appviewX

Private Key Generation for Apache (Windows) - Solution Guide

Version: 2020.2.0

Copyright AppViewX, Inc.

External Reference Links

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

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

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

Contact Information

AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: info@appviewx.com

Web: www.appviewx.com

Contents

Preface

Revision History

Revision	Description	Date
1.0	Solution Guide AppViewX v20.2.0	May 2020

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.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`codeblock`	Indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Chapter 1: Introduction

This document includes the problem statement, solution, configuration of the Apache server, and creation of Certificate Signing Request (CSR) and private key in the Apache server.

Chapter 2: Problem Statement

Users want to enroll a certificate from a third-party certificate authority by securing CSR and private key in the end device. Users want to secure it in the Apache server that is installed in the Amazon AWS cloud environment.

Chapter 3: Solution

Users can secure the private key and CSR in the Apache server by configuring the Apache server in AppViewX.

Chapter 4: Prerequisites

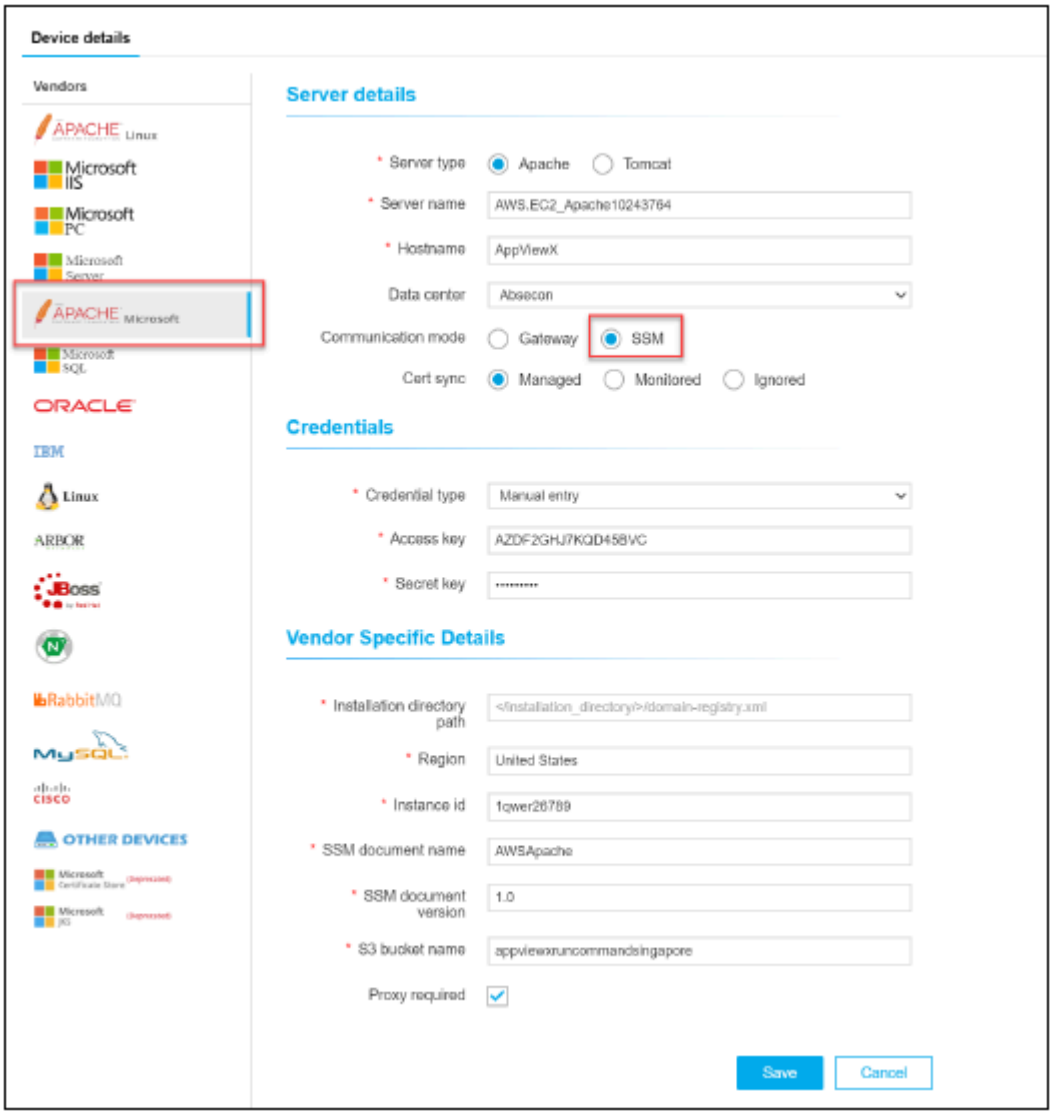
- SSM agents should be running in the Apache server.
- Configure the Apache server in AppViewX.

