



AT&T Business Messaging Account Management

Administrator User Guide

March 2018



Copyright

© 2018 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.



About this Guide

Welcome to the AT&T Business Messaging Account Management Administrator User Guide! This guide is a resource for using AT&T Business Messaging Account Management. If you need assistance as you work your way through this guide, please contact Customer Support.

Updates

New editions of this guide contain information about functionality that has been revised or added *since the previous edition*. For details about changes, see *What's New (page 4)*.

Finding Information

This user guide contains a variety of types of topics, including step-by-step instructions, general information, tips, and descriptions of features and functions.

Features and Functions

This guide may describe features and functions that are not present in your software or your service agreement. Contact your account representative to learn more about what is available with this product.



What's New

Date	Notes
February 2015	Added Getting Started.
April 2015	Added information on adding users who are not AT&T customers. Added instructions for adding multiple users at one time. Added User Messages section.
June 2015	Updated Seat License Administrator functionality. Added Enterprise Administrator functionality. Added instructions for Enterprise Administrators, such as seat license information, PIN policies, security policies, and password policies. Added tables that describe columns for various screens. Added Audit Reports section for Enterprise Administrators. Added instructions for remotely wiping a user's mobile phone or tablet. Added error messages specific to the Administrator.
August 2015	Added instructions for enabling secure messaging for new and current users. Updated seat license view information to include viewing the availability of secure user seat licenses.
October 2015	Updated instructions to reflect support for users with data-capable tablets, including both Wi-Fi and LTE tablets. Revised the menu option for sending a test message to a user from "Test" to "Test Text."
December 2015	Updated instructions for adding multiple users to identify secure and non-secure users in the template. Changed the menu option for adding a data-capable tablet user from "Wi-Fi only user" to "Data-capable tablet". Added instructions for suppressing Welcome messages.



Date	Notes
January 2016	Added instructions for setting temporary passwords for new activations. Updated instructions for adding multiple users to specify User name field for each new user entered in the template file. Changed the menu option for sending a test message from “Test Text” to “Test”.
March 2016	Revised all processes and procedures to reflect a newly redesigned user interface.
May 2016	Added information about Corporate Directory Address Book.
July 2016	Added information about Corporate SSO Login.
October 2016	Added Enable Directory Services and Admins able to create users from Directory Services.
January 2017	Support for controlled welcome message.
October 2017	Added features that will allow the admin to set messaging options. Added feature that will allow admin to control access to mobile app and web client.
March 2018	Added feature that allows Enterprise Admin to enable messaging only within the enterprise.



Table of Contents

1. Getting Started	10
<i>What You Need</i>	11
<i>Using the Web Portal</i>	11
<i>Logging In to the Application</i>	12
<i>Corporate Login</i>	14
<i>Creating an Account</i>	16
<i>Resetting a Forgotten Password</i>	17
<i>Logging Out of the Application</i>	18
2. User Administration.....	19
<i>Viewing Activated Users</i>	20
<i>Adding a New User</i>	22
Adding Multiple Users	24
Adding users via Directory Server.....	26
<i>Activating a User</i>	27
Cross Carrier Users.....	28
<i>Editing a Current User</i>	29
<i>Enabling Secure Messaging for a Current User</i>	30
Disabling Secure Messaging for a Current User.....	31
<i>Enabling Secure Messaging for Multiple Users</i>	32
Disabling Secure Messaging for Multiple Users.....	32
<i>Deactivating a User</i>	33
<i>Sending a Test Message to a User</i>	34
<i>Deleting a User</i>	35
<i>Remotely Wiping a User's Mobile Device</i>	36
<i>Suppressing Welcome Messages</i>	38
3. Group Administration	40
<i>Viewing Current Public Groups</i>	41
<i>Adding a New Public Group</i>	42
<i>Activating a Group</i>	43
<i>Editing a Current Group</i>	44
<i>Deactivating a Group</i>	45
<i>Deleting a Group</i>	46
4. Enterprise Administration	47
<i>Viewing the User's Plan Type</i>	48
<i>Setting the PIN Policy for Secure Users</i>	49
PIN Timeout	50
PIN Change Frequency.....	50
PIN Lockout Policy.....	50
<i>Enabling Initiation of Non-Secure Messaging for Secure Users and Setting up Messaging Options</i>	51
<i>Setting the Password Policy for All Users</i>	52
Password Complexity.....	53
Password Lockout Policy.....	53
<i>Corporate Directory Address Book</i>	54



<i>Enterprise Single Sign On</i>	56
<i>Enable Directory Services</i>	60
<i>Allow Messaging Only Within the Enterprise</i>	63
<i>Controlled Welcome Message.....</i>	64
<i>Viewing Seat License Information</i>	65
<i>Viewing Information Per Seat License Administrator.....</i>	67
<i>Updating the Company or Organization Name.....</i>	69
<i>Additional Enterprise Administrator Functionality.....</i>	69
5. Reports.....	70
<i>Messaging Report</i>	71
<i>Accounts Report</i>	72
<i>Daily Report.....</i>	73
<i>Audit Reports</i>	74
<i>Access Report</i>	75
<i>Provisioning Report</i>	76
6. Whitelist Administration.....	77
7. Site Licensing for Business Messaging – FAQ	78
<i>Site Licensing – General FAQ.....</i>	78
<i>Site Licensing – Product FAQ</i>	81
8. User Messages.....	83
9. Error Messages on the Client	86



Figures List

Figure 1. Business Messaging Account Management View (Seat License Administrator View)	10
Figure 2. Login Screen	12
Figure 3. New User Registration Screen	13
Figure 4. Corporate Login Screen Option	14
Figure 5. Sign In Screen (This is a sample login screen and will be based on your enterprise login page)	14
Figure 6. Error Message	15
Figure 7. New User Verification.....	16
Figure 8. Reset Password Screen.....	17
Figure 9. Logout Option	18
Figure 10. Admin Option	20
Figure 11. User Administration Screen (Seat License Administrator View).....	20
Figure 12. User Administration Screen (Enterprise Administrator View)	20
Figure 13. Add a New User.....	23
Figure 14. Add Multiple Users.....	25
Figure 15. Directory Server	27
Figure 16. Activate a User (Seat License Administrator View)	27
Figure 17. Opt-In History Window.....	28
Figure 18. Edit Current User.....	29
Figure 19. Edit User Profile Screen.....	29
Figure 20. Enable Secure Messaging	30
Figure 21. Enable Secure Messaging for Multiple Users	32
Figure 22. Deactivate a User (Seat License Administrator View)	33
Figure 23. Send Test Message to a User (Seat License Administrator View)	34
Figure 24. Delete a User (Seat License Administrator View)	35
Figure 25. Remotely Wipe a User's Mobile Device (Seat License Administrator View)	36
Figure 26. Remote Wipe History Screen	36
Figure 27. Welcome Message Suppression Screen	38
Figure 28. New User Password Settings Screen	39
Figure 29. Group Administration Screen (Enterprise Administrator View)	41
Figure 30. Add a New Public Group	42
Figure 31. Activate a Group (Enterprise Administrator View)	43
Figure 32. Edit the Current Group	44
Figure 33. Edit Group Screen (Enterprise Administrator View)	44
Figure 34. Deactivate a Group (Enterprise Administrator View)	45
Figure 35. Delete a Group (Enterprise Administrator View).....	46
Figure 36. User Administration Screen (Enterprise Administrator View)	48
Figure 37. Set the PIN Policy for Secure Users	49
Figure 38. Enable Non-Secure Messaging	51
Figure 39. Set the Password Policy.....	52
Figure 40. Admin Option	54
Figure 41. Admin Menu.....	54
Figure 42. Corporate Directory Address Book.....	55
Figure 43. Un-check message for Corporate Address Book	55
Figure 44. Admin Option	56
Figure 45. Admin Menu.....	56
Figure 46. Admin Option	56



Figure 47. Admin Menu.....	57
Figure 48. Enterprise Single Sign On Screen.....	58
Figure 49. Admin Option	60
Figure 50. Admin Menu.....	60
Figure 51. Directory Services Screen.....	61
Figure 52. Messaging within the enterprise.....	63
Figure 53. Controlled Welcome Message.....	64
Figure 54. Seat License View Screen	65
Figure 55. User Administration Screen by Seat License Administrator View	67
Figure 56. User Seat Licenses Screen	68
Figure 57. Edit Company or Organization Name for Enterprise Administrator View	69
Figure 58. Messaging Report Screen.....	71
Figure 59. Accounts Report Screen	72
Figure 60. Daily Report Screen	73
Figure 61. Audit Reports Screen.....	74
Figure 62. Access Report.....	75
Figure 63. Provisioning Report	76
Figure 64. Whitelist Administration Screen.....	77

Tables

Table 1. User Administration Field Descriptions	21
Table 2. Cross Carrier User Opt-in Status Values	28
Table 3. Remote Wipe Status Values	37
Table 4. Group Administration Field Descriptions	41
Table 5. User Plan Type Values	48
Table 6. Enterprise Single Sign On	58
Table 7. Enable Directory Services	62
Table 8. Seat License View Field Descriptions	66
Table 9. Access Report Field Descriptions	75
Table 10. Provisioning Report Field Descriptions	76
Table 11. User Messages	83
Table 12. Error Messages on the Client.....	86



1. Getting Started

Users with Business Messaging Account Management (BMAM) access will be able to view the Admin portion of the AT&T Business Notification Center Web portal, including user and group administration, white list administration, security administration, and reports.

Number	Name	E-Mail	Secure Capable	Wireless Operator	Admin Activation Status	Remote Wipe Status	User Optin Status	Test
1231021077	Joe Thomas	tarator333@abv.bg	-	-	Not activated	Not Applicable	Not Applicable	Not tested
1231021078	Peter Walters	tarator555@abv.bg	-	-	Not activated	Not Applicable	Not Applicable	Not tested

Figure 1. Business Messaging Account Management View (Seat License Administrator View)

There are two levels of administrator roles available:

- **Seat License Administrator:** Responsible for managing users, groups and whitelist information. The Seat License Administrator also has access to the Messaging Report, Accounts Report, and Daily Reports.
- **Enterprise Administrator:** Responsible for managing organization settings, such as the PIN policy, security policy, and password policy. The Enterprise Administrator can also view audit reports and information about all the Site License Administrators in a given enterprise. A seat license role can be assigned to an enterprise admin for managing seat licenses.

This guide describes how to perform various administrator tasks, and contains the following sections:

- User Administration (page 19)
- Group Administration (page 40)
- Enterprise Administration (page 47)
- Reports (page 70)
- Whitelist Administration (page 77)
- FAQ (page 78)



What You Need

To use AT&T Business Messaging Account Management you need:

- Desktop computer or tablet (iOS or Android)
- One of the following supported browsers:
Internet Explorer 11+
Google Chrome 37+
Apple Safari
Mozilla Firefox 27

Note: It is recommended that users use the most current versions of their browser for maximum optimization. If an unsupported version of Internet Explorer is used, the user will not be able to log in until they upgrade to one of the supported browsers listed above. For example, if a user tries to log in with Internet Explorer 7, 8, 9, or 10, a message appears to inform them that the browser support has been discontinued and the user should upgrade to the latest browser.

Using the Web Portal

Users of the AT&T Business Notification Center Web portal include:

- Users who can access the Business Notification Center (BNC)
- Users who can access Business Messaging Account Management (BMAM)
- Users who can access BNC and BMAM



Logging In to the Application

You need to log in to the application when you open AT&T Business Messaging Account Management.

1. Open your Internet browser and go to <https://bnc-businessmessaging.att.com/login.do>.
2. Enter your wireless number and password.
3. If you want the application to remember your login information, select **Remember me** option.
4. Click **Login**.

The screenshot shows the login page of the AT&T Business Notification Center. At the top, there's a blue header bar with the AT&T logo and the text "Business Notification Center". Below the header, a large orange banner on the left side says "Welcome to the AT&T Business Notification Center". To the right of the banner is a login form titled "Login with your wireless number". The form includes fields for "Corporate Login" (with a placeholder "Wireless Number" and a "Forgot password?" link), "Password", and "Remember me" (with a checkbox). A "Login" button is at the bottom right of the form. At the very bottom of the page, there's a footer with links to "att.com", "FAQ", "REST APIs", "Terms of Use", "Privacy Policy", and "Contact Us", along with copyright information and a version number "v1.0.1709141546 (r13388)".

Figure 2. Login Screen

5. If this is the first time you are logging in, you will need to complete the registration form. Fields with an asterisk (*) are required.
6. Select the option to accept the terms and agreements for using this application.
7. Click **Submit**.



Business Notification Center

Registration
To create a new account, enter the following information and select "Submit".

Change Password

*Current Password

*New Password

*Re-Type Password

Password Requirements

At least 8 characters
One or more uppercase letters
One or more lowercase letters
One or more numbers
One or more special characters
Does not match any of your previous 5 passwords
No more than two sequential letters or numbers
Password cannot be same as the userID

Messaging Information

*First Name

*Last Name

Contact Information

Work Phone

Home Phone

*E-Mail

Terms and Conditions

AT&T Business Messaging
End User License Agreement

IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE, DO NOT CLICK THE "ACCEPT" BUTTON OR DOWNLOAD, INSTALL, OR USE THE APPLICATION. Your access to and use of the AT&T Business Messaging application ("Application"). This Agreement (the "License") governs Your access to and use of the AT&T Business Messaging application ("Application"). THIS APPLICATION IS NOT INTENDED FOR USE BY PERSONS UNDER THE AGE OF 13. IF YOU ARE UNDER 13 YEARS OLD, YOU MAY NOT USE THIS APPLICATION OR PROVIDE AT&T WITH ANY PERSONALLY IDENTIFIABLE INFORMATION. IF YOU ARE 13 OR OLDER BUT NOT OF LEGAL AGE TO ENTER INTO A CONTRACT, YOU SHOULD REVIEW THESE TERMS AND CONDITIONS WITH YOUR PARENT OR GUARDIAN TO MAKE SURE THAT YOU AND YOUR PARENT OR GUARDIAN UNDERSTAND THESE TERMS AND CONDITIONS. BY CLICKING THE "ACCEPT" BUTTON OR DOWNLOADING OR USING THE APPLICATION, YOU AFFIRM THAT YOU HAVE READ AND AGREE TO THESE TERMS AND CONDITIONS.

