ensure the CiscoASA version is supported by AppViewX and has proper privilege to login.

Issue in Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Received failed response from batch	Interfaces are not associated with any trustpoints.	Kindly ensure the interfaces are bounded with required trustpoints. Command to verify SSL-config: show running-config SSL

Issues in Certificate Push

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**.
The **Server Certificate** page is displayed.
4. Click any **Cisco ASA Firewall**.
A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, select **Add App Connector**.
6. Push the certificate to the device.

The screenshot displays the 'Server Certificate' page in the AppViewX application. The breadcrumb navigation at the top reads: 'Server Certificate > gs-cucm-pe1.lab.appviewx.net > View Work order Status'. On the left sidebar, the 'Request View' tab is active, showing a workflow with steps: 'Push and Bind Reque...', 'Review', 'Implement', 'Pre Push Script Exec...', 'Backup Task', and 'Push Task'. The 'Push Task' step is highlighted in red with a failure icon. The main content area shows a diagram of a cloud connected to a server, with a red 'X' indicating failure. Below the diagram, the text reads 'Push Task' and 'Certificate push failed'. At the bottom, a 'Logs - Push Task' section shows the following log entries:

```

1 03/11/2021 08:03:42 - Initiating Push Task
2 03/11/2021 08:05:05 - Cert push got failed due to Error while importing trust certificate.
3 03/11/2021 08:05:05 - Push Task Failed
4

```

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Certificate push failed due to Unsupported bit length.Please provide valid one.	Unsupported bit length.	Kindly ensure the bit length of certificate is supported by ciscoASA
Cert push got failed due to ERROR: Import PKCS12 operation failed	Issues in creating trustpoints	Kindly ensure that the trust points get created successfully.

Issues in Certificate Bind

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**.
The **Server Certificate** page is displayed.
4. Click any **Cisco ASA Firewall**.
A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, select **Edit Connector**.
6. On the **Edit Connector**, select **interfaces** to be associated with the trust point.
7. Push the certificate to the device.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Certificate bind failed due to invalid interface name or error while communicating with device.	Invalid trustpoint.	Kindly ensure the trustpoint is available on the device.

Troubleshooting Cisco CallManager

- [Overview of Cisco CallManager Troubleshooting Guide](#)
- [Issues in Cisco CallManager](#)

Overview of Cisco CallManager Troubleshooting Guide

This section will guide you to overcome the various issues faced by you during the use of Cisco CallManager and its various functionalities.

Issues in Cisco CallManager

- [Issues in Server Addition using AppViewX UI](#)
- [Issues in Device communication](#)
- [Issue in Discovery](#)
- [Issues in CSR generation at Endpoint](#)
- [Issues in Certificate Push](#)
- [Issues in Certificate Bind](#)

Issues in Server Addition using AppViewX UI

1. Log in to **AppViewX** application with valid credentials.
 2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
 3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
 4. On the **Device Management** page, click **Server** Tab.
 5. From the icon list at the top right corner, click **Add**.
The **Device Addition** page is displayed.
 6. From the **Device Details Section** on the left, click **CISCO**.
 7. Click **CUCM**.
 8. Fill in the appropriate details.
 9. Click **Add**.
- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A Cisco CallManager device exists in inventory with the same name.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Device communication

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**.
The **Device Communication Status** is displayed.

 cucm	gs-cucm-pe1.lab.appview	dc2	 Managed	 Cisco CallManager	11.5.1.15900-18	22	Manual entry
 cucm_invalid_port	gs-cucm-pe1.lab.appview	dc2	 Unresolved	 Cisco CallManager		500	Manual entry

+ Device Status Log: cucm_invalid_port(gs-cucm-pe1.lab.appviewx.net)

— **Device communication** (03/11/2021 06:38:02 AM) **Failure**

Communication to gs-cucm-pe1.lab.appviewx.net has failed.

Caused by: Error while establishing SSH connection

Possible Remediations:

1. Kindly check if the given IP/FQDN is reachable.
2. Kindly check the credentials provided.
3. Kindly check the port and firewall settings.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Communication to <hostname name> has failed.	1. Device unreachable. 2. Invalid credential. 3. Invalid port.	1. Kindly check if the given IP/FQDN is reachable. 2. Kindly check the credentials provided. 3. Kindly check the port and firewall settings.
Cisco Tomcat service is not active	Cisco Tomcat service is not in an up and running state.	Kindly restart the Cisco Tomcat Service. Command to verify the status of services is: <pre>utils service list</pre>

Issue in Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Received failed response from batch	Required Services may not be in an up and running state.	Please ensure the supported services are up and running state and services are associated with SSL configs.

Error Message	Possible Cause	Possible Solution
		Services supported by AppViewX : Cisco tomcat Command to verify the status of services is: utils service list

Issues in CSR generation at Endpoint

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab.
The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, click correct **Category**.
7. From the **Vendor** dropdown, click **Cisco CallManager**.
A list of devices will be generated in the **Devices dropdown**.

• Error Messages

Error Messages

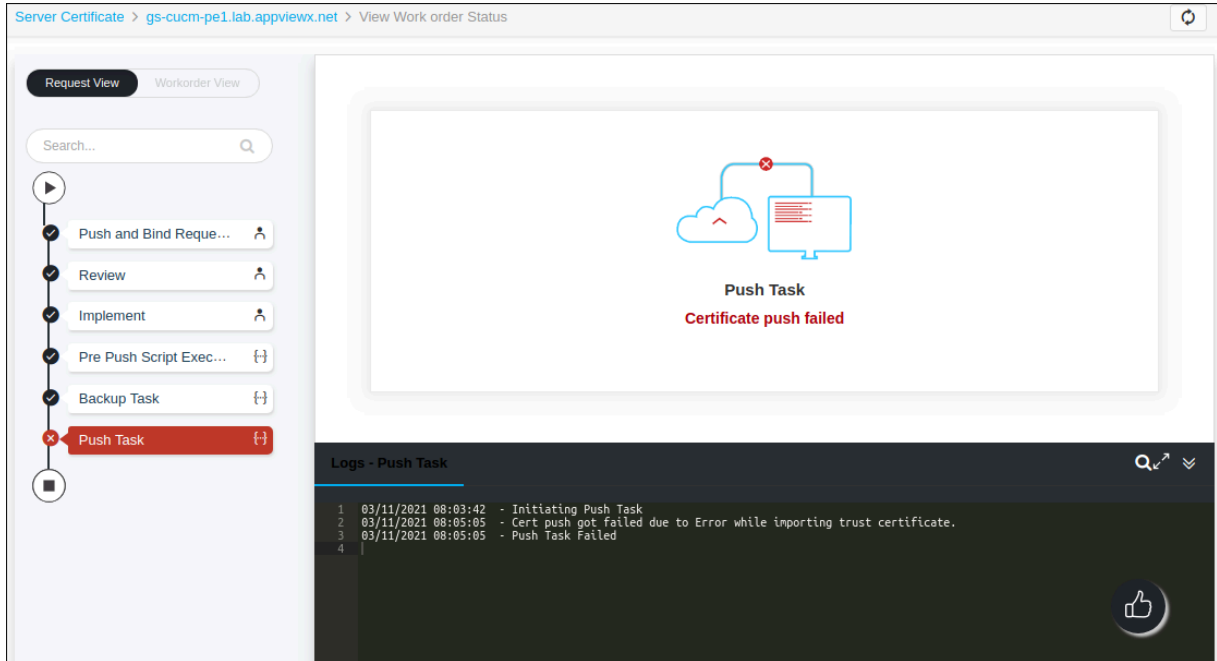
Error Message	Possible Cause	Possible Solution
CUCM CSR gen command failed	Command execution may fail.	Kindly ensure all CSR gen commands are executed properly.

Issues in Certificate Push

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and Click **Server**.
The **Server Certificate** page is displayed.
4. Click any **Server**.

A holistic view of the **Certificate** will be displayed.

5. From the dropdown of **Connector Actions**, click **Add App Connector**.
6. Push the certificate to the device.



• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Cert push got failed due to Error while importing server certificate.	- The certificate should be issued from CSR generated by device. - CUCM will not allow to push the same cert again.	- Kindly ensure the certificate issued by the CSR generated from Device.CUCM will not support to push any other certs. - CUCM will delete the CSR information from the device on successful cert push. Kindly ensure you are pushing the newly issued certificate and respective CSR information for the same should be available in the device.
Cert push got failed due to	CA/Intermediate cert with the same	AppViewX will not overwrite the existing CA configurations. Kindly delete/rename the old certificates to proceed with push.

Error Message	Possible Cause	Possible Solution
Error while importing trust certificate.	name may already exist in the device.	

Issues in Certificate Bind

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and Click **Server**.
The **Server Certificate** page is displayed.
4. Click any **Server**.
A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, click **Add App Connector**.
6. On successful certificate push, Select the services to be restarted.
7. Push the certificate to the device.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Cert bind got failed.Cause : Service restart failure.	Connection timeout or Invalid Services	Kindly check if the device is in a reachable state to execute the command.

Troubleshooting Common Functionality of Servers

- [Overview](#)
- [Issues in Common Functionality of Servers](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when dealing with the common functionality of servers. The guide will give more troubleshooting processes on issues

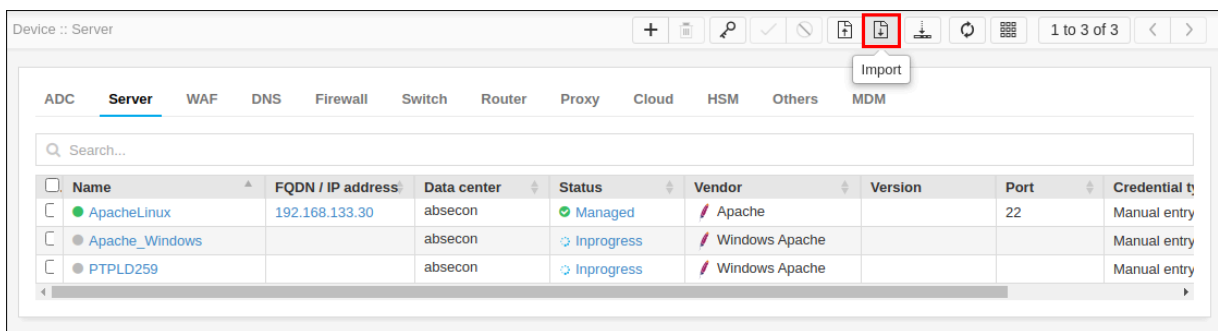
encountered during handling of devices like addition using import option, adding to credential list, including the server in managed servers, unmanaging the server or server export.

Issues in Common Functionality of Servers

- [Issues in Device Addition using Import Option](#)
- [Issues in Credential List Addition](#)
- [Issues in Server Unmanage functionality](#)
- [Issues in Server Manage functionality](#)
- [Issues in Server Export](#)

Issues in Device Addition using Import Option

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device and click **Import**.



- [Error Messages](#)

Error Messages

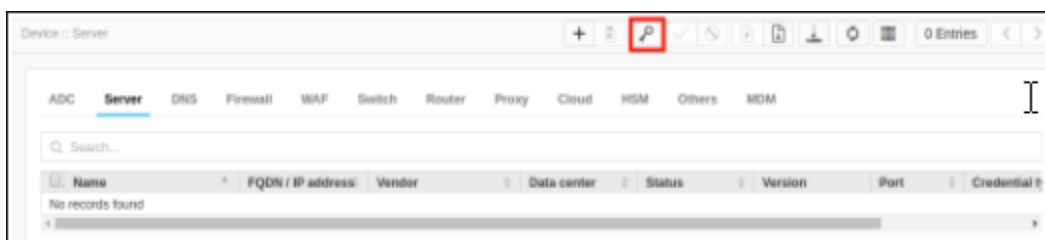
Error Message	Possible Cause	Possible Solution
Invalid file type. Please select a valid file format (csv / xlsx / xls).	File type uploaded is not in expected format.	Supported file types are csv/xls/xlsx only. Check for the uploaded file extension.
Maximum five files allowed, please delete any completed file.	In the file history of the import page maximum 5 files can be maintained.	Delete any of the parsed/completed files to upload a new one.

Invalid file type. Please select a valid file format (csv / xlsx / xls).

Maximum five files allowed, please delete any completed file.

Issues in Credential List Addition

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** Page, click **Server** Tab.
5. Select the device and click **Credential**.
The **Credentials List** page will be displayed.



- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid details	Mandatory credential details are missing.	Provide all the mandatory details to store the credential.
credentials already exist.	Credential List with the same name already exists.	Provide a unique name to each credential list.
Invalid file format. Accepted formats are .pem and .txt.	The Identity Key file uploaded is not in the correct format.	Provide key file with correct format (.pem or .txt)

Invalid details

The screenshot shows the 'Add credential' form in the AppViewX interface. A red error banner at the top reads 'Invalid details'. The form fields are as follows:

- Credential name:** Empty field with a red asterisk and an 'x' icon.
- User name:** Empty field with a red asterisk and an 'x' icon.
- Credential type:** Radio buttons for 'Password' (selected) and 'Identity key'.
- Password:** Field with masked characters (dots) and a red asterisk.
- Secondary password:** Empty field.

Buttons for 'Save' and 'Cancel' are at the bottom.

Credentials already exist

The screenshot shows the 'Add credential' form in the AppViewX interface. A red error banner at the top reads 'credentials already exist.'. The form fields are as follows:

- Credential name:** Field containing 'tomcatKeyWithoutPassphrase' with a red asterisk.
- User name:** Field containing 'admin' with a red asterisk.
- Credential type:** Radio buttons for 'Password' (selected) and 'Identity key'.
- Password:** Field with masked characters (dots) and a red asterisk.
- Secondary password:** Empty field.

Buttons for 'Save' and 'Cancel' are at the bottom.

Invalid file format. Accepted formats are .pem and .txt

Device > Modify > Modify credential

Invalid file format. Accepted formats are .pem and .txt

appviewX

Credential details

* Credential name: tomatKeyWithoutP

* User name: admin

Credential type: ☐ Password ☒ Identity key

* Identity key: [Browse]

Passphrase: []

[Update] [Cancel]

Issues in Server Unmanage functionality

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device and click **Unmanage**.

appviewX

Mon Mar 01 2021 14:52:20 GMT+0530 (IST)

Device :: Server

Unmanage

Name	FQDN / IP address	Data center	Status	Vendor	Version	Port	Credential type
ApacheLinux	192.168.133.30	absecon	Managed	Apache		22	Manual entry
Apache_Windows		absecon	Inprogress	Windows Apache			Manual entry
PTPLD259		absecon	Inprogress	Windows Apache			Manual entry

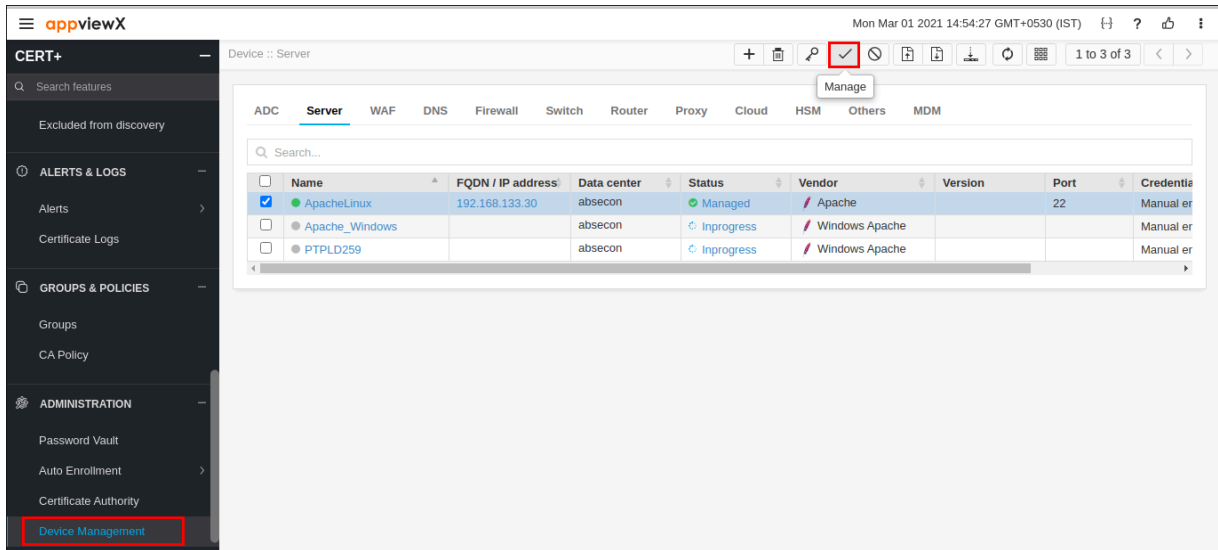
- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
The selected devices are already unmanaged. The operation cannot be performed.	Device cannot be unmanaged because it is already in the unmanaged state.	Manage the device(s) in an unmanaged state before performing action.
Fetch config not allowed for Unmanaged devices	Fetch config operation is only allowed on the devices which are in managed state.	Manage the device(s) in an unmanaged/in-progress state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

Issues in Server Manage functionality

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click on **Server** Tab.
5. Select the device and click **Manage**.



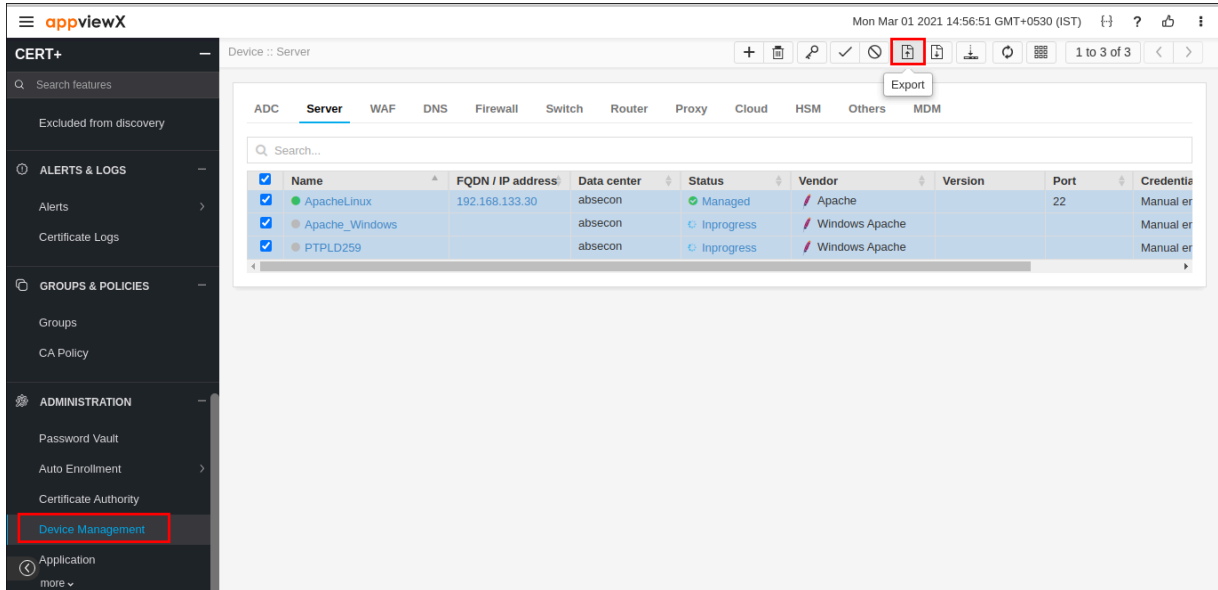
• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
The selected devices are managed. The operation cannot be performed.	Device cannot be managed because it is already in the managed state.	Unmanage the device(s) in the managed state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

Issues in Server Export

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. Click on **Server** Tab on the **Device Management** Page.
5. Select the device and click **Export**.



- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Exception while exporting	General failure - Unable to create file on the local system due to permission issue.	Provide access to be able to create the file on the local system. (For example, check the directory where it is trying to export and give access to AppViewX for that directory.)
	Unable to fetch device list from the database.	Make sure the database is running and has correct data.

Troubleshooting Data Power Server

- [Overview](#)
- [Issues in Data Power Server](#)

Overview

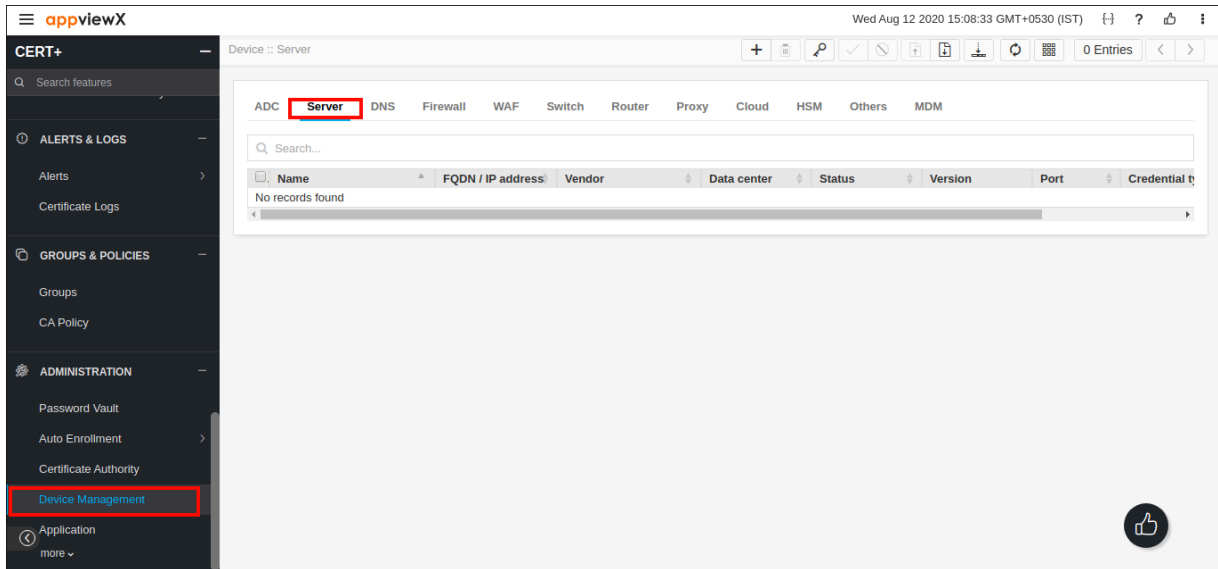
This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with the Data Power server.

Issues in Data Power Server

- [Issues in Data Power Server Addition using AppViewX UI](#)
- [Issues in Communicating to Data power Server](#)
- [Issues in Accessing Server](#)
- [Issues in Certificate Discovery](#)
- [Issues in Push and Rollback](#)

Issues in Data Power Server Addition using AppViewX UI

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. From the icon list at the top right corner, click **Add**.
The **Device Addition** page is displayed.
6. From the **Device Details Section** on the left, click **Data Power**.
7. Fill in the appropriate details.
8. Click **Add**.



Server details

* Server type

* Server name

* IP address/FQDN

Data center

* Rest port

Cert sync ☒ Managed ☐ Monitored ☐ Ignored

Credentials

* Credential type

* Username

* Password

- [Error Messages](#)

Error Messages

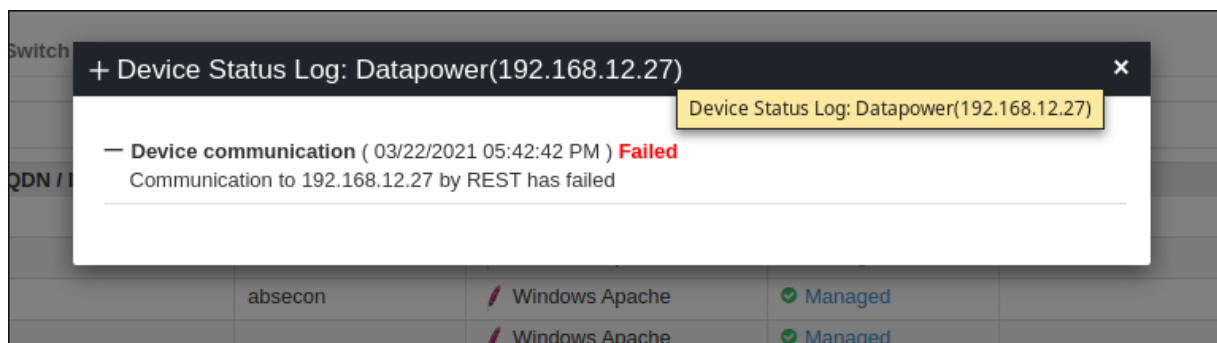
Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Communicating to Data power Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**.

The **Device Communication Status** is displayed.

☐	Apache_Windows_SSM		absecon	Windows Apache	Unresolved		Manual entry	
☐	Datapower	192.168.12.27	absecon	IBMDataPower	Unresolved		Manual entry	5558
☐	IBMClient_Windows		absecon	Windows IBMClient	Managed	9.0.0.2	Manual entry	



- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-', '_', ':', '*', ' ', '!' and spaces.
Device IP/FQDN cannot be null or empty.	Device IP/FQDN is empty.	Provide device IP/FQDN as it is a mandatory field.
Invalid device IP/FQDN address.	IP/FQDN address is not valid.	Provide valid IP/FQDN address.
Domain fetch has failed.	Domain not configured in Data Power	Check manually if domains are configured.

Issues in Accessing Server

Access Issues might be reproduced when communicating with servers while discovering or fetching domains. These errors can be collected either from logs, API responses, or in the status field for the particular server.

Error Message	Possible Cause	Possible Solution
Rest communication failed	Unable to access the Rest APIs exposed by Data Power	Login via Postman to check if the APIs are accessible

Issues in Certificate Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	- Discovery name is not given or length is less than 2 characters. - Interval between batches info. is missing when execution type is sequential.	- Enter a valid name with a minimum of 2 characters. - Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “ Discover By ” section.	Select at least one device to discover certificates from.

Issues in Push and Rollback

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.

The **Server Certificate** page is displayed.

- From the left pane, expand **Certificate Inventory** and click **Server**.

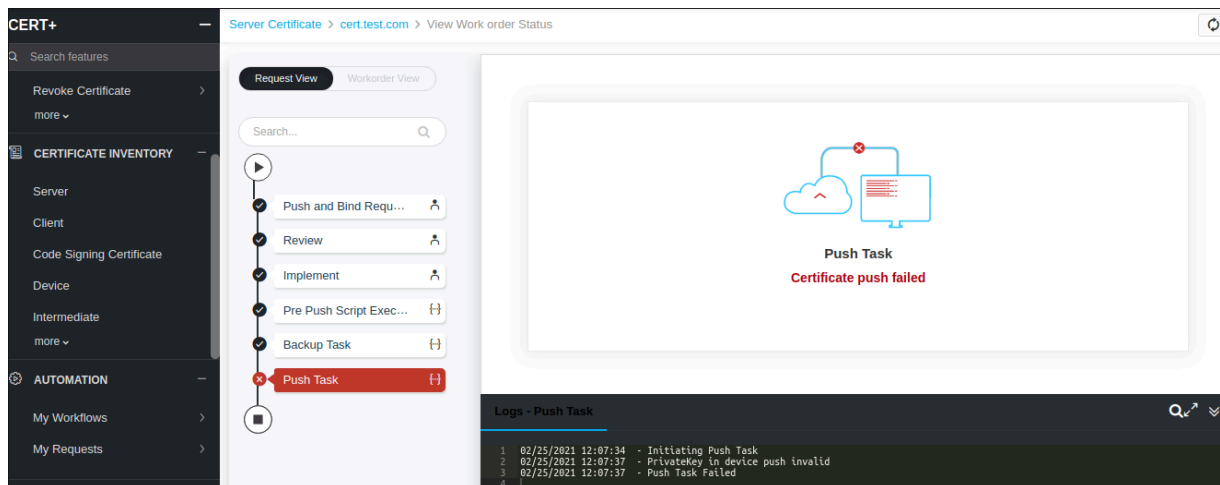
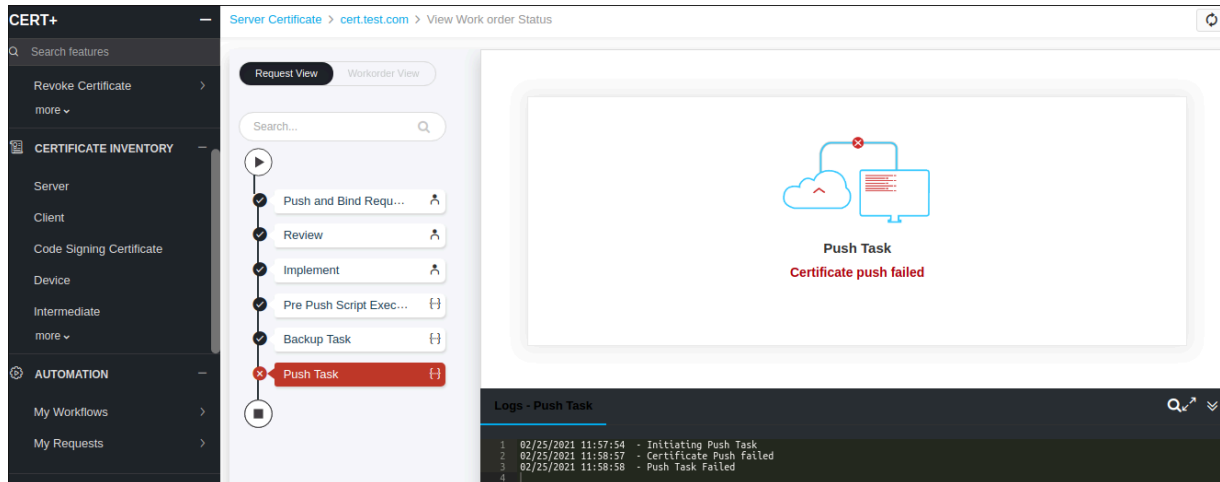
The **Server Certificate** page is displayed.

- Click any **Data Power** server.

A holistic view of the **Certificate** will be displayed.

- From the dropdown of **Connector Actions**, select **Add App Connector**.

- Push the certificate to the device.



• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Certificate Push failed	User has restricted access to the store to push the certificate in the application connector	Kindly ensure the user has access to the store to push the certificates to.

Troubleshooting F5 WAF

- [Overview](#)
- [Supported Web Browsers](#)
- [Issues in F5 WAF](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using the F5 WAF functionalities. This guide will give more troubleshooting processes on F5 WAF certificate config fetch, discovery, CSR creation, backup, push, bind, rollback, and other actions associated with F5 WAF.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in F5 WAF

- [Issues in Fetch Config](#)
- [Issues in Discovery](#)

- [Issues in CSR Generation](#)
- [Issues in F5 WAF Backup, Push, Bind, and Rollback](#)

Issues in Fetch Config

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **WAF** Tab.
5. Select the device, click **Fetch Config**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Authentication failed for the device	Invalid credentials specified for the device.	Provide valid credentials for the device.
Failed to fetch partitions from the device	Partition fetch failed.	1. Check the device partitions. 2. Please check the associated error message.
SSH connection failed	Unable to establish the SSH connection.	Please ensure that the device can be connected via SSH from AppViewX.

Issues in Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	Discovery name is not given or length is less than 2 characters.	Enter a valid name with a minimum of 2 characters.
	Interval between batches info. is missing when execution type is sequential.	Provide a time interval between batches in minutes.
Please select a device	No device is selected in the Discover By section.	Select at least one device to discover certificates from.
Authentication failed for the device	Invalid credentials specified for the device.	Provide valid credentials for the device.
Failed to fetch partitions from the device	Partition fetch failed.	1. Check the device partitions. 2. Please check the error message associated.
SSH connection failed	Unable to establish the SSH connection.	Please ensure that the device can be connected via SSH from AppViewX.

Issues in CSR Generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab.
The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the **Category dropdown**, click **Firewall**.
7. From the dropdown, click the correct **Vendor**.
A list of devices will be generated in the **Devices dropdown**.
8. To generate **CSR**, select the F5 device.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Authentication failed for the device	Invalid credentials specified for the device	Provide valid credentials for the device.
SSH connection failed	Unable to establish the SSH connection.	Please ensure that the device can be connected via SSH from AppViewX.
CSR Generation using HSM on this device version is not supported.	Version not supported.	Please use the supported version device to create CSR using HSM. Supported versions are v13 and v12.
1) CSR content unavailable in device 2) Requested CSR is not available in device 3) Csr could not be fetched	CSR content unavailable on device.	For some reasons CSR creation has failed, please check the logs to reproduce.
CSR already exists in this scope with the same Key reference name	The name is already used on the device.	Please use a different name.
Csr generation is device failed	CSR generation has failed.	CSR generation has failed. Please refer to the associated error message.
Thales HSM is not installed in the device. Please install and try again.	Thales is not installed in the device.	Please install Thales HSM and try again.
Invalid module. Please specify the valid module and try again.	Invalid module specified.	Specify a valid module and try again.
The CSR <name> was not found in the device.	CSR content is not available in the name specified.	Please check the name in the CA connector.

Error Message	Possible Cause	Possible Solution
NetHSM private key is not available/installed in device	NetHSM private key is not available/installed in the device.	Please install NetHSM private key on the device.

Issues in F5 WAF Backup, Push, Bind, and Rollback

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**, select **Server**.
4. At the top right corner of the page, click **List**.
The **Server Certificate** page is displayed.
5. Click the certificate to be pushed or rolled back.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
	Previous work order is in progress and not completed.	Initiate push after previous work order is finished.
	AppConnector might not be in sync.	Synchronize the appConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state.	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.

Error Message	Possible Cause	Possible Solution
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Authentication failed for the device	Invalid credentials specified for the device.	Provide valid credentials for the device.
SSH connection failed	Unable to establish the SSH connection.	Please ensure that the device can be connected via SSH from AppViewX.
Invalid profile type	Specified profile type is not supported.	Please use client-SSL or server-SSL.
Certificate fetch failed	Certificate fetch failed.	Check the error message associated to know more about the problem.
Certificate already exists	Certificate is already available with the same.	Either change the name or enable overwrite in the application connector.
Key already exists	Key is already available with the same.	Either change the name of the key or enable overwrite in the application connector.
Certificate is expired	Certificate is expired.	Push the certificate which is currently valid.
Unknown certificate algorithm	Unknown certificate algorithm.	Push the certificates only with RSA or EC.
certificate is not yet valid	Certificate valid from value is greater than the current time.	Only valid certificates only can be pushed.

Troubleshooting Fortigate Firewall

- [Overview](#)
- [Supported Web Browsers](#)
- [Issues in Fortigate Firewall](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using the Fortigate firewall in CERT+ functionalities. This guide will give more troubleshooting processes on Fortigate firewall certificate config fetch, discovery, CSR creation, backup, push, bind, rollback, and other actions associated with Fortigate firewall.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Fortigate Firewall

- [Issues in Fetch Config](#)
- [Issues in Discovery](#)

- [Issues in CSR Generation](#)
- [Issues in Fortigate Firewall Backup, Push, Bind and Rollback](#)

Issues in Fetch Config

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Firewall** Tab.
5. Select the device, click **Fetch Config**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Error occurred in command execution - <Error message>	Error occurred in command execution	Command execution has failed. Please refer to the error message associated with this.

Issues in Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	Discovery name is not given or length is less than 2 characters.	Enter a valid name with a minimum of 2 characters.
	Interval between batches info. is missing when execution type is sequential.	Provide a time interval between batches in minutes.
Please select a device	No device is selected in the Discover By section.	Select at least one device to discover certificates from.
Error occurred in command execution - <Error message>	Error occurred in command execution.	Command execution has failed. Please refer to the associated error message.

Issues in CSR Generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab.
The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the **Category** dropdown, click **Firewall**.
7. Click correct **Vendor** from the dropdown.
A list of devices will be generated in the **Devices dropdown**.
8. For generating **CSR**, select device as **Fortigate**.
9. Click **Add**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Exception occurred while getting Api key - Invalid credentials.	Credentials may be invalid.	Provide valid credentials.
Unsupported Key type provided	Unsupported key type is selected.	Please select RSA or EC.
Csr name exists in the device, and cannot be overwritten.	Name is already used in the device.	Please use a different name.
Csr generation is device failed	CSR generation has failed.	CSR generation has failed. Please refer to the associated error message.

Issues in Fortigate Firewall Backup, Push, Bind and Rollback

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**, select **Server**.
4. At the top right corner of the page, click **List**.
The **Server Certificate** page is displayed.
5. Click the certificate to be pushed or rolled back.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
	Previous work order is in progress and not completed.	Initiate push after previous work order is finished.

Error Message	Possible Cause	Possible Solution
	AppConnector might not be in sync.	Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state.	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Certificate content is mandatory parameter	Certificate content should be available.	Please specify certificate content in the request.
Intermed certificate content is mandatory for pushing CA certificate	Intermediate certificate content should be available.	Please specify intermediate certificate content in the request.
Root certificate content is mandatory for pushing CA certificate	Root certificate content should be available.	Please specify root certificate content in the request.
Certificate name is mandatory parameter	Certificate file name is mandatory.	Please specify the certificate file name in the connector.

Error Message	Possible Cause	Possible Solution
Profile details are missing in Application connector	Profile details are missing.	Please specify profile details in the request.
Private key password is mandatory parameter	Private key password is mandatory.	Specify private key password in the connector.
Given certificate name does not exist in a device with a private key. Certificate with private key should exist either in device or AppViewX	Private key not available in the certificate.	Certificate should be pushed with the private key to bind with the profile.
Root certificate name already exists in ca store, Cannot overwrite until Overwrite is enabled in Connector	Overwrite is not enabled in the application connector.	Enable overwrite option in the application connector.
Intermediate certificate with name: <name> already exists in ca store, Cannot overwrite until Overwrite is enabled in Connector	Overwrite is not enabled in the application connector.	Enable overwrite option in the application connector.
Certificate name already exists in inventory, Cannot overwrite until Overwrite is enabled in Profile connector	Certificate with the same name already exists on the device.	Please change the certificate name or enable overwrite in the application connector.
Certificate is expired	Certificate is expired.	Push the certificate which is currently valid.
Unknown certificate algorithm	Unknown certificate algorithm.	Push the certificates only with RSA or EC.
certificate is not yet valid	Certificate valid from value is greater than the current time.	Only valid certificates can be pushed.

Troubleshooting HP ILO

- [Overview](#)
- [Issues in HP ILO](#)

Overview

This section will guide you to overcome the various issues faced by you during the use of HP ILO and its various functionalities.

Issues in HP ILO

- [Issues in Device communication](#)
- [Issues in Certificate Discovery](#)
- [Issues in CSR generation at Endpoint](#)
- [Issues in Certificate Push](#)

Issues in Device communication

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**.

The **Device Communication Status** is displayed.

ilo	1.2.3.4	dc2	Unresolved	hp ILO		Manual entry
ilo.appviewx.net	ilo.appviewx.net	dc2	Managed	hp ILO	iLO Standard	Manual entry

The screenshot shows the AppViewX interface with a modal window titled "+ Device Status Log: ilo(1.2.3.4)". The modal displays a message: "Device communication (03/01/2021 07:32:08 PM) Failure" and "Communication to 1.2.3.4 has failed". In the background, a table lists various devices with their status and details.

Name	FQDN	Status	OS	OS Version	Credential type
105 IIS		Managed	Microsoft Server	Microsoft Windows ...	Manual entry
107 MS		Managed	Microsoft PC	Microsoft Windows ...	Manual entry
108 MSE		Managed	Microsoft Server	Microsoft Windows ...	Manual entry
212 pc		Managed	Microsoft PC	Microsoft Windows ...	Manual entry
228		Managed	Microsoft Server	Microsoft Windows ...	Manual entry
228 PC		Managed	Microsoft PC	Microsoft Windows ...	Manual entry
PTPLD259		Managed	Windows Apache		Manual entry
ilo	1.2.3.4	Unresolved	hp ILO		Manual entry

- [Error Messages](#)

Error Messages

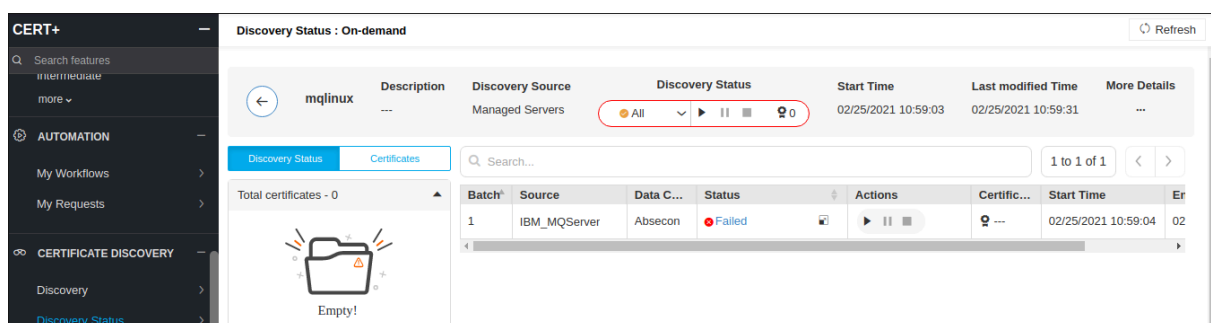
Error Message	Possible Cause	Possible Solution
Communication to <ip/fqdn> has failed.	IP/FQDN provided is not reachable. Credentials not valid.	Check if the provided IP/FQDN is correct Check if the provided username and password for device addition is correct The HPILO python package is not installed properly in AppViewX VM.

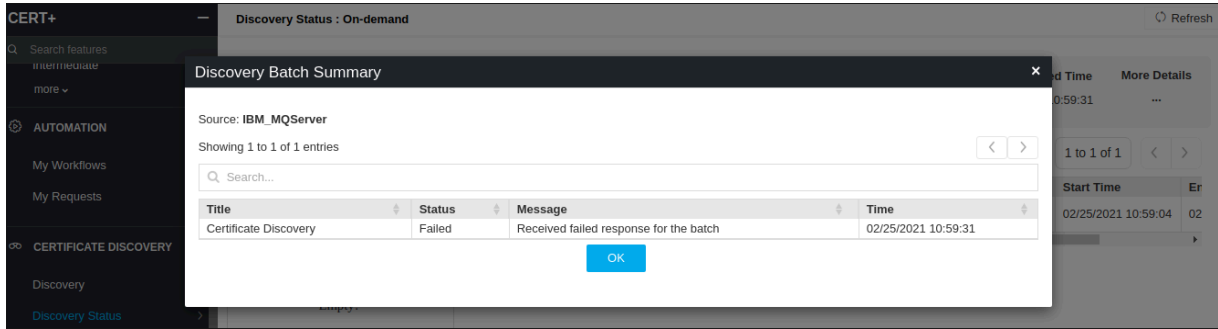
Issues in Certificate Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.





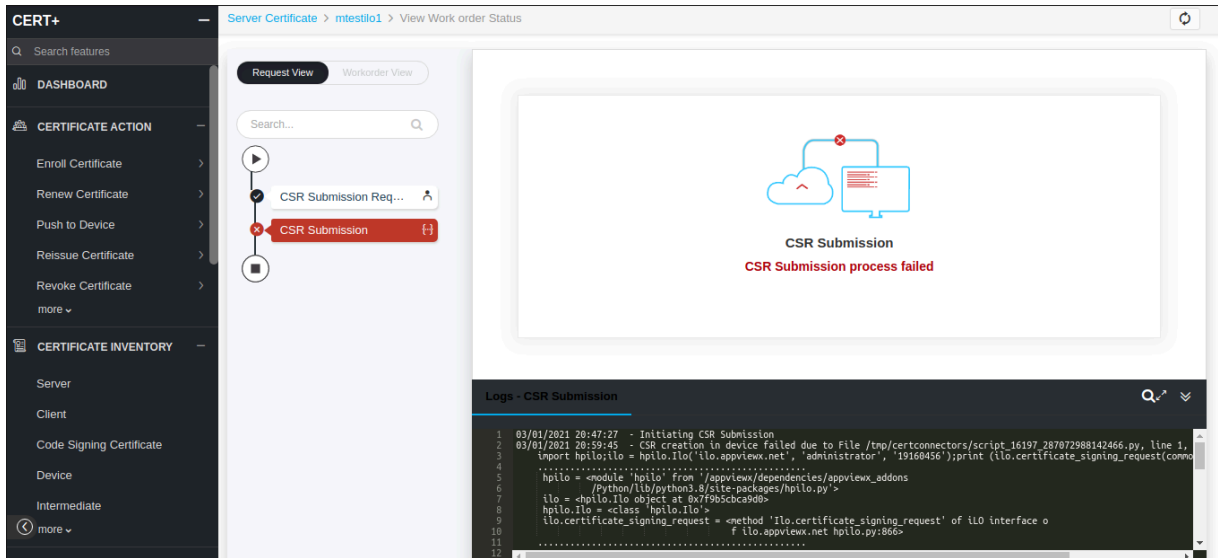
- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Received failed response from batch	ILO portal is not up and running Network issues in reaching the portal	Kindly ensure the ILO web portal is up and running. Kindly ensure a proper identity certificate is associated with the web portal

Issues in CSR generation at Endpoint

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab.
The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, click correct **Category**.
7. From the **Vendor** dropdown, click **ILO**.
A list of devices will be generated in the **Devices dropdown**.



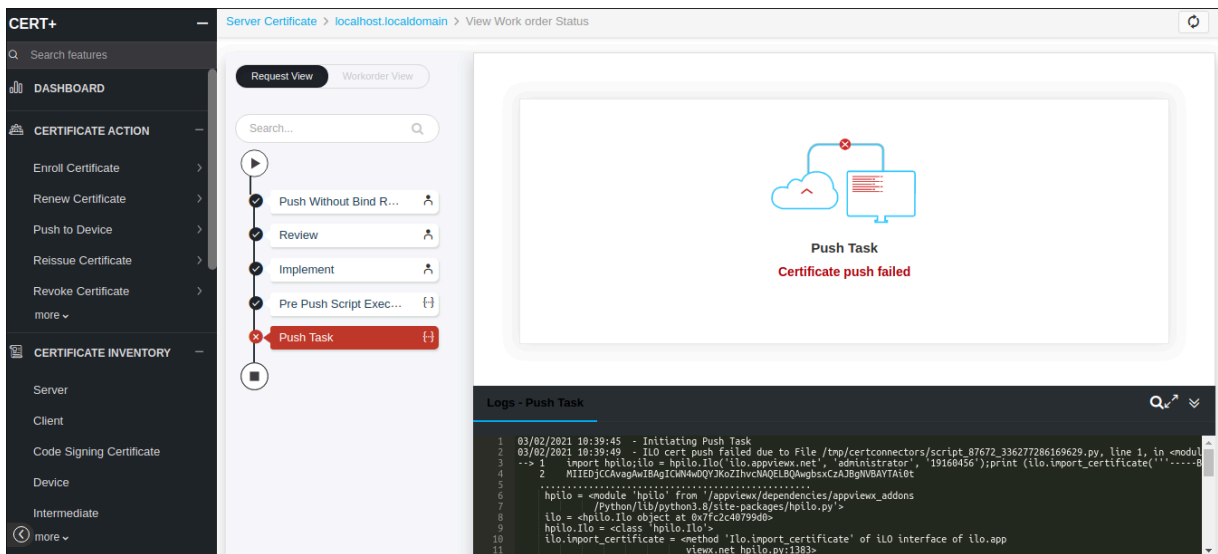
- Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
CSR generation failed. 03/01/2021 20:59:45 - CSR creation in device failed due to File /tmp/certconnectors/script_16197_287072988142466.py, line 1, in <module> <pre>import hpilo;ilo = hpilo.Ilo('ilo.AppViewX.net', 'administrator', '19160456');print (ilo.certificate_signing_request(common_name='mtestilo1'));</pre> IloGeneratingCSR: The iLO subsystem is currently generating a Certificate Signing Request(CSR), run script after 10 minutes or more to receive the CSR. 03/01/2021 20:59:45 - CSR Submission Failed	1. Input parameters might not be valid for the CSR request. 2. Multiple CSR requests might be triggered within a short span of time.	Kindly ensure the CSR parameters are configured properly. Kindly ensure multiple CSR requests are not submitted to the same device in any mode. Kindly ensure we keep at least 15mins interval between CSR request submission else the response for the previous request is triggered before submitting the next request.

Issues in Certificate Push

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**.
The **Server Certificate** page is displayed.
4. Click any **ILO device**.
A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, select **Add App Connector**.
6. Push the certificate to the device.



• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Certificate Push failed 03/02/2021 10:39:49 - ILO cert push failed due to File /tmp/certconnectors/script_87672_336277286169629.py, line 1, in <module>	Certificate is not generated with CSR from device	Kindly ensure the certificate is signed with a CSR request generated from the target device.

Error Message	Possible Cause	Possible Solution
<pre>--> 1 import hpilo;ilo = hpilo.Ilo('ilo.AppViewX.net', 'administrator', '19160456');print (ilo.import_certificate("-----BEGIN CERTIFICATE----- IloError: Invalid certificate common name 03/02/2021 10:39:49 - Push Task Failed</pre>		

Troubleshooting IBMClient Linux

- [Overview](#)
- [Issues in IBMClient Linux](#)

Overview

This section will guide you to overcome the various issues faced by you during the use of IBMClient Linux and its various functionalities.

Issues in IBMClient Linux

- [Error Messages](#)
- [Issues in Device communication](#)
- [Issue in Discovery](#)
- [Issues in CSR generation at Endpoint](#)
- [Issues in Certificate Push](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Communication to <hostname> failed	Gateway agent not reachable. Device not reachable from the gateway agent GSKit is not installed on any given device.	Ensure gateway is configured properly and the APIs are accessible from AppViewX. Ensure device and gateway agent are in the same domain and device is accessible from gateway agent. Please ensure GSKit is installed properly.

Error Message	Possible Cause	Possible Solution
Communication to <hostname> failed Device version fetch has failed.	Hostname or Credentials configured is wrong	Ensure hostname and the device credentials configured while device addition is valid.

Issues in Device communication

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server Tab**.
5. Select the device, click **Status**.

The **Device Communication Status** is displayed.

	IBMClient_Windows	absecon	Unresolved	Windows IBMClient		Manual entry
	IBMClient_wind	absecon	Unresolved	Windows IBMClient		Manual entry

+ Device Status Log: IBMClient_wind
×

— **Device communication** (03/03/2021 04:01:05 PM) **Failure**

Communication to PTPLD259 has failed

— **Device Version** (03/03/2021 04:01:05 PM) **Failure**

Device version fetch has failed

+ Device Status Log: IBMClient_Windows
×

— **Device Communication** () **Failure**

Device communication failed.

