6UCSCG0001-29A
September 2010

ADTRAN

Configuration Guide

Configuring User Class of Service in the NetVanta UC Server

This configuration guide describes the functionality and configuration of the user class of service (CoS) settings in the NetVanta Unified Communications (UC) Server. The user CoS is configured through the administrator's interface of the UC server graphical user interface (GUI). This guide contains an overview of the user CoS feature, and describes how to create the CoS, configure the CoS settings, and apply the CoS to user profiles.

This guide consists of the following sections:

Overview of the UC Server User CoS

The user CoS feature of the NetVanta UC Server helps the system administrator to configure settings for multiple user accounts by configuring a single CoS and applying it to multiple users. CoS configuration includes specifying user account behavior, mailbox limitations, and user access to UC server features. Each of the features covered by the CoS can be specified for a single user on an individual basis (without the CoS), or a single CoS can be created and applied to multiple users. Employing the user CoS feature can be beneficial in UC server deployments with a large number of users that require the same account settings. The NetVanta UC Server User CoS includes settings for local voice mailbox limits, specifying rules for user passwords and personal identification numbers (PINs), authentication lockout and tracking of user accounts, and enabling user access to certain UC server features. Each of these settings is described in the following sections.

Specifying Voice Mailbox Limits

Voice mailbox limits allow administrators to limit the amount of data users can create and store. In the UC server, the voice mailbox limits apply only to the locally stored message mailboxes, and are not applied to any unified messaging mailboxes (such as those in Microsoft® Exchange or Internet Message Access Protocol (IMAP) messaging systems).

Administrators can limit the amount of data stored in the voice mailbox by specifying the maximum number of voice messages allowed in a single mailbox, the maximum total length of all voice messages, and the maximum length of time messages are stored in the mailbox. When the maximum number of messages or total length of the stored messages is exceeded, the mailbox is considered full and the user is notified the next time he or she accesses the mailbox. Users cannot continue to receive new messages when the mailbox limits are exceeded. In addition, any messages older than the specified storage time must be deleted. The user is also notified that message deletion must occur when he or she accesses the mailbox.

Specifying User Password and PIN Rules

Administrators can specify the rules users must adhere to when configuring their passwords and PINs for logging into their voice mailbox. These password and PIN rules revolve around enforcing a certain level of complexity when defining passwords and PINs, defining minimum and maximum lengths for both the password and PIN, and mandating password and PIN changes after a certain amount of time. Specifying these rules helps maintain a more secure voicemail system.

Specifying Account Lockout Actions

Also in the interest of a more secure voicemail system, administrators can enable an automatic lockout feature to lock users out of an account if there have been too many failed access attempts. In addition, the UC server can track the number of failed login attempts for a specified amount of time. If the user reaches the maximum number of failed attempts during the specified tracking time, the user is locked out of the system until the tracking time expires. The account lockout feature does not apply to Windows authentications.

Specifying User Access to UC Server Features

Administrators can also specify the UC server features that users can access. The features include transferring calls using the NetVanta Personal Assistant, using Active Message Delivery (AMD) in the NetVanta Personal Assistant, using pager and email message notifications in the NetVanta Personal Assistant, and creating bulletin voice messages in the UC server voicemail system. These features can each be enabled or disabled in the user CoS.

Hardware and Software Requirements and Limitations

The NetVanta UC Server User CoS feature is only available in UC server products running NetVanta UC Server version 4.6 or later.

The CoS features can be applied to multiple users by applying the CoS to multiple users, or each feature can be configured individually on a per-user basis (without using the CoS). However, a CoS and an individual configuration cannot be applied to a single user at the same time. If a CoS is applied to the user, individual settings cannot be applied to override specific aspects of the CoS. If a different variation of settings is necessary, the user either must be individually configured, or a new CoS with the desired settings must be created and applied to that user.

When adding new users to the UC server system, the default CoS is available to all users. The default CoS of **System Voice Mail** is available as the user's CoS default during a new installation of the UC server or a system upgrade. If another CoS has been configured, it is also available during a new installation or system upgrade. If another CoS is set as the default, then it will be available as the default CoS to all new users. If the default CoS does not exist, then the CoS of **None** is available for all users.

Voicemail greetings and bulletin messages are not subject to individual mailbox limits.

If automatic lockouts are enabled, users will be locked out of the account after the configured number of failed attempts in the defined period. Regardless of whether automatic lockouts are enabled, users only have a maximum of **3** sequential attempts to log into the system before the system terminates access. This access termination does not in and of itself cause account lockout.

If the administrator has to reset a user's password or PIN, only the password/PIN length rules are applied. Administrators do not have to follow password/PIN complexity or history rules when resetting a password.

It is not possible for the administrator to lock a user out of the system. A user can only be locked out of the system due to failed login attempts. The administrator must then unlock the system for the user to regain access.

Administrators can disable a user's local authentication (password) but cannot disable a user's PIN.

It is possible for the administrator to be locked out of the system from a remote computer if there have been too many failed administrator login attempts; however, if the administrative authentication is being used from the local system (where the UC client is running on the same computer as the UC server), then the administrator lockout status is ignored. If authentication is disabled in the UC server, then lockout settings are not applied.

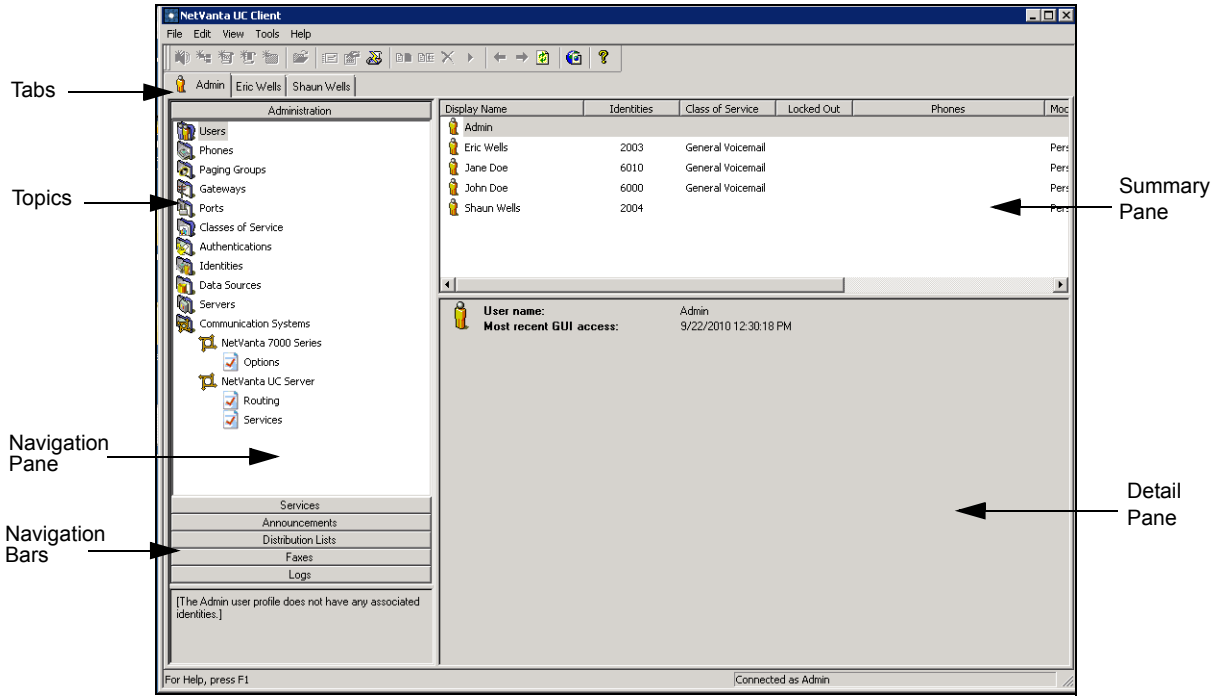
Configuring the User CoS

There are three main steps in the configuration of a user CoS. First, you must create a user CoS. Second, you must configure the various components of the CoS. Third, you must apply the CoS to the appropriate user profiles. These steps are covered in the following sections.