AT&T Acceptable Use Policy [AT&T Acceptable Use Policy](#)

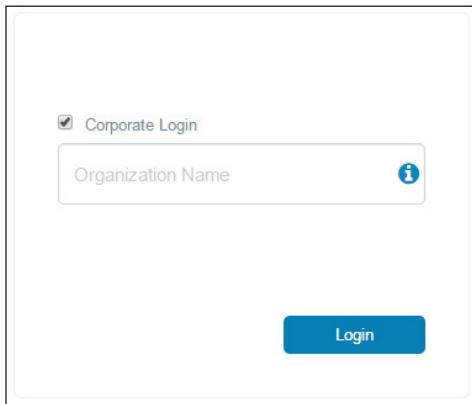
Submit or **Cancel**

Figure 3. New User Registration Screen



Corporate Login

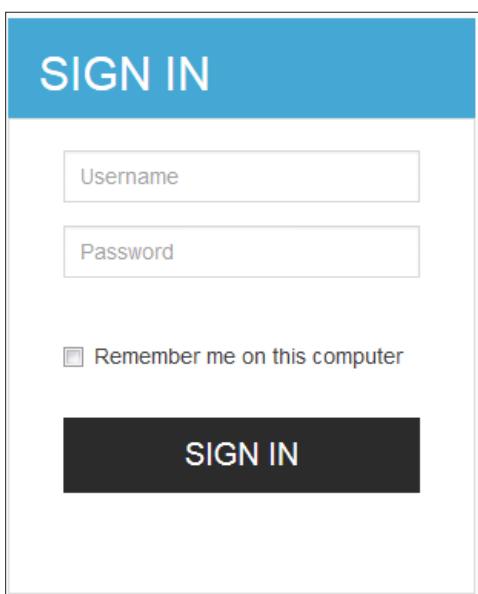
1. If you want to login using Corporate SSO, check the **Corporate Login** option.
2. Enter the **Organization Name**.
3. Click **Login**.



A screenshot of a login interface. At the top left is a checked checkbox labeled "Corporate Login". Below it is a text input field labeled "Organization Name" with a small blue information icon to its right. At the bottom center is a blue "Login" button.

Figure 4. Corporate Login Screen Option

4. You will be required to enter the **Username** and **Password** on the next screen.
5. Click **SIGN IN**



A screenshot of a "SIGN IN" page. The title "SIGN IN" is at the top in a blue bar. Below it are two text input fields: one for "Username" and one for "Password". Underneath the password field is a checkbox labeled "Remember me on this computer". At the bottom is a large black "SIGN IN" button with the words "SIGN IN" in white.

Figure 5. Sign In Screen (This is a sample login screen and will be based on your enterprise login page)

6. You will be prompted to the Conversations screen.

**Notes:**

- You can obtain the Organization Name from your Welcome Message. If you do not find it there, please contact your Enterprise Admin to get the organization name.
- If you enter an invalid Organization Name, you will receive the following error:



Figure 6. Error Message

- If access is denied you will receive the following error message: "Your account is not provisioned to access Business Notification Center. Please reach out to your Enterprise Admin to provision your account."



Creating an Account

You must create an account before you can use the AT&T Business Messaging Account Management.

1. On the Login screen, click **New User**.
 2. Enter your wireless number.
 3. Click **Verify**.
 4. Click **Submit**.
- If your account is successfully created, a message stating that your account has been successfully activated for AT&T Business Messaging Account Management appears. Log in using your password or click the **Forgot password?** option (page 17) to reset your password.
 - If your wireless number is not a provisioned account, a message stating that the user is not provisioned will appear.
 - If you are an SMS user, a message stating that the wireless number must have a qualified AT&T Business Messaging Account feature added to your wireless device account appears.
 - If you are a new IP messaging user who has not yet registered, a message appears indicating that a new PIN has been sent to the handset.

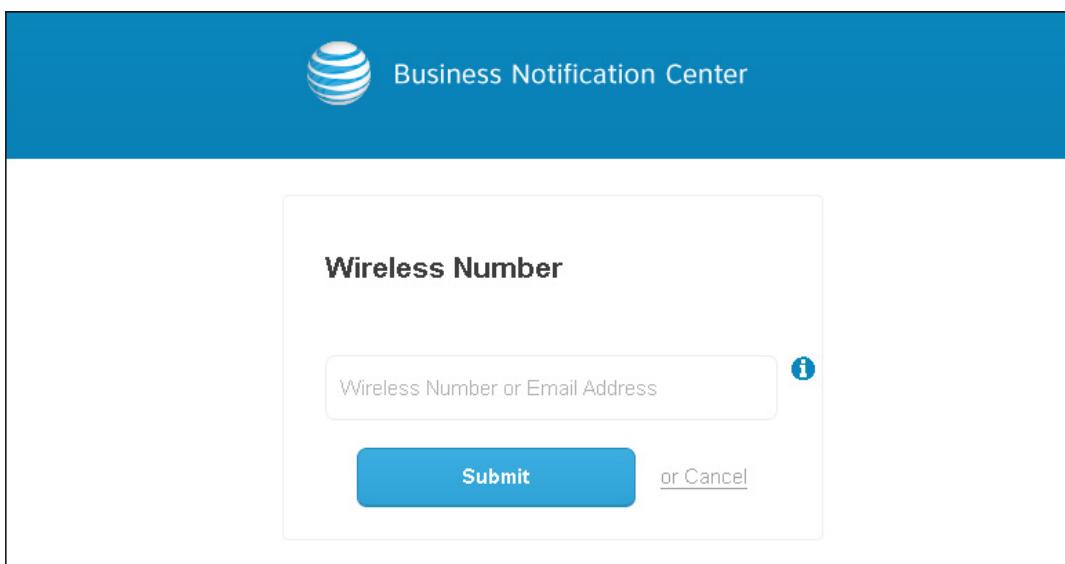
A screenshot of a web-based application titled "Business Notification Center". The main heading is "Create AT&T Business Messaging Account". Below it, a message reads: "We need to validate your account to create a AT&T Business Messaging account. Please enter your wireless number below and click "Verify" below." There is a text input field labeled "Wireless Number or Email Address" with a small info icon (i) to its right. Below the input field are two large blue buttons: "Verify" on top and "Cancel" on the bottom.

Figure 7. New User Verification



Resetting a Forgotten Password

1. On the Login screen, click the **Forgot password?** option.
2. When the Reset Password screen appears, enter your wireless number if it doesn't already appear in the *Wireless Number* field.
3. Click **Submit**. A new password will be sent to you as a text message.
4. Log in using the new password.



The image shows a screenshot of the AT&T Business Notification Center's Reset Password screen. At the top, there is a dark blue header bar with the AT&T logo on the left and the text "Business Notification Center" on the right. Below the header is a white content area. In the center of this area, there is a form titled "Wireless Number". Inside the form, there is a text input field labeled "Wireless Number or Email Address" with a small blue information icon to its right. Below the input field are two buttons: a blue "Submit" button on the left and a link "or Cancel" on the right. The entire interface has a clean, modern design with a white background and blue accents.

Figure 8. Reset Password Screen



Logging Out of the Application

1. In the top right-hand corner of the screen, click the icon for your user ID.
2. Select the **Logout** option at the bottom of the panel that appears.
3. Verify that you want to log out of the application by clicking **Yes** in the confirmation message that appears.

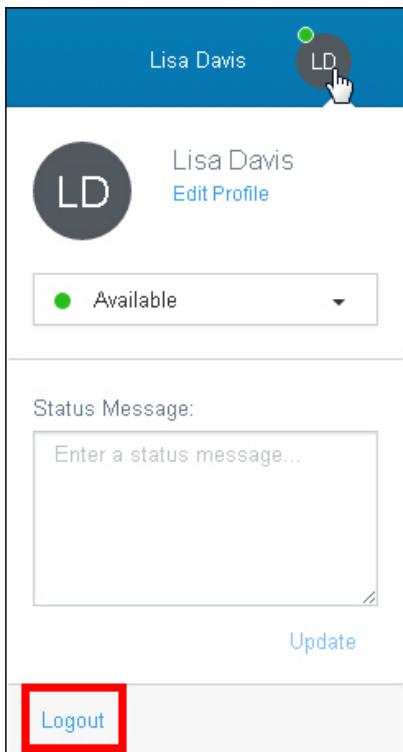


Figure 9. Logout Option



2. User Administration

This chapter describes how to perform the tasks listed below. These tasks are typically performed by the Seat License Administrator.

- Viewing Activated Users (page 20)
- Adding a New User (page 22)
- Activating a User (page 27)
- Editing a Current User (page 29)
- Enabling Secure Messaging for a Current User (page 30)
- Enabling Secure Messaging for Multiple Users (page 32)
- Deactivating a User (page 33)
- Sending a Test Text Message to a User (page 34)
- Deleting a User (page 35)
- Remotely Wiping a User's Mobile Device (page 36)
- Suppressing Welcome Messages (page 38)
- Setting Temporary Passwords for New Activations (page 39)



Viewing Activated Users

Administrators have the ability to provision both AT&T and non-AT&T MDNs (for US operators only).

1. Select the **Admin** option on the left side of the screen, and then select **Users**.



Figure 10. Admin Option

2. On the User Administration screen, a list of current, activated users appears.

Manage features + New User									
Seat Licenses									
	Number	Name	E-Mail	Secure Capable	Wireless Operator	Admin Activation Status	Remote Wipe Status	User Optin Status	Test
<input type="checkbox"/>	1231021077	Joe Thomas	tarator333@abv.bg	<input type="checkbox"/>	-	Not activated	Not Applicable	Not Applicable	Not tested
<input type="checkbox"/>	1231021078	Peter Walters	tarator555@abv.bg	<input type="checkbox"/>	-	Not activated	Not Applicable	Not Applicable	Not tested

Figure 11. User Administration Screen (Seat License Administrator View)

Manage features + New User									
Seat Licenses									
	Number	Name	Plan Type	E-Mail	Secure Capable	Wireless Operator	Admin Activation Status	Remote Wipe Status	User Optin Status
<input type="checkbox"/>	5673456704	Lisa Davis	Bulk - Admin	jdoe@tbd.com	<input checked="" type="checkbox"/>	AT&T Wireless	Activated	Not Applicable	Not Initiated
<input type="checkbox"/>	5673456714	Mark Wilson	Bulk - Admin	jdoe@tbd.com	<input type="checkbox"/>	T-Mobile USA Inc.	Not Activated	Not Applicable	NA
<input type="checkbox"/>	5673456715	James Thomas	Bulk - Admin	jdoe@tbd.com	<input type="checkbox"/>	Verizon Wireless	NA	Not Applicable	Opted Out
<input type="checkbox"/>	5673456716	Jane Matthews	Bulk - Admin	jdoe@tbd.com	<input type="checkbox"/>	Sprint Spectrum L.P.	NA	Not Applicable	NA
<input type="checkbox"/>	7892345678	Marsha Watson	Bulk - Admin	jdoe@tbd.com	<input type="checkbox"/>	AT&T Wireless	Activated	Not Applicable	NA

Figure 12. User Administration Screen (Enterprise Administrator View)

**Table 1. User Administration Field Descriptions**

Field	Description
Number	The mobile directory number for the user. This is the Account ID for the Business Messaging application. For Enterprise Administrators, this number is hyperlinked if the selected user is a Seat License Administrator. Selecting this link opens the Seat License View screen, as described on page 65. The system-generated mobile number for data-capable tablet users also appears in this column.
Name	The name of the user.
Plan Type	(Visible to Enterprise Administrators only) The means through which a user was provisioned to Business Messaging. For more information, see Table 5. User Plan Type Values (page 48).
Email	The email address associated with the account.
Secure Capable	This checkbox indicates that the user was provisioned with the Secure Messaging feature. See page 30 for more information.
Wireless Operator	The wireless operator to which the user's phone number is subscribed. No operators appear in this field for data-capable tablet users. Instead, this field is populated with “-”.
Admin Activation Status	The activation status for the user's phone number. For more information, see <i>Activating a User</i> (page 27).
Remote Wipe Status	Indicates whether the Administrator has removed the Business Messaging service from the user's mobile device using remote wipe functionality as described on page 36.
User Opt-in Status	Indicates whether the user has opted in to the Business Messaging service. This field only applies to cross carrier users. For more information, see Table 2. Cross Carrier User Opt-in Status Values (page 28).
Test	Indicates whether a test message has been sent to the user. For more information, see <i>Sending a Test Message to a User</i> (page 34). Note: This option is not available to users who are using data-capable tablets without a mobile number associated with their account.



Adding a New User

1. On the User Administration screen, click the **+ New User**.
2. Select the **Single** option for the number of users to add. To add multiple users at one time, see *Adding Multiple Users (page 24)*.
3. To enable secure messaging, select the **Secure user** option. If the Administrator does not have secure licenses available, then this option will be unavailable.
4. Complete the user profile. Required fields are indicated with a icon.
 - If the user has a mobile number, then the *Mobile Number* field is required. Carrier information appears to the right of the mobile number.
 - If the user is a data-capable tablet user (without a mobile number associated with their account), select the **Data-capable tablet** option and enter the business email address. In the case of a data-capable tablet user, the email address is required and the *Mobile Number* field is unavailable.

