CHAPTER 2

Preventing Toll Fraud in Cisco Unity Connection

In this chapter, you will find a description of toll fraud—a potential security issue in any organization. You will also find information that may help you to develop preventive measures, and best practices to avoid toll fraud.

See the following sections:

Using Restriction Tables to Help Prevent Toll Fraud in Cisco Unity Connection

Toll fraud is defined as any toll (long distance) call that is made at the expense of your organization and in violation of its policies. Cisco Unity Connection provides restriction tables that you can use to help guard against toll fraud. Restriction tables control the phone numbers that can be used for transferring calls, for message notification, and for other Connection functions. Each class of service has several restriction tables associated with it, and you can add more as needed. By default, restriction tables are configured for basic toll fraud restrictions for a dial plan with a trunk access code of 9. Restriction tables should be adjusted for your specific dial plan and international dialing prefixes.

Best Practices

To prevent toll fraud by users, administrators, and even outside callers who have improperly gained access to a Cisco Unity Connection mailbox, implement the following changes:

- Set up all restriction tables to block calls to the international operator. When this is done, a person cannot dial out to or configure call transfers from an extension to the international operator (for example, a trunk access code of 9 followed by 00 to dial the international operator) for placing international calls.
- If Connection is integrated with two phone systems, add restriction table patterns to match applicable trunk access codes for both phone system integrations. For example, if the trunk access code for one of the phone system integrations is 99 and you want to restrict the call pattern 900, you would also restrict the pattern 99900. When patterns that include the trunk access codes are restricted, attempts to bypass the restriction table by first accessing either trunk and then dialing the international operator will be blocked.

- For those in your organization who do not need to access international numbers to do their work, set up restriction tables to block all calls to international numbers. This prevents a person who has access to a Connection mailbox that is associated with the restriction table from configuring call transfers or fax delivery from that extension to an international number.
- Set up restriction tables to permit calls only to specific domestic long distance area codes or to prohibit calls to long distance area codes. This prevents a person who has access to a Connection mailbox that is associated with the restriction table from configuring call transfers or fax delivery from that extension to a long distance number.
- Restrict the numbers that can be used for system transfers—a feature that allows callers to dial a number and then transfer to another number that they specify. For example, set up the applicable restriction tables to allow callers to transfer to a lobby or conference room phone, but not to the international operator or to a long distance phone number.

To learn more about how restriction tables work and how to set them up, see the Managing Restriction Tables in Cisco Unity Connection 9.x chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

Restricting Collect Calling Options

We recommend that you work with your telecommunications provider to restrict the collect calling option on your incoming phone lines, if appropriate.