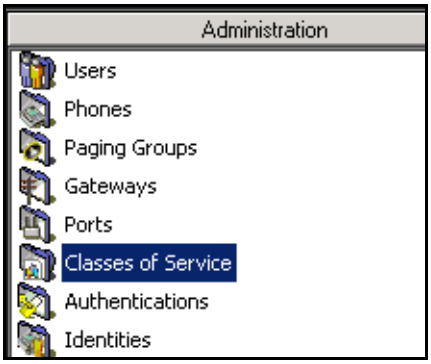
Creating a User CoS

To create a new user CoS, follow these steps:

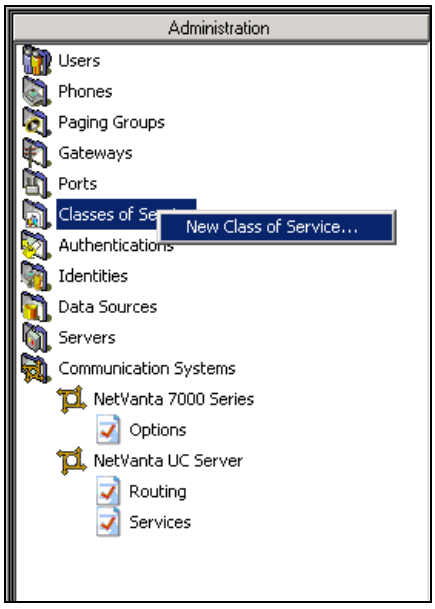
1. Log into the UC server as the administrator. Connect to the UC server client and navigate to the **Admin** tab. Select the **Administration** navigation bar to access the **Administration** navigation pane.



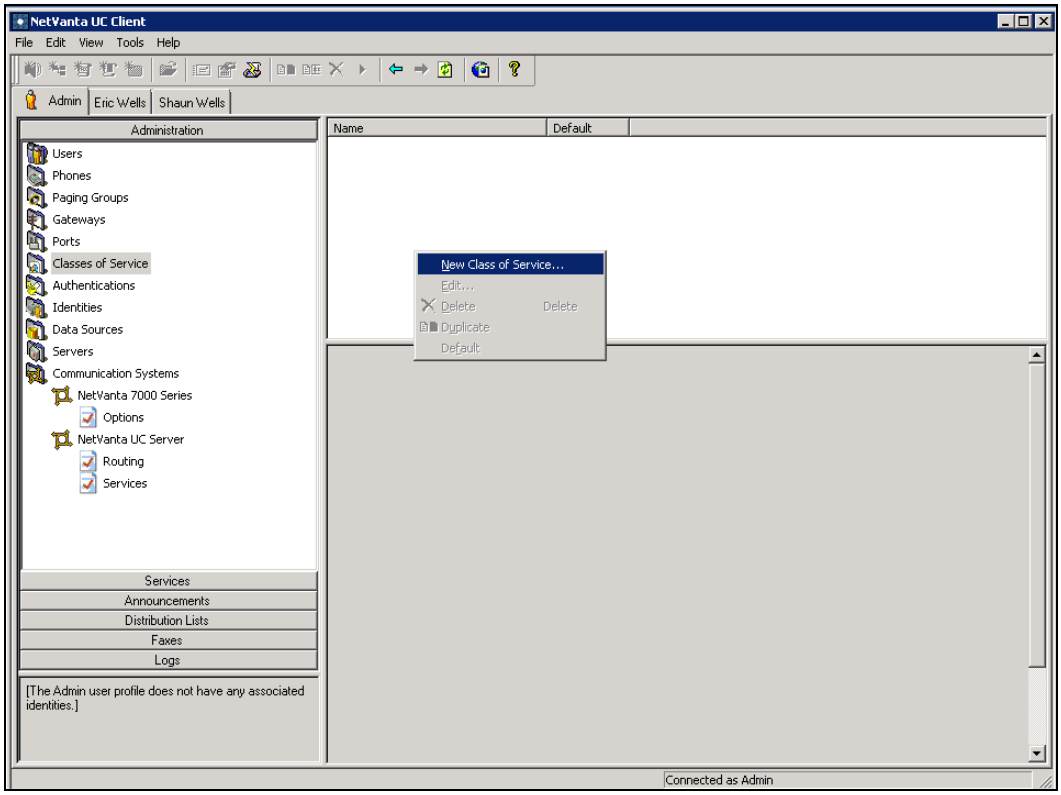
2. Select the **Classes of Service** topic from the list in the **Administration** pane.



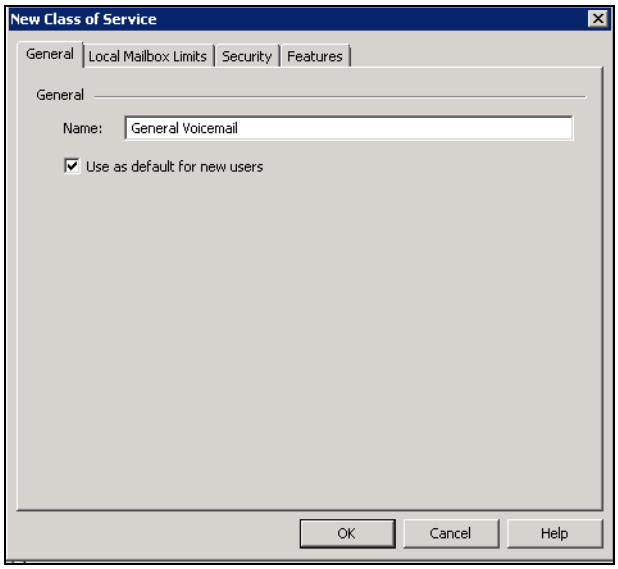
3. Then, right-click on the **Classes of Service** topic in the **Administration** pane and select **New Class of Service**.



You can also create a new CoS by highlighting the **Classes of Service** topic in the **Administration** pane and right-clicking on the summary pane. Select **New Class of Service** from the menu.



4. Next, specify the name for the CoS in the dialog box. The name should be a unique identifier specifically for this CoS. If you want this CoS to be the default CoS, select the check box next to **Use as default for new users**. In the following example, the CoS, named **General Voicemail**, will be the default CoS for new users.



> NOTE *Once a CoS has been created, you can make that CoS the default by right-clicking on the CoS name in the CoS summary pane and selecting **Default** from the drop-down menu.*

5. After you have named the CoS, you will configure the different aspects of the CoS using the tabs at the top of the **New Class of Service** dialog box. The configuration tabs are described in the following section.

