INSTALLATION AND CONFIGURATION GUIDE

Mobile Admin Server

Version 8.2

solarwinds

Last Updated: April 24, 2018

Table of Contents

Introduction

SolarWinds® Mobile Admin® Server is a client-server application that allows you to manage servers and computers on your network from your wireless device.

You can install Mobile Admin Server on a dedicated computer or a virtual machine with access to all network servers you want to manage. The Mobile Admin Client software can be installed on any supported wireless device.

For information about installing or using the Mobile Admin Client or supported wireless devices, see the Mobile Admin Client Installation and Usage Guide.

Supported servers

You can use Mobile Admin to manage the following:

- SolarWinds Network Configuration Manager (NCM)
- SolarWinds Network Performance Monitor (NPM)
- SolarWinds Network Traffic Analyzer (NTA)
- SolarWinds Server and Application Monitor (SAM)
- SolarWinds User Device Tracker (UDT)
- Amazon® Elastic Compute Cloud (EC2)
- Microsoft® Windows® and Windows Server® computers and networks
- Microsoft Active Directory®
- Microsoft Exchange Server® 2003, 2007, and 2010
- Microsoft Exchange ActiveSync® (for Exchange Server 2007 and Exchange Server 2010)
- Microsoft SQL Server®
- Microsoft Internet Information Services® (IIS)
- Microsoft DHCP
- Microsoft DNS
- Microsoft Cluster Servers
- Microsoft System Center Operations Manager
- Microsoft System Center Mobile Device Manager
- IBM® Lotus Domino
- Novell® eDirectory/NDS
- BlackBerry® Enterprise Server®
- Oracle®
- Citrix® XenApp

- RSA Authentication Manager
- HP® iLO 2 & 3
- Symantec® BackupExec®
- Symantec NetBackup®
- VMware® Infrastructure
- Nagios Core
- BMC Remedy Service Desk
- BMC Performance Manager Portal
- CA Service Desk
- Microsoft Hyper-V®
- RDP, VNC, SSH, Telnet

Mobile Admin allows you to use your smartphone to perform a full range of administrative tasks on these servers, such as:

- Managing users, groups, event logs, services, and print jobs
- Rebooting servers
- Resetting passwords
- Editing server documents
- Deleting mailbox messages

Mobile Admin allows you to create Telnet and SSH connections to manage Unix, Linux, IBM AS/400™, and Novell NetWare® devices, routers and switches. Telnet connections provide VT100, IBM 5250 and 3720 terminal emulation. SSH connections provide VT100 emulation and allow for public/private key authentication.

Mobile Admin also allows you to create RDP/VNC connections to Microsoft Windows, Apple® OS X, Linux, Oracle Solaris®, QNX® and IBM OS/2® operating systems to view the screen and control the keyboard and mouse of a remote computer.

Mobile Admin security

There are several layers of security available for Mobile Admin, including options for both encryption and authentication.

Encryption options include:

- Triple Data Encryption Standard (TDES) or Advanced Encryption Standard (AES) on the BlackBerry® wireless network (if you are using a BlackBerry Enterprise Server with BlackBerry smartphones)
- Virtual Private Network (VPN) encryption (if you are using Android or iOS devices)
- HyperText Transport Protocol - Secured (HTTPS) encryption

If you are using BlackBerry Enterprise Server, all data sent between the BlackBerry server and the BlackBerry device are encrypted using TDES or AES. The U.S. Government certified TDES and AES as compliant with Federal Information Processing Standards (FIPS). Additionally, if a BlackBerry smartphone is lost, you can use the BlackBerry Enterprise Server to "kill" it remotely—a process that disables and erases all contents of the BlackBerry (including the Mobile Admin application).

If you are using VPN, all data sent between the VPN server and these devices can be encrypted with any encryption method is offered by the VPN you have chosen.

Mobile Admin allows you to add HTTPS encryption to all data sent between the Mobile Admin Server and Mobile Admin Clients. HTTPS is HTTP encrypted with the Transport Layer Security (TLS) protocol. This option is highly recommended for BlackBerry users who decide to use Mobile Admin without a BlackBerry Enterprise Server or users of any client without a VPN connection. For more information, see Configuring network access for BlackBerry smartphones, or Configuring network access for Android and iOS Devices. Mobile Admin also supports RSA SecurID two-factor authentication and has been officially approved as an RSA®-Certified application. This option requires users to log in with their RSA SecurID® tokens before they can access Mobile Admin.

For more information about using RSA SecurID Authentication, see the RSA website.

Remote Authentication Dial-In Service (RADIUS) authentication allows Mobile Admin to act as a RADIUS client or RADIUS device for any type of RADIUS server and authentication system you are using (such as SafeWord).

Authentication options include:

- Primary login authentication (required) from a choice of:
  - Windows user name and password
  - Mobile Admin-specific username and password
  - Device-level password (optional)
- RSA SecurID two-factor authentication (optional) (Mobile Admin Professional Only)
- RADIUS authentication (optional) (Mobile Admin Professional Only)

Mobile Admin requires that you choose a primary form of authentication that each user must enter to log in to the Mobile Admin application, no matter what other forms of authentication (such as device-level, or RSA SecurID) you may have configured. You can also configure how frequently the user is required to enter the primary login authentication. For example, you can configure Mobile Admin to require the primary login every time the Mobile Admin Client is opened, or after specified time-out intervals.

Getting started

To get started with Mobile Admin, perform the following steps:

1. Install the Mobile Admin Server.
2. Configure your network to allow your wireless devices to access Mobile Admin.
   If you are using wireless devices with BlackBerry Enterprise Server, see Using Mobile Admin with BlackBerry Enterprise Server.
3. Configure the servers in your network (if required), to work with Mobile Admin.
4. Connect to the Mobile Admin server through the client of your choice.
5. In the Configuration Interface, set up your servers, users, and security.
6. Install the Mobile Admin Client software on the wireless devices of the administrators in your organization.

After you install and configure the Mobile Admin Server, consider sending an email to all users who will be installing the Mobile Admin Client on their wireless devices. Be sure to provide the URL or network location of where the client software is located.

Install Mobile Admin Server

You can install Mobile Admin Server software on one computer in your network. This installation allows you to manage servers in your network if:

- The servers are accessible and in the same network as Mobile Admin Server
- You have a valid license for each Mobile Admin user

The Mobile Admin free trial allows you to manage unlimited servers. If you want to run Mobile Admin with FIPS enabled, SolarWinds recommends that you enable FIPS before installing Mobile Admin.

Minimum system requirements

Depending on the number of users, Mobile Admin can either be installed on an existing computer, a VM, or a dedicated server.

The Mobile Admin Server supports 25 concurrent users. If you expect additional, concurrent users, you can deploy multiple Mobile Admin servers.

