appviewX

Connectors - 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 section of the documentation includes the problem statement, solution, implementation of the CUCM Certificate Enrollment and App Connector Configuration, and Cisco Call Manager limitations.

Chapter 2: Problem Statement

Users want to automate the certificate enrollment from a third-party Certificate Authority for Cisco VoIP info - Call manager tool (CUCM) by generating the CSR in the end device. Users expect to automate all the Certificate Lifecycle Management (CLM) actions without any manual intervention.

Chapter 3: Solution

Cisco VoIP info - Call Manager tool (CUCM) is integrated with AppViewX. The user can provide their CUCM details in AppViewX which helps AppViewX to communicate with CUCM. After the CUCM configuration in AppViewX, services running within CUCM are listed on the AppViewX GUI. The user can select the service to enroll a certificate from a third-party Certificate Authority. Similarly, the user can configure the **certificate push** in the app connector that helps users to associate the certificate directly to the selected service. Once the certificate is created, it is automatically pushed to the CUCM. The regenerate option in AppViewX allows the user to regenerate the same certificate when the certificate is about to expire. On successful regeneration of the certificate, AppViewX automatically pushes the certificate to CUCM with the details provided in the app connector.

Chapter 4: Implementation

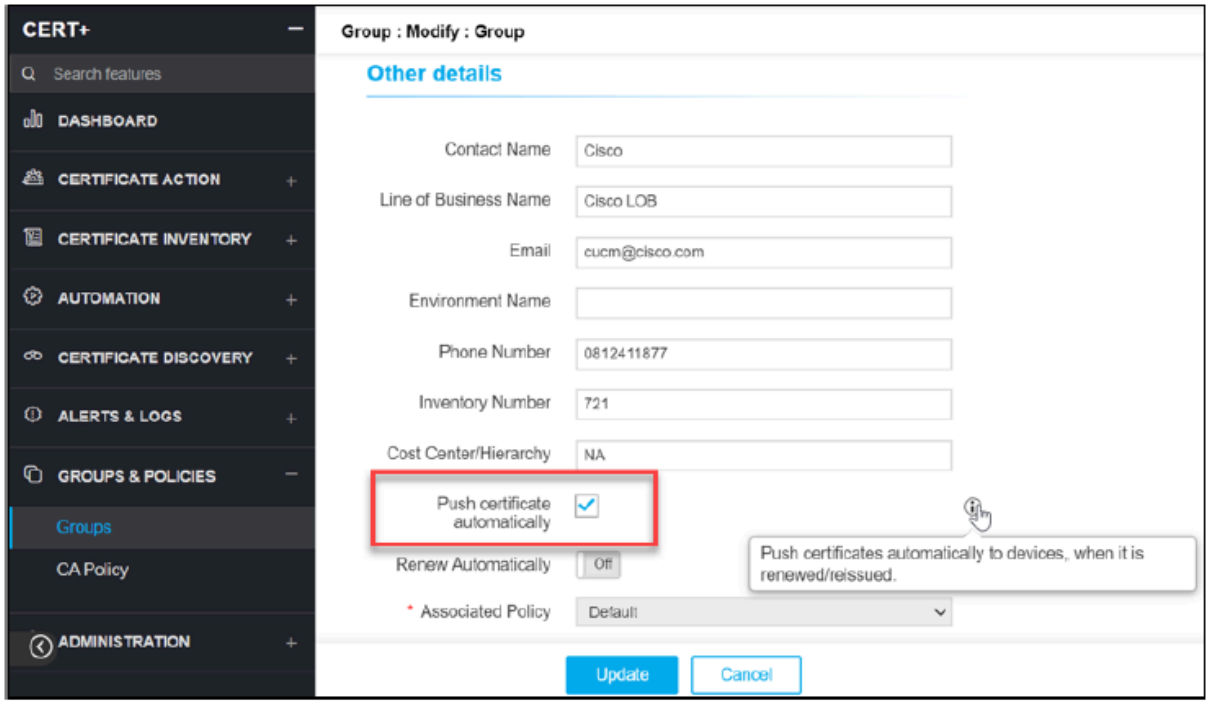
Prerequisites

- Enable the **Push Certificate Automatically** option in the respective group.
- Make sure you have added the Cisco (CUCM) device.

