Cisco IP Telephony Security Token Advisory

Used for Cisco Unified Communications Manager and Cisco Unified IP Phone authentication, the Cisco System Administrator Security Token is a USB device that contains a certificate that the Cisco Certificate Authority issues. You use a minimum of two security tokens when you configure the Cisco Certificate Trust List (CTL) client. The Cisco CTL client is a Cisco Unified Communications Manager application that supports authentication. To use the security tokens with the Cisco CTL client, you must install the Cisco CTL client on a single Windows workstation that has a USB port. After you configure the Cisco CTL client, the security tokens create and sign the CTL file. The CTL file is a list of trusted entities that support authentication.

The security token is supported with Cisco Unified Communications Manager Release 7.1(5) and later releases. Releases 7.1(5) through 9.1 require a driver after you install the Cisco CTL client.

For more information about the security token, authentication, the Cisco CTL client, and specific Windows versions that Cisco supports, see the *Cisco Unified Communications Manager Security Guide* for the release that you are using.

Use the following procedure to download the driver update.

Procedure

Step 1 To download the driver update,

a. Go to Cisco.com and navigate to the download page for the version of Cisco Unified Communications Manager that you are using.

b. Click the **Unified Communications Manager / CallManager / Cisco Unity Connection Utilities** link.

c. Select and download SecurityTokenDriver8.2.exe

Note If you have multiple versions of Cisco Unified Communications Manager, you only need to download this file once. The same file is posted for each version.

Step 2 Install the Cisco CTL Client, if it isn't already installed. Instructions are located in the *Cisco Unified Communications Manager Security Guide*.

CISCO SYSTEMS

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Step 3 Uninstall the Safenet Authentication Client 8.0 driver.

a. Navigate to the Windows uninstall program. Examples are **Start > Programs > Uninstall or Change a Program,** or **Start > Control Panel > Programs and Features**.

b. Uninstall Safenet Authentication Client 8.0

Step 4 Install SecurityTokenDriver8.2.exe

Caution Cisco requires a minimum of two security tokens to configure the Cisco CTL client. If you want to do so, purchase additional security tokens and immediately add the tokens to the CTL file. If you need to update the CTL file for any reason, you must use one security token that already exists in the file.

Cisco recommends that you store the security tokens in a location that you will remember. If you want to do so, keep one security token in the USB port at all times.

Tip When you confgure the Cisco CTL client, a prompt asks you to enter a password for the security token. Enter the default password, **Cisco123**. The password is case sensitive.

FCC Compliance

The Cisco System Administrator Security Token has been tested and complies with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

The Cisco System Administrator Security Token generates, uses, and can radiate radio frequency energy and, if you do not install and use it in accordance with the instructions, it may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If the Cisco System Administrator Security Token does cause harmful interference to radio or television reception, which you can determine by turning the equipment off and on, Cisco encourages you to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment to an outlet on a different circuit from the one to which the receiver is connected.
- Consult the dealer or an experienced radio and TV technician.

FCC Warning

Modifications that are not expressly approved by the manufacturer could void your authority to operate the Cisco System Administrator Security Token under FCC rules.

Class B Notice for Canada

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

VCCI Compliance for Class B Equipment

This is a Class B product based on the standard of the VCCI Council. If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.
