
# BEST PRACTICES GUIDE: MANAGING ADDS, CHANGES AND DELETES

TABLE OF CONTENTS

## INTRODUCTION

It is important to leverage a combination of automated and manual processes to maintain adds, updates and deletes as users come and go, and as variables in their environment change. This guide offers best practices on how to manage data in the Spok database to accommodate adds, updates and deletes of users and devices when administering Spok Mobile – Spok's secure text messaging application. The goal of this guide is to help administrators of Spok systems develop scalable workflows and ensure compliance with security standards. Please note that this guide is not intended to provide step-by-step training, but rather to provide best practices to consider when administering Spok Mobile (see Spok's Administrator's Guides for more detailed step-by-step instructions).

## PRE-IMPLEMENTATION

**Pre-Registration**: Prior to taking new requests for Spok Mobile secure text messaging services, it is recommended that users are added to the database in bulk, to create a directory of person records that contain required data attributes.

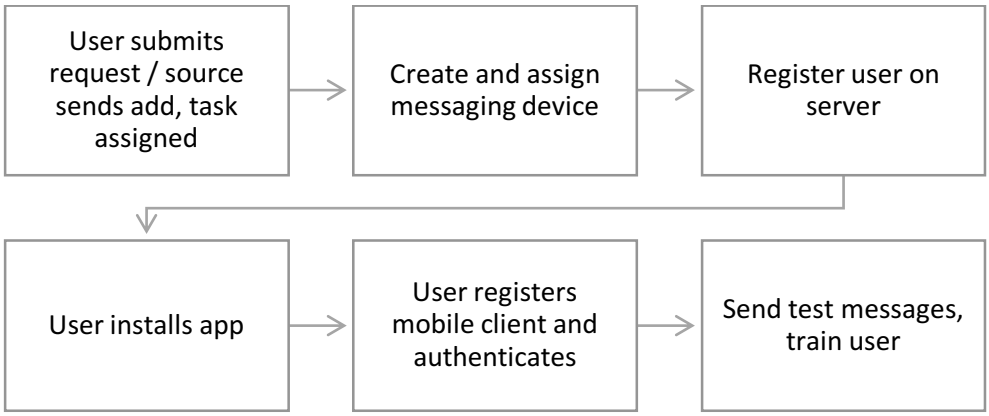
- ✓ *Add Users*
  Before implementing Spok Mobile and starting to register users, a database of person records will need to be created. The Spok Mobile application will require a first and last name, suffix, messaging ID, username, employee ID, password, email address and department for each user at a minimum to be fully functional. It is highly recommended that this data is pulled from an existing authoritative source (often Active Directory) and that a data feed is automated (via batch file or EDIX). This feed should include the aforementioned data, as well as, contact/phone information, billing information, title(s), office location(s) and any relevant notes. If a feed cannot be automated, person records will need to be created and maintained manually (this is not recommended and will thus not be covered in this guide).
- ✓ *Add Usernames and Passwords*
  When developing a strategy for populating username and password, it is recommended to consider purchasing and using Single Sign On (SSO) for web applications. Spok Mobile does not support SSO (native authentication only), so the username and password fields in the database will still need to be populated. If SSO can be used for web applications, it is recommended to use a hospital AD username as the username (except Smart Suite, where messaging ID must be used) and to use a generic password for all users. If SSO is used for web applications, Spok Mobile will be the only application using the native username and password and because Spok Mobile requires both registration and directory authentication, the directory password can be generic w/o jeopardizing security.
- ✓ *Add Messaging Devices*
  If possible, it is a great best practice to build messaging device records into the database prior to going live with Spok Mobile, If this data can be collected from mobile carrier/provider databases (Corporate Liable devices) and/or user surveys (BYOD), it can be pre-populated and assigned to users prior to go-live, saving steps in the request fulfillment/registration process. If it cannot be collected from a source

(as within most cases), it will need to be added as part of the registration process for new requests. If dual deployment is used, it is recommended to populate pager device numbers prior to go live – this data can be acquired from Spok.

- ✓ *Add Community Physicians*
  Most hospitals support many users who work outside of the hospital system, but are credentialed to work in the hospital. In many cases, these physicians may not be included in AD/HR data feeds and may need to be added, updated and deleted via a separate, manual process. If possible, it is considered a best practice to create sponsored accounts for these physicians and to include them in data feeds, or to leverage a feed from a credentialing database. If this is not available, administration of these records will need to be managed manually.
- ✓ *Provision Default Settings*
  It is important to verify that all default settings are adjusted to be in accordance with organizational policy (access codes, message retention) and user preferences (alert tones, message templates) before transitioning the service into production. Settings can be adjusted later, but changes will impact users.

