



CHAPTER 6

Account Policy Settings

Account Policy Phone Password Restrictions Page

Table 6-1 Subscribers > Account Policy > Phone Password Restrictions Page

Field	Considerations
Maximum Phone Password Age	Select one of the following settings: <ul style="list-style-type: none">• Password Never Expires—Subscribers are never prompted to change their passwords, although they are able to change passwords at any time.• Days Until Password Expires—Subscribers are prompted to change their passwords every X days. X is the value specified in the adjacent field.
Phone Password Length	Select one of the following settings: <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 and toll fraud.• Minimum Number of Characters—Subscribers are required to create a password at least X characters long. X is the value specified in the adjacent field. In general, shorter passwords are easier to use, but longer passwords are more secure. Eight or more digits is recommended. When you change the minimum password length, subscribers will be required to use the new length the next time that they change their passwords.
Phone Password Uniqueness	Select one of the following settings: <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. If the Permit Blank Password check box is selected, the Phone Password Uniqueness fields are disabled.

Table 6-1 *Subscribers > Account Policy > Phone Password Restrictions Page (continued)*

Field	Considerations
Check Against Trivial Passwords for Extra Security	<p>Check this check box to have Cisco Unity verify that a new password meets the following criteria when subscriber phone passwords are changed by using the Cisco Unity Administrator, the Cisco Unity Assistant, or the Cisco Unity conversation:</p> <ul style="list-style-type: none"> • The digits are not all the same (for example, 9999). • The digits are not consecutive (for example, 1234 or 4321). • The password is not the same as the primary extension assigned to the subscriber. <p>If Permit Blank Password has been selected, the Check Against Trivial Passwords for Extra Security field is disabled.</p>

Account Policy Unity Account Lockout Page

Table 6-2 *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 who use the phone to access Cisco Unity. When this option is selected, Cisco Unity allows unlimited logon attempts to a subscriber account.
Account Lockout	<p>Click this option if you want to specify an account lockout policy for subscribers who use the phone to access Cisco Unity. When this option is selected, enter the applicable values in the following fields:</p> <ul style="list-style-type: none"> • Lock Account After __ Invalid Attempts • Reset Count After __ Minutes • Lockout Duration
Lock Account After __ Invalid Attempts	<p>Enter the number of failed logon attempts after which subscribers cannot access Cisco Unity by phone.</p> <p>This option is unavailable when the No Account Lockout option is selected.</p>
Reset Count After __ Minutes	<p>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).</p> <p>This option is unavailable when the No Account Lockout option is selected.</p>

Table 6-2 *Subscribers > Account Policy > Unity Account Lockout Page (continued)*

Field	Considerations
Lockout Duration	<p>Select one of the following settings:</p> <ul style="list-style-type: none"> • 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 > Subscribers > 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 and toll fraud. • 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 and toll fraud. <p>This option is unavailable when the No Account Lockout option is selected.</p>

