



GLOBALCOM®.IP

Topic: Configuring GCK Telephone Extension(s) in Cisco Unified Call Manager v11.0

Background

This document describes the steps necessary to configure Cisco Unified Call Manager (CUCM) version 11.0 in order to interface with AtlasIED GCK version 1.0 or higher running in Extension Mode. In this mode, GCK acts like a series of softphone(s) belonging to CUCM. In Cisco nomenclature, the required device is known as a "Third Party SIP Device (Basic)". GCK is configured independently of CUCM; it does not query CUCM for configuration information. Configuration of GCK is not described in this document. See the GCK System Configuration Console User's Manual for details on how to configure GCK in Extension Mode. Although screenshots provided are for CUCM 11.0, the process is very similar to previous versions of CUCM, if not identical.

This document assumes the following:

- The user has a functioning installation of CUCM.
- CUCM has enough license units available to allow a SIP device to be installed. Contact Cisco for licensing information.

Installation

The process of creating a new SIP Device consists of the following steps:

1. Adding a New Security profile.
2. Adding an End User profile.
3. Adding a New Device.
4. Associating a Device with a User.
5. Testing.

Adding a New Security Profile

To set up a security profile, navigate back to the CUCM Administration page using the dropdown menu in the top right and then follow these steps:

1. Navigate to System > Security > Phone Security Profile to open the Find and List Phone Security Profiles window.
2. Click "Find" to list all of the phone security profiles (Figure 1).

Phone Security Profile (1 - 50 of 158)

Find Phone Security Profile where

Name begins with

Find

Clear Filter

Name

Description

Copy

Analog Phone - Standard SCCP Non-Secure Profile

Carrier-integrated Mobile - Standard SIP Non-Secure Profile

Cisco 12 S - Standard SCCP Non-Secure Profile

Cisco 12 SP - Standard SCCP Non-Secure Profile

Cisco 12 SP PLUS - Standard SCCP Non-Secure Profile

Cisco 30 SP PLUS - Standard SCCP Non-Secure Profile

Cisco 30 VIP - Standard SCCP Non-Secure Profile

Cisco 3905 - Standard SIP Non-Secure Profile

Cisco 3911 - Standard SIP Non-Secure Profile

Cisco 3951 - Standard SIP Non-Secure Profile

Cisco 6901 - Standard SCCP Non-Secure Profile

Cisco 6901 - Standard SIP Non-Secure Profile

Cisco 6911 - Standard SCCP Non-Secure Profile

Cisco 6911 - Standard SIP Non-Secure Profile

Cisco 6921 - Standard SCCP Non-Secure Profile

Cisco 6921 - Standard SIP Non-Secure Profile

Analog Phone - Standard SCCP Non-Secure Profile

Carrier-integrated Mobile - Standard SIP Non-Secure Profile

Cisco 12 S - Standard SCCP Non-Secure Profile

Cisco 12 SP - Standard SCCP Non-Secure Profile

Cisco 12 SP+ - Standard SCCP Non-Secure Profile

Cisco 30 SP+ - Standard SCCP Non-Secure Profile

Cisco 30 VIP - Standard SCCP Non-Secure Profile

Cisco 3905 - Standard SIP Non-Secure Profile

Cisco 3911 - Standard SIP Non-Secure Profile

Cisco 3951 - Standard SIP Non-Secure Profile

Cisco 6901 - Standard SCCP Non-Secure Profile

Cisco 6901 - Standard SIP Non-Secure Profile

Cisco 6911 - Standard SCCP Non-Secure Profile

Cisco 6911 - Standard SIP Non-Secure Profile

Cisco 6921 - Standard SCCP Non-Secure Profile

Cisco 6921 - Standard SIP Non-Secure Profile

Rows per Page 50

Figure 1



9701 Taylorsville Rd. • Louisville, KY U.S.A.
Telephone: 502.267.7436 • Fax: 502.267.9070

3. Scroll down the list and click on “Third-party SIP Device Basic – Standard SIP Non-Secure Profile”.
4. Click “Copy” and you will see the Phone Security Profile Configuration screen (Figure 2).

Phone Security Profile Information

Product Type: Third-party SIP Device (Basic)
Device Protocol: SIP
Name* Third-party SIP Device Basic - Standard SIP Non-Secure Profile
Description Third-party SIP Device (Basic) - Standard SIP Non-Secure Profi
Nonce Validity Time* 600
Transport Type* TCP+UDP
☐ Enable Digest Authentication

Parameters used in Phone

SIP Phone Port* 5060

*- indicates required item.

Figure 2

5. Change the Name (we recommend a name such as “Third-Party SIP Device Basic – Digest”).
6. Change the transport type to UDP.
7. Check the “Enable Digest Authentication” box.
8. Click “Save”.

Adding an End User Profile

Next, you need to add a new end user profile. Follow these steps:

1. Navigate to User Management -> End User.
2. Click “Add New” to bring up the End User Configuration screen (Figure 3).

End User Configuration

User Information

User Status Enabled Local User

User ID* 5555

Password

Confirm Password

Self-Service User ID

PIN

Confirm PIN

Last name* 5555

Middle name

First name

Display name

Title

Directory URI

Telephone Number

Home Number

Mobile Number

Pager Number

Mail ID

Manager User ID

Department

User Locale < None >

Associated PC

Digest Credentials

Confirm Digest Credentials

Figure 3

3. Enter a unique User ID.
4. Enter a Last Name.
5. Enter the digest password in the Digest Credentials box and the Confirm Digest Credentials box.
6. Click “Save”.