Issue in Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

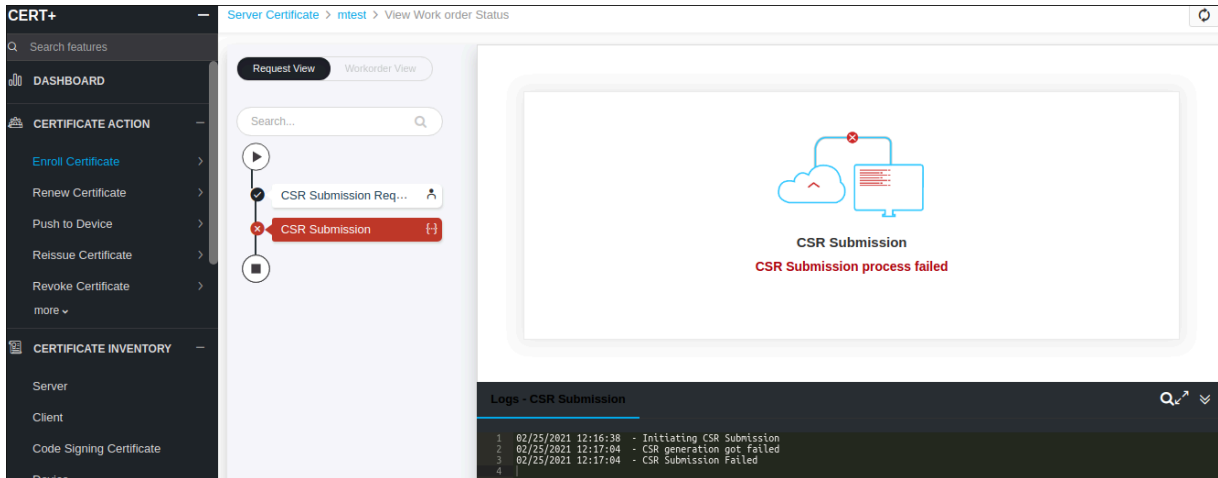
• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Received failed response from batch	No valid KDB/keystore files available in the given path.	Ensure the given certificate location has a valid KDB/keystore and KDB/keystore has certs.
Discovery completed successfully. (with 0 certs even if valid certs exist in given path)	1. Respective Keystores password is not added in Password Vault to parse certs. 2. User may not have read permission to parse certs	1. Please enter the password of keystores in the Password Vault to parse certs. 2. Please ensure the user has appropriate permission to read files.

Issues in CSR generation at Endpoint

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab.
The **Enroll Server Certificate** page is displayed.
5. Select **End Point** as **CSR Generation Source** option.
6. From the dropdown, click correct **Category**.
7. From the **Vendor** dropdown, click **Windows MQServer**.
A list of devices will be generated in the **Devices dropdown**.



• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
CSR generation got failed/User has no permission for the given location to perform the operation.	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issues in Certificate Push

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**.
The **Server Certificate** page is displayed.
4. Create an **Application connector** with “**Create KDB/Create Keystore**” profile
5. Push the certificate to the device.

Troubleshooting Server, Firewalls, WAF, and Rapid SB Connectors

CERT+ Server Certificate > cert.test.com > View Work order Status

Request View Workorder View

Search...

Push and Bind Requ... Review Implement Pre Push Script Exec... Backup Task **Push Task**

Push Task
Certificate push failed

Logs - Push Task

1	02/25/2021 11:57:54	- Initiating Push Task
2	02/25/2021 11:58:57	- Certificate Push Failed
3	02/25/2021 11:58:58	- Push Task Failed
4		

CERT+ Server Certificate > cert.test.com > View Work order Status

Request View Workorder View

Search...

Push and Bind Requ... Review Implement Pre Push Script Exec... Backup Task **Push Task**

Push Task
Certificate push failed

Logs - Push Task

1	02/25/2021 12:07:34	- Initiating Push Task
2	02/25/2021 12:07:37	- PrivateKey in device push invalid
3	02/25/2021 12:07:37	- Push Task Failed
4		

CERT+ Server Certificate > avxpushRSA4096SHA512.appviewx.comYOLS2 > View Work order Status

Request View Workorder View

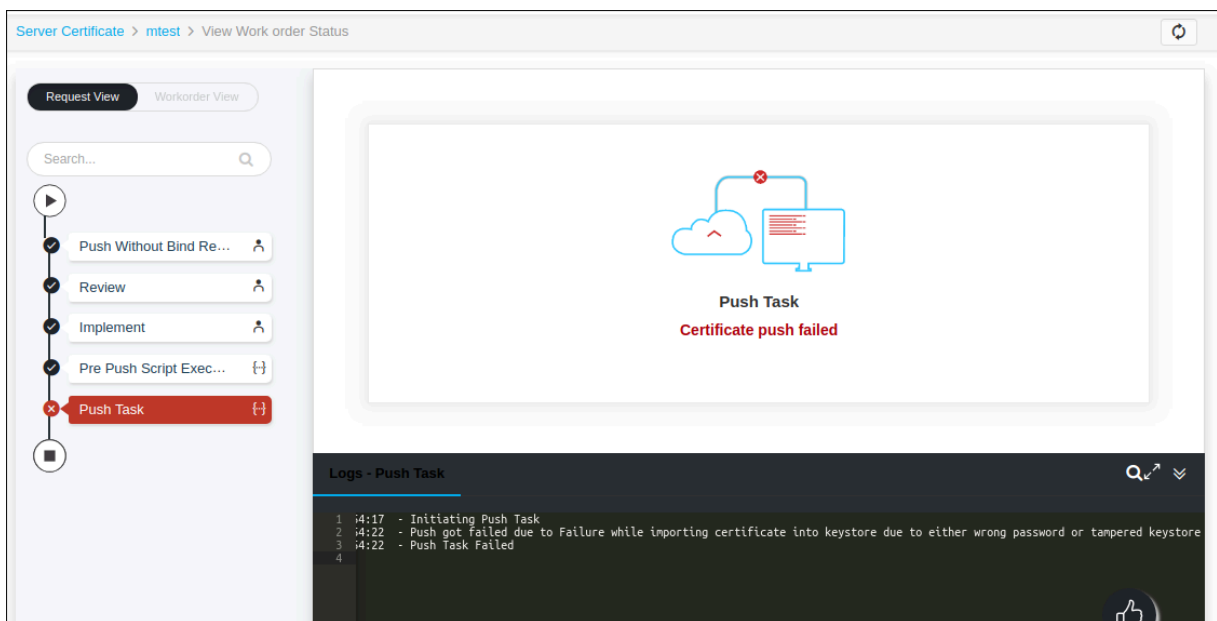
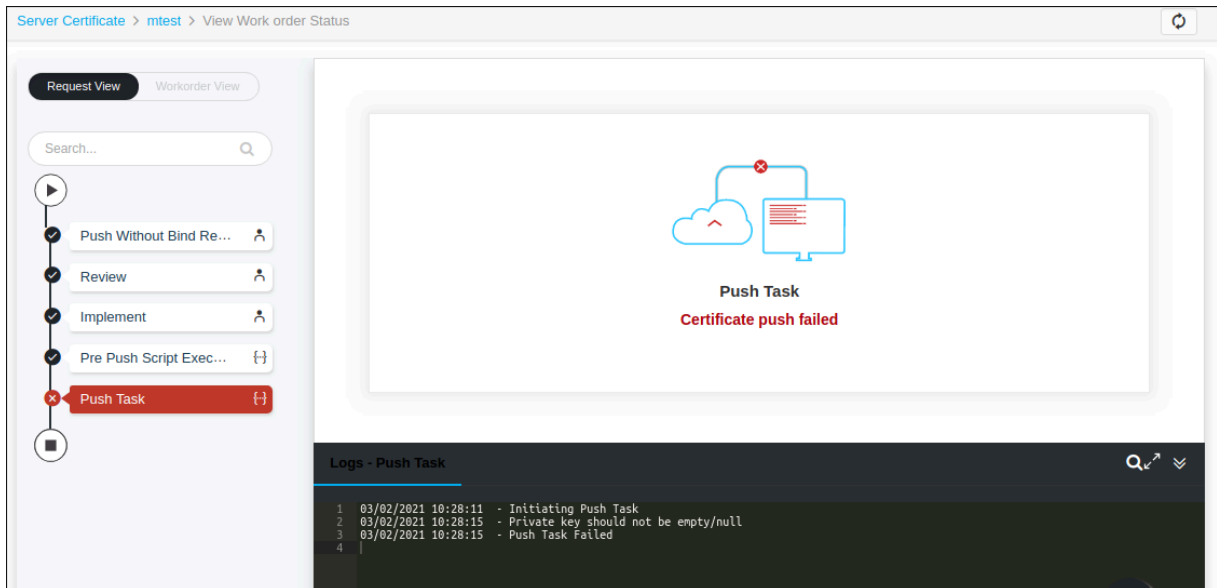
Search...

Push and Bind Requ... Review Implement Pre Push Script Exec... Backup Task **Push Task**

Push Task
Certificate push failed

Logs - Push Task

1	02/25/2021 12:37:58	- Initiating Push Task
2	02/25/2021 12:39:02	- Push Failed due to KDB push got failed.
3	02/25/2021 12:39:02	- Push Task Failed
4		



- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Certificate Push failed. Or Push got failed due to User has no permission for the given location to perform the operation	User has restricted access to the path configured to push the certificate in the application connector	Please ensure the user is configured while device addition has the read/write access to the path configured in application connector to certificate push.
PrivateKey in device push invalid	“Private key in Device” is enabled in application connector, but key is not available on device.	Ensure to enable “Private key in Device” attribute in application connector, if the certificate does not have the key and the certificate is generated using CSR gen option from Device.
Push Failed due to KDB push got failed.	Target KDB file does not exist in the device.	Ensure the target KDB file, for which certificate push configured is available and has read/write access.
1. Private key should not be empty/null. 2. Push failed due to Failure while importing certificate into keystore due to either wrong password or tampered keystore.	Trying to push certs without a keyfile.	Please ensure the certificate to be pushed has a private key file. Or if key file exists in device please select privateKeyInDevice option.

Troubleshooting IBMClient Windows

- [Overview of IBMClient Windows Troubleshooting Guide](#)
- [Issues in IBMClient Windows](#)

Overview of IBMClient Windows Troubleshooting Guide

This document will guide you to overcome the various issues faced by you during the use of IBMClient Windows and its various functionalities.

Issues in IBMClient Windows

- [Issues in Server Addition using AppViewX UI](#)
- [Issues in Device communication](#)
- [Issue in Discovery](#)
- [Issues in CSR generation at Endpoint](#)
- [Issues in Certificate Push](#)

Issues in Server Addition using AppViewX UI

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. From the icon list at the top right corner, Click **Add**.
The **Device Addition** page is displayed.
6. From the **Device Details Section** on the left, click **IBM**.
7. Click **IBMClient(Windows)**.
8. Fill in the appropriate details.
9. Click **Add**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Device communication

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**.

The **Device Communication Status** is displayed.

☐	IBMClient_Windows	absecon	Unresolved	Windows IBMClient		Manual entry
☐	IBMClient_wind	absecon	Unresolved	Windows IBMClient		Manual entry

+ Device Status Log: IBMClient_wind

Device communication (03/03/2021 04:01:05 PM) **Failure**

Communication to PTPLD259 has failed

Device Version (03/03/2021 04:01:05 PM) **Failure**

Device version fetch has failed

• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Communication to <hostname> failed	Gateway agent not reachable. Device not reachable from the gateway agent GSKit is not installed on any given device.	Ensure gateway is configured properly and the APIs are accessible from AppViewX. Ensure device and gateway agent are in the same domain and device is accessible from gateway agent. Please ensure GSKit is installed properly.

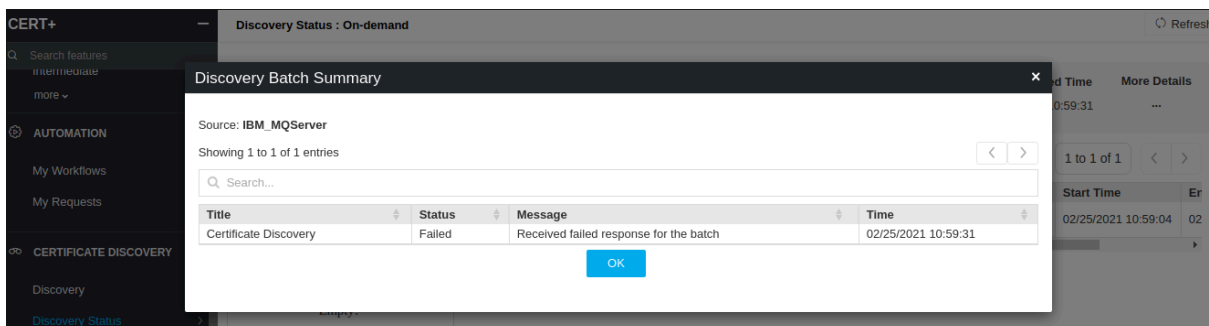
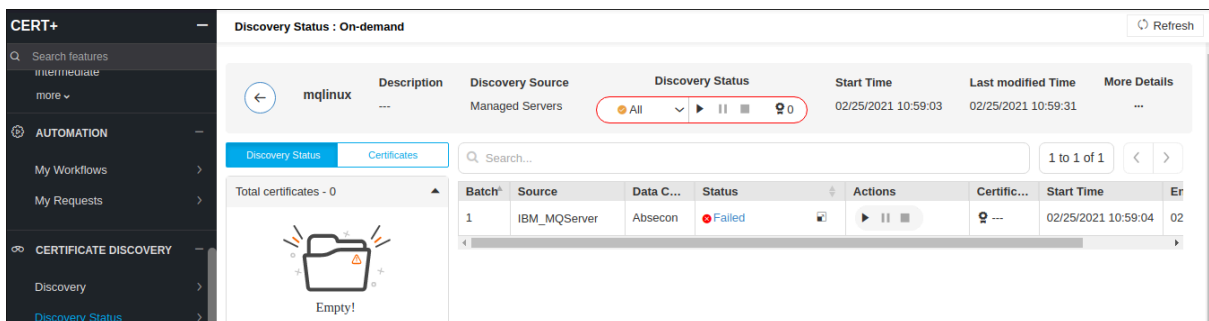
Error Message	Possible Cause	Possible Solution
Communication to <hostname> failed Device version fetch has failed.	Hostname or Credentials configured is wrong	Ensure hostname and the device credentials configured while device addition is valid.

Issue in Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+** .
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.



- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Received failed response from batch	No valid KDB/keystore files available in the given path.	Ensure the given certificate location has a valid KDB/keystore and KDB/keystore has certs.
Discovery completed successfully. (with 0 certs even if valid certs exist in given path)	1. Respective Keystores password is not added in Password Vault to parse certs. 2. User may not have read permission to parse certs	1. Please enter the password of keystores in the Password Vault to parse certs. 2. Please ensure the user has appropriate permission to read files.

Issues in CSR generation at Endpoint

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab.
The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, click correct **Category**.
7. From the **Vendor** dropdown, click **Windows MQServer**.
A list of devices will be generated in the **Devices dropdown**.

The screenshot shows the CERT+ interface with the following components:

- Left Sidebar:** Contains 'CERTIFICATE ACTION' (Enroll Certificate, Renew Certificate, Push to Device, Reissue Certificate, Revoke Certificate, more) and 'CERTIFICATE INVENTORY' (Server, Client, Code Signing Certificate, Device).
- Header:** 'Server Certificate > mtest1 > View Work order Status'.
- Workflow View:** A vertical sequence of steps: 'CSR Submission Req...' (checked), 'Approval' (checked), 'Implementation' (checked), and 'CSR Submission' (failed, highlighted in red).
- Main Content Area:** Displays a diagram of a cloud and a server with a red 'X' indicating failure. Below the diagram, it says 'CSR Submission' and 'CSR Submission process failed' in red.
- Logs - CSR Submission:** A log table showing the following entries:

1	03/02/2021 13:07:08	- Initiating CSR Submission
2	03/02/2021 13:07:11	- Failure response obtained on consuming REST API
3	03/02/2021 13:07:11	- CSR Submission Failed
4		

The screenshot shows the CERT+ interface with the following components:

- Left Sidebar:** Same as the first screenshot.
- Header:** 'Server Certificate > pkgen > View Work order Status'.
- Workflow View:** A vertical sequence of steps: 'CSR Submission Req...' (checked), 'Approval' (checked), 'Implementation' (checked), and 'CSR Submission' (failed, highlighted in red).
- Main Content Area:** Displays a diagram of a cloud and a server with a red 'X' indicating failure. Below the diagram, it says 'CSR Submission' and 'CSR Submission process failed' in red.
- Logs - CSR Submission:** A log table showing the following entries:

1	03/03/2021 16:29:18	- Initiating CSR Submission
2	03/03/2021 16:29:19	- CSR Submission Failed
3		

- Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
1. Failure response obtained on consuming REST API. 2. CSR submission failed	User has restricted access to the path configured for the "CSR FileName" and "Key File name"	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issues in Certificate Push

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**.
The **Server Certificate** page is displayed.
4. Click any **IBMClient server**.
A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions** with "Create KDB/Create Keystore" profile, select **Add App Connector**.
6. Push the certificate to the device.

Server Certificate > NginxWSPush.appviewx.comQF6YD > View Work order Status

Request View Workorder View

Search...

Push Without Bind Re...
Review
Implement
Pre Push Script Exec...
Push Task

Push Task
Certificate push failed

Logs - Push Task

```

1 03/03/2021 16:08:22 - Initiating Push Task
2 03/03/2021 16:08:25 - Push got failed due to Windows Gateway Error Response : a693c520-948d-478a-8aed-7c06c3a707c2: No path found
3 03/03/2021 16:08:25 - Push Task Failed
4

```

Server Certificate > AVXAgentEntCA.avxdevlab.net > View Work order Status

Request View Workorder View

Search...

Push Without Bind Re...
Review
Implement
Pre Push Script Exec...
Push Task

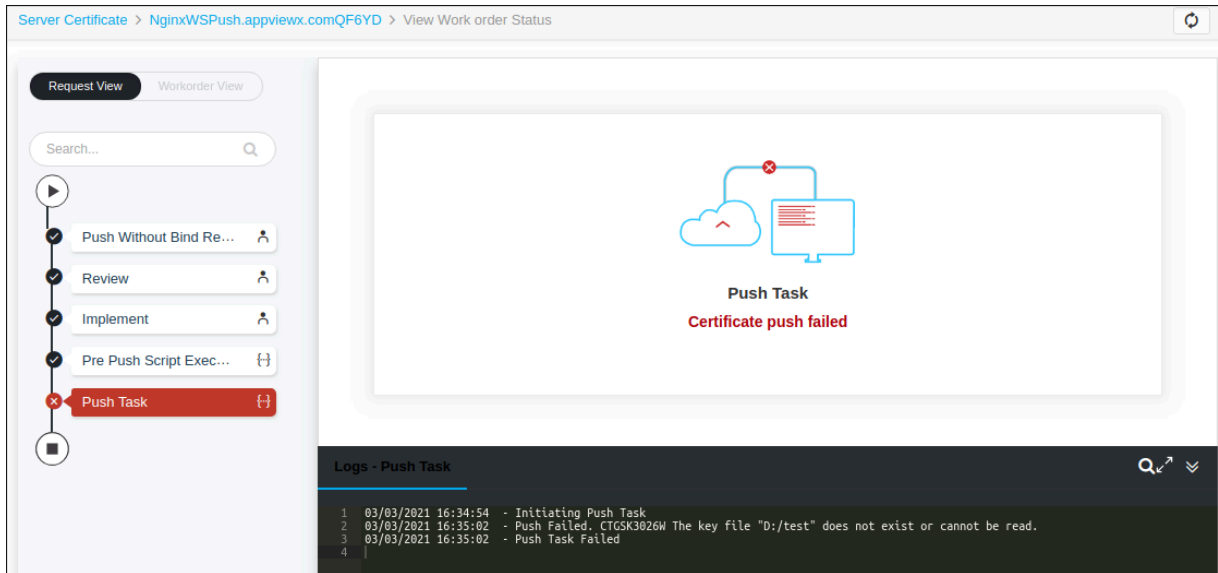
Push Task
Certificate push failed

Logs - Push Task

```

1 03/03/2021 16:14:50 - Initiating Push Task
2 03/03/2021 16:14:52 - Private key is not available. Failing the push
3 03/03/2021 16:14:52 - Push Task Failed
4

```



• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
1. Push Failed. CTGSK3026W The key file "D:/mtest/mtest.kdb" does not exist or cannot be read. 2. Push got failed due to Windows Gateway Error Response : a693c520-940d-478a-8aed-7c06c3a707c2: No path found	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/write access to the path configured in application connector to certificate push.
Push Failed due to KDB push failed.	Target KDB file does not exist in the device	Ensure the target KDB file, for which certificate push configured is available and has read/write access.
Private key is not available. Failing the push	Trying to push certificates without a keyfile.	Please ensure the certificate to be pushed has a private key file Or if key file exists in device please select privateKeyInDevice option.

Troubleshooting Imperva WAF

- [Overview of Imperva WAF Troubleshooting Guide](#)
- [Issues in Imperva WAF](#)

Overview of Imperva WAF Troubleshooting Guide

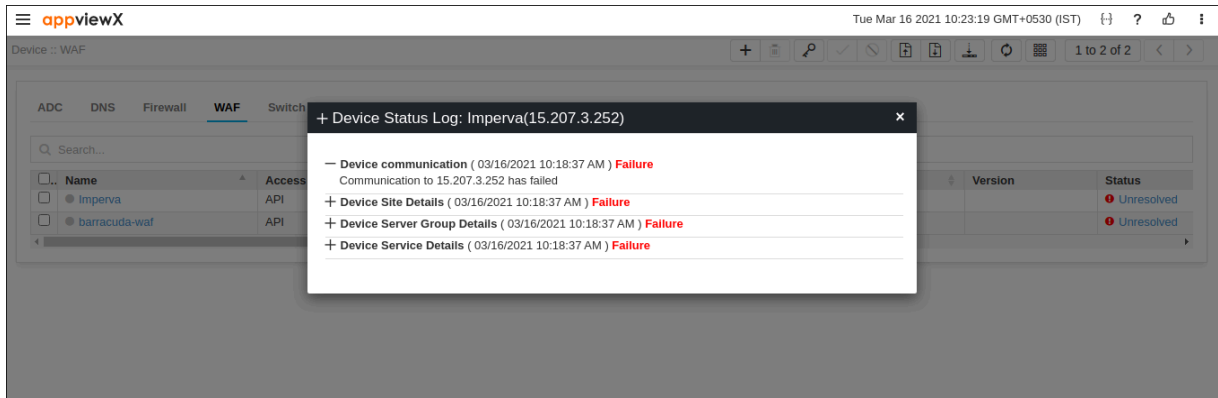
This section will guide you to overcome the various issues faced by you during the use of Imperva WAF and its various functionalities.

Issues in Imperva WAF

- [Issues in Communicating to Imperva](#)
- [Issues in Config Fetch](#)
- [Issue in Discovery](#)
- [Issue in Push and Rollback](#)

Issues in Communicating to Imperva

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **WAF** Tab.
5. Select the device, click **Status**.
The **Device Communication Status** is displayed.



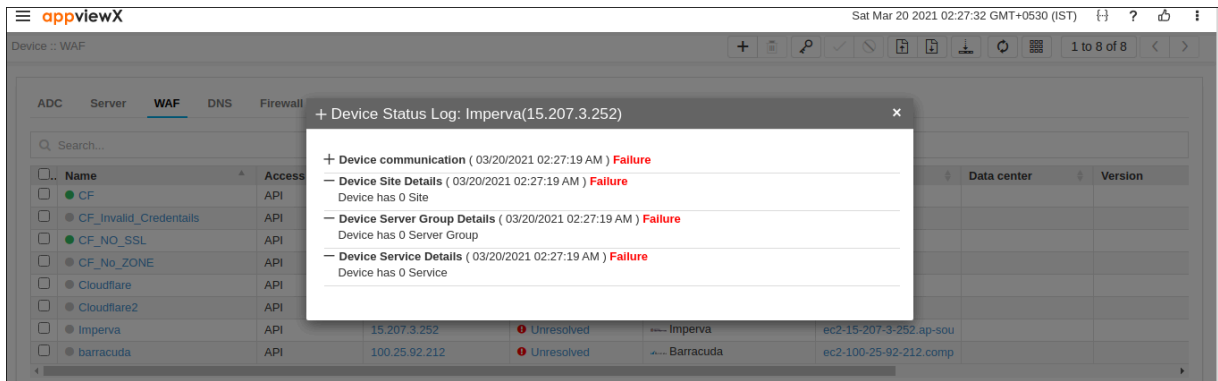
- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Communication to <ip> has failed	Invalid credentials Imperva WAF is down.	Please check if the correct Imperva credentials are provided. Please login to the SecureSphere console to check if Imperva is running.
Connection timeout	Internet / Proxy connection is not provided from AppViewX node. Firewall settings blocking the REST API request	Login to AppViewX portal and provide proxy details in Menu->Settings->General->Proxy and Check Firewall settings

Issues in Config Fetch

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **WAF** Tab.
5. Select the **Device**, click **Fetch Config**.



- Error Messages

Error Messages

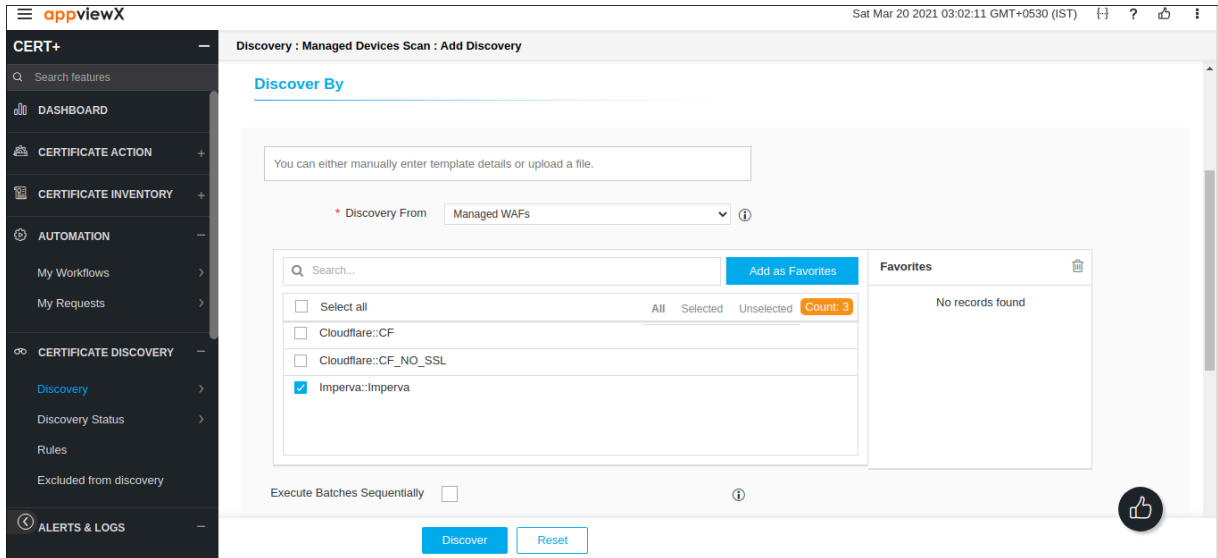
Error Message	Possible Cause	Possible Solution
Communication to <ip> has failed	Invalid credentials Imperva WAF is down.	Please check if a correct Imperva credentials are provided Please login to the SecureSphere to check if Imperva is running.
Device has 0 sites.	No sites configured in Imperva.	Please login to the SecureSphere to check if Sites are configured.
Device has 0 Server Group	No Server Groups configured in Imperva.	Please login to the SecureSphere to check if Server Groups are configured.
Device has 0 Services	No Services configured in Imperva	Please login to the SecureSphere to check if Services are configured.

Issue in Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.



• Error Messages

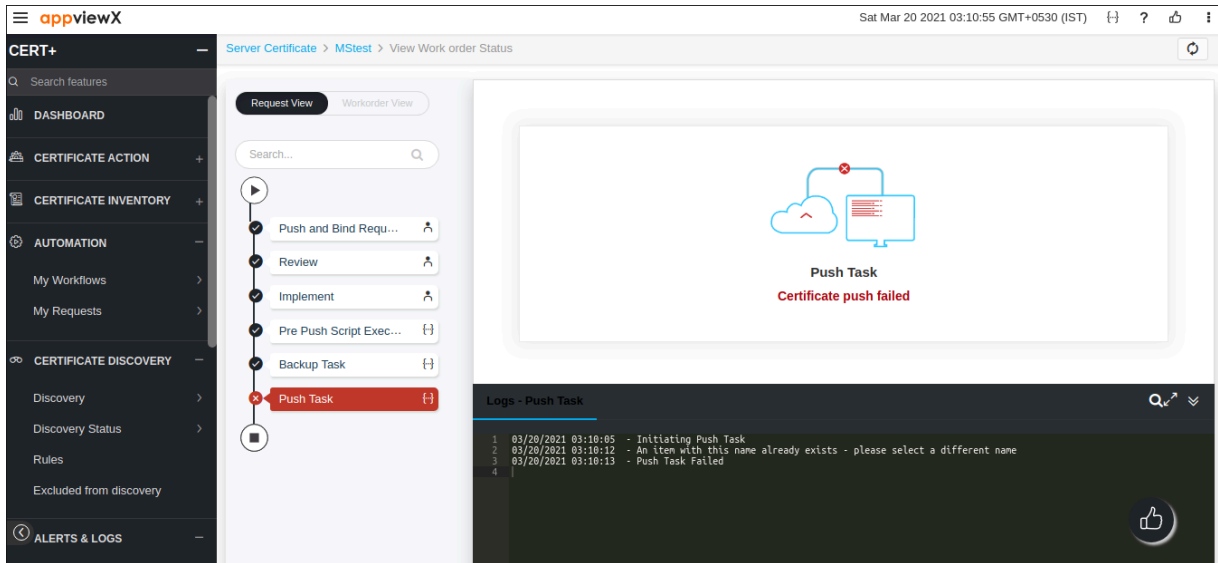
Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a devices	No WAF account is selected in the “Discover By” section.	Select at least one device to discover certificates from.

Error Message	Possible Cause	Possible Solution
Discovery Status Failed	Check if internet /Proxy connection is provided in AppViewX node.	Login to AppViewX portal and provide proxy details in Menu->Settings->General->Proxy.
No Certificates discovered from Imperva WAF	SSL Certificates are not discovered from Imperva due to API restrictions. Imperva Rest API doesn't allow the public Certificate String in the API responses. Only Certificate attributes like common name, signature, Expiry date and Issuer details are captured.	Check with AppViewX PM team / SME for more details

Issue in Push and Rollback

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **WAF**.
The **Server Certificate** page is displayed.
4. Click any **server**.
A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, select **Add App Connector**.
6. Push the certificate to the device.



- Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
An item with this name already exists - please select a different name	SSLKeyName should be unique.	Kindly ensure to provide a unique name in "Certificate File Name" field on Connector page.
Site not found	Unable to find the site to push the certificate	Please login to SecureSphere to check if the Site is available.
Server Group not found	Unable to find the Server Group to push the certificate	Please login to SecureSphere to check if the Server Group is available.
Services not found	Unable to find the Service to push the certificate	Please login to SecureSphere to check if the Service is available.

Troubleshooting Linux JBoss Server

- [Overview](#)
- [Supported Web Browsers](#)
- [Issues in Linux JBoss Server](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with Linux JBoss server.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

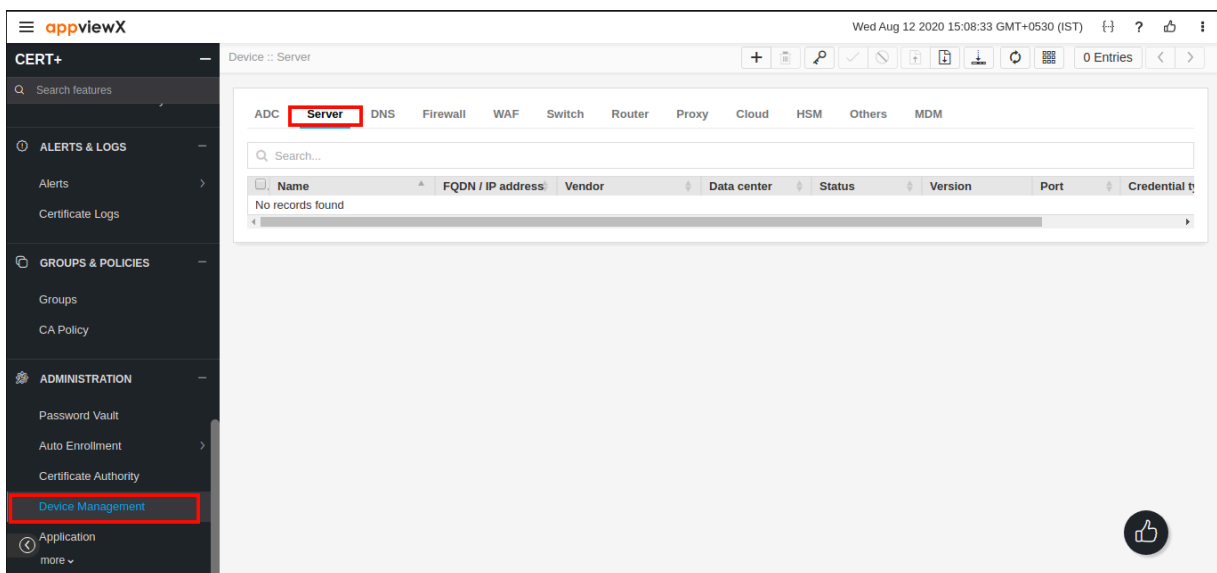
Issues in Linux JBoss Server

- [Issues in Linux JBoss Server Addition using AppViewX UI](#)
- [Issues in Communicating to Linux JBoss Server](#)
- [Issues in Accessing Server](#)

- [Issues in Credential List](#)
- [Issues in Managed Server](#)
- [Issues in Unmanaged Server](#)
- [Issues in Import Server](#)
- [Issues in Export Server](#)
- [Issues in Config Fetch](#)
- [Issues in Certificate Discovery](#)
- [Issues in CSR generation](#)
- [Issues in Push and Rollback](#)

Issues in Linux JBoss Server Addition using AppViewX UI

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. From the icon list at the top right corner, click **Add**.
The **Device Addition** page is displayed.
6. From the **Device Details Section** on the left, click **JBoss**.
7. Select **Operating System** as **Linux**.



Device :: Server > Add

Vendors

- APACHE Linux
- Microsoft IIS
- Microsoft PC
- Microsoft Server
- APACHE Microsoft
- Microsoft SQL
- ORACLE
- IBM
- hp
- Linux
- ARBOR
- JBoss
- N7
- RabbitMQ

Server details

* Operating system type ☒ Linux ☐ Windows

* Server name

* IP address

Data center

Communication mode ☒ SSH ☐ SSM

* SSH Port

Cert sync ☒ Managed ☐ Monitored ☐ Ignored

Credentials

* Credential type

* Username

* Password

Vendor Specific Details

Access Elevation ⓘ

• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Communicating to Linux JBoss Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.

- From the left pane, expand **Administration** and click **Device Management**.

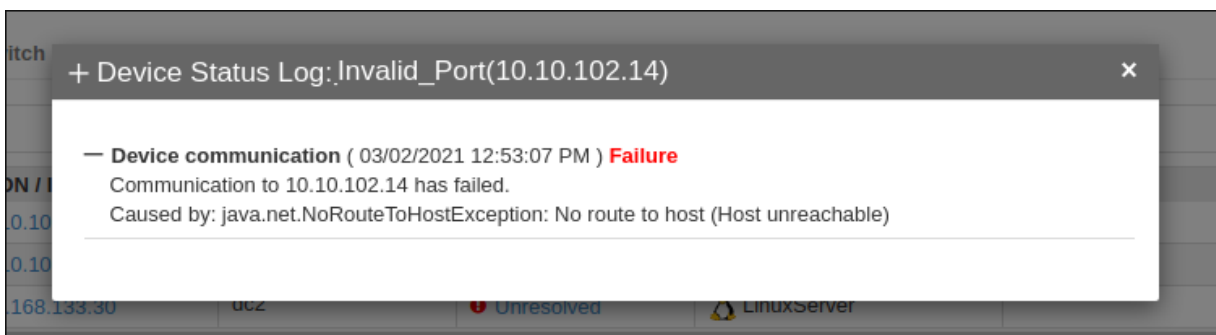
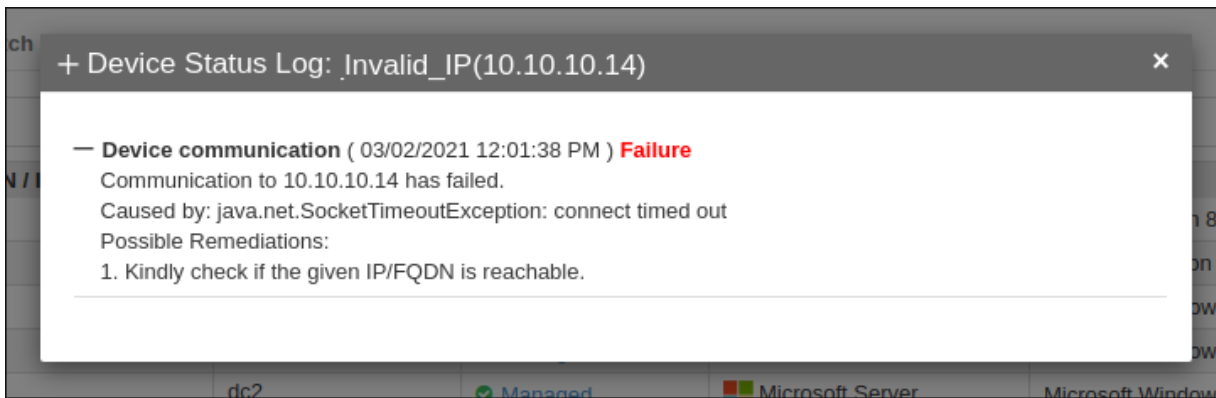
The **Device Management** page is displayed.

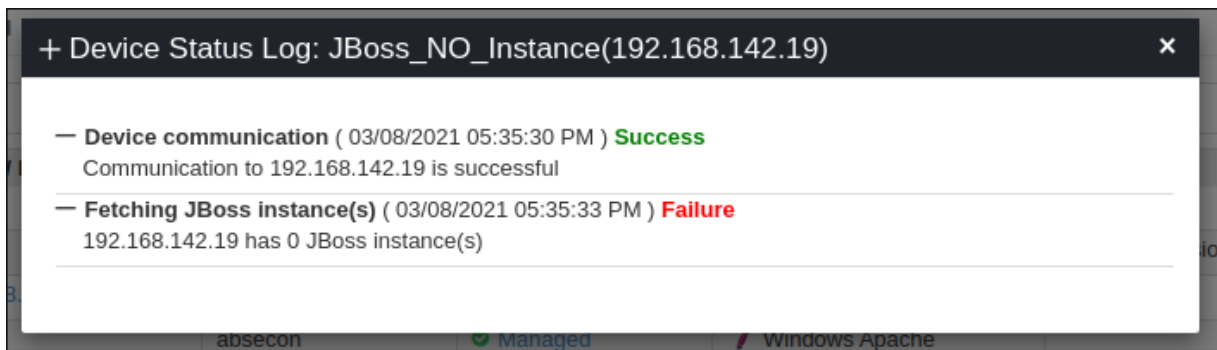
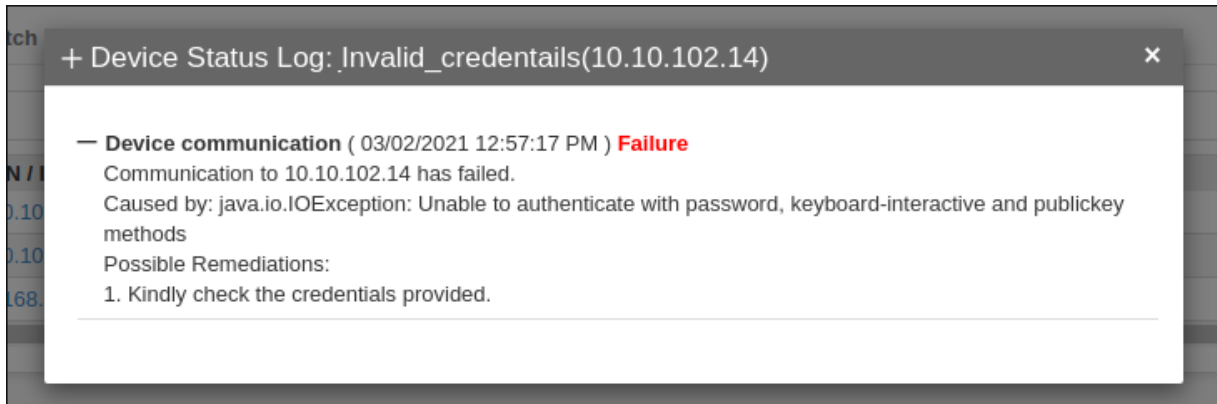
- On the **Device Management** page, click **Server** Tab.

- Select the device, click **Status**.

The **Device Communication Status** is displayed.

Name	FQDN / IP address	Data center	Status	Vendor	Version	Port	Credential type
Invalid_IP	10.10.102.14	absecon	Inprogress	JBoss		22	Manual entry
JBoss	192.168.133.30	absecon	Managed	JBoss	6.4	22	Manual entry





- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is either null or empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-', '_', '.', '*', ' ', '!' and spaces.
Device IP/FQDN cannot be null or empty.	Device IP/FQDN is empty.	Provide device IP/FQDN as it is a mandatory field.

Error Message	Possible Cause	Possible Solution
Invalid device IP/FQDN address.	IP/FQDN address is not valid.	Provide valid IP/FQDN address.
Communication to <ip/fqdn> has failed. Caused by: java.io.IOException: Unable to authenticate with password, keyboard-interactive and publickey methods Possible Remediations: 1. Kindly check the credentials provided.	Password of the device added might be wrong.	Click on the device name in the Inventory Page. Update the correct password and click Save.
Communication to <ip/fqdn> has failed. Caused by: java.net.SocketException: Network is unreachable (connect failed)	IP/FQDN provided is not reachable	Check manually by establishing an SSH session to the target device with the provided IP/FQDN.
Communication to <IP/FQDN> has failed. Caused by: java.net.ConnectException: Connection refused (Connection refused) Possible Remediations: 1. Kindly check the SSH Port configurations. 2. Kindly check the firewall settings	Problem with port configuration	Check if the configured port in the device addition page is correct.
Communication to <IP/FQDN> has failed. Caused by: java.io.IOException: Key exchange was not finished, connection is closed.	Problem with SSH key handshake	Request to check the ciphers, key and HMACs configured in the target device and ensure AppViewX SSH-plugin supports the same

Error Message	Possible Cause	Possible Solution
<IP/FQDN> has 0 JBoss instance(s)	No JBoss server running in the target device,	Login via SSH to the target device and execute the below command to check the status of the JBoss server "ps -ef grep jboss".

Issues in Accessing Server

Access Issues might be reproduced when communicating with servers while discovering or fetching configuration files. These errors can be collected either from logs, API responses, or in the status field for the particular server.

Error Message	Possible Cause	Possible Solution
Sudo Access failure	Linux Commands execution with sudo fails.	Verify if the system has the correct sudo setup.
dzdo Access failure	Linux Commands execution with dzdo fails.	Verify if the system has the correct dzdo setup.
Permission denied for file/location.	File might not be present in the avx environment. User might not have permission to read in the given source location. Device communication might not be established when service has started.	Check whether someone deleted the file from AppViewX environment. Verify if read permission is given for the location. Verify the device connection and restart the service.

Issues in Credential List

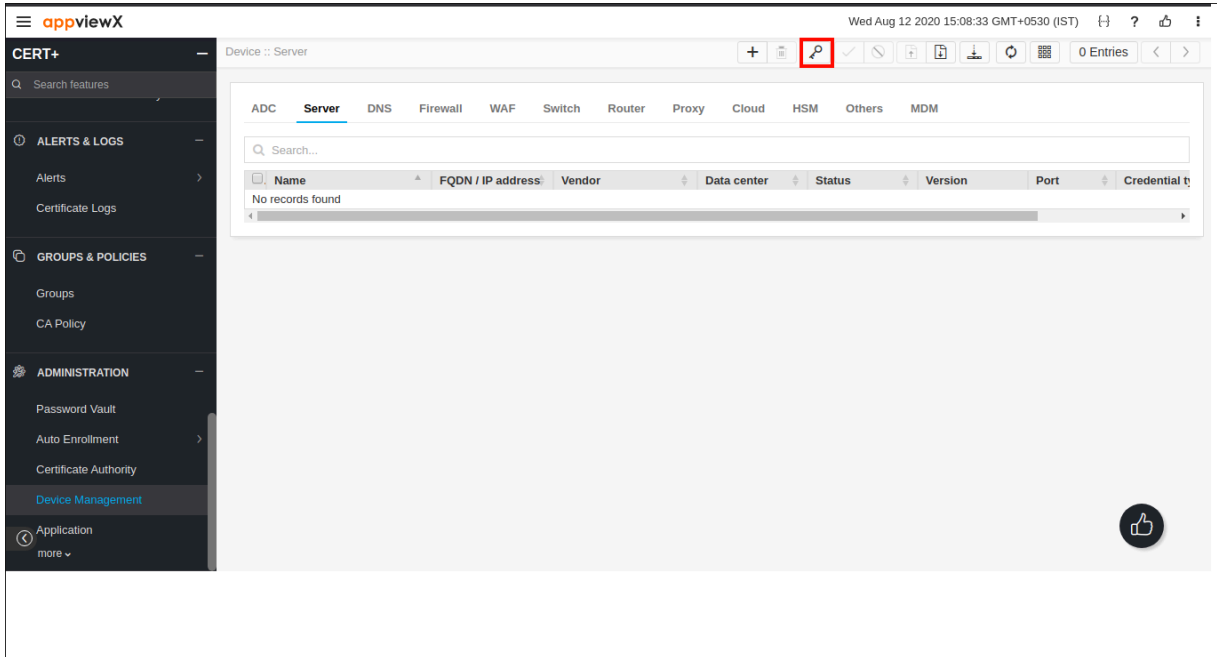
1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.

The **Device Management** page is displayed.

4. On the **Device Management** page, click **Server** Tab.

5. Select the device, click **Credentials**.

The **Credential List** page is displayed.



• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid details	Mandatory credential details are missing.	Provide all the mandatory details to store the credential.
credentials already exist.	Credential List with the same name already exists.	Provide a unique name to each credential list.
Invalid file format. Accepted formats are .pem and .txt	The Identity Key file uploaded is not having the correct format.	Provide key file with correct format (.pem or .txt)

Invalid details

The screenshot shows the 'Add credential' form for 'appviewX'. A red error banner at the top states 'Invalid details'. The form fields are as follows:

- Credential name:** Empty field with a red asterisk and an 'x' icon.
- User name:** Empty field with a red asterisk and an 'x' icon.
- Credential type:** Radio buttons for 'Password' (selected) and 'Identity key'.
- Password:** Field containing masked characters with a red asterisk.
- Secondary password:** Empty field.

Buttons at the bottom: 'Save' and 'Cancel'.

Credentials already exist

The screenshot shows the 'Add credential' form for 'appviewX'. A red error banner at the top states 'credentials already exist.'. The form fields are filled with the following values:

- Credential name:** 'appviewx'
- User name:** 'appviewx'
- Credential type:** Radio buttons for 'Password' (selected) and 'Identity key'.
- Password:** Field containing masked characters with a red asterisk.
- Secondary password:** Empty field.

Buttons at the bottom: 'Save' and 'Cancel'.

Invalid file format. Accepted formats are .pem and .txt

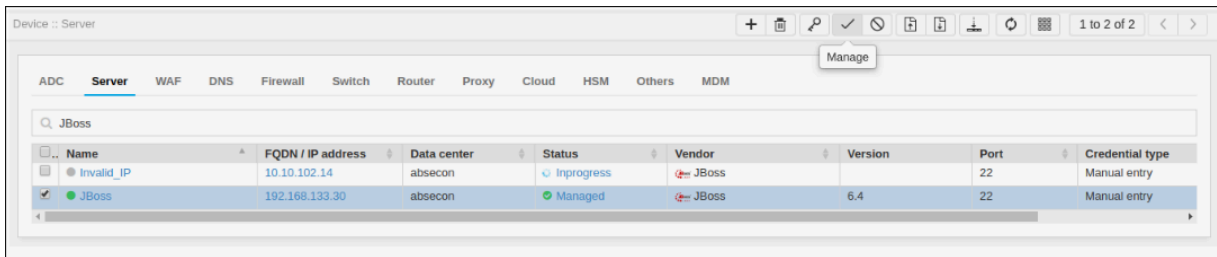
The screenshot shows the 'Add credential' form for 'appviewX'. A red error banner at the top states 'Invalid file format. Accepted formats are .pem and .txt'. The form fields are as follows:

- Credential name:** 'appviewx'
- User name:** 'appviewx'
- Credential type:** Radio buttons for 'Password' and 'Identity key' (selected).
- Identity key:** Field with a 'Browse' button and an information icon.
- Passphrase:** Empty field.

Buttons at the bottom: 'Save' and 'Cancel'.

Issues in Managed Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device and click **Manage**.



• Error Messages

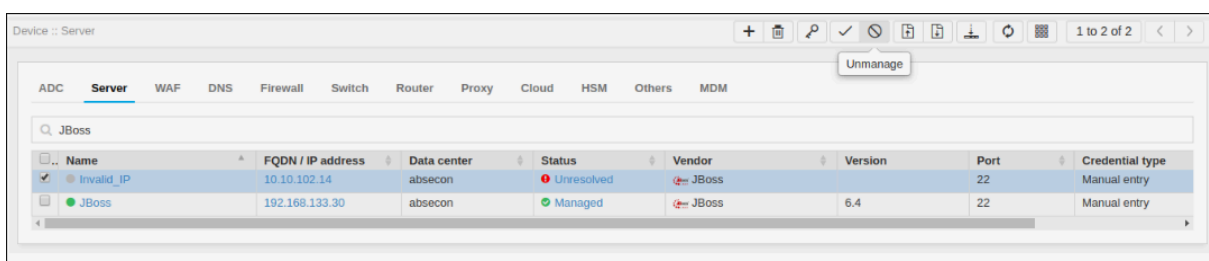
Error Messages

Error Message	Possible Cause	Possible Solution
The selected devices are managed. The operation cannot be performed.	Device cannot be managed because it is already in the managed state.	Unmanage the device(s) in the managed state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

Issues in Unmanaged Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.