Note: Data capable tablets cover both Wi-Fi and LTE devices.

5. Click **Save Changes**. The User Administration screen appears.

Note: For data-capable tablet users, a message appears with a system-generated mobile number. After clicking **OK**, the user will receive an email welcome message that includes a one-time password.

6. The Seat License Admin has a new field to allow “Mobile app and web client access”. Selecting this field allows users to login to mobile app and web application. If this option is not selected, then the users will not be able to access these. The default option is to allow access.



The screenshot shows a user interface for adding a new user. At the top, there is a section for 'Number of Users' with three radio button options: 'Single' (selected), 'Multiple', and 'Directory Server'. Below this is a section for 'Additional Features' with two checkboxes: 'Secure user' (unchecked) and 'Mobile app and web user' (checked). A red box highlights the checked checkbox. There is also a 'Data-capable Tablet' checkbox which is unchecked. To the right of the tablet checkbox is a small blue circular icon with a white question mark. Below these sections are several input fields with placeholder text: 'Mobile Number' (1234567890), 'First Name' (Robert), 'Last Name' (Jefferson), 'Business E-Mail' (example@att.com), and 'Personal E-Mail' (empty). On the far right, the text 'Wireless Operator' is visible. The entire form is contained within a light gray rectangular border.

Figure 13. Add a New User

If you select the **Activate Automatically** option, you will not need to activate the user separately as described on page 27.

If you select this option for a non-AT&T customer, the user will receive an SMS message asking them to opt in to the service. The user will appear with an “Opt-in Pending” status on the User Administration screen until they respond with a positive keyword such as “START” or “YES”, via SMS.

The user can choose to opt out of the service by sending a keyword such as “STOP”, “CANCEL”, or “END” via SMS.

The Opt-in message expires after 30 days if the user does not respond to the opt-in message.

Data-capable tablet users will not receive opt-in messages via SMS. A welcome message is sent via email upon provisioning.



Adding Multiple Users

1. On the User Administration screen, click **+ New User**.
2. Select the **Multiple** option for the number of users to add.
3. If you haven't already done so, download the template by clicking the **Please use this template to ensure correct format** link.
4. Complete the template. The Username (Phone Number/Email Address) column is required. This field must be entered with the phone number for mobile device users and the email address for data-capable tablet users.

For data-capable tablet users (without a mobile number associated with their account), select the **Data-capable tablet** option. Files cannot contain both mobile users and data-capable tablet users. To upload a file of data-capable tablet users, please enter the business email address for each user in the Email Address column.

Note: CSV template files are different for BNC users and Admin users. The Username (Phone Number/Email Address) column is required for both. A banner appears briefly to inform Administrators that there has been a change to both template files. It appears the first time the Administrator logs in after a template change.

Note: If the Data-capable tablet user option has been selected, any MDNs within the file will be ignored.

Note: The Admin has an option to allow mobile app and web client access in the bulk upload template. In the “Mobile app and web access” column, the admin can enter “Yes” to indicate that the user will receive access to these clients. Indicating “No” will not provide access to the clients.

In the *Secure User* column in the template, enter “Yes” for secure users and “No” for non-secure users. If this column is blank, the system will default to a non-secure user.

Upon upload, the system verifies that you have a sufficient number of secure and non-secure seat licenses. For example, if you have 25 secure licenses and 75 non-secure licenses available, and you try to upload a file with 30 secure seat licenses and 85 non-secure seat licenses, the upload report will reflect:

25 secure users uploaded successfully
75 non-secure users uploaded successfully
15 unsuccessful

The error report will list all of the MDNs that were unsuccessful.

5. Click **Choose file**.
6. Browse to the appropriate file directory and file that contains the list of users to add.
7. Click **Save Changes**. The User Administration screen appears.

A screenshot of a web-based application interface titled "New User". The form includes fields for selecting the number of users (radio buttons for Single, Multiple, or Directory Server, with "Multiple" selected), a file upload input ("Select file for Upload") with a "Choose file" button and a message stating "No file chosen", and a note "* Please use [this template](#) to ensure correct format." Below these are checkboxes for "Activate Automatically" (with a note "(An opt-in message will be sent via SMS to cross carrier wireless numbers.)") and two buttons: "Save Changes" and "View Last Upload Status".

Figure 14. Add Multiple Users

If you select the **Activate Automatically** option, you will not need to activate each user separately as described on page 27.

If you select this option for a non-AT&T customer, the user will receive an SMS message asking them to opt in to the service. The user will appear with an “Opt-in Pending” status on the User Administration screen until they respond with a positive keyword such as “START” or “YES”, via SMS.

The user can choose to opt out of the service by sending a keyword such as “STOP”, “CANCEL”, or “END” via SMS.

The Opt-in message expires after 30 days if the user does not respond.

Data-capable tablet users will not receive opt-in messages via SMS. A welcome message is sent via email upon provisioning.



Adding users via Directory Server

1. On the User Administration screen, click **+ New User**.
2. Select the **Directory Server** option.
3. There will be multiple filter criteria available to the admins where they can search users based on their first name, last name, mobile number, email address, city, state, zip code and group name.

Notes:

- The admin can choose to sort users, for example provide the list of all users from a specific group or city, and then sort the users by first name or last name.
 - The Admin can also search for users by first name and then sort them by last name, group name, city, state or zip code.
 - The admin can choose to create a single user or multiple users – can also select all users in the search results (see wireframe).
 - The admin can choose to provide mobile app and web client access to the user. The default option is to allow access.
 - If the Data-capable tablet user option has been selected, the Mobile Number will be ignored.
4. Click on Search based on the search criteria mentioned above.
 5. The users from the directory server will be shown in the Search results.
 6. The admin can select the users and provision them directly via the directory server interface.
 7. Newly created users will show up under Admin > Users tab.



The screenshot shows a form for creating a new user. At the top, there's a radio button group for 'Number of Users' with options 'Single' (selected), 'Multiple', and 'Directory Server'. Below this is a section for 'Additional Features' with two checkboxes: 'Secure user' (unchecked) and 'Mobile app and web user' (checked and highlighted with a red box). The form includes fields for 'Mobile Number' (1234567890), 'First Name' (Robert), 'Last Name' (Jefferson), 'Business E-Mail' (example@att.com), 'Personal E-Mail' (empty), 'Business Address' (Street), 'Service Address' (Street), and ZIP codes. There's also a checkbox for 'Activate Automatically' (unchecked) and a note about opt-in messages via SMS. At the bottom are 'Save Changes' and 'Cancel' buttons.

Figure 15. Directory Server

Activating a User

1. On the User Administration screen, select the appropriate user.
2. Click the **Options** icon that appears in the top right-hand corner of the screen.
3. Select **Activate**.

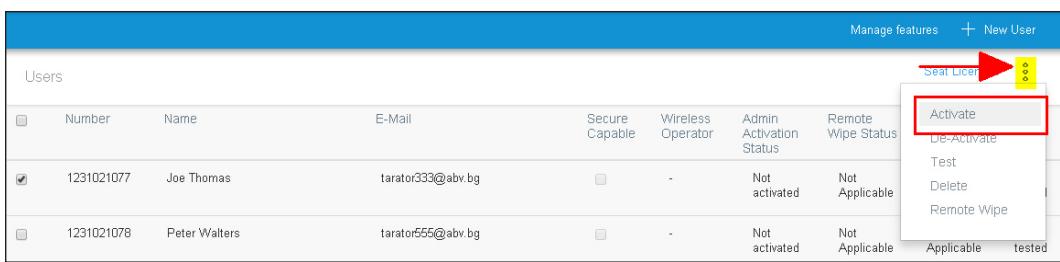


Figure 16. Activate a User (Seat License Administrator View)

Note: Data-capable tablet users will not receive opt-in messages via SMS. A welcome message is sent via email upon provisioning.



Cross Carrier Users

If you activate a user who is not an AT&T customer, the user will receive the following SMS message asking them to opt in to the service.

*AT&T Business Messaging: Reply YES to receive ongoing messages. Msg&Data Rates May Apply.
Msg Freq may vary. Reply STOP to cancel, HELP for help or 1-866-563-4703.*

The user will appear with an “Opt-in Pending” status on the User Administration screen until they respond.

Table 2. Cross Carrier User Opt-in Status Values

Status	Description
Opt-in Pending	SMS message sent to user asking them to opt in to the service.
Opted In	User responds to opt-in message and opts in to the service. System sends a welcome SMS message to the user.
Opted Out	User who previously opted in to the service chooses to opt out or has been deactivated by the Administrator. System sends an SMS message to the user indicating that they have opted out of the service and won't receive additional messages.

To view the opt-in history for a non-AT&T customer, click the linked value in the User Opt-in Status for the appropriate row. Administrators can use this window to manually send the opt-in request SMS message to users whose status is Opt-in Pending or Opted Out users.

The screenshot shows a window titled "History" with a list of opt-in and opt-out events. Each event includes the date and time of the action and the corresponding opt-in or opt-out request sent. At the bottom of the window are two buttons: "Resend Opt-In request" and "Cancel".

Action	Date	Time	Request Sent
Opted-In	10-Apr-2015	14:42:04	10-Apr-2015 14:40:33
Optin Request Sent			
Opted-Out	8-Apr-2015	19:06:45	
Opted-In	2-Apr-2015	01:29:20	
Optin Request Sent			2-Apr-2015 01:27:54
Opted-Out	2-Apr-2015	01:27:54	
Opted-In	25-Mar-2015	16:43:07	
Optin Request Sent			25-Mar-2015 16:42:52
Opted-Out	25-Mar-2015	16:32:56	
Opted-In	25-Mar-2015	15:35:16	
Optin Request Sent			25-Mar-2015 15:34:30

Figure 17. Opt-In History Window



Editing a Current User

1. On the User Administration screen, select the appropriate user.
2. Click the **Options** icon to the left of the user.
3. Select **Edit**.



Figure 18. Edit Current User

4. On the Edit User Profile screen, make the appropriate edits.
5. Click **Save Changes**.

The Edit User Profile screen displays the following fields:

- User Type: Secure user (checkbox)
- Data-capable Tablet: (checkbox)
- *Mobile Number: 3544561004 (text input)
- Wireless Operator: AT&T Wireless (text)
- *First Name: Marsha (text input)
- *Last Name: Thompson (text input)
- Business E-Mail: email@test.com (text input)
- Personal E-Mail: (text input)
- Business Address:
 - Street: (text input)
 - ZIP: (text input)
 - State: (text input)
 - City: (text input)
 - Country: United States (dropdown)
- Service Address:
 - Street: (text input)
 - ZIP: (text input)
 - State: (text input)
 - City: (text input)
 - Country: United States (dropdown)
- Active: (checkbox) Setting Active will also add the user to your address book.
- Save Changes: (button)

Figure 19. Edit User Profile Screen



Enabling Secure Messaging for a Current User

1. On the User Administration screen, select the appropriate user.
2. Click the Options icon to the left of the user.
3. Select **Edit**.
4. On the Edit User Profile screen, select the **Secure user** option. If the Administrator does not have secure licenses available, then this option will be unavailable.
5. Select **Save Changes**.

Edit User

User Type	<input checked="" type="checkbox"/> Secure user	
Data-capable Tablet	<input type="checkbox"/>	
*Mobile Number	3544561004	Wireless Operator: AT&T Wireless
*First Name	Marsha	
*Last Name	Thompson	
Business E-Mail	email@test.com	
Personal E-Mail		
Business Address	Street	City
	ZIP	State
	United States ▾	
Service Address	Street	City
	ZIP	State
	United States ▾	
<input type="checkbox"/> Active	Setting Active will also add the user to your address book.	
Save Changes		

Figure 20. Enable Secure Messaging



Disabling Secure Messaging for a Current User

1. On the User Administration screen, select the appropriate user.
2. Click the **Options** icon to the left of the user.
3. Select **Edit**.
4. On the Edit User Profile screen, deselect the **Secure user** option.
5. Click **Save Changes**.



Enabling Secure Messaging for Multiple Users

1. On the User Administration screen, select the appropriate user(s).
2. Select **Manage Features**.
3. Select **Secure Capable**.
4. Click **Save Changes** at the bottom of the screen.

The screenshot shows a user administration interface with a table of users. The columns are: Number, Name, E-Mail, Secure Capable, Wireless Operator, Admin Activation Status, Remote Wipe Status, User Optin Status, and Test. Two users are selected: Joe Thomas and Peter Walters. Both have their 'Secure Capable' status checked. At the bottom left are 'Save Changes' and 'Cancel' buttons.

Manage features + New User									
Seat Licenses :									
Users									
Number	Name	E-Mail	Secure Capable	Wireless Operator	Admin Activation Status	Remote Wipe Status	User Optin Status	Test	
<input checked="" type="checkbox"/>	1231021077	Joe Thomas	tarator333@abv.bg	<input type="checkbox"/>	-	Not activated	Not Applicable	Not Applicable	Not tested
<input checked="" type="checkbox"/>	1231021078	Peter Walters	tarator555@abv.bg	<input type="checkbox"/>	-	Not activated	Not Applicable	Not Applicable	Not tested

Figure 21. Enable Secure Messaging for Multiple Users

Disabling Secure Messaging for Multiple Users

1. On the User Administration screen, select the appropriate user(s).
2. Click **Manage Features**.
3. Deselect the **Secure Capable** option for each user.
4. Click **Save Changes**.



Deactivating a User

1. On the User Administration screen, select the appropriate user.
2. Click the **Options** icon that appears in the top right-hand corner of the screen.
3. Select **Deactivate**.