## NEW REQUESTS

**New Registration**: Once a database of users and required user attributes is established, new requests can be accepted in accordance with request fulfillment processes. In addition to the user/person record, a new request for Spok Mobile will an associated device record is built and the Spok Mobile registration process is completed.




- ✓ *Add and Assign Messaging Device*
  In some cases, data will need to be collected from users (either in person or via an online request form), prior to fulfilling a request. This data includes name or employee ID and phone number at a minimum (some Spok console platforms also require mobile carrier, device type and device platform/OS). This data can be used to build the messaging device. It is highly recommended to use phone number as the unique device/pager address/ID for each user (unless dual deployment is used, in which case a pager number will be used). Phone numbers are unique and known to each user (in

most cases) and will be important for the use of some features. Once the device has been built into the database, it will need to be assigned to the user.

- **Note**: If the user already has a device assigned, make sure the new device is assigned a lower priority/higher device order until registration is completed. After completing registration, the priority/order will need to be adjusted. If the user will need to receive message son both a Spok Mobile device and another messaging device, such as a pager, "send to all devices" should be configured.

✓ *Register the Device on the Server*

The device will need to be registered on the server, which will initiate an email to the end user containing instructions, and username and password for registration. This step is most often managed by an IT Admin, handling a request via a formal request fulfillment process.

- **Note**: Some users may already be registered at another hospital Site or in Spheres. If this is the case, it is essential that the number and email address used at the first registered Site be used on all subsequent Sites to prevent registration issues or other Sites from disappearing from the user's app. Once registered in multiple Sites, the phone number and email address combination for registration cannot be changed.

✓ *Register the Mobile Client*

The app will need to be installed on the iOS or Android device. This will need to be pushed via a Mobile Device Management (MDM) tool by IT, or installed by the user from the Apple AppStore or Google PlayStore. If the user is installing the app on an iOS device, they will need to have an Apple account (ID and password) with updated credit card information for Apple to allow the download. Once downloaded, they user will need to access the email for the username and password and register the app. If possible, it is best to help user's complete registration, testing and training in person.

- **Note**: If the registration email cannot be found, the user can use the 'Forgot Password' link in the mobile app (on the Registration screen) to initiate a new email containing the password. If the email is still not received, the IT admin will need to verify that the number is not registered to another Site with a different email address and that the Registration Service is running on the Spok Mobile server.

✓ *Test Messaging*

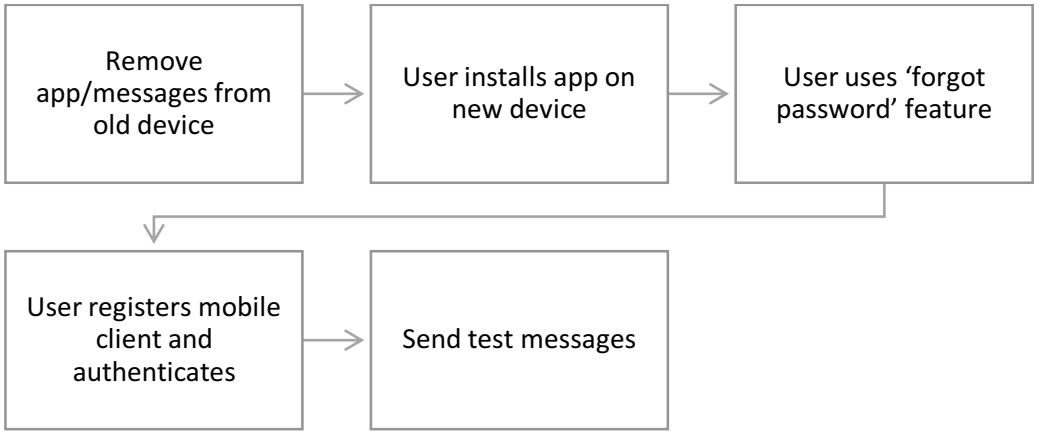
Once registered, the user should be instructed to send a test message (best practice is for them to send one to themselves to test sending and receiving messages). Upon searching the directory in the app, the user will be prompted to authenticate to the local Spok directory. The user will need to use the username/messaging ID and password combination in the Spok database to authenticate locally. Note that This can be configured to be a one-time authentication, but cannot be SSO/AD integrated. Upon completing the directory authentication, the user can send a test message and confirm receipt.

