Confidential Access Level Setup

This chapter provides information about using Cisco Unified Communications Manager Administration to configure Confidential Access Levels (CAL).

About Confidential Access Level Setup

In Cisco Unified Communications Manager Administration, use the **Bulk Administration** > **Confidential Access Level** > **Import Confidential Access Level Matrix** menu path to configure CAL. CAL feature is used for restricting calls and other supplementary features such as transfer, forward, conferences including Meet-Me, and so on.

CAL is a numerical value assigned to an entity:

- Device (for example, an IP Phone)
- Line (for example, a Directory Number)
- Trunk (for example, a SIP trunk)

CAL has two main functions:

- Controls call completion based on configuration.
- Displays information on the phone that conveys additional information about the call.

Format of CAL Matrix

The Confidential Access Level (CAL) matrix is an X/Y matrix that is used to compare one CAL to another for implementing a call policy. The CAL from the originating number is selected along the X-axis of the matrix and compared against the destination number along the Y-axis of the matrix. The intersection of these two values is known as the resolved CAL. The resolved CAL determines whether the call should proceed and also the message that is displayed to the users.

A sample CAL matrix is as follows:

Column 1	Column 2	Column 3	Column 4	Column 5
Description	CAL	1	2	3
Unrestricted	1	1	1	1
Restricted	2	1	2	2
Confidential	3	1	2	3
END	Description	Unrestricted	Restricted	Confidential

Important The matrix must be symmetrical. For example, in the sample CAL matrix above, the value at the intersection of CAL 2 and CAL 3 is same as the value at the intersection of CAL 3 and CAL 2. Thus, the resolved CAL in both the cases is 2 (Restricted). Cisco Unified Communications Manager does not validate if the imported matrix is symmetrical. So it is the responsibility of the administrator to configure a matrix that aligns with the desired calling policy.

You can configure different CALs as per the requirement. The following CALs have been configured in this sample matrix:

- 1 - Unrestricted
- 2 - Restricted
- 3 - Confidential

The first row of the CAL matrix must contain all the valid CALs that you want to import into Cisco Unified Communications Manager. Description and CAL values are optional. The CALs in the remaining columns can be any numeric values that you want to import. The subsequent rows define the textual description, as seen in column 1, and its relationship with other CALs in column 3 and the subsequent columns. For every CAL entered in the first row, there should be a resulting row that contains a textual description for that value. In other words, column 1 must contain textual descriptions for all the CALs that are entered in the first row. The last line (END, Description) indicates the end of the CAL matrix. The CALs beyond this row are not imported.

If a call is originated from a number whose CAL is 1 (Unrestricted) to a destination number whose CAL is 2 (Restricted), the resolved CAL is 1 (the intersection of CAL 1 and CAL 2). Hence, the text corresponding to CAL 1—Unrestricted is displayed on both the phones. Similarly, if the call is between a Restricted party (with CAL 2) and a Confidential party (with CAL 3), then Restricted (corresponding to the resolved CAL 2) will be displayed on both the phones. Thus, the CAL matrix resolves to the highest common value possible between all parties of the call.

CAL Enforcement Level

In Cisco Unified Communications Manager 10.0(1), the CAL feature is not configurable on internal Cisco Unified Communications Manager devices that are used in features such as Directed Call Park, Built in Bridges, and so on, and also on a few endpoints such as MGCP BRI devices, Mobility, and CTI based endpoints. If you apply CAL resolution restriction strictly for all the calls, it may result in undesired call failures. Also, applying the CAL restriction without assigning CAL values to all the devices may result in call failures.

To avoid undesired call failures and to facilitate smooth deployment of the CAL feature, the following modes of CAL enforcement are implemented in Cisco Unified Communications Manager Release 10.0(1):

- Strict Mode-in this mode, the CAL Enforcement Level enterprise parameter is set to Strict. If the CAL value is not configured for a device or if a feature that does not support CAL is invoked, the call is allowed.
- Lenient Mode-in this mode, the CAL Enforcement Level enterprise parameter is set to Lenient. Even if the CAL value is not configured for a device or if a feature that does not support CAL is invoked, the call is allowed. However, if CAL values are configured for all the devices and the CAL resolution fails, the call is not allowed.

Note Cisco recommends that you deploy the CAL feature in Lenient mode in Cisco Unified Communications Manager Release 10.0(1).

Note To set the CAL enforcement level, choose **System** > **Enterprise Parameters** and select the CAL enforcement level from the CAL Enforcement Level drop-down list.

Important To ensure that the Lenient mode functions properly, it is highly recommended that you configure appropriate warning text on the 'CAL Resolution Warning Message Text' enterprise parameter. For example, Warn: CAL unknown. The warning text is displayed on the phones whenever the CAL values are not configured but the call is allowed.

CAL Limitations

The following limitations apply to the CAL feature:

- The built-in bridges (BIB) on the phones are not assigned CAL values. In Barge and Monitoring features, where BIBs are used, a warning message is displayed on the phones that use these features. The warning text is displayed based on the warning message that is configured in the CAL Resolution Warning Message Text enterprise parameter.
- Unlike SIP trunks, as the MGCP and H323 devices do not pass the resolved CAL values from one cluster to another, you may see different resolved CAL values on the calling and called entities on the call.
- The CAL feature is not supported on all phone models. To check if CAL is supported on your phone, see the Cisco Unified IP Phone User Guide that is specific to your phone model.
- In Cisco Unified Communications Manager Release 10.0(1), Directed Call Park and Mobility features can work only in Lenient mode.
- Extension Mobility applies only the CAL values that are associated with the lines.
- The calling SIP phones do not display PENDING message until the call is answered even if the CAL header is included in the SIP 180 Ringing message. To overcome this limitation, you can apply a LUA script at the SIP Profile level associated with the phone. The LUA script removes the CAL Header in the SIP 180 ringing message and updates the Remote Party ID to PENDING. An example of a LUA script is provided below. You can apply this script to display PENDING message on the calling phone until the call is answered.

```
M = {}
trace.enable()
function M.outbound_180_INVITE(msg)
local cal =msg:getHeader("Confidential-Access-Level")
if cal then
msg:removeHeader("Confidential-Access-Level")
1
CAL limitations
REVIEW DRAFT - CISCO CONFIDENTIAL
local rpi =msg:getHeaderValues("Remote-Party-ID")
local uri = "\"PENDING\" "
rpi[1] = uri .. string.match(rpi[1], "(<.+)")
msg:modifyHeader("Remote-Party-ID", rpi[1])
msg:addHeader("Remote-Party-ID",rpi[2])
end
end
return M
```

- When you disable Auto Pickup, the 418 Incompatible SIP message is not sent to the phones when CAL resolution fails during the pickup.
- When a phone with the CAL associated with its line receives an INVITE message, where the Directory number in the From header is different from the value configured in the Cisco Unified Communications Manager database for that phone, the Cisco Unified Communications Manager sends a SIP 418 Invalid CAL message to the phone if the CAL feature is enabled. If the CAL feature is disabled, the Cisco Unified Communications Manager retains the original behavior and sends a SIP403 Forbidden message.

Set Up Confidential Access Level

Follow these steps to set up confidential access level:

Procedure

Step 1 Choose **Bulk Administration** > **Confidential Access Level** > **Import Confidential Access Level Matrix**.

The Confidentiality Access Level Matrix Upload window opens.

Step 2 Click **Browse** and select the csv file that you want to upload.

Note The csv file contains the CAL table which is an X/Y matrix used to find the resolved CAL value.

Step 3 Click **Upload.**

Note The Upload button is enabled only for CCM Super Users and Standard Confidential Access Level Users access groups.