Enabling the Push Certificate Automatically

To enable the push certificate automatically option,

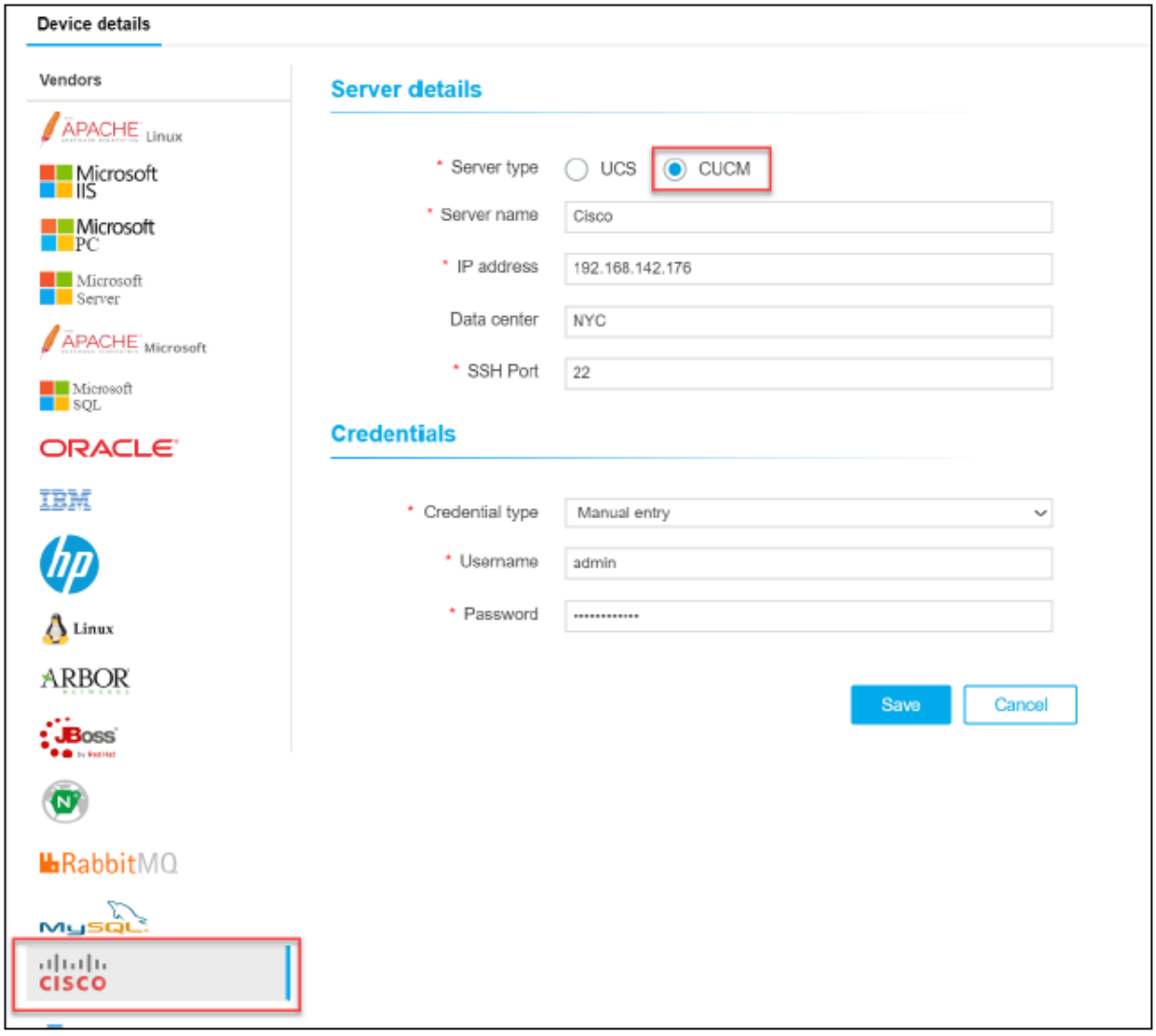
1. Log in to the AppViewX application with valid credentials.
2. Click the menu button.
3. Select **CERT+ > Groups & Policies > Groups**.
4. On the Groups list view page, select the respective group.
5. On the Groups details page, under **Other Details** section, select the **Push Certificate Automatically** checkbox. Enabling this option will push certificates automatically to devices when it is renewed, regenerated, or reissued.
6. Click **Update**.