The screenshot shows the 'Users' section of the User Administration screen. A red arrow points from the text 'Select the Options icon that appears in the top right-hand corner of the screen.' to the 'Seat License' icon in the top right corner of the table header. A red box highlights the 'De-Activate' option in the dropdown menu that appears when the icon is clicked.

Number	Name	E-Mail	Secure Capable	Wireless Operator	Admin Activation Status	Remote Wipe Status
<input checked="" type="checkbox"/> 1231021077	Joe Thomas	tarator333@abv.bg	<input type="checkbox"/>	-	Not activated	Not Applicable
<input type="checkbox"/> 1231021078	Peter Walters	tarator555@abv.bg	<input type="checkbox"/>	-	Not activated	Not Applicable

Manage features + New User
Seat License
Activate
De-Activate
Test
Delete
Remote Wipe

Figure 22. Deactivate a User (Seat License Administrator View)



Sending a Test Message to a User

Note: This option is not available to users who are using data-capable tablets without a mobile number associated with their account.

1. On the User Administration screen, select the appropriate user.
2. Click the **Options** icon that appears in the top right-hand corner of the screen.
3. Select **Test**. The user receives a test SMS message on their mobile device.
 - Test passed indicates that the user successfully received the test message.
 - Test failed indicates that the user did not receive the test message, for example the user is not activated to receive messages.

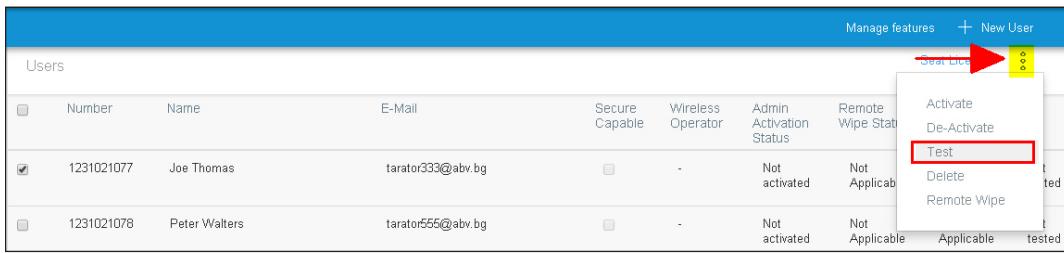


Figure 23. Send Test Message to a User (Seat License Administrator View)



Deleting a User

1. On the User Administration screen, select the appropriate user.
2. Click the **Options** icon that appears in the top right-hand corner of the screen.
3. Select **Delete**.

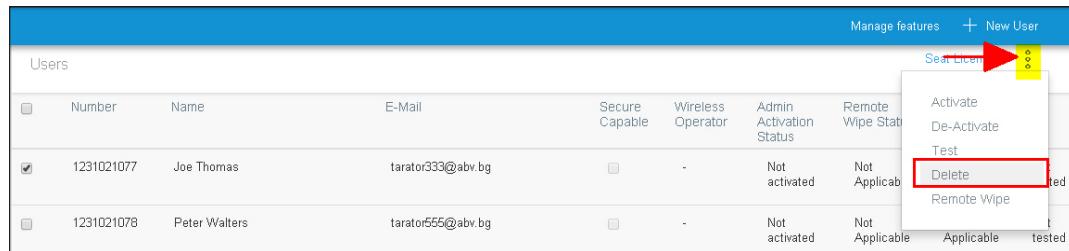


Figure 24. Delete a User (Seat License Administrator View)



Remotely Wiping a User's Mobile Device

The Administrator can remotely remove all Business Messaging data stored on a user's mobile device (phone or tablet). The secure and non-secure data that will be removed includes all messages, attachments, contacts, and groups (private, public, and shared public), user name, password, and PIN.

This process does not apply to AT&T Business Notification Center (Web) accounts. To remove a Web user account, please refer to *Deactivating a User* (page 33).

Note: This task can be completed by Seat License Administrators and Enterprise Administrators.

1. On the User Administration screen, select the appropriate user.
2. Click the **Options** icon that appears in the top right-hand corner of the screen.
3. Select **Remote Wipe**.

The screenshot shows a table of users with columns for Number, Name, E-Mail, Secure Capable, Wireless Operator, Admin Activation Status, and Remote Wipe Status. A red arrow points to the 'Options' icon (three vertical dots) for the user 'Joe Thomas'. A yellow box highlights the 'Remote Wipe' option in the dropdown menu that appears, with a red box around it.

	Number	Name	E-Mail	Secure Capable	Wireless Operator	Admin Activation Status	Remote Wipe Status
<input type="checkbox"/>	1231021077	Joe Thomas	tarator333@abv.bg	<input type="checkbox"/>	-	Not activated	Not Applicable
<input type="checkbox"/>	1231021078	Peter Walters	tarator555@abv.bg	<input type="checkbox"/>	-	Not activated	Not Applicable

Figure 25. Remotely Wipe a User's Mobile Device (Seat License Administrator View)

4. Verify that you want to wipe the device. If a user has multiple devices, the Wipe Devices screen appears. Select the device(s) that should be wiped and click **Wipe Selected Devices**.
5. Once you have initiated the remote wipe, you can view the status by selecting the **Status** hyperlink in the Remote Wipe Status column to view the Remote Wipe History screen.

The screenshot shows a list of devices with their operating system and Business Messenger version, along with their current status. The first item is 'iPhone 5 OS 7.1.2;BusinessMsgr 1.4.6517 - Initiated'. The second item is 'iPhone7,2 OS 8.1.3;BusinessMsgr 1.4.63... - Completed'. The third item is 'iPhone7,2 OS 8.1.3;BusinessMsgr 1.4.63... - Pending'. The fourth item is 'iPhone7,2 OS 8.1.3;BusinessMsgr 1.4.63... - Completed'.

Device	Status
iPhone 5 OS 7.1.2;BusinessMsgr 1.4.6517	- Initiated
iPhone7,2 OS 8.1.3;BusinessMsgr 1.4.63...	- Completed
iPhone7,2 OS 8.1.3;BusinessMsgr 1.4.63...	- Pending
iPhone7,2 OS 8.1.3;BusinessMsgr 1.4.63...	- Completed

Figure 26. Remote Wipe History Screen



The Remote Wipe Status column on the Users screen indicates the status of the wipe as described in the table below.

Table 3. Remote Wipe Status Values

Status	Description
Not Applicable	Indicates that a remote wipe has never been attempted on the account.
Status	Indicates that a remote wipe has been attempted at least one time on the account. This value is a hyperlink that enables the Administrator to view the wipe history. <ul style="list-style-type: none">• Initiated: Indicates that the remote wipe has been initiated.• Pending: Indicates that the mobile device was switched off or unavailable. The wipe will take place automatically when the device is available.• Successful: Indicates that the remote wipe has been successfully completed.• Failed: Indicates that the remote wipe failed.

If the user is using the application on their mobile device when the wipe takes place, a message appears indicating that configuration of the application is in progress and they will not be able to interrupt the process.

When the user tries to log in following a successful wipe, they will be presented with the Login screen. When they attempt to log in, the following message appears:

A remote wipe request for the Business Messaging application on this device has been executed. If you have any questions about this action, please contact your Business Administrator for additional information about this remote wipe.



Suppressing Welcome Messages

The Administrator can opt to suppress the Welcome messages that are sent to new users. When enabled, welcome message and temporary passwords are not sent to users upon activation.

The Welcome message normally contains a temporary password that users need if they intend to use the Business Notification Center on the Web or the Business Messenger application on mobile devices. Users can still obtain a password by clicking the **Forgot password?** option on the Login page of the mobile application or Web portal.

Note: Opt-in messages will still be sent to new cross carrier users. These users must consent to receive messages from the system before they can receive any messages.

1. Select the **Admin** option on the left of the screen, and then select **Suppress welcome message**.
2. On the Welcome message suppression screen, select the **Suppress welcome message** option.
3. Click **Save Changes**. A confirmation message appears.

The screenshot shows a user interface for managing welcome message suppression. At the top, it says "Welcome message suppression". Below that, there is a section titled "Suppress welcome message" with a checked checkbox. Underneath this, a note says "When you suppress welcome messages:" followed by two bullet points explaining the consequences. At the bottom is a blue "Save Changes" button.

Suppress welcome message	<input checked="" type="checkbox"/>
When you suppress welcome messages:	
<ul style="list-style-type: none">Temporary passwords will not be sent to users when they are activated. The welcome message contains a temporary password users would need if they intend to use the business messaging portal or mobile application. Users can still obtain a password by using the "Forgot Password" feature in the mobile application or web portal.Opt-in messages will still be sent to a new user on a different carrier. These users have to consent to receive messages from the business messaging system before they can receive any API, web portal or mobile application messages.	
Save Changes	

Figure 27. Welcome Message Suppression Screen

To resume sending Welcome messages, deselect the **Suppress welcome message** option and click **Save Changes**.



Setting Temporary Passwords for New Activations

When creating new users, the Administrator can use a system-generated temporary password or enter a static temporary password. Newly activated users will log in to the Web or mobile application with the temporary password and then will be required to change their password.

Note: These settings apply to new activations and re-activation of deactivated users.

1. Select the **Admin** option on the left side of the screen, and then select **New User Password Settings**.
2. On the New User Password Settings screen, select the desired option.
 - **System-generated temporary password for activated users:** This option sends a system-generated, temporary password. A different temporary password is sent to each new user. This is the default option.
 - **Enter a static temporary password for newly activated users:** This option enables the Administrator to set a single, temporary password that will be sent. For this option, enter the desired password and re-enter to confirm the password.
3. Click **Save Changes**. A confirmation message appears.

New User Password Settings

System generated temporary password for activated users

When you select system generated temporary password option
All new users will receive a welcome message that will have a different temporary password. The users will login into the web or mobile app using temporary password. They will be required to change the password on the next screen.

Enter a static temporary password for new activated users

When you select static temporary password option
All new users will receive a welcome message that will have same temporary password. The users will login into the web or mobile app using temporary password. They will be required to change the password on the next screen.

Enter the password

Re-enter the password

Save Changes

Figure 28. New User Password Settings Screen



3. Group Administration

This chapter describes how to perform the tasks listed below. These tasks are typically performed by the Seat License Administrator.

- Viewing Current Public Groups (page 41)
- Adding a New Public Group (page 42)
- Activating a Group (page 43)
- Editing a Current Group 1 (page 44)
- Deactivating a Group (page 45)
- Deleting a Group (page 46)



Viewing Current Public Groups

1. Select the **Admin** option on the left side of the screen, and then select **Groups**. The application is limited to 100 public groups.
2. On the Group Administration screen, a list of groups appears.

Groups				10 of 100 Allowed Groups
	Group Name	Group Owner	Description	Status
<input type="checkbox"/>	NationalAnnouncements	Created by Lisa Davis		Activated
<input type="checkbox"/>	OfficeBroadcasts	Created by Lisa Davis		Activated
<input type="checkbox"/>	PublicBroadcasts	Created by SecureSprint User		Activated

Figure 29. Group Administration Screen (Enterprise Administrator View)

Table 4. Group Administration Field Descriptions

Field	Description
Group Name	The name of the group.
Group Owner	(Visible to Enterprise Administrators only) The owner of the group.
Description	A description for the group.
Status	The status of the group.



Adding a New Public Group

Administrators can create public groups, but cannot create private groups.

1. On the Group Administration screen, click **+ New Group**.
2. Complete the group profile and add users. See *Adding a Contact to an Existing Group* (in the BNC user guide) for more information.
3. Click **Create Group**. The Group Administration screen appears.
4. On the Group Administration screen, select the appropriate group.
5. Click the **Options** icon that appears in the top right-hand corner of the screen.
6. Select **Activate**.

A screenshot of a web-based application interface titled "New Group". The form includes fields for "Group name" (with a note: "Group name should be a uppercase or lowercase alphanumeric, starting with a character."), "Description" (with a note: "Max 400 characters."), and "Add Contacts" (with a search bar: "Search to add contacts"). There is also a checkbox for "Activate Automatically" and a blue "Create group" button at the bottom.

Figure 30. Add a New Public Group

Note: If you select the **Activate Automatically** option, you will not need to activate the user separately as described on page 27.



Activating a Group

1. On the Group Administration screen, select the appropriate group.
2. Click the **Options** icon that appears in the top right-hand corner of the screen.
3. Select **Activate**.

The screenshot shows a table of groups with columns for Group Name, Group Owner, Description, Status, and Actions. A context menu is open over the row for 'NationalAnnouncements', with options 'Activate', 'De-Activate', and 'Delete'. A red arrow points to the 'Activate' button. The status column for 'NationalAnnouncements' shows '11 of 100 Allowed Groups'.

Group Name	Group Owner	Description	Status	Actions
NationalAnnouncements	Lisa Davis		11 of 100 Allowed Groups	<ul style="list-style-type: none">ActivateDe-ActivateDelete
OfficeBroadcasts	Lisa Davis		Activated	
PublicBroadcasts	SecureSprint User		Activated	

Figure 31. Activate a Group (Enterprise Administrator View)



Editing a Current Group

1. On the Group Administration screen, select the appropriate group.
2. Click the **Options** icon to the left of the group name.
3. Select **Edit**.

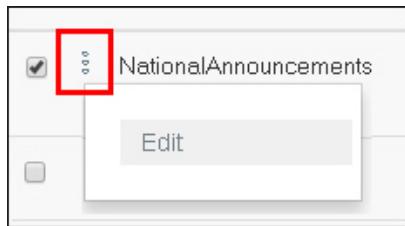


Figure 32. Edit the Current Group

4. On the Edit Group screen, make the appropriate edits.
5. Click **Update group**.

Groups					10 of 100 Allowed Groups
	Group Name	Group Owner	Description	Status	
<input checked="" type="checkbox"/>	NationalAnnouncements	Created by Lisa Davis		Activated	Edit
<input type="checkbox"/>		Created by Lisa Davis		Activated	
<input type="checkbox"/>	PublicBroadcasts	Created by SecureSprint User		Activated	

Figure 33. Edit Group Screen (Enterprise Administrator View)



Deactivating a Group

1. On the Group Administration screen, select the appropriate group.
2. Click the **Options** icon that appears in the top right-hand corner of the screen.
3. Click **De-Activate**.