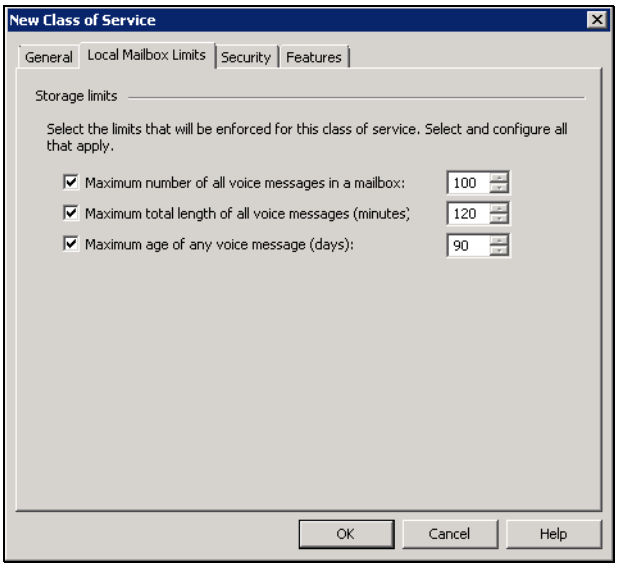
> NOTE *Do not select **OK** until the CoS is completely configured and you are ready to apply the settings. Selecting **OK** closes the **New Class of Service** dialog box.*

Configuring the User CoS

The user CoS is configured using the configuration tabs at the top of the **New Class of Service** dialog box. You can specify the local mailbox limits, password and PIN rules, authentication lock settings, and user access to UC server features. To configure the user CoS, follow these steps:

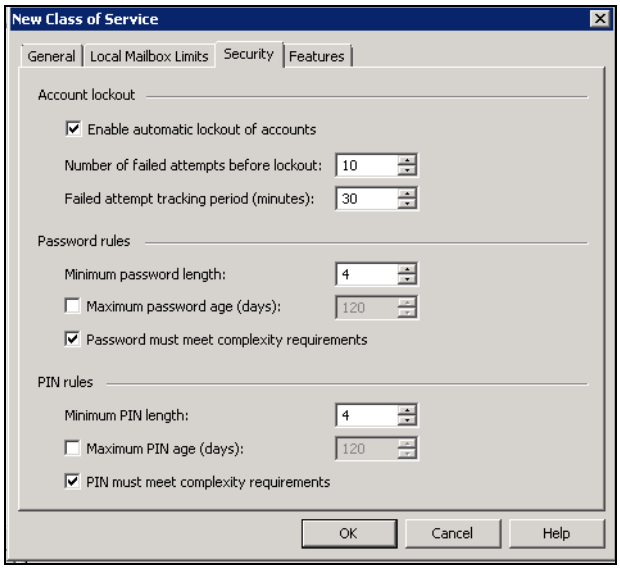
1. To configure the local mailbox limits for the CoS, select the **Local Mailbox Limits** configuration tab in the **New Class of Service** dialog box. Here you can specify the maximum number of voice messages in the mailbox, the maximum combined length of all stored messages, and the maximum time messages

are stored. To enable these limits, select the check box next to the appropriate option. You can then specify the maximums for each option.



By default, all mailbox limits are disabled. When enabled, the maximum number of voice messages allowed in the mailbox defaults to **100** messages. The valid maximum message range is **1** to **9999**. When enabled, the maximum combined length of voicemail messages defaults to **120** minutes. The valid maximum message length range is **1** to **9999** minutes. When enabled, the maximum storage time for voicemail messages defaults to **90** days. The valid storage range is **1** to **9999** days.

2. After you have configured the local mailbox limits, specify the authentication lockout behavior of the user account and the user password and PIN rules by selecting the **Security** configuration tab in the **New Class of Service** menu. Here you can specify that account lockout behavior is enabled and set the lockout parameters, as well as specify the maximum and minimum password and PIN lengths, the frequency with which passwords and PINs must be changed, and enable the complexity rules for passwords and PINs. Each setting is enabled by selecting the check box next to the desired option and entering a value (where appropriate).



By default, automatic lockout of accounts after a number of failed login attempts is enabled. You can disable this feature by selecting the check box next to the option. In addition, you can specify the number of failed attempts that are allowed before a lockout occurs by entering the number in the appropriate field. By default, a lockout occurs after **10** failed attempts. The valid attempt range is **1** to **99**.

The user authentication lockout is tracked for a specified number of minutes. This setting specifies the time period in which failed attempts are logged and counted against the maximum allowed number of failed attempts. When the time period ends, the tracked number of failed attempts is reset and begins again. By default, login attempts are tracked for **30** minutes. The valid tracking range is **1** to **525600** minutes (1 year). Even if a successful login attempt occurs during this time period, after a number of failed login attempts, the logged number of failed attempts is not reset until the tracking time period expires.

*If automatic lockouts are enabled, users will be locked out of the account after the configured number of failed attempts in the defined period. Regardless of whether automatic lockouts are enabled, users only have a maximum of **3** sequential attempts to log into the system before the system terminates access. This access termination does not in and of itself cause account lockout.*

By default, complexity rules for both passwords and PINs are enabled. The following table outlines the complexity rules for both passwords and PINs.

Table 1. Password/PIN Complexity Rules

Password Rules	PIN Rules
Must not match the authentication name.	Must not match the mailbox number.
Must have at least one uppercase and one lowercase alphabet character.	Must not be the reverse of the mailbox number.
Must have at least one digit or symbol.	Must not be a single repeated digit (for example, **1111**).
A new password cannot be the same as the previous password.	Must not be a consecutive sequence of ascending or descending numbers (for example, **1234**).
	Must not be a consecutive sequence of ascending or descending odd or even numbers (for example, **7531**).
	A new PIN cannot be the same as the previous PIN.

By default, the maximum password length is **128** characters and the minimum is **4**. The valid password length range is **4** to **128** characters.

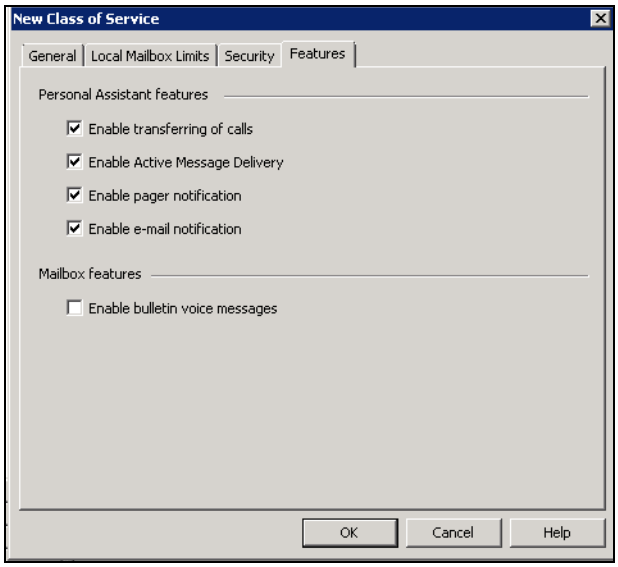
By default, the maximum PIN length is **15** characters, and the minimum length is **4**. The valid range for PIN length is **4** to **15** characters.

By default, passwords and PINs can be used for **120** days. To specify that passwords or PINs must be

changed after a certain amount of time, select the check box next to **Maximum PIN age** and enter the number of days until the next password or PIN change is required. The valid range is **1** to **9999** days.