- **Note**: This step is often confusing to users and will require additional support, as users tend to become confused by multiple login steps. Take note that the username and password for directory authentication (prompted upon composing the first message in the app and leveraging username/messaging ID and password in the Spok database), is different than the username and password for initial registration (prompted upon first opening the app and leveraging the username and password in the registration email).

- ✓ *Train User*
  Once registration, authentication and testing has been completed, the user should begin receiving training. Onboarding training (best to provide in person, if possible) should include only essential things users need to know – additional training should be provided incrementally as part of the service. Onboarding training should include the following:
  - Basic training on app settings, status, Sites, sending, receiving and replying to messages.
  - Training on device settings such as push notification settings, Low Power Mode, Do Not Disturb, Wi-Fi settings, etc.
  - Training on use cases, workflows and policies.

## CHANGE REQUESTS

**Device Changes**: When a user is provided with / purchases a new iOS or Android device, the app will need to be registered and authenticated on the new device. Data on the old device will also need to be removed to prevent security violations/breeches/risk.

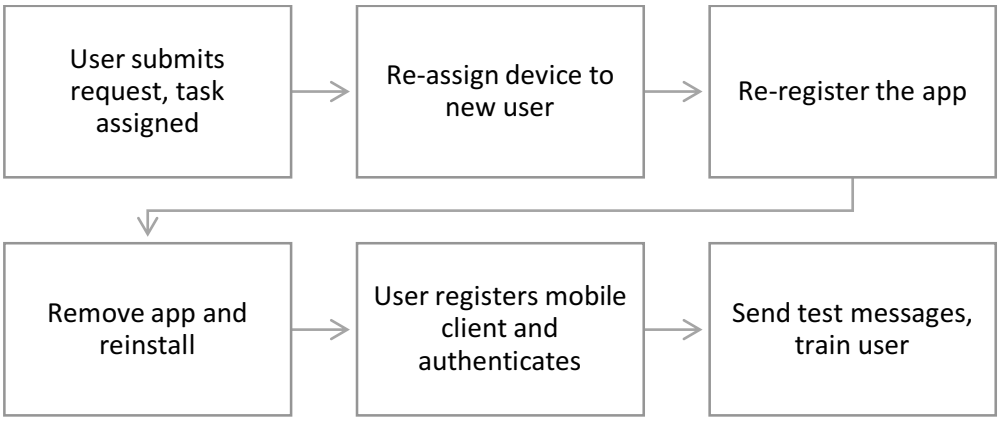



- ✓ *Remove Data from Old Device*
  Before registering the new device, it is important to remove any sensitive data from the old device. If the old device is owned by the hospital, the best practice is to wipe the old device (physically, or via MDM). IF the device is owned by the user, the best practice is to remove the app (via MDM or by the user, enforced by policy). If the app is not removed before the device no longer in possession and the device is unmanaged, the best practice is to use the Spok Admin tool to wipe messages form the app.
- ✓ *Install Spok Mobile on the New Device*
  The app will need to be installed on the new iOS or Android device. This will need to be pushed via a Mobile Device Management (MDM) tool by IT, or installed by the user from the Apple AppStore or Google PlayStore.
- ✓ *User Uses 'Forget Password' Option*
  Once installed, the user can access the app and tap 'Forgot Password' to generate a new email (to the address used during initial registration) containing the password for registration. The email can be

accessed to obtain the password, which can them be populated into the app to register the new device.

- ✓ *Register and Authenticate the App on The New Device*
  The email generate by taping 'Forgot Password' can be accessed to obtain the new password, which can them be populated into the app to register the new device. Once registered, the user should attempt to send a test message. Upon searching the directory in the app, the user will be prompted to authenticate to the local Spok directory. The user will need to use the username/messaging ID and password combination in the Spok database to authenticate locally.
- ✓ *Test Messaging*
  After registering a new device, test messages should always be sent and receipt confirmed to ensure all messaging services have been registered and configured properly.

**Re-Assignments**: As users change roles, responsibilities and shift duties, there is often a need to re-assign a device from one user to another, particularly if the device is owned by the hospital and is shared by multiple users. In many cases, the best practice to manage this scenario with Spok solutions is to provision a 'function record' (for example, Nurse A) that the device is registered to and remains registered to regardless of who has it. In some cases, however, such as when a user leaves the organization and another replaces that person in his/her role, the device may need to be un-registered and re-registered to the new user.