Non-dedicated servers and virtual machines

SOFTWARE OR HARDWARE	REQUIREMENTS
Operating system	Windows Server 2003 32-bit (recommended) Windows Server 2008 64-bit Windows Server 2008 R2 64-bit (recommended) Windows Server 2012 Windows XP, Windows Vista®, Windows 7, and Windows 8 for trial purposes
CPU	Intel Pentium 4 CPU
Memory	1 GB or more
Disk Space	200 MB for installation 20 GB or more for optimum performance
Privileges	Local Admin privileges for Windows Vista or Windows 7
Server Roles	Application Server Role for Windows Server 2008 and Windows Server 2008 R2

Software or Hardware	Requirements
.NET Framework	Version 4.0
PowerShell	Version 2.0

Dedicated servers

Software or Hardware	Requirements
Operating system	Windows Server 2003 32-bit (recommended) Windows Server 2008 Windows Server 2008 R2 64-bit (recommended) Windows Server 2012 Windows XP, Windows Vista, Windows 7, and Windows 8 for trial purposes
CPU	2.66 MHz Intel® Core 2 Quad CPU
Memory	2 GB or more
Disk Space	200 MB for installation 20 GB or more for optimum performance
Privileges	Local Admin privileges for Windows Vista or Windows 7
Server Roles	Application Server Role for Windows Server 2008 and Windows Server 2008 R2
.NET Framework	Version 4.0
PowerShell	Version 2.0

Where to install Mobile Admin Server

You can install Mobile Admin Server on any system in your network that meets the minimum system requirements. This single installation allows you to manage several servers in your network.

Mobile Admin database backup

The SQLite database used in Mobile Admin is a flat-file database. You can back up the database by backing up the database file. By default, the Mobile Admin database is located at:

```
C:\Program Files\Rove\Mobile Admin\db\MobileAdminDB.sqlite
```

If Mobile Admin is installed on a 64-bit operating system, the default database path is:

```
C:\Program Files (x86)\Rove\Mobile Admin\db\MobileAdminDB.sqlite
```

> To avoid possible inconsistencies in the application, when you back up the SQLite database, ensure that the Mobile Admin service is not running.

When you back up the SQLite database, use the following guidelines:

- Restoring and using a backup version of the SQLite database reverts the configuration and settings to reflect the configuration in effect when the backup was performed.
- If you back up the current version of Mobile Admin with an older version, new feature changes may not be supported.
- Sensitive data in the database is encrypted and can only be decrypted on the Mobile Admin Server where it was originally encrypted.

Install the Mobile Admin Server software

1. Make sure that the computer where you are installing the Mobile Admin Server software meets the minimum system requirements.
2. Navigate to the location where you saved the Mobile Admin software and double-click:
   `MobileAdminInstaller.exe`
   > If your system responds with a security warning, click Run.

   A popup describing software prerequisites appears.
3. Click OK.
   The Mobile Admin Setup window displays.
4. Click Next.
   The Mobile Admin Setup window displays.
5. Click Next.
6. If you accept the End User License Agreement, click I Agree.
   > If you have not installed the prerequisite software, Mobile Admin prompts you to download and install the software.
7. Click Next.
8. In the Installation Options screen, select Help make Mobile Admin better by automatically sending usage statistics and crash reports if you wish to provide this information.
   > See the SolarWinds Privacy Statement for details.
9. After you select your desired options, click Next.

10. In the Choose Install Location window, browse to where you would like to install Mobile Admin, and click Next.

    > If you installed Microsoft .NET® 4.0 as part of the Mobile Admin installation, you may need to restart your computer.

11. In the Installation Checklist window, ensure the information is correct, and click Install.
12. After the installation is complete, click Finish.
    The Mobile Admin Licensing tool opens.
13. Click Enter Licensing Information.
14. Select I have internet access and an activation key.
    If you cannot access the Internet from the Mobile Admin Server, see License the software on a computer without Internet access.
15. Click the Customer Portal link to access the customer portal on the SolarWinds site.
16. Log on to the portal using your SolarWinds customer ID and password.

    > You should have received this information in an email sent by SolarWinds when you purchased your software.

17. Click License Management on the left navigation bar.
18. Navigate to your product, choose an activation key from the Unregistered Licenses section, and copy the activation key. You only need to apply a single activation key.

    > If you cannot find an activation key in the Unregistered Licenses section, contact SolarWinds customer support.

19. Return to the Activate Mobile Admin window and enter the activation key in the Activation Key field.
    If you the Internet through a proxy server, click I access the internet through a proxy server and enter the proxy address and port.
    If your computer accesses the Internet through an authenticated proxy server, complete the procedure for activating without Internet access.
20. Click Next.
21. Enter your email address and other registration information, and then click Next.
22. After your Mobile Admin server is licensed, click Finish.
    You can now view your license status.
23. Click Close.
    The Mobile Admin Deployment Integrity Checklist displays.
    The Checklist provides a list of potential issues. You can address the issues and rerun the Checklist.
    If the checklist indicates that the installation completed properly, click Launch to open the Mobile Admin Web Client.

License the software

You can license the software with or without an Internet connection. Locate your SolarWinds Customer ID (SWID) to log on to the SolarWinds Customer Portal and view your activation key.

Contact Support for your SWID and to view the Licensing FAQ.

License the software on a computer with Internet access

1. If you are licensing the software as part of the installation, click Enter Licensing Information when prompted.
   If you are licensing the software after an evaluation period, you can access the Mobile Admin Licensing Tool by opening Start > All Programs > Mobile Admin > Mobile Admin Licensing on the Mobile Admin server and clicking Licensing Information.
   If you are licensing the software after an evaluation period and the Mobile Admin server is installed on a server running Windows Server 2012, you can access the Mobile Admin Licensing Tool by searching for Mobile Admin Licensing on the Mobile Admin Server and clicking Enter Licensing Information.
2. Select I have internet access and an activation key.
3. Click the Customer Portal link to access the customer portal on the SolarWinds site.
4. Log on to the portal using your SolarWinds customer ID and password.
   You should have received this information in an email sent by SolarWinds when you purchased your software.
5. Click License Management on the left navigation bar.
6. Navigate to your product, choose an activation key from the Unregistered Licenses section, and copy the activation key.

   You only need to apply a single activation key. If you cannot locate an activation key in the Unregistered Licenses section, contact SolarWinds Customer Support.
7. Return to the Activate Mobile Admin window.
8. Enter the activation key in the Activation Key field.
9. If you access the Internet through a proxy server, click I access the internet through a proxy server, and enter its proxy address and port.
   If you access the Internet through an authenticated proxy server, complete the procedure for activating without Internet access.
10. Click Next.
11. Enter your email address and registration information, and then click Next.
12. After your Mobile Admin Server has been licensed, click Finish.
    You can then view your license status.
13. Click Close.