> **Note:** For information on SSM agents, refer to SSM agents.

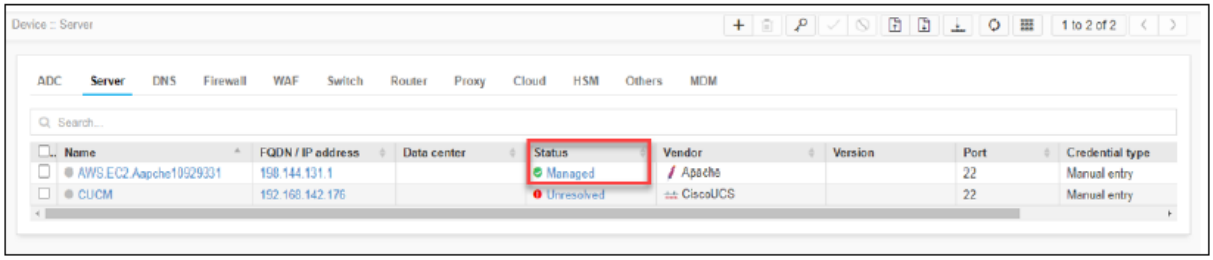
Configure the Apache Server

To configure the Apache server in AppViewX,

1. Log in to the AppViewX application with valid credentials.
2. Click the menu button.
3. Select **Inventory > Device**.
4. By default, the **Server** tab is selected or click **Server**.
5. On the Server list view page, click **+** icon on the top.
6. On the Server details page, select **Apache Microsoft** from the **Vendors** pane on the left.
7. Under the **Server Details** section, select the **Server Type** as **Apache**.
8. Enter the **Server Name, Hostname,** and **Data Center**.
9. Select the **Communication Mode** as **SSM** and **Cert Sync** as **Managed**.
10. Under the **Credentials** section, select the **Credential Type** as **Manual Entry**.
11. Enter the **Access Key** and **Secret Key**.
12. Under the **Vendor Specific Details** section, enter the **Installation Directory Path**.
13. Enter the Region, Instance ID, SSM Document Name, SSM Document Version, and S3 Bucket Name.
14. Select the **Proxy Required** checkbox to communicate through the default proxy configured in **General Settings**.