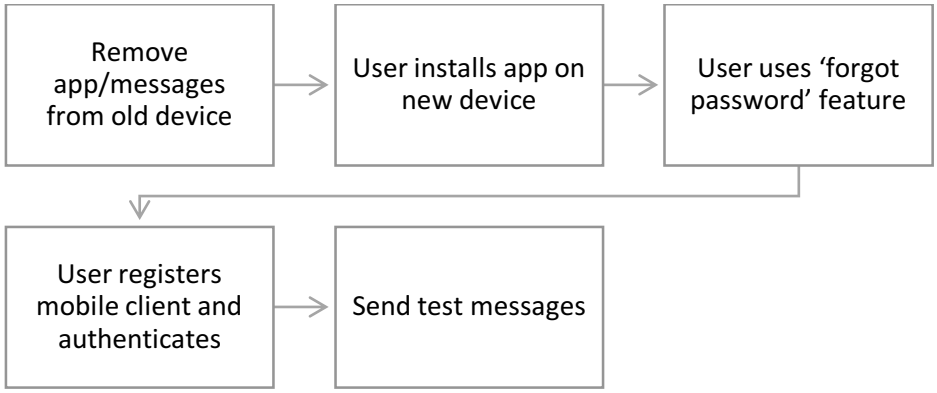



- ✓ *Re-Assign the Device to The New User*
  The device will need to be re-assigned to the new user in the database. Simply updating the Messaging ID associated with the device in the Spok database will accomplish this. This step is usually handled by an IT administrator.
- ✓ *Re-Register the Device*
  The device will need to be unregistered on the server and re-registered with the new user's email address. This step is usually handled by an IT administrator.

- ✓ *Remove the App and Reinstall*
  In order to get the app to re-prompt for directory authentication (and remove all messages and other data from the device), the app will need to removed and reinstalled. This step may be completed by the user.
- ✓ *Register and Authenticate the App*
  The registration email can be accessed to obtain the username and password to be populated into the app for registration. Once registered, the user should attempt to send a test message. Upon searching the directory in the app, the user will be prompted to authenticate to the local Spok directory. The user will need to use the username/messaging ID and password combination in the Spok database to authenticate locally.
- ✓ *Test Messaging and Train User*
  After registering a new device, test messages should always be sent and receipt confirmed to ensure all messaging services have been registered and configured properly. The user should be trained on essentials they need to know (see new registration workflow).

## INCIDENTS

**Lost/Damaged Devices**: While using Spok Mobile, users may lose or damage a device and require a replacement. This may require that the hospital provide a replacement, or that the user procures a replacement device, depending on device ownership and policy. It is considered a best practice to provide immediate temporary or permeant replacements (in some cases, temporary pagers may be preferred) for critical responders who lose or damage devices. Once a replacement is provided, the new device will need to be registered in a very similar way to a device change request.

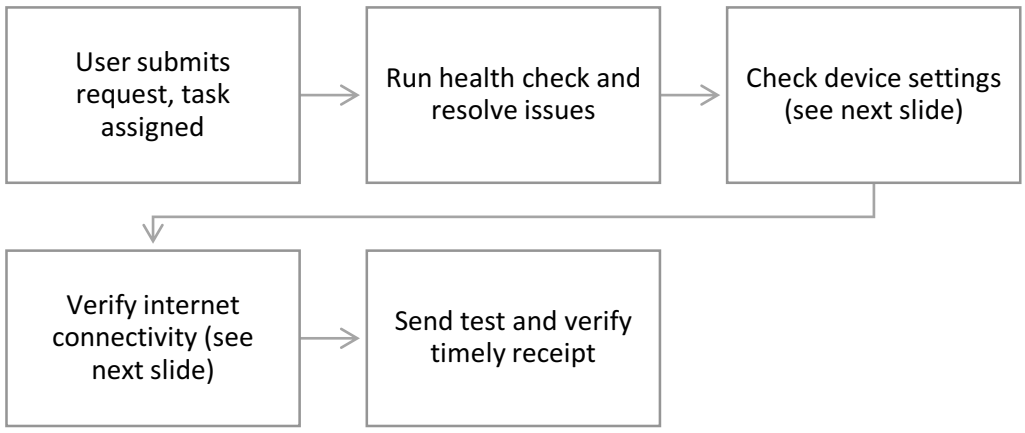



- ✓ *Remove Data from Old Device*
  Before registering the new device, it is important to remove any sensitive data from the old device. If the old device is owned by the hospital, the best practice is to wipe the old device (physically, or via

MDM). IF the device is owned by the user, the best practice is to remove the app (via MDM or by the user, enforced by policy). If the app is not removed before the device no longer in possession and the device is unmanaged, the best practice is to use the Spok Admin tool to wipe messages form the app.