License the software on a computer without Internet access

1. If you are licensing the software as part of the installation, click Enter Licensing Information when prompted.
   If you are licensing the software after an evaluation period, you can access the Mobile Admin Licensing Tool by opening Start > All Programs > Mobile Admin > Mobile Admin Licensing on the Mobile Admin Server, and the click Enter Licensing Information.
   If you are licensing the software after an evaluation period and the Mobile Admin server is installed on Windows Server 2012, you can access the Mobile Admin Licensing Tool by searching for Mobile Admin Licensing on the Mobile Admin Server, and then click Enter Licensing Information.
2. Select This server does not have internet access, and then click Next.
3. Copy the Unique Machine ID to a text file.
4. Transfer the file to a computer with Internet access.
5. On the computer with Internet access, complete the following steps:
   a. Log in to the SolarWinds Customer Portal using your SolarWinds Customer ID and password.
   b. Click Licenses > Manage Licenses.
   c. Navigate to your product, and then click Activate license manually.
      If the Activate license manually option is not available for your product, contact SolarWinds Customer Support.
   d. Enter the Machine ID you saved in step 3, and then download your license key file.
6. Transfer the license key file to the Mobile Admin server.
7. Return to the Activate Mobile Admin window.
8. Browse to the license key file, and click Next.
9. After your Mobile Admin Server is completed, click Finish.
   You can now view your license status.
10. Click Close.

Modify or deactivate the software

For information about managing your licenses for SolarWinds products, including how to deactivate or reuse a license, see License Manager.

Uninstall the Mobile Admin Server software

1. In the Windows Control Panel, double-click Add or Remove Programs.
2. Locate Mobile Admin in the list of programs or in the Start menu, and then click Remove.
3. When prompted, click Uninstall.

4. When prompted to remove the server-specific settings and log files created by Mobile Admin, click Yes or No.
   If you are uninstalling Mobile Admin permanently, click Yes.
   If you are uninstalling Mobile Admin for troubleshooting purposes and plan to reinstall it, click No.

Configure Mobile Admin

To configure Mobile Admin, you must have Mobile Admin administrator privileges.

> If you are installing Mobile Admin for the first time, the software provides you with administrator privileges by default. Only an administrator can assign administrator privileges to other users.

You can configure Mobile Admin from the Mobile Admin Web Interface or your wireless device. After you enable the software and access the Mobile Admin configuration interface, you can:

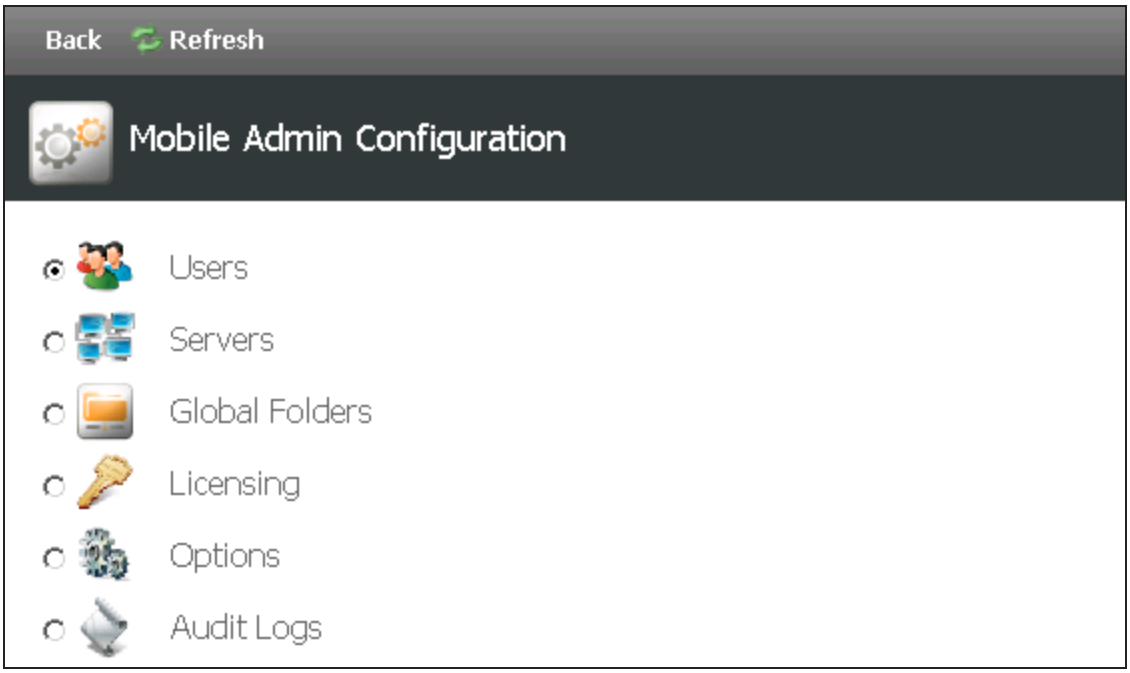
- Add users and servers
- Manage users and servers
- Manage global folders
- View licenses
- Configure default Mobile Admin Client settings
- View audit logs

Access the Mobile Admin Configuration Interface

You can access the Mobile Admin Configuration Interface from any computer or device using a web browser or the Mobile Admin application on your mobile device.

> The procedures in this section assume you are using the Mobile Admin Web Interface. All Mobile Admin configuration tasks can be carried out from any supported device.

In the Mobile Admin Web Interface Home Screen, locate the Actions pane and click Configuration. The following window displays.



Add users and servers

All Mobile Admin users must have login rights to Mobile Admin Server. A Mobile Admin administrator must have local admin privileges on the server hosting Mobile Admin Server. A Mobile Admin users' Windows permissions control the actions a Mobile Admin user can perform. To administer a server, you will need the appropriate rights for the targeted server.

Configure users so they can add or remove servers from their server list in the Mobile Admin Client. If you do not give users permission to add and remove servers from their Client server lists, each user's server list in the Mobile Admin Client will reflect exactly what is defined for them in the Configuration Interface.

If you give a user permission to add or remove servers, the user can add any server to their server list from the Mobile Admin Client. This server will appear in the server list in the Configuration Interface. If a user with permission removes a server from the Mobile Admin Client, it is removed from the user's server list and not the Configuration Interface server list.

The server where Mobile Admin Server was installed displays in the Configuration Interface server list by default. You can remove this server from the server list if you do not want to manage it with Mobile Admin.

Manage users

In the Configuration Interface, select the Users option to open the Users page. The page includes a list of users, as well as a list of actions you can perform.

All procedures in this section assume that you are on this page.

By default, users are added to the Configuration Interface when they log in to Mobile Admin for the first time. Typically, it is not required to manually add users in the Configuration Interface. However, you can manually add specific users to the Configuration Interface before they log in. When you are finished, you can create user lists for each server.

Add or remove a user

To add a user, click Add, complete the User Name and Domain fields, and click Save. To remove a user, select the and click Remove.

Manage default user permissions

1. In the Users page, click Permissions.
2. Select or clear the check boxes for the default user permissions.
3. Click Save Selections.

Manage specific user permissions

1. Select a user, and then click Permissions.
2. Select or clear the check boxes for the user rights.
3. Click Save Selections.