Adding the CUCM Device

To add the CUCM device in AppViewX,

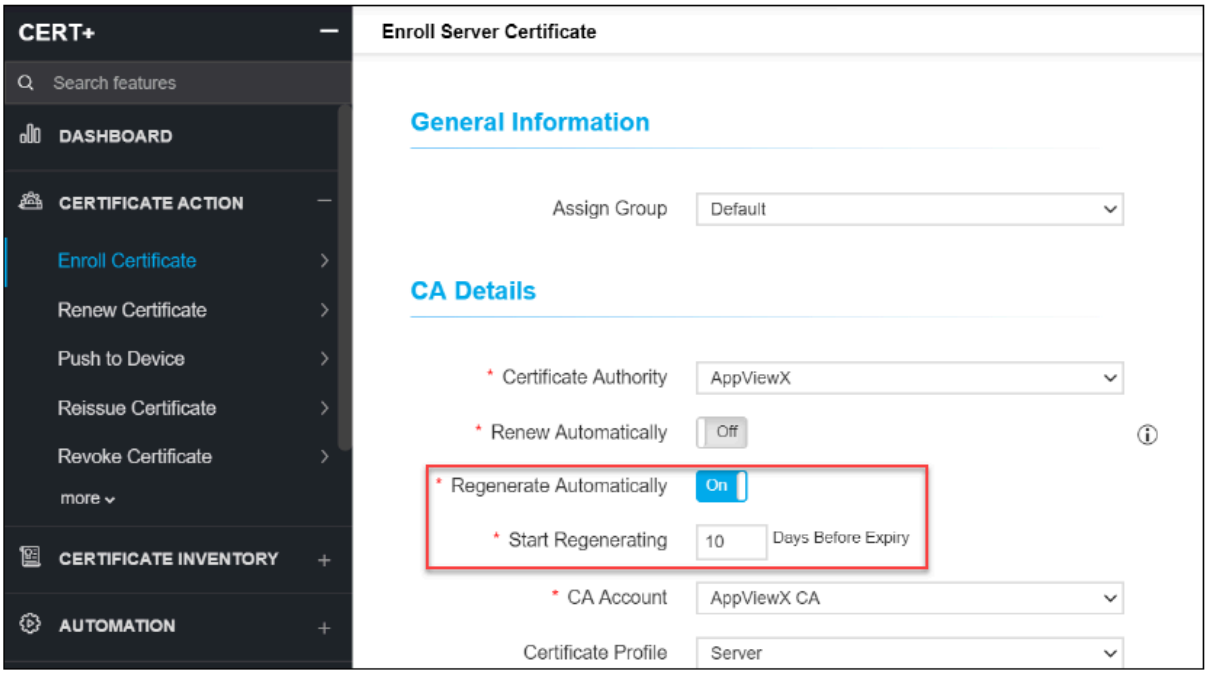
1. Click the menu button.
2. Select **Inventory > Device**.
3. By default, the **Server** tab is selected or click **Server**.
4. On the Server list view page, click **+** icon on the top.
5. On the Server details page, select **Cisco** from the **Vendors** pane on the left.
6. Under the **Server Details** section, select the **Server Type** as **CUCM**.
7. Enter the Server Name, IP Address, and SSH Port number in the respective fields.
8. Under the **Credentials** section, select the **Credential Type** as **Manual Entry**.
9. Enter the **Username** and **Password**.
10. Click **Save**.
11. Post device addition, the device status is marked as **Managed** in the server inventory.