> *There are special rules for administrator passwords/PINs and for administratively reset passwords/PINs. By default, the administrator account does not have to follow password or PIN complexity rules; its passwords and PINs can be used indefinitely, and the minimum password/PIN length is set to **4**. When the administrator resets a user password or PIN, the complexity rules are not enforced. In addition, administrators can choose to force the user to change their password/PIN upon their next attempt to login to the system by selecting the appropriate check box when resetting the user password/PIN.*

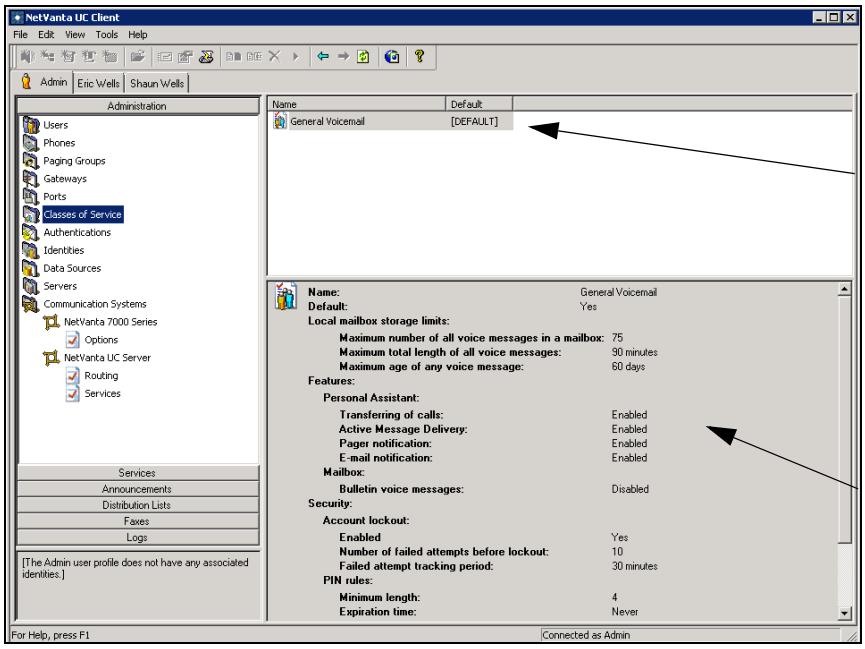
3. The next step in configuring the user CoS is to set the user permissions for access to various UC server features. Select the **Features** tab in the **New Class of Service** menu to specify user permissions.



You can specify that users have access to transferring calls, using AMD, and pager and email message notifications in the NetVanta UC Server Personal Assistant, as well as that users can create and send bulletin voice messages. By default, all Personal Assistant features are user accessible. By default, users cannot create bulletin voice messages. Select the check box next to each feature to enable user access to that feature. If you do not want users to access a certain feature, clear the check box next to that feature.

> *These settings apply to the NetVanta UC Server Personal Assistant, but not the NetVanta UC Server Personal Business Assistant.*

4. After you have configured the mailbox limits, password and PIN rules, authentication lockout behaviors, and user permissions, the user CoS configuration is complete. Select **OK** to apply the settings and create the new CoS. The newly created CoS appears in the **Classes of Service** summary pane, and details of the CoS appear in the detail pane.



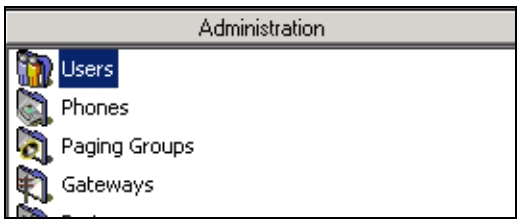
Applying the CoS to User Profiles

After you have created the user CoS, it is available for application to various user accounts. There are a number of ways to apply the CoS to user accounts. You can apply the CoS to multiple users already configured on the system, you can apply the CoS to multiple users you are importing into the system, and you can apply the CoS to individual users already in the system or that are being added or imported into the system. The following sections outline the different methods of applying a user CoS to various user accounts.

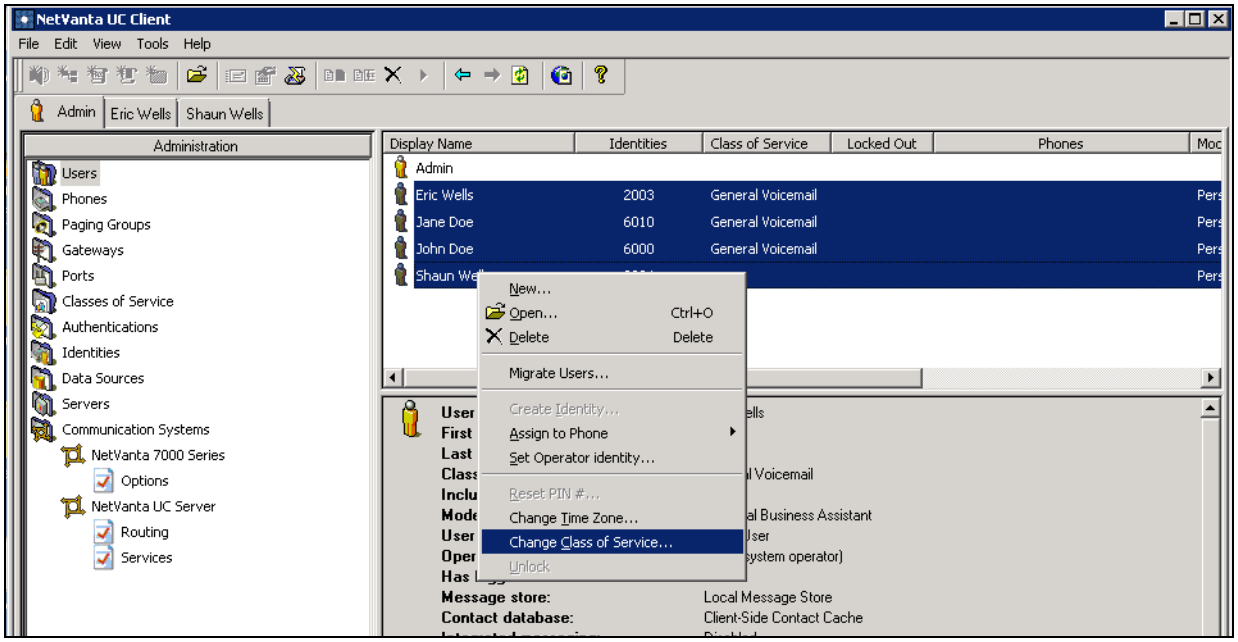
Applying the CoS to Users Already in the System

If you have users that have already been entered into the UC server system, you can create a user CoS and apply it to an individual user or multiple users at once. To apply a configured user CoS to existing users, follow these steps:

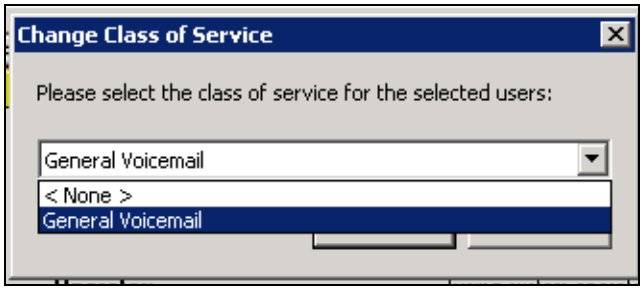
1. Select the **Users** topic from the list in the **Administration** navigation pane.