Manage user rights

1. In the Users screen, select the targeted user.
2. Select or clear the Rights check boxes.
3. Click Save.

Manage user license types

1. In the Users screen, select the targeted user.
2. Select Basics, Professional or Mobile Admin from the User Type drop-down menu.
3. Click Save.

Manage user devices

When a ProPlus user logs in to Mobile Admin and sets up feeds, the device becomes associated with this user. The user and device association can be removed if it is no longer appropriate (for example, when your device changes). You can send a test notification to a device to ensure the push notifications are received.

Manage user server lists

You can also manage a user's server list through the Server option in the Configuration Interface.

1. In the Users screen, select the targeted user and click Servers.
2. Perform one of the following procedures:
   - Click Add, select the check boxes of the servers you want to add, and then click Add.
   - Select the servers you want to remove, and then click Remove.

Manage servers

The Servers page displays when you click Servers in the Configuration Interface. The menu contains a list of options, as shown below.

All procedures in this section assume that you are on the Servers page.

Add and remove servers from the configuration interface

Follow this procedure to identify the servers that users will manage with Mobile Admin.

Add a server

1. In the Actions pane, click Add.
2. Locate and add a server.
   To add a server, complete the Host Name field and click Add. You can enter an alias in addition to a host name.
   To locate a server, click Browse Network. Navigate to the server you want to add, and click Add. You can search the displayed network(s) for a server by clicking Find, entering the server name or a wildcard, and clicking Find to display a list of results. Select the desired server and click Add on the Actions pane.
   To find the server in the network, click Browse Network in the menu and click Find in the Action Pane.
3. Click OK.

An administrator can organize the server list in the Configuration Interface by creating user lists for individual servers. User lists do not provide a user administrative access to servers, but they do determine which servers display in the user's server list.

Remove a server

Select a server that you want to remove and click Remove on the menu.

Mobile Admin users will see the changes in the server list the next time they log in, or when they refresh the server list on their wireless device. Removing a server from the Configuration Interface also removes the server from any Global Folders that contain it.

Manage a server user list

1. From a view of the server that you want to manage user lists for, click Users on the menu.
2. Perform one of the following procedures:
   - To add a user to a server, click Add on the menu, select the user(s) you want to add, and click Add.
   - To remove a user from a server, select the user(s) you want to remove, and click Remove.

You can also manage a server's user list through the User option on the Configuration Interface.

Manage permissions

If a user has permission to manage their server list, they can add a server in the Configuration section. If a server is removed, the changes do not display in the server list.

If a new server you want to manage is added to the Configuration Interface server list after your first Mobile Admin Client login, you must manually add it to your server. The server will not be automatically added to the list.

Manage default user permissions for a server

1. From a view of the server that you want to manage permissions for, click Permissions on the menu.
2. Select or clear the check boxes for default server permissions.
3. Click Save Selections.

View and modify server permissions

1. From a view of the server for which you want to view or edit permissions, click Permissions in the menu.
2. Select or clear the check boxes for server permissions.
3. Click Save Selections.

Manage global folders

Manage global folders (Mobile Admin professional only)

The Global Folders page displays when you select Global Folder in the Configuration interface.

Global Folders allow you to organize servers. You can keep specific servers together to sort large numbers of servers into meaningful groups. Global Folders are accessible to any user who has permissions to any server in the folder.

All procedures in this section assume that you have selected Global Folders on the Configuration Interface.

Create a global folder

1. In the Actions menu, click Add Folder.
2. In the Name field, enter a global folder name.
3. Click Add.

Remove a global folder

Servers within a global folder are not removed from Mobile Admin when the folder is removed.

1. Select the folder you wish to remove.
2. Click Remove.

Add servers to a global folder

1. Select the global folder you want to add to a server.
2. Click Add Servers.
3. Select the servers you want to add.
4. Click Add.

Create a global folder within a global folder

1. Select the global folder in which you want to create a new global folder, and click Add Folder.
2. In the Name field, enter a name for the global folder, and click Add.

View the users of a global folder

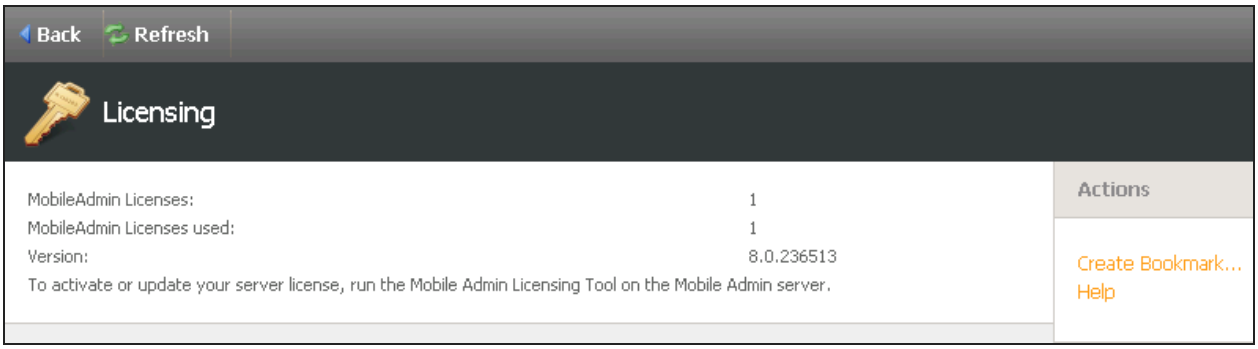
1. Select the global folder whose user list you want to view.
2. Click Users on the menu.

Add a user to a global folder

1. In the global folder, click Users on the menu.
2. Click Add User.
3. Select the users you want to add.
4. Click Add.

View licenses

The Licensing page displays when you select Licensing in the Configuration interface. This page lists the server license and version.



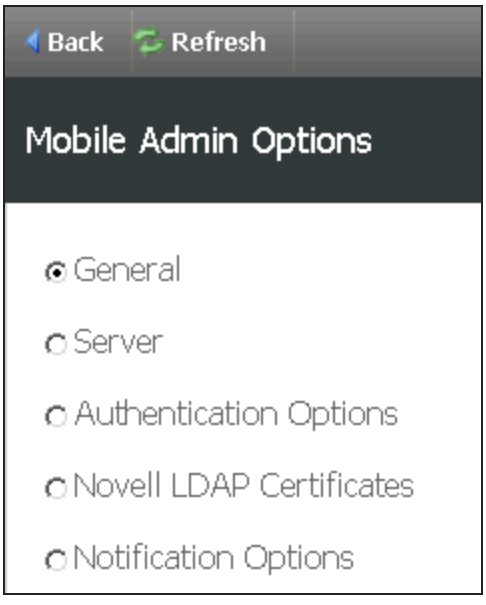
See License the software for details about activating the Mobile Admin Server.

See the SolarWinds License Manager documentation for information about managing your licenses for SolarWinds products.

Options

Select Options to open the Mobile Admin Options page.

