Table of Contents

Welcome to Sprint ................................................................. 1

Getting Started ................................................................. 2

What is the Sprint Business Mobility Framework (SBMF)? .............. 3

What is the Sprint Business Mobility Framework Manager (SBMFM)? 3

Enabling a Third-Party Organization to Deploy Applications .......... 4

Accessing the SBMFM Administrative Portal .................................. 5

Signing onto SBMFM ................................................................ 5

Exiting the SBMFM Administrative Portal .................................... 7

Administrator Reminders ......................................................... 8

Changing and Retrieving Passwords ........................................... 9

Changing The Initial Password ................................................ 9

Retrieving Passwords ............................................................ 12

My Work List ........................................................................... 12

Navigating in the SBMFM Administrative Portal ............................. 13

Managing Domains .................................................................. 14

About Domains ...................................................................... 15

Domain Management .............................................................. 15

Viewing Domain Information .................................................. 15

Assigning Telecom Administrators ........................................... 17

Viewing Messages ................................................................... 18

Managing SBMFM Administrative Portal Users ............................. 20

About SBMFM Administrative Portal User Roles ....................... 21

SBMFM Administrative Portal User Management ........................................ 21

Viewing SBMFM Administrative Portal User Profile Information .... 22

Creating and Maintaining SBMFM Users ................................. 23

Adding SBMFM Administrative Portal Users ............................... 23

Deleting SBMFM Administrative Portal Users ............................. 25

Editing SBMFM Administrative Portal User Profiles .................... 26

Managing SBMFM Administrative Portal User Passwords .......... 26

Resetting SBMFM User Passwords .......................................... 27

Changing SBMFM Administrative Portal Passwords ................. 27

Viewing SBMFM Administrative Portal User Activity Record ......... 29

Managing Applications .......................................................... 31

About Applications ................................................................ 32

Application Types ................................................................ 32

Application Status ................................................................ 32

Pre-Approved and Pre-Rejected Lists ........................................ 33

Application Management ......................................................... 33

SBMFM Administrative Portal Third-Party Administration Guide
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing Application Details</td>
<td>34</td>
</tr>
<tr>
<td>Filtering Application Search Results</td>
<td>36</td>
</tr>
<tr>
<td>Application Details</td>
<td>37</td>
</tr>
<tr>
<td>Editing Application Info</td>
<td>39</td>
</tr>
<tr>
<td>Viewing Service Level Agreement Info</td>
<td>41</td>
</tr>
<tr>
<td>Viewing Service Usage</td>
<td>42</td>
</tr>
<tr>
<td>Viewing New Applications</td>
<td>44</td>
</tr>
<tr>
<td>Managing Administrators Assigned to Applications</td>
<td>45</td>
</tr>
<tr>
<td>Assigning Telecom Managers to Applications</td>
<td>45</td>
</tr>
<tr>
<td>Removing a Telecom Manager</td>
<td>47</td>
</tr>
<tr>
<td>Maintaining Pre-Approved and Pre-Rejected Lists</td>
<td>48</td>
</tr>
<tr>
<td>Maintaining Pre-Approved Lists</td>
<td>48</td>
</tr>
<tr>
<td>Removing Devices from the Pre-Approved List</td>
<td>49</td>
</tr>
<tr>
<td>Adding Devices to the Pre-Approved List</td>
<td>51</td>
</tr>
<tr>
<td>Maintaining Pre-Rejected Lists</td>
<td>56</td>
</tr>
<tr>
<td>Removing Devices from the Pre-Rejected List</td>
<td>57</td>
</tr>
<tr>
<td>Adding Devices to the Pre-Rejected List</td>
<td>59</td>
</tr>
<tr>
<td>Managing Application Invitations</td>
<td>64</td>
</tr>
<tr>
<td>Inviting Devices to Join Applications</td>
<td>64</td>
</tr>
<tr>
<td>Canceling Invitations</td>
<td>70</td>
</tr>
<tr>
<td>Managing Subscriptions Requests</td>
<td>70</td>
</tr>
<tr>
<td>Approving and Rejecting Subscription Requests</td>
<td>70</td>
</tr>
<tr>
<td>Approving a Subscription Request (Method 1)</td>
<td>71</td>
</tr>
<tr>
<td>Rejecting a Subscription Request (Method 1)</td>
<td>71</td>
</tr>
<tr>
<td>Approving a Subscription Request (Method 2)</td>
<td>72</td>
</tr>
<tr>
<td>Rejecting a Subscription Request (Method 2)</td>
<td>73</td>
</tr>
<tr>
<td>Approving a Subscription Request (Method 3)</td>
<td>75</td>
</tr>
<tr>
<td>Rejecting a Subscription Request (Method 3)</td>
<td>77</td>
</tr>
<tr>
<td>Canceling Subscriptions</td>
<td>79</td>
</tr>
<tr>
<td>Managing Devices</td>
<td>80</td>
</tr>
<tr>
<td>About Devices</td>
<td>81</td>
</tr>
<tr>
<td>Device Management</td>
<td>81</td>
</tr>
<tr>
<td>Viewing Device Details</td>
<td>82</td>
</tr>
<tr>
<td>Looking Up Device Details</td>
<td>82</td>
</tr>
<tr>
<td>Viewing Group Membership</td>
<td>84</td>
</tr>
<tr>
<td>Updating Device Details</td>
<td>85</td>
</tr>
<tr>
<td>Updating the Display Name</td>
<td>85</td>
</tr>
<tr>
<td>Allowing SMS Invitations</td>
<td>86</td>
</tr>
<tr>
<td>Managing Administrators Assigned to Devices</td>
<td>86</td>
</tr>
<tr>
<td>Removing a Telecom Manager</td>
<td>87</td>
</tr>
</tbody>
</table>
Welcome to Sprint.

Sprint is a global telecommunications service provider that offers a total networking solution - one that integrates wireline and wireless services – so you and your employees can stay connected seamlessly virtually anytime, anywhere. With a single point of contact for data, internet, voice and wireless solutions, responsive customer service, and uncompromising network reliability, no wonder more than 95 percent of the Fortune 500 choose Sprint.

This guide is intended for employees of Sprint business customers or third parties who are deploying/developing applications using Sprint Business Mobility Framework (SBMF) services. It is intended specifically for employees with administrative privileges on the Sprint Business Mobility Framework Manager (SBMFM) administrative portal. It lists in detail the functions available on the SBMFM administrative portal and the process for third parties to manage applications and devices.
Getting Started

In This Section

- What is the Sprint Business Mobility Framework (SBMF)?
- Enabling a Third-Party Organization to Deploy Applications
- Accessing the SBMFM Administrative Portal
- Changing and Retrieving Passwords
- My Work List
- Navigating in the SBMFM Administrative Portal
What is the Sprint Business Mobility Framework (SBMF)?

The Sprint Business Mobility Framework (SBMF) environment enables third-party applications to access Sprint network services to enhance application offerings to their customers, employees or individual users who use Sprint as their wireless carrier.

Network services supported in the SBMF environment include:

- Voice alert services, services that enable third party applications to play an announcement on a target device
- Location services, services that enable third party applications to get location of an authorized Sprint PCS Vision enabled device or group
- Presence services, services that enable third party applications to get the status (on or off of the network) of an authorized Sprint PCS Vision enabled device or group.
- Messaging services, services that enable third party applications to send an SMS to a Sprint device.
- Event notification services, services that enable third party applications to be notified of location changes or presence changes for authorized Sprint PCS Vision enabled devices or groups.

What is the Sprint Business Mobility Framework Manager (SBMFM)?

From the network service and application management perspective, the Sprint Business Mobility Framework Manager consists of two web-based portals: an administrative portal and a consumer portal. The administrative portal enables third parties to manage business applications and device permissions. The consumer portal, accessible through sprintpcs.com’s My PCS environment, allows individual users to manage their applications.
Enabling a Third-Party Organization to Deploy Applications

The following table summarizes the steps required by each user role, to enable a third-party to deploy and manage applications in the Sprint network using the SBMFM administrative portal.

<table>
<thead>
<tr>
<th>Sprint Administrator (SA)</th>
<th>Third-Party Telecom Administrator (TA)</th>
<th>Third-Party Telecom Administrator (TA) and Telecom Manager (TM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 – Set up 3rd Party Domain</td>
<td>2 – Manage SBMFM Portal Users (TAs and TMs)</td>
<td>3 – Manage Devices &amp; Applications</td>
</tr>
<tr>
<td>Create Domain</td>
<td>Create TAs and TMs as required</td>
<td>Create Device Groups</td>
</tr>
<tr>
<td>Assign TA</td>
<td>Create Device Groups</td>
<td>Manages Device Requests</td>
</tr>
<tr>
<td></td>
<td>Assign Applications to TMs (optional)</td>
<td>Manage Application Invitations</td>
</tr>
</tbody>
</table>

There are a number of steps that must be completed by a Sprint Administrator before a third-party can use the Sprint Business Mobility Framework (SBMF) environment network services.

Once the Sprint Administrator has completed the initial setup, an organization can then use the SBMF environment to manage its administrative users, devices and applications using the SBMFM administrative portal. For example, to deploy an application using SBMFM, a Telecom Administrator would do the following:

1. Create the additional Telecom Administrators and needed Telecom Managers. See the section Managing SBMFM Users in this guide for more information.

2. Assign applications to administrators. See the section Managing Applications for more information.

3. Define the device groups and assign a Telecom Manager to the device group. See the section Managing Device Groups in this guide for more information.

4. Manage the subscription of applications in a domain. This would be done by either a Telecom Manager or Telecom Administrator. This person would manage the device groups, application invite lists and application requests from employees in his group. See the section Managing Devices in this guide for more information.

5. Approve the application request for a device. See the section Managing Applications in this guide for more information.

The tasks in this guide, the SBMFM Administrative Portal Third-Party Administration Guide, outline how Telecom Administrators and Telecom Managers use the SBMFM administrative portal to manage third-party applications, or manage devices for business use.

The SBMFM Administrative Portal Sprint Administration Guide, outlines how Sprint Administrators use the SBMFM administrative portal to manage third-party applications in the SBMF environment.

The SBMFM Consumer Portal User Guide outlines how individual users use the SBMFM consumer portal to access corporate and third-party applications.
Accessing the SBMFM Administrative Portal

A Sprint Administrator is responsible for the initial setup of assigning one administrator to a domain. After a domain and a Telecom Administrator (TA) role have been created, the TA can create as many TA and Telecom Manager (TM) profiles that are necessary to manage domains and associated users, devices and applications. It is recommended that there are two TAs per domain.

Signing onto SBMFM

In order to access the SBMFM administrative portal, your TA or TM user profile must exist in the Sprint Business Mobility Framework Manager (SBMFM) environment prior to sign on.

For initial sign on, you are instructed to use your email address as your User ID and a temporary password, that will be sent to you in an email by a Sprint Administrator. Contact a Sprint representative if you did not receive your initial password. When you have successfully signed on, the My Work List page appears.