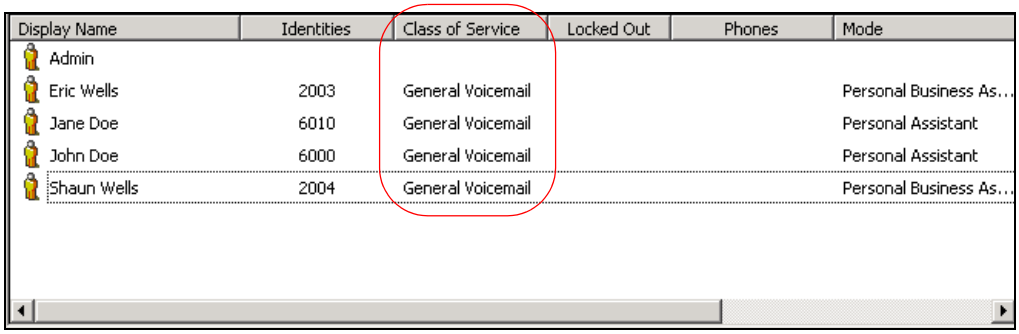
2. In the **Users** summary pane, select the users to which you want to apply the CoS. To select multiple users, hold down the **Shift** key while making your selection. Once you have selected the users to which you want to apply the CoS, right-click in the highlighted area and select **Change class of service** from the drop-down menu.



3. In the **Change class of service** dialog box that appears, select the appropriate CoS from the drop-down menu.



4. Once you have made your selection, select **OK**. The CoS field, in the **Users** summary pane, displays each user's assigned CoS.



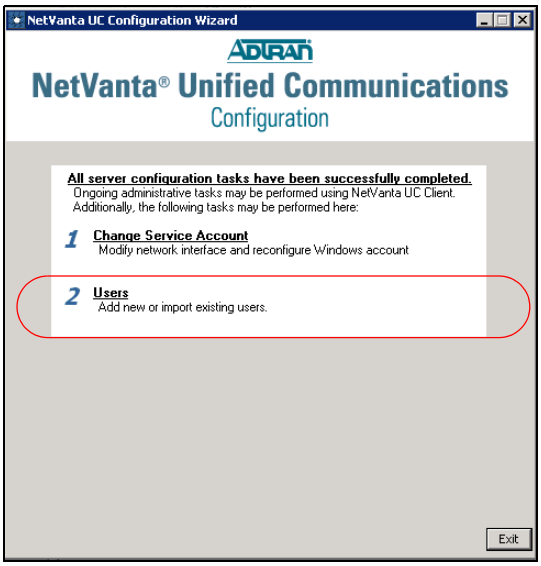
5. Repeat this process for as many existing users as necessary. A user's CoS can be changed by following the same procedure.

> NOTE *You can also change a user's CoS assignment in the **Edit User** menu. To access this menu, right-click on a user in the **Users** summary pane and select **Open**. In the **Edit User** menu, select the **General** tab and then select the appropriate CoS from the drop-down menu. When you have finished with your changes, select **OK** to apply the new CoS to the user.*

Applying the CoS to Multiple Users Being Imported into the System

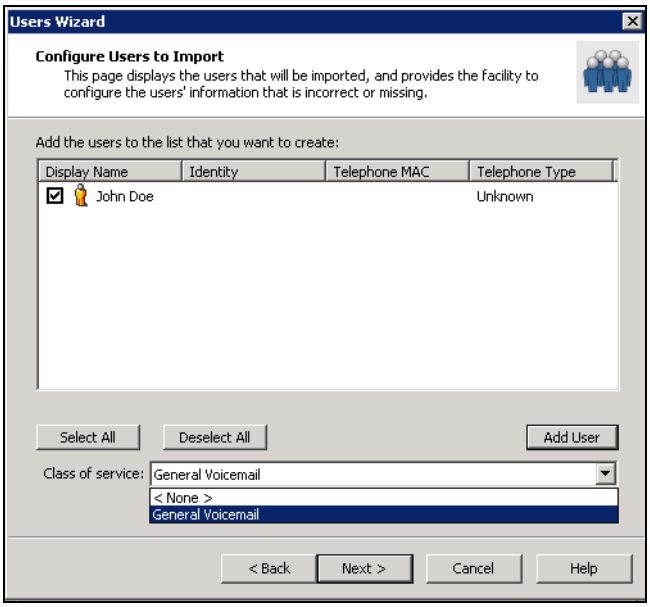
If you are importing a large number of users into the UC server system, you can apply a configured user CoS as you import the users. To apply a CoS as you import users using the NetVanta UC Configuration Wizard, follow these steps:

1. In the NetVanta UC Configuration Wizard, select the **Users** wizard.



> NOTE *The NetVanta UC Configuration Wizard can be accessed at any time by navigating to **Start** > **All Programs** > **ADTRAN** > **NetVanta UC Server Configuration Wizard**. You will be prompted for your name and password before you can select the **Users** wizard.*

2. After the wizard introduction screen, select **Next**. Work through the steps of the **Users** wizard, entering the user import method, file location, etc. Whether you import users from Microsoft Exchange, from a text-based file, or manually enter them, you have the option to select (from a drop-down menu) a CoS to apply to the users as you add them.



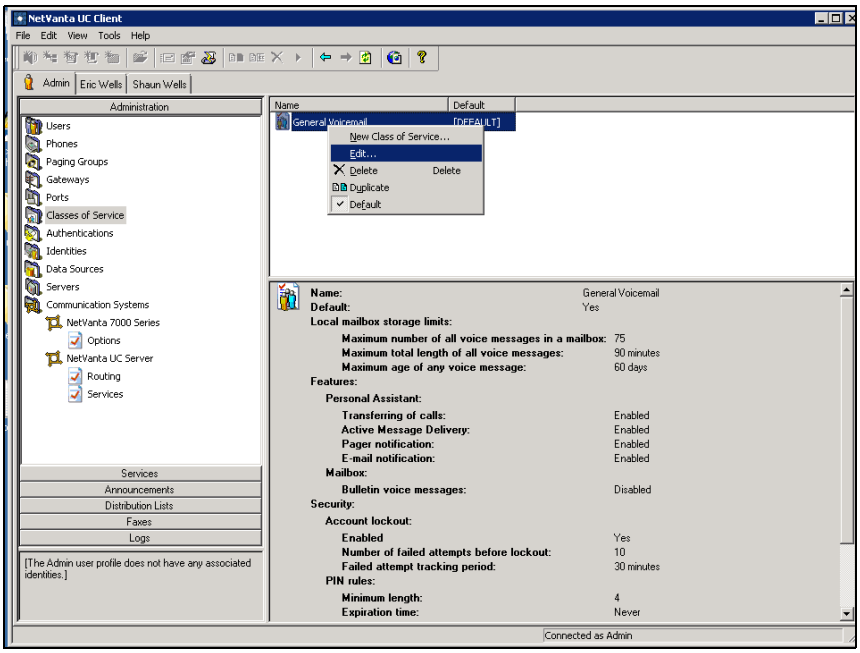
3. Once you have selected the correct CoS for the imported users, follow the remaining steps in the **Users** wizard to add these users to the system. When you have completed importing the users, their information (and CoS type) appears in the **Users** summary pane.