> All procedures in this section assume you selected Options in the Configuration Interface and are on the Mobile Admin Options page.



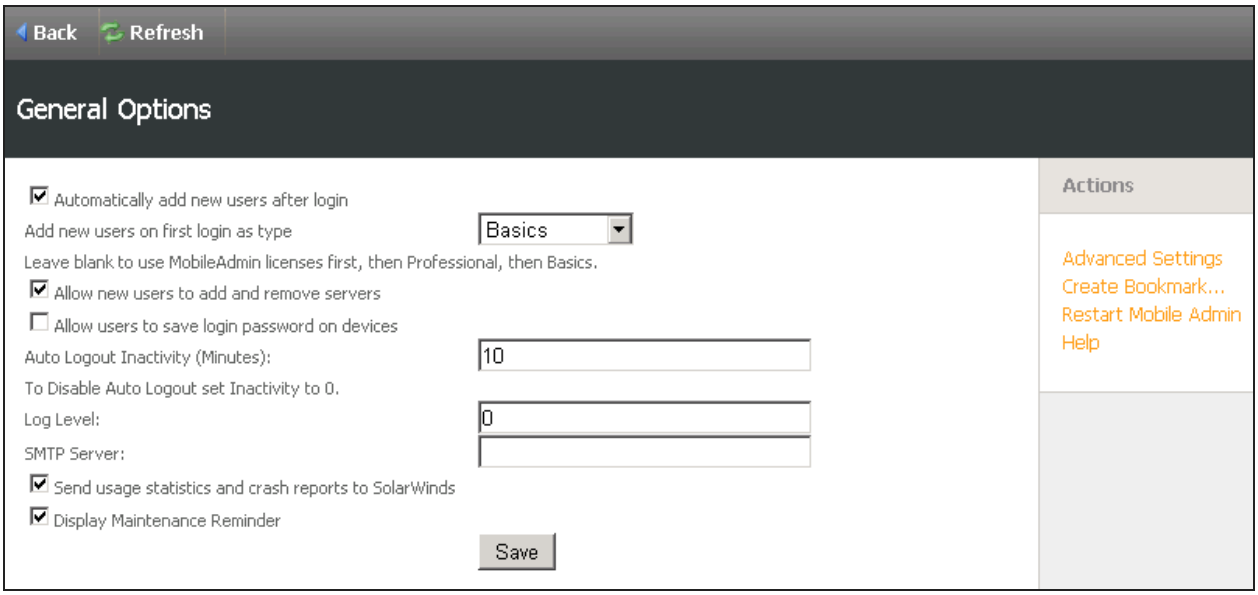
The Mobile Admin Options page includes the following options:

- General
- Server
- Authentication Options
- Novell LDAP Certificates
- Notification Options

General options

The General Options page displays configuration options that indicate how the Mobile Admin Client works with the Mobile Admin server. This page includes links to Advanced Settings and Restart Mobile Admin.

> All procedures in this section assume that you have selected General from the Mobile Admin Options page, and are on the General Options page.



Enable and disable automatic addition of new users after login

1. Select or clear the Automatically add new users after login check box.
2. Click Save.

Set a license type for users added at first login

This setting determines what user license type is to be assigned to a new user added at first login. If a selected license type is not available at new user first login time then the new user is not added.

1. In the General Options screen, select a license type.
2. Leave the selection blank to use available ProPlus licenses. When these licenses are exhausted, use Professional licenses, and then Basic licenses as your last option.

   > A user license type can be changed at any time.

Enable and disable user permission to add and remove servers

If you set the default for new users, you can change whether or not a specific user is allowed to add and remove servers at any time.

1. In the General Options screen, select or clear the Allow new users to add and remove servers check box.
2. Click Save.

Enable and disable storing passwords on Mobile Admin clients

Enabling Allow users to save login password on devices results in the Mobile Admin Client showing a Save Password checkbox in the log on screen. The client Save Password check box is not available if Allow users to save login password on devices is not checked. The default setting is not checked.

Manage client auto-logout settings

1. In the General Options screen, enter the number of minutes of inactivity after which Mobile Admin automatically logs out a user in the Auto Logout Inactivity (Minutes) field.
   Entering a value of 0 disables the auto-logout feature. The default setting is 0.
2. Click Save.

Enable extended server logging

Follow this procedure to use extended server logging to temporarily collect system information for troubleshooting purposes. Because extended server logging can slow performance, only enable extended server logging when advised by Technical Support.

If you installed the Mobile Admin server on Windows Server 2012 or Windows 8, log in as the domain administrator to make changes to the log levels.

1. In the General Options screen, enter the number provided by Technical support in the Log level field.
2. Click Save.

Send usage statistics and crash reports to Rove

Follow this procedure to send crash traces and logs to SolarWinds. This program is completely optional.

See the SolarWinds Privacy Statement for details.

1. In the General Options screen, click the Send usage statistics and crash reports to SolarWinds check box.
2. Click Save.

Change the SMTP settings

Follow this procedure to enable Mobile Admin Client users to email files from their handhelds using the File Explorer.

1. In the General Options screen, enter the hostname of your mail server in the SMTP Server text field.
2. Click Save.

Restart the Mobile Admin Service

Follow this procedure to restart the Mobile Admin service. You will be prompted to do this after certain administrative changes, or by Technical Support.

1. Click Restart Mobile Admin.
2. Click OK.

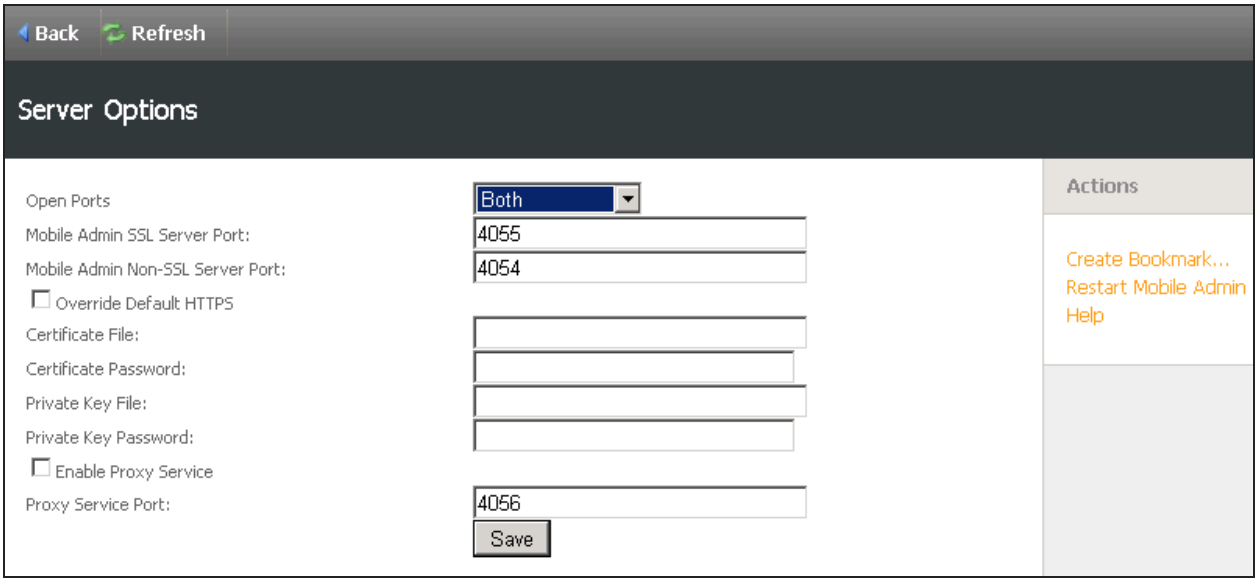
Server options

The Server Options page displays the different port and HTTPS security configuration options available for Mobile Admin. Mobile Admin provides an SSL port and a non-SSL port. You can choose which port you want to configure. The default Mobile Admin SSL and non-SSL server ports are 4055 and 4054, respectively, and can be changed according to your needs.