To sign onto the SBMFM:


2. Enter your user ID. This is your email address.

3. Enter your password. See the section entitled “Password Policy” for reference. Click Sign on. (The My Work List page appears).
### My Work List

** gayda@telus.net | [Sign off] | Domain ID: RTE25TC

### My Applications

<table>
<thead>
<tr>
<th>Application ID</th>
<th>Application Name</th>
<th>Application Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0042651900</td>
<td>TPA TESTING ACCOUNT</td>
<td>Corporate</td>
</tr>
</tbody>
</table>

Display 1 - 1 of 1  
[Work/Show all]

### Pending Device Requests (24)

<table>
<thead>
<tr>
<th>Application ID</th>
<th>Application Name</th>
<th>Device User Name</th>
<th>Device User Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>004258998</td>
<td>IBM TPA THREE</td>
<td>4192153021</td>
<td>IGSF.TEST12</td>
</tr>
<tr>
<td>0042590008</td>
<td>IBM'S TPA ONE</td>
<td>4192153021</td>
<td>IGSF.TEST12</td>
</tr>
<tr>
<td>004259014</td>
<td>IBM TPA FOUR</td>
<td>4192153021</td>
<td>IGSF.TEST12</td>
</tr>
<tr>
<td>004259019</td>
<td>IBM TPA.FIVE</td>
<td>4192153021</td>
<td>IGSF.TEST12</td>
</tr>
<tr>
<td>0042589986</td>
<td>IBM TPA TWO</td>
<td>4192153022</td>
<td>IGSF.TEST12</td>
</tr>
</tbody>
</table>

Display 1 - 5 of 24  
[Work/Show all]

### Devices

<table>
<thead>
<tr>
<th>Device ID</th>
<th>Device User Name</th>
<th>Account Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>3032461060</td>
<td>TPA TESTING ACCOUNT</td>
<td>Corporate</td>
</tr>
<tr>
<td>3032461012</td>
<td>TPA TESTING ACCOUNT</td>
<td>Corporate</td>
</tr>
</tbody>
</table>

Display 1 - 2 of 2  
[Work/Show all]

### Pending Application Invitations (13)

<table>
<thead>
<tr>
<th>Device User Name</th>
<th>Application ID</th>
<th>Application Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>THOKALA, SRDHER</td>
<td>0042590008</td>
<td>IBM'S TPA ONE</td>
</tr>
<tr>
<td>THOKALA, SRDHER</td>
<td>0042590008</td>
<td>IBM'S TPA ONE</td>
</tr>
<tr>
<td>THOKALA, SRDHER</td>
<td>0042590008</td>
<td>IBM'S TPA ONE</td>
</tr>
<tr>
<td>THOKALA, SRDHER</td>
<td>0042590008</td>
<td>IBM'S TPA ONE</td>
</tr>
</tbody>
</table>

Display 1 - 5 of 13  
[Work/Show all]

---

**Tip:** Telecom Administrators and Telecom Managers are prompted to change their passwords upon initial sign on. See “Changing and Retrieving Your Password” for details.
Exiting the SBMFM Administrative Portal

You can exit the SBMFM administrative portal at any point during a session. If you input any data or take any action, make sure you complete the process as specified, otherwise the information will be lost when you exit the session.

After thirty minutes of non-activity, the system may automatically log you off because of data security considerations. If this occurs, simply sign on as required to start a new session. Make sure that you do not leave an incomplete action or data input for more than 30 minutes to avoid losing the data.

To exit the SBMFM Administrative Portal:

- Click **Sign off** located under the page title on any main content page.
Administrator Reminders
There must be two TAs assigned to a domain. If you are signing onto the SBMFM administrative portal as the only TA for a domain, you will be reminded that you are the only TA assigned to the domain.

Once a second TA has been created, this reminder notice will not appear.

See “Managing Administrators on Existing Domains” in the Managing Domains section for details on how to add a TA to a domain.
Changing and Retrieving Passwords

When you first sign into the portal as a TA or TM, you are instructed to change your password.

If you have forgotten your password, you can submit a request to have it reset. A Sprint representative will send you an email with a one-time password and a URL to the SBMFM administrative portal. See “Retrieving Passwords.”

Password Policy

Passwords for the SBMFM administrative portal follow a password policy. This password policy is as follows:

- The password must be 8 characters long.
- The password must include 1 upper-case letter and 1 numeral. The numeral cannot be in the first position.

Changing The Initial Password

When you first sign on, you will need to change your password. TAs and TMs can also change their passwords at any time. See “Changing SBMFM Administrator Portal Passwords” in the Managing SBMFM Administrative Portal Users section of this guide.

To change a TA or TM password:

1. After signing on for the first time, the Password Change Request page displays.

   ![Password Change Request Page](image)

   See “Password Policy” for details.

2. Your User ID, which is your email address, is displayed. This field cannot be edited.

3. Enter the old password, which you were given for the first-time sign on.
Section 1: Getting Started

4. Enter and confirm your new password. Click Change Password. (The Password Change Information page displays)

   ! [Password Change Information](image)
   
   **Password Change Information**

  _raydateus.net, your new password has been set.

   Use this new password the next time you log into your account.

   Continue

5. Click Continue. (The My Work List page displays)
For details about the information displayed, see “My Work List.”
Section 1: Getting Started

Retrieving Passwords

If you have forgotten your password or need to have it reset, you can follow the steps given below:

To retrieve your password:

1. From the Sprint Business Mobility Framework Manager page, click I Forgot my password (The Retrieve Password page appears).

2. Enter your email address for the User ID.

3. Click Submit. A confirmation page displays indicating your request to reset the password has been successful.

   An error message is displayed if there is a problem with resetting your password. You will be prompted to re-enter your email address and resubmit your request.

4. Check your email to retrieve the new password.

5. Click return to Business Mobility Framework link in the email to sign onto the portal with the new password. (The Business Mobility Framework page displays).

My Work List

Upon successful sign on to the portal, as a TA or TM, the My Work List page displays. The worklist identifies tasks that need your attention and require you to take appropriate action. From this page, you can view and work with resources in your domain.

- New Applications
- Pending Device Requests
- New Devices
- Pending Application Invitations

For more information about viewing new applications, see “Viewing New Applications” in the Managing Applications section of this guide.

For more information about handling pending subscription requests, see “Managing Subscription Requests” in the Managing Applications section of this guide.

For more information about viewing new devices, see “Viewing New Devices” in the Managing Devices section of this guide.

For more information about handling invitations, see “Managing Application Invitations” in the Managing Applications section of this guide.
Navigating in the SBMFM Administrative Portal

The Sprint Business Mobility Framework Manager (SBMFM) administrative portal is based on “portlets.” Portlets are mini-portal applications, usually depicted as a small box on a web page. Portlets are developed, deployed, managed, and displayed independent of other portlets, and therefore, their state is retained with the portlet itself. This affects the way you navigate in the SBMFM administrative portal.

Use Cancel or Back if you decide to cancel a task that you initiated; otherwise, you will leave off at the point where you last halted the task. For example, you start a task such as assigning an administrator to a domain in SBMFM administrative portal, and then decide to start another task by selecting it from the left-navigation menu such as viewing new devices. The next time you select the Domains item in the left-navigation menu, you will revisit the task you were last performing such as assigning an administrator to a domain. It is important to use the Cancel or Back links in the portal if you want to accurately reflect where you are in the process of performing a task.
Managing Domains

In This Section

- About Domains
- Viewing Domain Information
- Assigning Telecom Administrators
- Viewing Messages
About Domains

A domain is a way of grouping together the Sprint Business Mobility Framework Manager (SBMFM) administrative portal users, applications and devices of a particular company so they can be administered. Sprint administrators are responsible for creating domains and assigning these domains to administrators of third-party companies.

Each domain reflects a contract, an agreement between Sprint and a third-party organization. Domains control and define the applications and devices that third-party administrators are responsible for. In effect, domains are used to segregate the administrators and their applications from other organizations in the Sprint Business Mobility Framework (SBMF) environment.

Note:
Third-party administrators are referred to as Telecom Administrators (TAs) in the SBMFM administrative portal. Third-party administrators manage applications that use Sprint network services.

You cannot create SBMFM administrative portal user profiles as a third-party administrator, if a domain has not yet been created for you. Contact a Sprint representative if a domain has not been created for your organization.

Domain Management

The domain management function in the SBMFM administrative portal allows Telecom Administrators (TAs) and Telecom Managers (TMs) to:

- View domain information
- Assign other administrators to the domain they manage

It is recommended that domains have at least two TAs assigned to them. If you are the only TA assigned to a domain, you should consider assigning another TA as a backup.

Domains include Corporate Liable and Employee Liable devices and applications. A corporate liable device is a device that is billed to the company, an employee liable device is a device that is part of the company hierarchy but billed to the employee.

Viewing Domain Information

As a TA, you can view details that are associated with the domain you manage but cannot update the details for the domain.

To view domain information:

- From the left-navigation menu, click **Domains**. (The **Domain Details** page, listing the details of the domain you manage, displays).
Section 2: Managing Domains

Tip:
To contact a Telecom Administrator by email, click the email address link on the Domain Details page. This will launch your email application and a note directed to the selected Telecom Administrator.
Assigning Telecom Administrators

There should be at least one TA responsible for a domain. If you are currently the only TA for a domain, you will be prompted by the SBMFM administrative portal the next time you sign on to assign another TA. See “Administrator Reminders” in the Getting Started section of this guide for more information.

To add a TA to an existing domain:

1. From the Domain Details page, click Assign telecom admin. (The Assign Telecom Admin page displays).

2. Enter the profile information such as:
   - Administrator’s first and last name (required)
   - Email address (required)
   - Primary and secondary contact phone number (optional).

3. Click Submit to add the TA to the account.
   OR
   Click Cancel to return to the Domain Details page without adding another TA.
Viewing Messages

Sprint Administrators (SA)s can create messages that are displayed to users of the Sprint Business Mobility Framework Manager (SBMFM) administrative portal to notify them about such things as scheduled and unscheduled outages or other general information. As a Telecom Administrator (TA) or Telecom Manager (TM), you are able view these messages.

To view the message board:
1. In the My Work List page, go to the Message Board section.

![My Work List](image)

The Message Board lists all the active messages on the system, by title.
2. Click a Message Title in the Message Board. (The My Work List page is refreshed with the Message Description displayed in the Message Board).
Managing SBMFM Administrative Portal Users

In This Section

- About SBMFM Administrative Portal User Roles
- Viewing SBMFM Administrative Portal User Profile Information
- Creating and Maintaining SBMFM Users
- Managing SBMFM Administrative Portal User Passwords
- Viewing SBMFM Administrative Portal User Activity Record
About SBMFM Administrative Portal User Roles

The Sprint Business Mobility Framework Manager (SBMFM) administrative portal offers centralized administration of users. This enables third-party application administrators (referred to in the SBMFM administrative portal as Telecom Administrators) to create SBMFM administrative portal users and define access to applications in the Sprint Business Mobility Framework (SBMF) environment.

Before a Telecom Administrator (TA) can define SBMFM administrative portal users and assign those users to manage domains and other resources in the SBMF environment, a Sprint Administrator must first create a TA user profile. Once a domain and a TA have been defined, the third-party organization can then use the SBMFM administrative portal to manage its domains, users, device groups, devices and applications.

The following table describes the user privileges of the TA and Telecom Manager (TM) that use the SBMFM administrative portal.