> NOTE
>
> *If you are creating new users manually, rather than importing users, you can also use the **New User Wizard** from the **Administration** navigation pane. To access this wizard, right-click in the **Users** summary pane and select **New**. Using this method, you can configure each individual user's information (including the CoS), the user password and PIN, messaging store, answering mode and operator, and finish the wizard.*

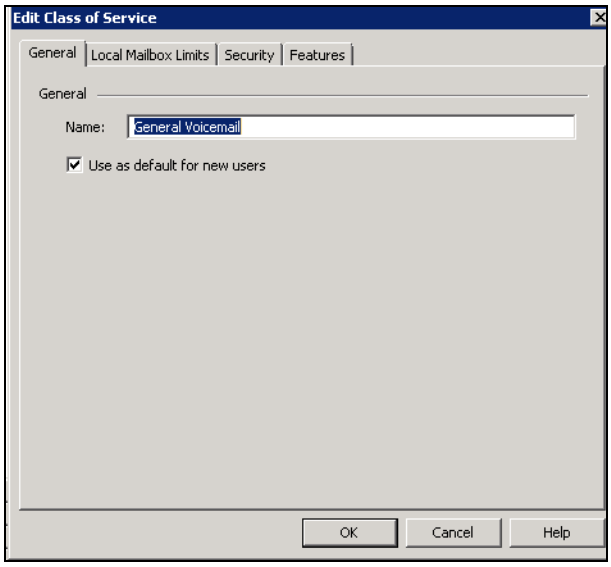
Editing the User CoS

The configured user CoS can be edited at any time by following these steps:

1. Select the **Classes of Service** topic from the list in the **Administration** navigation pane. In the CoS summary pane, right-click on the CoS you want to change. Select **Edit** from the drop-down menu.



2. The **Edit Class of Service** dialog box appears. From this dialog box, you can select the appropriate configuration tab for the changes you want to make.



NOTE *For more information about each CoS configuration tab, refer to Configuring the User CoS on page 4.*

3. When you have finished making the changes, select **OK**. The changes are now applied to the CoS and to each user that has that particular CoS applied.

Applying User CoS Settings on an Individual Basis

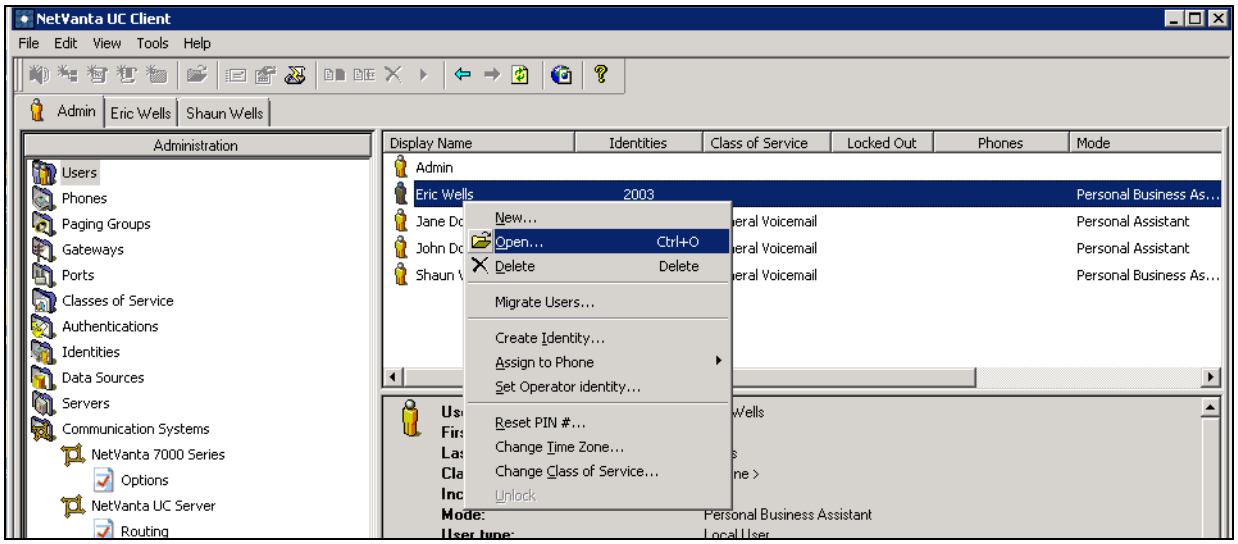
In addition to creating a single CoS to apply to multiple users, each feature of the CoS can be applied individually. These settings include local mailbox limits, password and PIN rules, user account authentication lockout behavior, and which UC server features are available to the user. Applying these features on an individual basis allows you to create individualized settings for the CoS features when necessary. However, individual settings cannot be used to override an applied CoS. If a different variation of settings is necessary, the user must either be individually configured, or a new CoS with the desired settings must be created and applied to the user. To apply particular feature settings to an individual user, follow these steps.

NOTE *If the user you want to update has a CoS assigned, you must remove that CoS before attempting to change individual CoS settings. You can do this by setting the user's CoS to **<None>**. If a CoS other than **<None>** is applied to the user, the features covered in the CoS will not be available for configuration.*

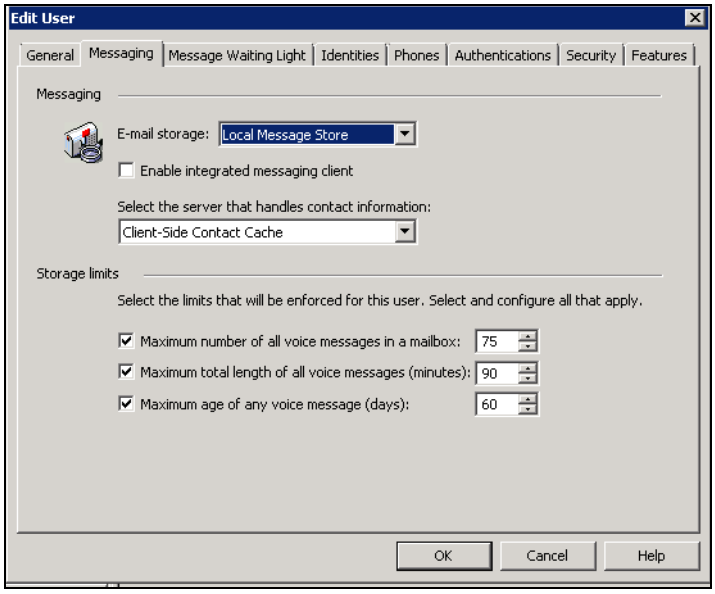
Setting the Local Mailbox Limits

To specify the local mailbox limits and settings for an individual user, follow these steps:

1. Select the **Users** topic from the list in the **Administration** navigation pane. In the **Users** summary pane, right-click on the user you want to edit and select **Open** from the drop-down menu.



2. When the **Edit User** dialog box opens, navigate to the **Messaging** tab. In the lower portion of the menu, you can enable each mailbox limit by selecting the check box next to the appropriate option. You can also specify these limits by entering the appropriate value in the field next to the option.