HTTPS is enabled by default, and contains an embedded HTTPS certificate. You can choose to override this certificate by providing credentials for your own HTTPS certificate.

The Mobile Admin proxy service supports SSH/Telnet and RDP/VNC connections in network environments where direct paths between the device and the target server (such as networks with a BES) are difficult to create. The proxy service is configured by an administrator, then enabled/disabled on individual clients by the user as part of their connection settings.

All procedures in this section assume that you selected Server from the Mobile Admin Options. Be sure to configure the Mobile Admin Client to connect to the appropriate port.



Open the SSL port, Non-SSL port, or both

Be sure to open the appropriate port on your firewall. If you installed the Mobile Admin server on a system running Windows Server 2012 or Windows 8, log in as the domain administrator to change the ports.

1. In the Server Options home screen, click the Open Ports drop-down menu and select SSL Only, Non-SSL Only, or Both.
2. Click Save.

Change the default SSL or Non-SSL port

Be sure to open the appropriate port on your firewall. If you installed Mobile Admin Server on a system running Windows Server 2012 or Windows 8, log in as the domain administrator to change the ports.

1. In the Mobile Admin SSL Server Port or Mobile Admin Non-SSL Server Port text field, enter the port number that you want Mobile Admin to use.
2. Click Save.

Override the default HTTPS certificate

Use a PKCS12-formatted and password protected PFX certificate file to configure Mobile Admin to use a user-selected certificate for HTTPS.

The PFX file must include the certificate private key. If you are exporting the PFX file from secure storage on a Windows platform, make sure that Export the private key is selected during the export process. The subject name in the certificate does not need to match the server name for the Mobile Admin Client to trust the certificate and set up a secure connection.

1. In the Server Options screen, select the Override Default HTTPS check box.
2. If you are configuring Mobile Admin to use a PKCS12 file to enable HTTPS, ensure that:
   - The PFX file path is provided in the Certificate File field.
   - The password used to protect the PFX file is provided in the Certificate Password field.

   If you included a path to the PFX file, leave the Private Key File and Private Key Password fields blank.
3. Click Save.

Configure the Mobile Admin Proxy Service

You must also open the appropriate port on your firewall, if there is one in your network.

1. In the Server Options screen, select the Enable Proxy Service check box.
2. In the Proxy Service Port field, enter the port number you want to use for the proxy.
3. Click Save.

Authentication options

The Authentication Options page displays the various authentication options available for Mobile Admin. The authentication options available for Mobile Admin are:

- Windows Authentication
- RADIUS
- RSA SecurID

All procedures in this section assume that you selected Authentication Options from the Mobile Admin Options page.

If you run Mobile Admin on a host with FIPS enabled, you cannot select RADIUS authentication.

Authentication method

The Authentication Method page displays configuration options used to set up authentication. hoose a primary form of authentication that each user must enter to log in to the Mobile Admin application, no matter what other forms of authentication (such as device-level, or RSA SecurID) that you may configure for the user. You can configure how frequently a user is required to enter primary login authentication information. For example, you can configure Mobile Admin to require the primary login every time a user opens the Mobile Admin Client, or after time-out intervals that you specify.

Choose a primary login authentication method from the following options:

- Windows user name and password
- Mobile Admin-specific username and password

Windows user name and password authentication

You can configure administrative access to Mobile Admin Server using the Windows user settings for your network. Using this option, users enter their Windows user name and password to log in to Mobile Admin.

If you choose to use the Windows settings, you can configure Mobile Admin users to have access to the same servers and services in Mobile Admin as they do in your network or a subset of the servers and services they have permissions to manage in your network.

Mobile Admin user name and password authentication

If you decide not to use Windows login data for Mobile Admin, you can configure administrative access to Mobile Admin Server that is specific to Mobile Admin. Because Mobile Admin includes Windows security, you must specify at least one Windows account for the Mobile Admin Server to use to authenticate Mobile Admin users when a user logs in with their Mobile Admin-specific username and password.

If you specify one Windows account, Mobile Admin will use this account as the default Windows authentication for all Mobile Admin users when they enter their Mobile Admin-specific username and password. However, for each user, you can choose to either use the default Windows account or use any other Windows account. You can also configure or limit access to specific network servers, as long as these servers are a subset of the servers that the associated Windows account has permission to manage.

There are several ways to configure user access to your network if you choose to use Mobile Admin-specific passwords. The following sample configurations provide some examples.

Sample configuration 1

1. In Mobile Admin, set up one existing Windows account as the default account for Mobile Admin with a wide range of permissions, such as a domain administrator or administrator account.
2. In Mobile Admin, add users, and set up Mobile Admin-specific passwords for each user.
3. In Mobile Admin, configure access for each user to an appropriate subset of network servers.

Sample configuration 2

1. In Windows, create a specific Windows account that includes the permissions for all Mobile Admin users.
2. In Mobile Admin, set up the new Windows account as the default account for Mobile Admin.
3. In Mobile Admin, add users and set up Mobile Admin-specific passwords for each user.

Sample configuration 3

1. In Windows, create a specific Windows account with the permissions you want most Mobile Admin users to have.
2. In Mobile Admin, set up the new account as the default account for Mobile Admin.
3. In Mobile Admin, add users and set up Mobile Admin-specific passwords for each.
4. For users who require different permissions than the default Windows account, configure these users to use separate Windows accounts to authenticate with Mobile Admin.

Configuring Windows or Mobile Admin password authentication

1. In the Authentication Options screen, click Authentication Method.
2. In the Authentication Type drop-down menu, select an authentication type.
3. Complete the text fields, and click Save.

RADIUS authentication (Mobile Admin Professional and ProPlus)

Mobile Admin supports RADIUS authentication, unless Mobile Admin Server is installed on a host enabled with FIPS. RADIUS authentication allows Mobile Admin to act as a RADIUS client or RADIUS device for a RADIUS server and authentication system, such as SafeWord.