CUCM Certificate Enrollment and Application Connector Configuration

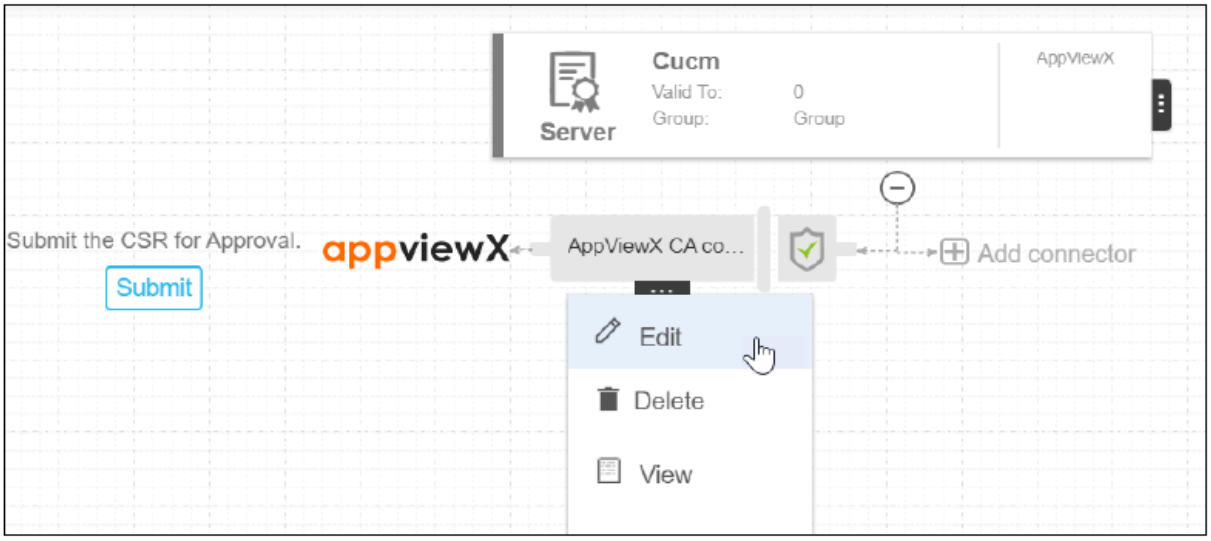
To enroll a certificate and configure an application connector,

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.
4. Under the **CA Details** section, enable the **Regenerate Automatically** toggle and enter the number of days before expiry in the **Start Regenerating** field.



5. Select the **CSR Generation** mode as **End Point**.
6. Select **Server** from the **Category** dropdown list, **Cisco Call Manager** from the **Vendor** dropdown list, and the respective **Service** from the **Service** dropdown list.
7. Based on the service selected, CSR parameters are auto-filled and are non-editable.
8. Click **Add** to generate the certificate. The certificate holistic view with the newly created CSR appears.
9. If you have failed to enable the **Regenerate Automatically** option while creating the certificate, you can enable it from the certificate topology (holistic view).

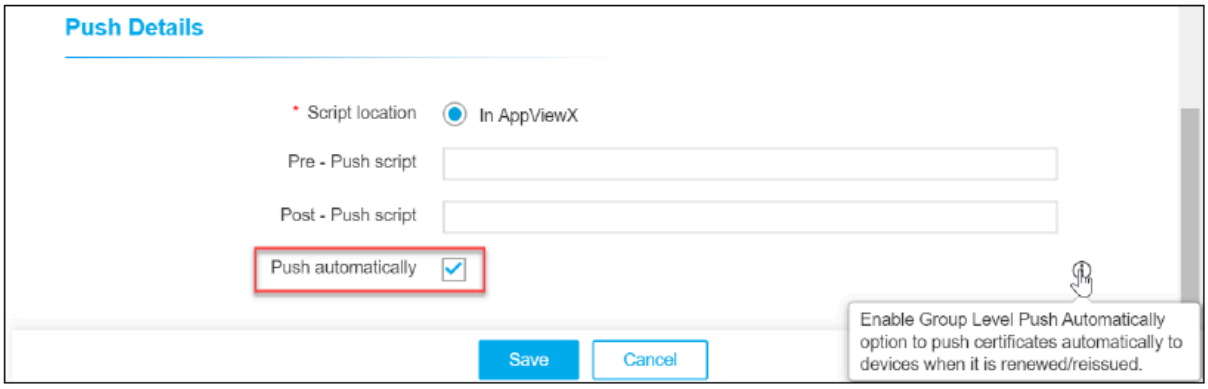
10. Hover over the icon on the CA connector and select **Edit** from the list.