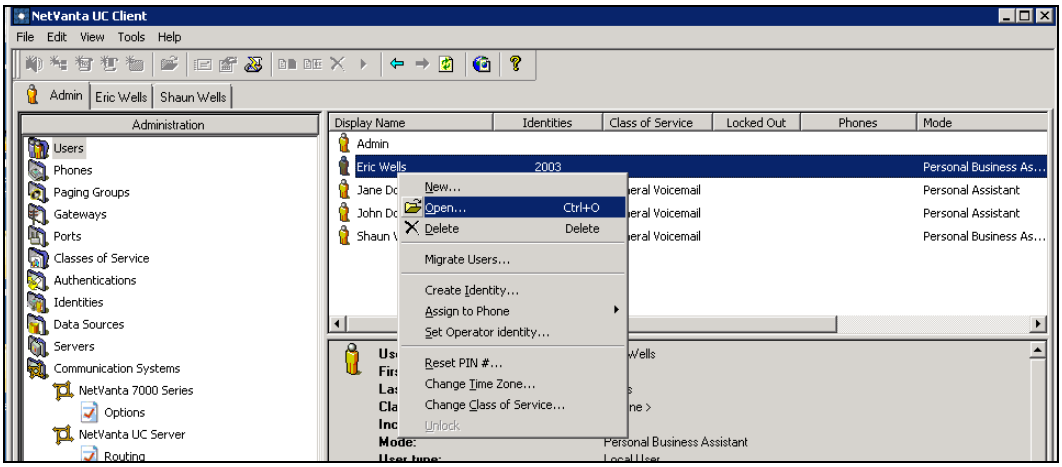
By default, all mailbox limits are disabled. When enabled, the maximum number of voice messages allowed in the mailbox defaults to **100** messages. The valid maximum message range is **1** to **9999**. When enabled, the maximum combined length of voicemail messages defaults to **120** minutes. The valid maximum message length range is **1** to **9999** minutes. When enabled, the maximum storage time for voicemail messages defaults to **90** days. The valid storage range is **1** to **9999** days.

3. When you have adjusted the local mailbox limit settings, select **OK** to apply the changes to the user and close the **Edit User** dialog box.

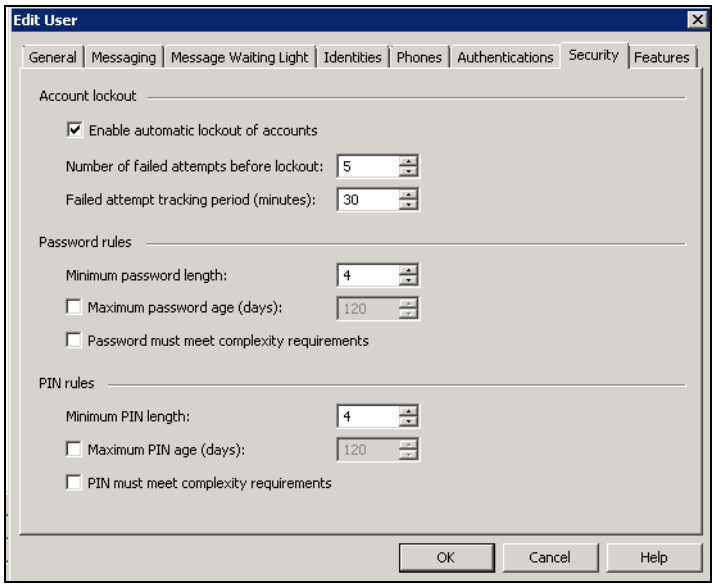
Setting the Password and PIN Rules

To specify the password and PIN rules for an individual user, follow these steps:

1. Select the **Users** topic from the list in the **Administration** navigation pane. In the **Users** summary pane, right-click on the user you want to edit and select **Open** from the drop-down menu.



2. When the **Edit User** dialog box opens, navigate to the **Security** tab. In this menu, you can specify the maximum and minimum password and PIN lengths, the frequency with which passwords and PINs must be changed, and enable the complexity rules for passwords and PINs. Each setting is enabled by selecting the check box next to the desired option and entering a value (where appropriate).



By default, complexity rules for both passwords and PINs are enabled. *Table 1 on page 9* outlines the complexity rules for both passwords and PINs.

By default, the maximum password length is **128** characters and the minimum is **4**. The valid password length range is **4** to **128** characters.

By default, the maximum PIN length is **15** characters, and the minimum length is **4**. The valid range for PIN length is **4** to **15** characters.

By default, passwords and PINs can be used indefinitely. To specify that passwords or PINs are changed after a certain amount of time, enter the number of days until the next password or PIN change is required. The valid range is **1** to **9999** days, or an unlimited number of days.

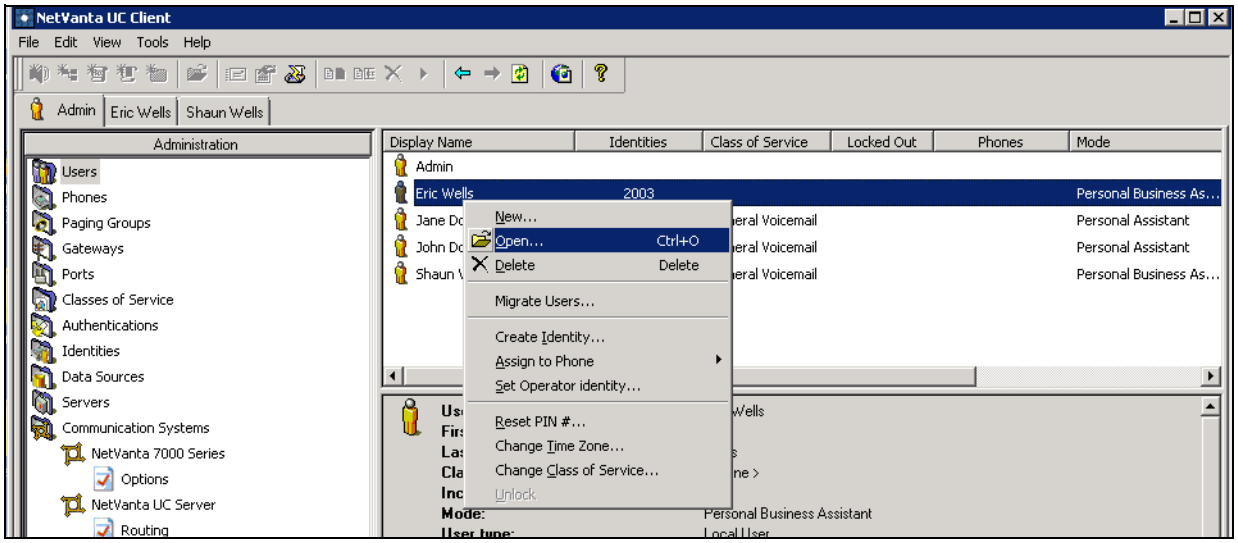
*There are special rules for administrator passwords/PINs and for administratively reset passwords/PINs. By default, the administrator account does not have to follow password or PIN complexity rules; its passwords and PINs can be used indefinitely, and the minimum password/PIN length is set to **4**. When the administrator resets a user password or PIN, the complexity rules are not enforced. In addition, administrators can choose to force the user to change their password/PIN upon their next attempt to login to the system by selecting the appropriate check box when resetting the user password/PIN.*

3. When you have adjusted the password and PIN settings, select **OK** to apply the changes to the user and close the **Edit User** dialog box.