The screenshot shows a table of groups. The first row, 'NationalAnnouncements', has a checked checkbox. A red arrow points to the 'De-Activate' button in the 'Options' menu for this row. The table columns are: Group Name, Group Owner, Description, Status, and Action. The status for 'NationalAnnouncements' is 'Activated'.

Group Name	Group Owner	Description	Status	Action
NationalAnnouncements	Lisa Davis		Activated	Activate De-Activate Delete
OfficeBroadcasts	Lisa Davis		Activated	
PublicBroadcasts	SecureSprint User		Activated	

Figure 34. Deactivate a Group (Enterprise Administrator View)



Deleting a Group

1. On the Group Administration screen, select the appropriate group.
2. Click the **Options** icon that appears in the top right-hand corner of the screen.
3. Click **Delete**.

The screenshot shows a table of groups with columns for Group Name, Group Owner, Description, Status, and Actions. A row for 'NationalAnnouncements' is selected, indicated by a checked checkbox. In the 'Actions' column, a dropdown menu is open, showing options: 'Activate', 'De-Activate', and 'Delete'. The 'Delete' option is highlighted with a red box and has a red arrow pointing to it from the top right.

Groups				
	Group Name	Group Owner	Description	Status
<input type="checkbox"/>	NationalAnnouncements	Created by Lisa Davis		Active
<input type="checkbox"/>	OfficeBroadcasts	Created by Lisa Davis		Activated
<input type="checkbox"/>	PublicBroadcasts	Created by SecureSprint User		Activated

Figure 35. Delete a Group (Enterprise Administrator View)



4. Enterprise Administration

This chapter describes how to perform the tasks listed below. These tasks are performed by the Enterprise Administrator.

- Viewing the User's Plan Type (page 48)
- Setting the PIN Policy for Secure Users (page 49)
- Enabling Initiation of Non-Secure Messaging for Secure Users (page 51)
- Setting the Password Policy for All Users (page 52)
- Corporate Directory Address Book (page 54)
- Enterprise Single Sign On (page Enterprise Single Sign On (page 56))
- Enable Directory Services (page Enable Directory Services (page 60))
- Controlled Welcome Message (page Controlled Welcome Message (page 64))
- Viewing Seat License Information (page 65)
- Viewing Information Per Seat License Administrator (page 67)
- Updating the Company or Organization Name (page 69)
- Additional Enterprise Administrator Functionality (page 69)



Viewing the User's Plan Type

Enterprise Administrators can view the method used to provision a user to Business Messaging on the User Administrator screen.

Note: Refer to Table 1. User Administration Field Descriptions (page 21) for a description of the columns on this screen.

Manage features + New User									
Users Seat Licenses									
	Number	Name	Plan Type	E-Mail	Secure Capable	Wireless Operator	Admin Activation Status	Remote Wipe Status	User Optin Status
<input type="checkbox"/>	5673456704	Lisa Davis	Bulk - Admin	jdoe@tbd.com	<input checked="" type="checkbox"/>	AT&T Wireless	Activated	Not Applicable	Not Initiated
<input type="checkbox"/>	5673456714	Mark Wilson	Bulk - Admin	jdoe@tbd.com	<input type="checkbox"/>	T-Mobile USA Inc.	Not Activated	Not Applicable	NA
<input type="checkbox"/>	5673456715	James Thomas	Bulk - Admin	jdoe@tbd.com	<input type="checkbox"/>	Verizon Wireless	NA	Not Applicable	Opted Out
<input type="checkbox"/>	5673456716	Jane Matthews	Bulk - Admin	jdoe@tbd.com	<input type="checkbox"/>	Sprint Spectrum L.P.	NA	Not Applicable	NA
<input type="checkbox"/>	7892345678	Marsha Watson	Bulk - Admin	jdoe@tbd.com	<input type="checkbox"/>	AT&T Wireless	Activated	Not Applicable	NA

Figure 36. User Administration Screen (Enterprise Administrator View)

Table 5. User Plan Type Values

Plan Type	Description
Individual	Indicates that the user was provisioned by AT&T, but was not provisioned the Seat License Administrator or the Enterprise Administrator.
Bulk – Admin	Indicates that the user provisioned is a Seat License Administrator.
Bulk – Provisioned by	<p>Indicates that the user was provisioned by the Seat License Administrator or the Enterprise Administrator. The name of the appropriate Administrator will be displayed here.</p> <p>Clicking the hyperlinked Administrator name opens the user's information on the User Administration screen. See page 67 for more information.</p> <p>Note: If the Administrator name is not available, the Administrator's MDN will be included. For example, Bulk – Provisioned by 1-813-555-1234.</p>



Setting the PIN Policy for Secure Users

Enterprise Administrators can enable PIN access at the enterprise level for all secure users. If the PIN access is enabled, all secure users in the enterprise will have PIN access. The default setting for PIN access for secure users is ON.

Note: Enterprise Administrators cannot enforce a PIN policy for non-secure users. Non-secure users can enable a PIN specific to their own mobile device.

The PIN should be a four-digit number.

1. Select the **Admin** option on the left side of the screen, and then select **Organization settings**.
2. On the Organization Settings screen, enable PIN access by selecting the **ON** option in the *PIN enabled* field.
3. Select the PIN timeout and the frequency required for a user to change their PIN.

The default setting for PIN timeout is five minutes. See *PIN Timeout* on the following page for more information about changing this value.

The default setting for PIN change frequency is 90 days. See *PIN Change Frequency* on the following page for more information about changing this value.

4. Click **Save Changes**.

The screenshot shows the 'Organization settings' page. At the top right, there is a search bar with placeholder text 'Enter your organization name (please type h...)' and a magnifying glass icon. Below the search bar, the title 'Organization settings' is displayed. In the center of the page, there is a section titled 'PIN Access for secure client users using iOS or Android devices'. This section contains three configuration options:

- 'PIN enabled': A radio button group where the 'ON' option is selected (indicated by a blue outline).
- 'PIN timeout': A dropdown menu set to 'After 60 minutes'.
- 'PIN change frequency': A dropdown menu set to 'After 90 days'.

A red rectangular box highlights this entire section. Below this section, there is a note: 'Secure client users can send / receive secure messages and receive non-secure messages. Secure client users can also reply to existing non-secure messages.' Further down, there is a checkbox labeled 'Initiate new non-secure conversations' which is checked. Under the heading 'Password policy', there is a dropdown menu for 'Password change frequency' set to 'Never expires'. At the bottom of the page is a blue 'Save Changes' button.

Figure 37. Set the PIN Policy for Secure Users



PIN Timeout

The duration of the PIN timeout for all secure users in the enterprise can be set. This duration will require that a user enters a PIN to unlock the mobile application after the selected period of time has passed since they last used it.

The default setting for PIN timeout is five minutes. Valid options include:

- Required immediately
- After one minute
- After five minutes
- After 15 minutes
- After 30 minutes
- After one hour

PIN Change Frequency

This policy determines the frequency with which all secure users in the enterprise must change their PIN for the application. Users will be prompted to enter a new 4-digit PIN when they launch the mobile application.

The default setting for PIN change frequency is 90 days. Valid options include:

- 30 days
- 60 days
- 90 days

If the new PIN that a user enters has been used within the last five occurrences, the following message appears on the mobile device: *"The PIN was used recently. Please use a different PIN."*

PIN Lockout Policy

The PIN lockout policy for all secure users in the enterprise is listed below.

1. If a user enters the wrong PIN in the mobile application, there will be a one-hour lockout after **seven** failed attempts.
2. Following the one-hour lockout, if the user continues to enter the wrong PIN, there will be a 24-hour lockout after **six** failed attempts.
3. Following the 24-hour lockout, if the user continues to enter the wrong PIN, there will be a remote wipe of the data after **six** failed attempts.
4. Following the remote wipe, if the user launches the mobile application, they will be prompted with the Login screen as if they were a new user. Once the user enters the wireless number and password, the user will be prompted to set new PIN for the application.



Enabling Initiation of Non-Secure Messaging for Secure Users and Setting up Messaging Options

Enterprise Administrators can enable non-secure messaging at the enterprise level for all secure users. If initiation of non-secure messaging is enabled, all secure users in the enterprise can initiate non-secure conversations, messaging options “Message Expiration” and “Delete on Read” will be greyed out if the enterprise admin set the messaging policies.

By default, secure users can send and receive secure messages, initiate non-secure conversations, receive non-secure messages, and reply to existing non-secure messages.

1. Select the **Admin** option on the left side of the screen, and then select **Organization settings**.
2. On the Organization Settings screen, select the **Initiate new non-secure conversations** option.
3. Click **Save Changes**.
4. To set the message options that include “Message Expiration” and “Delete on Read”, select the **Message options for secure users**.
5. This will allow the admin to set the “Message Expiration” and “Delete on Read” for all secure users in the enterprise.

The screenshot shows the 'PIN Access for secure client users using iOS or Android devices' section. It includes fields for PIN enabled (ON), PIN timeout (After 5 minutes), and PIN change frequency (After 90 days). Below this, a red box highlights the 'Message options for secure users' section, which contains:

- Enable message options for secure users (checkbox checked)
- Message Expiration (radio buttons: No, Yes - No is selected)
- Delete on Read (checkbox)

Figure 38. Enable Non-Secure Messaging



Setting the Password Policy for All Users

Enterprise Administrators can enable a required password change frequency at the enterprise level for all users. This policy determines the frequency with which all users in the enterprise must change their password for the Business Messaging application.

The default setting for password change frequency is “Never expires”.

1. Select the **Admin** option on the left side of the screen, and then select **Organization settings**.
2. On the Organization Settings screen, select the password change frequency from one of the following options.
 - 30 days
 - 60 days
 - 90 days
 - Never expires
3. Click **Save Changes**.

The screenshot shows the 'Organization settings' page. At the top, there's a search bar with placeholder text 'Enter your organization name (please type h...)' and a pencil icon. Below the search bar, the title 'PIN Access for secure client users using iOS or Android devices' is displayed. Under this title, there are three settings: 'PIN enabled' (radio button selected for 'ON'), 'PIN timeout' (dropdown set to 'After 60 minutes'), and 'PIN change frequency' (dropdown set to 'After 90 days'). A note below these says: 'Secure client users can send / receive secure messages and receive non-secure messages. Secure client users can also reply to existing non-secure messages.' There is a checkbox for 'Initiate new non-secure conversations'. The 'Password policy' section is highlighted with a red box. It contains a dropdown for 'Password change frequency' which is set to 'Never expires'. At the bottom of the form is a blue 'Save Changes' button.

Figure 39. Set the Password Policy



Password Complexity

- Passwords must contain at least one uppercase letter.
- Passwords must contain at least one lowercase letter.
- Passwords must contain at least one numeric character.
- Passwords must contain at least one special character.
- Passwords must not match one of the five previous passwords.
- Passwords must not contain more than two sequential numbers or letters.
- Passwords must be at least eight characters long.
- Passwords must not match the User ID.

Password Lockout Policy

The password lockout policy for all users in the enterprise is listed below.

1. If a user enters the wrong password in the mobile application, there will be a one-hour lockout after **seven** failed attempts.
2. Following the one-hour lockout, if the user continues to enter the wrong password, there will be a 24-hour lockout after **six** failed attempts.
3. Following the 24-hour lockout, if the user continues to enter the wrong password, the account will be locked. The user can click the **Forgot password?** option on the Login screen to obtain a confirmation number that allows them to create a new password and log in to the application.



Corporate Directory Address Book

1. Select the **Admin** arrow from the menu on the left side of the screen. The **Admin** submenu opens.



Figure 40. Admin Option

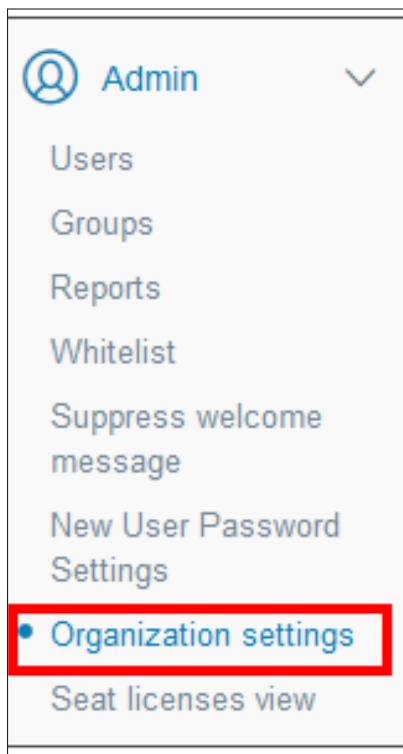


Figure 41. Admin Menu

2. Select **Organization settings** option. The **Organization settings** screen opens.
3. Scroll down the screen and the **Enable Corporate Address Book Sync** checkbox appears automatically.



Corporate Directory Address Book

Enable Corporate Address Book Sync

Selecting this option will populate all enterprise users in the enterprise as contacts in the users address book. All the entries will be removed from users' corporate address book once this option is un-checked.

Save Changes

Figure 42. Corporate Directory Address Book

Notes:

- The checkbox will be selected by default.
- If the checkbox is not selected, then no users will be populated in users address book.
- If the checkbox is selected, then un-checked, all the users in this scenario will be removed from the users address book.
- If the checkbox is selected and the Enterprise Admin unchecks it, there will be a pop up shown to the Admin:

"This action will remove all entries from users' corporate address book. You will not be able to select this option again for next 24 hours."