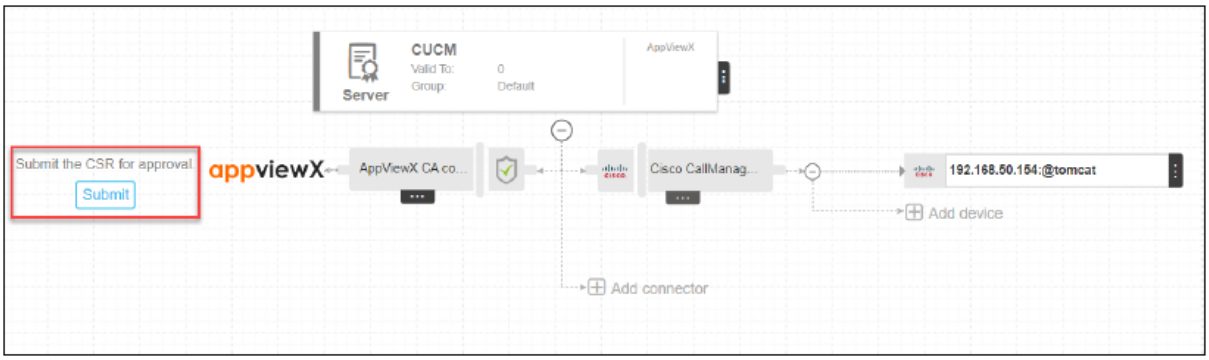
11. On the **Server Certificate** details page, under the **CA Details** section, enable the **Regenerate Automatically** toggle and enter the number of days before expiry in the **Start Regenerating** field.
12. Click **Update** to update the changes.
13. To add a connector, on the certificate topology (holistic view), click **+ Add Connector**.

14. On the **Add Connector** window, under the **General Information** section, select **Server** from the Category dropdown list and **Cisco Call Manager** from the **Vendor** dropdown list.
15. In the **Connector Name** field, enter a name for the connector.
16. Under the **SSL Templates** section, select the device from the **Available Devices** column (select the same device selected for the certificate enrolment).
17. Under the **Certificate Details** section, select the **Certificate Type** from the dropdown list.
18. Under the **Push Details** section, by default, the **Script Location** is selected as **In AppViewX**.

19. Select the **Push Automatically** checkbox.



20. Click **Save** to save the Cisco Call Manager connector and to view it on the certificate topology.
21. On the certificate topology, click **Submit**.