Enabling and disabling RSA SecurID authentication

To enable or disable RSA authentication, install the RSA security agent on the same computer as the Mobile Admin Server. For more information about using RSA SecurID Authentication, see the RSA website at www.rsa.com.

After you enable RSA SecurID authentication, you are automatically logged out of Mobile Admin. You will be required to enter your RSA SecurIDlogin information to log back in.

Enable RSA SecurID

1. In the Authentication Options screen, click RSA SecurID.
2. Select the Enable RSA SecurID check box.
3. Click Save.

Disable RSA SecurID

1. In the Authentication Options screen, click RSA SecurID.
2. Clear the Enable RSA SecurID check box.
3. Click Save.

Novel LDAP certificate options

The following procedures assume that you selected Novell LDAP Certificates from the Mobile Admin Options page and are on the Novell LDAP Certificates page.

Import a Novell certificate

Perform the following procedure to manage Novell servers and set up an encrypted channel between the Novell server and the Mobile Admin Server.

1. In the Novell LDAP Certificates screen, enter the full file path to where your certificate is stored in the Import Certificate file text field.
2. Click Import.

View imported Novell certificate information

1. In the Installed Novell Certificates screen, click the List Installed link on the menu.
2. Click a certificate name to view more details.

Remove imported Novell certificates from Mobile Admin

1. In the Installed Novell Certificates screen, click the List Installed link on the menu.
2. Select the Novell certificate you want to remove and click Remove on the menu.

Notification options

The Dashboard is only available for the Android, BlackBerry and Apple iOS platforms. The Mobile Admin Server pushes notifications to the devices.

Blackberry

Configure Mobile Admin Server to send notifications to the BlackBerry devices.

1. Log into Mobile Admin.
2. Go to Configuration > Options > Dashboard Options.
3. In the BES Hostname field, enter the URL to the BES MDS-Connection Service web page.
   This is typically `http://hostname:8080`.
4. You can use the hostname or IP address.
   The hostname or IP address must be resolvable by the Mobile Admin Server operating system.

Apple

Ensure that Mobile Admin Server can send notifications to the iPhone and iPad devices over ports 2197 and 2198 across the Internet. No configuration is required within Mobile Admin. However, port access to the Internet may need to be addressed in some networks.

Android

Ensure that Mobile Admin Server can send notifications to Android devices over port 2199 across the Internet. No configuration is required within Mobile Admin, but port access to the Internet may need to be addressed in some networks.

1. Locate the option to select the update interval for notifications.
2. Select the desired update interval and click Save.
   The Mobile Admin Server is now set to send notifications to devices.

Before you can access the dashboard, a feed, or a set of feeds, must be configured by a user. The Dashboard will then display status and alert information for the selected feeds.

Each Mobile Admin user has an individual Dashboard view. For information about the client side setup of the dashboard, see the Mobile Admin Client Installation and Usage Guide.

Audit Logs

Audit logs provide information about actions executed from within Mobile Admin. Log entries contain the following information:

- Date/time - the date and time the action was executed
- User - the user who executed the action
- Server - the name of the server on which the action was executed
- Service type - any of the Mobile Admin services (Microsoft Exchange, Novell, ping, etc.)
- Action - the action performed (create, delete, modify or execute)
- Action details - additional information about the action

You can search and browse audit logs using these selections.

All procedures in this section assume that you selected Audit Logs on the Configuration Interface, and are on the Audit Logs page.

Browse and search audit logs

Search an audit log

1. In the Audit Logs screen, click Search.
2. Enter search criteria in the appropriate field, and click Search.
   Wildcards are supported, and indicated with an asterisk.
3. Click a log entry to view more information.

Browse an audit log

1. In the Audit Logs screen, click Browse.
2. Select the criteria. If your search includes more than 100 results, Mobile Admin prompts you to further refine by date and time.
3. Click a log entry to view more information.

Configure network access to Mobile Admin

This section explains how to configure your wireless devices to access the Mobile Admin Server on your network.

Configure network access for BlackBerry smart phones

If you are running BlackBerry Enterprise Server, skip this chapter and go to Use Mobile Admin with a BlackBerry Enterprise Server.

If you are not running BlackBerry Enterprise Server, rent BlackBerry Enterprise Server from a hosting company for a monthly fee or use Mobile Admin without a server.

Mobile Admin uses port 4054 to communicate between the BlackBerry Enterprise Server and the Mobile Admin Server. If you use a BlackBerry Enterprise Server hosting company or use Mobile Admin without a BlackBerry Enterprise Server, make sure that the gateway is able to contact your Mobile Admin Server through this port.

> You can choose to change the port that Mobile Admin uses. For more information, see Server Options.

To use Mobile Admin without a BlackBerry Enterprise Server:

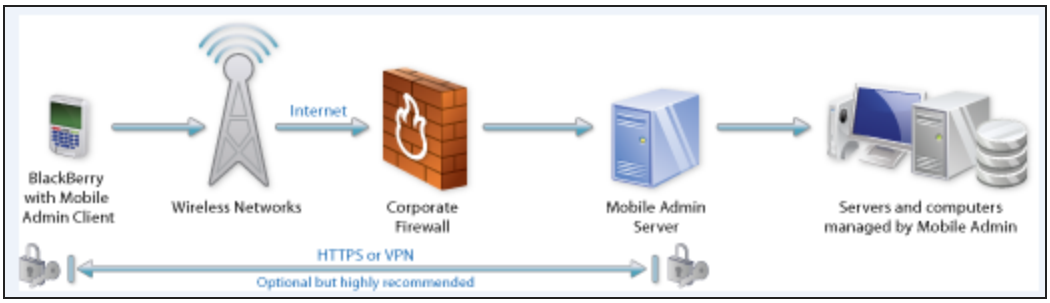
- Use a BlackBerry smartphone with OS 4.2.1 or later
- Connect from the Mobile Admin Client device to the Mobile Admin Server using Internet TCP/IP
- Make sure that your carrier has the Internet Access Point Name (APN) enabled for your device

> For more information about the Internet APN, see the BlackBerry Forums at www.blackberryforums.com.

Security without BlackBerry Enterprise Server

The BlackBerry network encrypts all data between BlackBerry Enterprise Server and BlackBerry handhelds with Triple Data Encryption Standard (TDES) or Advanced Encryption Standard (AES). When you do not use BlackBerry Enterprise Server, data sent between Mobile Admin Server and BlackBerry handhelds is no longer encrypted by default because it no longer channels through the BlackBerry Enterprise Server.

The following diagram shows how network security works for Mobile Admin without a BlackBerry Enterprise Server.



Configure network access for Android and iOS devices

If you use Mobile Admin with Windows Mobile, Nokia and/or iPhone/iPod Touch devices, you can connect to the Mobile Admin server from your wireless devices with or without a virtual private network (VPN). You can also choose to encrypt all Mobile Admin Data by connecting with HyperText Transport Protocol - Secured (HTTPS) if you do not have a VPN.