4. On the **Device Management** page, click **Server** Tab.
5. Select the device and click **Unmanage**.



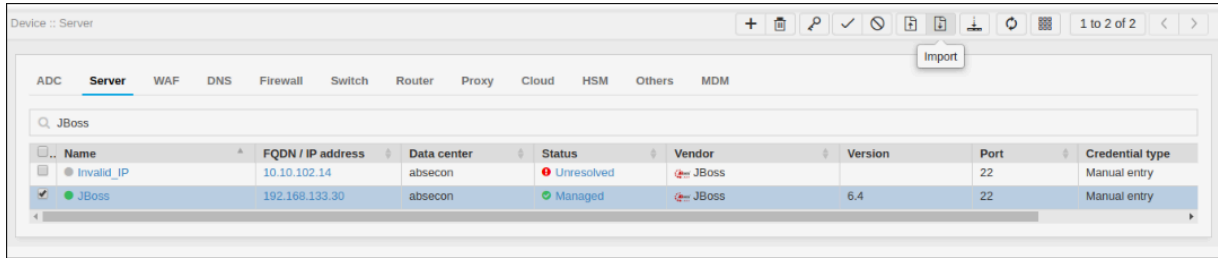
• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
The selected devices are already unmanaged. The operation cannot be performed.	Device cannot be unmanaged because it is already in the unmanaged state.	Manage the device(s) in an unmanaged state before performing action.
Fetch config not allowed for Unmanaged devices	Fetch config operation is only allowed on the devices which are in managed state.	Manage the device(s) in an unmanaged/in-progress state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

Issues in Import Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device and click **Import**.



- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid file type. Please select a valid file format (csv / xlsx / xls).	File type uploaded is not in expected format.	Supported file types are CSV/Xls/xlsx only. Check for the extension of the uploaded file.
Maximum five files allowed, please delete any completed file.	Maximum of 5 files can be maintained in file history of import page.	Delete any of the parsed/completed files to upload a new one.

Maximum five files allowed, please delete any completed file.

Device :: Server > Import

Maximum five files allowed, please delete any completed file.

Import

Click here to Browse and Upload (csv, xls, and.xlsx)

Uploader Info

Maximum 5 files (.xlsx or .csv) will be processed in parallel

Download sample file here

CSV

XLSX

File Histories

Refresh

File name	Status	Server count	Action
2020.3.0ServerimportSheet.xls	17% Available: 0 Uploaded: 1 Failed: 5	6	
2020.3.0ServerimportSheet.xls	0% Available: 0 Uploaded: 0 Failed: 6	6	
2020.3.0ServerimportSheet.xls	0% Available: 0 Uploaded: 0 Failed: 6	6	
2020.3.0ServerimportSheet.xls	0% Available: 0 Uploaded: 0 Failed: 6	6	
2020.3.0ServerimportSheet.xls	0% INITIATED	6	

Invalid file type. Please select a valid file format (csv / xlsx / xls).

The screenshot shows the 'Import' page in the AppViewX interface. At the top, a red error banner states: 'Invalid file type. Please select a valid file format (csv / xlsx / xls)'. Below this, the 'Import' section features a dashed box for file upload with a '19.3.png' file icon and a 'Download sample file here' link. To the right, the 'Uploader Info' section notes: 'Maximum 5 files (.xlsx or .csv) will be processed in parallel'. Below these sections is a 'File Histories' table with a 'Refresh' button.

File name	Status	Server count	Action	
2020.3.0ServerimportSheet.xls	17%	Available: 0 Uploaded: 1 Failed: 5	6	↶ ↷
2020.3.0ServerimportSheet.xls	0%	Available: 0 Uploaded: 0 Failed: 6	6	↶ ↷

Issues in Export Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device and click **Export**.

The screenshot shows the 'Device Management' page with the 'Server' tab selected. A search bar contains 'JBoss'. Below the search bar is a table of servers. An 'Export' button is visible in the top right corner of the table area.

Name	FQDN / IP address	Data center	Status	Vendor	Version	Port	Credential type
Invalid_IP	10.10.102.14	absecon	Unresolved	JBoss		22	Manual entry
JBoss	192.168.133.30	absecon	Managed	JBoss	6.4	22	Manual entry

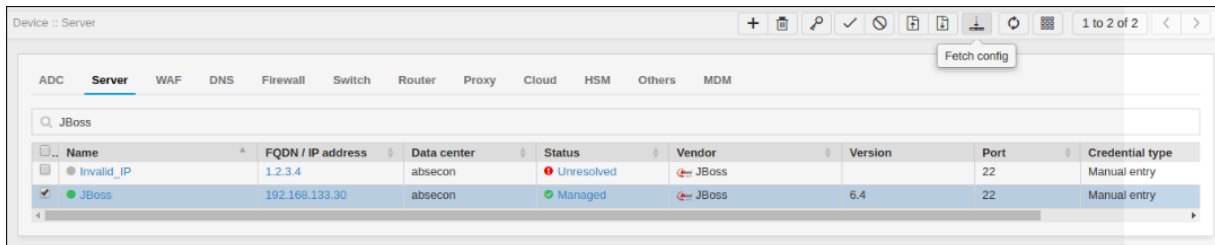
• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Exception while exporting	General failure - Unable to create file on the local system due to permission issue.	Provide access to be able to create the file on the local system. (e.g. check the directory where it is trying to export and give access to AppViewX for that directory)
	Unable to fetch device list from the database.	Make sure the database is running and has correct data.

Issues in Config Fetch

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Fetch Config**.



- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Communication to <IP/FQDN> has failed.	Device communication has failed due to invalid credentials / SSH Port	Verify the input details and check device status error messages Issues in Communicating to Linux JBoss Server

Issues in Certificate Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

The screenshot shows the AppViewX CERT+ interface. On the left, the 'CERTIFICATE DISCOVERY' menu is expanded, and 'Discovery' is selected. The main panel is titled 'Discovery : Managed Devices Scan : Add Discovery'. It contains a form with the following fields: 'Discovery Instance Name' (JBOSSE_Discovery), 'Description' (empty), and 'Discover By' (Managed Servers). Below the form, there is a section for 'Discover By' with a search bar containing 'JBoss'. A table lists the discovered items, showing one entry: 'JBoss::JBoss'. The table has columns for 'Select all', 'All', 'Selected', 'Unselected', and 'Count: 1'. At the bottom, there are 'Discover' and 'Reset' buttons.

• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.

Issues in CSR generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab.
The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, click correct **Category**.
7. From the **Vendor** dropdown, click **JBoss**.
A list of devices will be generated in the **Devices** dropdown.

appviewX

CERT+

Search features

DASHBOARD

CERTIFICATE ACTION

- Enroll Certificate
- Renew Certificate
- Push to Device
- Reissue Certificate
- Revoke Certificate
- more

CERTIFICATE INVENTORY

- Server
- Client
- Code Signing Certificate
- Device

Enroll Server Certificate

* CSR Generation ☐ AppViewX ☐ Upload CSR ☐ HSM ☒ End Point

Category

Vendor

* Devices

* CSR file name .csr

* Key File Name .key

CSR Parameters

* Common Name

Subject Alternative Name

DNS ⓘ 0 value

Organization

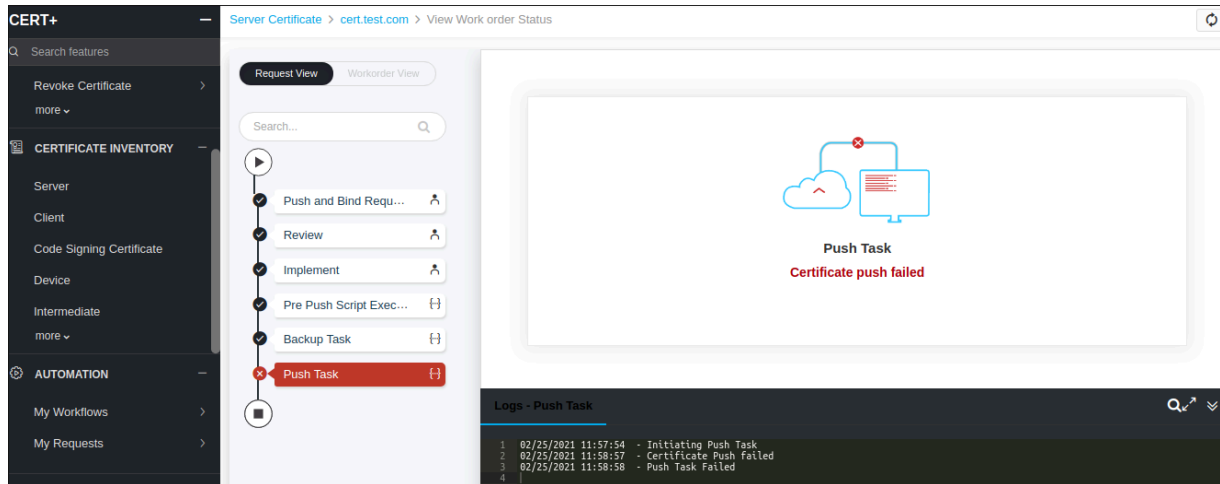
• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Problem while generating csr on target server	General Failure - SSH/SFTP communication failure	Provide correct credentials and make sure device communication is successful.
Invalid key type specified in the request	Given key type might not be supported by open SSL in the target machine.	Provide valid key type.
Problem while generating csr on the target server.	Location might not have the required permission.	Check the permission and provide it.
CSR and Private key has been failed	Open SSL configuration might be wrong in the target machine.	Check and correct open SSL configuration in the device.
CSR generation got failed	User has restricted access to the path configured for the "CSR FileName" and "Key File name"	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issues in Push and Rollback

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**.
The **Server Certificate** page is displayed.
4. Click any **JBoss server**.
A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, select **Add App Connector**.
6. Push the certificate to the device.



- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	- Pushing to device when certificate is unavailable, i.e, in a new state. - Previous work order is in progress and not completed. - AppConnector might not be in sync.	- Push to device after certificate has been retrieved from CA. - Initiate push after previous work order is finished. - Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.

Error Message	Possible Cause	Possible Solution
Application connector(s) not found	Application connector info was not found.	Provide the correct “connectorId” if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Certificate Push failed	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/write access to the path configured in application connector to certificate push.
PrivateKey in device push invalid	“Private key in Device” is enabled in application connector, but key is not available in device.	Ensure to enable “Private key in Device” attribute in application connector, if the certificate does not have the key and the certificate is generated using CSR generate option from Device.

Troubleshooting Microsoft Enterprise CA

- [Overview](#)
- [Supported Web Browsers](#)
- [Issues in Microsoft Enterprise CA](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using functionalities like setting addition, certificate enrollment, renewal, revocation, suspension, reinstatement, discovery, and other actions associated with Microsoft Enterprise.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Microsoft Enterprise CA

- [Issues in Microsoft Enterprise CA setting addition and fetch CAs](#)
- [Issues in Enrolling, Fetching, Renewing, Regenerating Microsoft Enterprise certificate](#)
- [Issues in Revoking Microsoft Enterprise certificate](#)
- [Issues in Suspending Microsoft Enterprise certificate](#)
- [Issues in Reinstating Microsoft Enterprise certificate](#)
- [Issues in Discovering Microsoft Enterprise certificates](#)

Issues in Microsoft Enterprise CA setting addition and fetch CAs

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Certificate Authority**.
The **Certificate Authority** page is displayed.
4. On the **Certificate Authority** page, click **Microsoft**, select **Enterprise**.
5. Click **Add**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for Microsoft Enterprise already exists in inventory.	Check the CA Setting name, it should be unique.
1) This field should not be null or empty 2) Mandatory Field(s) - <Field name> is/are empty 3) CA Settings - [<Fields>] mandatory fields cannot be empty.	Some of the mandatory fields might be missing or invalid.	Add all the valid information in the mandatory section.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.

Error Message	Possible Cause	Possible Solution
	may not be configured. 3. AppViewX may not be able to reach CA.	
767cf2b6-bfc3-45a0-9490-a95cf841e693: Connecting to remote server <SERVER> failed with the following error message : WinRM cannot process the request. The following error occurred while using Kerberos authentication: The computer <SERVER> is unknown to Kerberos. Verify that the computer exists on the network, that the name provided is spelled correctly, and that the Kerberos configuration for accessing the computer is correct. The most common Kerberos configuration issue is that an SPN with the format HTTP/<SERVER> is not configured for the target. If Kerberos is not required, specify the Negotiate authentication mechanism and resubmit the operation. For more information, see the about_Remote_Troubleshooting Help topic	Kerberos configuration is not configured for the target machine. The most common Kerberos configuration issue is that an SPN with the format HTTP/<SERVER> is not configured for the target.	The issue occurs with Powershell Remoting since it uses Kerberos Authentication. • In Agent Machine start command prompt as Administrator and execute the following command • setspn -s http/machinename domain\username. • Please note this will work in environments where Kerberos Authentication is set up and there is an AD Domain Setup • If no kerberos authentication is set up then we need to communicate via WMI. • Verify that the computer exists on the network, that the name provided is spelled correctly, and that the Kerberos configuration for accessing the computer is correct. • If Kerberos is not required, specify the Negotiate authentication mechanism and resubmit the operation.

Error Message	Possible Cause	Possible Solution
		For more information, see the about_Remote_Troubleshooting Help topic.
PowerShell ScriptExecution Error: Access is denied. 0x80070005 (WIN32: 5) OR Error Code 0x80070005 - Access is denied	Access is denied.	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group. 3. Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group.
The WinRM client received an HTTP status code of 502 from the remote WS-Management service. For more information, see the about_Remote_Troubleshooting Help topic	Powershell remoting not configured.	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force". 4. Execute "netsh winhttp show proxy" and if a proxy is configured then we need to reset it via "netsh winhttp reset proxy". 5. For more information, see the about_Remote_Troubleshooting Help topic.

Error Message	Possible Cause	Possible Solution
41783361-015b-453f-b321-e31709b1850c: Connecting to remote server <SERVER> failed with the following error message : Access is denied. For more information, see the about_Remote_Troubleshooting Help topic.	Access is denied.	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group. 3. Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group. 4. Check if WinRM service is running. 5. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 6. Execute "Enable-PSRemoting -force". 7. For more information, see the about_Remote_Troubleshooting Help topic.
The client cannot connect to the destination specified in the request. Verify that the service on the destination is running and is accepting requests. Consult the logs and documentation for the WS-Management service running on the destination, most commonly IIS or WinRM. If the destination is the WinRM service, run the following command on the	Powershell remoting is not configured.	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force". 4. Verify that the service on the destination is running and is accepting requests.

Error Message	Possible Cause	Possible Solution
destination to analyze and configure the WinRM service: "winrm quickconfig"		- Consult the logs and documentation for the WS-Management service running on the destination, most commonly IIS or WinRM. - If the destination is the WinRM service, run the following command on the destination to analyze and configure the WinRM service: "winrm quickconfig".
d4f98a6a-41ef-4864-9848-03a07e113d75: CCertRequest::Submit: The RPC server is unavailable. 0x800706ba (WIN32: 1722 RPC_S_SERVER_UNAVAILABLE)	The Remote Procedure Call Service is not responding.	Navigate to the target machine and start RPC service if it has stopped.
727838ed-151e-46bf-883c-07ccb3a3989f: Connecting to remote server ptpld005 failed with the following error message : The user name or password is incorrect. For more information, see the about_Remote_Troubleshooting Help topic.	The username or password is incorrect.	- The username should be configured as "Username@Domain". - The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group. - Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group. - Check if WinRM service is running. - Navigate to Powershell on the target machine and run "WinRM QuickConfig".

Error Message	Possible Cause	Possible Solution
		6. Execute "Enable-PSRemoting -force". 7. For more information, see the about_Remote_Troubleshooting Help topic.
fd3812f9-030a-421c-81e7-0e0510ce49e0: Access to the path <PATH> is denied.	The username or password is incorrect.	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group. 3. Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group.
This site can't be reached	This site can't be reached.	1. Windows Gateway is not reachable from AppViewX. 2. Windows Gateway service is down.
Html response : Access is denied	Access is denied.	1. In Target machine's Local Computer certificate store, Trusted Root Certification Authorities should have Root CA certificates and Intermediate Certification Authorities should have intermediate certificates only. 2. Client certificate used in AppViewX is not imported in Target machine's Local computer store.

Error Message	Possible Cause	Possible Solution
More than 5 connections are not allowed	Powershell configuration has restricted access for concurrent script executions.	Run Powershell as Administrator 1. Check existing config winrm get winrm/config. 2. Change the settings to increase the maxshellsperUser to 100 on the Remote machine wherein this issue is occurring <pre>winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}'</pre> <pre>winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}'</pre> <pre>winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'</pre> .
Connecting to the remote server failed with the following error message : The WS-Management service cannot process the request. This user is allowed a maximum number of 4 concurrent shells, which has been exceeded. Close existing shells or raise the quota for this user.	Powershell configuration has restricted access for concurrent script executions.	Run Powershell as Administrator 1. Check existing config winrm get winrm/config. 2. Change the settings to increase the maxshellsperUser to 100 on the Remote machine wherein this issue is occurring <pre>winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}'</pre> <pre>winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}'</pre> <pre>winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'</pre> .

Error Message	Possible Cause	Possible Solution
Client Certificate gives Permission Denied 403 error. This can happen in certain environment and its intermittent	CA Store mismatch or invalid client certificate used.	1. Check if the Client certificate is installed correctly by checking the chain in the Personal Store. 2. Root of the client certificate should be available in the Trusted Root Certification Store of the Server. 3. Intermediate of the client certificate can be available in the Intermediate Certification authorities of the Server. 4. If all the above looks good then go to the agent server and do the following steps a. MMC. b. Add "Add/Remove SnapIn. c. select certificates. d. select "LocalMachine". e. Navigate to the Personal Store and click on the client certificate. f. Navigate to Chain. g. Export the Root certificate and save it as Root.cer in a location. h. Import the "Root.cer" into trusted Root back again. i. If the issue still remains unsolved, then check if the Trusted root contains and non-root certificates. j. Click on the "Trusted Root" store and check if there are certificates that have

Error Message	Possible Cause	Possible Solution
		different IssuedTo and IssuedBy. k. Take a backup of such certificates and move it to respective stores. l. If the issue remains unsolved, then add the root certificate to "Client Certificate Issuers".
the permission on the certificate template do not allow the current user to enroll for this type of certificate	User does not have access to the certificate template used for enrollment.	1. Navigate to CA Server. 2. open Certificate Authority. 3. Select the CA Server. 4. Right click on properties. 5. Click on Security Tab. 6. Check if the user used in Agent has necessary permissions to read, issue and manage certificates and request certificates. 7. If a user is part of a group then please ensure that the group has permissions. 8. Click on Certificate Templates and right-click to manage templates. 9. Right-click on the template which has the issue and navigate to security. 10. Add permission to the user or group.
An attempt was made to open a Certification Authority database session, but there are already too many active sessions" on a request using CERTADMINLib.IenumCERTVIEWROW.Next().	The Certification Authority database	In CA server navigate to registry via regedit command and set the following:

Error Message	Possible Cause	Possible Solution
	has too many active sessions.	1. HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBSessionCount to 64 hex (100 Dec). 2. HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBMaxReadSessionCount is also set to 64 hex (100 Dec).
803f4314-3a11-486a-87e5-367b8c5c6f9f: The user name or password is incorrect.\r\n	The user name or password is incorrect.	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of the Local Administrator group. 3. Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group
42abe1ef-2bff-40e8-82e2-c97c5707a0c1: Connecting to remote server avxstca failed with the following error message : The user name or password is incorrect. For more information, see the about_Remote_Troubleshooting Help topic.	The user name or password is incorrect.	Check if the credentials are valid.
Connecting to remote server ptpld334 failed with the following error message : WinRM cannot complete the operation. Verify that the specified computer name is valid, that the computer is accessible over the network, and that a firewall exception for the WinRM service is enabled and allows access from this computer. By default, the WinRM firewall exception for public profiles limits access to remote computers within the	Powershell remoting is not configured.	1. C:\Windows\system32>WinRM quickconfig 2. WinRM service is already running on this machine. 3. WinRM is not set up to allow remote access to this machine for management. 4. The following changes must be made:

Error Message	Possible Cause	Possible Solution
same local subnet. For more information, see the about_Remote_Troubleshooting Help topic.		• Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine. • Make these changes [y/n]? y • WinRM has been updated for remote management. • Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.
1. There is not enough space on the disk 2. The WSMAN service could not launch a host process to process the given request. Make sure the WSMAN provider host server and proxy are properly registered. For more information, see the about_Remote_Troubleshooting Help topic. 3. Execute process failed Machinename mspwvadsnybcc01.csc.nycnet, ProcessName Powershell -NoProfile - ExecutionPolicy Bypass -Command C:\\Windows\\Temp\\1jmtip3g.sjl\\1jmtip3g.sjl.ps1, Error is, Stack trace Management Connect to remote machine mspwvadsnybcc01.csc.nycnet as user failed with the following error Value does not fall within the expected range.	There is not enough space on the disk.	Ensure that your hard disk has enough free space.
Management Connect to remote machine VMEUSWPCA021.us.int.safelite.net as user failed with the following error User credentials cannot be used for local connections	User credentials cannot be used for local connections.	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of the Local Administrator group.

Error Message	Possible Cause	Possible Solution
		3. Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group. 4. or configure the credentials in AppViewX.CertPlus.Service Logon option.
Device Communication failed while using Native option to connect to CA remotely	Local System Account doesn't have access to CA. Please change the logon credentials in service.	1. Navigate to agent machine.. 2. Open services.msc using Start>>Run command on the windows machine. 3. Find the service "AppViewXCertPlus". 4. Right-click and view properties. 5. Click "log on" tab. 6. Change the option to this account and enter the user account and password information. 7. Click on "Apply" and a message will pop up to add an account as "Log on as service". Click "OK" and save the changes. 8. Click on restart the service 9. Remove the username and password from AppViewX.

Issues in Enrolling, Fetching, Renewing, Regenerating Microsoft Enterprise certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.

3. From the left pane, expand **Certificate Inventory**.

4. Click **Server/Client/Code Signing Certificate** Tab.

The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.

5. From the menu bar at the top of the page, click **List**.

6. Click any **Microsoft Enterprise certificate**.

A holistic view of **Server Certificate** with the **Certificate number** will be displayed.

7. From the dropdown menu next to the **Certificate**, click **Regenerate**.

• [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	- The configured CA details may be incorrect. - Proxy details may not be configured. - AppViewX may not be able to reach CA.	Check the CA details configured on the CA settings page. Check whether proxy details are configured in proxy settings. Check whether network access is available.
Empty response received from windows gateway.	CA certificate stores may have mixed type certificates.	Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store

Error Message	Possible Cause	Possible Solution
	2. Client certificate may be wrong.	should have Intermediate certificates only. 2. Check whether the client certificate is valid.
The account configured in Application pool identity don't have access to the requested Template	User doesn't have access to the template.	Please give access to the user.
DATA is invalid log message	Invalid header for CSR.	Replace (----BEGIN NEW CERTIFICATE REQUEST----) with (----BEGIN CERTIFICATE REQUEST----) and Replace (----END NEW CERTIFICATE REQUEST----) with (----END CERTIFICATE REQUEST----)
Error Code 0x80070005 - Access is denied	Access not available.	1. Agent and CA Should be under the same domain. 2. ApplicationPoolIdentity of IIS Agent site should be a Custom account with admin credentials. 3. To verify template name, Go to CA portal, Right. Click on Certificate templates, Select Manage, Select the template, right-click on it, and select properties, In General Tab, you can find Template name which needs to be used in AppViewX. 4. To check Template permission, Go to the CA portal, Right. Click on Certificate templates, Select Manage, Select the template,

Error Message	Possible Cause	Possible Solution
		right-click on it and select properties, in the security tab check all permissions given for the user.
Retrieving the COM class factory for remote component with CLSID	Unable to connect to certificate authority.	1. The Component used for accessing CA (certadm.dll) is not installed or has permission issues. 2. Check if dll is available in C:\Windows\System32 folder else install Microsoft Remote Server Administration Tools (RSAT) for the respective OS. EX: for Windows 10 https://www.microsoft.com/en-in/download/details.aspx?id=45520
PowerShell ScriptExecution Error: Access is denied. 0x80070005 (WIN32: 5) OR Error Code 0x80070005 - Access is denied	Access is denied.	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group 3. Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group.
the permission on the certificate template do not allow the current user to enroll for this type of certificate	User does not have access to the certificate	1. Navigate to CA Server. 2. Open Certificate Authority. 3. Select the CA Server. 4. Right-click on properties.

Error Message	Possible Cause	Possible Solution
	template used for enrollment.	- Click on Security Tab. - Check if the user used in Agent has the necessary permissions to read, issue and manage certificates and request certificates. - If a user is part of a group then please ensure that the group has permissions. - Click on Certificate Templates and right-click to manage templates. - Right-click on the template which has the issue and navigate to security. - Add permission to the user or group.
An attempt was made to open a Certification Authority database session, but there are already too many active sessions" on a request using CERTADMINLib.IenumCERTVIEWROW.Next().	The Certification Authority database has too many active sessions.	In CA server navigate to registry via regedit command and set the following: - HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBSessionCount to 64 hex (100 Dec). - HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBMaxReadSessionCount is also set to 64 hex (100 Dec).
The WinRM client received an HTTP status code of 502 from the remote WS-Management service. For more information, see the about_Remote_Troubleshooting Help topic	Powershell remoting not configured.	- Check if WinRM service is running. - Navigate to Powershell on the target machine and run "WinRM QuickConfig".

Error Message	Possible Cause	Possible Solution
		3. Execute "Enable-PSRemoting -force". 4. Execute "netsh winhttp show proxy" and if a proxy is configured then we need to reset it via "netsh winhttp reset proxy".
The client cannot connect to the destination specified in the request. Verify that the service on the destination is running and is accepting requests. Consult the logs and documentation for the WS-Management service running on the destination, most commonly IIS or WinRM. If the destination is the WinRM service, run the following command on the destination to analyze and configure the WinRM service: "winrm quickconfig"	Powershell remoting is not configured.	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force".
More than 5 connections are not allowed	Powershell configuration has restricted access for concurrent script executions.	Run Powershell as Administrator 1. Check existing config 2. winrm get winrm/config. 3. Change the settings to increase the maxshellsperUser to 100 on the Remote machine wherein this issue is occurring: • winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}' • winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}' • winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'.

Error Message	Possible Cause	Possible Solution
Connecting to the remote server failed with the following error message : The WS-Management service cannot process the request. This user is allowed a maximum number of 4 concurrent shells, which has been exceeded. Close existing shells or raise the quota for this user.	Powershell configuration has restricted access for concurrent script executions	Run Powershell as Administrator 1. Check existing config 2. winrm get winrm/config. 3. Change the settings to increase the maxshellsperUser to 100 on the Remote machine wherein this issue is occurring: • winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"} • winrm set winrm/config/winrs '@{MaxShellsPerUser="100"} • winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'.
Client Certificate gives Permission Denied 403 error. This can happen in certain environment and its intermittent	1. Certificate store mismatch. 2. Invalid client certificate specified.	1. Check if the Client certificate is installed correctly by checking the chain in the Personal Store. 2. Root of the client certificate should be available in the Trusted Root Certification Store of the Server. 3. Intermediate of the client certificate can be available in the Intermediate Certification authorities of the Server. 4. If all the above looks good then go to the agent server and do the following steps: a. MMC. b. Add "Add/Remove SnapIn. c. select certificates. d. select "LocalMachine".

Error Message	Possible Cause	Possible Solution
		e. Navigate to the Personal Store and click on the client certificate. f. Navigate to Chain. g. Export the Root certificate and save it as Root.cer in a location. h. Import the "Root.cer" into trusted Root back again. i. If this also doesn't solve the issue then check if the Trusted root contains and non-root certificates. j. Click on the "Trusted Root" store and check if there are certificates that have different IssuedTo and IssuedBy. k. Take a backup of such certificates and move it to respective stores. l. Even after this if it doesn't solve then add the root certificate to "Client Certificate Issuers".
Certificate Request (CSR) is using different account to request certificate from CA as compared to account configured in AppViewX		1. Navigate to the agent machine. 2. Open services.msc using Start>>Run command on the windows machine. 3. Find service "AppViewXCertPlus" 4. Right-click and view properties. 5. Click on "log on" tab

Error Message	Possible Cause	Possible Solution
		6. Change the option to this account and enter the user account and password information. 7. Click on "Apply" and a popup message will appear and ask you to add an account as "Log on as service". Click "OK" and save the changes. 8. Click on restart the service. 9. Remove the username and password from AppViewX.
CSR Parameters invalid error	CSR Parameters supplied mismatch with Selected template/CA's Policy.	Supply valid CSR values accepted by template or CA policy.
Denied by Policy Module 0x80094800, The request was for a certificate template that is not supported by the Active Directory Certificate Services policy: WebServer1.	Incorrect certificate template used.	Use template name instead of the template display name.
Connecting to remote server ptpld334 failed with the following error message : WinRM cannot complete the operation. Verify that the specified computer name is valid, that the computer is accessible over the network, and that a firewall exception for the WinRM service is enabled and allows access from this computer. By default, the WinRM firewall exception for public profiles limits access to remote computers within the same local subnet. For more information, see the about_Remote_Troubleshooting Help topic.	Powershell remoting is not configured.	C:\Windows\system32>WinRM quickconfig WinRM service is already running on this machine. WinRM is not set up to allow remote access to this machine for management. The following changes must be made:

Error Message	Possible Cause	Possible Solution
		• Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine. • Make these changes [y/n]? y • WinRM has been updated for remote management. • Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.

Issues in Revoking Microsoft Enterprise certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Revoke Certificate** submenu.
4. Click **Server/Client/Code Signing Certificate**.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **Microsoft Enterprise certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Revoke**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Invalid reason specified for revocation	Please use the correct reason supported by the CA.

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether client certificate is valid.

Issues in Suspending Microsoft Enterprise certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and Click **Server/Client/Code Signing Certificate**.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
4. From the menu bar at the top of the page, click **List**.
5. Click any **Microsoft Enterprise certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
6. From the dropdown menu next to the **Certificate**, click **Suspend**.

• [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Invalid reason specified for suspension.	Please use the correct reason supported by the CA.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured in the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether client certificate is valid.

Issues in Reinstating Microsoft Enterprise certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and Click **Server/Client/Code Signing Certificate**.
The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
4. From the menu bar at the top of the page, click **List**.
5. Click any suspended **Microsoft Enterprise certificate**.
A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
6. From the dropdown menu next to the **Certificate**, click **Reinstate**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Invalid reason specified for reinstatement.	Please use the correct reason supported by the CA.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured in the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.

Issues in Discovering Microsoft Enterprise certificates

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery** and select **Discovery**.
4. Click **Certificate Authority Scan**.
The **Discovery: Certificate Authority Scan: Add Discovery** page is displayed.

5. Select **CA** as **Microsoft Enterprise**.
6. Click **Discover** at the bottom of the page.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.

Troubleshooting Microsoft Tomcat

- [Overview](#)
- [Issues in Microsoft Tomcat Server](#)

Overview

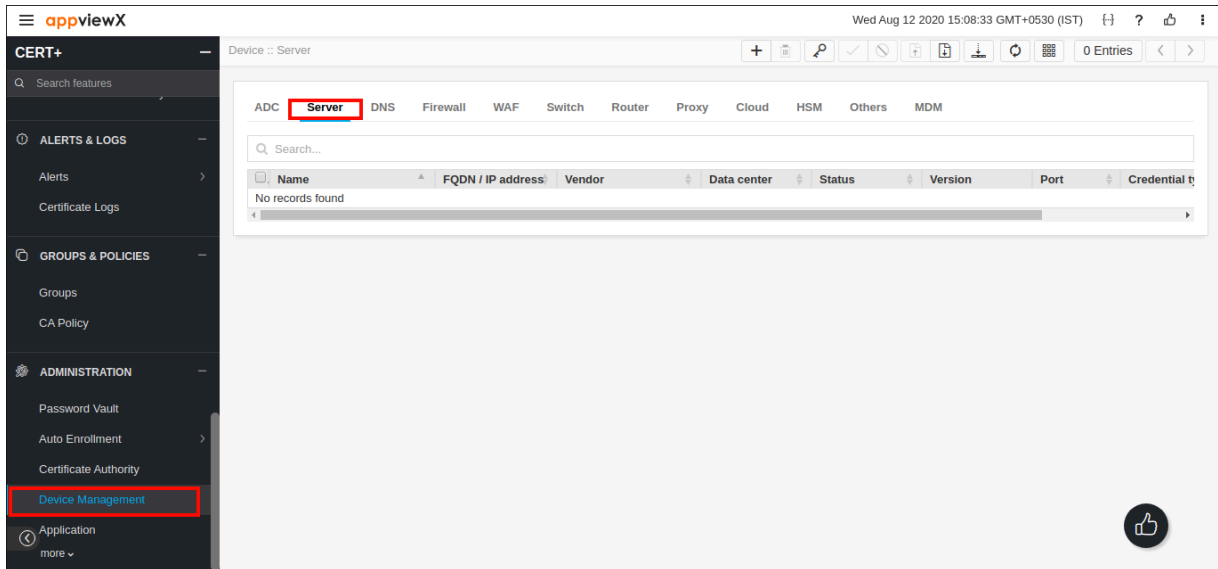
This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with Microsoft Tomcat server.

Issues in Microsoft Tomcat Server

- [Issues in Microsoft Tomcat Server Addition using AppViewX UI](#)
- [Issues in Communicating to Tomcat Server](#)
- [Issues in Accessing Server](#)
- [Issues in Config Fetch](#)
- [Issues in Certificate Discovery](#)
- [Issues in CSR generation](#)
- [Issues in Push and Rollback](#)

Issues in Microsoft Tomcat Server Addition using AppViewX UI

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. From the icon list at the top right corner, click **Add**.
The **Device Addition** page is displayed.
6. From the **Device Details Section** on the left, click **APACHE Microsoft, server type Tomcat**.
7. Fill in the appropriate details.
8. Click **Add**.



Device :: Server > Add

Vendors

- APACHE Linux
- Microsoft IIS
- Microsoft PC
- Microsoft Server
- APACHE Microsoft
- Microsoft SQL
- ORACLE
- IBM
- hp
- DELL
- Linux
- ARBOR

Server details

* Server type ☐ Apache ☒ Tomcat

* Server name

* Hostname

Data center

Communication mode ☒ Gateway ☐ SSM

Cert sync ☒ Managed ☐ Monitored ☐ Ignored

Credentials

* Credential type

* Username

* Password

Windows gateway details

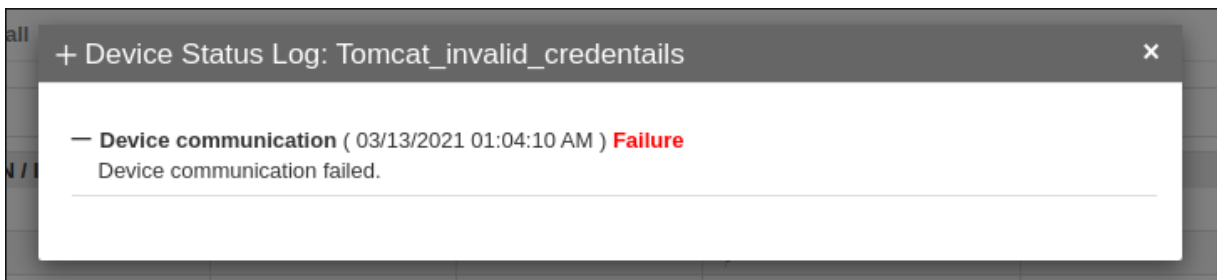
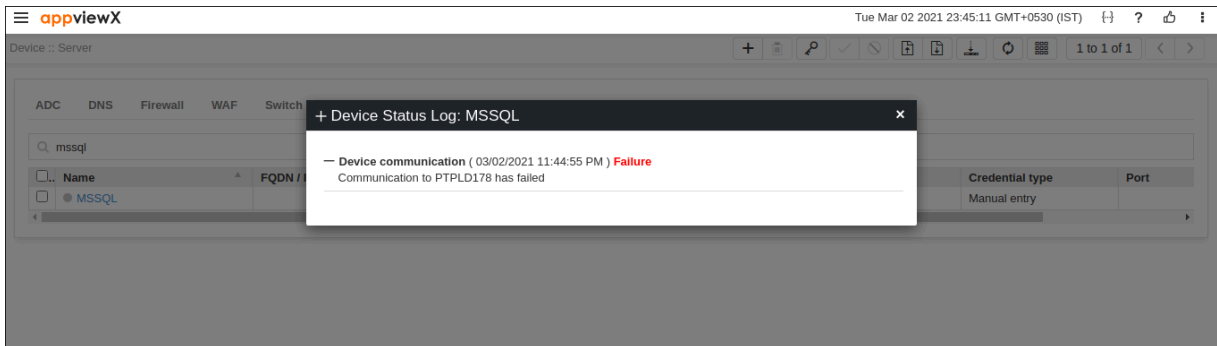
• Error Messages

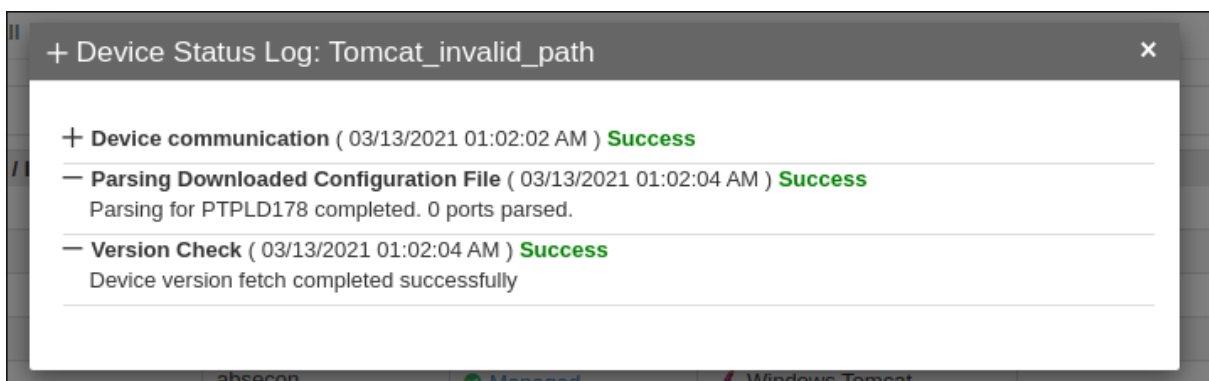
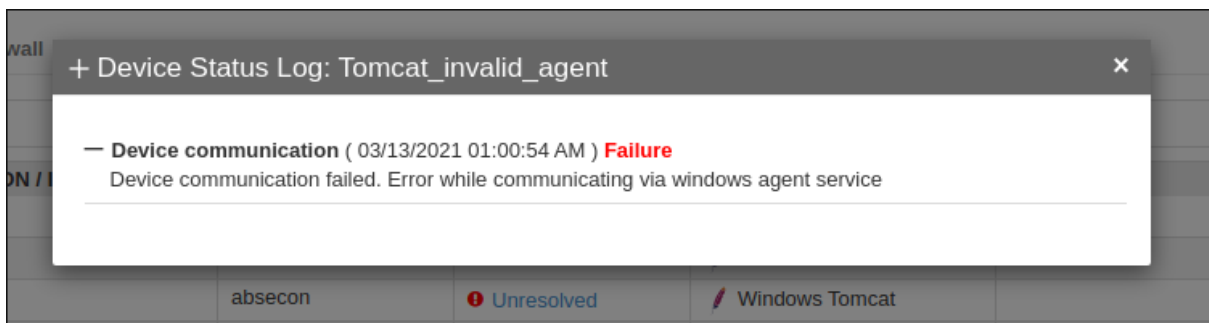
Error Messages

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Communicating to Tomcat Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**.
The **Device Communication Status** is displayed.





- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-', '_', '.', '*', ' ', '!' and spaces.
Communication to <hostname> has failed	Hostname / Username / Password of the	Click on the device name in the Inventory Page. Update the correct details and click Save.

Error Message	Possible Cause	Possible Solution
	device added might be wrong.	
Communication to <Hostname> has failed due to Error while communicating via windows agent service	Windows agent provided is not reachable	Check Windows agent is Up and running and update the valid agent in the device addition page.
Parsing for PTPLD178 completed. 0 ports parsed.	Invalid Tomcat Server path	Login manually into the windows server and find the Tomcat installation directory path and provide the same path in Server path attribute of tomcat device addition page
Error on fetching Tomcat instance, config fetch process failed due to df9cbf67-e1af-4d8c-8a7c-fe88bb83e0b3: PowerShell ScriptExecution Error in PTPLD178 : Cannot find path 'C:\tmp_1615504487924.tmp' because it does not exist.	Invalid Server path	Login manually into the windows server and find the Tomcat installation directory path and provide the same path in Server path attribute of tomcat device addition page

Issues in Accessing Server

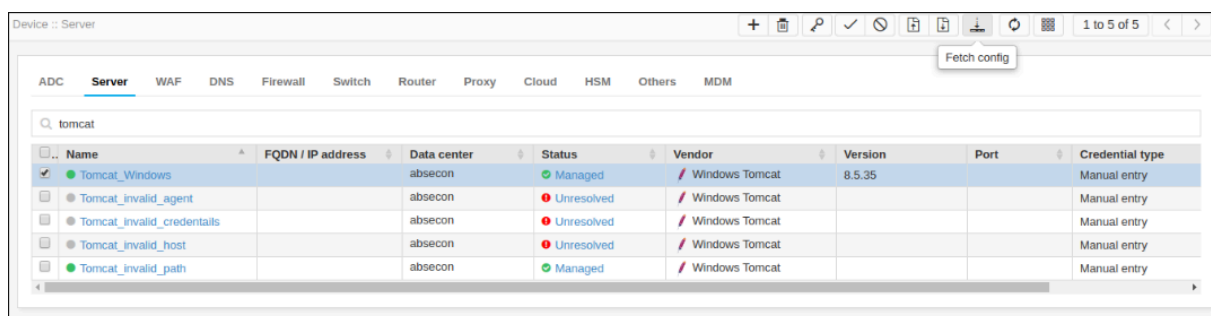
Access Issues might be reproduced when communicating with servers while discovering or fetching configuration files. These errors can be collected either from logs, API responses, or in the status field for the particular server.

Error Message	Possible Cause	Possible Solution
Permission denied for file/location.	1. File might not be present in the avx environment. 2. user might not have permission to read in the given source location	1. Check whether someone deleted the file from AppViewX environment. 2. Verify if read permission is given for the location.

Error Message	Possible Cause	Possible Solution
	3.Device communication might not be established when service has started.	3.Verify the device connection and restart the service.

Issues in Config Fetch

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Fetch Config**.



- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Communication to <hostname> has failed	Hostname / Username / Password of the device added might be wrong.	1.Verify the input details and check for device status error messages Issues in Communicating to Tomcat Server

Issues in Certificate Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.

The **Server Certificate** page is displayed.

3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	- Discovery name is not given or length is less than 2 characters. - Interval between batches info. is missing when execution type is sequential.	- Enter a valid name with a minimum of 2 characters. - Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.

Issues in CSR generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab.
The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, click correct **Category**.
7. From the **Vendor** dropdown, click **Windows Tomcat**.

A list of devices will be generated in the **Devices** dropdown.

CERT+ — Enroll Server Certificate

Q Search features

DASHBOARD

CERTIFICATE ACTION —

- Enroll Certificate >
- Renew Certificate >
- Push to Device >
- Reissue Certificate >
- Revoke Certificate >
- more v

CERTIFICATE INVENTORY —

- Server
- Client
- Code Signing Certificate
- Device
- Intermediate
- more v

* CSR Generation ☐ AppViewX ☐ Upload CSR ☐ HSM ☒ End Point

Category

Vendor

* Devices

* CSR file name .csr

* Key File Name .key

CSR Parameters

* Common Name

Subject Alternative Name

DNS 0 value ⓘ

Add **Reset**

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Problem while generating csr on target server	General Failure - SSH/SFTP communication failure	Provide correct credentials and make sure device communication is successful.
Invalid key type specified in the request	Given key type might not be supported by open SSL in the target machine.	Provide valid key type.
Problem while generating csr on the target server.	Location might not have permission.	Check the permission and provide it.
CSR and Private key has been failed	Open SSL configuration might be wrong in the target machine.	Check and correct open SSL configuration in the device.
CSR generation got failed	User has restricted access to the path configured for the "CSR FileName" and "Key File name"	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issues in Push and Rollback

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**.
The **Server Certificate** page is displayed.
4. Click any **Windows Tomcat server**.
A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, select **Add App Connector**.
6. Push the certificate to the device.

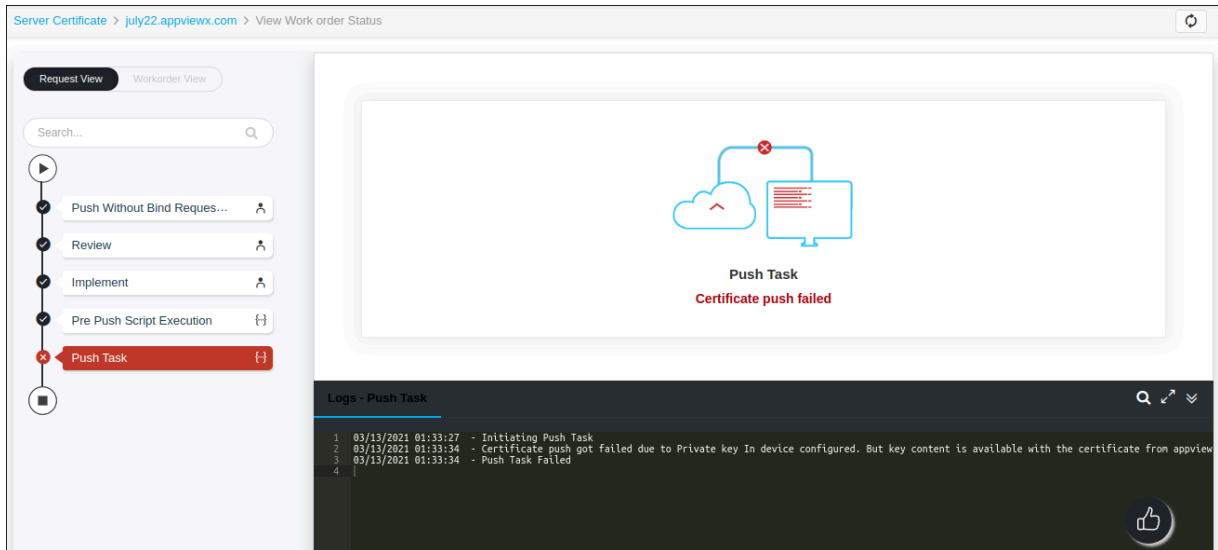
Troubleshooting Server, Firewalls, WAF, and Rapid SB Connectors

The screenshot displays the CERT+ interface for a 'Server Certificate' on 'cert.test.com'. The left sidebar shows the 'AUTOMATION' section with a workflow diagram. The 'Push Task' step is highlighted in red, indicating a failure. The main panel shows a diagram of a cloud and a server with a red 'X' over the connection, and the text 'Push Task Certificate push failed'. Below this, the 'Logs - Push Task' section shows the following log entries:

Line	Timestamp	Event
1	02/25/2021 11:57:54	- Initiating Push Task
2	02/25/2021 11:58:57	- Certificate Push Failed
3	02/25/2021 11:58:58	- Push Task Failed
4		

The screenshot displays the CERT+ interface for a 'Server Certificate' on 'cert.test.com'. The left sidebar shows the 'AUTOMATION' section with a workflow diagram. The 'Push Task' step is highlighted in red, indicating a failure. The main panel shows a diagram of a cloud and a server with a red 'X' over the connection, and the text 'Push Task Certificate push failed'. Below this, the 'Logs - Push Task' section shows the following log entries:

Line	Timestamp	Event
1	02/25/2021 12:07:34	- Initiating Push Task
2	02/25/2021 12:07:37	- PrivateKey in device push invalid
3	02/25/2021 12:07:37	- Push Task Failed
4		



- Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.

Error Message	Possible Cause	Possible Solution
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e. in a new state.	Push to device after certificate has been retrieved from CA.
Certificate Push failed	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/write access to the path configured in application connector to certificate push.
Certificate push failed due to Private key In device configured. But key content is available with the certificate from appview pushRequest So failing push request.	"Private key in Device" is enabled in application connector and also private key is available in the certificate	Ensure "Private key in Device" attribute in application connector is unchecked.
PrivateKey in device push invalid	"Private key in Device" is enabled in application connector, but key is not available in device.	Ensure to enable "Private key in Device" attribute in application connector, if the certificate does not have the key and the certificate is generated using CSR gen option from Device.

Troubleshooting MQServer Linux

- [Overview](#)
- [Issues in MQServer Linux](#)

Overview

This section will guide you to overcome the various issues faced by you during the use of MQServer Linux and its various functionalities.

Issues in MQServer Linux

- [Issues in Device communication](#)
- [Issues in Certificate Discovery](#)
- [Issues in CSR generation at Endpoint](#)
- [Issues in Certificate Push](#)

Issues in Device communication

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**.

The **Device Communication Status** is displayed.

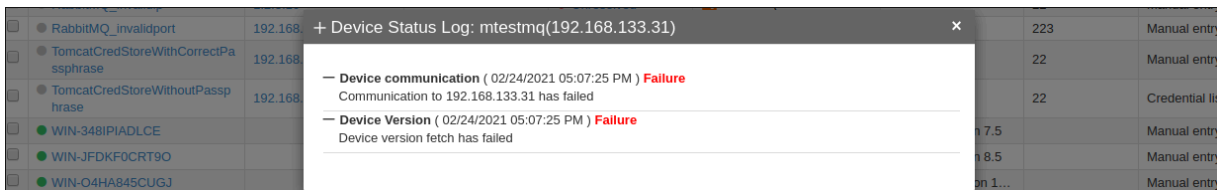
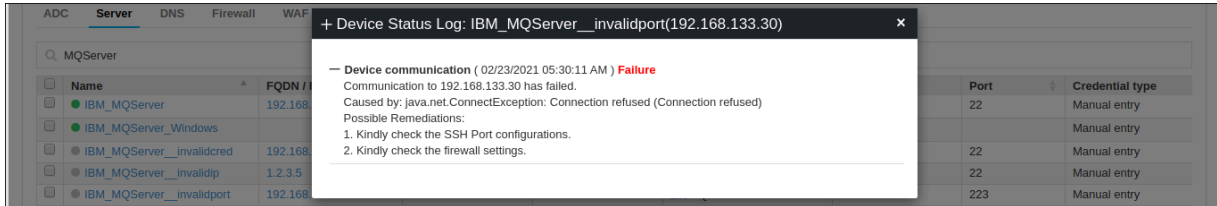
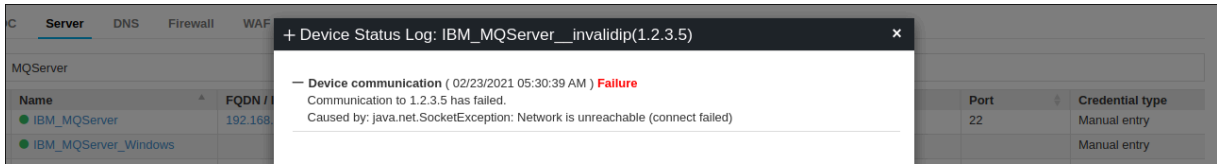
☐	IBM_MQServer__invalidcred	192.168.133.30	Unresolved	MQServer	8.0.0.4	22	Manual entry
☐	IBM_MQServer__invalidip	1.2.3.5	Unresolved	MQServer		22	Manual entry
☐	IBM_MQServer__invalidport	192.168.133.30	Unresolved	MQServer	8.0.0.4	223	Manual entry

+ Device Status Log: IBM_MQServer__invalidcred(192.168.133.30)

— Device communication (02/23/2021 05:30:13 AM) **Failure**

Communication to 192.168.133.30 has failed.
Caused by: java.io.IOException: Unable to authenticate with password, keyboard-interactive and publickey methods
Possible Remediations:
1. Kindly check the credentials provided.