<table>
<thead>
<tr>
<th>SBMFM Administrative Portal User Role</th>
<th>User Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telecom Administrator (TA)</td>
<td>Has full administrative rights throughout a single domain and can only perform tasks against user accounts belonging to his or her organization. The TA can administer Telecom Managers, applications and devices within their company's domain.</td>
</tr>
<tr>
<td>Telecom Manager (TM)</td>
<td>Has limited administration rights, known as managerial rights, within a single domain. The TM represents an organization having one or more applications but with jurisdiction over a subset of billing accounts, or groups within a billing account, within a domain assigned by a TA.</td>
</tr>
</tbody>
</table>

SBMFM Administrative Portal User Management

The user management function in the SBMFM administrative portal allows TAs and TMs to:

- View SBMFM Administrative Portal User Profile Info
- Create and Maintain SBMFM Administrative Portal User Profiles
- Manage SBMFM Administrative Portal User Passwords

A Sprint Administrator must create the first TA profile in the SBMFM administrative portal, for a specific domain, before the third-party administrator (TA) can create other TAs and TMs.
Section 3: Managing SBMFM Users

Viewing SBMFM Administrative Portal User Profile Information

As a TA, you can view summary information associated with SBMFM administrative portal users, in your domain. This information includes:

- Assigned third-party applications details such as the IDs and names
- Assigned device information details such as device IDs, names and the account type
- Assigned device groups

**Note:** Telecom Managers are only able to view their own profile details.

To view SBMFM administrative portal user profile information:
As a TA, you can view user profile details by using the My User List page. However, the list of users displayed will be restricted to your domain.

1. From the left-navigation menu, click **Telecom Users**. (The My User List page appears).

2. You can filter the results by selecting a SBMFM administrative portal user role and clicking **Go**.

3. Select a user for which you want to view details by clicking the user name. (The User Details page displays).
Creating and Maintaining SBMFM Users

Only Sprint Administrators (SAs) and TAs can create and delete SBMFM administrative portal users. Editing user profile information can be done by SAs, TAs and TMs with restricted access.

Adding SBMFM Administrative Portal Users

Users can be added to the SBMFM administrative portal, after a single TA has been created and assigned to a domain by a SA.

**To add a user to the SBMFM administrative portal:**
As a TA, you can add TA and TM user profiles to your domain.

1. From the left-navigation menu, click **Telecom Users**. (A submenu expands).
2. From the submenu, click **Add New User**. (The Add New User page appears).
3. Enter the first and last name for the user profile (required).
4. Select a role from the drop-down menu (required).
5. Enter and confirm the email address for the user (required).

**Note:** The email address will be used as the user ID to sign onto the SBMFM administrative portal.

6. Enter the primary and secondary phone number for the user profile (optional).
7. Click **Submit**. (The Add New User Confirmation page displays.)
Section 3: Managing SBMFM Users

8. Verify the user profile information.
   From this page you can click Add new user to add another user to the domain.

Deleting SBMFM Administrative Portal Users
TAs, as well as SAs, can delete users from the SBMFM administrative portal. TMs cannot delete users.

To delete a user from the SBMFM administrative portal:
As a TA, you can delete TA and TM user profiles from your domain.
1. From the left-navigation menu, click Telecom Users. (The My User List page appears).
2. From the list of user names, click the one that you want to delete. (A User Details page displays).
3. Click Delete to remove the user from the SBMFM administrative portal database. (The Delete Profile page displays).
4. Click Submit to confirm or Cancel to return to the User Details page.
Section 3: Managing SBMFM Users

Editing SBMFM Administrative Portal User Profiles

A TA or TM can edit user details such as the first or last name, as well as the primary or secondary phone number. Information such as the email address and the domain ID cannot be modified.

**Note:**
A Telecom Manager can only update their own SBMFM administrative portal user details, and not the details of other SBMFM administrative portal users.

To edit SBMFM administrative portal user profile details:

1. Select a user that you want to change details for. (A User Details page appears).
2. Click **Edit**. (The Edit User Details page displays).
3. Modify the names, SBMFM administrative portal user role or phone number field information as required.

**Note:**
If you are a Telecom Manager, you cannot modify the User Role field.
If you are a Telecom Administrator, you can modify this field for others but not if it is your own user profile.

4. Click **Submit** to save the details or **Cancel** to return to the User Details page.

Managing SBMFM Administrative Portal User Passwords

SBMFM administrative portal passwords are managed by SAs. See the *Getting Started* section in this guide for reference to the SBMFM administrative portal password policy.
Resetting SBMFM User Passwords

TAs can reset passwords for TMs and other TAs. To reset own password, see “Retrieving Passwords” in the Getting Started section of this guide.

To reset SBMFM administrative portal user passwords:

1. From the left-navigation menu, click Telecom Users. (The My User List page appears).
2. From the list of SBMFM administrative portal user names, click the user profile for which you want to reset the password. (The User Details page displays).
3. Click Reset Password. (The Reset Password page displays).
4. Enter the email address that was provided upon registration.
5. Click Submit to confirm or Cancel to return to the User Details page without requesting the password reset. Upon successfully resetting the password, an email message will be sent to the user’s email address with a one-time password and URL to the SBMFM administrative portal.

Changing SBMFM Administrative Portal Passwords

The first time that you sign onto the SBMFM administrative portal, you are required to change your password. See “Changing Your Initial Password” in the Getting Started section of this guide for more information. TAs and TMs can change their password at anytime.

To change your SBMFM administrative portal password:

1. From the left-navigation menu, click Telecom Users. (The User Details page appears).
2. Click **Change password**. (The Change Password page displays).

3. Enter the old password.

4. Enter the new password and confirm the new password.

5. Click **Submit** to confirm or **Cancel** to return to the **User Details** page.
Viewing SBMFM Administrative Portal User Activity Record

Telecom Administrators (TAs) and Telecom Managers (TMs) can view a record of past activity associated with users in their Domain, via the Sprint Business Mobility Framework Manager (SBMFM) administrative portal.

To view SBMFM administrative portal user activity record:
TAs can view activity associated with any TA or TM users in their domain. TMs can also view the same information.

As a TA, there are two ways you can view SBMFM administrative portal user activity. You can either enter a User ID to look up specific user's activity record or leave the User ID blank to view an activity record for all TAs and TMs associated with a domain.

1. From the left-navigation menu, click **Telecom Users**. (A submenu expands).
2. Click **Activity Record**. (The **Activity Record** page displays).
3. Specify the Begin Date and End Date for the activity period.

**Note:** The activity period begin date must be within the last 60 days and the end date must be within 31 days of the begin date.

4. Optionally enter a User ID and click **Get Record**. (The **Activity Record** page lists all activity for the specified criteria).
The following activity information is displayed:

- The number of items in the activity record for the specified date range
- The date and time of the activity (Time CST)
- The User ID of the user that requested the activity (Users).
- The categorization of activity performed (Area Affected)
- The name of the activity performed (Activity Performed)
- The result of the activity performed (0 for a successful activity or an error code). A number of error codes have been defined. These are specific to the system of error and are intended to be helpful for troubleshooting. (Result Code)
Managing Applications

In This Section

- About Applications
- Viewing Application Details
- Viewing Service Level Agreement Info
- Viewing Service Usage
- Viewing New Applications
- Managing Administrators Assigned to Applications
- Maintaining Pre-Approved and Pre-Rejected Lists
- Managing Application Invitations
- Managing Subscription Requests
About Applications
Sprint Business Mobility Framework (SBMF) applications are those that are operated by Sprint corporate customers and which have been mobile-enabled using Sprint’s network services. These business applications can range from personal productivity use to enterprise-wide system use, to specialized system administration tools for use by third-party administrators.

Note: Third-party administrators are referred to as Telecom Administrators (TAs) in the SBMFM administrative portal. Third-party administrators manage applications that use Sprint network services.

Applications are provisioned in the Sprint billing system and then activated by Sprint Administrators (SAs) using the Sprint Business Mobility Framework Manager (SBMFM) administrative portal.

Application Types
There are many values that define the application and their use in the SBMFM administrative portal. One of the main attributes defining an application and its use is the account type.

There are three account types associated with applications:

- Public - All SBMFM administrative portal users can view a public application and hence can request to join the application on behalf of devices in their domain. All SBMFM consumer portal users can also view a public application and hence can request to join the application.

- Corporate - A corporate application is one that can be viewed by a SBMFM administrative portal user in the same domain as the application. For example, a company-owned application such as a mobile-enabled employee directory. SBMFM consumer portal users who are part of the same company as the corporate application can view the application and hence can request to join the application.

- Private - A private application is one that can be viewed by a Telecom Administrator of the domain the application is part of, or by the Telecom Manager, that has been assigned to manage the application. SBMFM consumer portal users cannot view a private application and hence cannot request to join the application.

Applications are provisioned outside of the SBMFM administrative portal. During provisioning they are associated with different types of Sprint Business Mobility Framework (SBMF) services such as a location-based service (getLocation) or short-message service (sendSMS). These services cannot be changed in the SBMFM administrative portal once the application has been provisioned.

Application Status
In addition to type, an application also has a status associated with it which defines how it is used in the SBMFM administrative portal. Application states are as follows:

- Submitted for Testing
- In Testing
- Rejected
- Certified
- Active
- Disabled

Submitted for Testing - the application has been submitted to Sprint and is scheduled for testing.
In Testing - the application is currently undergoing testing in the Sprint network.
Rejected - the application failed testing and can not be deployed in the Sprint network.
**Certified** - the application has passed testing and can be deployed in the Sprint network.

**Active** - the application has been activated in the SBMFM administrative portal.

**Disabled** - the application has been made unavailable for service in the Sprint network.

Once an application is activated, its status can change from Active to Disabled, or Disabled to Active. It cannot change from Active to Rejected or Active to Certified.

An SA must first provision the application and then activate it before it can be made available to third-party administrators for use. When an application is provisioned, it must have the necessary details for associating it with Sprint’s network services. The SA must ensure that the associated virtual telephone number and invitation text are defined for an application. A virtual telephone number is displayed as the caller ID number on the receiving device when performing network-initiated voice browsing services. Invitation text is the message that will be displayed on the device when user clicks on the URL in the invite SMS.

Once the application has been provisioned, then activated, it can be made available to the appropriate SBMFM administrative portal administrators.

**Pre-Approved and Pre-Rejected Lists**

When an application is first activated, application subscription can be controlled through the mechanism of Pre-Approved and Pre-Rejected lists. Similar to managing unwanted e-mail, Pre-Approved and Pre-Rejected lists in the SBMFM administrative portal provide TAs and TMs with a means of filtering which devices can request subscriptions to join an application.

If a device is on a Pre-Approved List, it means that in the event the device requests access to the application, it will be automatically approved. If a device is on a Pre-Rejected list, it means that if the device requests access to the application, it will be automatically rejected. If you knew which devices you wanted to restrict and approve from application subscription, this would be the default option.

Other options to help you define access to applications in the SBMF environment are:

- Auto-accept if not on Pre-Rejected List and
- Auto-reject if not on Pre-Approved List

Auto-accept if not on Pre-Rejected List means that if a device is not on the Pre-Rejected List, a subscription request from the device will be automatically approved. If you don’t know who you want to approve, but you know who you want to reject, use this option.

Auto-reject if not on Pre-Approved List means that if a device is not on the Pre-Approved List, a subscription request from the device will be automatically rejected. If you know who you want to approve, but not reject, use this option. This is a good option as well if you only want to do invitations and not requests.