- ✓ *Install Spok Mobile on the New Device*
  The app will need to be installed on the new iOS or Android device. This will need to be pushed via a Mobile Device Management (MDM) tool by IT, or installed by the user from the Apple AppStore or Google PlayStore.
- ✓ *User Uses 'Forget Password' Option*
  Once installed, the user can access the app and tap 'Forgot Password' to generate a new email (to the address used during initial registration) containing the password for registration. The email can be accessed to obtain the password, which can them be populated into the app to register the new device.
- ✓ *Register and Authenticate the App on The New Device*
  The email generate by taping 'Forgot Password' can be accessed to obtain the new password, which can them be populated into the app to register the new device. Once registered, the user should attempt to send a test message. Upon searching the directory in the app, the user will be prompted to authenticate to the local Spok directory. The user will need to use the username/messaging ID and password combination in the Spok database to authenticate locally.
- ✓ *Test Messaging*
  After registering a new device, test messages should always be sent and receipt confirmed to ensure all messaging services have been registered and configured properly.

**Delayed Notifications and/or Messages**: Users may experience delays in delivery of notifications or messages while using secure text messaging services. This is usually related to device settings or network connectivity. Message traceability and automatic retires help alleviate the impact; however, any delays should be identified, isolated and resolved as soon as possible to ensure reliable service delivery.

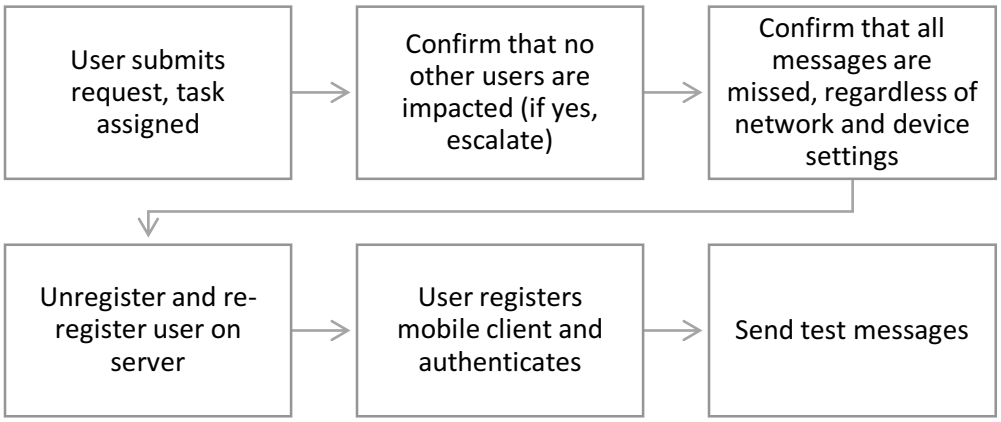



- ✓ *Run Health Check*
  A health check should be run within the client mobile app (Settings > Health Check) and any issues

found should be resolved.

- ✓ *Confirm Device Settings*
  The following device settings should be confirmed:
  Are push notifications turned on? Go to Settings > Notifications, select the app, make sure that Notifications are turned on.
  Are you signed in to your Apple ID on your iOS device? Go to Settings > iTunes & App Stores and enter your Apple ID and password.
  Is Do Not Disturb turned off? Go to Settings > Do Not Disturb and tap Manual if it's turned on.
  Is Lower Power Mode turned off? Go to Settings > Battery > and make sure Low Power Mode is off.
- ✓ *Verify Network Connection*
  Network connectivity should be confirmed by ensuring the device is connected to the internet over a network that does not restrict any required ports (restrictions can be identified via Health Check).
- ✓ *Test Messaging*
  After verifying/correcting all settings and connectivity, test messages should always be sent and receipt confirmed to ensure all messaging services have been registered and configured properly.

