



## Account Policy Settings

---

### Overview: Account Settings

The account policy settings on the Phone Password Restrictions Page and the Cisco Unity Account Lockout Page in the Cisco Unity Administrator apply when subscribers access Cisco Unity by phone. Changes to settings in the account policy affect all existing subscribers.

Note that the settings on the Account Policy pages represent a different account policy from the one that applies when subscribers use Cisco Unity web applications to access Cisco Unity. For information on specifying an account policy for the Cisco Personal Communications Assistant (PCA) and the Cisco Unity Administrator, see the [“Authentication Settings” section on page 26-11](#) section in the [“System Settings”](#) chapter for details.

See the following sections in this chapter for more information:

- [Phone Password Settings, page 17-1](#)—This section provides information about the settings on the Phone Password Restrictions page.
- [Account Lockout Settings, page 17-2](#)—This section provides information about the settings on the Cisco Unity Account Lockout page.

### Phone Password Settings

Phone password settings allow you to define the password policy that applies when subscribers log on to Cisco Unity by phone. For greater security, establish rules that prevent passwords from being easy to guess and from being used for a long time. It is also best to avoid requiring passwords that are so complicated or that must be changed so often that subscribers have to write them down to remember them. Subscribers can change their phone passwords by following the Cisco Unity subscriber conversation or by using the Cisco Unity Assistant.

Phone password restrictions settings cannot be changed for individual subscriber accounts.

Use the following table to learn more about phone password settings.

**Table 17-1** *Subscribers > Account Policy > Phone Password Restrictions Page*

Field	Considerations
Maximum Phone Password Age	<p>Select one of the following settings:</p> <ul style="list-style-type: none"> <li>• Password Never Expires—Subscribers are never prompted to change their passwords, although they are able to change passwords anytime.</li> <li>• Days Until Password Expires—Subscribers are prompted to change their passwords every X days. X is the value specified in the adjacent box.</li> </ul>
Phone Password Length	<p>Select one of the following settings:</p> <ul style="list-style-type: none"> <li>• Permit Blank Password—Subscribers are able to log on without entering a password. Note that this leaves subscriber messages vulnerable to unauthorized access.</li> <li>• Minimum Number of Characters—Subscribers are required to create a password at least X characters long. X is the value specified in the adjacent box. In general, shorter passwords are easier to use, but longer passwords are more secure. When you change the minimum password length, subscribers will be required to use the new length the next time they change their passwords.</li> </ul>
Phone Password Uniqueness	<p>Select one of the following settings:</p> <ul style="list-style-type: none"> <li>• Do Not Keep Password History—Cisco Unity does not compare a new password with previous passwords; thus a subscriber can reuse passwords.</li> <li>• Number of Passwords to Remember—Cisco Unity stores the specified number of previous passwords for a subscriber and compares a new password with them. Cisco Unity rejects the new password if it matches a password in the history.</li> </ul> <p>If the Permit Blank Password box is selected, the Phone Password Uniqueness fields are disabled.</p>
Check Against Trivial Passwords for Extra Security	<p>Check this box to have Cisco Unity verify that a new password meets the following criteria:</p> <ul style="list-style-type: none"> <li>• The password is not the same as previous passwords.</li> <li>• The digits are not all the same (for example, 9999).</li> <li>• The digits are not consecutive (for example, 1234).</li> <li>• The password is not the same as the extension assigned to the subscriber.</li> <li>• The password does not spell the name of the subscriber.</li> </ul> <p>If the Permit Blank Password box is selected, the Check Against Trivial Passwords for Extra Security field is disabled.</p>

## Account Lockout Settings

Cisco Unity account lockout settings allow you to specify whether you want Cisco Unity to use an account lockout policy which applies when subscribers access Cisco Unity by phone. To customize the account lockout policy for your organization, you can use the settings on the Cisco Unity Account Lockout page which dictate:

- How Cisco Unity handles situations when subscribers attempt to log on to Cisco Unity by phone and repeatedly enter incorrect phone passwords.

- The number of failed logon attempts that are allowed before Cisco Unity prohibits the subscriber from accessing Cisco Unity by phone.
- The length of time that a subscriber who is locked out must wait until they can attempt to access Cisco Unity by phone again.

Changes to account policy settings affect all Cisco Unity subscribers. You cannot change account policy settings for individual subscriber accounts, though you can lockout individual subscriber accounts to prevent subscribers from using the phone to access Cisco Unity. (For details, see the “[Subscriber Account Settings](#)” section in the “[Subscriber Settings](#)” chapter.)

Use the following table to learn more about account lockout settings.

**Table 17-2** *Subscribers > Account Policy > Unity Account Lockout Page*

Field	Considerations
No Account Lockout	Click this option if you do not want to specify an account lockout policy for subscribers using the phone to access Cisco Unity. When this option is selected, Cisco Unity allows unlimited logon attempts to a subscriber account.
Account Lockout	Click this option if you want to specify an account lockout policy for subscribers using the phone to access Cisco Unity. When this option is selected, enter the appropriate values in the following fields: <ul style="list-style-type: none"> <li>• Lock Account After __ Invalid Attempts</li> <li>• Reset Count After __ Minutes</li> <li>• Lockout Duration</li> </ul>
Lock Account After __ Invalid Attempts	Enter the number of failed logon attempts after which subscribers cannot access Cisco Unity by phone. This option is unavailable when the No Account Lockout option is selected.
Reset Count After __ Minutes	Enter the number of minutes after which Cisco Unity will clear the count of failed logon attempts to Cisco Unity by phone (unless the failed logon limit is already reached and the account is locked). This option is unavailable when the No Account Lockout option is selected.
Lockout Duration	Select one of the following settings: <ul style="list-style-type: none"> <li>• Forever—When you select this option, Cisco Unity will prevent subscribers from accessing Cisco Unity by phone until a system administrator unlocks the subscriber account on the Subscribers &gt; Subscribers &gt; Account Page for an individual subscriber. Use this setting only if a system administrator is readily available to assist subscribers or if the system is prone to unauthorized access.</li> <li>• Minutes—When you select this option, enter the number of minutes that Cisco Unity will prevent subscribers from accessing Cisco Unity by phone. Cisco Unity allows subscribers to access Cisco Unity by phone after the specified number of minutes has elapsed. Use this setting if a system administrator may not be available to assist subscribers; avoid using if the system is prone to unauthorized access.</li> </ul> This option is unavailable when the No Account Lockout option is selected.