Name	FQDN	Port	Credential type
IBM_MQServer	192.168.133.30	22	Manual entry
IBM_MQServer_Windows			Manual entry
IBM_MQServer__invalidcred	192.168.133.30	22	Manual entry
IBM_MQServer__invalidip	1.2.3.5	22	Manual entry
IBM_MQServer__invalidport	192.168.133.30	223	Manual entry



• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Communication to <ip/fqdn> has failed. Caused by: java.io.IOException: Unable to authenticate with password, keyboard-interactive and publickey methods Possible Remediations: 1. Kindly check the credentials provided.	Password of the device added could be wrong.	Click on the device name on the Inventory Page. Update the correct password and click Save.

Error Message	Possible Cause	Possible Solution
Communication to <ip/fqdn> has failed. Caused by: java.net.SocketException: Network is unreachable (connect failed)	IP/FQDN provided is not reachable	Check manually by establishing an SSH session to the target device with the provided IP/FQDN.
Communication to <IP/FQDN> has failed. Caused by: java.net.ConnectException: Connection refused (Connection refused) Possible Remediations: 1. Kindly check the SSH Port configurations. 2. Kindly check the firewall settings	Problem with port configuration	Check if the configured port in the device addition page is correct.
Device communication (02/24/2021 05:07:25 PM) Failure Communication to 192.168.133.31 has failed Device Version (02/24/2021 05:07:25 PM) Failure Device version fetch has failed	MQ is not configured in the target device	Check if MQ server is configured in the target device Check MQ toolkit is installed in the target device
Device communication (02/24/2021 06:12:50 PM) Failure Communication to 192.168.133.30 has failed. Caused by: java.io.IOException: Key exchange was not finished, connection is closed.	Problem with SSH key handshake	Request to check the ciphers, key and HMacS configured in the target device and ensure AppViewX SSH-plugin supports the same

Issues in Certificate Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

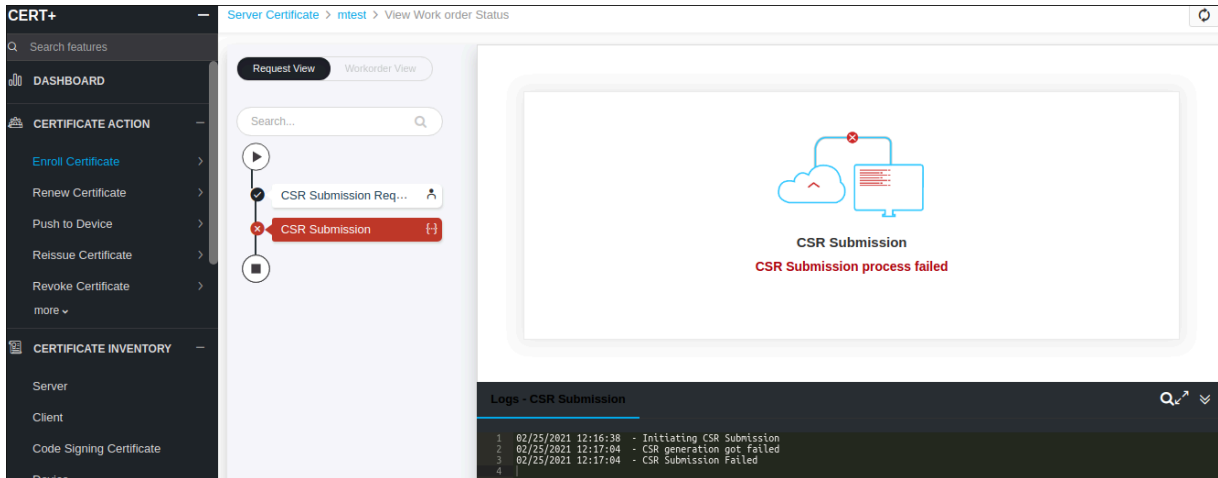
• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Received failed response from batch	MQServer QManager is not up and running.	1. Login to the target device 2. Switch to user which has mqm group access 3. start the QManager Command: <pre>strmqm <qname></pre>
Received failed response from batch	No valid KDB files available in the path configured to the QManager	Ensure the path configured in QManager has valid KDB files and KDB has certs. Command to find path: <pre>echo "DIS QMGR SSLKEYR" runmqsc</pre>

Issues in CSR generation at Endpoint

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab.
The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, click correct **Category**.
7. From the **Vendor** dropdown, click **MQServer**.
A list of devices will be generated in the **Devices dropdown**.



• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
CSR generation got failed	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issues in Certificate Push

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**.
The **Server Certificate** page is displayed.
4. Click any **Linux server**.
A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions** with “**Create KDB**” profile, click **Add App Connector**.
6. Push the certificate to the device.

CERT+

Search features

Revoke Certificate

CERTIFICATE INVENTORY

Server

Client

Code Signing Certificate

Device

Intermediate

AUTOMATION

My Workflows

My Requests

Server Certificate > cert.test.com > View Work order Status

Request View Workorder View

Search...

Push and Bind Requ...

Review

Implement

Pre Push Script Exec...

Backup Task

Push Task

Push Task

Certificate push failed

Logs - Push Task

1	02/25/2021 11:57:54	- Initiating Push Task
2	02/25/2021 11:58:57	- Certificate Push Failed
3	02/25/2021 11:58:58	- Push Task Failed
4		

CERT+

Search features

Revoke Certificate

CERTIFICATE INVENTORY

Server

Client

Code Signing Certificate

Device

Intermediate

AUTOMATION

My Workflows

My Requests

Server Certificate > cert.test.com > View Work order Status

Request View Workorder View

Search...

Push and Bind Requ...

Review

Implement

Pre Push Script Exec...

Backup Task

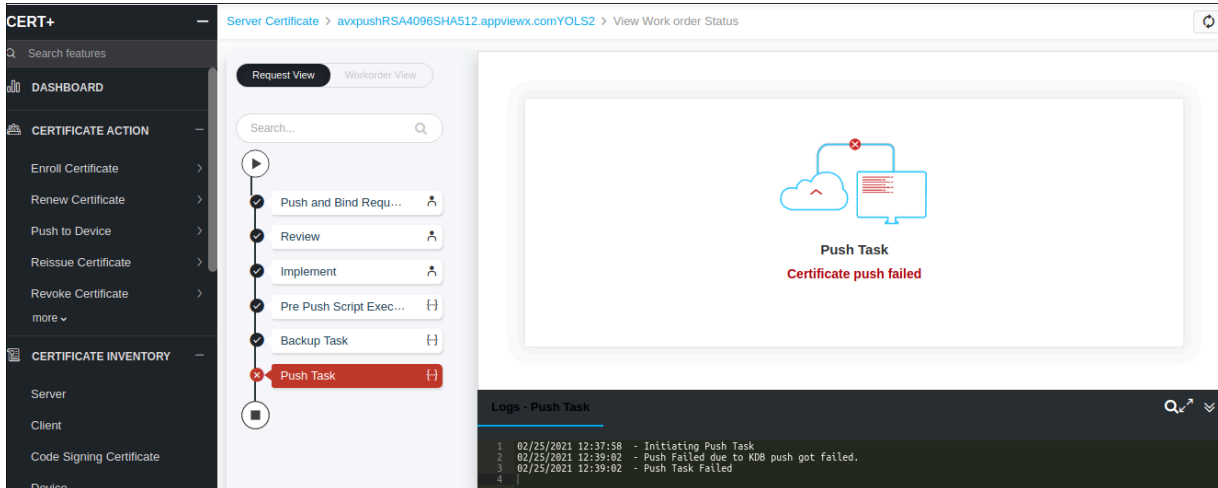
Push Task

Push Task

Certificate push failed

Logs - Push Task

1	02/25/2021 12:07:34	- Initiating Push Task
2	02/25/2021 12:07:37	- PrivateKey in device push invalid
3	02/25/2021 12:07:37	- Push Task Failed
4		



- Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Certificate Push failed	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/write access to the path configured in application connector to certificate push.
PrivateKey in device push invalid	“Private key in Device” is enabled in application connector, but key is not available in device.	Ensure to enable “Private key in Device” attribute in application connector, if the certificate does not have the key and the certificate is generated using CSR gen option from Device.
Push Failed due to KDB push got failed.	Target KDB file does not exist in the device	Ensure the target KDB file, for which certificate push configured is available and has read/write access.

Troubleshooting MQServer Windows

- [Overview](#)
- [Issues in MQServer Windows](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with MQServer Windows.

Issues in MQServer Windows

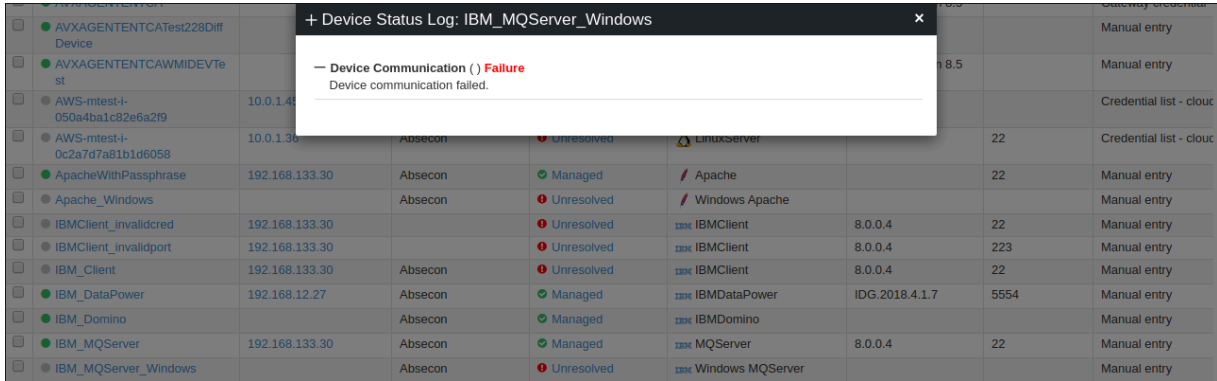
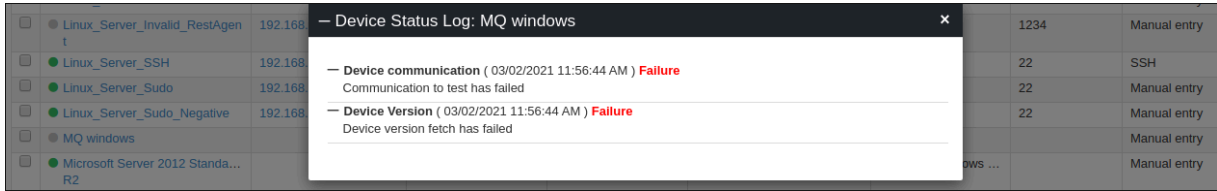
- [Issues in Device communication](#)
- [Issue in Discovery](#)
- [Issues in CSR generation at Endpoint](#)
- [Issues in Certificate Push](#)

Issues in Device communication

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**.

The **Device Communication Status** is displayed.

MQ windows	Absecon	Unresolved	Windows MQServer	Manual entry



• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Communication to <hostname> failed	Gateway agent not reachable. Device not reachable from the gateway agent	Ensure gateway is configured properly and the APIs are accessible from AppViewX. Ensure device and gateway agent are in the same domain and device is accessible from gateway agent.
Communication to <hostname> failed Device version fetch has failed.	Hostname or Credentials configured is wrong	Ensure hostname and the device credentials configured while device addition is valid.

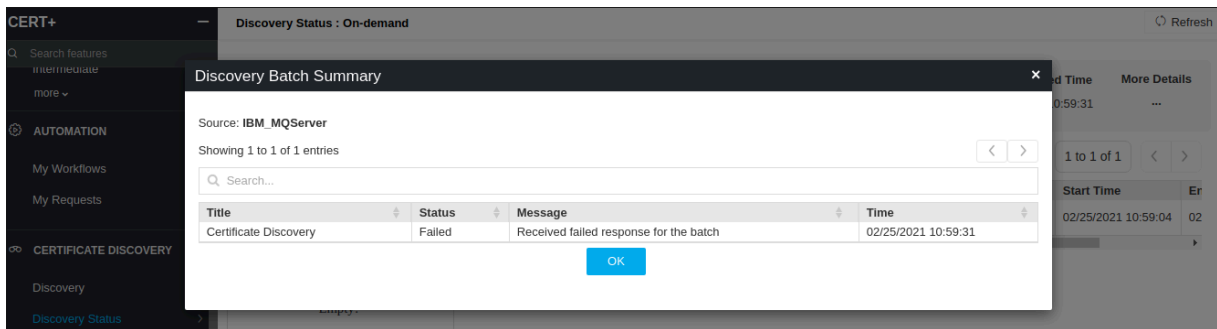
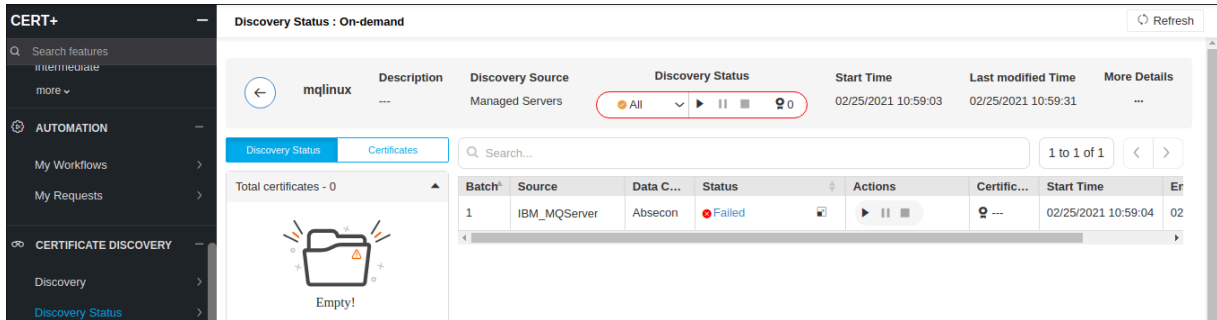
Issue in Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.

4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.



• **Error Messages**

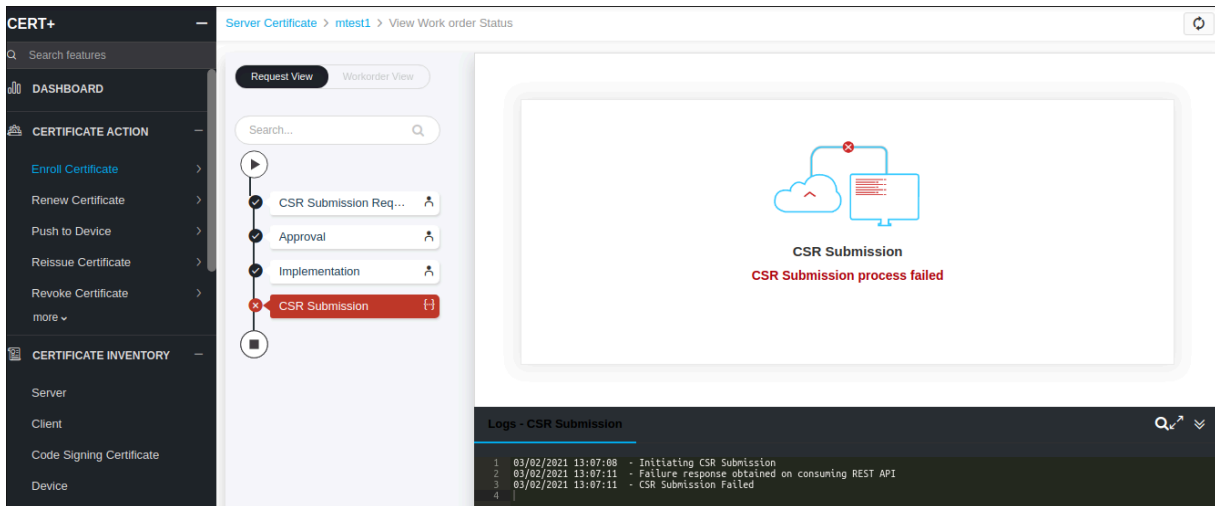
Error Messages

Error Message	Possible Cause	Possible Solution
Received failed response from batch	MQServer QManager is not up and running.	1. Login to the target device 2. Switch to user which has mqm group access 3. start the QManager Command:

Error Message	Possible Cause	Possible Solution
		strmqm <qname>
Received failed response from batch	No valid KDB files available in the path configured to the QManager	Ensure the path configured in QManager has valid KDB files and KDB has certs. Command to find path: echo "DIS QMGR SSLKEYR" runmqsc.

Issues in CSR generation at Endpoint

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab.
The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, Click correct **Category**.
7. From the **Vendor** dropdown, click **Windows MQServer**.
A list of devices will be generated in the **Devices** dropdown.



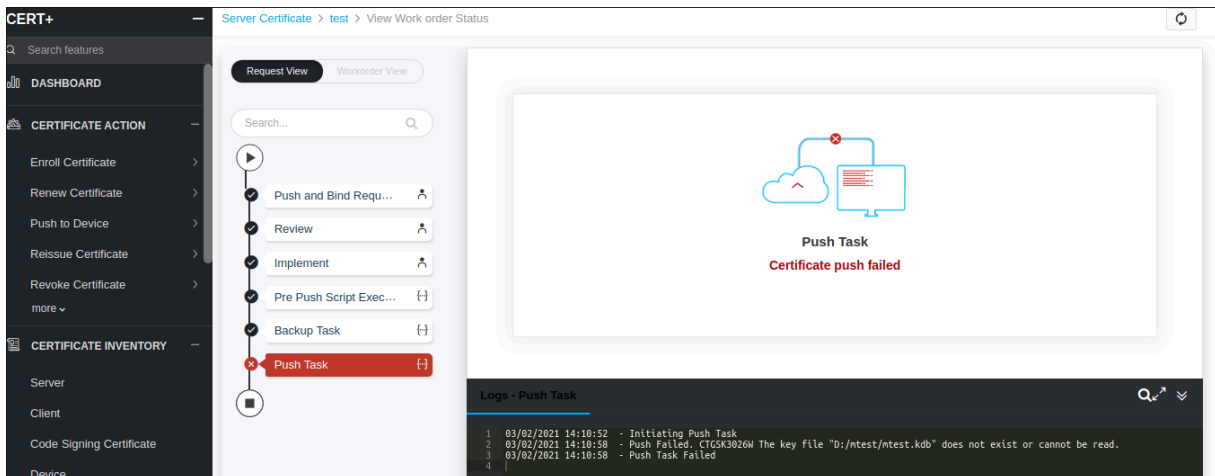
• Error Messages

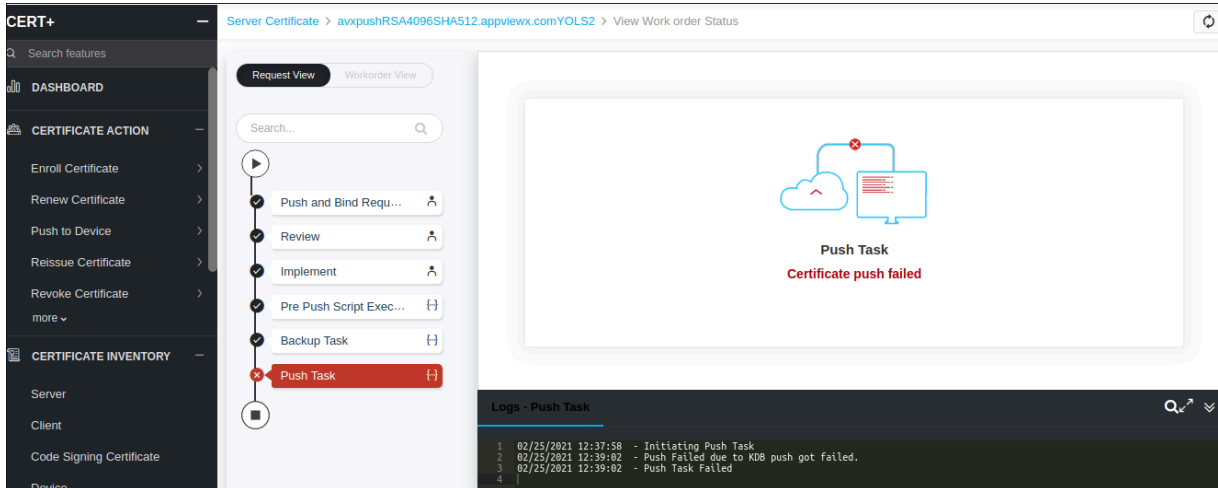
Error Messages

Error Message	Possible Cause	Possible Solution
Failure response obtained on consuming REST API. CSR submission failed	User has restricted access to the path configured for the "CSR FileName" and "Key File name"	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issues in Certificate Push

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**.
The **Server Certificate** page is displayed.
4. Click any **Linux server**.
A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions** with "Create KDB" profile, select **Add App Connector**.
6. Push the certificate to the device.





- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Push Failed. CTGSK3026W The key file "D:/mtest/mtest.kdb" does not exist or cannot be read.	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/write access to the path configured in application connector to certificate push.
Push Failed due to KDB push got failed.	Target KDB file does not exist in the device	Ensure the target KDB file, for which certificate push configured is available and has read/write access.

Troubleshooting MS SQL Windows

- [Overview](#)
- [Issues in MS SQL Windows](#)

Overview

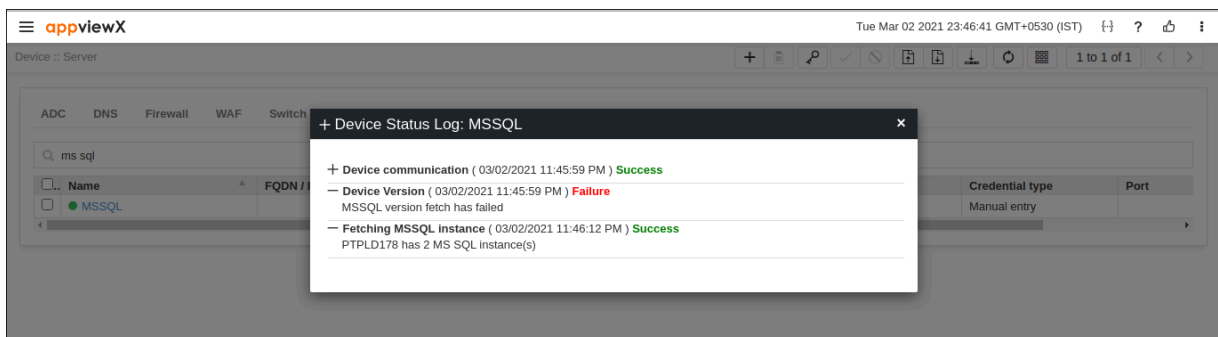
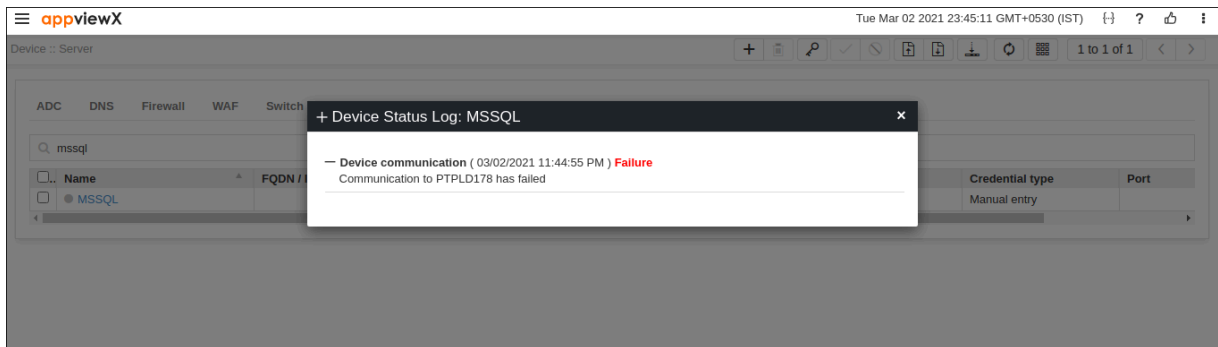
This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback and other actions associated with MS SQL Windows.

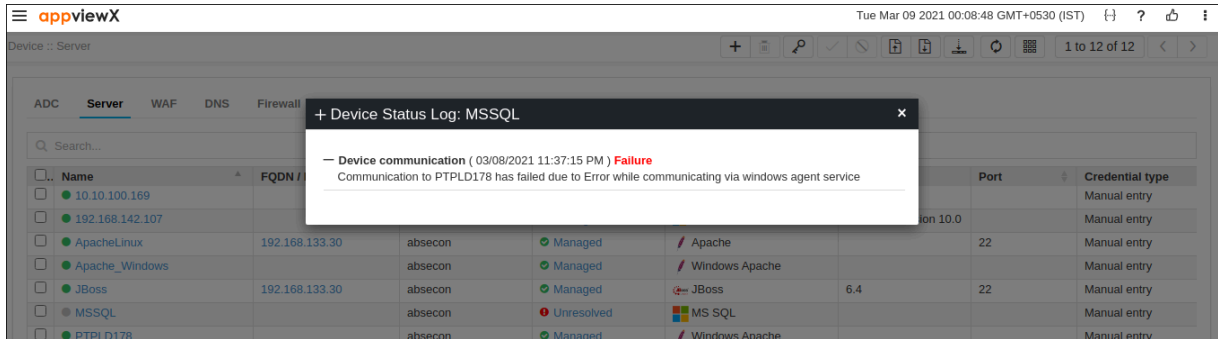
Issues in MS SQL Windows

- Issues in Communicating to MS SQL
- Issues in Config Fetch
- Issue in Discovery
- Issue in CSR generation
- Issue in Push and Rollback

Issues in Communicating to MS SQL

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**.
The **Device Communication Status** is displayed.





- Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Communication to <hostname> has failed	Gateway agent not reachable. Device not reachable from the gateway agent	Ensure gateway is configured properly and the APIs are accessible from AppViewX. Ensure device and gateway agent are in the same domain and device is accessible from gateway agent.
Communication to <hostname> has failed	Hostname or Credentials configured is wrong	Ensure hostname and the device credentials configured while device addition is valid.
Device version fetch has failed.	MSSQLSERVER service instance is down	Restart the MSSQLSERVER instance
Device version fetch has failed.	Command not supported by MS SQL version	Execute the version command SQLCMD -Q 'SELECT @@VERSION;' -t 3 in the CLI of the device to check if it returns version response

Issues in Config Fetch

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Fetch Config**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Communication to <hostname> has failed	Gateway agent not reachable. Device not reachable from the gateway agent	Ensure gateway is configured properly and the APIs are accessible from AppViewX. Ensure device and gateway agent are in the same domain and device is accessible from gateway agent.
PTPLD178 has 0 instances.	No installed MS SQL instances. Installed instances are not up and running.	Execute (get-itemproperty 'HKLM:\\SOFTWARE\\Microsoft\\Microsoft SQL Server').InstalledInstances in the device as a powershell script and check if it returns the MS SQL instances

Issue in Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

• Error Messages

Error Messages

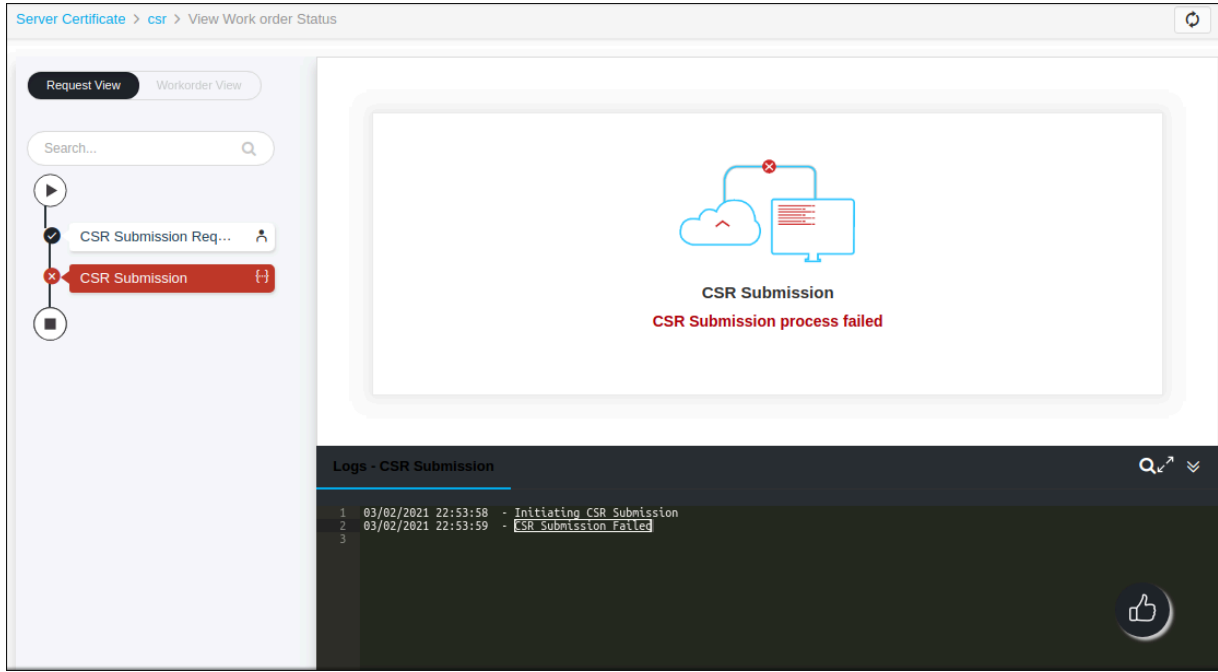
Error Message	Possible Cause	Possible Solution
Received failed response from batch	No valid certificates in store that are binded to the MS SQL instances.	Ensure the certificates are binded to a MS SQL instance.

Issue in CSR generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab.
The **Enroll Server Certificate** page is displayed.

5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, click correct **Category**.
7. From the **Vendor** dropdown, click **MS SQL**.

A list of devices will be generated in the **Devices dropdown**.



• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
CSR Submission Failed	User may have restricted access to the path configured for the "CSR FileName" and "Key File name"	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issue in Push and Rollback

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**.

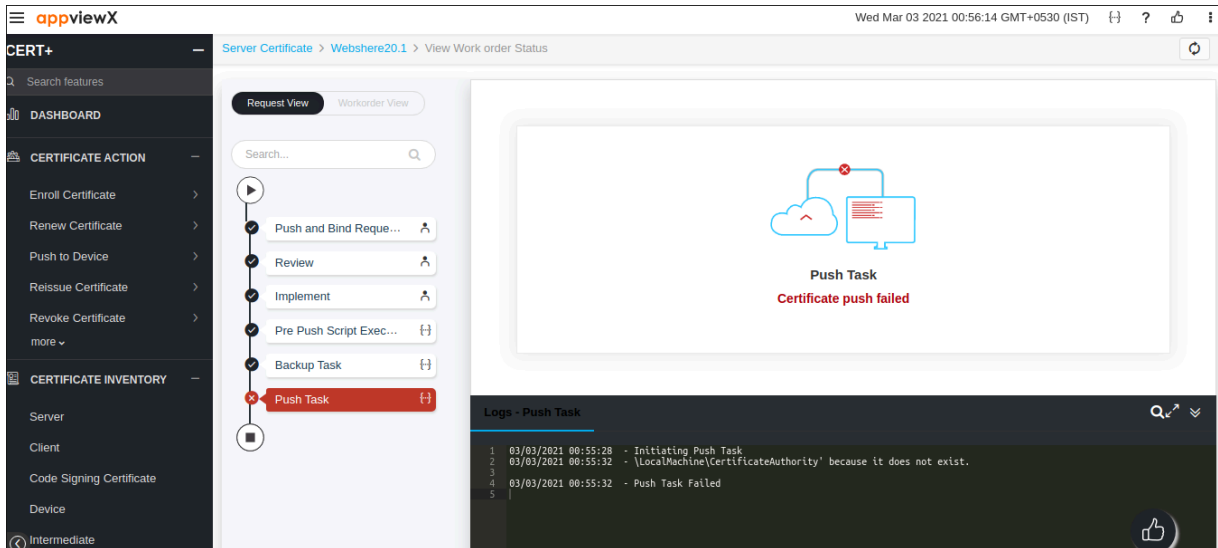
The **Server Certificate** page is displayed.

4. Click any **server**.

A holistic view of the **Certificate** will be displayed.

5. From the dropdown of **Connector Actions**, select **Add App Connector**.

6. Push the certificate to the device.



• Error messages

Error messages

Error Message	Possible Cause	Possible Solution
Error while pushing certificate in Device : <device name>.PrivateKey not available.	Private key is not available to parse certs.	Kindly ensure to push certs with private key.If privatekey is available in device please select privateKeyInDevice option.
Error: "/LOCAL_MACHINE/CertificateAuthority" does not exist	CertificateAuthority Store is removed from the Store	Create a CertificateAuthority store.

Troubleshooting Nginx Server

- [Overview](#)
- [Issues in Nginx Server](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using certificate Nginx Server functionalities.

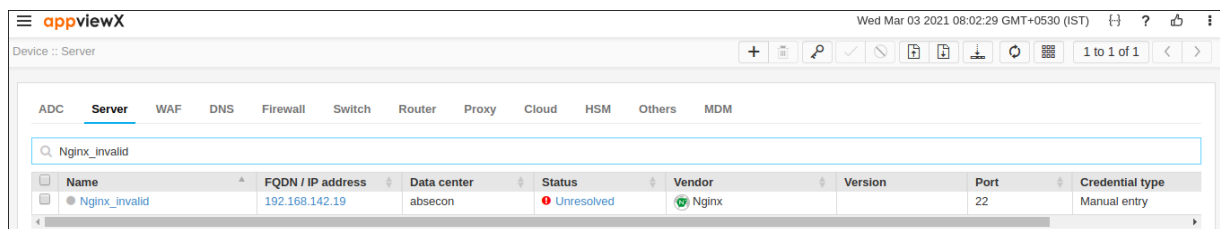
Issues in Nginx Server

- [Issues in Device communication](#)
- [Issue in Discovery](#)
- [Issues in CSR generation at Endpoint](#)
- [Issues in Certificate Push](#)

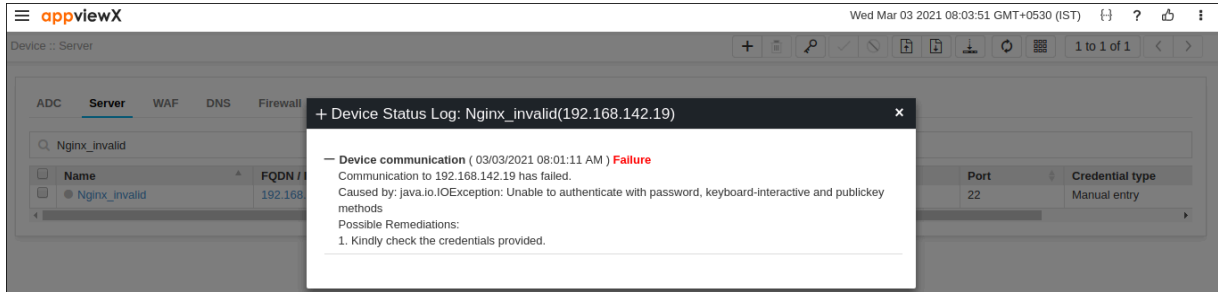
Issues in Device communication

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the **Nginx** Device, click **Status**.

The **Device Communication Status** is displayed.



Name	FQDN / IP address	Data center	Status	Vendor	Version	Port	Credential type
Nginx_invalid	192.168.142.19	absecon	Unresolved	Nginx		22	Manual entry



• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Communication to <IP> has failed. Caused by: java.io.IOException: Unable to authenticate with password, keyboard-interactive and publickey methods Possible Remediations: 1. Kindly check the credentials provided.	1. Given credentials are incorrect. 2. Given IP may be incorrect. 3. Device not reachable	1. Check and input the correct credential. 2. Check and input the correct IP 3. Ensure device is up and accessible

Issue in Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

ADCServerWAFDNSFirewallSwitchRouterProxyCloudHSMOthersMDM

nginx

Name	FQDN / IP address	Data center	Status	Vendor	Version	Port	Credential type
nginx	192.168.142.19	absecon	Managed	nginx	1.19.0 (nginx-plus-r...	22	Manual entry

Search...			
Title	Status	Message	Time
Certificate Discovery	Failed	Received failed response for the batch	02/25/2021 18:12:05
OK			

• Error Messages

Error Messages

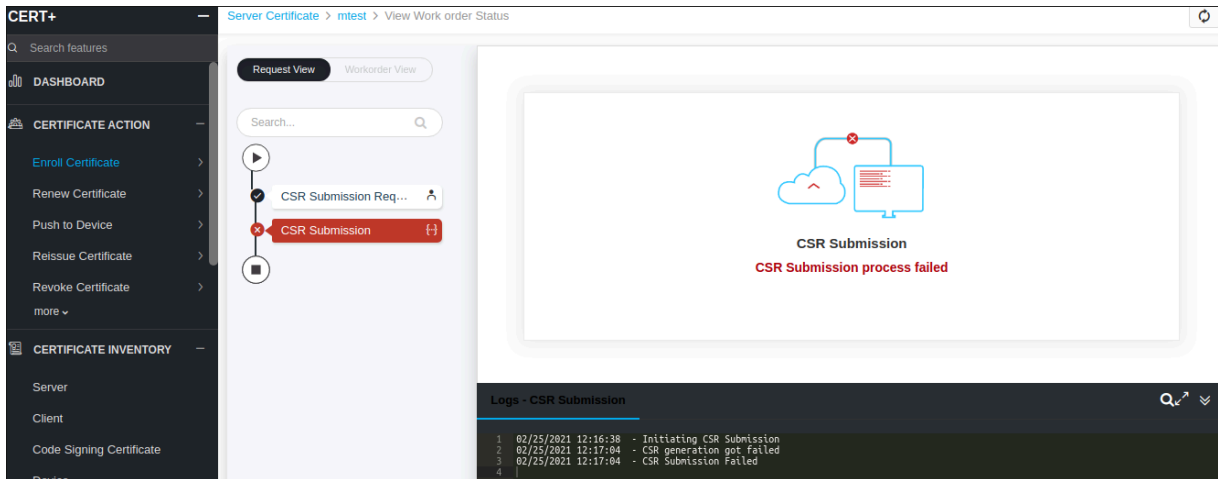
Error Message	Possible Cause	Possible Solution
Received failed response from batch	1. Device not running or not accessible 2. No valid certificates available	1. Ensure target device is up and running 2. Check the device has valid certificate files

Issues in CSR generation at Endpoint

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab.
The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, click correct **Category**.

7. From the **Vendor** dropdown, click **Nginx** device.

A list of devices will be generated in the **Devices** dropdown.



• Error Messages

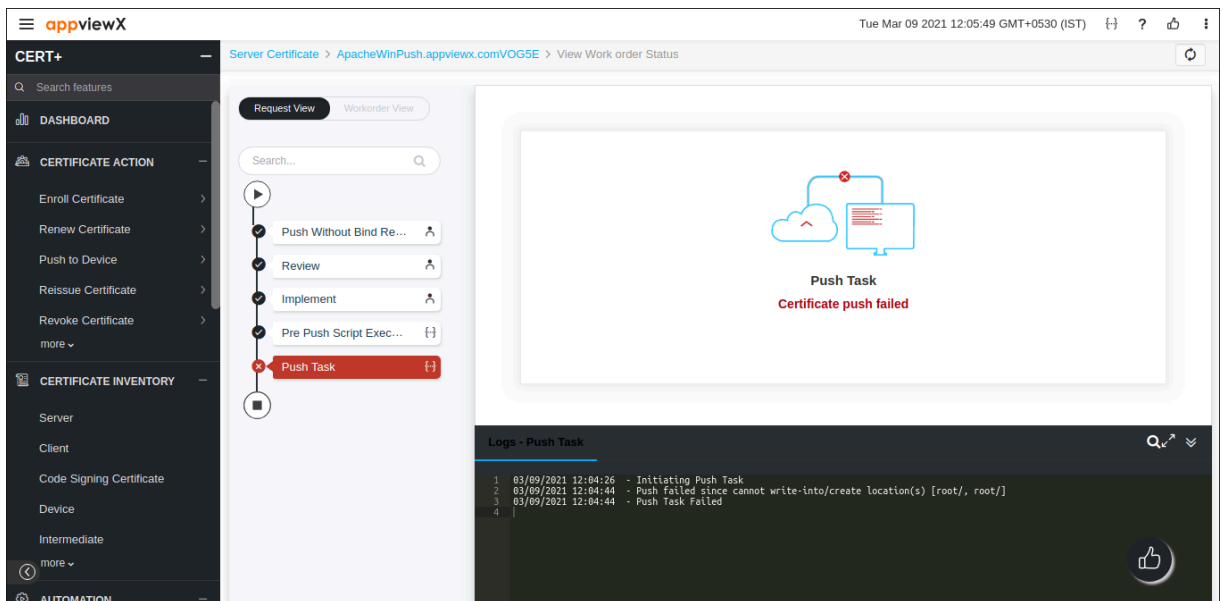
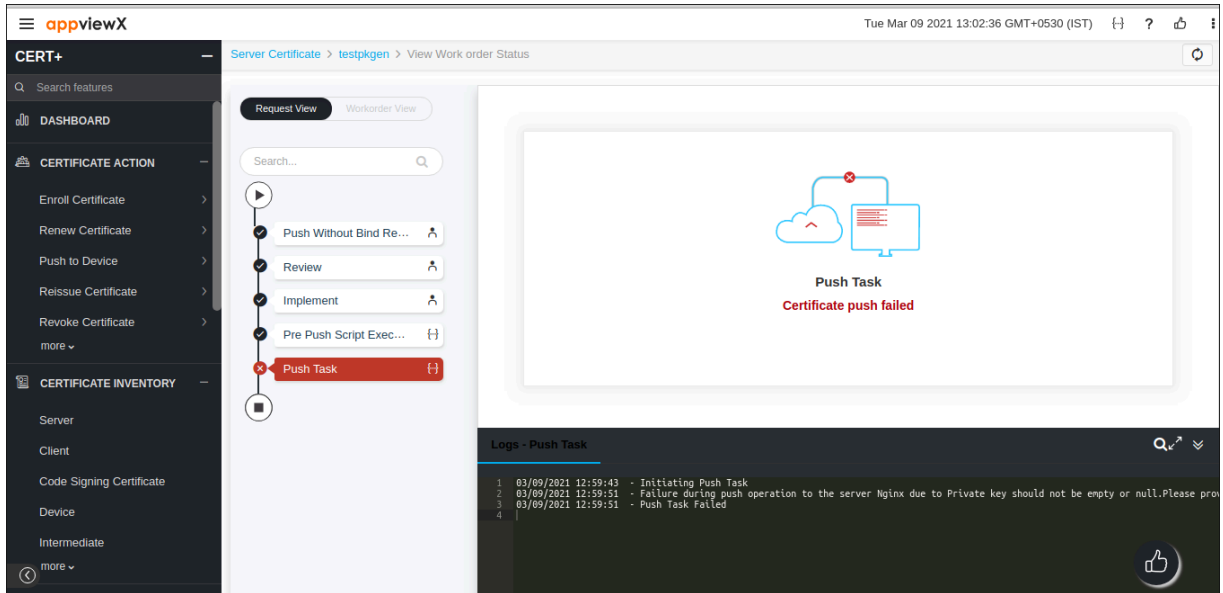
Error Messages

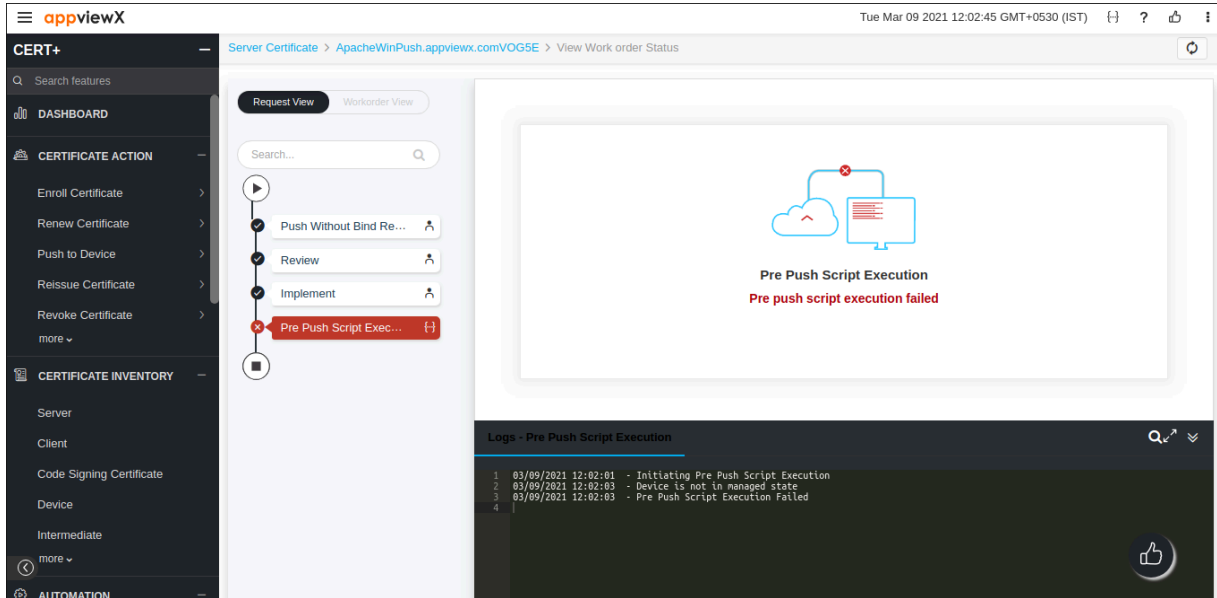
Error Message	Possible Cause	Possible Solution
CSR generation got failed/User has no permission for the given location to perform the operation.	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	1. Kindly ensure the user configured for device addition has read/write access to the path configured. 2. For sudo user, Please check the access elevation configured in device addition

Issues in Certificate Push

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**.
The **Server Certificate** page is displayed.
4. Click any **Nginx server**.
A holistic view of the **Certificate** will be displayed.

5. From the dropdown of **Connector Actions**, select **Add App Connector**.
6. Push the certificate to the device.





- Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Failure during push operation to the server Nginx due to Private key should not be empty or null.Please provide valid key to proceed push.	Private key not available in push request certificate	Please ensure the private key is available in request
Pivatekey In device configured. But key content is available with the certificate from AppViewX.. So failing push request.	Trying to push a certificate with key when the “Private key in device” enabled	Ensure the push certificate has no key when “Private key in device” is enabled.
Privatekey not exists in device.	Private key file not available in the given key location when “Private key in device” is enabled	Ensure the target device has key file in the given location
Push failed since cannot write-into/create location(s)	User does not have permission to perform the operation	1.Ensure the user has permission.

Error Message	Possible Cause	Possible Solution
		2.For sudo user, please check the access elevation value given in device addition
Device is not in managed state	Device is not available in managed	Please check the device status in device inventory

Troubleshooting NginxPlus ADC

- [Overview](#)
- [Issues in NginxPlus](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with NginxPlus ADC.

Issues in NginxPlus

- [Issue in Discovery](#)
- [Issues in CSR generation at Endpoint](#)
- [Issues in Certificate Push](#)

Issue in Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

Q Search...			
Title	Status	Message	Time
Certificate Discovery	Failed	Received failed response for the batch	02/25/2021 18:12:05
OK			

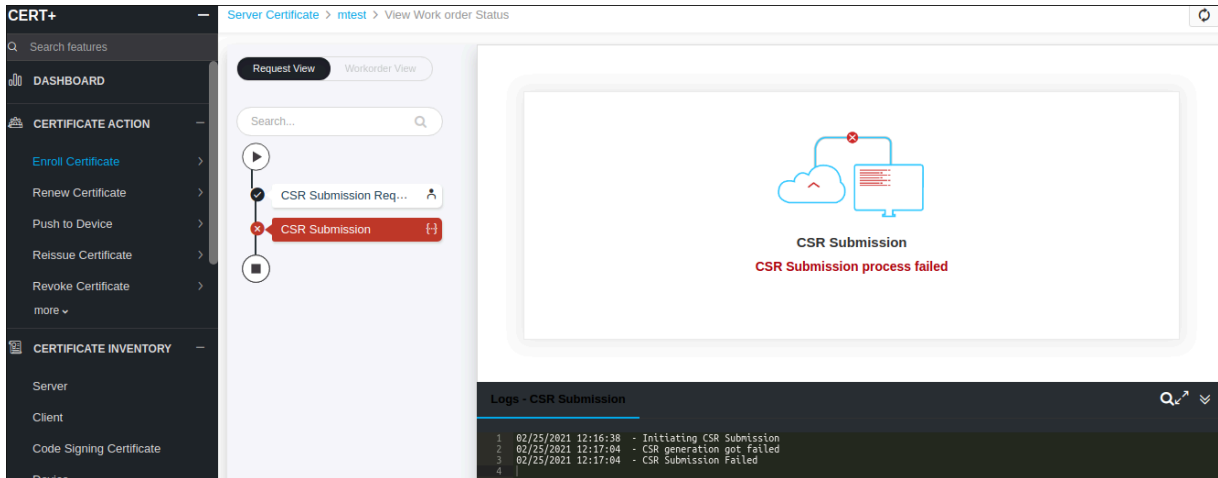
- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Received failed response from batch	1. Device not running or not accessible 2. No valid certificates available	1. Ensure target device is up and running 2. Check the device has valid certificate files

Issues in CSR generation at Endpoint

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab.
The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, click correct **Category**.
7. From the **Vendor** dropdown, click **NginxPlus**.
A list of devices will be generated in the **Devices dropdown**.



- **Error Messages**

Error Messages

Error Message	Possible Cause	Possible Solution
CSR generation got failed/User has no permission for the given location to perform the operation.	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issues in Certificate Push

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**.
The **Server Certificate** page is displayed.
4. Click any **NginxPlus** device.
A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, select **Add App Connector**.
6. Push the certificate to the device.

