Managing Cross-Origin Resource Sharing in Cisco Unity Connection 10.x

See the following sections:

Overview of Cross-Origin Resource Sharing (CORS)

Unity Connection 10.5 and later releases have extended the support to the client applications of a cross domain server to access content on a Unity Connection server using VMRest APIs.The entry for the cross domain server must pre-exist in Unity Connection to process the CORS requests.

CORS is a specification that allows client applications to process cross-origin requests in a more secure way. Typically for a web application, cross-origin requests from the original domain (where the application originated) to another domain are forbidden by the web browser due to a Single Origin Policy. CORS provide a way for the web browser and server to interact and determine whether or not to allow cross-origin request. CORS standard uses HTTP headers to establish an agreement between the web browser and Unity Connection server to provide services to permitted domains.

Configuring Cross-Origin Resource Sharing (CORS)

To configure Cross-Origin Resource Sharing (CORS) support on Unity Connection server, see the following sections:

Creating New Cross-Origin Resource Sharing (CORS)

To create a new Cross-Origin Resource Sharing (CORS), you need to make the entry of domain of that client application in Unity Connection following the given steps:

Step 1 Log on to Cisco Unity Connection Administration.

Step 2 Navigate to **System Settings> Cross-Origin Resource Sharing (CORS)**. Then select **Add New**.

Note The **Preflight Response Cache Settings** mentioned on Search Cross-Origin Resource Sharing (CORS) page, is by default set to 30 minutes. You can change this value but in case an improper value is entered, the following warning prompts on the screen: **Interval in minutes to do the Preflight check- valid range is 0 (always) to 525949 (once per year).**

Step 3 On the **New Cross-Origin Resource Sharing** page, enter the value of the client application domain in **Domain Name**. This field is mandatory.

Note Make sure the domain name of the client application starts with “http://” or “https://”.

Step 4 Select the **Access Level** operation type for the cross origin domain. By default, the value is **Read Only** but you can also select **Full-Access.**

Step 5 Select **Save**. This creates a Cross-Origin Resource Sharing (CORS) and a success message prompts on the screen: **Created Cross-Origin Resource Sharing (CORS)**.

Modifying Cross-Origin Resource Sharing (CORS)

To modify Cross-Origin Resource Sharing (CORS)

Step 1 In Cisco Unity Connection Administration, navigate to **System Settings> Cross-Origin Resource Sharing**.

Step 2 On the Search Cross-Origin Resource Sharing (CORS) page, select the display name of the client application domain that you want to modify.

Step 3 On the Edit Cross-Origin Resource Sharing (CORS) page, change settings as applicable. (For field information, on the fields on the Edit Cross-Origin Resource Sharing (CORS) page, navigate to **Help> This Page**).

Step 4 Select **Save**.

Deleting Cross-Origin Resource Sharing (CORS)

To delete Cross-Origin Resource Sharing (CORS)

Step 1 In Cisco Unity Connection Administration, navigate to **System Settings> Cross-Origin Resource Sharing**.

Step 2 On the Search Cross-Origin Resource Sharing page, select the check box adjacent to the display name of the domain name of client application that you want to delete.

You may select one or more domain names of client applications that you want to delete.

Step 3 Select **Delete Selected**.