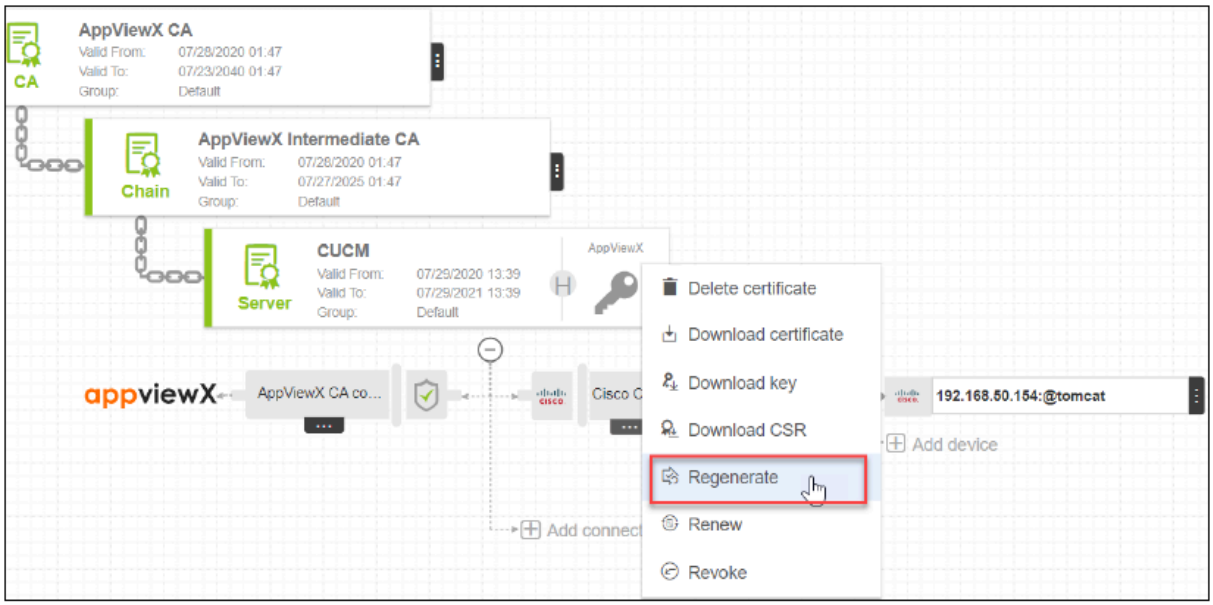


22. On the **Submit** dialog box, enter relevant comments and click **Yes**.
23. The work order status In **Progress** is displayed beside the connector on the topological view. Click Refresh on the top-right until the **Approve** button appears on the topology.
24. Click **Approve**.
25. On the **Approve** dialog box:
    - Turn **On** or **Off** the **Manual Implementation**.
    - Select the **Implementation** Time.
    - Enter comments to approve the CSR and click **Yes**.
26. Click **Refresh** on the top-right until the **Implement** button appears on the topology.
27. Click **Implement**.
28. 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**.

29. Click **Refresh** on the top-right to refresh the topology. Refresh the topology until the status updates to **Push – Completed**.

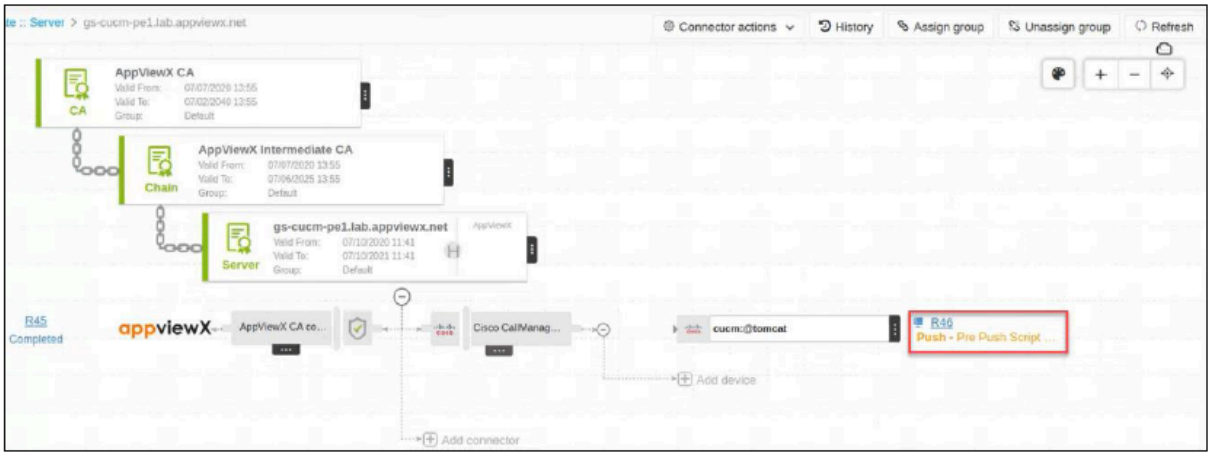
30. You can also regenerate the certificate manually from the certificate topology.

Hover over the ⋮ icon on the certificate and select **Regenerate** from the list.



31. On the Regenerate details page, scroll down to the bottom and click **Regenerate**.
32. On the certificate topology, click **Refresh** on the top-right.

33. Refresh the topology until the status updates to **Push – Pre Push Script Execution In Progress**.



34. Refresh the topology until the status updates to **Push – Push Task In Progress, Push – Post-Push Script Execution In Progress**, and then to **Push – Completed**.

Chapter 5: Cisco Call Manager (CUCM) Limitations

1. AppViewX supports **<.pem>** certificate format. It does not support **<.der>** format due to binary issues and unable to paste in the console.
2. As per the current requirement, the Cisco Tomcat service is supported.
3. Only server certificates are discovered from Cisco Call Manager.
4. When you create a certificate, CSR should be generated from the device. Any external certificates created in AppViewX cannot be pushed to the Cisco Call Manager (CUCM).
5. When you import a certificate to the device, Cisco Call Manager (CUCM) validates the certificate against the CSR parameters and accepts the certificates only when the validation is successful. After the certificate import, CUCM discards the CSR and restricts importing the same certificate into the device again.
6. The service restart command is triggered and AppViewX will wait up to 4 minutes for the restart response from the device. If the time exceeds, AppViewX will close the session with a warning message, Service restart command has been triggered since the maximum timeout has reached, we are closing the connection. Please make sure the service has restarted.