9701 Taylorsville Rd. • Louisville, KY U.S.A.
 Telephone: 502.267.7436 • Fax: 502.267.9070

Adding a New Device

Next, you will need to add in the device that you want to set up. Follow these steps:

1. Navigate to Device > Phone.
2. Click "Add New".
3. Select "Third-party SIP Device (Basic)" (Figure 4).

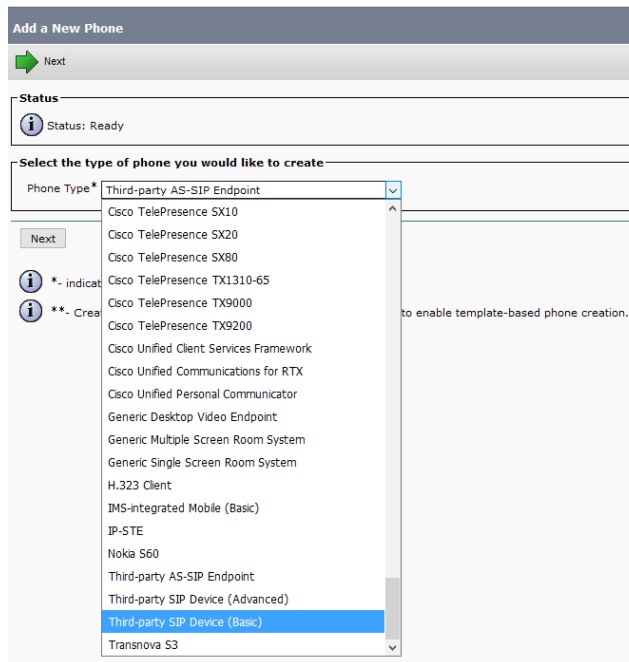


Figure 4

4. Click "Next" to open the Phone Configuration window (Figure 5).

The screenshot displays the 'Device Information' configuration window. It features a warning icon at the top left stating 'Device is not trusted'. The form contains several fields and dropdown menus: 'MAC Address*' (84802D409E25), 'Description' (SEP84802D409E25), 'Device Pool*' (Default), 'Common Device Configuration' (< None >), 'Phone Button Template*' (Third-party SIP Device (Basic)), 'Common Phone Profile*' (Standard Common Phone Profile), 'Calling Search Space' (< None >), 'AAR Calling Search Space' (< None >), 'Media Resource Group List' (< None >), 'Location*' (Hub_None), 'AAR Group' (< None >), 'Device Mobility Mode*' (Default), 'Owner' (User), 'Owner User ID*' (5555), 'Use Trusted Relay Point*' (Default), 'Always Use Prime Line*' (Default), 'Always Use Prime Line for Voice Message*' (Default), and 'Geolocation' (< None >). There are also checkboxes for 'Ignore Presentation Indicators (internal calls only)', 'Logged Into Hunt Group', and 'Remote Device'. 'View Details' links are present next to the 'Device Pool', 'Common Phone Profile', and 'AAR Group' dropdowns.

Figure 5

5. Fill in the MAC address of the device you are adding. This will automatically fill out the description of the device with the device ID.
6. Go to the Device Pool dropdown menu and select "Default".
7. Go to the phone button template dropdown menu and select "Third-party SIP Device (Basic)".
8. Go to the owner user ID dropdown menu and select the user profile that you want to be associated with the device.



9701 Taylorsville Rd. • Louisville, KY U.S.A.
Telephone: 502.267.7436 • Fax: 502.267.9070

9. Go to the Device Security Profile dropdown menu and select the security profile that you wish to use with this device (Figure 6).

Figure 6

10. Go to the SIP profile dropdown menu and select "Standard SIP Profile".
11. Go to the digest user dropdown menu and select the user which was added in the steps above.
12. Click "Save".
13. Click on Line[1] in the association section (Figure 7) which should have appeared in the top-left after clicking save". This will bring up the Directory Number Configuration screen.

Figure 7

14. Fill in the directory number then click save (Figure 8).

Figure 8

15. Click "Apply Config".
16. Click "OK" on the window that pops up.



9701 Taylorsville Rd. • Louisville, KY U.S.A.
Telephone: 502.267.7436 • Fax: 502.267.9070

Associating a Device with a User

Next, you will need to associate the device created above with the user. Follow these steps:

- 1.Navigate to User Management > End User.
- 2.Click “Find” and then click on the user that you wish to associate with a device.
- 3.Go to “Device Information” section and click “Device Association”. (Figure 9)

Device Information

Controlled Devices

SEP28F10E5384C5

Available Profiles

CTI Controlled Device Profiles

Device Association

Line Appearance Association for Presence

Figure 9

- 4.Click Find to list all of the available devices.
- 5.Check the box next to the device you wish to associate with the user (Figure 10), then click “Save Selected/Changes”.

Find User Device Association where

Name

begins with



Find

Clear Filter

+

-

☒ Show the devices already associated with user

		Device Name	Directory Number
<input type="checkbox"/>		SEP28F10E5384C5	5555
<input checked="" type="checkbox"/>		SEP28F10E5384C5	5555
<input type="checkbox"/>		SEP84802D409E25	1111

Select All

Clear All

Select All In Search

Clear All In Search

Save Selected/Changes

Remove All Associated

Figure 10

- 6.Select “Select Back to User”.
- 7.Click “Save”.

Testing

Configure a 3rd party phone to register as extension 1111. Call the phone from a Cisco CUCM phone. Verify two-way audio. Repeat the call from the 3rd party phone to the Cisco phone. Verify two-way audio. If the calls are successful, the same extension will be able to work in GCK.



9701 Taylorsville Rd. • Louisville, KY U.S.A.
Telephone: 502.267.7436 • Fax: 502.267.9070