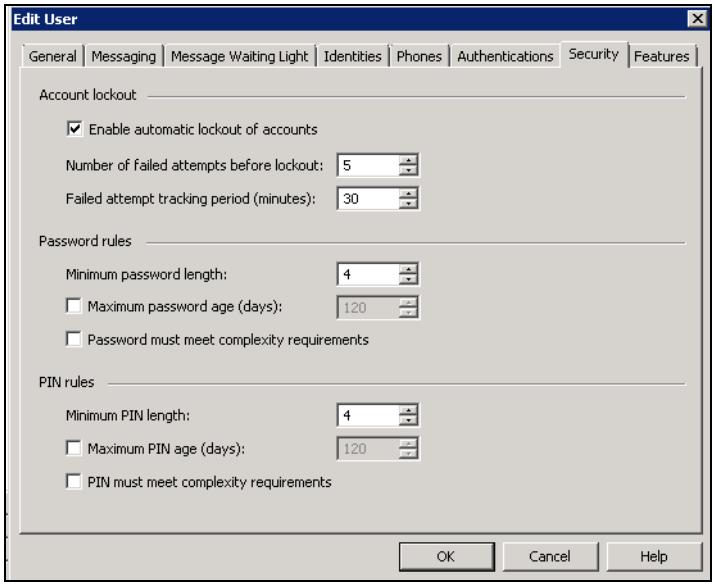
Setting the User Account Authentication Lockout Behavior

To specify the authentication lockout behavior for an individual user, follow these steps:

1. Select the **Users** topic from the list in the **Administration** navigation pane. In the **Users** summary pane, right-click on the user you want to edit and select **Open** from the drop-down menu.



2. When the **Edit User** dialog box opens, navigate to the **Security** tab. From this menu, you can enable the automatic lockout of accounts (by selecting the check box), specify the number of failed login attempts allowed before the lockout, and specify the tracking time for failed attempts.



By default, automatic lockout of accounts after a number of failed login attempts is enabled. You can disable this feature by selecting the check box next to the option. In addition, you can specify the number of failed attempts that are allowed before a lockout occurs by entering the number in the appropriate field. By default, a lockout occurs after **5** failed attempts. The valid attempt range is **1** to **99**.

The user authentication lockout is tracked for a specified number of minutes. This setting specifies the time period in which failed attempts are logged and counted against the maximum allowed number of failed attempts. When the time period ends, the tracked number of failed attempts is reset and begins again. By default, login attempts are tracked for **30** minutes. The valid tracking range is **1** to **525600** minutes (1 year). Even if a successful login attempt occurs during this time period, after a number of failed login attempts, the logged number of failed attempts is not reset until the tracking time period expires.

*If a user is locked out, their locked out status is reflected in the **Locked Out** column of the **Users** summary pane. If you need to reset the user's authentication status, right-click on the user's name in the **Users** summary pane and select **Unlock Authentication**.*

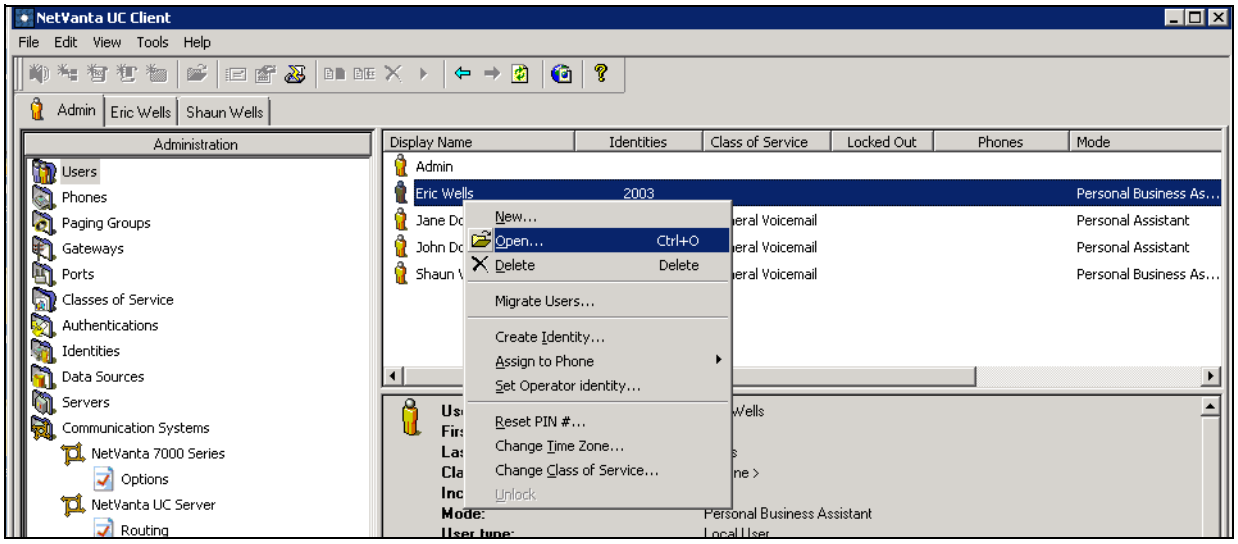
*If automatic lockouts are enabled, users will be locked out of the account after the configured number of failed attempts in the defined period. Regardless of whether automatic lockouts are enabled, users only have a maximum of **3** sequential attempts to log into the system before the system terminates access. This access termination does not in and of itself cause account lockout.*

3. When you have adjusted the authentication lockout settings, select **OK** to apply the changes to the user, and close the **Edit User** dialog box.

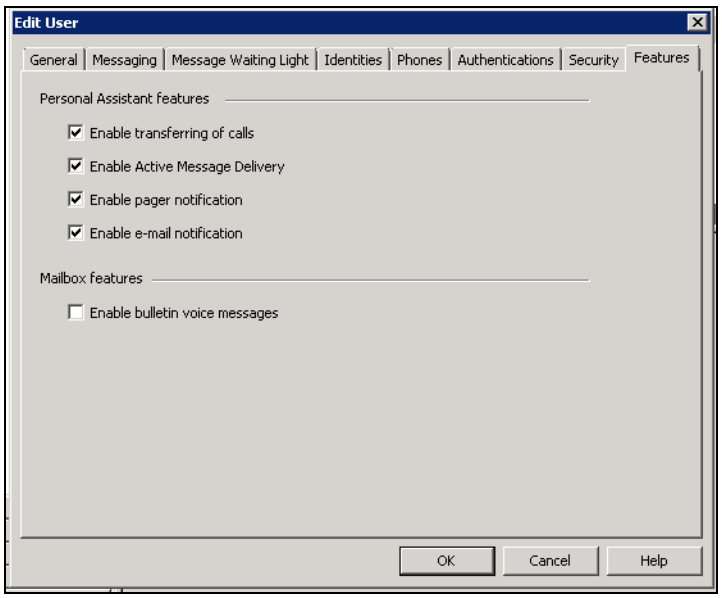
Setting the User Permissions to Access UC Server Features

To specify the UC server features available to an individual user, follow these steps:

1. Select the **Users** topic from the list in the **Administration** navigation pane. In the **Users** summary pane, right-click on the user you want to edit and select **Open** from the drop-down menu.



2. When the **Edit User** dialog box opens, navigate to the **Features** tab. From this menu, you can specify that users have access to transferring calls, using AMD, and pager and email message notifications in the NetVanta UC Server Personal Assistant, as well as that users can create and send bulletin voice messages.



By default, all Personal Assistant features are user accessible. By default, users cannot create bulletin voice messages. Select the check box next to each feature to enable user access of that feature. If you do not want users to access a certain feature, clear the check box next to that feature.

3. When you have adjusted the user permission settings, select **OK** to apply the changes to the user and close the **Edit User** dialog box.

