Secure Cisco IP Phone under CUCM Mixed Mode Cluster

Document ID: 113333

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
Certificate Trust List
How to Secure the IP Phone
Related Information

Introduction

This document describes the step−by−step procedure to move one IP phone in secure mode from a source Cisco Unified Communication Manager (CUCM) cluster to a destination CUCM cluster without any manually manipulation of the Certified Trust List (CTL) file installed on such an IP phone.

Note: This procedure is independent of:

1. Signaling protocol used by the phone. It is assumed that signaling protocol in source and destination cluster remain the same for an specific IP phone.
2. Phone model that excludes Cisco 7940/7960 models because the 7940/7960 phones require the end user intervention to input an authentication string since they do not have a built−in MIC.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the Cisco Unified Communications Manager 7.x.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Certificate Trust List

All servers in the CUCM cluster generates self−signed certificates. The phones get their own certificates, which is of two types.

1. Manufacturing installed certificate given by Cisco when you buy a new phone.
2. Locally significant certificate handed by Cisco Authority Proxy Function.

The CTL is a list of self−signed certificates from all the servers in the CUCM cluster which the phone can trust. The CTL is stored on the TFTP server and sent to the IP phones.

The device, file, and signaling authentication rely on the creation of the CTL file, which is created when you install and configure the Cisco CTL Client on a single Windows workstation or server that has a USB port.

The CTL file contains a server certificate, public key, serial number, signature, issuer name, subject name, server function, DNS name, and IP address for each server. When you configure a firewall in the CTL file, you can secure a Cisco ASA Firewall as part of a secure Cisco Unified Communications Manager system. The Cisco CTL Client displays the firewall certificate as a *CCM* certificate. Cisco Unified Communications Manager Administration uses an eToken to authenticate the TLS connection between the Cisco CTL Client and Cisco CTL Provider.

On CUCM version 8.X and later, the IP phones request a CTL file by default even if this has not been created. The CTL files are not considered essential; they are just part of the new security features that come with the CUCM 8.x. Refer to Configuring the Cisco CTL Client for more information.

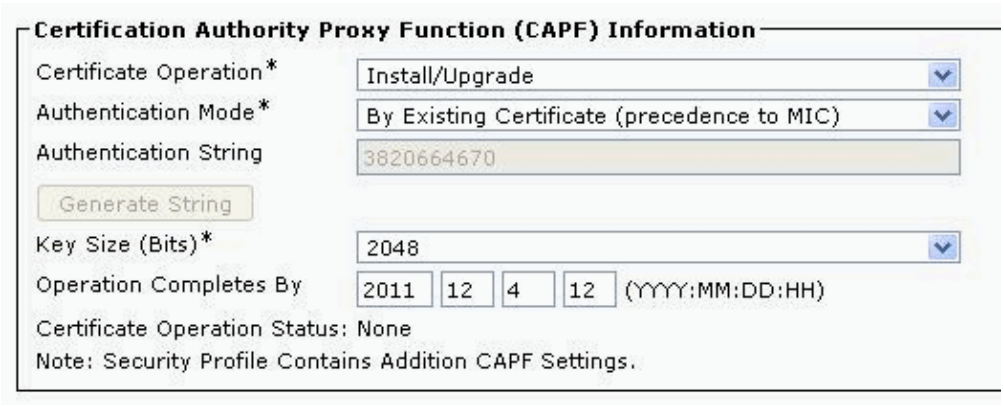
How to Secure the IP Phone

In order for the phone to accept the CTL file from any cluster without the need to delete the existing one requires that each cluster's CTL file has to be signed by the same shared set of eTokens. In other words, we need to create a CTL File for every cluster and sign them all with the same eToken. Additionally, in order to phones trust in the Centralized TFTP servers, you also have to add the Centralized TFTP servers in each CTL File.

Complete these steps in order to configure the security properties for an IP phone.

