Phone Hardening

This chapter provides information about phone hardening. To tighten security on the phone, you can perform phone hardening tasks in the **Phone Configuration** window in Unified Communications Manager Administration.

Gratuitous ARP Disable

By default, Cisco Unified IP Phones accept Gratuitous ARP packets. Gratuitous ARP packets, which devices use, announce the presence of the device on the network. However, attackers can use these packets to spoof a valid network device; for example, an attacker could send out a packet that claims to be the default router. If you choose to do so, you can disable Gratuitous ARP in the **Phone Configuration** window.

Note Disabling this functionality does not prevent the phone from identifying its default router.

Web Access Disable

Disabling the web server functionality for the phone blocks access to the phone internal web pages, which provide statistics and configuration information. Features, such as CiscoQuality Report Tool, do not function properly without access to the phone web pages. Disabling the web server also affects any serviceability application, such as CiscoWorks, that relies on web access.

To determine whether the web services are disabled, the phone parses a parameter in the configuration file that indicates whether the services are disabled or enabled. If the web services are disabled, the phone does not open the HTTP port 80 for monitoring purposes and blocks access to the phone internal web pages.

PC Voice VLAN Access Disable

By default, Cisco IP Phones forward all packets that are received on the switch port (the one that faces the upstream switch) to the PC port. If you choose to disable the PC Voice VLAN Access setting in the Phone Configuration window, packets that are received from the PC port that use voice VLAN functionality will drop. Various Cisco IP Phones use this functionality differently.

- Cisco Unified IP Phones 7942 and 7962 drop any packets that are tagged with the voice VLAN, in or out of the PC port.
- Cisco Unified IP Phone 7970G drops any packet that contains an 802.1Q tag on any VLAN, in or out of the PC port.

Setting Access Disable

By default, pressing the Applications button on a Cisco IP Phone provides access to a variety of information, including phone configuration information. Disabling the Setting Access parameter in the Phone Configuration window prohibits access to all options that normally display when you press the Applications button on the phone; for example, the Contrast, Ring Type, Network Configuration, Model Information, and Status settings.

The preceding settings do not display on the phone if you disable the setting in Unified Communications Manager Administration. If you disable this setting, the phone user cannot save the settings that are associated with the Volume button; for example, the user cannot save the volume.

Disabling this setting automatically saves the current Contrast, Ring Type, Network Configuration, Model Information, Status, and Volume settings that exist on the phone. To change these phone settings, you must enable the Setting Access setting in Unified Communications Manager Administration.

PC Port Disable

By default, Unified Communications Manager enables the PC port on all Cisco IP Phones that have a PC port. If you choose to do so, you can disable the PC Port setting in the Phone Configuration window. Disabling the PC port proves useful for lobby or conference room phones.

Note The PC port is available on some phones and allows the user to connect their computer to the phone. This connection method means that the user only needs one LAN port.

Set Up Phone Hardening

Phone Hardening consists of optional settings that you can apply to your phones in order to harden the connection. You can apply settings using one of three configuration windows:

- Phone Configuration - use **Phone Configuration** window to apply the settings to an individual phone

- Common Phone Profile - use the **Common Phone Profile** window to apply the settings to all of the phones that use this profile
- Enterprise Phone - use the **Enterprise Phone** window to apply the settings to all of your phones enterprise wide

Note If conflicting settings appear in each of these windows, following is the priority order the phone uses to determine the correct setting: 1) Phone Configuration, 2) Common Phone Profile, 3)Enterprise Phone

To setup phone hardening, perform the following procedure:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device** > **Phone**.

Step 2 Specify the criteria to find the phone and click **Find** to display a list of all phones.

Step 3 Click the device name.

Step 4 Locate the following product-specific parameters:

a) PC Port
b) Settings Access
c) Gratuitous ARP
d) PC Voice VLAN Access
e) Web Access

Tip To review information on these settings, click the help icon that appears next to the parameters in the **Phone Configuration** window.

Step 5 Choose **Disabled** from the drop-down list for each parameter that you want to disable. To disable the speakerphone or speakerphone and headset, check the corresponding check boxes.

Step 6 Click **Save**.

Step 7 Click **Reset**.

Where to Find More Information About Phone Hardening