15. Click **Save**.
16. After configuration, the server is added to the server inventory with the status **Managed**.

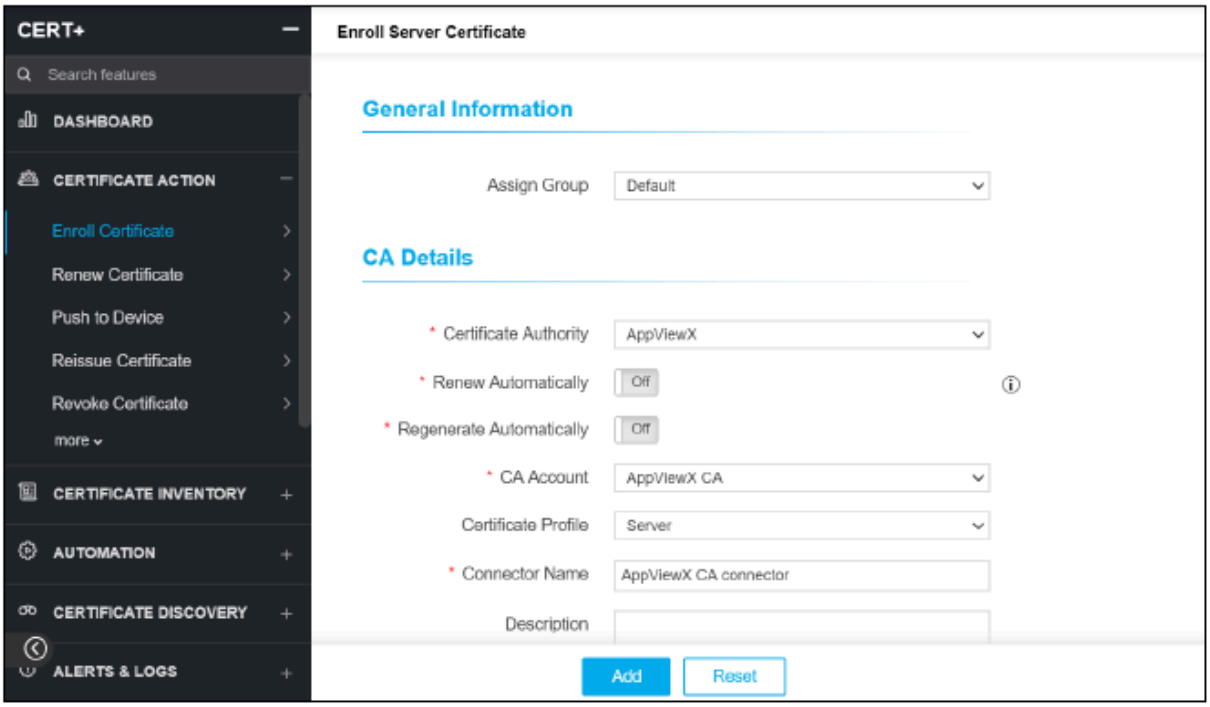


Chapter 5: Generate CSR and Private Key in the Apache Server

After you configure the Apache server in AppViewX, you can generate the CSR and private key in the Apache server. To generate,

1. Click the menu button.
2. Select **CERT+ > Certificate Action > Enroll Certificate > Server**.
3. On the **Enroll Server** Certificate details page, under the **General Information** section, select the respective group from the **Assign Group** dropdown list.

> **Note:** To create a certificate group, refer to Create a Certificate Group.

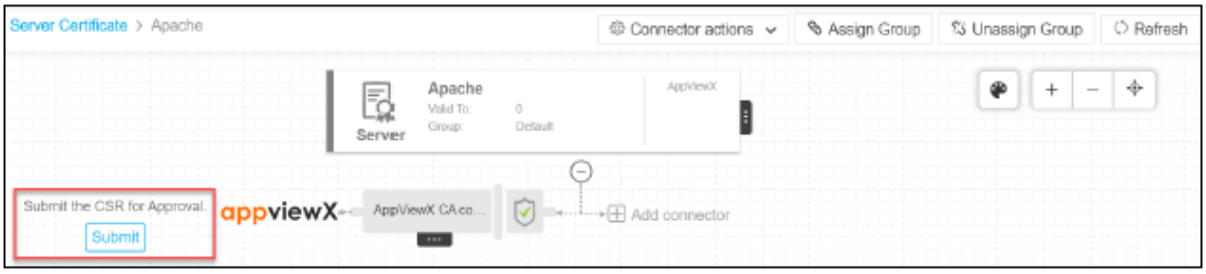


4. Under the **CA Details** section, select the **Certificate Authority, CA Account,** and **Certificate Profile** from the respective dropdown list.

> **Note:** To configure a Certificate Authority, refer to Create a Certificate Authority.

5. Enter the CA connector name and description in the **Connector Name** and **Description** fields respectively.
6. Select the **CSR Generation** mode as **End Point** to generate CSR and private key in the end device.

7. Select **Server** from the **Category** dropdown list and **Apache** from the **Vendor** dropdown list.
8. Select the respective device from the **Devices** dropdown list. Servers added in the server inventory are listed under devices.
9. Enter the **CSR File Name** and **Key File Name**.
10. Under the **CSR Parameters** section, enter the **Common Name** and fill all other required fields.
11. Click **Add** to generate the certificate. The certificate holistic view with the newly created CSR appears.

