



Account Policy Settings

Overview: Account Settings

The Cisco Unity account policy includes the same settings as the Windows account policy. They are separate policies, however; subscribers have a Windows password which is used to access Cisco Unity by computer and a Cisco Unity password which is used to access Cisco Unity by phone.

Changes to settings in the account policy affect all existing subscribers. For example, if you change the passwords setting, subscribers whose passwords do not conform to the new setting are required to conform to it the next time they change their passwords. Account policy settings cannot be changed in individual subscriber Cisco Unity accounts.

Refer to 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 17-3](#)—This section provides information about the settings on the Account Lockout page.

Phone Password Settings

Phone password settings allow you to define the characteristics of the phone passwords that subscribers use to log on to Cisco Unity. 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.

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"> • Password Never Expires—Subscribers are never prompted to change their passwords, although they are able to change passwords anytime. • Days Until Password Expires—Subscribers are prompted to change their passwords every X days. X is the value specified in the adjacent box.
Phone Password Length	<p>Select one of the following settings:</p> <ul style="list-style-type: none"> • Permit Blank Password—Subscribers are able to log on without entering a password. Note that this leaves subscriber messages vulnerable to unauthorized access. • 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.
Phone Password Uniqueness	<p>Select one of the following settings:</p> <ul style="list-style-type: none"> • Do Not Keep Password History—Cisco Unity does not compare a new password with previous passwords; thus a subscriber can reuse passwords. • 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. <p>If the Permit Blank Password box is selected, the Phone Password Uniqueness field is disabled.</p>

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

Field	Considerations
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"> • The password is not the same as previous passwords. • The digits are not all the same (for example, 9999). • The password is not the same as the extension assigned to the subscriber. • The password does not spell the name of the subscriber. <p>If the Permit Blank Password box is selected, the Check Against Trivial Passwords for Extra Security field is disabled.</p>

Account Lockout Settings

The account lockout settings allow you to lock subscriber accounts when incorrect phone passwords are entered repeatedly. The settings specify the number of invalid logon attempts that are allowed before the account is locked, and specify whether the account must be unlocked by a system administrator.

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

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

Field	Considerations
Cisco Unity Account Lockout	<p>Select one of the following settings:</p> <ul style="list-style-type: none"> • No Account Lockout—Cisco Unity allows unlimited logon attempts to a subscriber account. • Account Lockout—Cisco Unity blocks phone access to a subscriber account when the limit of logon attempts is reached, though the subscriber can access the account by using the ActiveAssistant, and can play messages from the mail Inbox. <p>Once the account has been accessed with a valid logon, Cisco Unity resets the number of logon attempts to zero.</p>

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

Field	Considerations
Lock Account After __ Invalid Attempts	Enter the number of unsuccessful logon attempts after which Cisco Unity will block phone access to a subscriber account.
Reset Count After __ Minutes	Enter the number of minutes after which Cisco Unity will clear the count of logon attempts, unless the limit is reached and the account is locked.
Lockout Duration	<p>Select one of the following settings:</p> <ul style="list-style-type: none"> • Forever—A subscriber whose account is locked with Lockout Duration set to Forever must contact a system administrator to change the password. Use this setting only if a system administrator is readily available to assist subscribers or if the system is prone to unauthorized access. • Minutes—Cisco Unity unlocks an account automatically after the specified number of minutes. Use this setting if a system administrator may not be available to assist subscribers; avoid using if the system is prone to unauthorized access.