**Missing Notifications and/or Messages**: Type



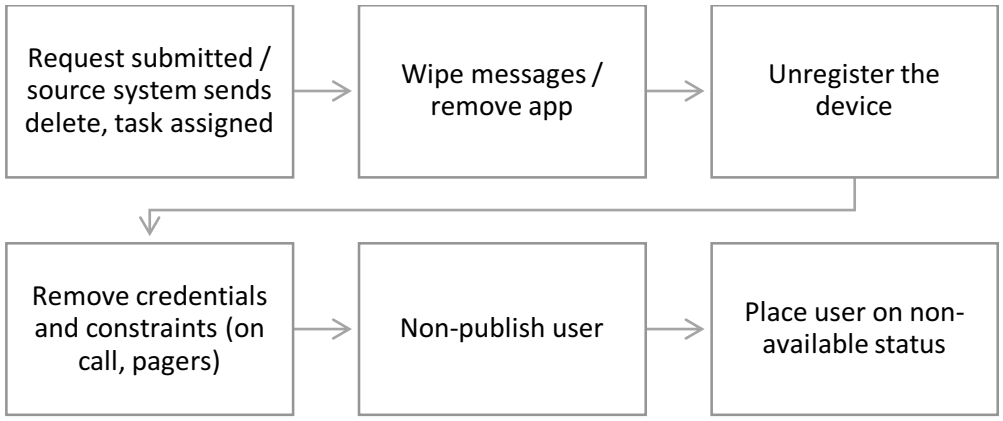

- ✓ *Confirm that Other Users Are Not Impacted*
  Before proceeding with handling missed messages as an isolated incident, IT will need to confirm that all users are not being impacted by a Major Incident / Outage. Checking the message logs to ensure there are not significant delays and/or checking incident reports should be completed before proceeding to troubleshoot as an isolated incident.
- ✓ *Confirm Device and Network Settings*
  All device and network settings (see delayed notification and/or messages workflow) to ensure they are not impacting notification/message delivery.
- ✓ *Unregister and Re-Register the Device*
  Occasionally, Spok registrations may not complete properly. Devices must be properly and completely

registered in order to receive notifications and messages. If notifications/messages are only delayed, this means the device is properly registered and something else is at play. If all notifications/messages are completely missed by an individual user, there may be a registration issue. The user should be unregistered and re-registered on the server.

- ✓ *Register and Authenticate the App*
  After registration has been updated on the server, the user will need re-register the app. Once registered, the user should attempt to send a test message. Upon searching the directory in the app, the user will be prompted to authenticate to the local Spok directory. The user will need to use the username/messaging ID and password combination in the Spok database to authenticate locally.
- ✓ *Test Messaging and Train User*
  After registering a new device, test messages should always be sent and receipt confirmed to ensure all messaging services have been registered and configured properly. The user should be trained on essentials they need to know (see new registration workflow).

## TERMINATIONS

**Deactivations**: As users leave the organization, IT admins need to be able to remove and archive data in a secure way without impacting the user's non-hospital related data. Removing data from systems can be challenging as many healthcare users are in multiple roles and/or may leave only temporarily at times. Therefore, it is considered a best practice to 'deactivate' records by removing access and visibility without fully deleting all trace of a user, until they are known to have left the organization permanently in every capacity. An automated script should be written to remove records that have been 'deactivated' for a period of time.




- ✓ *Remove Data from Device*
  It is important to remove any sensitive data from the user's device. If the device is owned by the hospital, the best practice is to wipe the device (physically, or via MDM). If the device is owned by the user, the best practice is to remove the app (via MDM or by the user, enforced by policy). If the app is not removed before the device no longer in possession and the device is unmanaged, the best practice is to use the Spok Admin tool to wipe messages from the app.

- ✓ *Unregister the Device*
  The device should be unregistered on the server, to prevent the user from registering any new devices.
- ✓ *Remove User Credentials and Constraints*
  All credentials should be removed from the system, such as login and password. Database constraints such as on call assignments, pagers and billing information should also be reconciled and removed.
- ✓ *Non-Publish User*
  The user should be non-published and/or the device should be removed from his/her record so that they are no longer visible in searches within Spok applications.
- ✓ *Place User On Unavailable Status*
  The user should be placed on an unavailable status to ensure that no one is able to send a message to the user. Note that removing all messaging devices from the user's profile will also require the status to reflect unavailable.

## CONCLUSION

There may be exceptions and corner-cases that need to be considered that require a departure from the advice in this document – however, the intention of this guide is to offer a comprehensive baseline on how to manage adds, changes and deletes while supporting users of the Spok Mobile secure text messaging service. By following the best practices workflows outlined in this guide, IT administrators can help provide a service that offers utility and warranty of service and an excellent user experience. This will help lead to higher levels of user satisfaction and adoption, ultimately ensuring value can be delivered to the organization.