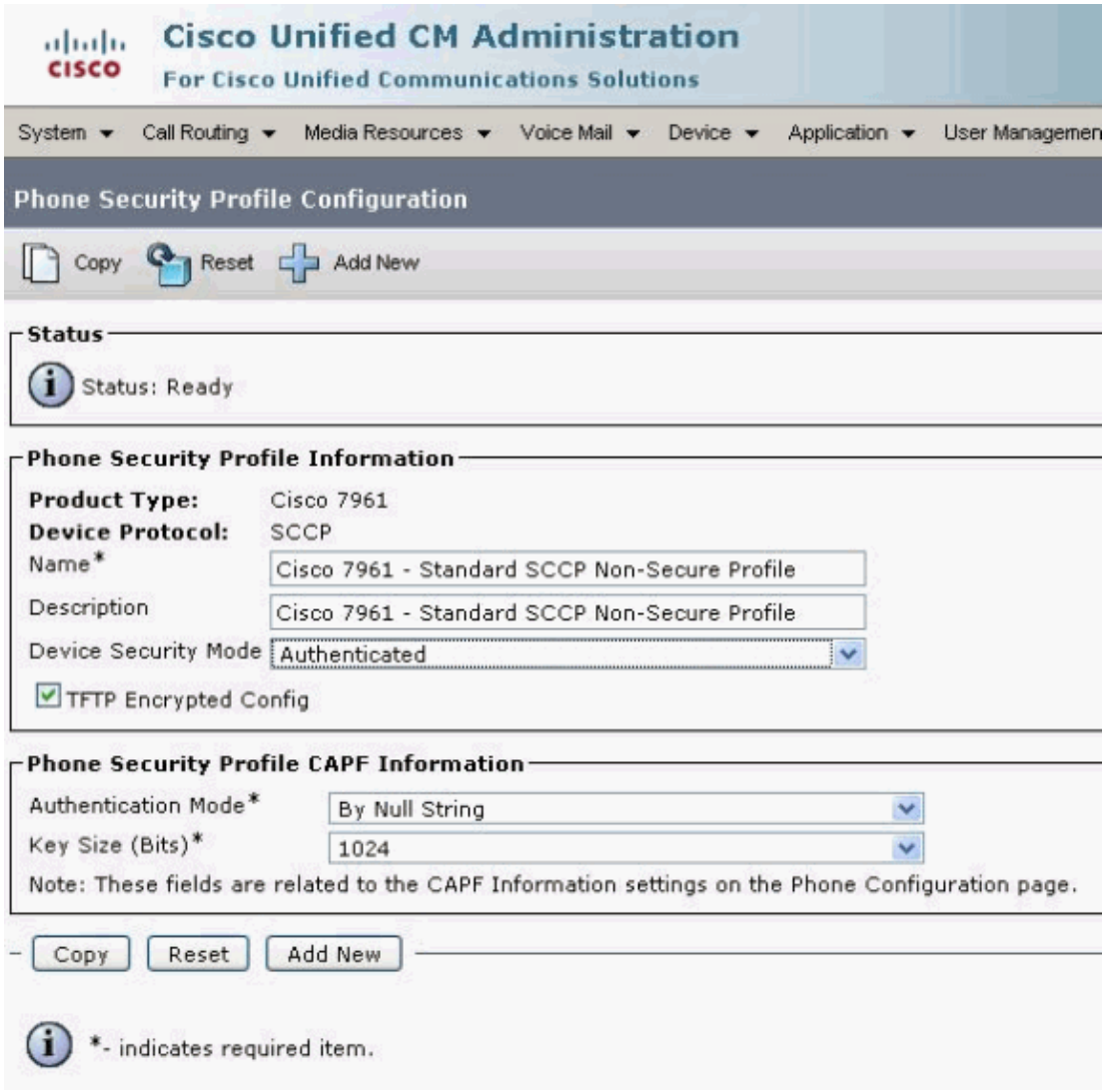
1. Configure the Device Security Profile. If a proper device Security Profile does not exist in the drop−down list from the IP phone configuration page, leave it as default, **Standard Non−Secure Profile**.
2. Configure Certification Authority Proxy Function (CAPF) Information, for the IP phone to get a new LSC, signed by the destination CUCM cluster.

   This is done on the phone configuration page of CUCM. Choose the values from dropdown menu as shown and then click **Save**.