**Application Management**

The Application Management function in the SBMFM administrative portal allows TAs to:

- Find and View Application Information
- Update Application Details
- Assign Applications to Telecom Managers
- Manage Application Invitations
- Maintain Pre-Approved and Pre-Rejected lists for Applications
- Manage Subscription Requests

Before an application can be used by a third-party administrator, a SA must perform some setup activities. An application’s status must be Active before it can be assigned to a TM or invitations to join an application can be sent.
Section 4: Managing Applications

Viewing Application Details

As a TA, you can search for a specific application if you know its ID or list applications within your domain to view details associated with it.

To view application information:

1. From the left-navigation menu, click Applications. (The My Application List page displays).

   ![Applications Page](image.png)

All of the applications in your domain are listed. You can change the display results for the applications listed in your domain. See “Filtering Application Search Results”.

2. Select an application from the results listed to view its detail. (An Application Details page displays).

   If you want to search for a specific ID, enter the Application ID (max. 15 characters) and click Look up. (An Application Details page displays).
To learn more about details associated with a specific application, see “Application Details”.

<table>
<thead>
<tr>
<th><strong>Domain ID</strong></th>
<th>RTB2STIC</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application ID</strong></td>
<td>0042580084</td>
</tr>
<tr>
<td><strong>Application Name</strong></td>
<td>IBM TPAS TWO</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>Active</td>
</tr>
<tr>
<td><strong>Website</strong></td>
<td><a href="http://www.sprint.com">http://www.sprint.com</a></td>
</tr>
<tr>
<td><strong>Help Desk Number</strong></td>
<td>9188309999</td>
</tr>
<tr>
<td><strong>Virtual Telephone Number</strong></td>
<td>9188309999</td>
</tr>
<tr>
<td><strong>Invitation Text</strong></td>
<td>You are invited to use an application</td>
</tr>
<tr>
<td><strong>Automatic Handling</strong></td>
<td>N</td>
</tr>
</tbody>
</table>

**Telecom Manager**
- **Email**: dmoran@comcast.com

**Device Association**

**Subscription Request**
- Show All

**Application Invitations**
- Show All

**Current Subscriptions**
- Show All

**Application Pre-Rejected List**
- Show details
- Add more devices to the Pre-Rejected List

**Application Pre-Approved List**
- Show details
- Add more devices to the Pre-Approved List

**Modifed Date**: 12/29/2004
Section 4: Managing Applications

Filtering Application Search Results

You can use display filters to refine your search results.

To change the results of the listed application information, select one or more of the filters and click Go.

To filter application search results:

To list applications by assigned TM, change the Assigned Telecom Manager value to one of the following:

- Yes
- No

The All (default) setting lists applications that have been and haven’t been assigned to TMs.

To list applications by type, change the Application Type value to one of the following:
Corporate
Public
Private

The All (default) setting lists applications of all account types.

To list applications by status, change the **Application Status** value to one of the following:

- Active
- Certified
- Disabled
- Rejected
- Submitted For Testing
- In Testing

The All (default) setting lists applications in all states.

**Application Details**

You can view details such as the description, type of service, status, and assigned TMs by viewing the application’s details. From the Application Details page, you can:

- Update Application details
- Add and remove TMs from the application
- View Service Level Agreement info
- Approve or reject subscription info
- Invite or cancel devices to join the application
Details associated with the application include:

- domain associated with the application (Domain ID)
- ID associated with the application (Application ID)
Section 4: Managing Applications

- user-friendly name identifying the application (Application Name)
- text description of the application (Description)
- whether the application is for corporate, public or private use (Account Type)
- associated SBMF service; Location, User Status, Messaging etc
- whether the application is Active, Certified, Disabled, Rejected, Submitted for Testing, In Testing (Status)
- company URL that is associated with the application (Application Website)
- contact phone number for support-related issues for the application (Company Help Desk Number)
- phone number that is displayed as the caller ID number on the receiving device when doing network-initiated voice browser (Virtual Phone Number)
- message text that will be displayed when the recipient clicks the URL in the text message sent to the device to join applications (Invitation Text)
- whether the invitations to join applications are automatically handled, accept invitation if not on pre-rejected list (Auto-accept if not on Pre-Rejected List), reject invitation if not on pre-approved list (Auto-reject if not on Pre-Approved List), exempt from using Pre-Approved or Pre-Rejected lists (Per Pre-Approved and Pre-Rejected Lists)
- person who last edited the application details (Last Modified By)
- date when the application details were last edited (Modified Date)

Editing Application Info
As a TA or TM, you can update the details for an application such as the name of an application, its description and account type.

To edit application details:
1. From the Application Details page, click Edit. (The Edit Application Details page displays).
2. Edit any of the following fields:
   - Name
   - Description (max. 4000 characters)
   - Account Type
   - Application Website
   - Help Desk Number
   - Automatic Handling (for Subscription Requests)

   You cannot change the Application ID, Business Mobility Service, Status, Virtual telephone number or Invitation Text fields. Refer to the previous task “Viewing Application Details” for a description of the fields listed.

3. Click **Submit** to save your changes.
   OR
   **Cancel** to return to the Application Details page without saving.
Section 4: Managing Applications

**Viewing Service Level Agreement Info**

Service Level Agreement (SLA) defines the number of transactions for each of the Sprint Business Mobility Framework (SBMF) services that an application is entitled to send within a certain period of time. Applications exceeding their SLA transactions will encounter errors. The SA sets up the SLA data for an application before it can be used in the SBMF environment.

**To view service level agreement info for an application:**

- From the Application Details page, click **Service Level Agreement**. (The Service Level Agreement page displays for the selected application).

The virtual phone number for the application along with the following details is listed:

- SBMF service APIs associated with the application. Valid values include SMS, Location, Triggered Location, Status, Triggered Status, Make a Call, Charge Volume.
- Maximum number of Transactions per second (TPS) for each service and combined TPS for all services.
- Whether the associated service API state is On or off.
Viewing Service Usage

TAs and TMs can view detailed report information about service usage for each application. You also have the option of downloading the summary report or printing it.

To view service usage information for an application:

1. From the left-navigation menu, click Service Usage. (The My Service Usage page displays).

2. Enter the application ID for the application that you want to run a service usage report for.

3. Click Look up. (The Service Usage Summary page displays).

4. In the View Usage section, specify the Begin and End dates for the report. Select a month, date and year for each field. You must select valid dates for these fields in order to proceed.

Note: The requested report can only span 31 days at a time.
5. Click **Get Report**. (The Service Usage Summary (with Results) page displays).

The following service usage information is displayed:

- The number of usage transactions for the specified date range (Date/Time CST)
- The names of the services associated with the application (API Name)
- The devices associated with these services (Target Device)

**Note:** If you receive an error during your search, limit your search to a lesser number of days. The maximum number of transactions that can be displayed is 48,000.

From this page, you can print the report, download it or look up service usage for another application.

- To print the report, click **Printable Version**.
- To download, click **Download Report**.
- To look up the service usage for another application, click **Look up another application**. Repeat steps 1-5.
Section 4: Managing Applications

Viewing New Applications

Applications that are added to a billing account show up as new applications in the domain that the billing account is part of. TAs can view these applications in the “New Applications” section for 7 days beginning the day the application is added to the billing account. TMs can only view new applications assigned to them.

To view new applications:

1. From the left-navigation menu, click Applications. (A submenu expands).


3. From this page, you can view details associated with an application or assign a TM to an application. See the following section “Managing Administrators Assigned to Applications” for more information.
Managing Administrators Assigned to Applications

Once an application is activated, you can assign a TM to administer the application to manage Pre-Approved and Pre-Rejected lists, invitations and subscriptions. You can also remove a TM from managing the application.

**Note:** Only Sprint Administrators and Telecom Administrators can assign Telecom Managers to applications. Telecom Managers cannot assign Telecom Managers to applications.

Assigning Telecom Managers to Applications

As a TA, you can assign a TM to manage an application.

**To assign a Telecom Manager to an application:**

1. Select an application for which you want to assign a TM. (The Application Details page displays).
2. In the Application Details page, go to the Telecom Managers section.
3. Click **Assign manager**. (The Assign Telecom Manager page displays).
4. From the list of TMs, select the one that you want to assign to the application. Only one TM can be assigned at a time.
5. Click **Assign**. The TM has been assigned to the application.
   OR
   Click **Cancel** to return to the Application Details page without assigning the TM.
To assign several applications to a single Telecom Manager:
1. In the My Applications List page, select the check box beside each application you wish to assign the particular Telecom Manager to.

2. Click Assign Telecom Manager. (The Assign Telecom Manager page displays).
3. Verify that the list of applications is correct.

4. Select the radio button next to the name of the Telecom Manager you wish to assign to the chosen applications.

5. Click **Assign**. (The My Applications List page displays with the updated information).

**Removing a Telecom Manager**

As a TA, you can remove a TM assigned to an application.

**To remove a Telecom Manager from an application:**

1. Select an application for which you want to remove a TM. (The Application Details page displays).

2. In the Application Details page, go to the Telecom Managers section.

3. Click **Remove** beside the TM name that you want to remove from the application. (A confirmation page displays).
Section 4: Managing Applications

4. Verify that this is the TM that you want to remove and click **Remove**. The TM will be removed from the list of TMs listed for the application.

   OR

   Click **Cancel** to return to the Application Details page without removing the TM.

Maintaining Pre-Approved and Pre-Rejected Lists

As defined in the Introduction to this section, the devices that an application can access can be controlled through the mechanism of Pre-Approved and Pre-Rejected lists. TAs or TMs assigned to the application can manage Pre-Approved and Pre-Rejected Lists.

Maintaining Pre-Approved Lists

Pre-Approved Lists identify a list of devices, subscription requests coming from which are automatically approved and hence do not require the administrator to approve the subscription request. As a TA or TM, you can view, remove and add devices to Pre-Approved Lists for an application.

To view the Pre-Approved List for an application:

1. Select an application for which you want to view the list of devices that have been pre-approved for application subscription. (The Application Details page displays).

2. In the Application Details page, go to the Pre-Approved List section.

3. Click **Show details**. (The Application Pre-Approved List page displays).
Any pre-approved devices are listed in the Application Pre-Approved List page. If there are no devices on the Pre-Approved List, you can add some devices to this list. See “Adding Devices to the Pre-Approved List” for details.

For each device that appears in the Pre-Approved List, the following is displayed:

- The device identifier
- The user-friendly description or name of the device
- The account type. These types are: Corporate, Employee or Individual.

Removing Devices from the Pre-Approved List

As a TA or TM, you can remove a device from the Pre-Approved List for an application. Subscription requests from such a device will then have to be approved by an administrator.

Devices can only be removed from the Pre-Approved List if the application’s status is Active. If it is not active, you cannot remove a device from the Pre-Approved List.

To remove a device from the Pre-Approved List:

1. Select an application for which you want to remove devices that have been pre-approved for application subscription. (The Application Details page displays).

2. In the Application Details page, go to the Pre-Approved List section.
3. Click **Show details**. (The Application Pre-Approved List page displays).

4. In the **Application Pre-Approved List** page, select the devices that you want to remove.

5. Click **Remove**. A confirmation page displays.

6. The devices that you have removed are listed on the confirmation page. When you click **Back to Pre-Approved List**, the devices that were removed will no longer appear on the application’s Pre-Approved List.