- Similarly, if the checkbox was not selected and the Enterprise Admin checks it, there will be a pop up shown to the Enterprise Admin:

"This action will add entries in users' corporate address book. You will not be able to un-check this option again for next 24 hours."

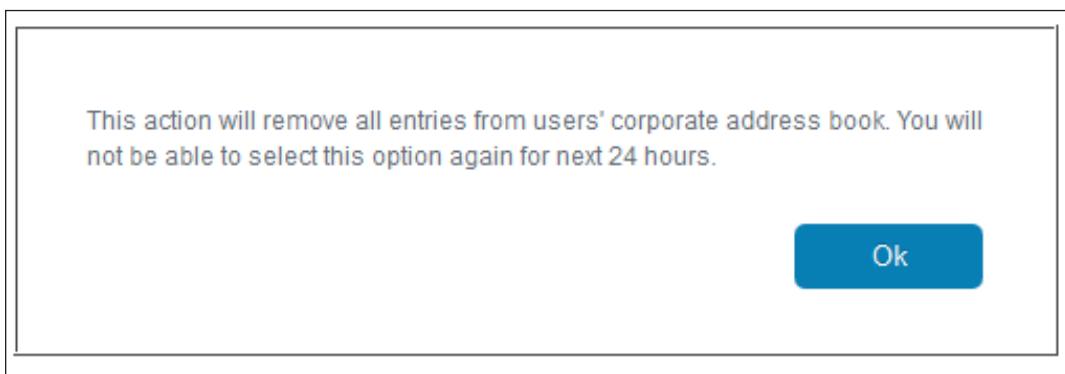


Figure 43. Un-check message for Corporate Address Book



Enterprise Single Sign On

1. Select the **Admin** arrow from the menu on the left side of the screen. The **Admin submenu** opens.



Figure 44. Admin Option

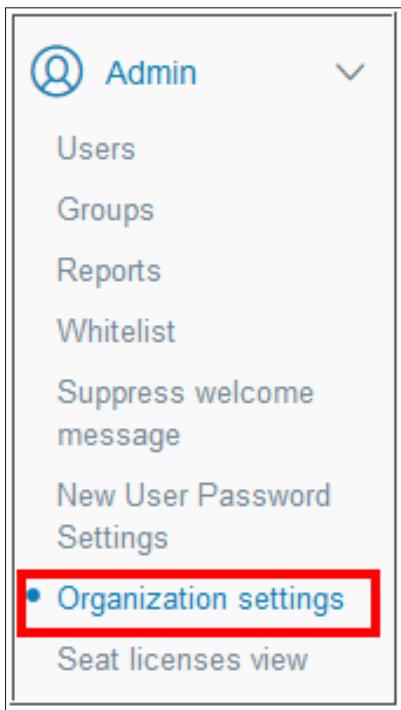


Figure 45. Admin Menu

2. Select **Organization settings** option. The **Organization settings** screen opens.
3. Scroll down the screen and the Select the **Admin** arrow from the menu on the left side of the screen. The **Admin submenu** opens.



Figure 46. Admin Option

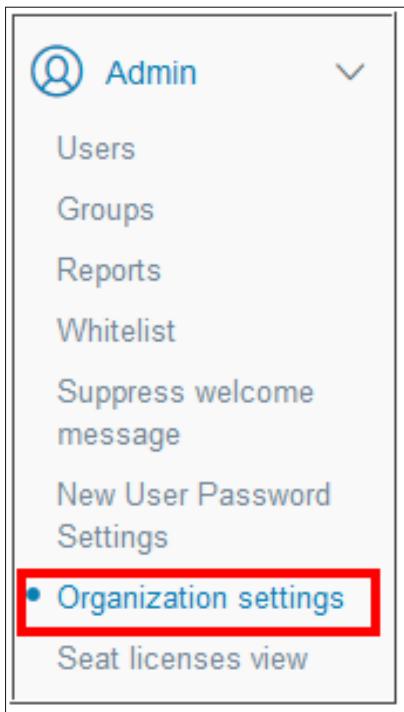


Figure 47. Admin Menu

4. Select **Organization settings** option. The **Organization settings** screen opens.
5. Scroll down the screen and the **Enterprise Single Sign On** appears.



Enterprise Single Sign On

Enable Enterprise Single Sign On

Selecting this option will allow the users to login into Business Messaging application with their wireless numbers or corporate user IDs.

Optional SSO Required SSO

Selecting Optional SSO will allow the users to login with their wireless numbers or their corporate user IDs. Selecting Required SSO will allow the users to login with their corporate user IDs only.

Organization Name

Enter an organization name here. New users will receive organization name in their welcome messages. The users will enter the same organization name on the Business Messaging login screen when they select Corporate Login.

Identity Provider URL (POST URL)

Enter the URL where Business Messaging will post the SAML request

Identity Provider Certificate [Upload Certificate](#) USCensus.crt

Upload your Identity Provider certificate for enabling encrypted SAML response

Identity Provider Logout URL

Business Messaging will post single SAML Logout Request to Identity Provider Logout URL

Service Name

Business Messaging will be sending Service Name as an issuer field in the SAML Request to identity provider.

Callback URL

Identity Provider will call back this Business Messaging URL in the SAML Response

Business Messaging Certificate [Download Certificate](#)

Download the Service Provider Certificate and provision in your Identity Provider to enable SAML request and SAML logout

Business Messaging Logout URL

Identity Provider will post a single Logout SAML Request to this URL

Figure 48. Enterprise Single Sign On Screen**Table 6. Enterprise Single Sign On**

Field	Description
Enable Enterprise Single Sign On	Selecting this option will allow the users to login into Business Messaging application with their wireless numbers or corporate user IDs.
Optional SSO and Required SSO radio buttons	Selecting Optional SSO will allow the users to login with their wireless numbers or their corporate user IDs. Selecting Required SSO will allow the users to login with their corporate user IDs only.
Enter Organization Name	Enter an organization name here. New users will receive organization name in their welcome messages. The users will enter the same organization name on the Business Messaging login screen when they select Corporate Login.



Field	Description
Enter Identity Provider URL (POST URL)	Enter the URL where Business Messaging will post the SAML request during the login process.
Identity Provider Certificate	Upload your Identity Provider certificate to validate the Authentication SAML Response and Assertion.
Identity Provider Logout URL	Business Messaging will post single SAML Logout Request to Identity Provider Logout URL.
Service Name	Business Messaging will send Service Name as an Issuer field in the SAML Request to IDP.
Callback URL	Identity Provider will call back this URL in the SAML Response.
Service Provider Certificate	Download the Service Provider Certificate and provision in your Identity Provider to enable SAML request and SAML logout.
Service Provider Logout URL	Identity Provider will post a single Logout SAML Request to this URL.



Enable Directory Services

1. Select the **Admin** arrow from the menu on the left side of the screen. The **Admin** submenu opens.



Figure 49. Admin Option

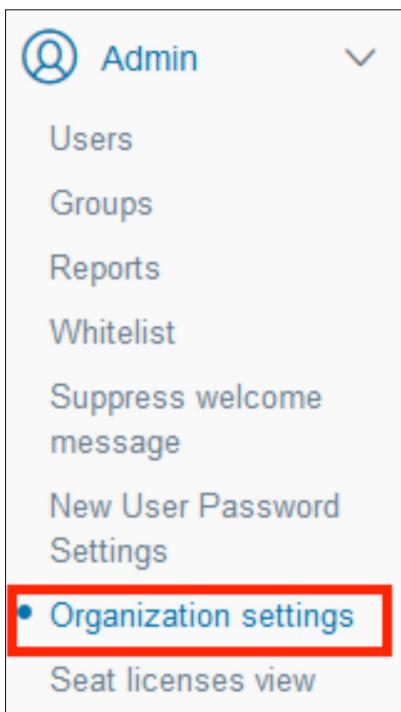


Figure 50. Admin Menu

2. Select **Organization settings** option. The **Organization settings** screen opens.
3. Scroll down the screen to the **Directory Services** section.



Directory Services

Enable Directory Services

Active Directory Microsoft Azure

LDAP URL

Base DN

User DN

LDAP Password

Certificate [Upload Certificate](#)

User Attributes

First Name

Last Name

Number

Email address

City

State

ZIP Code

Photo

Controlled Welcome Message [Send](#)

Last Welcome message was sent on 2nd January, 2017

[Save Changes](#)

Figure 51. Directory Services Screen

**Table 7. Enable Directory Services**

Field	Description
Enable Directory Services	Selecting this option will allow Seat License Admins to search users in your Directory Service and provision them directly via this interface.
LDAP URL	The URL must begin with ldaps:// when connecting to the LDAP server through a secure tunnel.
Base DN	Base DN of the LDAP node.
User DN	The distinguished name (DN) of the LDAP user who is allowed to search the LDAP directory. Anonymous access is not supported.
LDAP Password	Enter user DN password.
Certificate	Upload a valid certificate to enable secure connection with your LDAP.
User Attributes	Map the user attributes from your directory service. For example, if the Distinguished Name (DN) for Last Name is lastname, enter last name in the Last Name field.

Note: Disabling the directory service will de-provision the users.



Allow Messaging Only Within the Enterprise

1. Select the **Admin** arrow from the menu on the left side of the screen. The **Admin** submenu opens.
2. Select **Organization settings** option. The **Organization settings** screen opens.
3. Scroll down the screen to the **Messaging only within the Enterprise** section.
4. Check the box to allow all enterprise users to send messages only within the enterprise.

The screenshot shows the 'Organization settings' page in the AT&T Business Notification Center. On the left, there's a navigation sidebar with various options like Conversations, Contacts, Groups, Admin, Reports, and Support. The 'Admin' section is expanded, showing sub-options like Organization settings, Secure API Management, and Support. The main right panel is titled 'Organization settings' and contains several sections: 'PIN Access for secure client users using iOS or Android devices' (with PIN enabled set to ON), 'Message options for secure users' (with 'Enable message options for secure users' checked), and 'Messaging only within the enterprise' (with 'Enable messaging only within the enterprise' checked). A red arrow points to the checkbox in the 'Messaging only within the enterprise' section.

Figure 52. Messaging within the enterprise

Note: Default state is un-checked, that will allow the users to send messages to anyone.



Controlled Welcome Message

This option allows the Enterprise Admins to send a welcome message at their convenience.

The screenshot shows the AT&T Business Notification Center interface. On the left, there's a sidebar with various navigation options like Conversations, Contacts, Corporate Directory, Groups, Admin (with sub-options like Users, Groups, Reports, Whitelist, Suppress welcome message, New User Password Settings, Organization settings, and Seat licenses view), Support, and Help. The main content area is titled 'Organization settings'. It includes sections for PIN Access for secure client users using iOS or Android devices (PIN enabled: ON, PIN timeout: After 5 minutes, PIN change frequency: After 90 days), Password policy (Password change frequency: Never expires), Corporate Directory Address Book (Enable Corporate Address Book Sync: checked), Enterprise Single Sign On (Enable Enterprise Single Sign On: checked), Directory Services (Enable Directory Services: checked), and Controlled Welcome Message (Send button). A note at the bottom states 'Last Welcome message was sent on 23rd January, 2017'. At the bottom right is a 'Save Changes' button.

Figure 53. Controlled Welcome Message

1. Once in the Organization settings, scroll down to the Controlled Welcome Message.
2. Enterprise Admin clicks the **Send** button.
3. A pop up informing the admin whether s/he really wants to send the welcome messages to all the users in the enterprise appears.
4. Click **Yes** to send the welcome message immediately to all users in the enterprise, or click **No** to not send the welcome message.

Notes:

- Selecting this option will send a welcome message to all the users in your enterprise.
- The users will continue to use their existing passwords. The welcome message will include a text to use “Forgot Password” link. This will help the user who does not remember the password.
- Welcome message text: ‘FREE MSG from AT&T. Your number is now activated to receive Business Messaging messages. If you would like to use our app that has an enhanced set of messaging features, please visit www.att.com/busmsgr to download the Business Messaging app. Log in with your mobile \$\$mobileNumber\$\$ and current password. You can use the “Forgot Password” link on the mobile app login screen if you do not remember your password. Please visit www.att.com/businessmessaging for more info.’



Viewing Seat License Information

Enterprise Administrators can view the total number of seats and available seats under a particular Seat License Administrator.

1. Select the **Admin** option on the left side of the screen, and then select the **Seat licenses view**.
2. On the Seat License View screen, a list of Seat License Administrators, as well as the number of seats available, and the total number of seats appears. This information appears in both tabular and graphic formats.