The screenshot shows the AppViewX interface with the following details:

- Header:** Tue Mar 09 2021 13:02:36 GMT+0530 (IST)
- Navigation:** CERT+ > Server Certificate > testpkgen > View Work order Status
- Left Panel:**
 - CERTIFICATE ACTION:** Enroll Certificate, Renew Certificate, Push to Device, Reissue Certificate, Revoke Certificate, more
 - CERTIFICATE INVENTORY:** Server, Client, Code Signing Certificate, Device, Intermediate, more
- Workflow:**
 - Request View (selected)
 - Search...
 - Push Without Bind Re...
 - Review
 - Implement
 - Pre Push Script Exec...
 - Push Task** (highlighted in red)
- Main Content:**
 - Diagram showing a cloud and a server with a red 'X' indicating failure.
 - Push Task**
 - Certificate push failed**
- Logs - Push Task:**

```

1 03/09/2021 12:59:43 - Initiating Push Task
2 03/09/2021 12:59:51 - Failure during push operation to the server Nginx due to Private key should not be empty or null.Please provide the correct private key
3 03/09/2021 12:59:51 - Push Task Failed
4

```

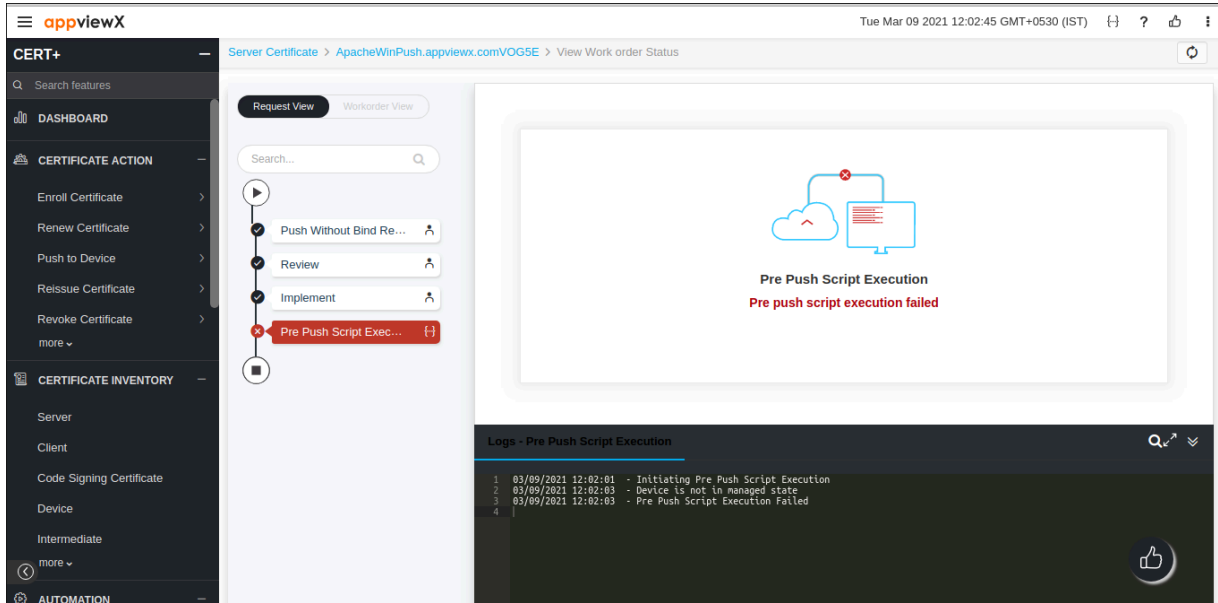
The screenshot shows the AppViewX interface with the following details:

- Header:** Tue Mar 09 2021 12:05:49 GMT+0530 (IST)
- Navigation:** CERT+ > Server Certificate > ApacheWinPush.appviewx.com\VOG5E > View Work order Status
- Left Panel:**
 - CERTIFICATE ACTION:** Enroll Certificate, Renew Certificate, Push to Device, Reissue Certificate, Revoke Certificate, more
 - CERTIFICATE INVENTORY:** Server, Client, Code Signing Certificate, Device, Intermediate, more
 - AUTOMATION:** (visible at the bottom)
- Workflow:**
 - Request View (selected)
 - Search...
 - Push Without Bind Re...
 - Review
 - Implement
 - Pre Push Script Exec...
 - Push Task** (highlighted in red)
- Main Content:**
 - Diagram showing a cloud and a server with a red 'X' indicating failure.
 - Push Task**
 - Certificate push failed**
- Logs - Push Task:**

```

1 03/09/2021 12:04:26 - Initiating Push Task
2 03/09/2021 12:04:44 - Push Failed since cannot write-into/create location(s) [root/, root/]
3 03/09/2021 12:04:44 - Push Task Failed
4

```



• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Private key should not be empty or null.	Private key not available in push request certificate	Please ensure the private key is available in request
Private key In device configured. But key content is available with the certificate from AppViewX. So failing push request.	Trying to push a certificate with key when the "Private key in device" enabled	Ensure the push certificate has no key when "Private key in device" is enabled.
Privatekey not exists in device.	Private key file not available in the given key location when "Private key in device" is enabled	Ensure the target device has key file in the given location
Push failed since cannot write-into/create location(s)	User does not have permission to perform the operation	Ensure the user has permission.
Device is not in managed state	Device is not available in managed	Please check the device status in device inventory

Troubleshooting Paloalto Firewall

- [Overview](#)
- [Supported Web Browsers](#)
- [Issues in Paloalto Firewall](#)

Overview

This section helps you troubleshoot the common problems that you might encounter while using Paloalto firewall functionalities. This guide will give more troubleshooting processes on Paloalto firewall certificate config fetch, discovery, CSR creation, backup, push, bind, rollback, and other actions associated with Paloalto firewall.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Paloalto Firewall

- [Issues in Fetch Config](#)
- [Issues in CSR Generation](#)

- [Issue in Discovery](#)
- [Issue in Backup, Push, Bind and Rollback](#)

Issues in Fetch Config

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Firewall** Tab.
5. Select the device, click **Fetch Config**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Exception occurred while getting Api key - Invalid credentials.	Credentials may be invalid.	Provide valid credentials.

Issues in CSR Generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab.
The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the **Category** dropdown, click **Firewall**.
7. Click Paloalto as Vendor from the dropdown.
A list of devices will be generated in the **Devices dropdown**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Exception occurred while getting Api key - Invalid credentials.	Credentials may be invalid.	Provide valid credentials.
Unsupported Key type provided	Unsupported key type is selected.	Please select RSA or EC.
Csr generation is device failed	CSR generation has failed.	CSR generation has failed. Please refer to the associated error message.
Invalid parameter for number of bits Csr generation is device failed	Selected EC bit length may not be supported by Paloalto.	Please select valid bit length supported.

Issue in Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	Discovery name not given or length less than 2 characters.	Enter a valid name with a minimum of 2 characters.
	Interval between batches info. is missing when execution type is sequential.	Provide a time interval between batches in minutes.

Error Message	Possible Cause	Possible Solution
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.
Exception occurred while getting Api key - Invalid credentials.	Credentials may be invalid.	Provide valid credentials.

Issue in Backup, Push, Bind and Rollback

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**, select **Server**.
4. At the top right corner of the page, click **List**.
The **Server Certificate** page is displayed.
5. Click the certificate to be pushed or rolled back.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
	Previous work order is in progress and not completed.	Initiate push after previous work order is finished.
	AppConnector might not be in sync.	Synchronize the appConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.

Error Message	Possible Cause	Possible Solution
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Exception occurred while getting Api key - Invalid credentials.	Credentials may be invalid.	Provide valid credentials.
Certificate <cert name> is not a valid reference	Private key not available in the certificate or the certificate is not in the required partition to bind.	Certificate should be pushed with the private key to bind with the profile.
Creating local certificate file failed	Unable to create the folder in EXPORT_DIRECTORY.	Please check whether the user has permission to create a folder or file in EXPORT_DIRECTORY in AppViewX.
Certificate name already exists in inventory, Cannot overwrite until Overwrite is enabled in Profile connector	Certificate with the same name already exists on the device.	Please change the certificate name or enable overwrite in the application connector.
Certificate is expired	Certificate is expired.	Push the certificate which is currently valid.
Unknown certificate algorithm	Unknown certificate algorithm.	Push the certificates only with RSA or EC.
certificate is not yet valid	Certificate valid from value is greater than current time.	Only valid certificates can be pushed.

Troubleshooting Panorama Firewall

- [Overview](#)
- [Supported Web Browsers](#)
- [Issues in Panorama Firewall](#)

Overview

This document helps you troubleshoot the common problems that you might encounter when using the Panorama firewall functionalities. This guide will give more troubleshooting processes on Panorama firewall certificate config fetch, discovery, CSR creation, backup, push, bind, rollback, and other actions associated with Panorama firewall.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Panorama Firewall

- [Issues in Fetch Config](#)
- [Issues in Panorama Firewall Discovery](#)

- [Issues in Panorama Firewall CSR Generation](#)
- [Issues in Panorama Firewall Backup, Push, Bind, and Rollback](#)

Issues in Fetch Config

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Firewall** Tab.
5. Select the device, click **Fetch Config**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Exception occurred while getting Api key - Invalid credentials.	Credentials may be invalid	Provide valid credentials

Issues in Panorama Firewall Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	Discovery name is not given or the length is less than 2 characters.	Enter a valid name with a minimum of 2 characters.
	Interval between batches info. is missing when execution type is sequential.	Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.
Exception occurred while getting Api key - Invalid credentials.	Credentials may be invalid	Provide valid credentials

Issues in Panorama Firewall CSR Generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab.
The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the **Category** dropdown, click **Firewall**.
7. From the **Vendor dropdown**, click **Panorama**.
A list of devices will be generated in the **Devices dropdown**.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Exception occurred while getting Api key - Invalid credentials.	Credentials may be invalid	Provide valid credentials

Error Message	Possible Cause	Possible Solution
Unsupported Key type provided	Unsupported key type is selected	Please select RSA or EC
Csr generation is device failed	CSR generation is failed	CSR generation has failed. Please refer to the error message associated with this
1) Invalid parameter for number of bits 2) Csr generation is device failed	Selected EC bit length may not be supported by panorama	Please select valid bit length supported

Issues in Panorama Firewall Backup, Push, Bind, and Rollback

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**, select **Server**.
4. At the top right corner of the page, click **List**.
The **Server Certificate** page is displayed.
5. Click the certificate to be pushed or rolled back.

• [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
	Previous work order is in progress and not completed.	Initiate push after previous work order is finished.
	AppConnector might not be in sync.	Synchronize the appConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state.	Enable the push/rollback workflow from the Workflow section.

Error Message	Possible Cause	Possible Solution
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Exception occurred while getting Api key - Invalid credentials.	Credentials may be invalid.	Provide valid credentials
Certificate <cert name> is not a valid reference	Private key not available in the certificate or the certificate is not in the required partition to bind.	Certificate should be pushed with private key to bind with the profile
Creating local certificate file failed	Unable to create the folder in EXPORT_DIRECTORY.	Please check whether the user has permission to create a folder or file in EXPORT_DIRECTORY in AppViewX.
Certificate name already exists in inventory, Cannot overwrite until Overwrite is enabled in Profile connector	Certificate with the same name already exists on the device.	Please change the certificate name or enable overwrite in the application connector.
Certificate is expired	Certificate is expired.	Push the certificate which is currently valid.
Unknown certificate algorithm	Unknown certificate algorithm.	Push the certificates only with RSA or EC.

Error Message	Possible Cause	Possible Solution
certificate is not yet valid	Certificate valid from value is greater than current time.	Currently, valid certificates only can be pushed.

Troubleshooting RabbitMQ Server

- [Overview](#)
- [Issues in RabbitMQ Server](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. Effective troubleshooting documents depend on the availability of useful, detailed information. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with RabbitMQ server.

Issues in RabbitMQ Server

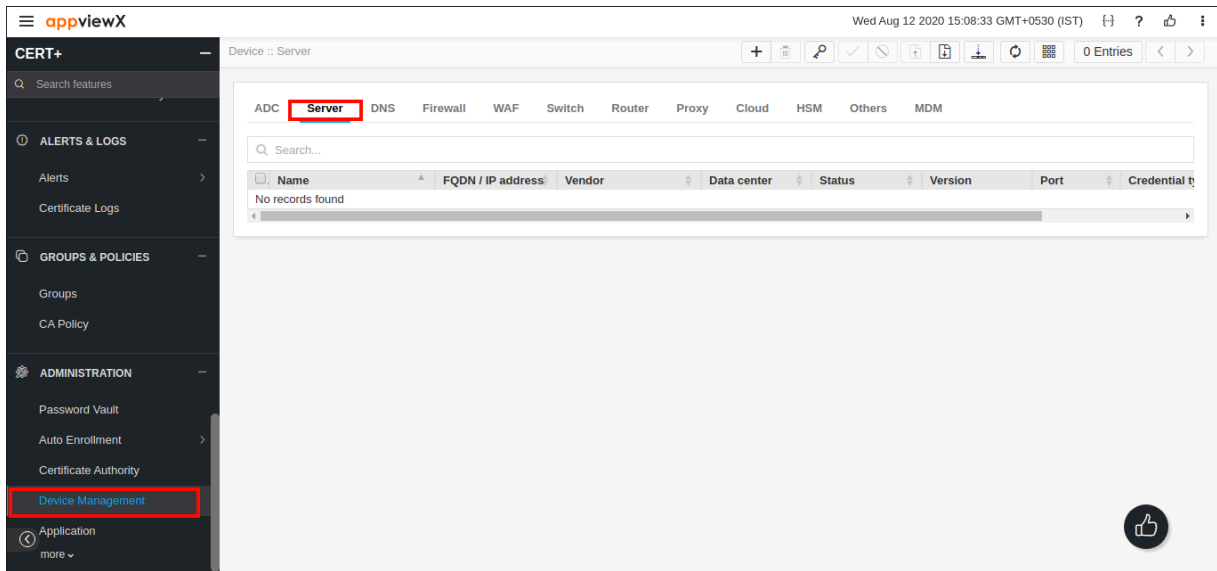
- [Issues in RabbitMQ Server Addition using AppViewX UI](#)
- [Issues in Communicating to RabbitMQ Server](#)
- [Issues in Accessing Server](#)
- [Issues in Config Fetch](#)
- [Issues in Certificate Discovery](#)
- [Issues in CSR generation](#)
- [Issues in Push and Rollback](#)

Issues in RabbitMQ Server Addition using AppViewX UI

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. From the icon list at the top right corner, click **Add**.

The **Device Addition** page is displayed.

6. From the **Device Details Section** on the left, click **RabbitMQ**.
7. Fill in the appropriate details.
8. Click **Add**.



Device :: Server > Add

Credentials

* Credential type:

* Username:

* Password:

Vendor Specific Details

Config path:

• Error Messages

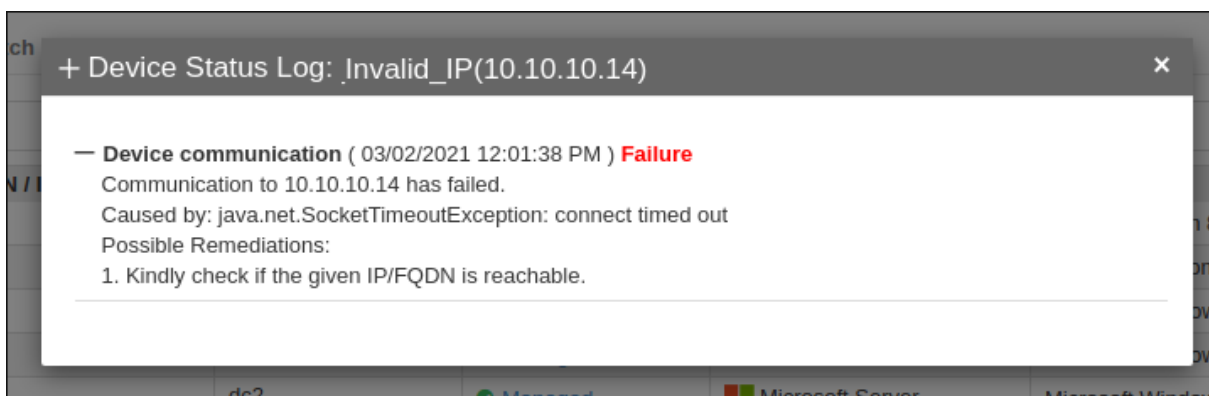
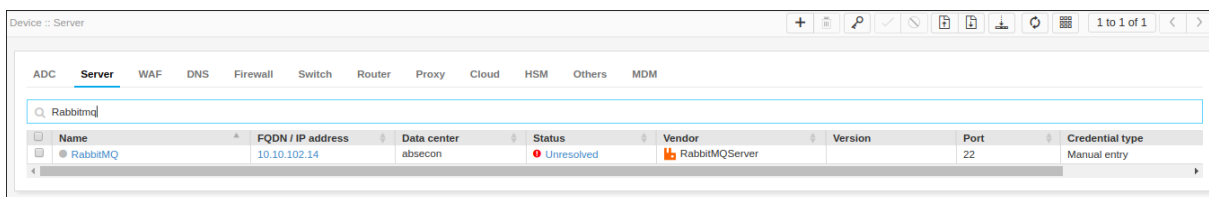
Error Messages

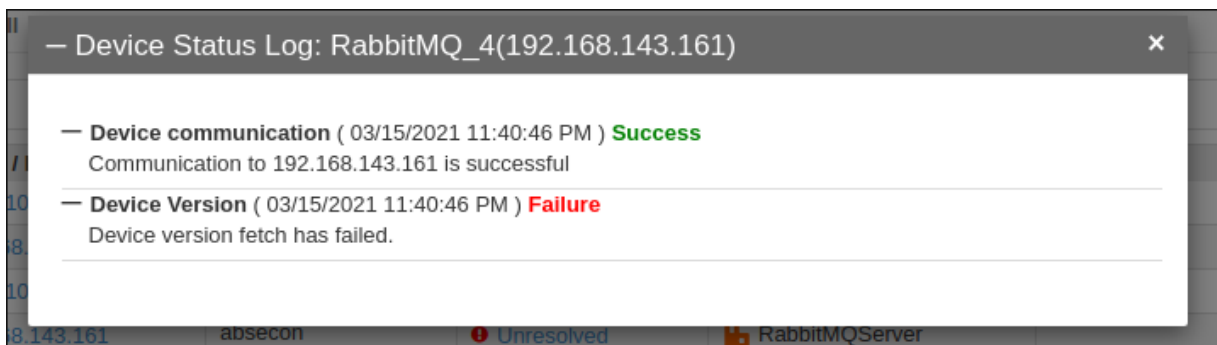
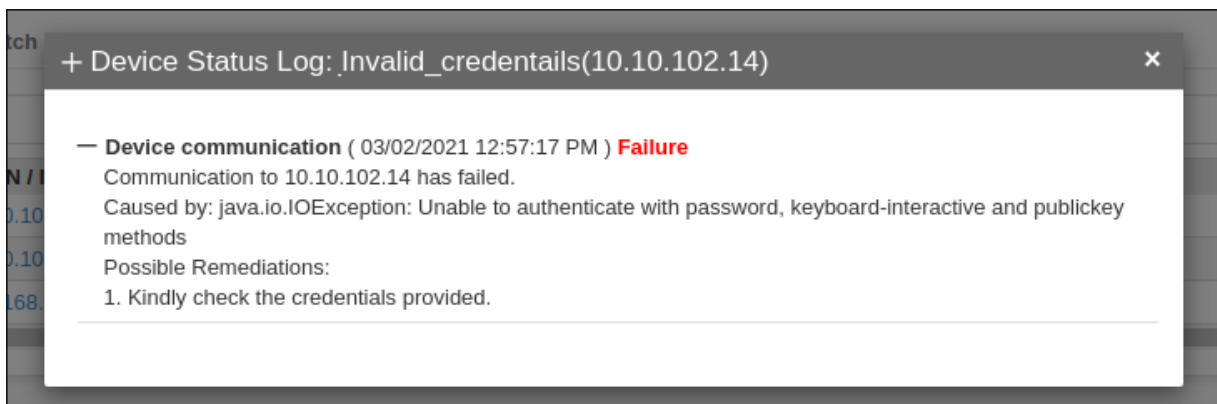
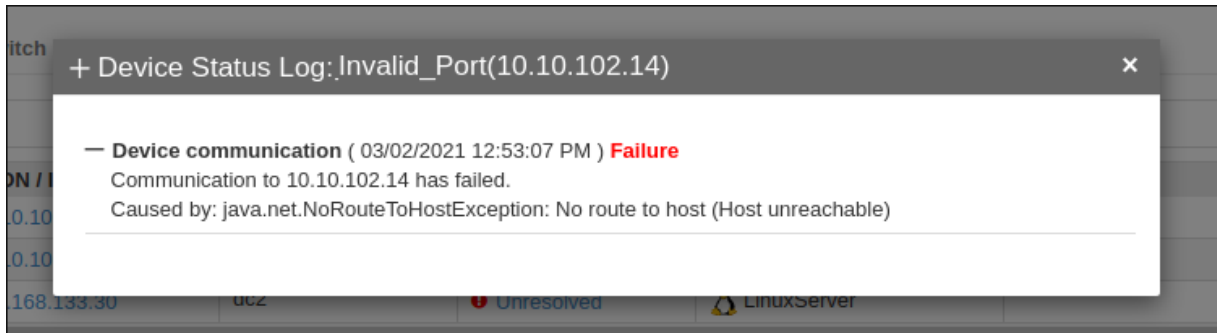
Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Communicating to RabbitMQ Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**.

The **Device Communication Status** is displayed.





- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-', '_', ':', '*', ' ', '!' and spaces.
Device IP/FQDN cannot be null or empty.	Device IP/FQDN is empty.	Provide device IP/FQDN as it is a mandatory field.
Invalid device IP/FQDN address.	IP/FQDN address is not valid.	Provide valid IP/FQDN address.
Communication to <ip/fqdn> has failed. Caused by: java.io.IOException: Unable to authenticate with password, keyboard-interactive and publickey methods Possible Remediations: 1. Kindly check the credentials provided.	Password of the device added might be wrong.	Click on the device name on the Inventory Page. Update the correct password and click Save.
Communication to <ip/fqdn> has failed. Caused by: java.net.SocketException: Network is unreachable (connect failed)	IP/FQDN provided is not reachable	Check manually by establishing an SSH session to the target device with the provided IP/FQDN.
Communication to <IP/FQDN> has failed. Caused by: java.net.ConnectException: Connection refused (Connection refused)	Problem with port configuration	Check if the configured port in the device addition page is correct.

Error Message	Possible Cause	Possible Solution
Possible Remediations: 1. Kindly check the SSH Port configurations. 2. Kindly check the firewall settings		
Communication to <IP/FQDN> has failed. Caused by: java.io.IOException: Key exchange was not finished, connection is closed.	Problem with SSH key handshake	Request to check the ciphers, key and HMacS configured in the target device and ensure AppViewX SSH-plugin supports the same
Device version fetch has failed.	Config path is incorrect / No RabbitMQ instances running in the target device	Check manually by establishing an SSH session to the target device and check RabbitMQ installations and find a valid configuration path and update the same in the device addition page.

Issues in Accessing Server

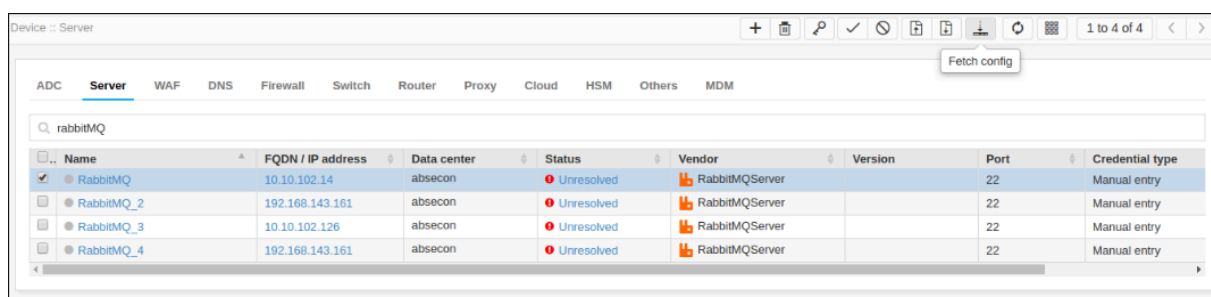
Access Issues might be reproduced when communicating with servers while discovering or fetching configuration files (/etc/rabbitmq/rabbitmq.config). These errors can be collected either from logs, API responses, or in the status field for the particular server.

Error Message	Possible Cause	Possible Solution
Custom Config Location	For default installation, The config location path is / etc/rabbitmq/rabbitmq. config, if any custom location is provided check the valid rabbitmq config file exists in that location	Login via SSH to the target device and check the “rabbitmq” installations and valid configuration file location path
Permission denied for file/ location.	1. File might not be present in the avx environment. 2. user might not have permission to read in the given source location	1.Check whether someone deleted the file from AppViewX environment.

Error Message	Possible Cause	Possible Solution
	3. Device communication might not be established when service has started.	2. Verify if read permission is given for the location. 3. Verify the device connection and restart the service.

Issues in Config Fetch

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Fetch Config**.



• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Communication to <IP/ FQDN> has failed.	Device communication has failed due to invalid credentials / SSH Port	1. Verify the input details and check device status error messages Issues in Communicating to RabbitMQ Server

Issues in Certificate Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

The screenshot shows the 'Discovery : Managed Devices Scan : Add Discovery' interface. On the left, the 'CERT+' menu is expanded to 'Discovery'. The main form includes fields for 'Discovery Run Type' (On-demand selected), 'Discovery Instance Name' (RabbitMQServer), and a 'Description' text area. Below, the 'Discover By' section has a 'Discovery From' dropdown set to 'Managed Servers'. At the bottom, a table lists discovered items with columns for selection, status, and count (3). A 'Discover' button is at the bottom right.

• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or the length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.

Error Message	Possible Cause	Possible Solution
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.

Issues in CSR generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab.
The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, click correct **Category**.
7. From the Vendor dropdown, click **RabbitMQServer**.

A list of devices will be generated in the **Devices** dropdown.

CERT+

Search features

DASHBOARD

CERTIFICATE ACTION

- Enroll Certificate
- Renew Certificate
- Push to Device
- Reissue Certificate
- Revoke Certificate
- more

CERTIFICATE INVENTORY

- Server
- Client
- Code Signing Certificate
- Device
- Intermediate
- more

AUTOMATION

- My Workflows

Enroll Server Certificate

CSR Generation: ☐ AppViewX ☐ Upload CSR ☐ HSM ☒ End Point

Category: Server

Vendor: RabbitMQServer

Devices: None

CSR file name: .csr

Key File Name: .key

CSR Parameters

Common Name:

Subject Alternative Name: DNS

DNS: 0 value

Organization:

Organization Unit:

Locality:

Add Reset

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Problem while generating csr on target server	General Failure - SSH/SFTP communication failure	Provide correct credentials and make sure device communication is successful.
Invalid key type specified in the request	Given key type might not be supported by open SSL in the target machine.	Provide valid key type.
Problem while generating csr on the target server.	Location might not have permission.	Check the permission and provide it.
CSR and Private key has been failed	Open SSL configuration might be wrong in the target machine.	Check and correct open SSL configuration in the device.
CSR generation got failed	User has restricted access to the path configured for the "CSR FileName" and "Key File name"	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issues in Push and Rollback

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**.
The **Server Certificate** page is displayed.
4. Click any **RabbitMQ server**.
A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, select **Add App Connector**.
6. Push the certificate to the device.

The screenshot shows the CERT+ interface for a 'Server Certificate' on 'cert.test.com'. The left sidebar contains a 'CERTIFICATE INVENTORY' section with 'Server' selected. The main panel displays a workflow with steps: 'Push and Bind Requ...', 'Review', 'Implement', 'Pre Push Script Exec...', 'Backup Task', and 'Push Task'. The 'Push Task' step is highlighted in red, indicating a failure. The right panel shows a diagram of a cloud and a server with a red 'X' and the text 'Push Task Certificate push failed'. Below the diagram, the 'Logs - Push Task' section shows the following log entries:

Line	Timestamp	Message
1	02/25/2021 11:57:54	- Initiating Push Task
2	02/25/2021 11:58:57	- Certificate Push Failed
3	02/25/2021 11:58:58	- Push Task Failed
4		

The screenshot shows the CERT+ interface for a 'Server Certificate' on 'cert.test.com'. The left sidebar contains a 'CERTIFICATE INVENTORY' section with 'Server' selected. The main panel displays a workflow with steps: 'Push and Bind Requ...', 'Review', 'Implement', 'Pre Push Script Exec...', 'Backup Task', and 'Push Task'. The 'Push Task' step is highlighted in red, indicating a failure. The right panel shows a diagram of a cloud and a server with a red 'X' and the text 'Push Task Certificate push failed'. Below the diagram, the 'Logs - Push Task' section shows the following log entries:

Line	Timestamp	Message
1	02/25/2021 12:07:34	- Initiating Push Task
2	02/25/2021 12:07:37	- PrivateKey in device push invalid
3	02/25/2021 12:07:37	- Push Task Failed
4		

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.

Error Message	Possible Cause	Possible Solution
Certificate Push failed	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/write access to the path configured in application connector to certificate push.
PrivateKey in device push invalid	“Private key in Device” is enabled in application connector, but key is not available on device.	Ensure to enable “Private key in Device” attribute in application connector, if the certificate does not have the key and the certificate is generated using CSR gen option from Device.

Troubleshooting Rapid SB Server Inventory

- [Overview](#)
- [Supported Web Browsers](#)
- [Issues in Server Inventory](#)

Overview

This document will help you troubleshoot the issues faced during the use of the functionalities of Rapid SB connectors server inventory. It begins by troubleshooting the common functionalities and then goes on to handle the issues peculiar to various Rapid SB connectors Servers.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Issues in Server Inventory

- [Issues in Accessing Server](#)
- [Issues in Credential List](#)
- [Issues in Managed Server](#)
- [Issues in Unmanaged Server](#)
- [Issues in Import Server](#)
- [Issues in Export Server](#)
- [Issue in Discovery](#)

Issues in Accessing Server

Access Issues might be reproduced when communicating with servers while discovering or fetching configuration files. These errors can be collected either from logs, API responses, or in the status field for the particular server.

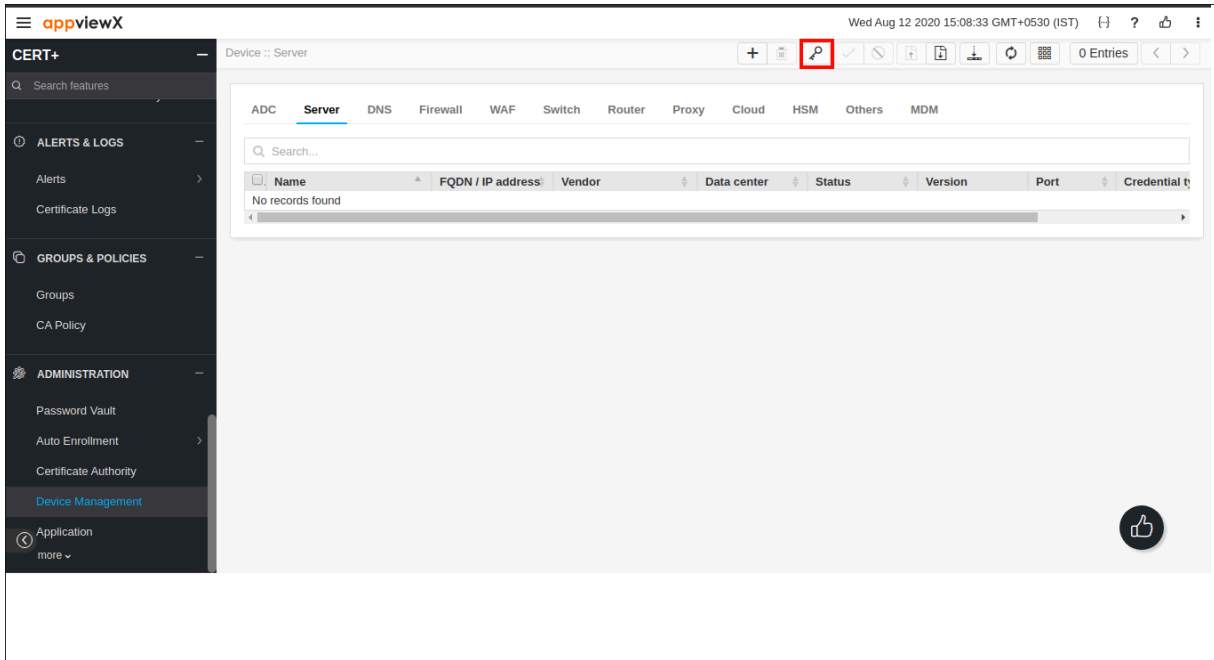
Error Message	Possible Cause	Possible Solution
Sudo Access failure	Linux Commands execution with sudo fails.	Verify if the system has the correct sudo setup.
dzdo Access failure	Linux Commands execution with dzdo fails.	Verify if the system has the correct dzdo setup.
Permission denied for file/location.	1. File might not be present in the avx environment. 2. user might not have permission to read in the given source location 3. Device communication might not be established when service has started.	1. Check whether someone deleted the file from AppViewX environment. 2. Verify if read permission is given for the location. 3. Verify the device connection and restart the service.

Issues in Credential List

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.

4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Credentials**.

The **Credential List** page is displayed.



- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid details	Mandatory credential details are missing.	Provide all the mandatory details to store the credential.
credentials already exist.	Credential List with the same name already exists.	Provide a unique name to each credential list.
Invalid file format. Accepted formats are .pem and .txt	The Identity Key file uploaded is not having the correct format.	Provide key file with correct format (.pem or .txt)

Invalid details

Device > Credential > Add credential

Invalid details

appviewX
CYBERARK

Credential details

* Credential name

* User name

Credential type ☒ Password ☐ Identity key

* Password

Secondary password

Save Cancel

Credentials already exist

Device > Credential > Add credential

credentials already exist.

appviewX
CYBERARK

Credential details

* Credential name

* User name

Credential type ☒ Password ☐ Identity key

* Password

Secondary password

Save Cancel

Invalid file format. Accepted formats are .pem and .txt

Device > Modify > Modify credential

Invalid file format. Accepted formats are .pem and .txt.

appviewX
CYBERARK

Credential details

* Credential name

* User name

Credential type ☐ Password ☒ Identity key

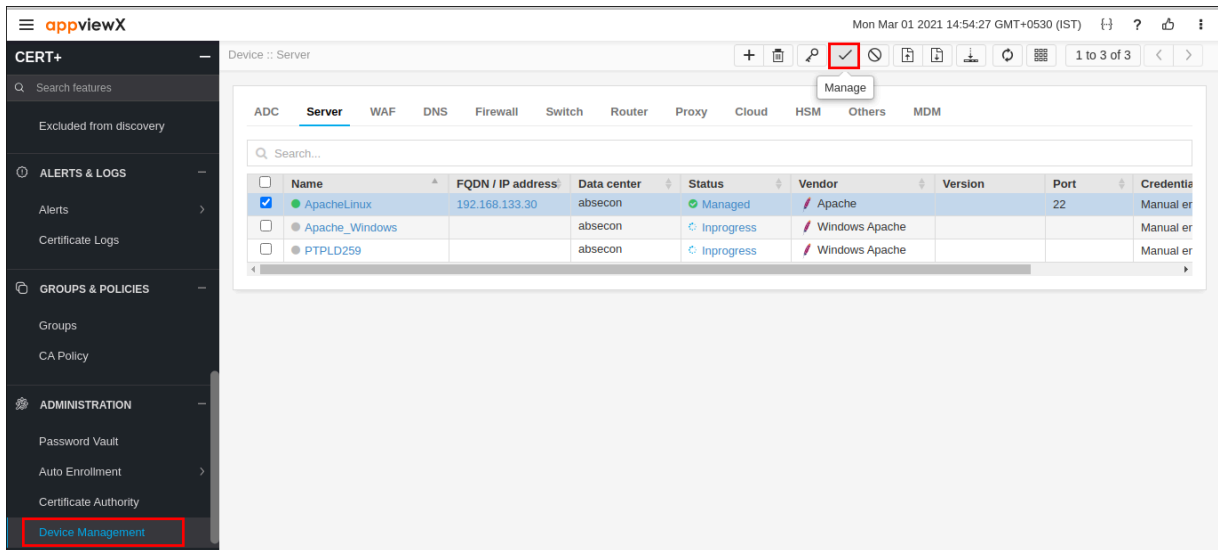
* Identity key
Browse

Passphrase

Update Cancel

Issues in Managed Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device and click **Manage**.



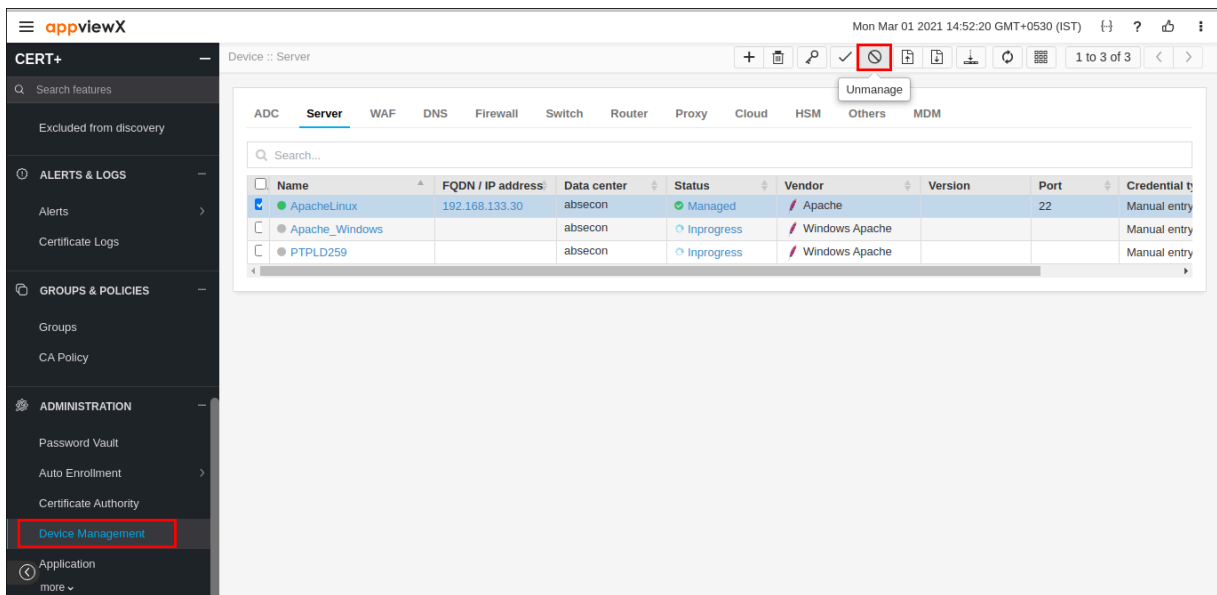
• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
The selected devices are managed. The operation cannot be performed.	Device cannot be managed because it is already in the managed state.	Unmanage the device(s) in the managed state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

Issues in Unmanaged Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device and click **Unmanage**.



• Error Messages

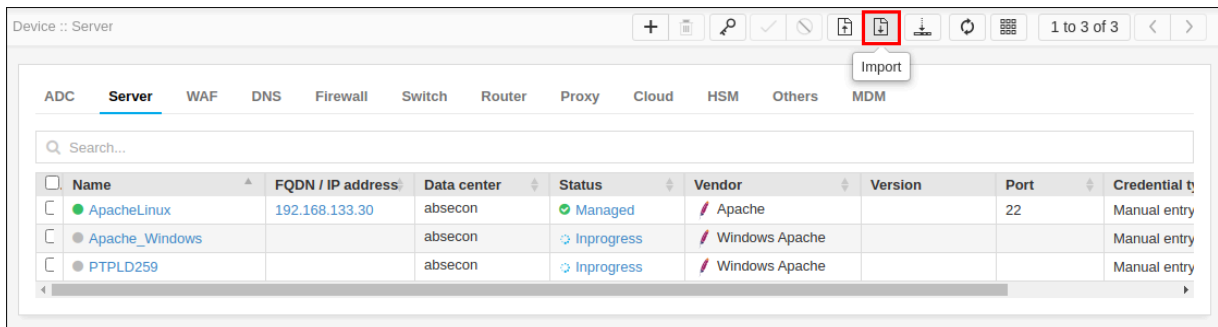
Error Messages

Error Message	Possible Cause	Possible Solution
The selected devices are already unmanaged. The operation cannot be performed.	Device cannot be unmanaged because it is already in the unmanaged state.	Manage the device(s) in an unmanaged state before performing action.

Error Message	Possible Cause	Possible Solution
Fetch config not allowed for Unmanaged devices	Fetch config operation is only allowed on the devices which are in managed state.	Manage the device(s) in an unmanaged/in-progress state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

Issues in Import Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device and click **Import**.



• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid file type. Please select a valid file format (csv / xlsx / xls).	File type uploaded is not in an expected format.	Supported file types are CSV/Xls/xlsx only. Check for the uploaded file extension.

Error Message	Possible Cause	Possible Solution
Maximum five files allowed, please delete any completed file.	In the file history of the import page maximum of 5 files can only be maintained.	Delete any of the parsed/completed files to upload a new one.

Maximum five files allowed, please delete any completed file.

The screenshot shows the 'Import' page with a sidebar on the left. A red banner at the top reads: 'Maximum five files allowed, please delete any completed file.' The 'File Histories' table contains the following data:

File name	Status	Available	Uploaded	Failed	Server count	Action
2020.3.0ServerimportSheet.xls	17%	Available: 0	Uploaded: 1	Failed: 5	6	[+][x]
2020.3.0ServerimportSheet.xls	0%	Available: 0	Uploaded: 0	Failed: 6	6	[+][x]
2020.3.0ServerimportSheet.xls	0%	Available: 0	Uploaded: 0	Failed: 6	6	[+][x]
2020.3.0ServerimportSheet.xls	0%	Available: 0	Uploaded: 0	Failed: 6	6	[+][x]
2020.3.0ServerimportSheet.xls	0%	Available: 0	Uploaded: 0	Failed: 6	6	[+][x]
2020.3.0ServerimportSheet.xls	0%	INITIATED			6	[+][x]

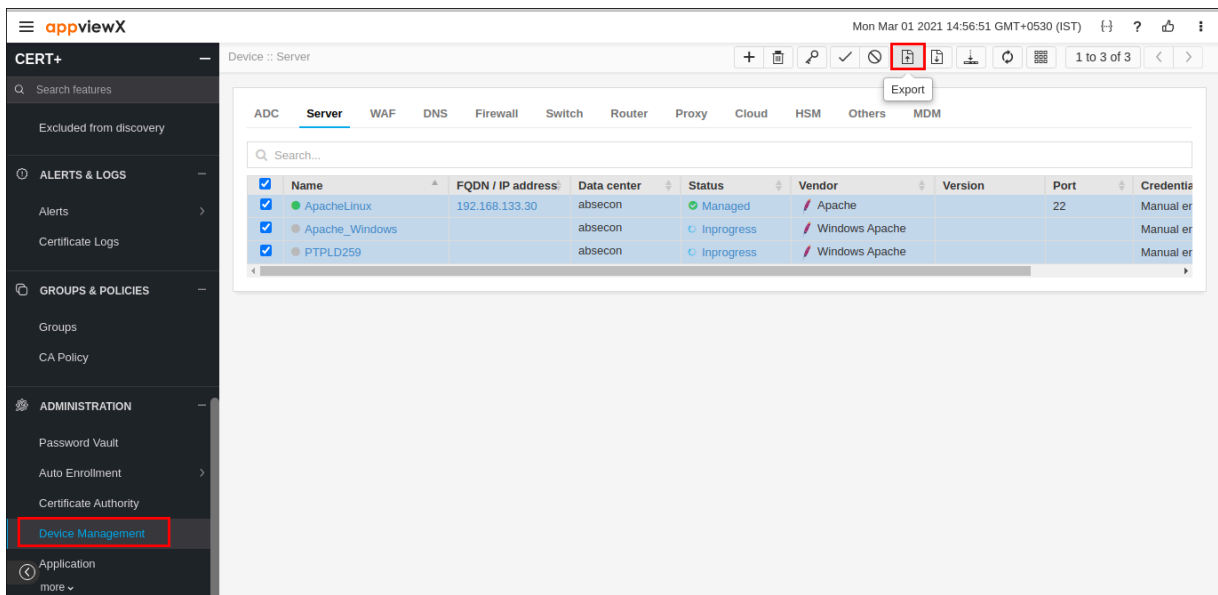
Invalid file type. Please select a valid file format (csv / xlsx / xls).

The screenshot shows the 'Import' page with a sidebar on the left. A red banner at the top reads: 'Invalid file type. Please select a valid file format (csv / xlsx / xls).' The 'File Histories' table contains the following data:

File name	Status	Available	Uploaded	Failed	Server count	Action
2020.3.0ServerimportSheet.xls	17%	Available: 0	Uploaded: 1	Failed: 5	6	[+][x]
2020.3.0ServerimportSheet.xls	0%	Available: 0	Uploaded: 0	Failed: 6	6	[+][x]

Issues in Export Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** Page is displayed.
4. On the **Device Management** Page, click **Server** Tab.
5. Select the device and click **Export**.



• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Exception while exporting	1.General failure - Unable to create file on the local system due to permission issue.	1. Provide access to be able to create the file on the local system. (For example, check the directory where it is trying to export and give access to AppViewX for that directory.) 2. Make sure the database is running and has correct data.

Error Message	Possible Cause	Possible Solution
	2.Unable to fetch device list from the database.	

Issue in Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

The screenshot shows the AppViewX interface for adding a new discovery. The left navigation pane has 'CERT+' expanded, and 'Discovery' is selected under 'CERTIFICATE DISCOVERY'. The main content area is titled 'Discovery : Managed Devices Scan : Add Discovery'. It contains fields for 'Discovery Run Type' (On-demand selected), 'Discovery Instance Name' (demoDiscovery), and a 'Description' text area. Below these is a 'Discover By' section with a dropdown menu set to 'Managed Servers'. A table below the dropdown shows search results for 'Apache::ApacheLinux' with one item selected. At the bottom are 'Discover' and 'Reset' buttons.

• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	- Discovery name is not given or length is less than 2 characters. - Interval between batches info. is missing when execution type is sequential.	- Enter a valid name with a minimum of 2 characters. - Provide a time interval between batches in minutes.
Please select a device	No device is selected in the "Discover By" section.	Select at least one device to discover certificates from.

Troubleshooting Rapid SB Linux Server

- [Overview](#)
- [Supported Web Browsers](#)
- [Issues in Linux Server](#)

Overview

This section helps you troubleshoot the common problems that you might encounter while using certificate server functionalities for Linux servers. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with Linux servers.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

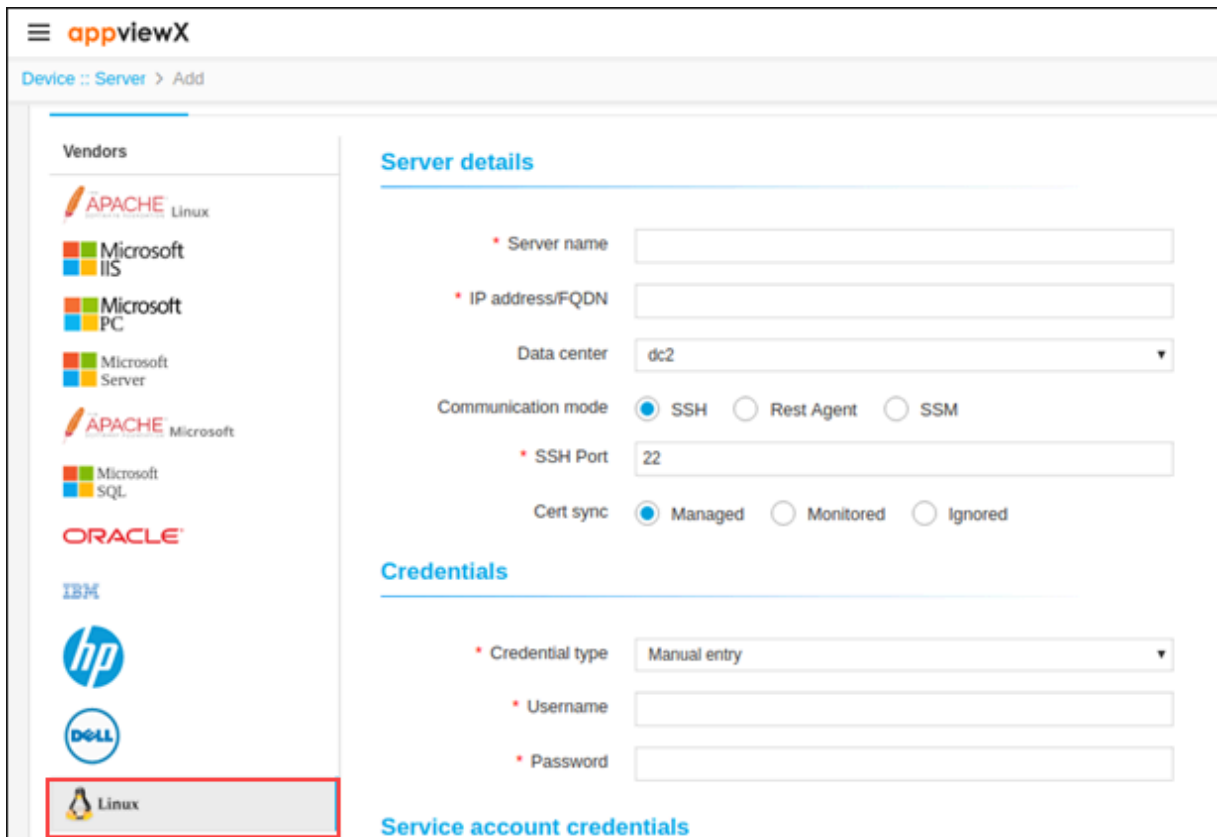
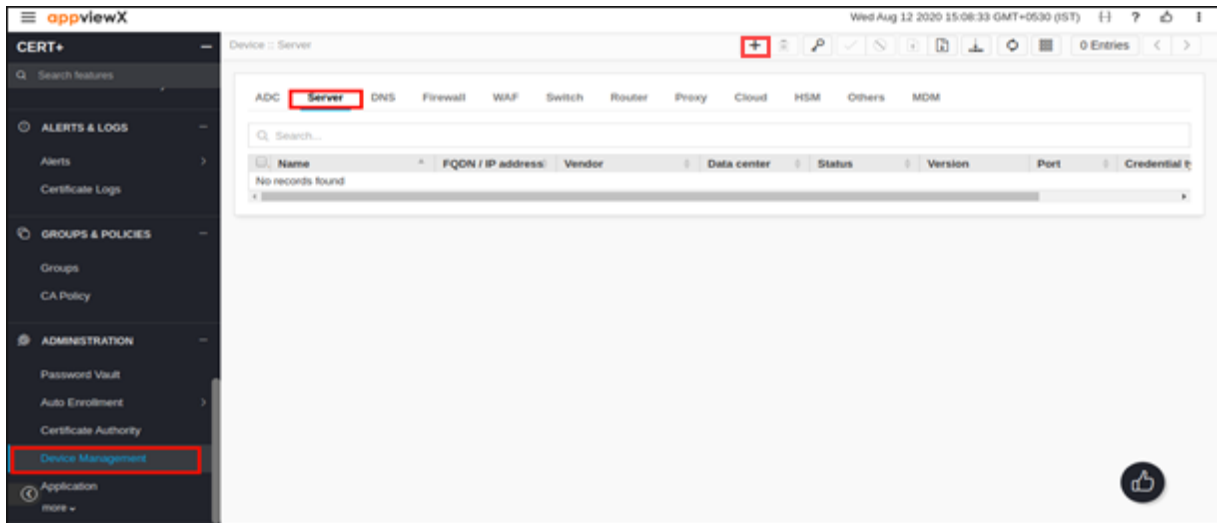
Issues in Linux Server

- [Issues in Linux Server Addition using AppViewX UI](#)
- [Issues in Communicating to Linux Server](#)
- [Issues in Accessing Server](#)
- [Issues in Credential List](#)
- [Issues in Managed Server](#)
- [Issues in Unmanaged Server](#)
- [Issues in Import Server](#)
- [Issues in Export Server](#)
- [Issues in Config Fetch](#)
- [Issues in Certificate Discovery](#)
- [Issues in CSR generation](#)
- [Issues in Push and Rollback](#)

Issues in Linux Server Addition using AppViewX UI

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. From the icon list at the top right corner, click **Add**.
The **Device Addition** page is displayed.
6. From the **Device Details Section** on the left, click **Linux**.
7. Fill in the appropriate details.