Not only can you remove devices from a Pre-Approved List but you can also automatically move them to the Pre-Rejected List. This ensures that the selected devices will no longer receive invitations to join an application.
To move devices from the Pre-Approved List to the Pre-Rejected list:

1. From the Application Pre-Approved List page, select the devices that you want to move.

2. Click Move to Pre-Rejected List. A confirmation page displays.

3. The devices that you have moved from the Pre-Approved List to the Pre-Rejected List are detailed on the confirmation page. When you click Back to Pre-Approved List, the devices that you moved will no longer appear on the application's Pre-Approved List and will have been added to the Pre-Rejected List.

Adding Devices to the Pre-Approved List

As a TA or TM, you can add devices to the Pre-Approved List. There are some options when adding devices to an application’s Pre-Approved List. You can

- add devices from the same domain as the application
- look up a specific device
- add devices from a specific device group

To add a device to the Pre-Approved List:

1. Option 1, on the Application Details page, go to the Pre-Approved List section, click Add more devices to the Pre-Approved List. (The Application Pre-Approved List page displays).

   OR
Section 4: Managing Applications

2. Option 2, from the Application Pre-Approved List page, click Add more devices. (The Add Devices to Pre-Approved List page displays).

3. Select the method on how devices will be added to the Pre-Approved List. You must select an option to proceed.

To add devices from the same domain:

- On the Add Devices to Pre-Approved List page, click Choose devices from within this Domain and click Continue. (The Add Devices: Choose from within this Domain page displays).
From the list of eligible devices, check the ones that you want to add. If you want to select all the eligible devices, click the **Select All** checkbox.

**Note:** This list excludes those devices currently on the Pre-Approved List.

Click **Add**. A page appears summarizing the devices that you added to the application’s Pre-Approved List.
Section 4: Managing Applications

To add a specific device:

- On the Add Devices to Pre-Approved List page, click **Look up a specific device** and click **Continue**.  (The Add Devices: Look up a specific device page displays).

- Enter the ID for the device you want to add. This ID must be 10 characters in length.

- Click **Add**. A page appears summarizing the device that you added to the application’s Pre-Approved List.
To add devices from a specific device group:

- On the Add Devices to Pre-Approved List page, click **Choose devices from a Device Group** and click **Continue**. (The Add Devices: Choose from a Device Group page displays).

- From the list of groups, check the one that you want to select devices from.

- Click **Select**. (The Add Devices Choose from a Device Group page displays).
Section 4: Managing Applications

- From the list of eligible devices, check the ones that you want to add. If you want to select all the eligible devices, click the **Select All** checkbox.

- Click **Add**. A page appears summarizing the devices that you added to the application’s Pre-Approved List.

4. Successful device additions to the Pre-Approved List are displayed on the confirmation page. To add more devices to the Pre-Approved List, click **Back to Pre-Approved List**.

**Maintaining Pre-Rejected Lists**

Pre-Rejected Lists identify a list of devices, subscription requests coming from which are automatically rejected and hence do not require the administrator to view and reject the subscription request. As a TA or TM you can view, remove and add devices to Pre-Rejected Lists for an application.

**To view the Pre-Rejected List for an application:**

1. Select an application for which you want to view the list of devices that have been pre-rejected for application subscription. (The Application Details page displays).

2. In the Application Details page, go to the Pre-Rejected List section.
3. Click **Show details**. (The Application Pre-Rejected List page displays).

Any pre-rejected devices are listed in the Application Pre-Rejected List page. If there are no devices on the Pre-Rejected List, you can add devices to this list. See “Adding Devices to the Pre-Rejected List” for details.

For each device that appears in the Pre-Rejected List, the following information is displayed:

- The device identifier
- The user-friendly description or name of the device
- The account type. These types are: Corporate, Employee or Individual.

**Removing Devices from the Pre-Rejected List**

As a TA or TM, you can remove a device from the Pre-Rejected List for an application.

Devices can only be removed from the Pre-Rejected List if the application’s status is Active. If it is not active, you cannot remove a device from the Pre-Rejected List.

**To remove a device from the Pre-Rejected List:**

1. On the Application Pre-Rejected List page, select the devices that you want to remove.
2. Click **Remove**. (A confirmation page displays).

![Confirmation page](image1.png)

3. The devices that you have removed are listed on the confirmation page. When you click **Back to Pre-Rejected List**, the devices that were removed will no longer appear on the application’s Pre-Rejected List.

You can not only remove devices from a Pre-Rejected List but also automatically move them to the Pre-Approved List.

**To move devices from the Pre-Rejected List to the Pre-Approved List:**

1. From the Application Pre-Rejected List page, select the devices that you want to move.

2. Click **Move to Pre-Approved List**. (A confirmation page displays).

![Confirmation page](image2.png)

3. The devices that you have moved from the Pre-Rejected List to the Pre-Approved List are detailed on the confirmation page. When you click **Back to Pre-Rejected List**, the devices that you moved will no longer appear on the application’s Pre-Rejected List and will have been added to the Pre-Approved List.
Adding Devices to the Pre-Rejected List

As a TA or TM, you can add more devices to the Pre-Rejected List. There are some options when adding devices to an application’s Pre-Rejected List. You can

- add devices from the same domain as the application
- look up a specific device
- add devices from a specific device group

To add a device to the Pre-Rejected List:

1. Option 1, on the Application Details page, go to the Pre-Rejected List section. Click Add more devices to the Pre-Rejected List. (The Add Devices to Pre-Rejected List page displays).

   OR

2. Option 2, from the Application Pre-Rejected List page, click Add more devices. (The Add Devices to Pre-Rejected List page displays).

3. Select the method on how devices will be added to the Pre-Rejected List. You must select an option to proceed.

   To add devices from the same domain:

   - On the Add Devices to Pre-Rejected List page, click Choose from within this Domain and click Continue. (The Add Devices: Choose from within this Domain page displays).
From the list of eligible devices, check the ones that you want to add. If you want to select all the eligible devices, click the **Select All** checkbox.

- **Note:** This list excludes those devices currently on the Pre-Rejected List.

- Click **Add**. A page appears summarizing the device(s) that you added to the application’s Pre-Rejected List.
To add a specific device:

- On the Add Devices to Pre-Rejected List page, click **Look up a specific device** and click **Continue**. (The Add Devices: Look up a specific device page displays).

- Enter the ID for the device you want to add. This ID must be 10 characters in length.

- Click **Continue**. A page appears summarizing the device that you added to the application’s Pre-Rejected List.
To add devices from a specific device group:

- On the Add Devices to Pre-Rejected List page, click **Choose devices from a Device Group** and click **Continue**. (The Add Devices: Choose from a Device Group page displays).

- From the list of groups, check the one that you want to select devices from.

- Click **Select**. (The Add Devices: Choose from a Device Group page displays).
• From the list of eligible devices, check the ones that you want to add. If you want to select all the eligible devices, click the Select All checkbox.

• Click Add. A page appears summarizing the devices that you added to the application’s Pre-Rejected List.

4. Successful device additions to the Pre-Rejected List are displayed on this page. To add more devices to the Pre-Rejected List, click Back to Add Device to the Pre-Rejected List.
Managing Application Invitations

An invitation is initiated by an application. The invitation has to be accepted by the device before the application can target the device with Sprint Business Mobility Framework (SBMF) services. Invitations to join applications are handled automatically through the use of Pre-Rejected Lists. This list specifies devices that cannot receive invitations from an application. There are several options to invite a device to join an application. You can

- choose devices from the same domain as the application
- look up a specific device
- choose devices from a specific device group

If an invitation fails, it could be due to

- a system failure when the invitation was sent, or
- the targeted device blocked the invitation to the application.

Telecom Administrators (TAs) and Telecom Managers (TMs) assigned to the application can manage application invitations.

Inviting Devices to Join Applications

As a TA or TM, you can invite devices to join an application.

To invite devices to join an application:

1. Select an application that you want to invite devices to join. (The Application Details page displays).
2. In the Application Details page, go to the Application Invitations section.

<table>
<thead>
<tr>
<th>Application Invitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invite more devices</td>
</tr>
<tr>
<td>Date</td>
</tr>
<tr>
<td>12/22/2004</td>
</tr>
<tr>
<td>12/22/2004</td>
</tr>
<tr>
<td>Display 1 - 2 of 2</td>
</tr>
<tr>
<td>Cancel Invitations</td>
</tr>
<tr>
<td>Hide All</td>
</tr>
</tbody>
</table>
3. Click **Invite more devices**. (The Invite Devices page displays).

4. Select the method on how devices will be invited to join an application. You must select an option to proceed.

   **To invite devices from the same domain:**
   
   - On the Invite Devices page, click **Choose from within this Domain** and click **Continue**. (The Invite Devices: Choose from within this Domain page displays).

   - From the list of eligible devices, check the ones that you want to invite to join this application. If you want to select all the eligible devices, click the **Select All** checkbox.
Section 4: Managing Applications

Note: This list excludes devices subscribed to the application and devices pre-rejected for the application. Devices that have pending invitations to the application that are under the same domain are included.

- Click **Invite**. A page appears summarizing the devices that you invited to join the application.

![Applicants](image1.png)

- Click **Submit** to confirm or **Cancel** to return to the previous page to select another device. (A confirmation page displays outlining successful and failed invitations).

![Confirmation](image2.png)

To invite a specific device:

- On the Invite Devices page, click **Look up a specific device** and click **Continue**. (The Invite Devices: Look up a specific device page displays).
Enter the ID of the device you want to invite. This field accepts 10 characters.

Click **Invite**. (The Device Invitations page appears summarizing the devices that you invited to join the application).

Click **Submit** to confirm or **Cancel** to return to the previous page to select another device. (A confirmation page displays outlining successful and failed invitations).
To invite devices from a specific device group:

- On the Invite Devices page, click Choose from a Device Group and click Continue. (The Invite Devices from this Group page displays).
- From the list of groups, check the one that you want to invite.
- Click Select. (The Invite Devices: Choose from a Device Group page appears summarizing the devices that belong to that group).
From the list of eligible devices, select the ones that you want to add. If you want to select all the eligible devices, click the **Select All** checkbox.

Click **Invite** to confirm and proceed with the action. (A confirmation page displays).

Successful and unsuccessful invitations are listed on this page. To add more devices to join the application, click **Back to Invite Devices**.
Section 4: Managing Applications

Canceling Invitations
As a TA or TM, if you’ve sent an invitation to a device to join an application that needs to be revoked, you can cancel it.

To cancel an invitation:
1. Select an application that you want to remove invitations for. (The Application Details page displays).
2. In the Application Details page, go to the Application Invitations section.
3. Select the devices that you want to cancel invitations to join the application and click Cancel invitation. (The Cancel Invitations page displays).
4. Click Submit to confirm and proceed with the action.

The invitation will be dropped from the application invitation list. While canceling an invitation, you can also choose to add the device(s) to the Pre-Rejected List for future requests. This will ensure that a device will no longer receive an invitation to join an application.

Managing Subscriptions Requests
Subscription requests are requests by devices to join an application. Unlike invitations which are sent by the application to the device to join it, requests are initiated by a device. They are in a pending state until you either approve or reject them.

Current subscriptions are those that have been approved. As a Telecom Administrator (TA), you can cancel subscriptions that are ineligible or no longer current. Telecom Managers (TMs) can manage subscription requests for the application that they are responsible for.