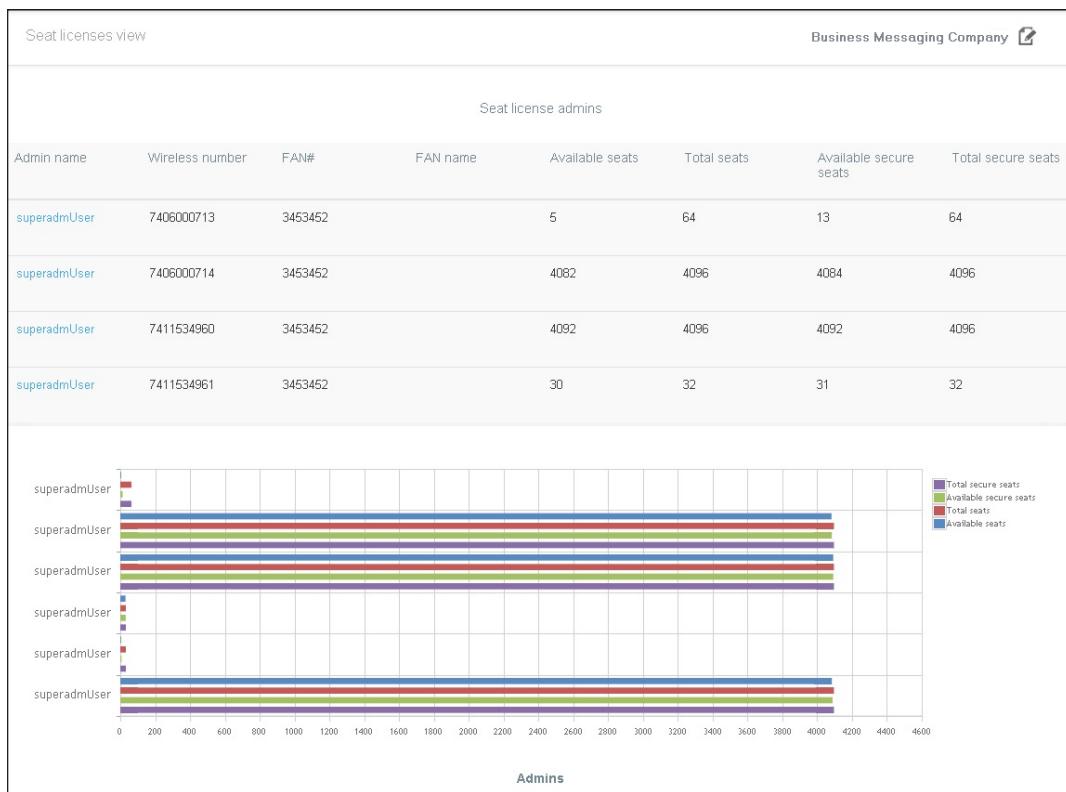


Figure 54. Seat License View Screen

Note: This screen can also be accessed by clicking the hyperlinked mobile number of a Seat License Administrator on the User Administration screen.

**Table 8. Seat License View Field Descriptions**

Plan Type	Description
Admin name	The name of the Seat License Administrator. Clicking the hyperlinked admin name opens the user's information on the User Administration screen. See page 65 for more information.
Wireless number	The mobile directory number for the Seat License Administrator.
FAN#	The functional account number for the Seat License Administrator.
FAN name	The name of the Seat License Administrator's functional account number.
Available seats	The number of available user seats in the Seat License Administrator's system.
Total seats	The total number of user seats in the Seat License Administrator's system.
Available secure seats	The number of available secure user seats in the Seat License Administrator's system.
Total secure seats	The total number of secure user seats in the Seat License Administrator's system.



Viewing Information Per Seat License Administrator

Enterprise Administrators can view information for each Seat License Administrator, such as the users added or modified, groups added or modified, reports, and whitelist information.

On the Seat License View screen, click the hyperlinked Seat License Administrator name. Alternatively, you can also click the hyperlinked Seat License Administrator name on the User Administration screen.

When the User Administration screen opens, it lists all users who have been added, modified, or deleted by the selected Seat License Administrator, as shown in the sample below.

Users > Saroj SiteBUpdate									Seat Licenses
	Number	Name	E-Mail	Secure Capable	Wireless Operator	Admin Activation Status	Remote Wipe Status	User Optin Status	Test
<input type="checkbox"/>	3544564001	Jane Williams		<input type="checkbox"/>	T-Mobile Usa Inc.	Not activated	Not Applicable	Not Initiated	Not tested
<input type="checkbox"/>	1231020657	Lisa Davis	verifydefect@testing.com	<input type="checkbox"/>	-	Activated	Not Applicable	Not Applicable	Not tested

Figure 55. User Administration Screen by Seat License Administrator View

From this screen, the Enterprise Administrator can also view groups, reports, and whitelist information for the particular Seat License Administrator by making the appropriate selection from the Admin menu at the top of the page.

To return to the root view that shows information for all users and Seat License Administrators, click the link for the appropriate menu item. For example, in the sample shown above, clicking the **Users** link returns the Enterprise Administrator to the User Administration screen.

To view a breakdown of available licenses, total licenses, secure licenses, and total secure licenses for the particular Seat License Administrator, click the **Seat Licenses** link to view the User Seat Licenses screen.



Figure 56. User Seat Licenses Screen



Updating the Company or Organization Name

The Enterprise Administrator can update the name of the company that appears in the upper right corner of Enterprise Administrator-specific screens, such as the Seat License View screen and the Organization Settings screen.

Note: This change only applies to the Enterprise Administrator's view and does not apply to Seat License Administrator or user views.

1. In the upper right corner of the Seat License View screen or the Organization Settings screen, click the **Edit** icon (>Edit).
2. Enter the new company or organization name. This field is limited to 100 characters.

A screenshot showing a text input field containing "Business Messaging Company". To the right of the field are two icons: a checkmark (Save) and a circle with a slash (Cancel).

Business Messaging Company	✓	✗
----------------------------	---	---

Figure 57. Edit Company or Organization Name for Enterprise Administrator View

3. Click the **Save** icon (✓) to accept the change. Alternatively, click the **Cancel** icon (✗) to cancel the change.

Additional Enterprise Administrator Functionality

Enterprise Administrators can perform the tasks listed below that are typically performed by Seat License Administrators.

- Enabling Secure Messaging Capability (page 30)
- Remotely Wiping a User's Mobile Device (page 36)



5. Reports

This chapter describes how to generate the reports listed below. Seat License Administrators and Enterprise Admins have access to the Messaging Report, Accounts Report, and Daily Reports. In addition, Enterprise Administrators also have access to the Audit Reports.

- Messaging Report (page 71)
- Accounts Report (page 72)
- Daily Report (page 73)
- Audit Reports (page 74)



Messaging Report

This report is used by Seat License Administrators and Enterprise Administrators.

1. Select the **Admin** option on the left side of the screen, and then select **Reports**.
2. Select **Messaging Report**.
3. Enter the mobile number of the recipient of the report.
4. Enter the date and time to include in the report.
5. Click **Generate Report**.

The screenshot shows the 'Messaging Report' screen within a 'Reports' interface. At the top, there are three tabs: 'Messaging Report' (which is selected and highlighted in blue), 'Accounts Report', and 'Daily Report'. Below the tabs, the 'Messaging Report' section has a field labeled 'Recipient' with a placeholder '(Required)'. A note next to it says: '% is a supported wild card character. You can search for messages by adding % to the recipient field, for example:'. It lists three examples: 'Add %1234 to view messaging activity for all users whose numbers end with 1234.', 'Add 1234% to view messaging activity for all users whose numbers start with 1234.', and 'Add %1234% to view messaging activity for all users whose numbers have 1234 in the middle of the number.' Below the recipient field are two sets of 'From' and 'To' fields, each with a date (03/06/2016) and a time (00:00:00 or 14:23:00). To the right of these times are 'H:M:S' labels. At the bottom left is a blue 'Generate report' button.

Figure 58. Messaging Report Screen

To search for a message, you can use the “%” symbol as a wild card character in the *Recipient* field. For example:

- Add %1234 to view messaging activity for all users whose numbers end with 1234.
- Add %1234 to view messaging activity for all users whose numbers start with 1234.
- Add %1234 to view messaging activity for all users whose numbers have 1234 in the middle of the number.



Accounts Report

This report is used by Seat License Administrators and Enterprise Administrators.

1. Select the **Admin** option on the left side of the screen, and then select **Reports**.
2. Select **Accounts Reports**.
3. On the Accounts Report screen, select the appropriate report(s) to view. Available options include:
 - All users
 - Activated users
 - Deactivated users
 - Not activated users
 - Test passed users
 - Test failed users
 - Not tested users
4. Click **Generate Report**.

The screenshot shows a user interface for generating an 'Accounts Report'. At the top, there is a navigation bar with four tabs: 'Reports' (grayed out), 'Messaging Report' (grayed out), 'Accounts Report' (highlighted in blue), and 'Daily Report' (grayed out). Below the tabs, the title 'Accounts Report' is displayed. Underneath the title is a list of filter options, each preceded by a checkbox. The filters are: 'All users', 'Activated users', 'De-activated users', 'Not Activated users', 'Test passed users', 'Test failed users', and 'Not tested users'. At the bottom of the list is a large blue button labeled 'Generate report'.

Figure 59. Accounts Report Screen



Daily Report

This report is used by Seat License Administrators and Enterprise Administrators.

1. Select the **Admin** option on the left side of the screen, and then select **Reports**.
2. Select **Daily Report**.
3. Enter the desired date.
4. Click **Generate Report**.

A screenshot of a web-based reporting interface. At the top, there's a navigation bar with tabs: 'Reports' (grayed out), 'Messaging Report' (grayed out), 'Accounts Report' (grayed out), and 'Daily Report' (highlighted in blue). Below the navigation bar, the title 'Daily Report' is displayed. Underneath the title, there's a date input field containing '03/06/2016'. To the right of the date input is a calendar for March 2016. The calendar shows the days of the week from Sunday (Su) to Saturday (Sa). The dates are arranged in a grid: Row 1: 1, 2, 3, 4, 5; Row 2: 6, 7, 8, 9, 10, 11, 12; Row 3: 13, 14, 15, 16, 17, 18, 19; Row 4: 20, 21, 22, 23, 24, 25, 26; Row 5: 27, 28, 29, 30, 31. The date '03/06/2016' is highlighted in orange. A blue button labeled 'Generate report' is located to the left of the calendar.

Figure 60. Daily Report Screen



Audit Reports

These reports are used by the Enterprise Administrator. These reports can be downloaded to a CSV file and opened in a spreadsheet program, such as Microsoft® Excel®.

1. Select the **Admin** option on the left side of the screen, and then select **Reports**.
2. Select **Audit Reports**.
3. Enter the desired date.
4. Select the report type.
 - **Access Report:** This report lists the number of user access attempts that took place on the selected date. See page 75 for more information.
 - **Provisioning Report:** This report lists the provisioning and feature changes that occurred on the selected date. See page 76 for more information.
5. Click the **Generate Report** button.
6. Save the CSV file to your desktop and open it in a spreadsheet program, such as Microsoft® Excel®.

A screenshot of a web-based application interface titled "Audit Report". At the top, there is a navigation bar with five tabs: "Reports", "Messaging Report", "Accounts Report", "Daily Report", and "Audit Report". The "Audit Report" tab is highlighted with a blue border. Below the tabs, the title "Audit Report" is displayed. Underneath the title, there is a date input field containing "03/08/2016" and a dropdown menu next to it with the option "Access report" selected. At the bottom of the screen, there is a blue button labeled "Generate report".

Figure 61. Audit Reports Screen



Access Report

This audit report is available on a daily basis and lists the number of user access attempts that took place on the selected date.

Wireless number	Source	Login attempt	Date of event	Time of event	Logon duration
8135551234	Web	Success	1/15/2015	13:00:00	3.05

Figure 62. Access Report

Table 9. Access Report Field Descriptions

Field	Description
Wireless Number	The mobile directory number for the user.
Source	The source of the login attempt. Valid values include: <ul style="list-style-type: none">• Web• Mobile iOS Phone• iOS tablet• Android Phone• Android Tablet
Login Attempt	Indicates whether the login attempt was successful. If the attempt failed, the reason for the failure is listed.
Date of Event	The date the login attempt took place.
Time of Event	The time the login attempt took place, reported in GMT.
Logon Duration	The duration the user was logged in to the application.



Provisioning Report

This audit report is available on a daily basis and lists the provisioning and feature changes that occurred on the selected date.

Wireless number	Provisioning / Feature change	Source	Provisioning attempt	Date of event	Time of event
8135551234	Provisioning	Seat License Admin	Success	1/15/2015	13:00:00

Figure 63. Provisioning Report

Table 10. Provisioning Report Field Descriptions

Field	Description
Wireless Number	The mobile directory number for the user.
Provisioning/Feature Change	Indicates the change that requested by the Administrator or AT&T. Valid values include: <ul style="list-style-type: none">• Provisioning• De-provisioning• Feature Changes• Remote Wipes
Source	The source of the request. Valid values include Seat License Administrators, Enterprise Administrators, and AT&T. If the source is a Seat License or Enterprise Administrator, the MDN number for the Administrator will be listed.
Provisioning Attempt	Indicates whether the request was successful. If the request failed, the reason for the failure is listed.
Date of Event	The date the request took place.
Logon Duration	The time the request took place, reported in GMT.



6. Whitelist Administration

1. Select the **Admin** option on the left side of the screen, and then select **Whitelist**. See *Submitting an SMTP Whitelist Request* (in the BNC user guide) for more information.
2. Complete all of the fields on the form.
3. Select the **I agree to the Terms and Conditions of White Listing Domain Names on SMTP** option.
4. Click **Submit**.

The screenshot shows the 'Whitelist for SMTP' page. At the top right are 'Submit' and 'Clear Form' buttons. Below them is a section titled 'SMTP Whitelist Request' with a note about filter settings. A 'About Spam Filters' link is present. The main form contains several input fields: 'My Phone Number' (650) 930-0113, 'Contact Name' (Deepak Narang), 'Company Name' (empty), 'E-Mail Address' (conrad.pienaar2@syniverse.com), and 'Add domain or e-mail address to whitelist' (empty). At the bottom are sections for 'Domains or email addresses to remove from whitelist' and 'Current Whitelist'.

Figure 64. Whitelist Administration Screen



7. Site Licensing for Business Messaging – FAQ

Site Licensing – General FAQ

Q: What is Site Licensing for Business Messaging?

A: Site Licensing is an add-on feature that allows customers to purchase bulk Business Messaging seat licenses; customers are provided with a Web interface where they can apply those licenses to the paging application of any valid AT&T subscriber.

