



Enhanced Phone Security

Overview: Enhanced Phone Security

You can set up Cisco Unity subscriber accounts to use a secure logon method known as two-factor user authentication. Cisco Unity works with the RSA SecurID system to provide this method of enhanced phone security. The RSA SecurID system is made up of three major components: RSA SecurID authenticators, the RSA ACE/Server, and the RSA ACE/Agent.

With the RSA SecurID system, each authorized Cisco Unity subscriber is assigned an RSA SecurID authenticator. Every 60 seconds, the authenticator generates and displays a new, unpredictable number—known as a secure ID or tokencode—that is unique to the subscriber. RSA offers authenticators as hardware, software, and smart cards.

Each Cisco Unity subscriber who has an authenticator must have a user account on the ACE/Server. You use the RSA Database Administrator program on the ACE/Server to create and maintain the user accounts. A user account contains the RSA alias and PIN, and information about the user authenticator. By using the information in a user account, the ACE/Server generates the same secure ID as the user authenticator.

In the Cisco Unity Administrator, you assign subscribers to a class of service for which enhanced phone security is enabled. By default, Cisco Unity uses a subscriber Exchange alias as the subscriber RSA alias.

When logging on to Cisco Unity over the phone, subscribers enter an ID as usual. Then, instead of a password, subscribers enter a passcode, which is a number that combines the subscriber PIN and the secure ID displayed on the subscriber authenticator. Cisco Unity uses the ID to look up the user RSA alias and sends the RSA alias and passcode to the ACE/Agent installed on the Cisco Unity server. The ACE/Agent encrypts the RSA alias and passcode and sends it to the ACE/Server. The ACE/Server looks up the user account, then validates the passcode by using the information stored in the account. The ACE/Server returns a code to the ACE/Agent, which in turn passes it along to Cisco Unity. The return code indicates one of the meanings shown in [Table 8-1](#).

Table 8-1 ACE/Server Return Codes

Return Code	Meaning
Passcode accepted	Cisco Unity gives the subscriber access to messages.
Access denied	Cisco Unity prompts the subscriber to enter the passcode again. (This return code can also indicate that the ACE/Server is unavailable.)

Table 8-1 ACE/Server Return Codes (continued)

Return Code	Meaning
Secure ID expired	Cisco Unity prompts the subscriber to enter the next secure ID displayed on the authenticator.
New PIN needed	Cisco Unity prompts the subscriber to enter a new PIN.

Unless you have assigned PINs, the first time subscribers log on they will have not yet created a PIN, so instead of a passcode, they will enter only a secure ID. The subscriber conversation guides the subscriber through the process of creating a PIN. Cisco Unity detects when New PIN mode is enabled or when a subscriber PIN has been cleared in the RSA Database Administrator, and the subscriber conversation prompts the subscriber to create a new PIN at the next logon. When subscribers log on to Cisco Unity after a PIN has been cleared, instead of a passcode, they enter only a secure ID.

Setting Up Enhanced Phone Security

If you have an existing ACE/Server, skip the steps below that do not apply. See the RSA documentation for information on setting up the ACE/Server and ACE/Agent and for creating and maintaining user accounts.

To set up enhanced phone security

- Step 1** Install and configure the ACE/Server. Install only the Local Access Authentication (Client) and the Control Panel Applet components. Do not install the Web Access Authentication (Server) component.
- Step 2** On the ACE/Server, use the RSA Database Administrator program to create the appropriate user accounts.

Note that when specifying settings for PIN assignments, indicate user-created PINs only. Cisco Unity does not support system-generated PINs.
- Step 3** Create a group that includes all the users who will use enhanced phone security on Cisco Unity.
- Step 4** Create an Agent Host for each Cisco Unity server (required on both the primary and secondary server when failover will be used). Specify **Communications Server** as the Agent Host type. Add the group you created in [Step 3](#) to the Group Activation section of the new client.
- Step 5** On each Cisco Unity server, install and configure the ACE/Agent to work with the Agent Host(s) you created on the ACE/Server.
- Step 6** Use the ACE/Agent Test Authentication utility to authenticate a user with the ACE/Server. If you cannot authenticate the user with the test program, troubleshoot the ACE client/server connection. If you are using failover, also test in a manual failover condition.
- Step 7** Start **Cisco Unity**.
- Step 8** In the Cisco Unity Administrator on each Cisco Unity server, go to the **System > Configuration > Settings** page and check the **RSA Two Factor** check box.
- Step 9** Log off of the **Cisco Unity Administrator**.
- Step 10** Shut down and restart each **Cisco Unity** server for enhanced phone security to take effect.
- Step 11** Create a new class of service (COS) or modify an existing COS for the subscribers who are using enhanced phone security. (See the [“Class of Service Settings”](#) chapter for detailed procedures.)

- Step 12** On the Subscribers > Class of Service > Profile Page of the appropriate COS, click **Enhanced Security** in the Phone Security section.
- Step 13** Assign subscribers to the enhanced phone security COS. When using failover, the COS and subscriber settings only need to be created on the primary Cisco Unity server. They will automatically replicate to the secondary server.
- Step 14** If the RSA alias for the subscriber is something other than the subscriber Exchange alias, go to the subscriber **Profile** page and enter the RSA alias in the Enhanced Security User Alias box.
- Step 15** Distribute the RSA authenticators to the appropriate subscribers.
-

To disable enhanced security system-wide

- Step 1** In the Cisco Unity Administrator on each Cisco Unity server, go to the System > Configuration > Settings page, and uncheck the **RSA Two Factor** check box.
- Step 2** For every class of service (COS) currently being used in your system, go to the appropriate Subscribers > Class of Service > Profile page on the Cisco Unity server, and click **Regular Phone Security**. This change is only required on the primary Cisco Unity server if failover is in use. The COS settings will automatically replicate to the secondary server.
-