Approving and Rejecting Subscription Requests
There are a few ways you can approve or reject subscription requests:

- From the Application Details page (Method 1)
- From the Pending Subscription Requests page (Method 2)
- From the My Work List page (Method 3)
Approving a Subscription Request (Method 1)

To approve a subscription request to an application:
1. In the Application Details page, go to the Subscription Request section.
2. Select the subscription requests that you want to approve from the device(s) listed. If you want to select all of them, click the Select All checkbox.
3. Click Approve. (A confirmation page displays).

The approved subscription request(s) now appear in the Current Subscriptions list.

Rejecting a Subscription Request (Method 1)

To reject a subscription request to an application:
1. In the Application Details page, go to the Subscription Request section.
2. Select the subscription requests that you want to reject from the device(s) listed. If you want to select all of them, click the Select All checkbox.

3. Click Reject. (The Reject Subscription Requests page displays).

4. Click Submit to confirm that the subscription requests from these devices will be rejected. The rejected subscription(s) no longer appear as pending.

   In addition to rejecting these requests, you can move these devices to the Pre-Rejected List so that they can no longer subscribe to this application.

   In the Reject Subscription Requests page, before clicking Submit, check the ones you want to move to the Pre-Rejected List.

Approving a Subscription Request (Method 2)

To approve a subscription request to an application:

1. From the left-navigation menu, click Subscription Requests. (The Pending Subscription Requests page displays).
2. Select the pending request you want to approve and click **Approve**. (The Approved Subscription Requests page displays).

The approved subscription requests now appear in the Current Subscriptions list.

**Rejecting a Subscription Request (Method 2)**

To reject a subscription request to an application:

1. From the left-navigation menu, click **Subscription Requests**. (The Pending Subscription Requests page displays).
2. Select the pending request you want to reject and click **Reject**. (The **Reject Subscription Requests** page displays).

3. Click **Submit** to confirm that the subscription requests from these devices will be rejected. The rejected subscriptions no longer appear as pending.

In addition to rejecting these requests, you can move these devices to the Pre-Rejected List so that they can no longer subscribe to an application. Before clicking **Submit** in the **Reject Subscription Requests** page, check the ones you want to move to the Pre-Rejected List.
Approving a Subscription Request (Method 3)

To approve a subscription request to an application:
1. In the My Work List page, go to the Pending Device Requests section.
2. Click **Work / Show all**. (The Pending Subscription Requests page displays).

![Pending Subscription Requests](image)

Click **Approve**. (A confirmation page displays).

![Confirmation](image)

The approved subscription request(s) now appear in the Current Subscriptions list.
Rejecting a Subscription Request (Method 3)

To reject a subscription request to an application:

1. In the My Work List page, go to the Pending Device Requests section.
2. Click **Work /Show all**. (The Pending Subscription Requests page displays).

![Screenshot of Subscription Requests page]

3. Select the pending request you want to reject and click **Reject**. (The Reject Subscription Requests page displays).

![Screenshot of Reject Subscription Requests page]

4. Click **Submit** to confirm that the subscription requests from these devices will be rejected. The rejected subscriptions no longer appear as pending.

In addition to rejecting these requests, you can move these devices to the Pre-Rejected List so that they can no longer subscribe to an application. Before clicking **Submit** in the Reject Subscription Requests page, check the ones you want to move to the Pre-Rejected List.
Canceling Subscriptions

As a TA or TM, you can cancel subscriptions at any time.

To cancel a subscription:

1. In the Application Details page, go to the Current Subscriptions section.

2. Select the current subscriptions that you want to cancel. If you want to select all of them, click the Select All checkbox.

3. Click Cancel Subscriptions. (The Cancel Subscriptions page displays).

4. Click Submit to confirm that these subscriptions will be canceled. The canceled subscriptions no longer appear in the Current Subscription list on the Application Details page.

In addition to canceling these requests, you can move these devices to the Pre-Rejected List so that they can no longer subscribe to this application. In the Cancel Subscriptions page, select the ones you want to move and click Submit. These devices will be moved to the Pre-Rejected List.
Managing Devices

In This Section

- About Devices
- Viewing Device Details
- Updating Device Details
- Managing Administrators Assigned to Devices
- Managing Application Invitations
- Blocking and Unblocking Applications
- Managing Subscription Requests
- Managing Pending Invitations
- Viewing New Devices
- Viewing Available Applications
About Devices

A device or MDN (mobile device number) is any peripheral that is attached to the Sprint PCS network. Applications in the Sprint Business Mobility Framework (SBMF) environment target devices with service requests.

There are three types of devices depending on the type of the billing account they are associated with. These are:

- **Corporate Liable** – These devices are attached to a corporate liable account. This means the user of the device does not actually receive the bill; rather it is paid by the company on their behalf.
- **Employee Liable** – These devices are attached to an individual liable account, and hence the user receives and pays the bill. However, this individual liable account is attached to a Corporate Node in the billing system; enabling the user to receive a discount.
- **Individual Liable** – These devices are attached to an individual liable account, which refers to a normal consumer account where the end user receives and pays the bills.

Devices become available in the SBMFM administrative portal when a billing account is added to a domain. Devices can then be managed as described in this section. Devices can also be imported from a file when creating a group as described in the section “Managing Groups”.

Device Management

The device management function in the SBMFM administrative portal allows Telecom Administrators to:

- View and Update Device Details
- Manage Administrators Assigned to a Device
- Manage Application Invitations
- Block and Unblock Applications
- Manage Subscription Requests
- Manage Existing Subscriptions
- Manage Pending Invitations
- View New Devices
- View Available Applications

Applications target devices with service requests for location or presence network services. This may result in sensitive data being given to a third-party or a charge being levied to an account if not managed correctly. **When you are using the SBMFM administrative portal to manage devices in an organization, you are giving permission for an application to use all the services for which it has been provisioned, against any allowed device.**
Section 5: Managing Devices

Viewing Device Details

Telecom Administrators (TAs) and Telecom Managers (TMs) can view summary information associated with devices in their organization’s domain.

Looking Up Device Details

As a TA or TM, you can look up a specific device by entering its ID or look at all devices you manage.

To look up device details:

1. From the left-navigation menu, click **Devices**. (The My Device List page appears).

2. Select a device to view the details for that device.

   OR

   Enter a Device ID and click **Go** to search for a specific ID. (Results are listed on the My Device List page).

   To change how the results are listed, use the display filters. For example, if you want to only list devices that have assigned TMs, change the Assigned Telecom Manager to **Yes**. If you want to list devices that do not have assigned TMs, change the Assigned Telecom Manager to **No**. The default is to list applications with and without assigned TMs.
Similarly, you can change the account type to filter the results to only show account types that are individual, corporate or employee-node. The default is to list applications of all account types.

3. Click a **Device ID** from the Results section. (The Device Details page appears).

   From this page, you can view application details associated with the device such as its application invitations, subscription requests and current subscriptions. Click **Show All** to view these details.
Section 5: Managing Devices

Viewing Group Membership

From the Device Details page for any given device, you can find out which device groups it is associated with within a domain.

To view group membership

1. Select a device for which you want to see associated device groups. (A Group Details page displays).
2. From the Device Details page, go to the Group Membership section.
3. Click Show All. (This section expands to list out group names the device is associated with).
Updating Device Details

There are two features that you can update for a device:

- Updating the display name of a device
- Enabling SMS (short message service) Invitations for a device

Updating the Display Name

The display name is the name of the device as it appears in the SBMFM administrative portal. You can change this field as required.

To update the Display Name:

1. In the Device Details page, go to the General Information section.
2. Click Edit. (The Edit Device Details page displays).
3. Enter the new name in the Name field.
4. Click Submit. (The Device Details page appears with the new information).
Section 5: Managing Devices

Allowing SMS Invitations
You can set up devices in your organization to receive an SMS (short message service) notification when an application invites devices to use its services. SMS is a network service function and is not managed by the SBMF administrative portal. If this feature is enabled, applications can send invitations as a text message to devices. The default for this setting is No for corporate-liable devices and Yes for employee- and individual-liable devices.

**TIP:** SMS message charges may apply. If you do not want to receive SMS messages from applications, you can disable this feature.

To allow SMS invitations:
1. In the Device Details page, go to the General Information section.
2. Click Edit. (The Edit Device Details page displays).
3. Select Yes or No from the Allow SMS Invitations drop-down menu.
4. Click Submit. (The Device Details page appears with the new information).

Managing Administrators Assigned to Devices
Before applications can be managed in the SBMF environment by a third-party, Telecom Administrators (TAs) can assign or remove Telecom Managers (TMs) to administer a third-party’s devices. Once assigned, TMs can manage pre-approved lists, pre-rejected lists and subscription requests to applications.

**Note:** Only Sprint and Telecom Administrators can assign or remove Telecom Managers to or from devices. Telecom Mangers can not assign or remove other Telecom Managers to or from devices.
Removing a Telecom Manager

This function lets you, as a TA to remove a TM from a device. TMs cannot remove administrators from devices.

To remove a Telecom Manager:

1. In the Device Details page, go to the Telecom Managers section.
2. Click **Remove** next to the name of the TM you wish to remove. (The Confirm Remove Telecom Manager page displays).

3. Verify that the information is correct.

4. Click **Remove**. (The Device Details page displays with the updated information).
Assigning a Telecom Manager
This function allows you, as a TA, to assign a TM to a device. TMs cannot assign administrators to devices.

To assign a telecom manager:
1. In the Device Details page, go to the Telecom Managers section.
2. Click Assign Manager. (The Assign Telecom Manager page displays).

Select a radio button next to the TM name you wish to assign to the chosen device.

3. Click Assign. (The Device Details page displays with the updated information).
To assign several devices to a single telecom manager:

6. In the My Device List page, select the check box beside each device you wish to assign the particular TM.

7. Click Assign Telecom Manager. (The Assign Telecom Manager page displays).

8. Verify that the list of devices is correct.
9. Select the radio button next to the name of the Telecom Manager you wish to assign to the chosen devices.

10. Click Assign. (The My Device List page displays with the updated information).

Managing Application Invitations

Applications can initiate an invitation for a device to join it. For any given device, you can:

- View application invitation details
- Accept application invitations
- Reject application invitations

Viewing Application Invitations

As a TA or TM, you can view application invitation details for a device.
To view invitation details for an application:
1. In the Device Details page, go to the Application Invitations section.

![Application Invitations Table]

- **Application Invitations**
  - Date: 12/16/2004
  - Application ID: 0045000000
  - Application Name: IBM TPA ONE
  - Application Type: Corporate

- **Application Invitations**
  - Date: 01/04/2005
  - Application ID: 004239999
  - Application Name: IBM TPA TWO
  - Application Type: Public

- **Display 1 - 2 of 2**
  - Accept
  - Reject

- **Subscription Requests**
  - Show All

- **Current Subscriptions**
  - Show All

- **Blocked Applications**
  - Show details
  - Block an application

- **Back to My Device List**
2. Click the **Application ID** of the application invitation you wish to view. (The Application Invitation Details page displays).

![Application Invitation Details](image_url)
Accepting Application Invitations
As a TA or TM, there are two ways you can accept an application invitation for a device:

- from the Application Invitations section of a Device Details page or
- from an Application Invitations Details page

Accepting an Application Invitation
If you need to review the terms and conditions for application use, or only have one invitation to select, you can do so from the Application Invitation Details page.