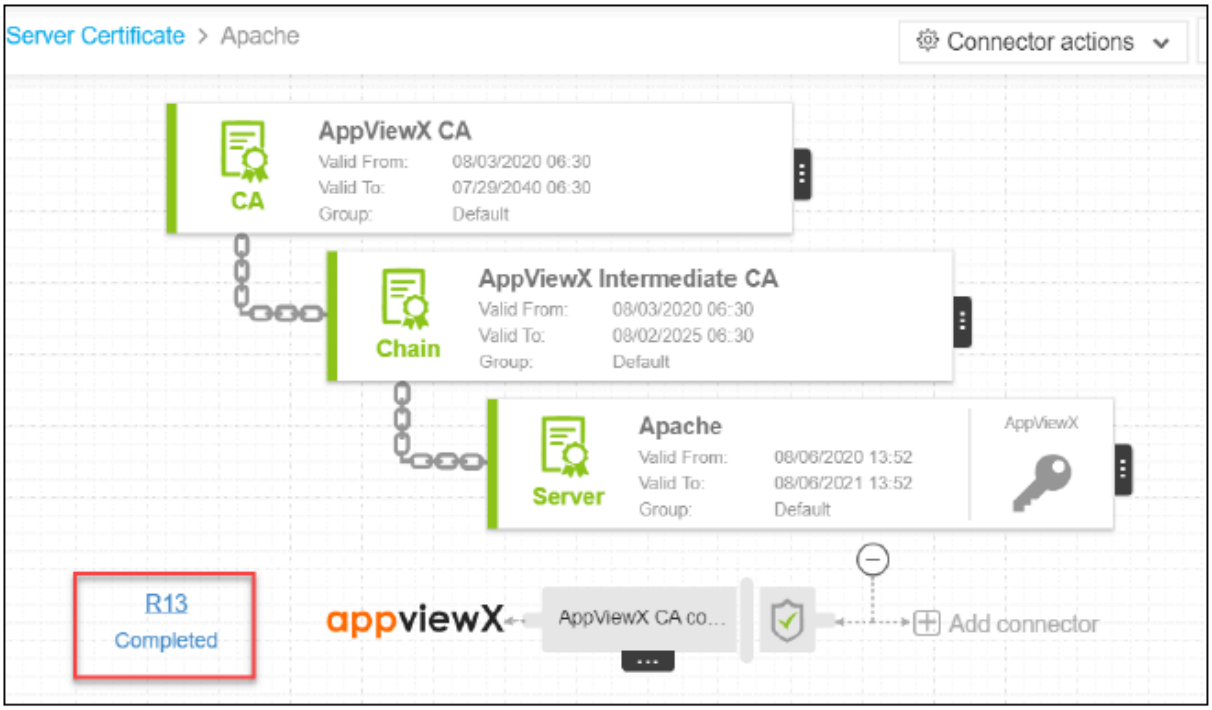


12. On the certificate topology, click **Submit**.
13. On the **Submit** dialog box, enter relevant comments and click **Yes**.
14. The work order status **In Progress** is displayed beside the connector on the topological view. Click **Refresh** on the top-right until the **Approve** button appears on the topology.

15. Click **Approve**.
16. On the **Approve** dialog box:
    - Turn **On** or **Off** the **Manual Implementation**.
    - Select the **Implementation Time**.
    - Enter comments to approve the CSR and click **Yes**.
17. Click **Refresh** on the top-right until the **Implement** button appears on the topology.

18. Click **Implement**.

19. On the **Implement** dialog box:
    - Turn **On** or **Off** the **Manual Implementation**.
    - Select the **Implementation Time**.
    - Enter comments to implement the request and click **Yes**.
20. Click **Refresh** on the top-right to refresh the topology. Refresh the topology until the status updates to **Completed**.



21. To verify the private key and CSR,
    a. Log in to the AWS portal with valid credentials.
    b. Search for the respective Apache server with the Instance ID.
    c. Verify if the CSR and private key are added to the server.

Chapter 6: Limitations

1. Supported bit type is RSA.
2. In RSA bit type, bit-length less than or equal to 4096 is supported.
3. Other bit types such as DSA, EC, and RSA with bit length greater than 4096 are not supported.