Q: How does Site Licensing work?

A: The Site License seats are provisioned by the customer's administrator through a Web interface. The administrator can add any AT&T wireless number to the account. The administrator is responsible for administering the individual seat licenses to users within that company; the administrator is usually the customer's IT manager.

Q: Are there any restrictions for getting Site Licensing?

A: Yes, the customer must be onboarded with the AT&T Advanced Solutions Care (ASC) Helpdesk. This requires a minimum of 100 open lines and a minimum of 100 subscribers on the corporate account.

Q: Can I provision a non-AT&T number?

A: No, you cannot provision a non-AT&T number.

Q: My number failed, what do I need to do?

A: You can call the ASC Helpdesk at the 888+pin number, or e-mail assistance will be provided by sending a message to BusinessMessaging@att.com. IT administrators can only use this service if they are onboarded.

Q: How do I upgrade to more seats?

A: You must call the ASC Helpdesk at the 888+pin number. This would be a request for a feature add, and would be handled by either NBS or the customer's account team.

Q: Does the administrator count as one of the seat licenses?

A: No, the administrator is not considered as a seat person. The administrator receives Business Messaging for free.

**Q: Is a welcome message sent to the seat user?**

A: Yes, a welcome message is sent to each of the licensed seat users.

Q: I am the administrator for my company. How do I change the password for the administrator's Web site?

A: Log in to the Administrator site, open the user profile and follow the directions for changing a password as outlined in the BNC user guide.

Q: I forgot my password. How do I get a new one?

A: Go to the Login screen for the Administrator Web site, enter your user name and click the **Forgot password?** option

Q: What is your user name?

A: It is the administrator's mobile number.

Q: Can an administrator be an administrator of two accounts?

A: No, because the user name is associated with the administrator's mobile number, this cannot be done unless the administrator has two accounts with AT&T.

Q: What is the wildcard?

A: The wildcard is the *. (i.e., 206* will give you all mobile numbers starting with 206).

Q: What is a CSV file?

A: The comma-separated values (CSV) file format is a delimited data format that has fields separated by the comma character and records separated by new lines. Fields, which contain a comma, a new line, or a double quote character, must be enclosed in double quotes. If a field's value contains a double quote character, it is escaped by placing another double quote character next to it (appearing as ""). The CSV file format does not require a specific character encoding, byte order, or line terminator format.

Q: I am an administrator. How do I get technical assistance?

A: Call the ASC Helpdesk at the 888+pin number. (IT administrators can only call if they are onboarded.) Email assistance will be provided at BusinessMessaging@att.com.

Q: What are the different possible statuses for a user?

A: Activated or deactivated—Activated users can receive pages, while deactivated users cannot.



Q: How many activated or deactivated users can I view on the Manage Users Web page?

A: You can only have as many activated users as you have seat licenses. However, you can have an unlimited number of deactivated users.

Q: How do I know how many seats I have left?

A: Access the Administrator Web site and select Users from the menu bar. You can read your current status in the top right-hand corner. It will tell you how many licenses you have bought and how many active users you currently have.

Q: How do I create reports?

A: Access the Administrator Web site and select Reports from the menu bar. You can choose from three different types of reports – Messaging Reports, Accounts Reports and Daily Reports.



Site Licensing – Product FAQ

Q: What is the address to the Site Licensing administrator site?

A: The URL is <https://bnc-businessmessaging.att.com>.

Q: How do I receive my user name and password?

A: Once you sign up for Site Licensing as the administrator, you will receive a welcome text message with your user name and password.

Q: What if I try to add a seat number that already has Business Messaging?

A: The system will allow you to do it, but you are essentially being double-billed.

Q: How do I change the designated administrator, as in the case of the administrator leaving the company?

A: Please email BusinessMessaging@att.com with the mobile number of the old administrator, and include the mobile number of the new administrator so that AT&T can migrate the service to a different administrator.

Q: I am a seat license user; if I have a problem who do I call?

A: Call your company's administrator or IT manager.

Q: How do I deactivate multiple users?

A: Access the Administrator Web site and select Users. Check all the boxes next to the mobile numbers you want to deactivate and then click Deactivate. The status should change to Deactive for all the users.

Q: What will the ASC Helpdesk log in to the Business Messaging Management (BMAM) tool give access to; and does it provide different screen views and/or administrative rights?

A: There will be one demonstration account for familiarization with the tool; however, the ASC Helpdesk will not be able see the same screen as the customer.

Q: Does the BMAM tool keep a timestamp of when changes were made and who made the changes?

A: This functionality is not available.

Q: If a care representative tries to add Business Messaging to a single line that already has the Site Licensing feature on the BAN, will they get a message stating it is already provisioned?

A: No, the message will be provided.



Q: Can a number be activated on two different licenses?

A: Yes.

Q: How does a user reduce the number of seat licenses in their account?

A: The ASC Helpdesk will have to let the customer know that they have to deactivate a certain number of users to equal their seat count. Email reminders will be sent to the administrator for the account reminding them that they should perform this function, since after five (5) business days, the system automatically reduces the number seat licenses in order to equal to the new number.

Q: If an account is suspended, will I be able to log in to the BMAM site?

A: No.

Q: If my account was suspended and then reactivated it, can I use my old password?

A: No, you will receive a text message with a new password.



8. User Messages

This chapter outlines the messages that appear within the application or are sent via SMS message to cross carrier users during the opt-in/opt-out process.

Messages longer than 160 characters may be split into multiple messages if the destination operator's SMSC does not support concatenation. Each section of these split messages will be identified in a format using the message section and the total number of messages the user will receive. For example, the first part of a message split into three sections will include (1/3) to indicate that it is the first of three SMS messages.

Table 11. User Messages

User Action	User Status	Application Behavior	Sample Message
User sends a start SMS message or taps the Start button.	The user does not exist / Deactivated	System sends a mobile-terminated message stating that the user should contact their Administrator.	AT&T Business Messaging: Your account has not been activated by the Administrator. Please contact your Enterprise Administrator to activate your account.
User selects the Forgot password? option.	Not Activated	Error message appears within the application.	Error: You are not provisioned. Please contact your Administrator to activate your account.
	Deactivated		
	Active (AT&T customer)	System sends a reset password SMS message.	Password reset for the AT&T Business Notification Center. Your new password is m1mlC4, you will be required to select a new password the next time you log in to the application
	Opted In (non-AT&T)	System sends a reset password SMS message.	AT&T Business Messaging: AT&T Password reset for the AT&T Business Notification Center. Your new password is ORA0aO. Select a new password the next time you log in to the application.
Opt-in Pending (non-AT&T) Opted Out (non-AT&T)	Opt-in Pending (non-AT&T)	Message appears in the application stating that the user has not opted in to the service.	AT&T Business Messaging: Reply YES to receive ongoing messages. Msg&Data Rates May Apply. Msg Freq may vary. Reply STOP to cancel, HELP for help or 1-866-563-4703.
	Opted Out (non-AT&T)	<i>New users:</i> System sends an opt-in SMS message. <i>Existing users:</i> Start button appears at the bottom of the Login page.	



User Action	User Status	Application Behavior	Sample Message
User selects the New User or Verify Now button.	Not Activated	Error message appears within the application.	Error: You are not provisioned. Please contact your Administrator to activate your account.
	Deactivated		
	Active (AT&T customer)	Message appears within the application.	You are already registered user for AT&T Business Messaging Business Notification Center. Please use your Business Notification Center password to log in or select the Forgot password? option to reset your password.
	Opted In (non-AT&T)	<i>New users:</i> System sends a reset password SMS message.	AT&T Business Messaging: Your new password is gdaMnZ for the AT&T Business Notification Center. You will be required to select a new password the next time you log in to the application.
		<i>Existing users:</i> Message appears within the application.	You are already a registered user for AT&T Business Messaging Business Notification Center. Please use your Business Notification Center password to log in or select the Forgot password? option to reset your password.
	Opt-in Pending (non-AT&T)	Message appears within the application.	You are already a registered user for AT&T Business Messaging Business Notification Center. Please reply with START to short code 266246 to opt in into the service.
User receives opt-in SMS message.	Opt-in Pending (non-AT&T)	Administrator activates new user. System sends an opt-in SMS message.	AT&T Business Messaging: Reply YES to receive ongoing messages. Msg&Data Rates May Apply. Msg Freq may vary. Reply STOP to cancel, HELP for help or 1-866-563-4703.
User responds to opt-in SMS message and opts in to the service.	Opted In (non-AT&T)	System sends an opt-in confirmation SMS message.	Welcome to AT&T Business Messaging. Msg&Data Rates May Apply. Msg Freq may vary. Reply HELP for help or call 1-866-563-4703. Reply STOP to cancel.
User receives welcome SMS message	Opted In (non-AT&T)	System sends a welcome SMS message.	MSG from AT&T. Your account is now activated for Business Messaging. Please visit www.att.com/busmsgr to download the Business Messaging app. Log in with your email address and temp password xxxyyzzz. You will be required to select a new password on your next login. You can also login to the app using Corporate SSO Login with your corporate username and password. You will be required to enter enterprise name as <enterprise_name> on the login screen. Please visit www.att.com/businessmessaging for more info.
User sends STOP message via SMS.	Opted Out (non-AT&T)	System sends a mobile-terminated message confirming that the service has been stopped.	AT&T Business Messaging. You have opted out. You will not receive additional messages. Contact: www.att.com/businessmessaging or 1-866-563-4703.



User Action	User Status	Application Behavior	Sample Message
User sends HELP message via SMS.	Opted In (non-AT&T)	System sends a mobile-terminated message.	AT&T Business Messaging: Msg&Data Rates May Apply. Msg Freq may vary. Contact: www.att.com/businessmessaging or 1-866-563-4703. Reply STOP to cancel.
N/A	N/A	System sends a reminder notification to subscribers. This reminder service is applicable only to those operators that support reminder service.	REMINDER: Subscribed to AT&T Business Messaging. Msg&Data Rates May Apply. Msg Freq may vary. Reply STOP to cancel, HELP for help or 1-866-563-4703.



9. Error Messages on the Client

This chapter describes the error messages that may appear for Administrators using the Web portal.

Table 12. Error Messages on the Client

Error Message	Description
3PP-provisioned users cannot be activated.	(for Enterprise Administrators only) The Enterprise Administrator attempted to activate a user provisioned by AT&T. These users appear as "Individual" or "Bulk-Admin" user plan types on the User Administration screen. Enterprise Administrators cannot activate these users.
3PP-provisioned users cannot be deactivated.	(for Enterprise Administrators only) The Enterprise Administrator attempted to deactivate a user provisioned by AT&T. These users appear as "Individual" or "Bulk-Admin" user plan types on the User Administration screen. Enterprise Administrators cannot deactivate these users.
3PP-provisioned users cannot be deleted.	(for Enterprise Administrators only) The Enterprise Administrator attempted to delete a user provisioned by AT&T. These users appear as "Individual" or "Bulk-Admin" user plan types on the User Administration screen. Enterprise Administrators cannot delete these users.
3PP-provisioned users cannot be tested.	(for Enterprise Administrators only) The Enterprise Administrator attempted to send a test to a user provisioned by AT&T. These users appear as "Individual" or "Bulk-Admin" user plan types on the User Administration screen. Enterprise Administrators cannot send tests to these users.
Error occurred accessing user's remote wipe history – please try again later.	The Seat License or Enterprise Administrator attempted to view a user's remote wipe history. This is a network or server issue. The Enterprise Administrator should try again later.
Failed to generate Audit report.	(for Enterprise Administrators only) The Enterprise Administrator failed to generate an audit report. This is a network or server issue. The Enterprise Administrator should try again later.
Failed to update the organization name.	(for Enterprise Administrators only) The Enterprise Administrator attempted to update the organization or company name on the Seat License View screen or the Organization Settings screen. Please try again.



Error Message	Description
Failed to update the organization settings.	<p>(for Enterprise Administrators only) The Enterprise Administrator attempted to update the organization or company name and the process failed.</p> <p>This is a network or server issue. The Enterprise Administrator should try again later.</p>
Failed to wipe %s.	<p>The Seat License or Enterprise Administrator attempted to perform a remote wipe, but the function failed. "%s" indicates the user name or MDN.</p> <p>The Administrator should select OK and proceed with the remote wipe.</p>
Organization name cannot be empty. Please enter a valid organization name.	<p>(for Enterprise Administrators only) The Enterprise Administrator attempted to update the organization or company name and left the field blank.</p> <p>This field cannot be blank. Add an organization or company name.</p>
Please select at least one device to wipe.	<p>The Seat License or Enterprise Administrator attempted to perform a remote wipe on a user with multiple devices provisioned, but did not select a device.</p> <p>Select the appropriate device to remote wipe.</p>
Please select only one user.	<p>The Seat License or Enterprise Administrator attempted to perform a remote wipe on more than one user.</p> <p>Select only one user.</p>
Secure License limit has exceeded. Activation failed.	<p>This occurs when the child user is created but not activated. When the admin tries to activate the child user who is assigned with secure capability, this error shows up. Admin will need to reach out to AT&T's account executive to procure more licenses.</p>
The maximum allowed length is 100 characters. Please modify and try again.	<p>(for Enterprise Administrators only) The Enterprise Administrator attempted to update the organization or company name using more than 100 characters.</p> <p>Update the organization or company name using no more than 100 characters.</p>
The Seat License Admin does not have enough licenses to provide secure capability to the user(s):	<p>This occurs when there are not sufficient licenses. The Administrator will need to reach out to AT&T's account executive to procure more licenses.</p>
There is an error requesting user remote wipe history.	<p>The Seat License or Enterprise Administrator attempted to view a user's remote wipe history.</p> <p>This is a network or server issue. The Enterprise Administrator should try again later.</p>