To accept an application invitation:
1. In the Device Details page, go to the Application Invitations section.
2. Click the Application ID of the application invitation you wish to accept. (The Application Invitation Details page displays).
3. Read the terms and conditions.
4. Select the Agree radio button if you agree to the terms and conditions.
5. Click **Accept** to confirm. (A confirmation page displays).

Accepting Multiple Application Invitations

If you have multiple application invitations for a device, and are familiar with the details of the terms and conditions of use for each application, you can accept multiple invitations from the Device Details page.

**To accept multiple application invitations:**

1. From the Device Details page, go to the Application Invitations section.
2. Click the box next to each application invitation that you wish to accept.

3. Click **Accept**. (The Pending Invitation page displays).

4. Select the box next to the terms and conditions once you have agreed to them.

5. Click **Submit**. (A confirmation page displays).
Rejecting Application Invitations
As a TA or TM, there are two ways you can reject an application invitation for a device:

- from the Application Invitations section of a Device Details page or
- from the Application Invitations Details page

Rejecting an Application Invitation
If you have one invitation to reject, you can do so from the Application Invitation Details page.

To reject an application invitation:
1. Select the device that you want to reject an application invitation for. (The Device Details page displays).
2. In the Device Details page, go to the Application Invitations section.
3. Click the Application ID of the application invitation you wish to reject. (The Application Invitation Details page displays).
4. Click **Reject**. You do not need to check whether you agree or disagree to the terms and conditions of use to the application to reject it. (The Reject Application Invitations page displays).

If you want to block future invitations from this application, select the check box before submitting.

5. Click **Submit** to confirm. (A confirmation page displays).

---

### Rejecting Multiple Application Invitations

If you have multiple application invitations for a device, and are familiar with the details of the terms and conditions of use for each application, you can reject multiple invitations from the **Device Details** page.

**To reject multiple application invitations:**

1. In the **Device Details** page, go to the Application Invitations section.
2. Click the box next to each application invitation that you wish to reject.
3. Click **Reject**. (The Reject Application Invitations page displays).

4. Verify that the information is correct. If you want to block future invitations from this application, select the check box for each application before submitting.

5. Click **Submit**. (A confirmation page displays).
**Blocking and Unblocking Applications**

You can control the access that an application has to a device by preventing application invitations to be sent to the device. This is referred to as blocking an application.

**Viewing Blocked Applications**

As a TA or TM, you can view blocked applications for a device.

**To view blocked applications:**

1. In the Device Details page, go to the Blocked Applications section.
2. Click **Show details**. (The Blocked Applications page displays).

![](image)

From this page, you can block or unblock an application.

**Blocking Applications**

Adding an application to a device's block list or blocking an application from a device means invitations from that application to the device will not be successful i.e. will result in an error. You can block applications in two ways:

- from the Blocked Applications section of a Device Details page or
- from the My Device List page

**Blocking an Application**

As a TA or TM, if you have an application to block for one device, you can do so from the Device Details page.
Section 5: Managing Devices

To block an application:
1. In the Device Details page, go to the Blocked Applications section.

2. Click Block an application. (A device confirmation page displays. This is the device for which application invitations will be blocked.).

3. Verify that the device listed is the one you want to block applications for.
4. Click **Continue**. (The Block an Application page displays).

![Block an Application](image1)

5. Click the radio button next to the application you wish to block.

6. Click **Block**. (A confirmation page displays).

![Confirmation](image2)
Blocking Applications for Multiple Devices
If you have multiple devices for which you want to block application invitations, you can do this from the My Device List page.

To block an application for multiple devices:

1. In the My Device List page, click the box next to each device you want to work with.

2. Click Block Application. (A device confirmation page displays. These are the devices for which application invitations will be blocked.)
3. Verify that the devices listed are the ones you don’t want to receive invitations from the application.

4. Click **Continue**. (The Block an Application page displays).

5. Select the radio button next to the application you wish to block.

6. Click **Block**. (A confirmation page displays).

**Unblocking Applications**

As a TA or TM, you can unblock applications for a device.
To unblock an application:

1. In the Device Details page, go to the Blocked Applications section.

2. Click Show Details. (The Blocked Applications page displays).

3. Click the radio button next to the application you wish to unblock.

4. Click Unblock.
Managing Subscription Requests

Subscription requests are initiated by a device to join an application. For any given device, you can

- View subscription requests
- Cancel subscription requests
- Allow subscription requests

Viewing Subscription Requests

As a TA or TM, you can view subscription requests from a specific device to an application.

To view a subscription request:

1. In the Device Details page, go to the Subscription Requests section.
2. Click **Show All** if the section is not expanded. (The section expands).
3. Click the **Application ID** of the subscription request if you wish to view details about the application. (The Application Details page displays).
Canceling Subscription Requests
As a TA or TM, if you have a subscription request to cancel for a device, you can do so from the Application Details page.

To cancel a subscription request:
1. In the Device Details page, go to the Subscription Requests section.
2. Click Show All if the section is not expanded. (The section expands).
3. Click the Application ID of the subscription request that you wish to cancel. (The Application Details page displays).
Section 5: Managing Devices

4. Click **Cancel Request**. (The Cancel Subscription Requests page displays).
5. If you want to block future invitations from an application, select its box before submitting.

6. Verify that the information is correct.

7. Click **Submit**. (A confirmation page displays).

---

**Canceling Multiple Subscription Requests**

As a TA or TM, if you have more than one subscription request to cancel for a device, you can do so from the **Device Details** page.

**To cancel multiple subscription request:**

1. In the **Device Details** page, go to the Subscription Requests section.
2. Click **Show All** if the section is not expanded. (The section expands).

3. Select the box next to each application in the Device Details page that you wish to cancel. Click **Cancel Request** (The Cancel Subscription Requests page displays).
4. If you want to block future invitations from an application, select its box before submitting.

5. Verify that the information is correct.

6. Click Submit. (A confirmation page displays).

**Requesting Subscriptions**

As a TA or TM, you can request a subscription to an application for a specific device.

**To request a subscription:**

1. In the Device Details page, go to the Subscription Requests or Current Subscriptions section.
2. Click **Show All** if the section is not expanded. (The section expands).

3. Click **Request another subscription**. (The Step 1 of 4 – Devices Requesting Subscription page displays).

4. Verify that the information is correct.
5. Click **Continue.** (The Step 2 of 4 – Select an Application to Subscribe page displays).

![Select an Application](image)

6. Select the radio button next to the application you wish to subscribe to.

7. Click **Continue.** (The Step 3 of 4 – Request an Application page displays).

![Request an Application](image)

8. Verify that the information is correct.
9. Scroll to the Accept Terms and Conditions section and click View to review the terms and conditions.

10. Select the radio button next to Agree once you have agreed to the terms and conditions of use.

11. Click Submit. (The Step 4 of 4 – Confirmation page displays).

Managing Current Subscriptions
Current subscriptions identify applications that a device has joined. For any given device, you can:

- View its current subscriptions
- Cancel a current subscription

Viewing Current Subscriptions
As a TA or TM, you can view current subscriptions that a device has subscribed to.

To view current subscriptions:
1. In the Device Details page, go to the Current Subscriptions section.
2. Click **Show All** if the section is not expanded. (The section expands).

Any applications that the device has subscribed to are listed.

3. Click the **Application ID** of the subscription if you wish to view more details. (An Application Details page displays).

**Canceling Current Subscriptions**

You can cancel a device’s current subscription to an application. If there are multiple subscriptions to cancel, you can do so from the **Device Details** page.

**To cancel a current subscription:**

1. In the **Device Details** page, go to the Current Subscription section.

2. Click **Show All** if the section is not expanded. (The section expands).

3. Select the applications you want to cancel subscriptions to by selecting the checkbox next to the application ID.
4. Click **Cancel subscription**. (The Cancel Current Subscriptions page displays).

5. Verify that the information is correct. If you want to block future invitations from an application, select its checkbox before submitting.

6. Click **Submit**. (A confirmation page displays).
Managing Pending Invitations

Pending invitations are those that have been initiated by an application to a device. Pending invitations must be approved by an administrator before it can be used by a device. For any given device, you can:

- View Pending Invitations
- Cancel one or more Pending Invitations

Viewing Pending Invitations

As a TA or TM, you can view pending invitations from an application that are awaiting approval.

To view a pending invitation:

1. From the left-navigation menu, click Devices. (A submenu expands).
2. From the submenu, click Pending Invitation. (The Pending Invitation page displays).

You can also work with pending invitations from the My Work List page. Click Work / Show all to list them. (The Pending Invitations page displays).

Accepting Pending Invitations

As a TA or TM, you can accept pending invitations from an application to a device.

To accept a pending invitation:

1. Click Pending Invitation from the left-navigation menu. (The Pending Invitation page displays).

You can also work with pending invitations from the My Work List page. Click Work / Show all to list them. (The Pending Invitations page displays).
2. In the Pending Invitation page, click the radio button next to the pending invitation you wish to accept.

3. Click Accept. (The Application Invitations page displays).

4. Select the box next to the terms and conditions.
5. Click **Submit**. (A confirmation page displays).

![Pending Invitation Image]

**Rejecting Pending Invitations**

As a TA or TM, you can reject pending invitations from an application to a device.

**To reject a pending invitation:**

1. From the left-navigation menu, click **Pending Invitation**. (The Pending Invitation page displays).

2. Select the radio button next to the pending invitation you wish to reject.
3. Click **Reject**. (The Reject Application Invitations page displays).

4. Verify that the information is correct. If you want to block future invitations from an application, select its checkbox before submitting.

5. Click **Submit**. (A confirmation page displays).
Section 5: Managing Devices

Viewing New Devices

Devices that are added to a billing account show up as new devices in the domain that the billing account is part of. TAs can view these devices in the “New devices” section for 7 days beginning the day the device is added to the billing account. TMs can only view new devices assigned to them.

Working with New Devices

As a TA or TM, you can find and work with any new devices that have been added to your domain.

To view new devices:

1. From the left-navigation menu, click Devices. (A submenu expands).
2. From the submenu, click New Devices. (The New Devices page displays).

You can also work with new devices from the My Work List page. Click Work / Show all to view. (The New Devices page displays).

From this page, you can select a device to:

- subscribe to applications
- block or unblock applications
- assign Telecom Managers

Note: Telecom Managers cannot assign administrators to devices.
Viewing Available Applications

As a TA or TM, you can view the applications that are available to devices within your organization’s domain.

To view available applications:
1. From the left-navigation menu, click Devices. (A submenu expands).
2. From the submenu, click Available Applications. (The Available Applications page displays).

Applications that are available for use by the devices in this domain are listed.
Managing Device Groups

In This Section

- About Device Groups
- Viewing Device Group Info
- Creating Device Groups
- Managing Device Group Administrators
- Managing Device Groups
About Device Groups

Device groups represent a collection of devices. Device groups can be useful to Telecom Administrators (TAs) and Telecom Managers (TMs), allowing administrative actions to be taken on a group of devices instead of one by one. For example, a TA might group a large number of devices to assign them to a TM. There is no limit on the number of devices in a group used for administrative purposes.

Device groups also provide a means for TAs and TMs to better organize devices so that they can be targeted by applications in the Sprint Business Mobility Framework (SBMF) environment. For device groups that will be used as targets by applications, SBMF suggests maximum group size be limited to 1/5 the total number of devices the application is intending on using SBMF services on. Applications that call SBMF services on device groups that do not adhere to this limit will receive errors. Also, device groups should have at least 1 device before they can be used as targets for SBMF services.