8. Click **Add**.



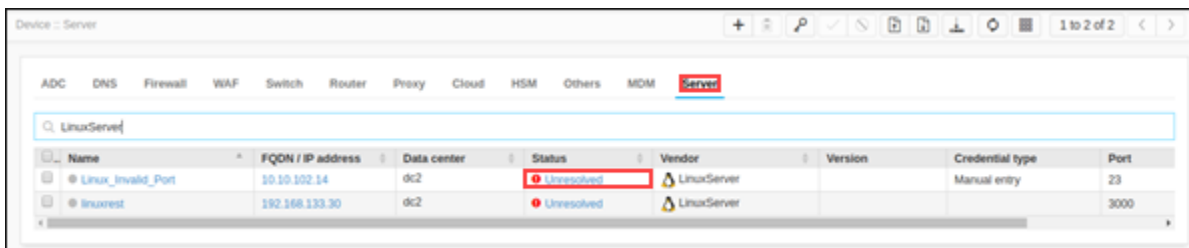
- [Error Messages](#)

Error Messages

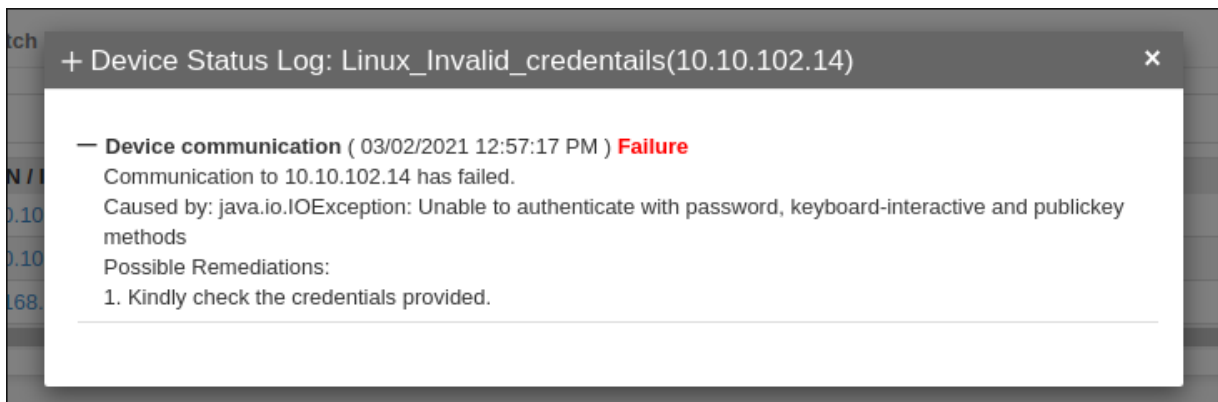
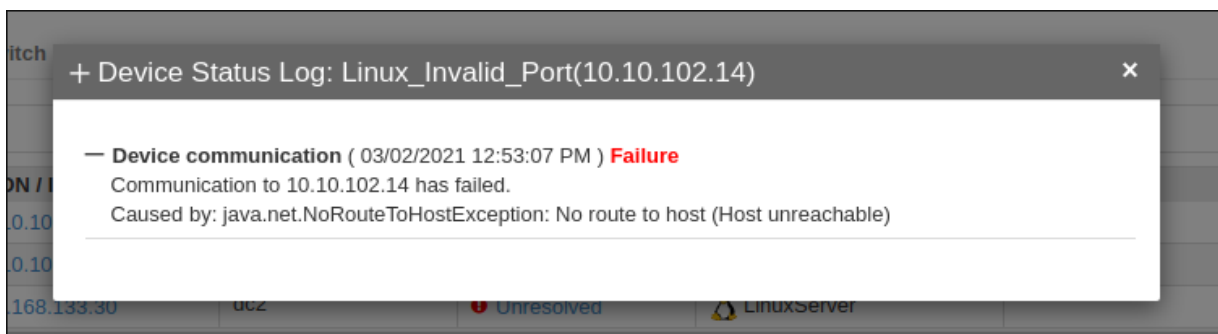
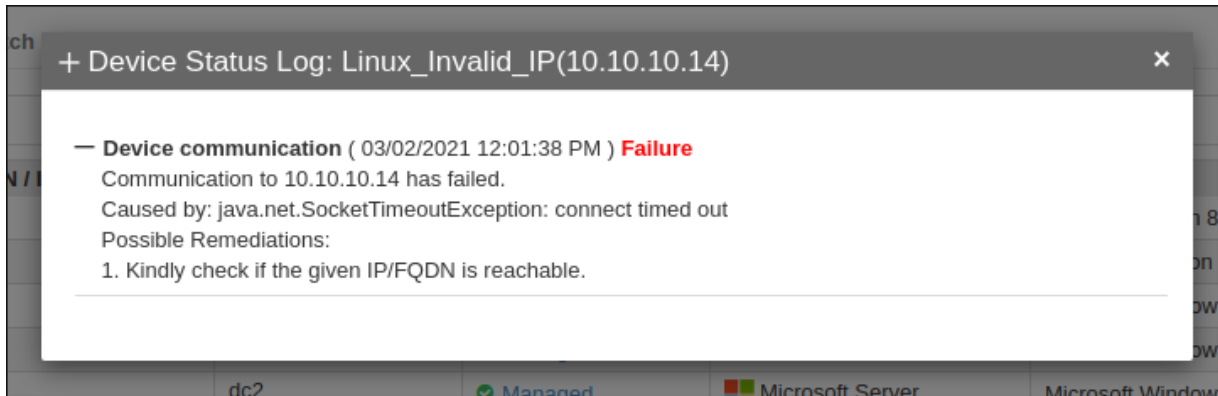
Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

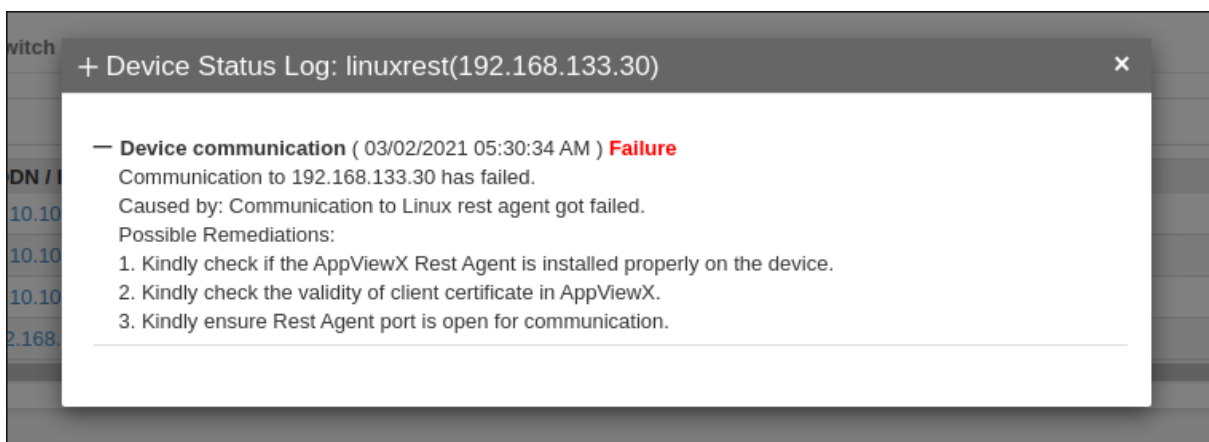
Issues in Communicating to Linux Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**.
The **Device Communication Status** is displayed.



Name	FQDN / IP address	Data center	Status	Vendor	Version	Credential type	Port
Linux_Invalid_Port	10.10.102.14	dc2	Unresolved	LinuxServer		Manual entry	23
linuxrest	192.168.133.30	dc2	Unresolved	LinuxServer			3000





• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can contain only alphanumeric characters, '-', '_', ':', '*', ' ', '!' and spaces.
Device IP/FQDN cannot be null or empty.	Device IP/FQDN is empty.	Provide device IP/FQDN as it is a mandatory field.
Invalid device IP/FQDN address.	IP/FQDN address is not valid.	Provide valid IP/FQDN address.
Communication to <ip/fqdn> has failed. Caused by: java.io.IOException: Unable to authenticate with password, keyboard-interactive and publickey methods Possible Remediations:	Password of the device added might be wrong.	Click on the device name on the Inventory Page. Update the correct password and click Save.

Error Message	Possible Cause	Possible Solution
1. Kindly check the credentials provided.		
Communication to <ip/fqdn> has failed. Caused by: java.net.SocketException: Network is unreachable (connect failed)	IP/FQDN provided is not reachable.	Check manually by establishing a SSH session to the target device with the provided IP/FQDN.
Communication to <IP/FQDN> has failed. Caused by: java.net.ConnectException: Connection refused (Connection refused) Possible Remediations: 1. Kindly check the SSH Port configurations. 2. Kindly check the firewall settings	Problem with port configuration.	Check if the configured port in the device addition page is correct.
Communication to <IP/FQDN> has failed. Caused by: java.io.IOException: Key exchange was not finished, connection is closed.	Problem with SSH key handshake.	Request to check the ciphers, key and HMacS configured in the target device and ensure AppViewX SSH-plugin supports the same.

Issues in Accessing Server

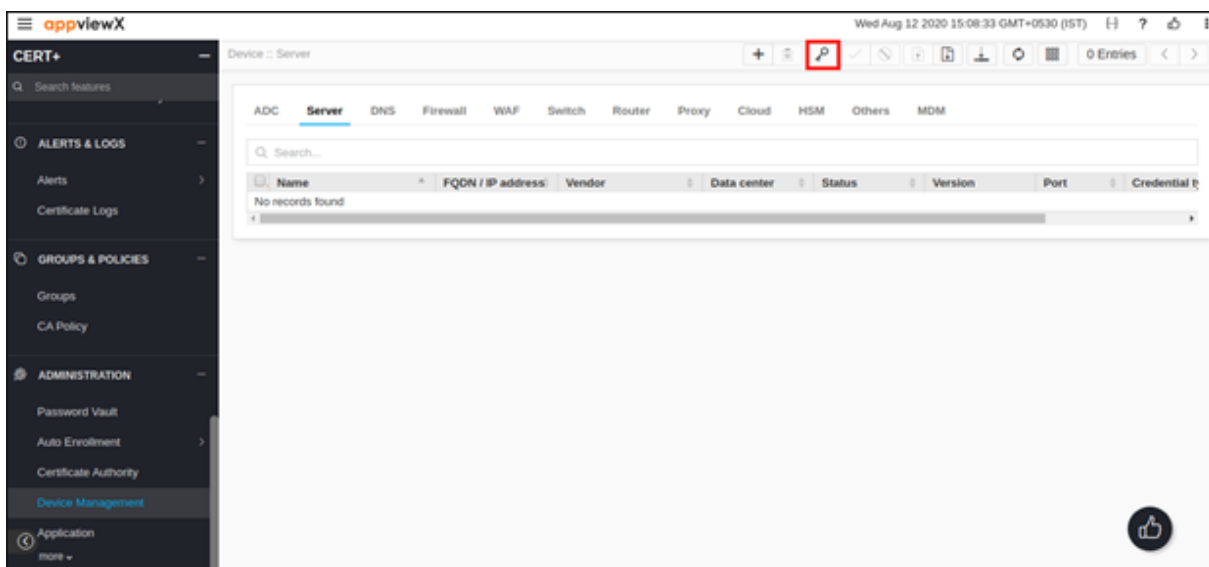
Issues with accessing servers can occur while communicating with servers or discovering or fetching configuration files. These errors can be collected either from logs, API responses or can be seen in the status field for that particular server.

Error Message	Possible Cause	Possible Solution
Sudo Access failure	Linux Commands execution with sudo fails.	Verify if the system has the correct sudo setup.
dzdo Access failure	Linux Commands execution with dzdo fails.	Verify if the system has the correct dzdo setup.

Error Message	Possible Cause	Possible Solution
Permission denied for file/ location.	1. File might not be present in the avx environment. 2. User might not have permission to read in the given source location. 3. Device communication might not be established when service has started.	1. Check whether someone deleted the file from AppViewX environment. 2. Verify if read permission is given for the location. 3. Verify the device connection and restart the service.

Issues in Credential List

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Credentials**.
The **Credential List** page is displayed.

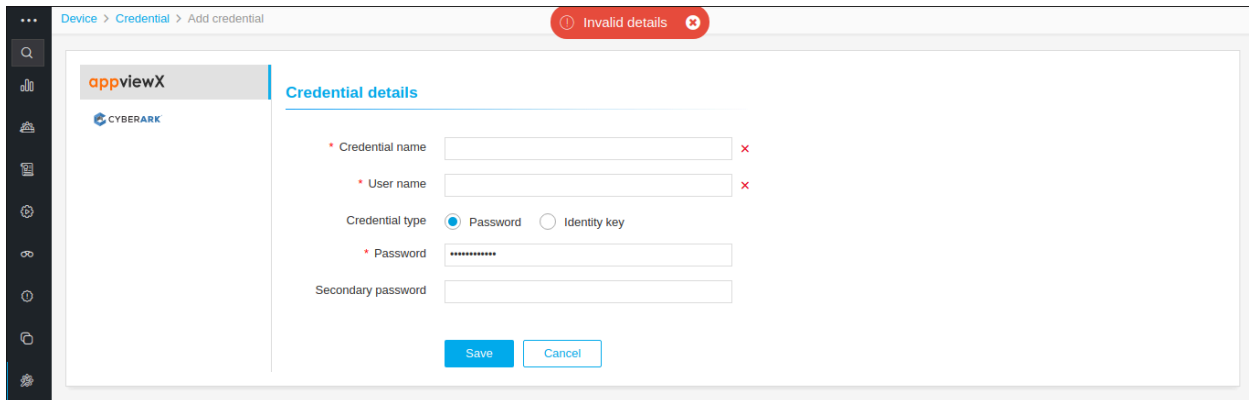


• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid details	Mandatory credential details are missing.	Provide all the mandatory details to store the credential.
credentials already exist.	Credential List with the same name already exists.	Provide a unique name to each credential list.
Invalid file format. Accepted formats are .pem and .txt	The Identity Key file uploaded does not have the correct format.	Provide key file with correct format (.pem or .txt)

Invalid details



Device > Credential > Add credential

Invalid details

appviewX

CYBERARK

Credential details

* Credential name

* User name

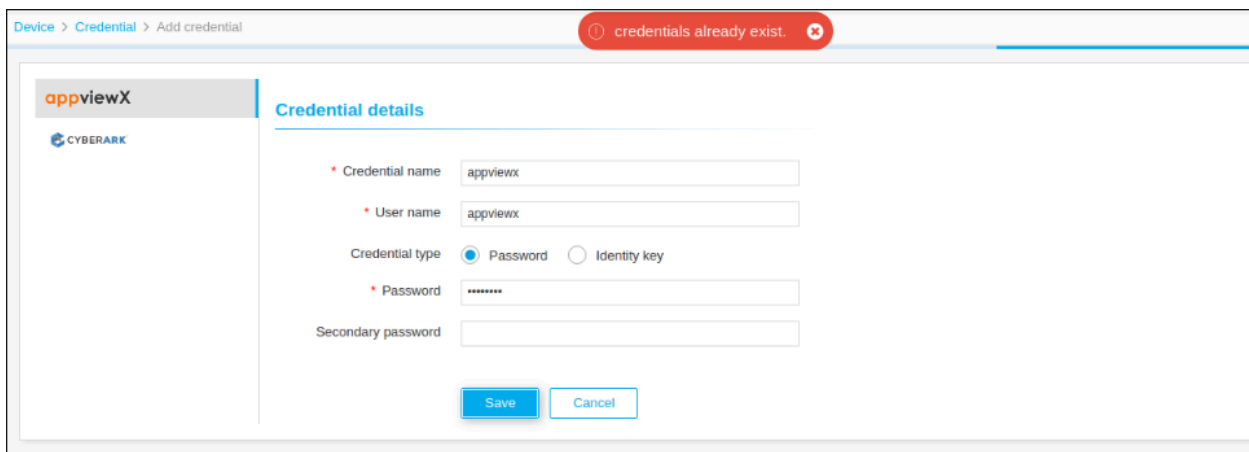
Credential type: ☒ Password ☐ Identity key

* Password

Secondary password

Save Cancel

Credentials already exist



Device > Credential > Add credential

credentials already exist.

appviewX

CYBERARK

Credential details

* Credential name: appviewx

* User name: appviewx

Credential type: ☒ Password ☐ Identity key

* Password: *****

Secondary password

Save Cancel

Invalid file format. Accepted formats are .pem and .txt

The screenshot shows the 'Add credential' form in the AppViewX interface. At the top, a red error banner displays the message: 'Invalid file format. Accepted formats are .pem and .txt'. The form fields include:

- Credential name:** appviewx
- User name:** appviewx
- Credential type:** Radio buttons for 'Password' and 'Identity key' (selected).
- Identity key:** A text field with a 'Browse' button next to it.
- Passphrase:** A text field.

At the bottom of the form are 'Save' and 'Cancel' buttons.

Issues in Managed Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device and click **Manage**.

The screenshot shows the 'Device Management' page in the AppViewX interface. The 'Server' tab is selected. A table lists several devices, and a 'Manage' button is visible above the table.

Name	FQDN / IP address	Data center	Status	Vendor	Version	Port	Credential type
Linux_Valid	10.10.102.14	absecon	Managed	LinuxServer		22	Manual entry
Linux	10.10.102.14	absecon	Unresolved	LinuxServer		22	Manual entry
Linux_DZDO	10.10.102.14	absecon	Unresolved	LinuxServer		22	Manual entry
Linux_SUDO	10.10.102.14	absecon	Unresolved	LinuxServer		22	Manual entry
Linux_Invalid	1.2.3.4	absecon	Unresolved	LinuxServer		22	Manual entry

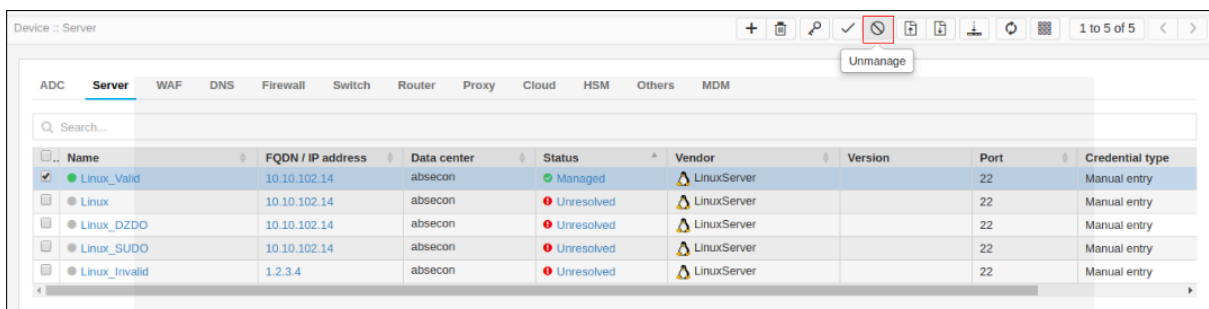
• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
The selected devices are managed. The operation cannot be performed.	Device cannot be managed because it is already in the managed state.	Unmanage the device(s) in the managed state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

Issues in Unmanaged Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device and click **Unmanage**.



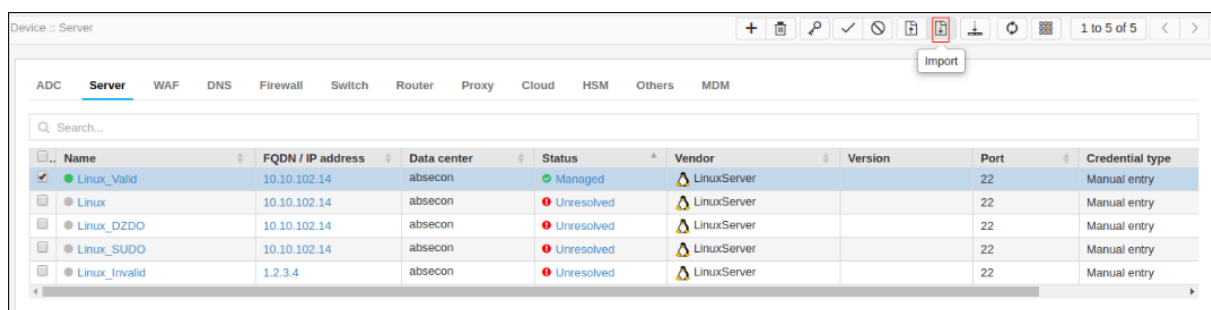
- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
The selected devices are already unmanaged. The operation cannot be performed.	Device cannot be unmanaged because it is already in the unmanaged state.	Manage the device(s) that is in unmanaged state before unmanaging it again.
Fetch config not allowed for Unmanaged devices	Fetch config operation is only allowed on the devices which are in managed state.	Manage the device(s) that is in an unmanaged/inprogress state before unmanaging it again.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an inprogress state.	Wait for the device to be resolved to a state before performing action.

Issues in Import Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device and click **Import**.



- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid file type. Please select a valid file format (csv / xlsx / xls).	File type uploaded is not in expected format.	Supported file types are csv/xls/xlsx only. Check for the uploaded file extension.
Maximum five files allowed, please delete any completed file.	In file history of import page maximum 5 files can only be maintained.	Delete any of the parsed/completed files to upload a new one.

Maximum five files allowed, please delete any completed file.

Device :: Server > Import

Maximum five files allowed, please delete any completed file.

Import

Click here to Browse and Upload (csv, xls, and.xlsx)

Uploader Info

Maximum 5 files (.xlsx or .csv) will be processed in parallel

Download sample file here

CSV

XLSX

File Histories

Refresh

File name	Status	Server count	Action	
2020.3.0ServerimportSheet.xls	17%	Available: 0 Uploaded: 1 Failed: 5	6	+ -
2020.3.0ServerimportSheet.xls	0%	Available: 0 Uploaded: 0 Failed: 6	6	+ -
2020.3.0ServerimportSheet.xls	0%	Available: 0 Uploaded: 0 Failed: 6	6	+ -
2020.3.0ServerimportSheet.xls	0%	Available: 0 Uploaded: 0 Failed: 6	6	+ -
2020.3.0ServerimportSheet.xls	0%	INITIATED	6	+ -

Invalid file type. Please select a valid file format (csv / xlsx / xls).

Device :: Server > Import

Invalid file type. Please select a valid file format (csv / xlsx / xls).

Import

19.3.png

Uploader Info

Maximum 5 files (.xlsx or .csv) will be processed in parallel
Download sample file here

File Histories

Refresh

File name	Status	Server count	Action
2020.3.0ServerimportSheet.xls	17% Available: 0 Uploaded: 1 Failed: 5	6	
2020.3.0ServerimportSheet.xls	0% Available: 0 Uploaded: 0 Failed: 6	6	

Issues in Export Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device and click **Export**.

Device :: Server

Export

ADC **Server** WAF DNS Firewall Switch Router Proxy Cloud HSM Others MDM

Search...

Name	FQDN / IP address	Data center	Status	Vendor	Version	Port	Credential type
Linux_Valid	10.10.102.14	absecon	Managed	LinuxServer		22	Manual entry
Linux	10.10.102.14	absecon	Unresolved	LinuxServer		22	Manual entry
Linux_DZDO	10.10.102.14	absecon	Unresolved	LinuxServer		22	Manual entry
Linux_SUDO	10.10.102.14	absecon	Unresolved	LinuxServer		22	Manual entry
Linux_Invalid	1.2.3.4	absecon	Unresolved	LinuxServer		22	Manual entry

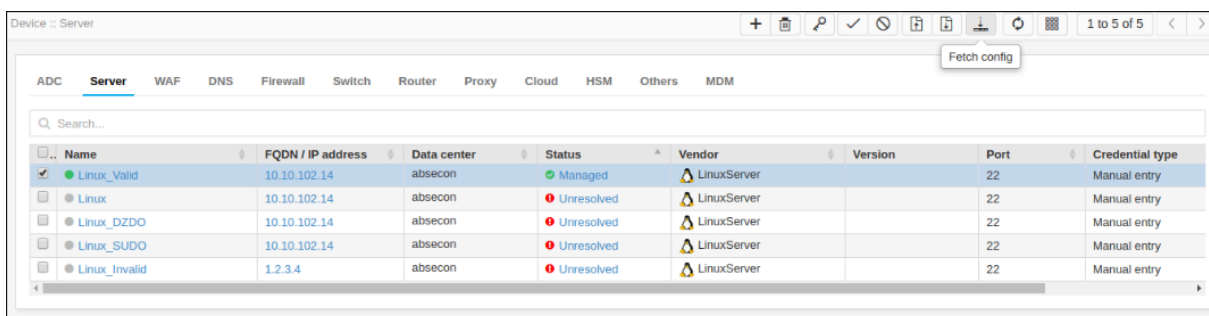
- Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Exception while exporting	1. General failure - Unable to create file on the local system due to permission issue. 2. Unable to fetch device list from the database.	1. Provide access to be able to create the file on the local system. (For example, check the directory where it is trying to export and give access to AppViewX for that directory.) 2. Make sure the database is running and has correct data.

Issues in Config Fetch

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Fetch Config**.



- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Communication to <IP/FQDN> has failed.	Device communication has failed due invalid credentials / SSH Port.	Verify the input details and check device status error messages in Issues in Communicating to Linux Server

Issues in Certificate Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

Discovery : Managed Devices Scan : Add Discovery

Discover Details

* Discovery Run Type ☒ On-demand ☐ Schedule ⓘ

* Discovery Instance Name ⓘ

Description

Discover By

You can either manually enter template details or upload a file.

* Discovery From ⓘ

Search...

☐ Select all All Selected Unselected Count: 1

☒ LinuxServer::Linux_Valid

Favorites

• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the "Discover By" section.	Select at least one device to discover certificates from.

Issues in CSR generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab.
The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. Click correct **Category** from the dropdown.
7. From the **Vendor** dropdown, click **Linux Server**.
A list of devices will be generated in the **Devices dropdown**.

CERT+

Search features

DASHBOARD

CERTIFICATE ACTION

- Enroll Certificate
- Renew Certificate
- Push to Device
- Reissue Certificate
- Revoke Certificate
- more

CERTIFICATE INVENTORY

- Server
- Client
- Code Signing Certificate
- Device
- Intermediate
- more

AUTOMATION

- My Workflows

Enroll Server Certificate

Certificate Profile: Server

* Connector Name: AppViewX CA connector

Description:

* CSR Generation: ☐ AppViewX ☐ Upload CSR ☐ HSM ☒ End Point

Category: Server

Vendor: LinuxServer

* Devices: Linux_Valid

Certificate Type: ☒ Default ☐ KDB

* CSR file name: .csr

* Key File Name: .key

CSR Parameters

* Common Name:

Subject Alternative Name:

Add Reset

- Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Problem while generating csr on target server	General Failure - SSH/SFTP communication failure	Provide correct credentials and make sure device communication is successful.
Invalid key type specified in the request	Given key type might not be supported by open SSL in the target machine.	Provide valid key type.
Problem while generating csr on the target server.	Location might not have permission.	Check the permission and provide it.
CSR and Private key has been failed	Open SSL configuration might be wrong in the target machine.	Check and correct open SSL configuration in the device.

Error Message	Possible Cause	Possible Solution
CSR generation got failed	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issues in Push and Rollback

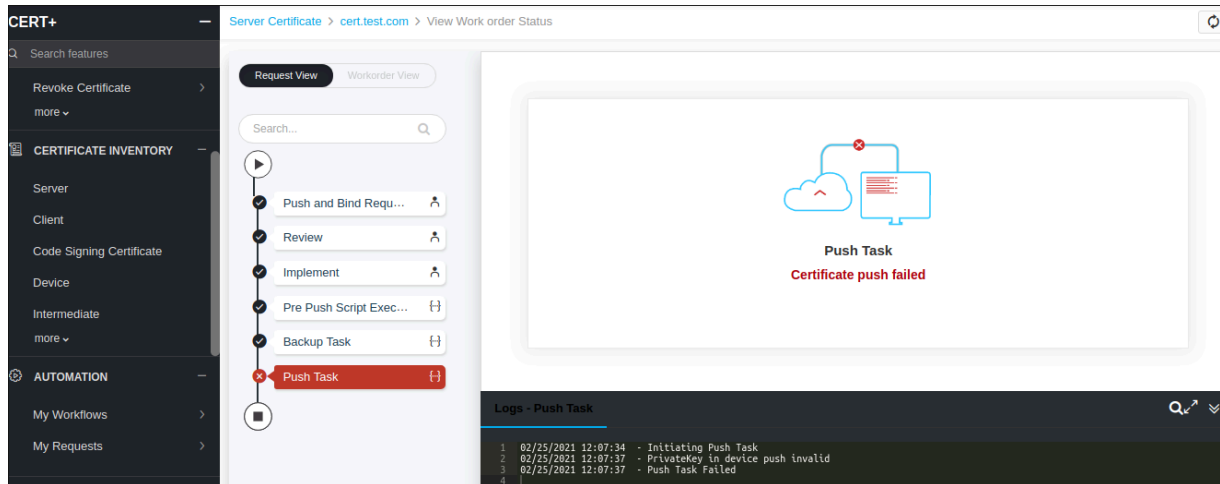
1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**.
The **Server Certificate** page is displayed.
4. Click any **Linux server**.
A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, select **Add App Connector**.
6. Push the certificate to the device.

The screenshot displays the AppViewX interface. On the left, the 'CERT+' sidebar is visible with 'CERTIFICATE INVENTORY' expanded and 'Server' selected. The main panel shows the 'Server Certificate' page for 'cert.test.com'. A workflow diagram on the left indicates the 'Push Task' step is failed (marked with a red 'X'). The central area shows a diagram of a cloud connected to a server with a red 'X' and the text 'Push Task Certificate push failed'. At the bottom, a 'Logs - Push Task' section shows the following log entries:

```

1 02/25/2021 11:57:54 - Initiating Push Task
2 02/25/2021 11:58:57 - Certificate Push Failed
3 02/25/2021 11:58:58 - Push Task Failed
4

```



• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	- Pushing to device when certificate is unavailable, i.e, in a new state. - Previous work order is in progress and not completed. - AppConnector might not be in sync.	- Push to device after certificate has been retrieved from CA. - Initiate push after previous work order is finished. - Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.

Error Message	Possible Cause	Possible Solution
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Certificate Push failed	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/write access to the path configured in application connector to certificate push.
PrivateKey in device push invalid	"Private key in Device" is enabled in application connector, but key is not available in device.	Ensure to enable "Private key in Device" attribute in application connector, if the certificate does not have the key and the certificate is generated using CSR gen option from Device.

Troubleshooting Tomcat Linux

- [Overview](#)
- [Issues in Tomcat Linux](#)

Overview

This document helps you troubleshoot the common problems that you might encounter when using Tomcat Linux functionalities. This guide will give more troubleshooting processes on issues related to

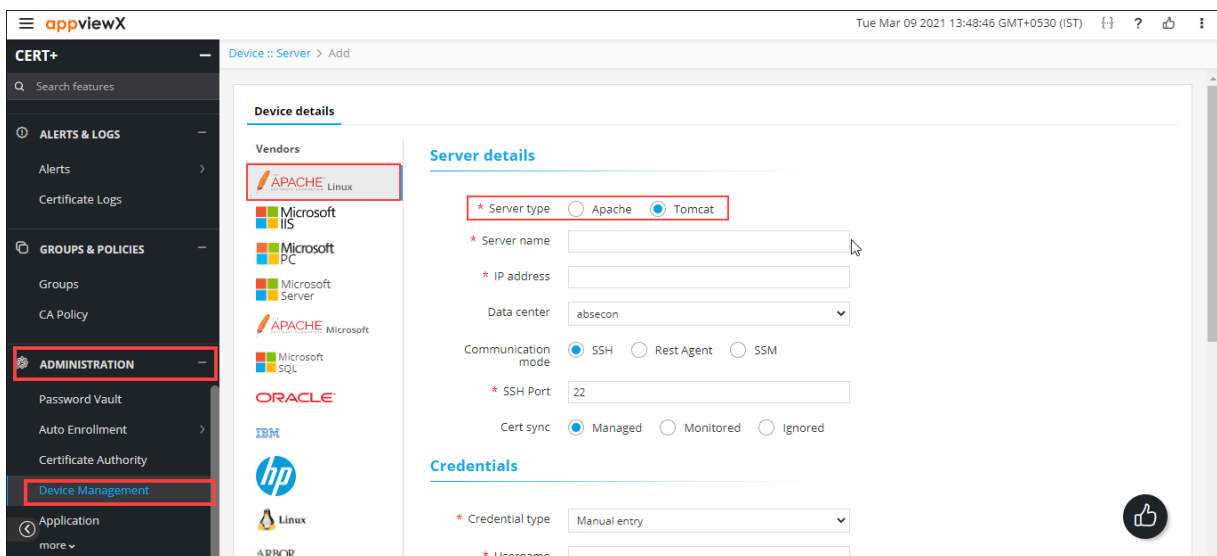
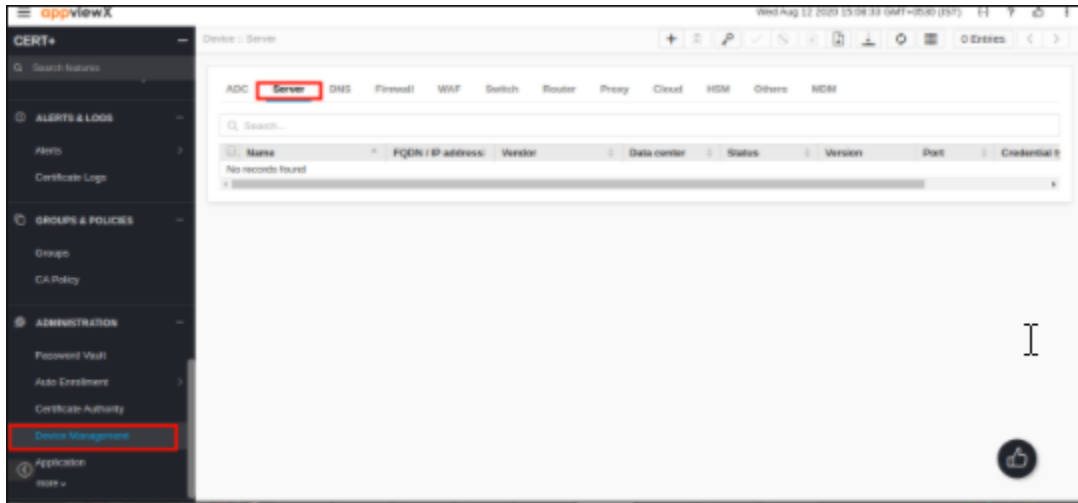
the Tomcat Linux server. The issues are device addition, communication to the server, CSR generation, access to the server, fetch configuration, discovery along with push and rollback.

Issues in Tomcat Linux

- [Issues in Device Addition using AppViewX UI](#)
- [Issues in Communicating to the server](#)
- [Issues in CSR Generation](#)
- [Issue in Access](#)
- [Issues in Fetch Config](#)
- [Issue in Discovery](#)
- [Issues in Push and Rollback](#)

Issues in Device Addition using AppViewX UI

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. From the icon list at the top right corner, click **Add**.
The **Device Addition** page is displayed.
6. From the **Device Details** section on the left, Click **Apache Linux**.
7. Click **Server type** as **Tomcat**.
8. Fill in the appropriate details.
9. Click **Add**.



- Error Messages

Error Messages

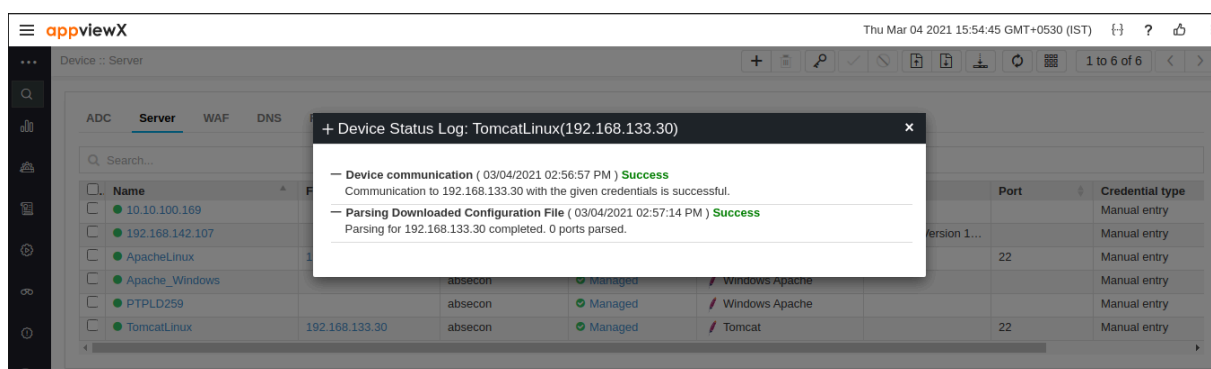
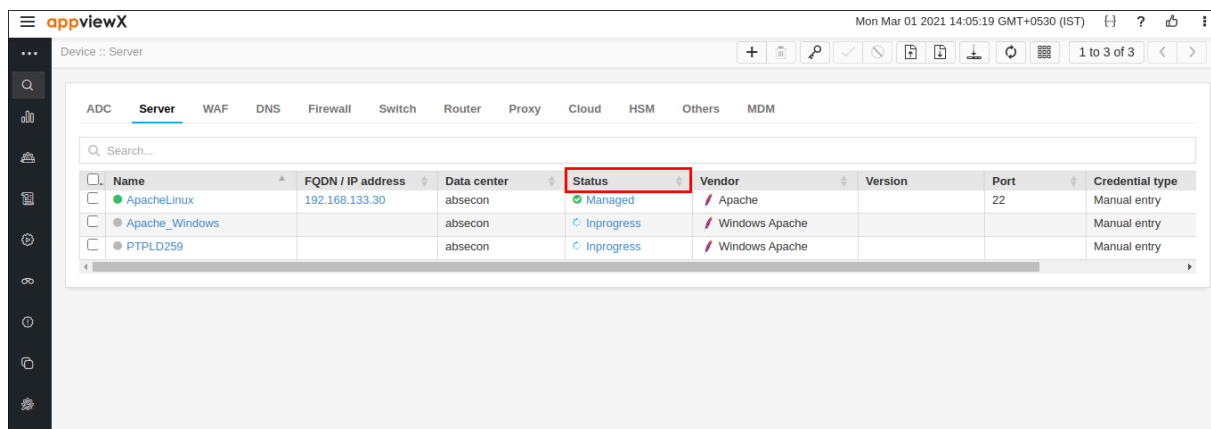
Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.

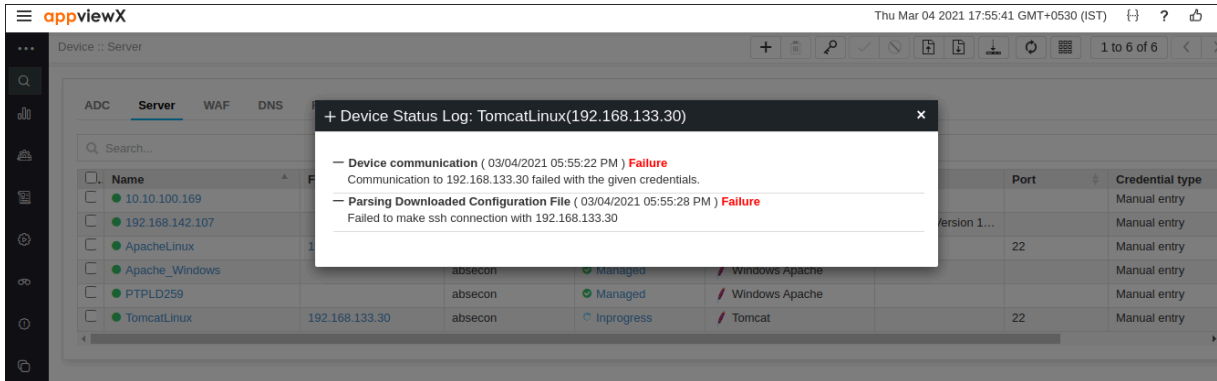
Error Message	Possible Cause	Possible Solution
Device name accepts '-', '_', '.', '*', ' ', '!' and space only, with min 2 and max 64 characters.	Server name is not valid.	Provide a server name with min 2 and max 64 characters with only the allowed characters.

Issues in Communicating to the server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**.

The **Device Communication Status** is displayed.





- **Error Messages**

Error Messages

Error Message	Possible Cause	Possible Solution
Failed to make the ssh connection with the given IP.	Given IP may not be connected to the network.	Validate whether username and password given during device addition are valid.
	Username/Password provided may be incorrect.	Ensure given IP is connected to the network.
	SFTP port is not open for SSH communication.	Open given port for the SSH communication.
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-', '_', ':', '*', ' ', '!' and spaces.
Device IP/FQDN cannot be null or empty.	Device IP/FQDN is empty.	Provide device IP/FQDN as it is a mandatory field.
Invalid device IP/FQDN address.	IP/FQDN address is not valid.	Provide valid IP/FQDN address.

Error Message	Possible Cause	Possible Solution
Access list for the device cannot be empty.	Credentials not provided for SSH communication.	Provide valid credentials for SSH communication.
Username cannot be null or empty.	Username is not provided or is empty.	Provide a valid username.
The Password cannot be null or empty.	Password is not provided or is empty.	Provide a valid password.
Key cannot be null or empty.	Key is not provided or is empty.	Provide a valid SSH key.
Password / key Mismatch or incorrect.	Unable to decrypt the password with the given key.	Provide a valid password that matches the key.
Device does not belong to Tomcat Server.	Device does not have any running tomcat instances.	Start any tomcat server in the device.
Failed to make ssh connection.	Target device may not be connected to the network.	Validate whether username and password given during device addition are valid.
	Username/Password provided may be incorrect.	Ensure the target device is connected to the network.
	The User may not have permission to execute the command.	Provide permission for the user to execute <code>"ps -ef"</code> command.
Linux rest agent communication failed	Rest agent installed in the device might not be running.	Install AppViewX Rest agent in device.
	The Client certificate installed in AppViewX might not be valid.	Install valid client certificate in AppViewX.
	Rest agent port might not be open for communication.	Ensure port is open for communication.
Error while decrypting password.	Password invalid for decryption key.	Check if the password matches with the decryption key.

Issues in CSR Generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.

The **Server Certificate** page is displayed.

3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab.

The **Enroll Server Certificate** page is displayed.

5. Click **End Point** as **CSR Generation Source** option.
6. Click correct **Category** from the dropdown.
7. Click correct **Vendor** from the dropdown.

A list of devices will be generated in the **Devices dropdown**.

8. For generating CSR, select **Apache** device.
9. Click **Add**.

The screenshot shows the 'Enroll Server Certificate' page in the AppViewX application. The page has a dark sidebar on the left with various icons. The main content area contains a form with the following fields:

- CA Account:** DigiCertCA
- Division:** AppViewX Inc.
- Certificate Type:** GeoTrust Standard DV
- Connector Name:** DigiCert GeoTrust Standard DV connector
- Description:** (empty text area)
- CSR Generation:**
 - ☐ AppViewX
 - ☒ End Point
 - ☐ Upload CSR
 - ☐ HSM
- Category:** Server
- Vendor:** Tomcat
- Devices:** TomcatLinux
- CSR Location:** /opt/automation
- CSR file name:** democert
- Key File Name:** demokey

• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
CSR Generation Failed.	Given CSR Location is not available in device.	Provide a valid path to store CSR and key.
	User does not have read/write permission for the location.	Ensure the user has read/write permission to the given location.
	“Openssl” package is not installed	Install “Openssl” package in the device
	The User does not have permission to execute “Openssl” commands.	Provide permission for user to execute “Openssl” commands

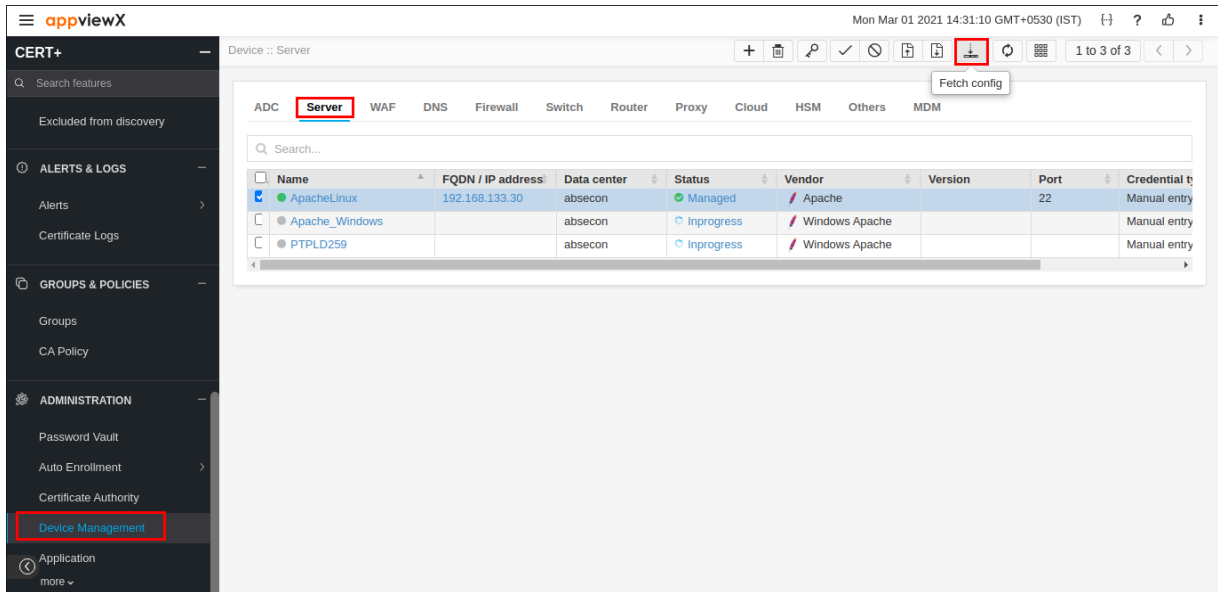
Issue in Access

Access Issues might occur when communicating with servers while discovering or fetching configuration files. These errors can be collected either from logs, API responses, or the status field of that server.

Error Message	Possible Cause	Possible Solution
Sudo Access failure	Linux Commands execution with sudo fails.	Verify if the system has the correct sudo setup.
File Download Failed.	User or User group does not have read/write permission for server.xml in device.	Provide read/write permission for user in device

Issues in Fetch Config

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Fetch Config**.



• Error Messages

Error Messages

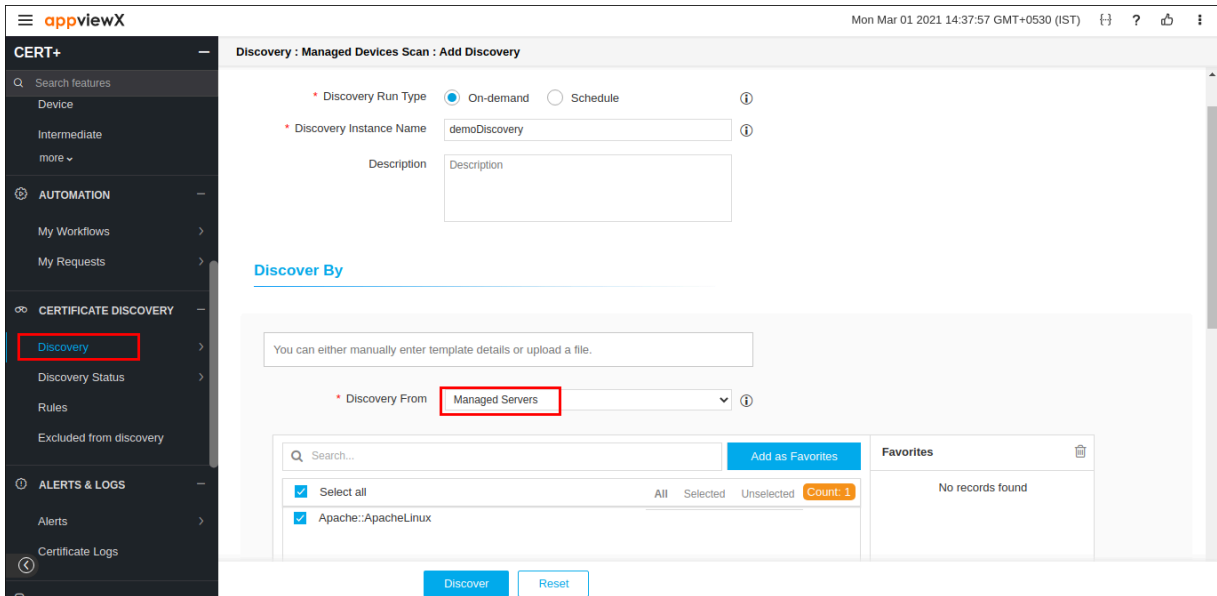
Error Message	Possible Cause	Possible Solution
XML Parsing Failure	FileName provided might not be a valid XML file.	Ensure the provided filename is a valid XML file.
File Download Failed.	server.xml is not found in the specified directory.	Ensure server.xml is present in the conf directory.

Issue in Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.



• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
File Not Found	server.xml is not present in the specified directory.	Ensure server.xml is present in the conf directory.
	SSL certificate or key file parsed from configuration file is not present in the specified directory.	Ensure parsed certificate or key file is present in the directory specified in server.xml
JKS Parsing Failure	Password for Keystore file may not be present in server.xml	Password given in server.xml might be incorrect.

Issues in Push and Rollback

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.

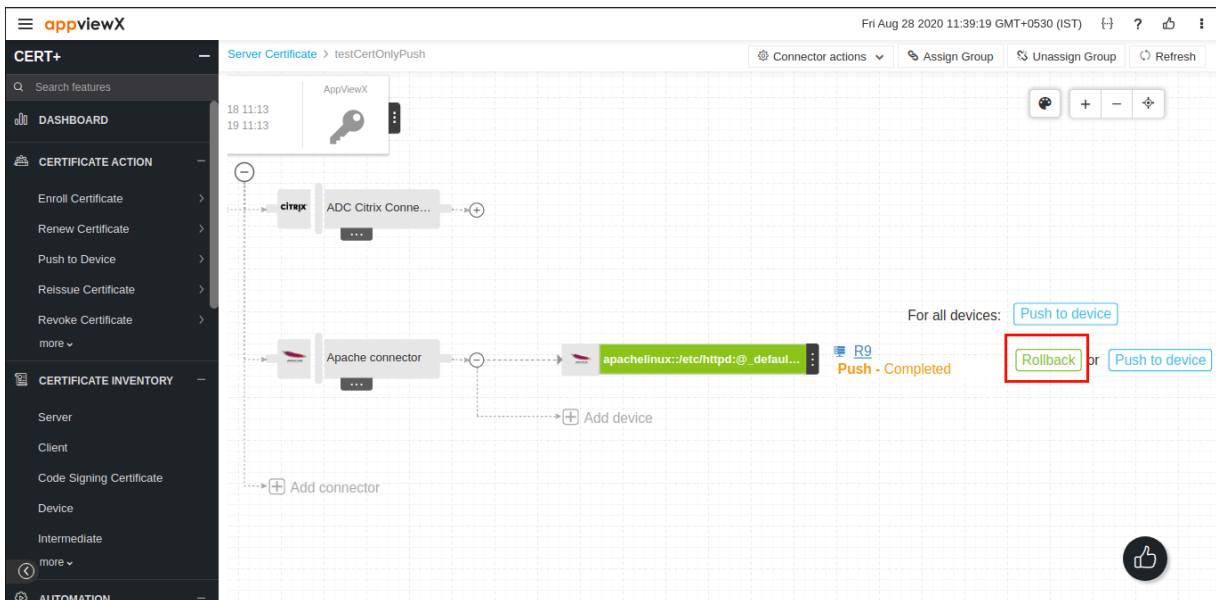
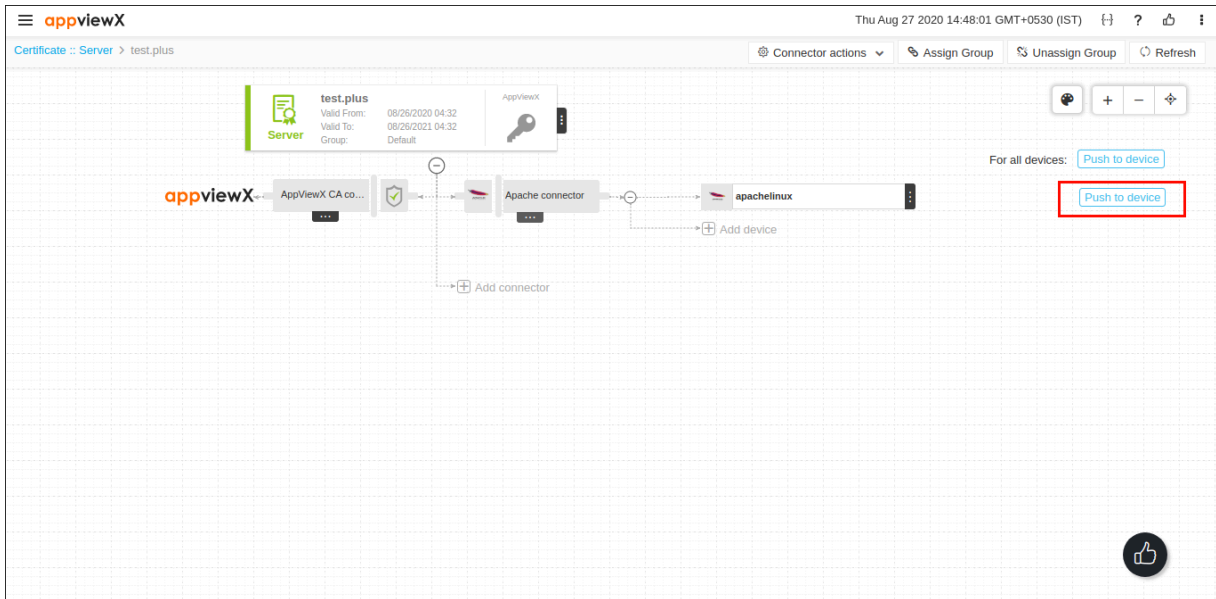
The **Server Certificate** page is displayed.

3. From the left pane, expand **Certificate Inventory**, select **Server**.

4. On the top right corner of the page, click **List**.

The **Server Certificate** page is displayed.

5. Click the certificate to be pushed or rolled back.



- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Push failed.	Creating local certificate files failed while Backup.	Provide required access to AppViewX to create local files
Certificate Push Failure	Invalid certificate, key, or trust location is given.	Provide the valid certificate, key, or trust location while adding an application connector.
Bind Failed as the SSL is disabled for the port	SSL is disabled for the given port on the server.	Kindly enable SSL for the port on the server.
KeyStore creation failed	Unable to create the Keystore locally.	Provide required access to AppViewX to create local files

Troubleshooting Weblogic Linux

- [Overview](#)
- [Issues in Weblogic Linux](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using Weblogic Linux functionalities. This guide will give more troubleshooting processes on issues related to Weblogic Linux server. The issues are device addition, communication to the server, CSR generation, fetch configuration, discovery along with push and rollback.

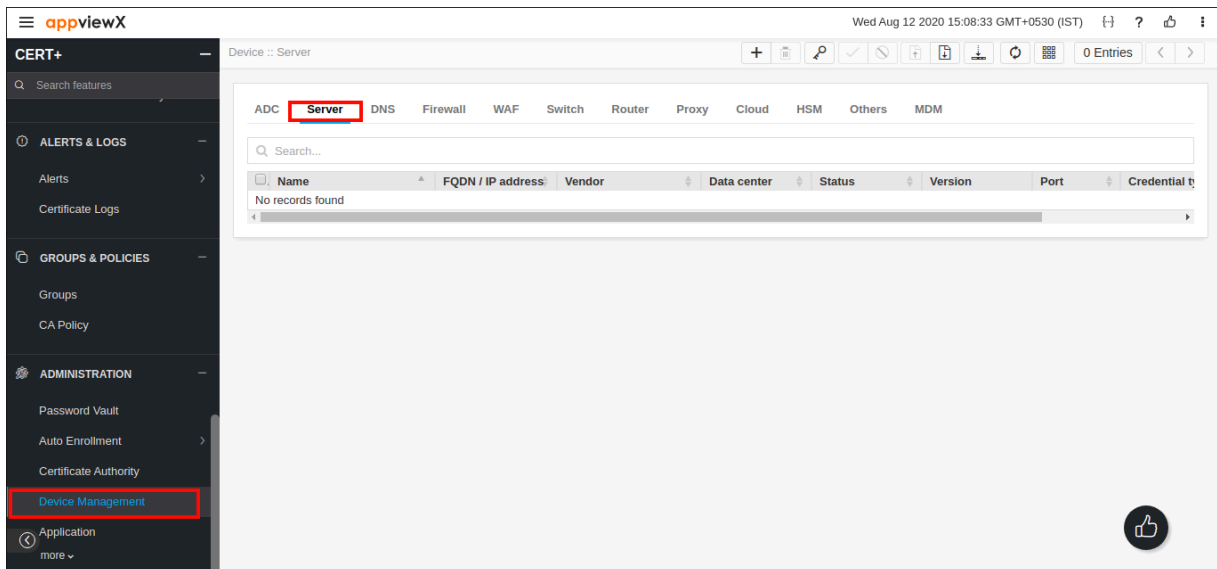
Issues in Weblogic Linux

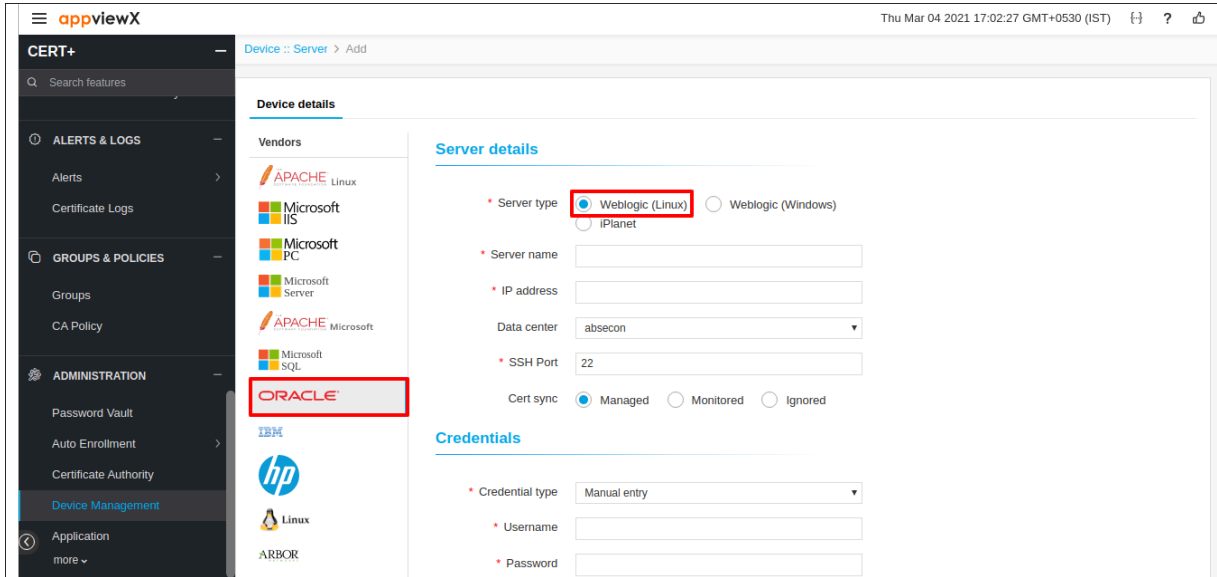
- [Issues in Device Addition using AppViewX UI](#)
- [Issues in Communicating to Weblogic Linux](#)
- [Issues in Fetch Config](#)
- [Issue in Discovery](#)

- [Issues in CSR generation](#)
- [Issues in Push and Rollback](#)

Issues in Device Addition using AppViewX UI

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. From the icon list at the top right corner, click **Add**.
The **Device Addition** page is displayed.
6. From the **Device Details Section** on the left, click **Oracle**.
7. Click **Server type** as **Weblogic(Linux)**.
8. Fill in the appropriate details.
9. Click **Add**.





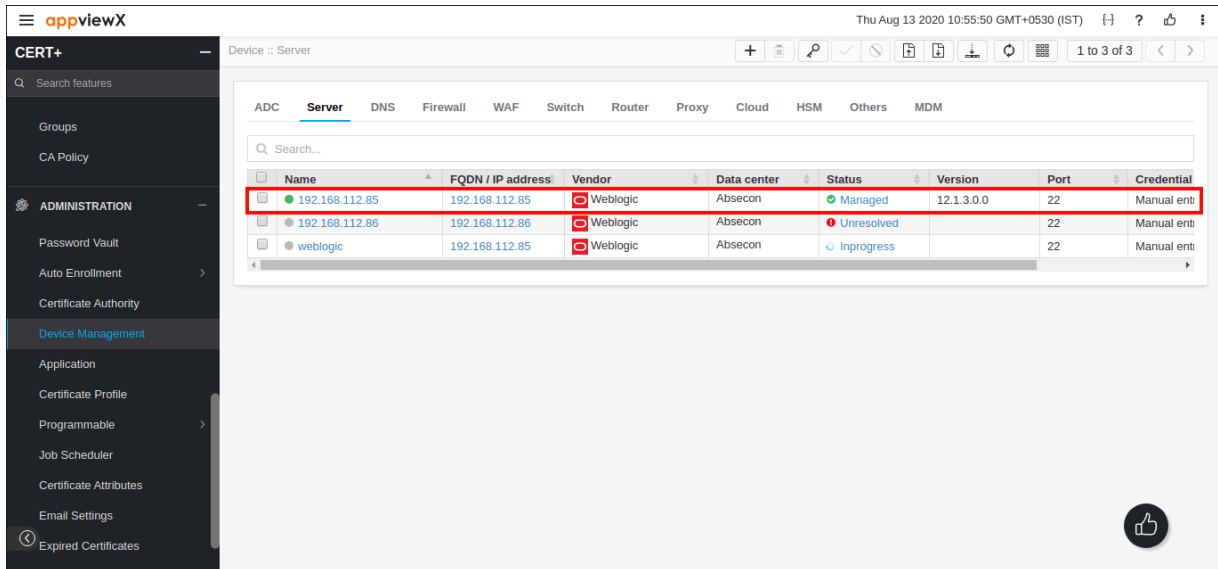
- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

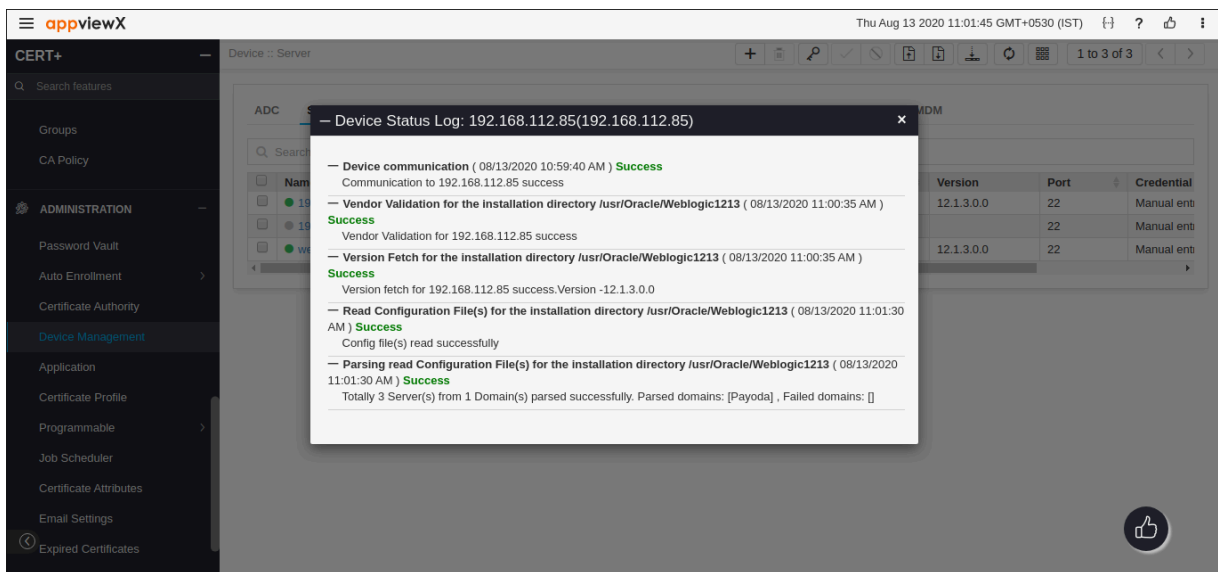
Issues in Communicating to Weblogic Linux

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**.
The **Device Communication Status** is displayed.



The screenshot shows the AppViewX interface with the 'Server' tab selected. A table lists devices with columns: Name, FQDN / IP address, Vendor, Data center, Status, Version, Port, and Credential. The first row is highlighted in red.

Name	FQDN / IP address	Vendor	Data center	Status	Version	Port	Credential
192.168.112.85	192.168.112.85	Weblogic	Absecon	Managed	12.1.3.0.0	22	Manual ent
192.168.112.86	192.168.112.86	Weblogic	Absecon	Unresolved		22	Manual ent
weblogic	192.168.112.85	Weblogic	Absecon	Inprogress		22	Manual ent



The screenshot shows the AppViewX interface with a 'Device Status Log' dialog box open. The dialog box displays a list of status messages for the device 192.168.112.85(192.168.112.85).

Device Status Log: 192.168.112.85(192.168.112.85)

- Device communication (08/13/2020 10:59:40 AM) **Success**
Communication to 192.168.112.85 success
- Vendor Validation for the installation directory /usr/Oracle/Weblogic1213 (08/13/2020 11:00:35 AM) **Success**
Vendor Validation for 192.168.112.85 success
- Version Fetch for the installation directory /usr/Oracle/Weblogic1213 (08/13/2020 11:00:35 AM) **Success**
Version fetch for 192.168.112.85 success:Version -12.1.3.0.0
- Read Configuration File(s) for the installation directory /usr/Oracle/Weblogic1213 (08/13/2020 11:01:30 AM) **Success**
Config file(s) read successfully
- Parsing read Configuration File(s) for the installation directory /usr/Oracle/Weblogic1213 (08/13/2020 11:01:30 AM) **Success**
Totally 3 Server(s) from 1 Domain(s) parsed successfully. Parsed domains: [Payoda] , Failed domains: []

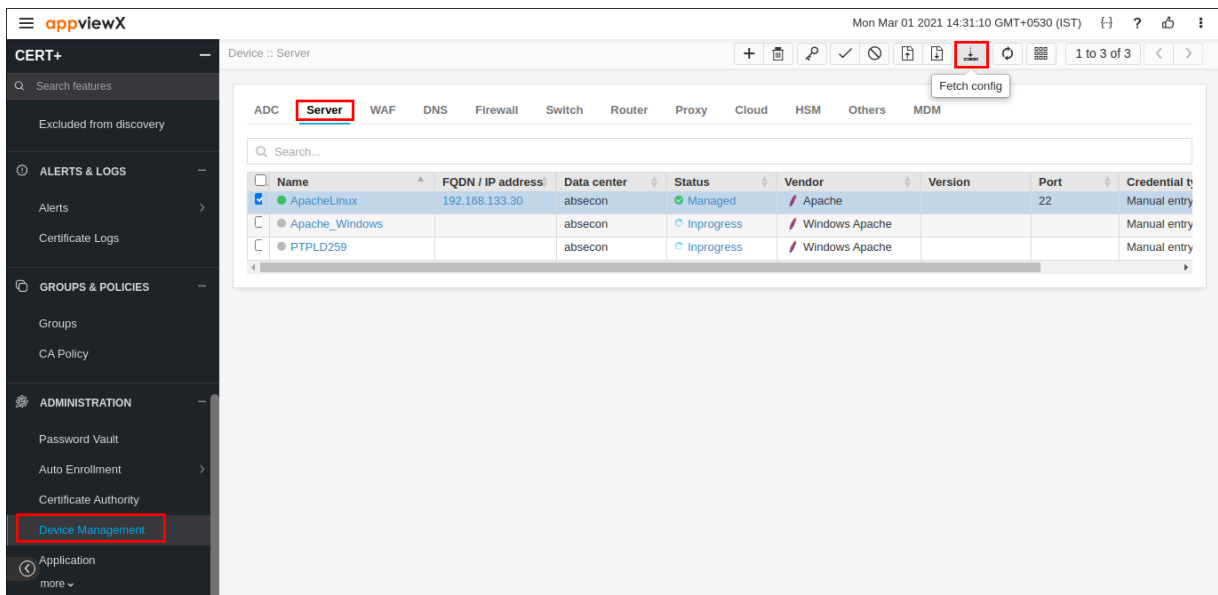
• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-', '_', ':', '*', ' ', '!' and spaces.
Device IP/FQDN cannot be null or empty.	Device IP/FQDN is empty.	Provide device IP/FQDN as it is a mandatory field.
Invalid device IP/FQDN address.	IP/FQDN address is not valid.	Provide valid IP/FQDN address.
Access list for device cannot be empty.	Access list provided is empty	Provide a valid access list to communicate with the device.
Username cannot be null or empty.	Username is null or empty.	Provide a valid username to communicate with the device.
Password cannot be null or empty.	Password is null or empty.	Provide a valid password to communicate with the device.
Key cannot be null or empty.	Key is null or empty.	Provide a valid key to communicate with the device.
Password / key Mismatch or incorrect.	Unable to decrypt the password with the given key.	Provide a valid password that matches with the key.
Failed to connect to the server.	Credentials to communicate with the device may be invalid.	Check and provide the proper credentials to communicate with the device.
No weblogic process is running	Weblogic processes running on the destination machine might be down.	Kindly check the status of the Weblogic process running in the destination machine.

Issues in Fetch Config

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Fetch Config**.



- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Password / key Mismatch or incorrect.	Unable to decrypt the password with the given key.	Provide a valid password that matches the key.
Domain-registry.xml is not accessible in the given path.	Given path may be invalid or AppViewX does not have	Please enter a valid path or Check permissions to access the file.

Error Message	Possible Cause	Possible Solution
	permission to access the file in the path.	
Config file parsing failed.	1. Configuration file might be corrupted/ empty. 2. AppViewX is not able to read/ parse the Config files from the server.	1. Verify if the configuration file is correct. 2. Check if the server has proper config files related to the Weblogic server and AppViewX has proper read permissions.

Issue in Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

The screenshot shows the AppViewX web interface. On the left, the 'Discovery' option under 'CERTIFICATE DISCOVERY' is highlighted with a red box. The main content area is titled 'Discovery : Managed Devices Scan : Add Discovery'. It contains a form with the following fields: 'Discovery Run Type' (radio buttons for 'On-demand' and 'Schedule', with 'On-demand' selected), 'Discovery Instance Name' (text input with 'demoDiscovery'), and 'Description' (text area). Below the form, there is a section titled 'Discover By' with a text input field. Underneath, 'Discovery From' is set to 'Managed Servers' (highlighted with a red box). At the bottom, there is a table with one entry 'Apache::ApacheLinux' and a 'Discover' button.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not entered or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.
Exception while fetching key and location details from request.	Certificate location details provided during the server addition might be wrong.	Check and provide the valid certificate location during server addition.

Issues in CSR generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab.
The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. Click the correct **Category** from the dropdown.
7. Select **Weblogic** as the **Vendor** from the dropdown.
A list of devices will be generated in the **Devices dropdown**.

The screenshot shows the 'Enroll Server Certificate' interface in the AppViewX console. The left-hand navigation menu is expanded, showing 'CERT+' at the top, followed by 'CERTIFICATE ACTION' with a sub-menu where 'Enroll Certificate' is selected and highlighted with a red rectangle. Below this are 'CERTIFICATE INVENTORY' and 'AUTOMATION'. The main content area is titled 'Enroll Server Certificate' and contains several form fields: 'CA Account' (AppViewX CA), 'Certificate Profile' (Server), 'Connector Name' (AppViewX CA connector), 'Description' (empty text area), 'CSR Generation' (radio buttons for AppViewX, End Point (selected), and Upload CSR; HSM is also present), 'Category' (Server), 'Vendor' (Weblogic, highlighted with a red rectangle), 'Devices' (None), 'CSR Location' (empty text area), 'CSR file name' (with a .csr file type indicator), and 'Key File Name' (with a .key file type indicator). At the bottom of the form are 'Add' and 'Reset' buttons.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Error while establishing SSH connection.	AppViewX is not able to establish a SSH connection using the given credentials.	Provide valid credentials to communicate with the device.
Error occurred while creating conf file to create csr.	AppViewX is not able to create a conf file in the export directory.	Check if AppViewX export directory has write permissions.
Invalid key type specified in the request	Given key type might not be supported by open SSL in the target machine.	Provide valid key type.
CSR and Private key has been failed	Open SSL configuration might be wrong in the target machine.	Check and correct open SSL configuration in the device.

Issues in Push and Rollback

Error Message	Possible Cause	Possible Solution
Error while establishing SSH connection.	AppViewX is not able to establish a SSH connection using the given credentials.	Provide valid credentials to communicate with the device.
Unable to parse configuration to fetch currently associated data.	AppViewX may not be able to fetch and parse the content of the certificate which is already associated.	Check if AppViewX has permissions for fetching the existing certificate content.
No server certificate is found	AppViewX may not be able to fetch and parse the content of the certificate which is already associated.	Check if AppViewX has permissions for fetching the existing certificate content.
Exception while downloading trust store / Exception while parsing certificate	AppViewX is not able to download the trust store from the server.	Check if AppViewX has permission to download the trust store from the device.
Certificate and/or key missing	Certificate provided in the push request might be invalid.	Check if the certificate that is being pushed is valid.
Unsupported Key Algorithm	Key algorithm of the certificate is not supported by the server.	Provide a valid key algorithm that is supported by Weblogic servers.
Push cannot be performed automatically for the Keystore type 'DemoidentityAndDemoTrust'. Kindly customize the keystore locations in the connector.	Customize push location not provided during push operation.	Provide a location to push the certificate inside the server.
Parsing a certificate is failed	Certificate content might be invalid.	Check the certificate content.

Error Message	Possible Cause	Possible Solution
Exception while writing file to avx local.	AppViewX may not have access to the local/export directory.	Check if AppViewX has permission for the local/export directory.
Certificate push is failed.	Invalid location provided. User is not having permission to push file to the location.	Check the location provided is valid. Check if the user has permission to access the location.
Unable to perform Bind for the server.	Server may not be running in the given address and port.	Check if the server is running in the given port and listen address
Unable to open edit session for the server.	AppViewX is not able to communicate with the server.	Check if the server is up and running and the server credentials are valid.
Unable to perform edit for the server.	AppViewX is not able to communicate with the server.	Check if the server is up and running and the server credentials are valid.
Unable to save the current changes made to the server.	AppViewX is not able to communicate with the server.	Check if the server is up and running and the server credentials are valid.
Unable to initiate request.	Pushing to device when certificate is unavailable, i.e, in a new state. Previous work order is in progress and not completed. AppConnector might not be in sync.	Push to device after certificate has been retrieved from CA. Initiate push after previous work order is finished. Synchronize the AppConnector and retry.

Error Message	Possible Cause	Possible Solution
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state.	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.

Troubleshooting Websphere Linux

- [Overview](#)
- [Issues in Websphere Linux](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using Websphere Linux functionalities. This guide will give more troubleshooting processes on issues related to

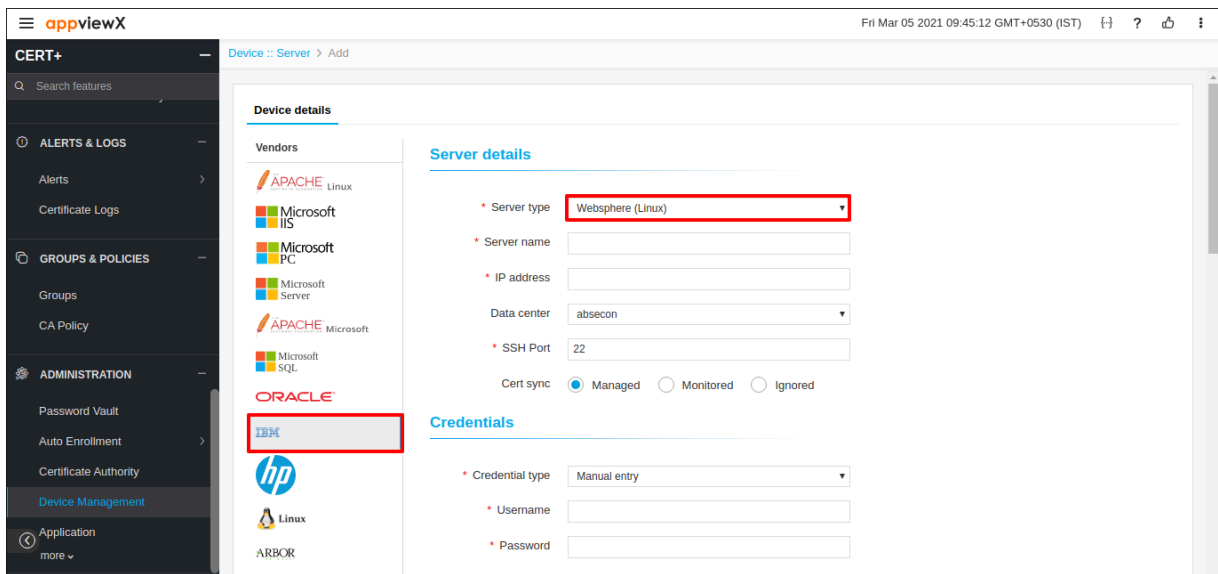
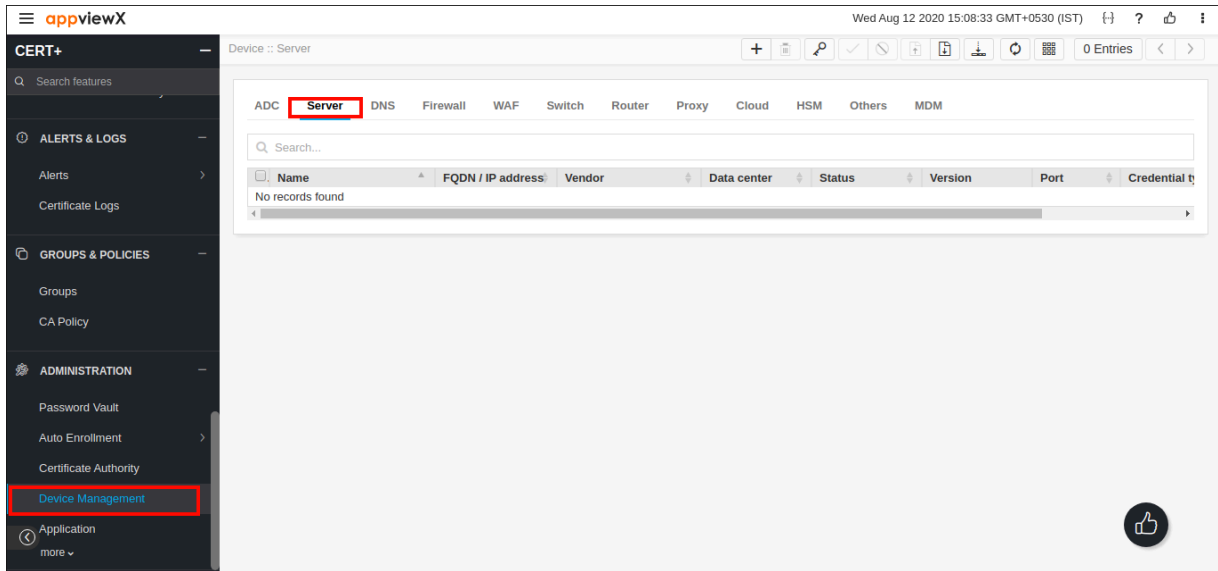
Websphere Linux server. The issues are device addition, communication to the server, CSR generation, fetch configuration, discovery along with push and rollback.

Issues in Websphere Linux

- [Issues in Device Addition using AppViewX UI](#)
- [Issues in Communicating to Apache Linux](#)
- [Issues in Fetch Config](#)
- [Issue in Discovery](#)
- [Issues in CSR generation](#)
- [Issues in Push and Rollback](#)

Issues in Device Addition using AppViewX UI

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. From the icon list at the top right corner, click **Add**.
The **Device Addition** page is displayed.
6. From the **Device Details Section** on the left, click **Oracle**.
7. Click **Server type** as **Websphere(Linux)**.
8. Fill in the appropriate details.
9. Click **Add**.



• Error Messages

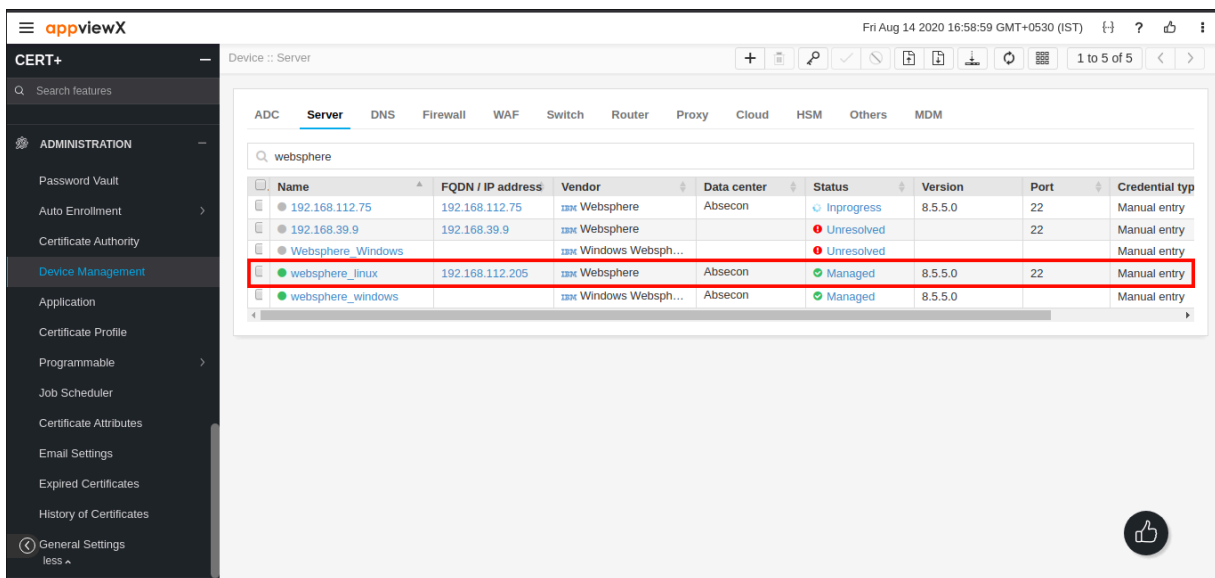
Error Messages

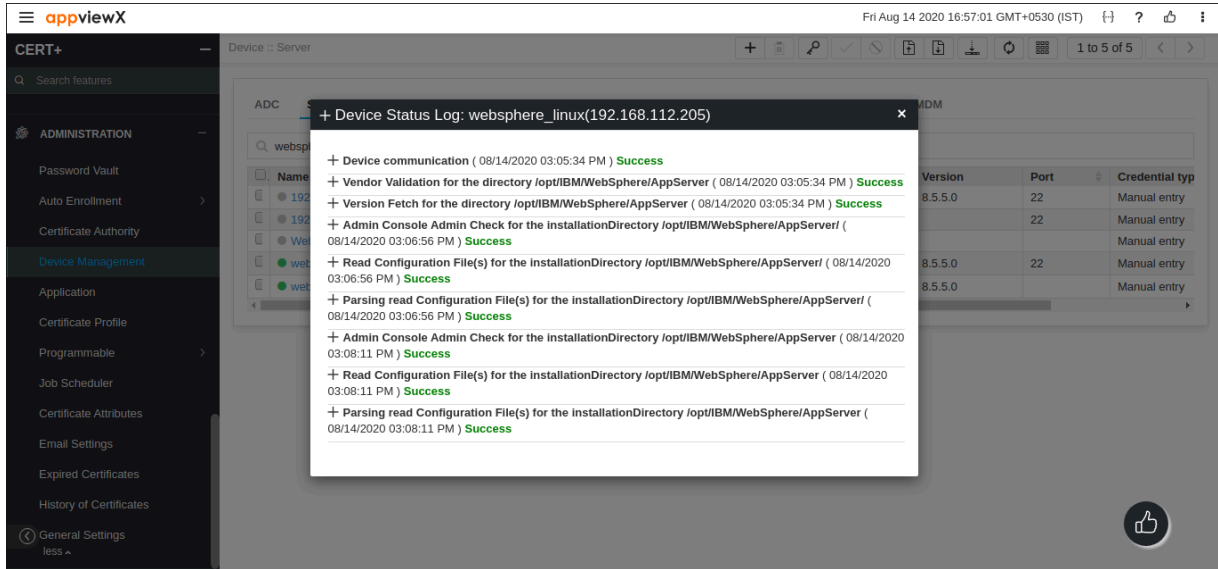
Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.

Error Message	Possible Cause	Possible Solution
Details incorrect	Some of the mandatory fields might either be missing or might be invalid.	Add all the valid information in the mandatory section.
WSadmin User name and WSadmin Password should not be empty	WSadmin username or password might be empty.	Add the valid WSadmin username and password.
Kindly add at least one WSadmin detail before saving.	WSadmin details are not added.	Add at least a single WS admin details.

Issues in Communicating to Apache Linux

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**.
The **Device Communication Status** is displayed.





• Error Messages

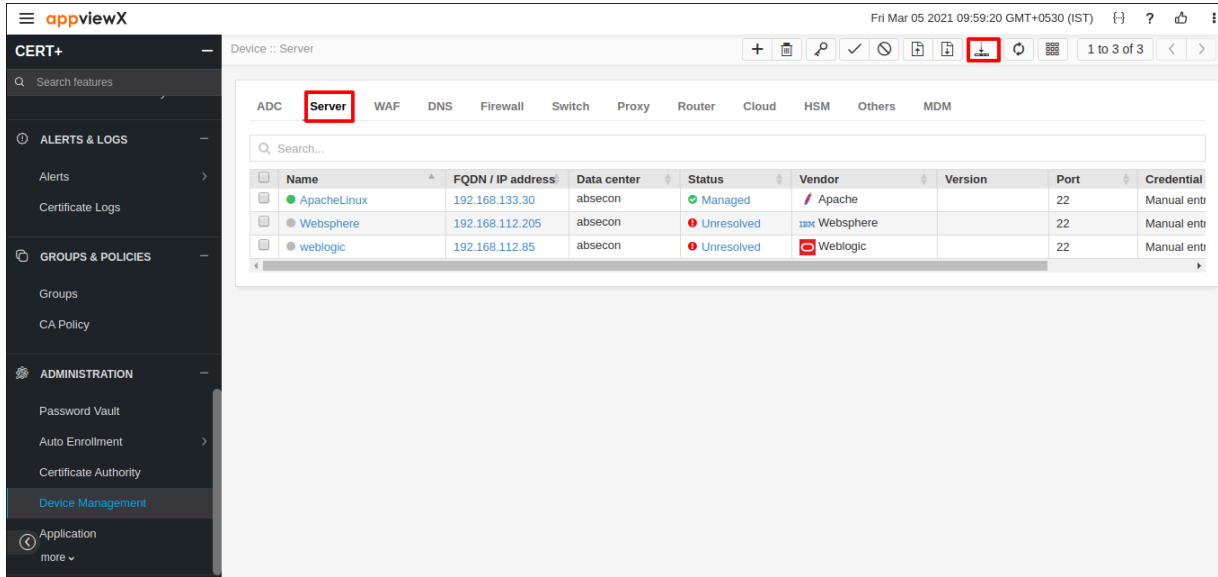
Error Messages

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-', '_', '.', '*', ' ', '!' and spaces.
Device IP/FQDN cannot be null or empty.	Device IP/FQDN is empty.	Provide device IP/FQDN as it is a mandatory field.
Invalid device IP/FQDN address.	IP/FQDN address is not valid.	Provide valid IP/FQDN address.
Access list for device cannot be empty.	Access list provided is empty	Provide a valid access list to communicate with the device.

Error Message	Possible Cause	Possible Solution
Username cannot be null or empty.	Username is null or empty.	Provide a valid username to communicate with the device.
Password cannot be null or empty.	Password is null or empty.	Provide a valid password to communicate with the device.
Key cannot be null or empty.	Key is null or empty.	Provide a valid key to communicate with the device.
Password / key Mismatch or incorrect.	Unable to decrypt the password with the given key.	Provide a valid password that matches with the key.
Service account user not found.	Credentials to communicate with the device may be invalid.	Check and provide the proper credentials to communicate with the device.
Authentication failure using Service account.	Credentials to communicate with the device may be invalid.	Check and provide the proper credentials to communicate with the device.
Ip does not belongs to Websphere	Destination machine might not have the required configuration for a Websphere application server.	Please check if the machine has Websphere configurations available in the destination machine.

Issues in Fetch Config

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click Fetch **Config**.



- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Password / key Mismatch or incorrect.	Unable to decrypt the password with the given key.	Provide a valid password that matches the key.
Service account user not found.	Credentials to communicate with the device may be invalid.	Check and provide proper credentials to communicate with the device.
Authentication failure using Service account.	Credentials to communicate with the device may be invalid.	Check and provide proper credentials to communicate with the device.
Permission denied to installation path.	AppViewX may not have the permission for the installation path.	Check if AppViewX has permission to access the installation path.
Invalid Credentials.	Invalid Credentials given for installation path.	Check if credentials have access to the installation path.
Permission denied	User does not have provision to access the installation path.	Check if AppViewX has permission to access the installation path.

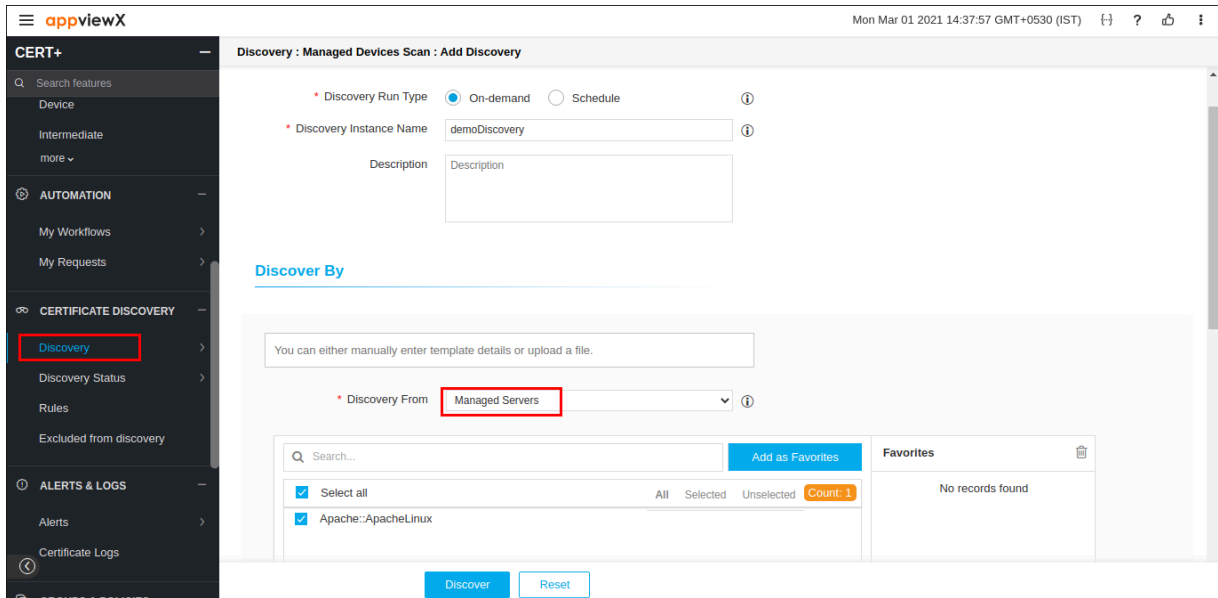
Error Message	Possible Cause	Possible Solution
Invalid installation path	Installation path does not exist.	Check if the installation path provided is a valid one.
Wsadmin objects unavailable	Wsadmin objects are unavailable	Check if the configurations related to WS are available in the destination machine.
security.xml file read operation failed	security.xml is not accessible in the given path.	Check if there is permission to access the file.
Config file parsing failed.	Configuration file might be corrupted/ empty.	Verify if the configuration file is correct.

Issue in Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.



- Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	Discovery name is not entered or its length is less than 2 characters. Interval between batches info. is missing when execution type is sequential.	Enter a valid name with a minimum of 2 characters. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.
Password / key Mismatch or incorrect.	Unable to decrypt the password with the given key.	Provide a valid password that matches the key.
Service account user not found.	Credentials to communicate with the device may be invalid.	Check and provide the proper credentials to communicate with the device.

Error Message	Possible Cause	Possible Solution
Authentication failure using Service account.	Credentials to communicate with the device may be invalid.	Check and provide the proper credentials to communicate with the device.
Permission denied to installation path.	AppViewX may not have the necessary permission for the installation path.	Check if AppViewX has permission to access the installation path.
Invalid Credentials.	Invalid Credentials are given to installation path.	Check if credentials have access to the installation path.
Permission denied	User does not have provision to access the installation path.	Check if AppViewX has permission to access the installation path.
Invalid installation path	Installation path does not exist.	Check the installation path provided is a valid one.
Wsadmin objects unavailable	Wsadmin objects unavailable	Check if the configurations related to WS are available in the destination machine.
security.xml file read operation failed	security.xml is not accessible in the given path.	Check for valid permission to access the file.
Config file parsing failed.	Configuration file might be corrupted/ empty.	Verify if the configuration file is correct.

Issues in CSR generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab.
The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. Click the correct **Category** from the dropdown.
7. Click **Websphere** as **Vendor** from the dropdown.
A list of devices will be generated in the **Devices dropdown**.

The screenshot shows the 'Enroll Server Certificate' interface in the AppViewX console. The left-hand navigation menu is expanded, showing 'CERT+' with sub-options like 'Enroll Certificate', 'Renew Certificate', 'Push to Device', 'Reissue Certificate', 'Revoke Certificate', and 'more'. The 'Enroll Certificate' option is selected and highlighted. The main content area contains a form with the following fields: 'CA Account' (AppViewX CA), 'Certificate Profile' (Server), 'Connector Name' (AppViewX CA connector), 'Description' (empty text area), 'CSR Generation' (radio buttons for AppViewX, End Point (selected), and HSM), 'Category' (Server), 'Vendor' (Websphere), 'Devices' (None), 'CSR Location' (empty text field), 'CSR file name' (with a .csr extension), and 'Key File Name' (with a .key extension). At the bottom of the form are 'Add' and 'Reset' buttons.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Error while establishing SSH connection.	AppViewX is not able to establish a SSH connection using the given credentials.	Check and provide valid credentials to communicate with the device.
Error occurred while creating conf file to create csr.	AppViewX is not able to create a conf file in the export directory.	Check if AppViewX export directory has write permissions.
Invalid key type specified in the request	Given key type might not be supported in the target machine.	Provide valid key type.
CSR and Private key has been failed.	Open SSL configuration might be wrong in the target machine.	Check and correct open SSL configuration in the device.

Issues in Push and Rollback

Error Message	Possible Cause	Possible Solution
security.xml file read operation failed	AppViewX may not be able to read security.xml of the profile.	Check if AppViewX has permissions to read security.xml of the profile.
Config file parsing failed	Configuration file might be corrupted/ empty.	Verify if the configuration file is correct.
Insufficient information to fetch backup data available in the server.	Configuration files fetched from the server may not have sufficient information.	Check if the config file has all the information related to server configuration.
Unsupported bit length	Bit length is not supported by the server.	Provide a valid bit length that is supported by Websphere server.
Unsupported Key Algorithm	Key algorithm of the certificate is not supported by the server.	Provide a valid key algorithm that is supported by Websphere servers.
Creating local certificate file failed - <Detailed Message>	AppViewX is not able to create file in a temporary folder.	Check the detailed message to determine the remedy.
Server certificate is not available to push.	Server certificate location may be invalid.	Check if the trust store location is available.
Private Key doesnot exists for certificate	Private key may not be available for the certificate.	Check if the private key for the certificate is available.
Private key parsing failed for the certificate.	Private key may be a invalid one.	Check if the private key is valid.
Writing of converted certificate related files into file in AppViewX local directory is failed.	AppViewX may not have permission to write a file in the export directory.	Check if AppViewX has proper permissions for the export directory.
Certificate created date is earlier than server present time	The starting of certificate validity period is earlier than the servers present time.	The starting of certificate validity period should match with the server's time. It should be greater than the server's present time.

Error Message	Possible Cause	Possible Solution
Unsupported Type	Certificate format is not supported by the server.	Check for the supported certificate formats.
Error found in wsadmin response	The WSadmin console may not be working on the server.	Kindly check WSadmin console is properly working or not
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.

Error Message	Possible Cause	Possible Solution
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.

Troubleshooting Websphere Windows

- [Overview](#)
- [Issues in Websphere](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with Websphere Windows.

Issues in Websphere

- [Issue in Server Addition using AppViewX UI](#)
- [Issues in Device communication](#)
- [Issue in Discovery](#)
- [Issues in CSR generation at Endpoint](#)
- [Issues in Certificate Push](#)

Issue in Server Addition using AppViewX UI

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. From the icon list at the top right corner, click **Add**.
The **Device Addition** page is displayed.
6. From the **Device Details Section** on the left, click **IBM**.