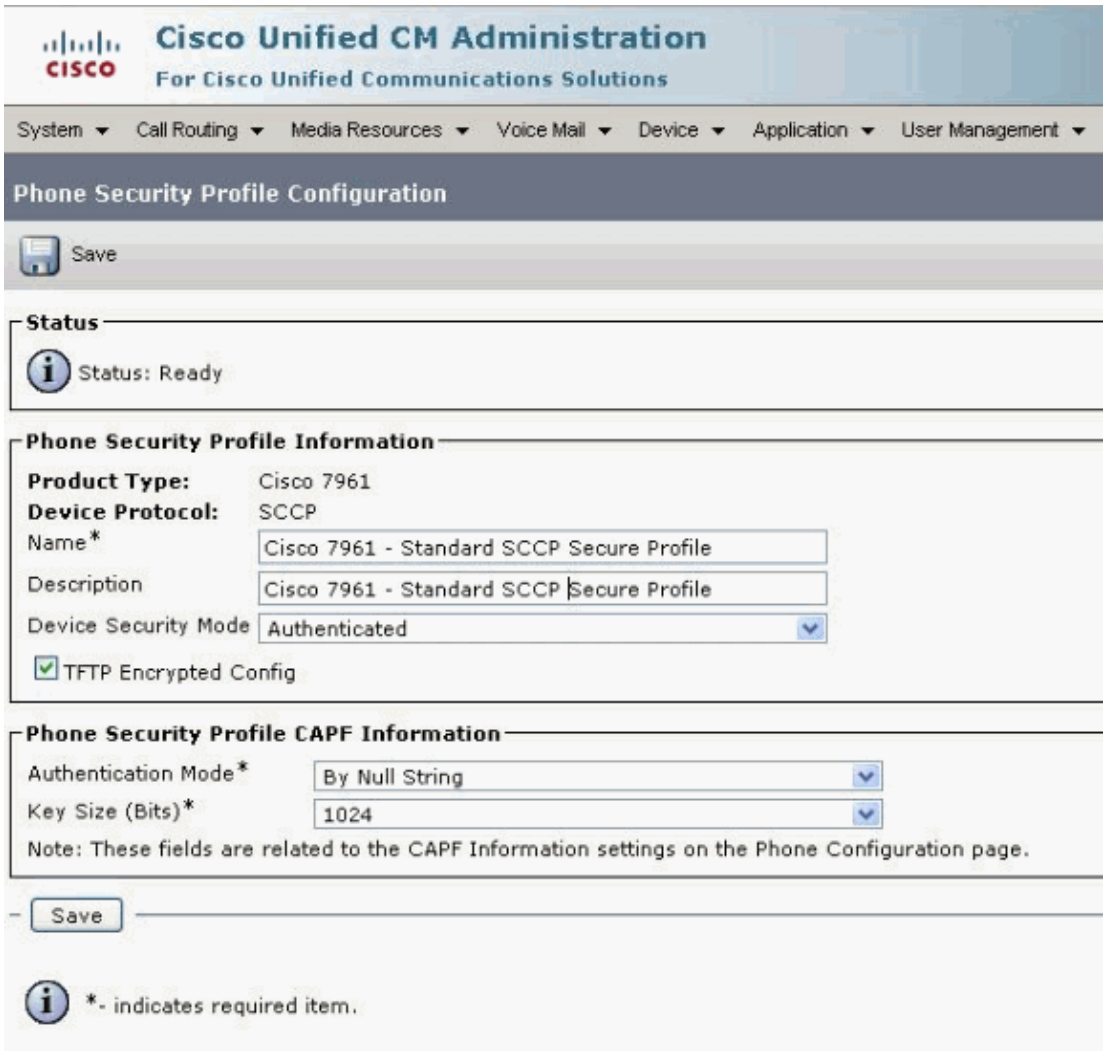


Configure the new created Device Security Profile:

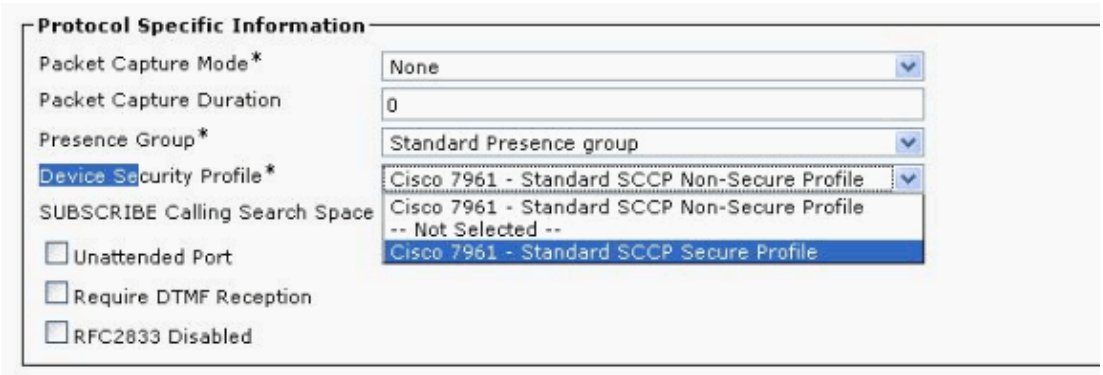
a. Choose **System > Security Profile > Phone Security Profile**.
b. Click **Find**.
c. Choose the phone type and enter the details:



d. Click **Copy**.
e. Now **Save** the configuration as shown here:

3. 

4. On the IP Phone configuration page, double−check that the proper *Device Security Mode* is configured.



5. Restart the IP Phone.
6. The phone should now download a new CTL file from the destination cluster and should get a LSC signed from the destination cluster.
7. The phone runs with the Security Mode configured in the Device Security Profile.

Related Information

- **Cisco Security Advisory: Cisco Unified Communications Manager CTL Provider Heap Overflow**
- **IP Phone Security and CTL (Certificate Trust List)**

- **Voice Technology Support**
- **Voice and Unified Communications Product Support**
- **Troubleshooting Cisco IP Telephony**
- **Technical Support & Documentation − Cisco Systems**

Updated: Nov 28, 2011 Document ID: 113333