Device groups do not provide a way to administer a subset of devices that can receive invitations from applications. For example, if you add a device group to a pre-approved or pre-rejected list and then add a device to this group, the device will not automatically be added to the list because it is associated with a device group.

Device Group Management

The Device Group management function in the Sprint Business Mobility Framework Manager (SBMFM) administrative portal allows TAs and TMs to:

- View Device Group Info
- Create Device Groups
- Maintain Administrators associated with Device Groups
- Maintain Devices associated with Device Groups

Before you can create device groups, a domain must exist. Device groups have to be associated with a domain. Contact a Sprint representative if a domain has not been created for your organization.
Section 6: Managing Device Groups

Viewing Device Group Details

As a TA or TM, you can list device groups to view their details. However, only device groups within your domain can be viewed.

To view device group information:

➢ From the left-navigation menu, click Device Groups. (The My Device Groups List page displays).

The device groups listed contain information such as the names, the amount of devices and the number of TMs assigned.

You can now select a device group to work with by selecting a name from the list.

Viewing Device Group Details

As a TA or TM, you can view specifics associated with a group such as the domain name, group name and TM details such as the name and contact info. You can also use the email function to directly contact an administrator responsible for managing a group by clicking a name.

To view device group details:

➢ From the My Device Groups page, select a group from the list to view the details. (The Group Detail page displays).
From this page, you can view general summary information about the device group such as the:

- The domain the device group belongs to
- The date the device group was last modified
- The names of the TMs assigned to the device group and their contact info

You can also view details about individual devices in the group if devices have been assigned to the group. The number of devices will be listed in the Device Membership section. Click **Show All** to see details such as the device number, user name and account type for each individual device listed in that group.
Adding Device Groups

Device groups can be created by a TA or TM.

The creator of the group automatically becomes the owner of that device group and is responsible to manage that group. A TA can assign a TM to manage the group.

There must be a domain in the SBMFM administrative portal before you can create device groups. TAs and TMs cannot associate a specific domain ID with a device group. Check with a Sprint representative if domains do not exist in the SBMFM administrative portal.

To add a device group:
1. From the left-navigation menu, click Device Groups. (A submenu appears).
2. Click Add New Group (The Add a Group page appears).
3. Enter the name of the device group. The group name must consist of numbers or letters. No spaces are allowed but can be represented by _. Maximum 64 characters. (Required).

Note: A device group name has to be unique within a domain.
4. Click **Submit**. (A Group Detail page displays with the newly added device group added).

At this point you can add more groups or return to the **My Device Groups** page. To add another group, click **Add Another Group**. Click **Device Groups** in the left-navigation menu to display the **My Device Groups** page. To add devices to the newly created group, see Maintaining Existing Device Groups.

## Deleting Device Groups

TAs and TMs can delete device groups as necessary.

**To delete a device group:**

1. From the Group Detail page, click **Delete**. (A confirmation page appears).

2. Confirm the details for the selected device group and click **Delete**. The device group will be removed from those listed on the **My Device Groups** page.
Managing Device Group Administrators

TAs can assign TMs to administer device groups. TMs can also be removed from the device group as required.

TMs cannot assign or remove administrators.

Assigning Telecom Managers to Device Groups

As a TA, you can assign a TM(s) to a device group to ensure the list of devices that can join applications is maintained.

To assign a Telecom Manager to a device group:

1. Select a device group for which you want to assign a TM user in the My Device Groups page. (A Group Detail page appears).

2. In the Telecom Manager section of the Group Detail page, click Assign manager. (The Assign Telecom Manager page displays).

3. Select the name of the TM from the list that you want to assign to this device group.

4. Click Assign. The name of the TM will be added to the list of TMs on the Group Detail page.
Section 6: Managing Device Groups

Removing Telecom Managers from Device Groups
As a TA, you can remove a TM from a device group at any time.

To remove a Telecom Manager from a device group:
1. From the Group Detail page, select a TA to remove.
2. Click Remove. (A confirmation page displays).
3. Review the information and click Remove to confirm. The name of the TM will be removed from the list of TMs on the Group Detail page.
   OR
   Click Cancel to return to the Group Detail page without removing the TM.
Maintaining Existing Device Groups

In addition to maintaining administrators assigned to device groups, TAs and TMs can add devices or remove devices from existing device groups.

Adding Devices to a Device Group

Devices can be added to existing device groups. There are a few options when adding devices to groups. You can add devices to a device group:

- From within a domain
- From other groups you manage
- By individual device lookup
- From another device group
- From an imported file

To add a device to a device group:

1. In the Group Detail page, go to the Device Membership section.
2. Click Show All to expand the section.
3. In the Group Detail page, click Add more devices. (The Add Devices page displays).

4. Select the method on how devices will be added to this device group.

   To add devices to a group from the same domain:
   
   a. Select Choose from within this Domain and click Continue. (The Add Devices: Choose from within this Domain page displays).
Section 6: Managing Device Groups

From the list of eligible devices, check the ones that you want to add to this device group. If you want to select all the eligible devices, click the **Select All** checkbox.

Click **Add to group**. A confirmation page appears summarizing the devices that you included as part of this device group.

To add devices from a group you manage:

a  Select **Choose from all devices you can view** and click **Continue**. (The Add Devices: List All Devices I Manage page displays).
b From the list of devices, check the ones that you want to add to this device group. If you want to select all the devices, click the **Select All** checkbox.

c Click **Add to group**. A confirmation page appears summarizing the device(s) that you included as part of this device group.
Section 6: Managing Device Groups

To add devices to a group using individual lookup:

a  Select **Look up a specific device** and click **Continue**. (The Add Devices: Look up a specific device page displays).

b  Enter the Device ID for the device you want to add (required).

c  Click **Continue**. A confirmation page appears summarizing the device that you included as part of this device group.

To add devices from another group:

a  Select **Choose from another Device Group** and click **Continue**. (The Add Devices: Choose from another Device Group page displays).

b  From the list of groups displayed, check the one group that you want to use as the basis for adding devices.
Click Select. (The Add Devices: Choose from another Device Group page displays).

From the list of devices, check the ones that you want to add to your device group. If you want to select all the devices, click the Select All checkbox.

Click Add to group. A confirmation page appears summarizing the device(s) that you included as part of this device group.

A confirmation page displays when each of the options for adding devices has been successful.
Importing MDN Lists

As a TA or TM, you can also import device from a data file and associate those devices to a device group. In order to add devices to a group from an import file, the file must:

- be in CSV format
- contain valid device phone numbers
- contain no more than 250 records

To add devices based on an imported file:

1. From the Group Detail page, click **Add more devices**. (The Add Devices (Options) page displays).

2. Select **Import from file** and click **Continue**. (The Add Devices: Import from File page displays).

3. If you know the name of the data file, enter it in the field or click **Browse** to select the appropriate file.
4. Click **Continue** to proceed. (The Add Devices: Imported MDNs page displays).

5. From the list of devices, check the ones that you want to add to your device group. If you want to select all the devices, click the **Select All** checkbox.

6. Click **Add**. A confirmation page appears summarizing the devices that you included as part of this group.

   - Click **Back to group details** to return to the Group Detail page.
   - OR
   - Click **Back to Groups** to return to the My Group List page.
Removing Devices from Device Groups
As a TA or TM, you may need to update group information and delete devices from device groups for maintenance.

To remove a device from a group:
1. In the Device Membership section of the Group Detail page, select the devices that you want to remove.
2. Click **Remove**. (A confirmation page displays).

3. Click **Remove** to confirm the removal of the selected devices from this group.  
   OR  
   Click **Cancel** to return to the Group Details page without removing the device from the device group.
## Index

**A**

- Activity Record
  - details associated with, 30

**Applications**

- accepting invitations for devices, 94
- accepting pending invitations to, 119
- approving subscription requests for, 71, 72, 75, 77
- assigning TMs to, 45
- blocking, 102
- canceling invitations from, 70
- canceling subscriptions to, 79
- description of, 32
- details associated with, 38
- editing details in the SBMFM, 39
- filtering search results, 36
- inviting devices to, 64
- rejecting invitations for devices, 97
- rejecting pending invitations to, 121
- rejecting subscription requests for, 71, 73
- removing TMs from, 47
- status in the SBMFM, 32
- types, 32
- unblocking, 106
- viewing blocked, 100
- viewing details of, 34
- viewing invitation details for, 92
- viewing new in the SBMFM, 44
- viewing pending invitations for, 119
- viewing Pre-Approved List for, 48
- viewing Pre-Rejected List for, 56

**C**

- Corporate Liable
  - device type, 81

**D**

- Device groups
  - adding devices to, 133
  - adding in BMFM, 129
  - and devices, 126
  - assigning TMs to, 131
  - deleting, 130
  - description, 126
  - details associated with, 128
  - importing MDN lists, 139
  - removing devices from, 141
  - removing TMs from, 132
  - viewing, 127

- Devices
  - accepting application invitations for, 94
  - accepting pending invitations for, 119
  - adding to device groups, 133
  - adding to Pre-Approved List, 51
  - adding to Pre-Rejected List, 59
  - and application invitations, 64
  - and device groups, 126
  - assigning TMs to, 89
  - blocking applications for, 102
  - canceling current subscriptions, 117
  - canceling invitations to, 70
  - description, 81
  - filtering search results, 82

---

*SBMFM Third-Party Administration Guide*
looking up new, 123
rejecting application invitations for, 97
rejecting pending invitations for, 121
removing from device groups, 141
removing from Pre-Approved List, 49
removing from Pre-Rejected List, 57
removing TMs from, 87
requesting subscriptions for, 113
unblocking applications for, 106
updating display name, 85
viewing available applications for, 124
viewing current subscriptions, 116
viewing details of, 82
viewing groups of, 84

Domains
assigning TAs to, 17
description, 15
viewing new applications in, 44

E
Employee Node
device type, 81

F
Filters
for application search, 36
for device search, 82

I
Individual Liable
device type, 81

M
MDN. See Devices
Message Board
viewing messages in, 18

P
Passwords
changing, 27
changing initial, 9
policy for SBMFM, 9
resetting other users, 27
retrieving, 12

Pre-Approved List
adding devices to, 51
description, 33
details associated with, 49
moving devices to Pre-Rejected List, 51
removing devices from, 49
viewing for applications, 48

Pre-Rejected List
adding devices to, 59
description, 33
details associated with, 57
moving devices to Pre-Approved List, 58
removing devices from, 57
viewing for applications, 56

S
SA. See Sprint Administrators
SBMF. See Sprint Business Mobility Framework
Service level agreements
details associated with, 41
updating, 42
Service usage
details associated with, 43
reporting for an application, 42
Sprint Administrator
SBMFM responsibilities, 33
Sprint Business Mobility Framework
description, 3
Sprint Business Mobility Framework Manager
Index

canceling, 79

T

Telecom Administrators
assigning to domains, 17
description of, 21
reminders, 8

Telecom Managers
assigning to applications, 45
assigning to device groups, 131
assigning to devices, 89
description of, 21
removing devices from, 87
removing from applications, 47
removing from device groups, 132

Third-Party
application status, 32
application types, 32
required setup for SBMFM Application Portal use, 4

TM. See Telecom Managers

V

Viewing
SBMFM administrative portal user activity record, 29