7. Select **Websphere(Windows)**.
8. Fill in the appropriate details.
9. Click **Add**.

- [Error Messages](#)

Error Messages

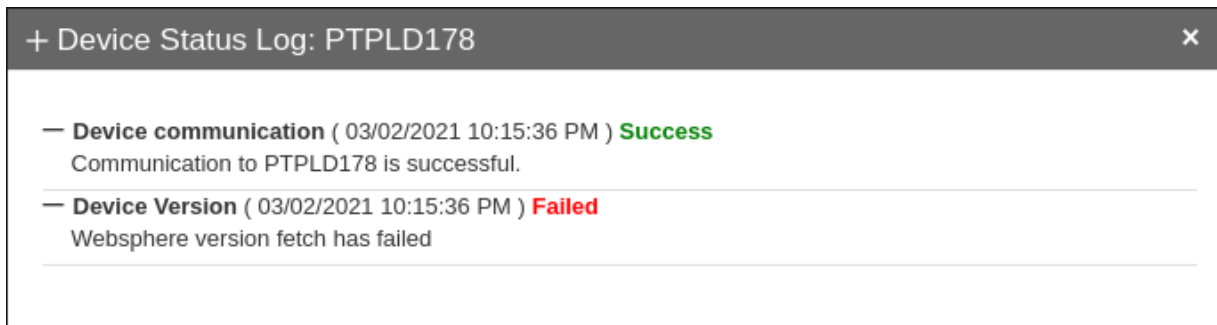
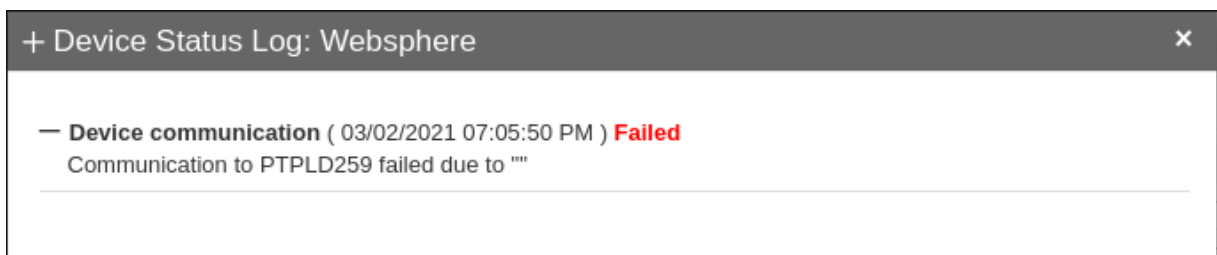
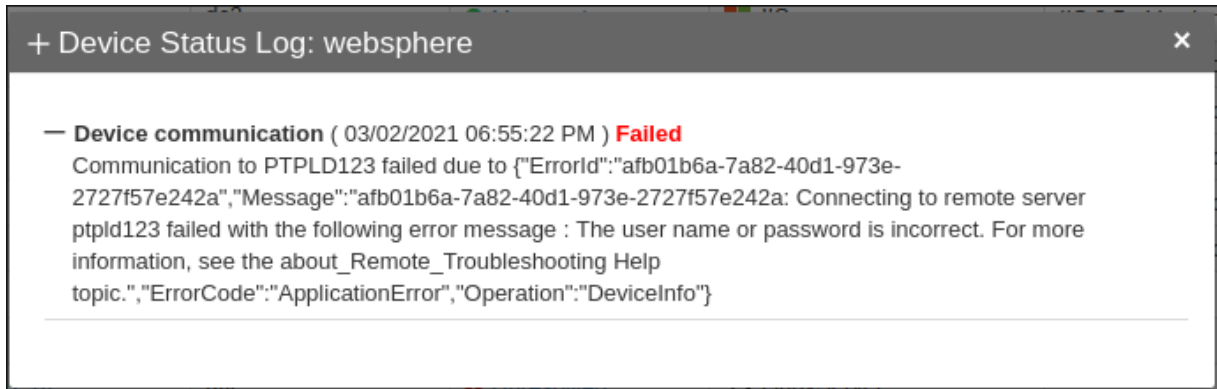
Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

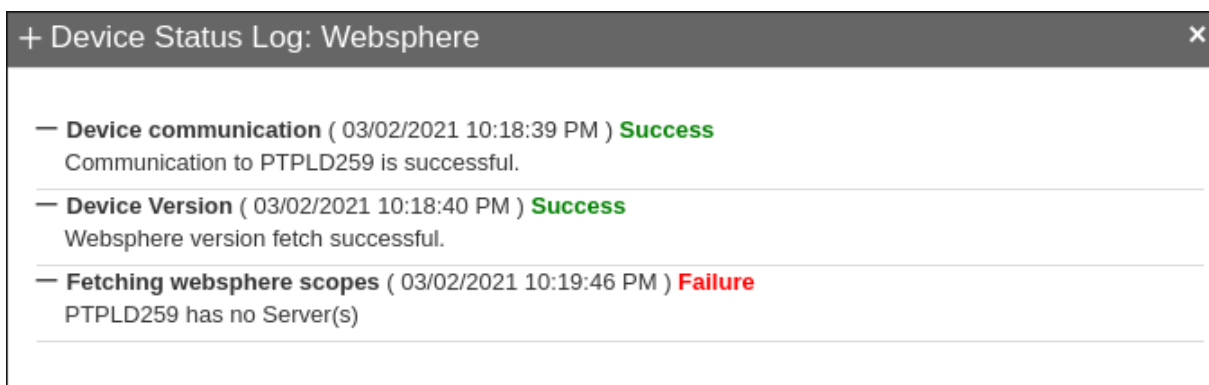
Issues in Device communication

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**.
The **Device Communication Status** is displayed.

	linuxrest	192.168.133.30	dc2	 Unresolved	 LinuxServer		
	websphere		dc2	 Unresolved	 Windows Websphere		Manual entry







- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Connecting to remote server ptpld123 failed with the following error message : The user name or password is incorrect. For more information, see the about_Remote_Troubleshooting Help topic.	Invalid hostname/ Invalid credential	Kindly check if the given host is reachable. Kindly provide valid credentials and update the device details.
Communication to <host> failed.	Windows Agent is not reachable or down	Kindly check if windows agent configured and in running state.
Websphere version fetch has failed	Websphere setup is not available/not configured in given device	Kindly validate is Websphere configured properly

Issue in Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.

The **Server Certificate** page is displayed.

3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

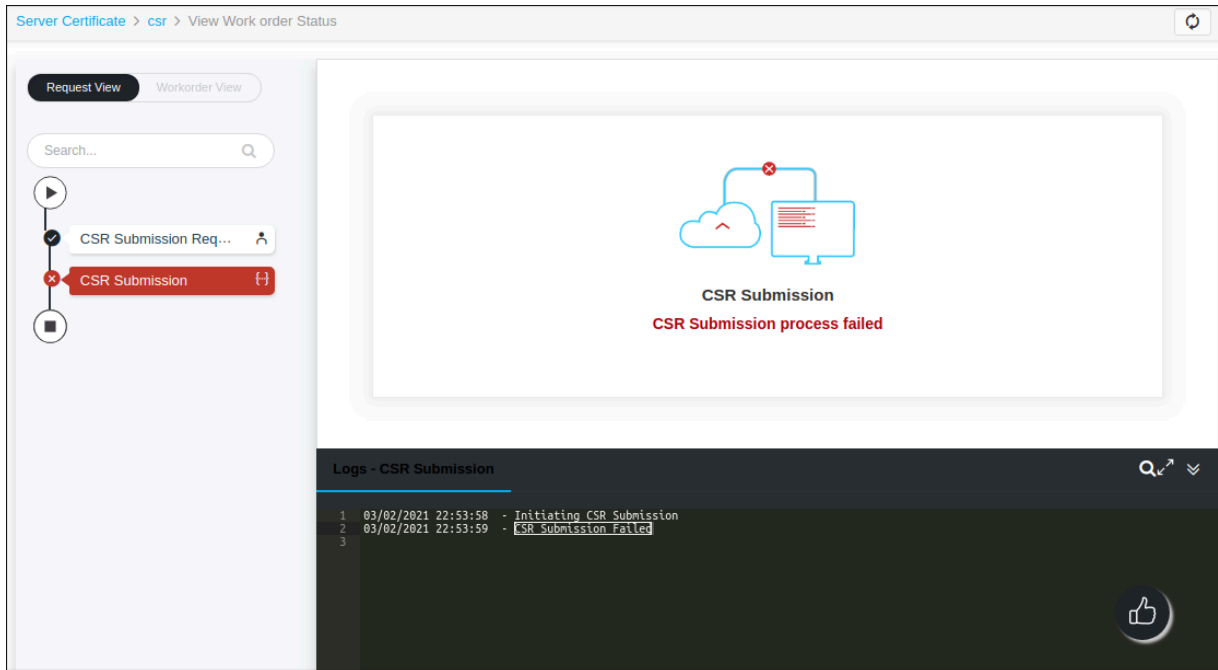
• [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Received failed response from batch.	1. No valid keystore files available in the given path. 2. Users don't have access for the configured location/file. 3. Web Server or WAS console is not active.	1. Kindly Ensure the given certificate location has a valid cert. 2. Kindly ensure users have proper access privilege to read certs. 3. Kindly ensure WebServer is in up and running state

Issues in CSR generation at Endpoint

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab.
The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, click correct **Category**.
7. From the **Vendor** dropdown, click **Websphere Windows**.
A list of devices will be generated in the **Devices dropdown**.



• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
CSR Submission Failed	User may have restricted access to the path configured for the "CSR FileName" and "Key File name"	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issues in Certificate Push

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**.
The **Server Certificate** page is displayed.
4. Click any **Linux server**.
A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, select **Add App Connector**.

6. Push the certificate to the device.

Server Certificate > Webi > View Work order Status

Request View Workorder View

Search...

Push Without Bind Re...
Review
Implement
Pre Push Script Exec...
Push Task

Push Task
Certificate push failed

Logs - Push Task

```

1 03/02/2021 22:46:35 - Initiating Push Task
2 03/02/2021 22:46:38 - Error while pushing certificate into device : Websphere due to java.lang.String cannot be cast to con.appvle
3 03/02/2021 22:46:38 - Push Task Failed
4

```

Server Certificate > PTPLD178.avxdevlab.net > View Work order Status

Request View Workorder View

Search...

Push Without Bind Re...
Review
Implement
Pre Push Script Exec...
Push Task

Push Task
Certificate push failed

Logs - Push Task

```

1 03/02/2021 22:48:41 - Initiating Push Task
2 03/02/2021 22:48:45 - Error while pushing certificate into device : Websphere due to Unsupported bit length:4096
3 03/02/2021 22:48:45 - Push Task Failed
4

```

Server Certificate > Wbi > View Work order Status

Request View Workorder View

Search...

☒ Push Without Bind Re...
☒ Review
☒ Implement
☒ Pre Push Script Exec...
☒ **Push Task**

Push Task
Certificate push failed

Logs - Push Task

```

1 03/02/2021 22:44:15 - Initiating Push Task
2 03/02/2021 22:44:18 - Error while pushing certificate into device : Websphere due to Unsupported Key Algorithm:DSA
3 03/02/2021 22:44:18 - Push Task Failed
4

```

Server Certificate > mtest > View Work order Status

Request View Workorder View

Search...

☒ Push Without Bind Re...
☒ Review
☒ Implement
☒ Pre Push Script Exec...
☒ **Push Task**

Push Task
Certificate push failed

Logs - Push Task

```

1 1/02/2021 22:57:49 - Initiating Push Task
2 1/02/2021 22:57:53 - Error while pushing certificate into device : Websphere due to Private key is not available. Failing the push
3 1/02/2021 22:57:53 - Push Task Failed
4

```

- Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Error while pushing certificate into device.	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/write access to the path configured in application connector to certificate push.
Error while pushing certificate into device : Websphere due to Unsupported bit length:4096.	Websphere will support bitlength up to 2048.	Kindly ensure the certificate issued is compatible with the Websphere.
Error while pushing certificate into device : Websphere due to Unsupported Key Algorithm:DSA	Unsupported key Algorithm.	Kindly ensure the certificate issued is compatible with the Websphere.
Error while pushing certificate in Device : <device name>.PrivateKey not available.	Private key is not available to parse certs.	Kindly ensure to push certs with private key. If privatekey is available in the device please select privateKeyInDevice option.

Troubleshooting Windows Apache Server

- [Overview](#)
- [Issues in Apache Server](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with Windows Apache server.

Issues in Apache Server

- [Issues in Device communication](#)
- [Issue in Discovery](#)
- [Issues in CSR generation at Endpoint](#)
- [Issues in Certificate Push](#)

Issues in Device communication

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the **Windows Apache Device**, click **Status**.
The **Device Communication Status** is displayed.

ADC

Server

WAF

DNS

Firewall

Switch

Router

Proxy

Cloud

HSM

Others

MDM

Q

Apache_Windows

Name	FQDN / IP address	Data center	Status	Vendor	Version	Port	Credential type
Apache_Windows		absecon	Unresolved	Windows Apache			Manual entry

+ Device Status Log: Apache_Windows

Device communication (03/10/2021 05:30:39 AM) **Failure**

Device communication failed.

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Device communication failed	1. Given credential is incorrect. 2. Windows agent may not be working. 3. Device not reachable 4. Hostname value is incorrect	1. Check and input the correct credential. 2. Check and input the correct hostname value 3. Ensure the device is reachable 4. Ensure windows agent is working for communication mode gateway 5. When the communication mode selected is SSM, Ensure SSM details given are correct

Issue in Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

ADC	Server	WAF	DNS	Firewall	Switch	Router	Proxy	Cloud	HSM	Others	MDM
Apache-windows											
☐	Name	FQDN / IP address	Data center	Status	Vendor	Version	Port	Credential type			
☐	Apache-windows		absecon	Managed	Windows Apache			Manual entry			

Search...			
Title	Status	Message	Time
Certificate Discovery	Failed	Received failed response for the batch	02/25/2021 18:12:05
OK			

- [Error Messages](#)

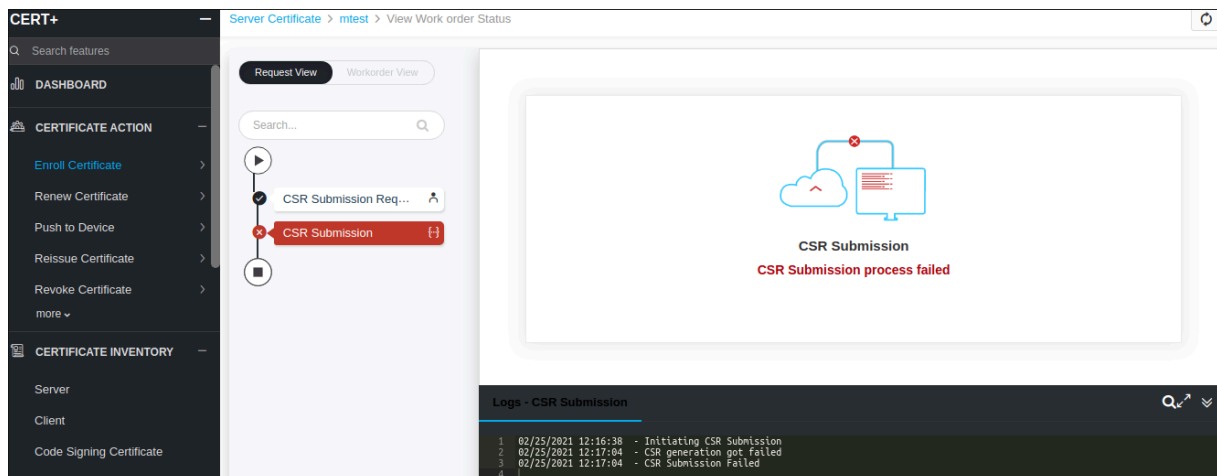
Error Messages

Error Message	Possible Cause	Possible Solution
Received failed response from batch	1. Device not running or not accessible 2. No valid certificates available	1. Ensure target device is up and running 2. Check the device has valid certificate files

Issues in CSR generation at Endpoint

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab.
The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, Click correct **Category**.
7. From the **Vendor** dropdown, click **Windows Apache**.

A list of devices will be generated in the **Devices** dropdown.



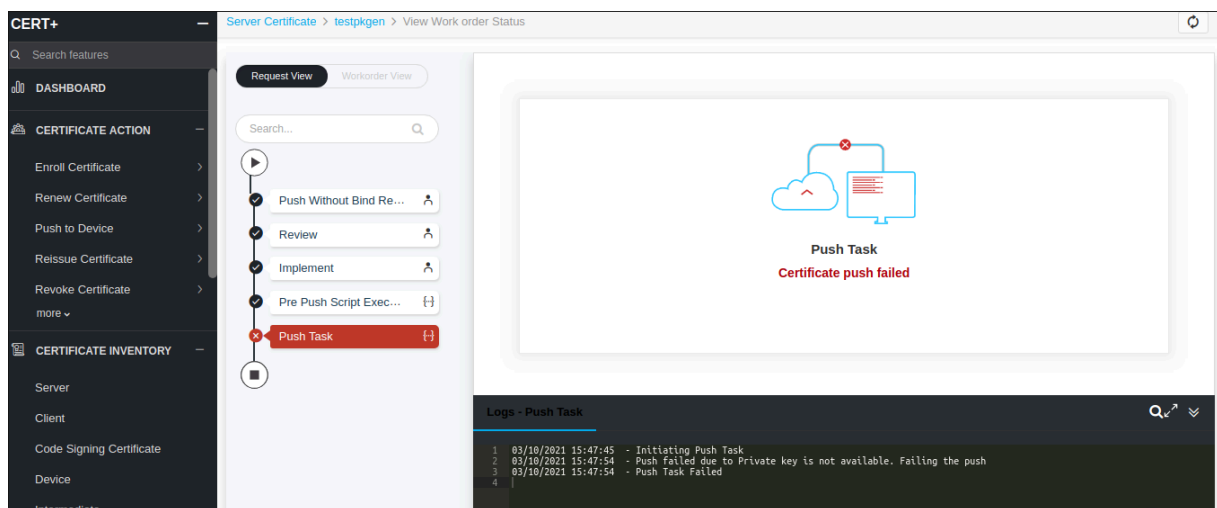
- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
CSR generation got failed/User has no permission for the given location to perform the operation.	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issues in Certificate Push

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**.
The **Server Certificate** page is displayed.
4. Click any **Windows Apache server**.
A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, select **Add App Connector**.
6. Push the certificate to the device.



CERT+ Server Certificate > ApacheWinPush.appviewx.comSTHEF > View Work order Status

Search features

DASHBOARD

CERTIFICATE ACTION

- Enroll Certificate
- Renew Certificate
- Push to Device
- Reissue Certificate
- Revoke Certificate
- more

CERTIFICATE INVENTORY

- Server
- Client
- Code Signing Certificate
- Device

Request View Workorder View

Search...

Push Without Bind Re...
Review
Implement
Pre Push Script Exec...
Push Task

Push Task
Certificate push failed

Logs - Push Task

```
1 03/10/2021 15:43:33 - Initiating Push Task
2 03/10/2021 15:43:44 - Push failed due to Private key In device configured. But key content is available with the certificate from
3 03/10/2021 15:43:44 - Push Task Failed
4
```

CERT+ Server Certificate > testpkgen > View Work order Status

Search features

DASHBOARD

CERTIFICATE ACTION

- Enroll Certificate
- Renew Certificate
- Push to Device
- Reissue Certificate
- Revoke Certificate
- more

CERTIFICATE INVENTORY

- Server
- Client
- Code Signing Certificate
- Device

Request View Workorder View

Search...

Push Without Bind Re...
Review
Implement
Pre Push Script Exec...
Push Task

Push Task
Certificate push failed

Logs - Push Task

```
1 03/10/2021 15:52:41 - Initiating Push Task
2 03/10/2021 15:52:51 - Push failed due to Private key is not available in device. Failing the push
3 03/10/2021 15:52:51 - Push Task Failed
4
```


The screenshot shows the AppViewX interface with the 'CERT+' section selected. The left sidebar lists various actions and inventory items. The main content area displays a workflow for 'Push Task' with steps: 'Push Without Bind Re...', 'Review', 'Implement', 'Pre Push Script Exec...', and 'Push Task'. The 'Push Task' step is highlighted in red, indicating a failure. The right panel shows a diagram of a cloud connected to a server with a red 'X' over the connection, and the text 'Push Task' and 'Certificate push failed'. Below this, a log entry shows the failure details.

Push Task
Certificate push failed

Logs - Push Task

```

1 03/09/2021 12:04:26 - Initiating Push Task
2 03/09/2021 12:04:44 - Push failed since cannot write-into/create location(s) [root/, root/]
3 03/09/2021 12:04:44 - Push Task Failed
4

```

The screenshot shows the AppViewX interface with the 'CERT+' section selected. The left sidebar lists various actions and inventory items. The main content area displays a workflow for 'Pre Push Script Execution' with steps: 'Push Without Bind Re...', 'Review', 'Implement', 'Pre Push Script Exec...', and 'Pre Push Script Execution'. The 'Pre Push Script Execution' step is highlighted in red, indicating a failure. The right panel shows a diagram of a cloud connected to a server with a red 'X' over the connection, and the text 'Pre Push Script Execution' and 'Pre push script execution failed'. Below this, a log entry shows the failure details.

Pre Push Script Execution
Pre push script execution failed

Logs - Pre Push Script Execution

```

1 03/09/2021 12:02:01 - Initiating Pre Push Script Execution
2 03/09/2021 12:02:03 - Device is not in managed state
3 03/09/2021 12:02:03 - Pre Push Script Execution Failed
4

```

• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Push failed due to Private key is not available. Failing the push	Private key not available in push request certificate	Please ensure the private key is available in request
Push failed due to Private key In device configured. But key content is available with the certificate from appview pushRequest So failing push request.	Trying to push a certificate with key when the "Private key in device" enabled	Ensure the push certificate has no key when "Private key in device" is enabled.
Push failed due to Private key is not available in device. Failing the push	Private key file not available in the given key location when "Private key in device" is enabled	Ensure the target device has key file in the given location
Push failed since cannot write-into/create location(s)	User does not have the permission to perform the operation	1.Ensure the user has permission. 2.For sudo user, please check the access elevation value given in device addition
Device is not in managed state	Device is not available in managed	Please check the device status in device inventory

Troubleshooting Windows JBoss Server

- [Overview](#)
- [Issues in Windows JBoss Server](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. Effective troubleshooting documents depend on the availability of useful, detailed information. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with Windows JBoss server.

Issues in Windows JBoss Server

- [Issues in Windows JBoss Server Addition using AppViewX UI](#)
- [Issues in Communicating to Windows JBoss Server](#)
- [Issues in Accessing Server](#)
- [Issues in Config Fetch](#)
- [Issues in Certificate Discovery](#)
- [Issues in CSR generation](#)
- [Issues in Push and Rollback](#)

Issues in Windows JBoss Server Addition using AppViewX UI

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. From the icon list at the top right corner, click **Add**.
The **Device Addition** page is displayed.
6. From the **Device Details Section** on the left, click **JBoss**.
7. Select **Windows** as **Operating System Type**.
8. Fill in the appropriate details.
9. Click **Add**.

Device :: Server > Add

Vendors

- APACHE Linux
- Microsoft IIS
- Microsoft PC
- Microsoft Server
- APACHE Microsoft
- Microsoft SQL
- ORACLE
- IBM
- hp
- DELL
- Linux
- ARBOR
- JBoss
- N
- hBabbitMQ

Server details

* Operating system type ☐ Linux ☒ Windows

* Server name

* Hostname

Communication mode ☒ Gateway ☐ SSM

Data center

Cert sync ☒ Managed ☐ Monitored ☐ Ignored

Credentials

* Credential type

* Username

* Password

Vendor Specific Details

* Installation directory path

Windows gateway details

* Gateway type ☒ PowerShell ☐ WMI

Device :: Server > Add

Vendors

- APACHE Linux
- Microsoft IIS
- Microsoft PC
- Microsoft Server
- APACHE Microsoft
- Microsoft SQL
- ORACLE
- IBM
- hp
- DELL
- Linux
- ARBOR
- JBoss
- N
- hBabbitMQ

Server details

* Operating system type ☐ Linux ☒ Windows

* Server name

* Hostname

Communication mode ☒ Gateway ☐ SSM

Data center

Cert sync ☒ Managed ☐ Monitored ☐ Ignored

Credentials

* Credential type

* Username

* Password

Vendor Specific Details

* Installation directory path

Windows gateway details

* Gateway type ☒ PowerShell ☐ WMI

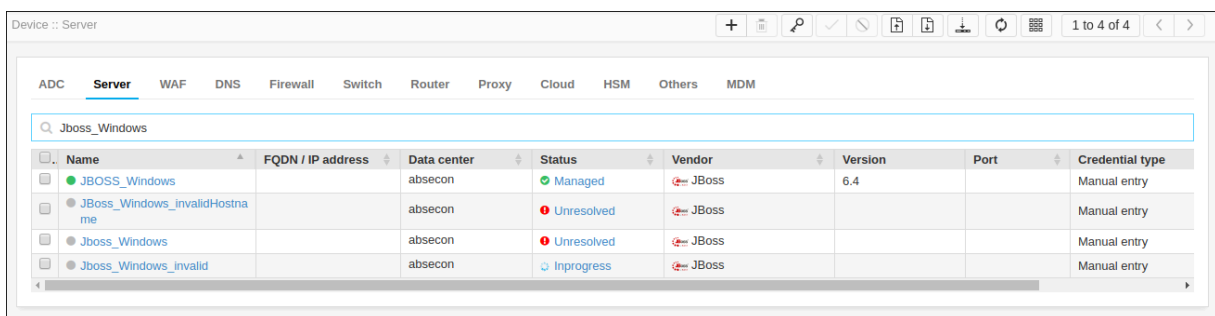
- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

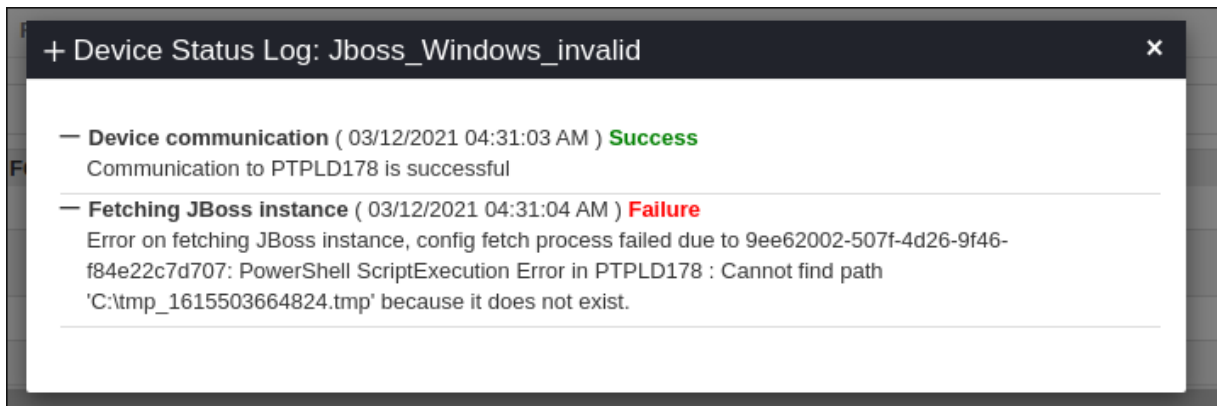
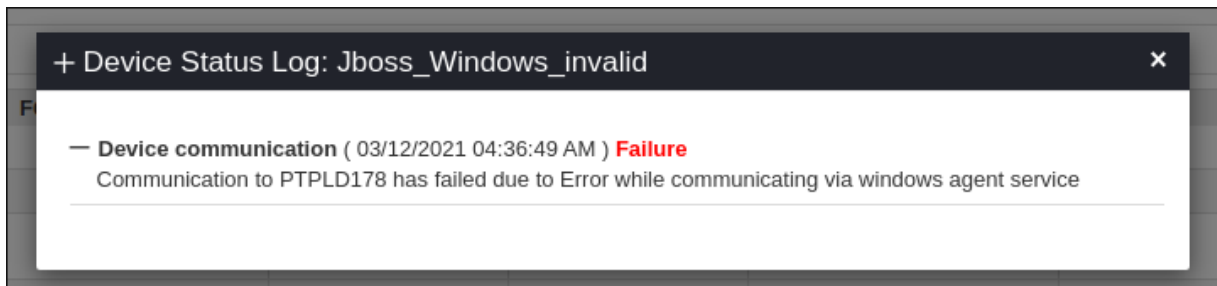
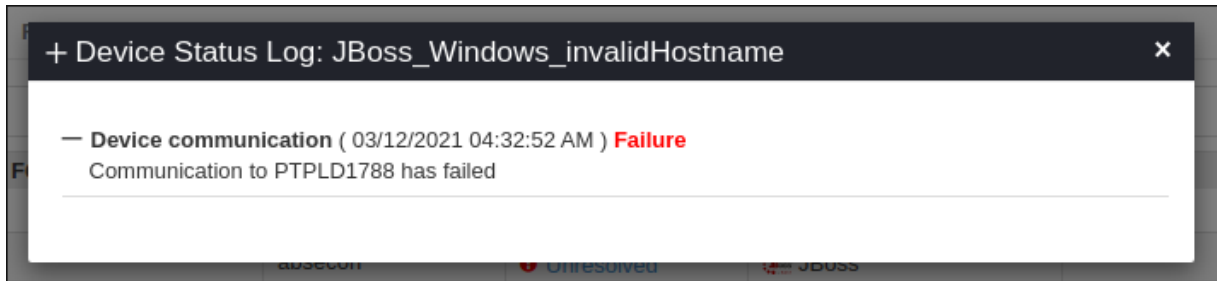
Issues in Communicating to Windows JBoss Server

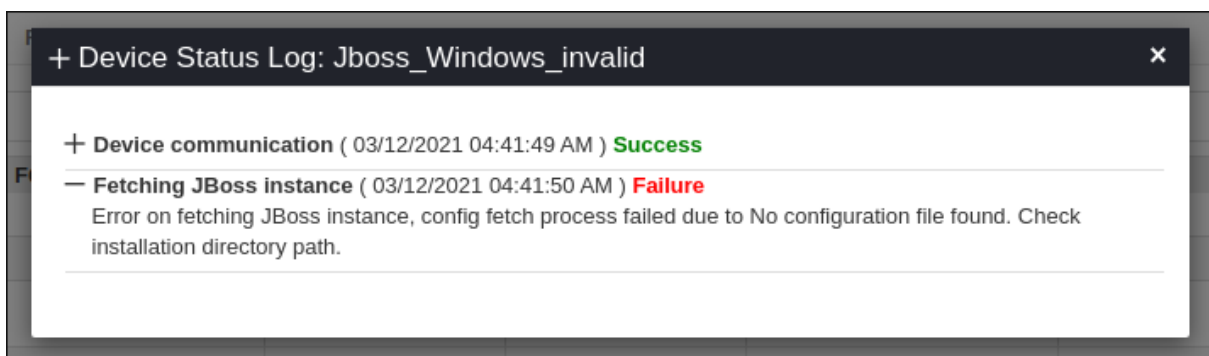
1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**.
The **Device Communication Status** is displayed.



The screenshot shows the 'Device :: Server' page in the AppViewX application. The interface includes a top navigation bar with tabs for ADC, Server (selected), WAF, DNS, Firewall, Switch, Router, Proxy, Cloud, HSM, Others, and MDM. Below the navigation bar is a search bar containing 'Jboss_Windows'. A table displays the status of four JBoss devices:

Name	FQDN / IP address	Data center	Status	Vendor	Version	Port	Credential type
JBOSS_Windows		absecon	Managed	JBoss	6.4		Manual entry
JBoss_Windows_invalidHostna me		absecon	Unresolved	JBoss			Manual entry
Jboss_Windows		absecon	Unresolved	JBoss			Manual entry
Jboss_Windows_invalid		absecon	Inprogress	JBoss			Manual entry





- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-', '_', '.', '*', ' ', '!' and spaces.
Communication to <hostname> has failed	Hostname / Username / Password of the device added might be wrong.	Click on the device name in the Inventory Page. Update the correct details and click Save.
Communication to <Hostname> has failed due to Error while communicating via windows agent service	Windows agent provided is not reachable	Check Windows agent is Up and running and update the valid agent in the device addition page.
Error on fetching JBoss instance, config fetch process failed due to No configuration file found. Check installation directory path.	Provided installation directory path does not have JBoss configuration files	Login manually into the windows server and find the installation directory path which has the JBoss configuration files (server.xml or standalone.xml) and provide the same directory path in JBoss device addition page.

Error Message	Possible Cause	Possible Solution
	like server.xml / standalone.xml	
Error on fetching JBoss instance, config fetch process failed due to df9cbf67-e1af-4d8c-8a7c-fe88bb83e0b3: PowerShell ScriptExecution Error in PTPLD178 : Cannot find path 'C:\tmp_1615504487924.tmp' because it does not exist.	Invalid installation directory path	Login manually into the windows server and find the installation directory path which has the JBoss configuration files (server.xml or standalone.xml) and provide the same directory path in JBoss device addition page.
JBoss version fetch is failed	No JBoss server running in the target device / something wrong in the JBoss installation	Login manually into the windows server and find the JBoss server bin directory and run the below command to validate the JBoss version For JBoss 4.0.5 <pre><JBoss_server_Directory>/bin/run.bat -V</pre> For JBoss 6.4 and 7.0 <pre><JBoss_server_Directory>/bin/standalone.bat -V</pre> Currently only JBoss 4.0.5, 6.4 and 7.0 versions are supported in AppViewX.

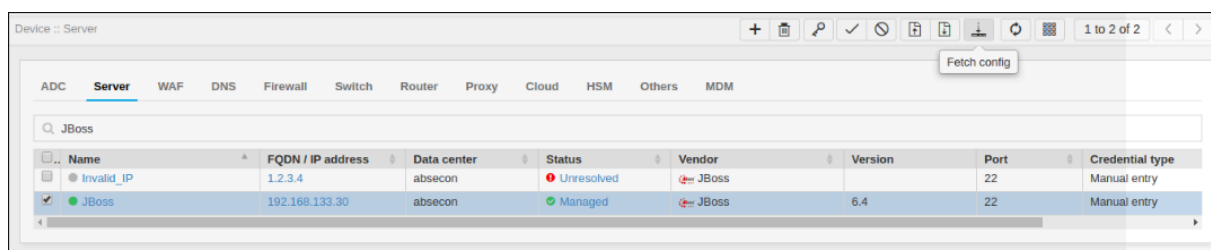
Issues in Accessing Server

Access Issues might be reproduced when communicating with servers while discovering or fetching configuration files. These errors can be collected either from logs, API responses, or in the status field for the particular server.

Error Message	Possible Cause	Possible Solution
Permission denied for file/location.	1. File might not be present in the environment. 2. User might not have permission to read in the given source location. 3. Device communication might not be established when service has started.	1. Check whether someone deleted the file from the environment. 2. Verify if read permission is given for the location. 3. Verify the device connection and restart the service.

Issues in Config Fetch

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Fetch Config**.



• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Communication to <hostname> has failed	Hostname / Username / Password of the device added might be wrong.	1. Verify the input details and check device status error messages Issues in Communicating to Windows JBoss Server

Issues in Certificate Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.

Error Message	Possible Cause	Possible Solution
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.

Issues in CSR generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab.
The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, click correct **Category**.
7. From the **Vendor** dropdown, click **JBoss**.

A list of devices will be generated in the **Devices** dropdown.

appviewX

CERT+

Search features

DASHBOARD

CERTIFICATE ACTION

- Enroll Certificate
- Renew Certificate
- Push to Device
- Reissue Certificate
- Revoke Certificate
- more

CERTIFICATE INVENTORY

- Server
- Client
- Code Signing Certificate
- Device

Enroll Server Certificate

* CSR Generation ☐ AppViewX ☐ Upload CSR ☐ HSM
☒ End Point

Category

Vendor

* Devices

* CSR file name .csr

* Key File Name .key

CSR Parameters

* Common Name

Subject Alternative Name

DNS ⓘ
0 value

Organization

- [Error Messages](#)

Error Messages

Error Message	Possible Cause	Possible Solution
Problem while generating csr on target server	General Failure - SSH/SFTP communication failure	Provide correct credentials and make sure device communication is successful.
Invalid key type specified in the request	Given key type might not be supported by open SSL in the target machine.	Provide valid key type.
Problem while generating csr on the target server.	Location might not have permission.	Check the permission and provide it.
CSR and Private key has been failed	Open SSL configuration might be wrong in the target machine.	Check and correct open SSL configuration in the device.
CSR generation got failed	User has restricted access to the path configured for the "CSR FileName" and "Key File name"	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issues in Push and Rollback

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**.
The **Server Certificate** page is displayed.
4. Click any **JBoss server**.
A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, select **Add App Connector**.
6. Push the certificate to the device.

CERT+

Search features

Revoke Certificate

CERTIFICATE INVENTORY

Server

Client

Code Signing Certificate

Device

Intermediate

AUTOMATION

My Workflows

My Requests

Server Certificate > cert.test.com > View Work order Status

Request View

Workorder View

Search...

Push and Bind Requ...

Review

Implement

Pre Push Script Exec...

Backup Task

Push Task

Push Task

Certificate push failed

Logs - Push Task

1 02/25/2021 11:57:54 - Initiating Push Task

2 02/25/2021 11:58:57 - Certificate Push Failed

3 02/25/2021 11:58:58 - Push Task Failed

4

CERT+

Search features

Revoke Certificate

CERTIFICATE INVENTORY

Server

Client

Code Signing Certificate

Device

Intermediate

AUTOMATION

My Workflows

My Requests

Server Certificate > cert.test.com > View Work order Status

Request View

Workorder View

Search...

Push and Bind Requ...

Review

Implement

Pre Push Script Exec...

Backup Task

Push Task

Push Task

Certificate push failed

Logs - Push Task

1 02/25/2021 12:07:34 - Initiating Push Task

2 02/25/2021 12:07:37 - PrivateKey in device push invalid

3 02/25/2021 12:07:37 - Push Task Failed

4

Copyright © 2022 AppViewX, Inc. All Rights Reserved.

537

Server Certificate > Jboss.nov16.avx.xom > View Work order Status

Request View Workorder View

Search...

Push and Bind Reque...
Review
Implement
Pre Push Script Exec...
Backup Task
Push Task

Push Task
Certificate push failed

Logs - Push Task

```

1 03/12/2021 23:54:46 - Initiating Push Task
2 03/12/2021 23:54:52 - Certificate push failed due to Unable to perform Javascript transformation
3 03/12/2021 23:54:52 - Push Task Failed
4

```

Server Certificate > Jboss.nov16.avx.xom > View Work order Status

Request View Workorder View

Search...

Push and Bind Request Form
Review
Implement
Pre Push Script Execution
Backup Task
Push Task

Push Task
Certificate push failed

Logs - Push Task

```

1 03/12/2021 23:57:06 - Initiating Push Task
2 03/12/2021 23:57:19 - Certificate push failed due to Private key In device configured. But key content is available with the certificate from appview pus
3 03/12/2021 23:57:19 - Push Task Failed
4

```

• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.

Error Message	Possible Cause	Possible Solution
Certificate Push failed	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/write access to the path configured in application connector to certificate push.
Certificate push failed due to Private key In device configured. But key content is available with the certificate from appview pushRequest So failing push request.	“Private key in Device” is enabled in application connector and also private key is available in the certificate	Ensure to uncheck “Private key in Device” attribute in application connector
PrivateKey in device push invalid	“Private key in Device” is enabled in application connector, but key is not available in device.	Ensure to enable “Private key in Device” attribute in application connector, if the certificate does not have the key and the certificate is generated using CSR gen option from Device.

Troubleshooting Windows Weblogic Server

- [Overview](#)
- [Issues in Windows Weblogic](#)

Overview

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with Windows Weblogic server.

Issues in Windows Weblogic

- [Issues in Device communication](#)
- [Issue in Discovery](#)

- [Issues in CSR generation at Endpoint](#)
- [Issues in Certificate Push](#)

Issues in Device communication

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**.
The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the **Windows Weblogic Device**, click **Status**.
The **Device Communication Status** is displayed.

ADC	Server	WAF	DNS	Firewall	Switch	Router	Proxy	Cloud	HSM	Others	MDM

Weblogic_Windows							
Name	FQDN / IP address	Data center	Status	Vendor	Version	Port	Credential type
Weblogic_Windows		absecon	Unresolved	Windows Weblogic			Manual entry

+ Device Status Log: webloigc-invalid ×

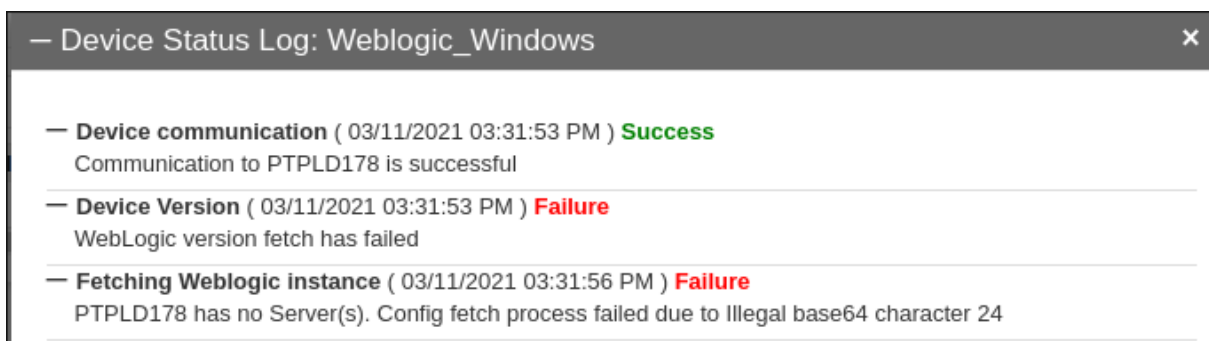
— **Device communication** (03/11/2021 03:47:57 PM) **Failure**

Communication to PTPLD12345 has failed

+ Device Status Log: Weblogic_Windows ×

— **Device communication** (03/11/2021 03:35:20 PM) **Failure**

Communication to PTPLD178 has failed due to Error while communicating via windows agent service



• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Device communication failed	1. The given credential is incorrect. 2. Device not reachable 3. Hostname value is incorrect	1. Check and input the correct credential. 2. Check and input the correct hostname value 3. Ensure the device is reachable
Error while communicating via windows agent service	Windows agent not reachable	Ensure windows agent is running and it's accessible
Version fetch failed and Fetch weblogic instance failed	Given "Weblogic Installation directory" is in-correct	Check and ensure the given installation path is correct

Issue in Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.



Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

ADC	Server	WAF	DNS	Firewall	Switch	Router	Proxy	Cloud	HSM	Others	MDM
weblogic-win											
☐	Name	FQDN / IP address	Data center	Status	Vendor	Version	Port	Credential type			
☒	weblogic-win		absecon	Managed	Windows Weblogic	WebLogic Server 1...		Manual entry			

Search...			
Title	Status	Message	Time
Certificate Discovery	Failed	Received failed response for the batch	02/25/2021 18:12:05
OK			

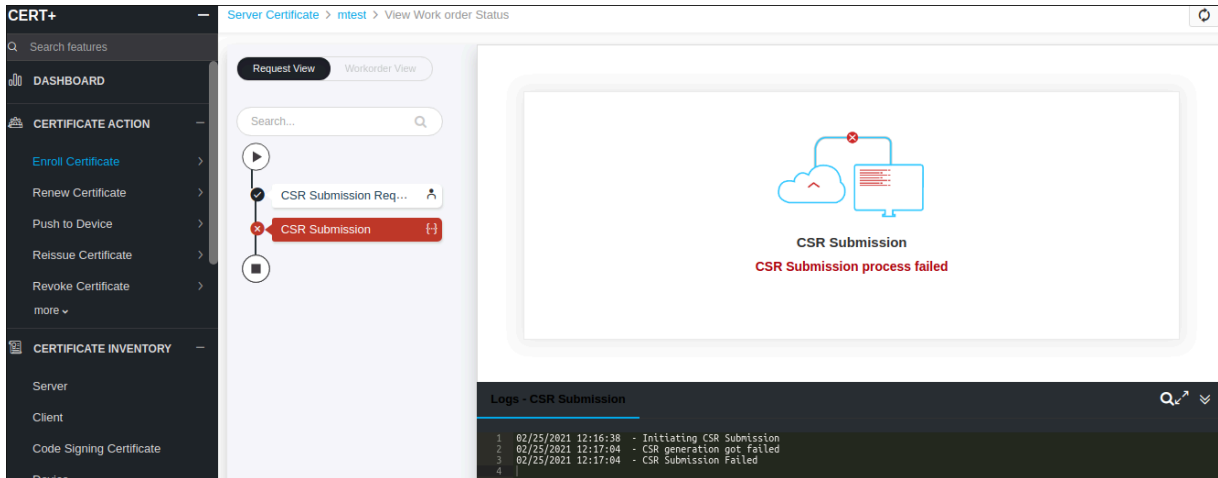
• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
Received failed response from batch	1. Device not running or not accessible 2. No valid certificates available	1. Ensure target device is up and running 2. Check the device has valid certificate files

Issues in CSR generation at Endpoint

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab.
The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, click correct **Category**.
7. From the **Vendor** dropdown, click **Windows Weblogic**.
A list of devices will be generated in the **Devices** dropdown.



• Error Messages

Error Messages

Error Message	Possible Cause	Possible Solution
CSR generation got failed/User has no permission for the given location to perform the operation.	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	1. Kindly ensure the user configured for device addition has read/write access to the path configured.

Issues in Certificate Push

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
3. From the left pane, expand **Certificate Inventory** and click **Server**.
The **Server Certificate** page is displayed.
4. Click any **Windows Weblogic** server.
A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, select **Add App Connector**.
6. Push the certificate to the device.

Troubleshooting Server, Firewalls, WAF, and Rapid SB Connectors

CERT+ Server Certificate > gs-cucm-pe1.lab.appviewx.net > View Work order Status

Request View Workorder View

Search...

Push and Bind Reque...
Review
Implement
Pre Push Script Exec...
Backup Task
Push Task

Push Task
Certificate push failed

Logs - Push Task

```
1 03/11/2021 16:20:30 - Initiating Push Task
2 03/11/2021 16:20:38 - Private key is not available. Failing the push
3 03/11/2021 16:20:38 - Push Task Failed
4
```

CERT+ Server Certificate > WeblogicPushRollback.appviewx.comYT3SV > View Work order Status

Request View Workorder View

Search...

Push Without Bind Re...
Review
Implement
Pre Push Script Exec...
Push Task

Push Task
Certificate push failed

Logs - Push Task

```
1 03/11/2021 16:17:32 - Initiating Push Task
2 03/11/2021 16:17:41 - Private key in device configured. But key content is available with the certificate from appview pushRequest
3 03/11/2021 16:17:41 - Push Task Failed
4
```

CERT+ Server Certificate > gs-cucm-pe1.lab.appviewx.net > View Work order Status

Request View Workorder View

Search...

Push and Bind Reque...
Review
Implement
Pre Push Script Exec...
Backup Task
Push Task

Push Task
Certificate push failed

Logs - Push Task

```
1 03/11/2021 16:23:48 - Initiating Push Task
2 03/11/2021 16:24:04 - Private key is not available in device. Failing the push
3 03/11/2021 16:24:04 - Push Task Failed
4
```

The screenshot shows the AppViewX web interface. The left sidebar contains a navigation menu with sections: CERT+, DASHBOARD, CERTIFICATE ACTION, and CERTIFICATE INVENTORY. The main content area displays a workflow for a 'Server Certificate' under the 'ApacheWinPush.appviewx.com/VOG5E' context. The workflow steps are: Push Without Bind Re..., Review, Implement, Pre Push Script Exec..., and Push Task. The 'Push Task' step is highlighted in red, indicating a failure. The right panel shows a diagram of a cloud connected to a server with a red 'X' over the connection, and the text 'Push Task Certificate push failed'. Below this, a log window titled 'Logs - Push Task' shows the following entries:

```

1 03/09/2021 12:04:36 - Initiating Push Task
2 03/09/2021 12:04:44 - Push failed since cannot write-into/create location(s) [root/, root/]
3 03/09/2021 12:04:44 - Push Task Failed
4

```

The screenshot shows the AppViewX web interface, similar to the one above. The workflow steps are the same, but the 'Pre Push Script Exec...' step is highlighted in red, indicating a failure. The right panel shows a diagram of a cloud connected to a server with a red 'X' over the connection, and the text 'Pre Push Script Execution Pre push script execution failed'. Below this, a log window titled 'Logs - Pre Push Script Execution' shows the following entries:

```

1 03/09/2021 12:02:01 - Initiating Pre Push Script Execution
2 03/09/2021 12:02:03 - Device is not in managed state
3 03/09/2021 12:02:03 - Pre Push Script Execution Failed
4

```

• Error Mesages

Error Messages

Error Message	Possible Cause	Possible Solution
Private key is not available. Failing the push	Private key not available in push request certificate	Please ensure the private key is available in request
Private key In device configured. But key content is available with the certificate from appview pushRequest So failing push request.	Trying to push a certificate with key when the "Private key in device" enabled	Ensure the push certificate has no key when "Private key in device" is enabled.
Private key is not available in device. Failing the push	Private key file not available in the given key location when "Private key in device" is enabled	Ensure the target device has key file in the given location
Push failed since cannot write-into/create location(s)	User does not have permission to perform the operation	1.Ensure the user has permission. 2.For sudo user, please check the access elevation value given in device addition
Device is not in managed state	Device is not available in managed	Please check the device status in device inventory

Chapter 6: Glossary

This table describes common terms used in this guide.

Terms	Definition
JSON	JSON stands for JavaScript Object Notation. JSON is a lightweight format used for storing and transporting data.
EJBCA	Enterprise Java Beans Certificate Authority.EJBCA covers everything from certificate management, registration and enrollment to certificate validation.
URL	URL stands for Uniform Resource Locator. A URL is nothing more than the address of a given unique resource on the Web.
URI	URI stands for Uniform Resource Identifier, and it's the official name for those things you see all the time on the Web that begin ' http: ' or ' mailto: ', for example http://www.w3.org/ , which is the URI for the home page of the World Wide Web consortium
CA	A certificate authority or certification authority (CA) is an entity that issues digital certificates.
CSR	A certificate signing request (CSR) is one of the first steps towards getting your own SSL/ TLS certificate. Generated on the same server you plan to install the certificate on, the CSR contains information (e.g. common name, organization, country) the Certificate Authority (CA) will use to create your certificate
SCEP	Simple Certificate Enrollment Protocol (SCEP) is an IETF RFC. This enables network users to request their digital certificate electronically and as simply as possible. Supported by most of the network devices.
EST	The Enrollment over Secure Transport or EST is a cryptographic protocol that describes an X. 509 certificate management protocol targeting public key infrastructure (PKI) clients that need to acquire client certificates and associated certificate authority (CA) certificates. EST is described in RFC 7030
ACME	Automatic Certificate Management Environment (ACME) protocol is a communications protocol for automating the certificate enrollment to the CA and is used to provide the certificate on the requesting entity.
IP	The Internet Protocol (IP) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables the working of the internet, and essentially establishes the Internet.

Terms	Definition
CSR - Certificate	A CSR or Certificate Signing request is a block of encoded text that is given to a Certificate Authority when applying for an SSL Certificate. It is usually generated on the server where the certificate will be installed and contains information that will be included in the certificate such as the organization name, common name (domain name), locality, and country.
pfx	A PFX file, also known as PKCS #12, is a single, password-protected certificate archive that contains the entire certificate chain plus the matching private key. Essentially it is everything that any server will need to import a certificate and private key from a single file.
pkcs	PKCS stands for "Public Key Cryptography Standards". These are a group of public-key cryptography standards devised and published by RSA
DNS	DNS, or the Domain Name System, translates human-readable domain names to machine-readable IP addresses.
AWS	Amazon Web Services (AWS) is a secure cloud services platform, offering compute power, database storage, content delivery and other functionality to help businesses scale and grow. In simple words AWS allows you to Run web and application servers in the cloud to host dynamic websites.
GCP	Google Cloud Platform (GCP), offered by Google (company), is a suite of cloud computing services that runs on the same infrastructure that Google uses internally for its end-user products, such as Google Search, Gmail, file storage, and YouTube.
IAM	Identity management, also known as identity and access management, is a framework of policies and technologies for ensuring that the proper people in an enterprise have the appropriate access to technology resources.
ACM	AWS Certificate Manager
CA	A certificate authority or certification authority (CA) is an entity that issues digital certificates.
UI	User Interface - The user interface (UI) is the point of human-computer interaction and communication in a device. This can include display screens, keyboards, a mouse and the appearance of a desktop. It is also the way through which a user interacts with an application or a website.
ELB	ELB supports the load balancing capabilities critical for you to migrate to AWS. ELB is well positioned to load balance both traditional as well as cloud native
Keyvault	Azure Key Vault is a cloud service for securely storing and accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords,

Terms	Definition
	certificates, or cryptographic keys. Key Vault service supports two types of containers: vaults and managed HSM pools.