Connect with a VPN or HTTPS

It is strongly recommended that you connect to Mobile Admin Server from your wireless device through a VPN or with HTTPS. A VPN provides encryption and authentication options for your Mobile Admin connection and network data.

To use Mobile Admin with HTTPS, open port 4055 in your firewall to allow the connection between the Mobile Admin Server and the Mobile Admin Client installed on your wireless device.

For more information about configuring the default HTTPS connection, see Server options.

Connect without a VPN or HTTPS

It is not recommended that you use Mobile Admin without a VPN or HTTPS. In these conditions, your network data will not be encrypted.

To use Mobile Admin without a VPN or HTTPS, you must open port 4054 in your firewall to allow the connection between the Mobile Admin Server and the Mobile Admin Client installed on your wireless device.

Use Mobile Admin with BlackBerry Enterprise Server

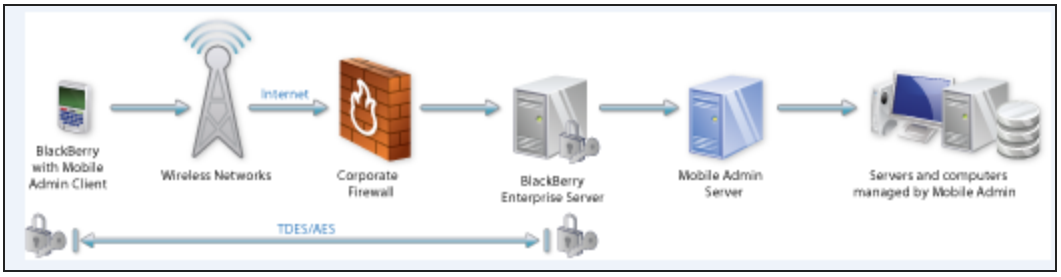
This section describes how Mobile Admin works through a BlackBerry Enterprise server.

If you are using a BlackBerry Enterprise server, Mobile Admin Server requires the BlackBerry Enterprise Server and Mobile Data Service (MDS) (also called the MDS Connection Service) to be configured correctly.

If you are not using a BlackBerry Enterprise Server, see Configure network access for BlackBerry smartphones.

How Mobile Admin works with BlackBerry Enterprise Server

The following illustration shows how Mobile Admin connects your BlackBerry smartphone to your network, and how your network data is protected when you use a BlackBerry Enterprise Server.



Mobile Admin Server is connected to the servers and computers that you want to manage with Mobile Admin. Information about these servers and computers is sent to BlackBerry Enterprise Server using an unencrypted connection or encrypted with HyperText Transport Protocol – Secured (HTTPS). BlackBerry Enterprise Server encrypts and transmits the data with TDES and/or AES through the Internet and the wireless network to the IT administrator's BlackBerry smartphone. The BlackBerry smartphone decrypts the data so that it can be viewed using the Mobile Admin Client.

Similarly, Mobile Admin Client commands from the BlackBerry smartphone are encrypted with TDES and/or AES, as well as HTTPS if you have configured it. The data is sent over the wireless network and the Internet to BlackBerry Enterprise Server. BlackBerry Enterprise Server decrypts the commands from TDES and/or AES and sends them to Mobile Admin Server, which decrypts them from HTTPS (if required) and performs the requested actions.

You can configure BlackBerry Enterprise Server to detect if network capabilities on the device are secured using RSA SecurID authentication. For information about securing network capabilities through BlackBerry Enterprise Server using RSA SecurID, see the BlackBerry Enterprise Solution and RSA SecurID white paper located at www.blackberry.com/products/pdfs/bb_rsa_whitepaper.pdf.

The above diagram shows Mobile Admin Server and BlackBerry Enterprise Server installed on separate servers. However, you can choose to install the Mobile Admin Server on the same computer as BlackBerry Enterprise server. For more information, see Install the Mobile Admin Server.

Configure specialized servers

Manage Microsoft servers with Mobile Admin

This section describes how to configure support for Microsoft servers (such as Microsoft Exchange and IIS) so they can be managed with Mobile Admin. Configuration is not required to manage Microsoft Active Directory, Microsoft Windows operating systems, or Microsoft DHCP.

Microsoft Windows 2008 Server

You can install Mobile Admin Server on a system running Windows Server 2008 (Windows 2008 Server R2 is recommended). On a Windows Server 2008 host, Mobile Admin requires the application server role. SolarWinds recommends granting Mobile Admin users local administrator rights to the Mobile Admin Server host, but it is not required.

Manage Microsoft Exchange

Mobile Admin can manage Microsoft Exchange using Local or Remote PowerShell Invocation. You can select the method used in the Host Properties page.

> Cross-domain administration of Microsoft Exchange 2007 and 2010 is not supported by Mobile Admin.

Local PowerShell Invocation

This method allows you to manage Exchange Server 2007, 2010, and 2013 systems. Some ActiveSync actions on Exchange Server 2013 may be limited with this method.

To use the Local PowerShell Invocation method, verify that:

- The corresponding Microsoft Exchange Management Tools and their prerequisites are installed on the Mobile Admin server host.
- The Mobile Admin server host is located in the same domain as the Microsoft Exchange server host.
- (Exchange 2007) The Microsoft administration toolkit (adminpak.msi) is installed in the operating system.

Remote PowerShell Invocation

This method allows you to manage Exchange Server 2010 and 2013 systems that are not included in the same domain as the Mobile Admin server host.

To use the Remote PowerShell Invocation Method, verify that:

- PowerShell version 2.0 is installed on the Mobile Admin server host.
- Windows PowerShell Remoting is enabled on the Mobile Admin server host.
- The corresponding Microsoft Exchange Management Tools (which includes PowerShell, and their prerequisites) is installed on the Exchange server host.
- Windows Authentication for PowerShell is enabled on the Exchange server host.
- PowerShell is configured to use FullLanguage mode on the Exchange server host.

Enable PowerShell Remoting

1. Open a command prompt with administrative privileges on the Mobile Admin server.
2. Run the following command:
   ```
   winrm quickconfig
   ```
3. Follow the onscreen instructions.

Enable Windows Authentication on PowerShell

1. On the Exchange server host, open Internet Information Services (IIS) Manager.
2. Navigate to Your Server > Sites > Default Web Site > PowerShell.
3. In the center panel, select Authentication.
4. Select Windows Authentication, and then select Enable in the Actions panel.
5. Restart IIS and recycle the Exchange application pools.

Enable FullLanguage

1. On the Exchange server host, open Internet Information Services (IIS) Manager.
2. Navigate to Your Server > Sites > Default Web Site > PowerShell.
3. In the center panel, select Application Settings.
4. Edit PSLanguageMode, and change the value to FullLanguage.
5. Restart IIS and recycle the Exchange application pools.

Manage Microsoft ActiveSync

Microsoft ActiveSync can only be managed using the Remote PowerShell Invocation option in the host properties of your Exchange server. Follow the instructions for Remote PowerShell Invocation to set up your Mobile Admin server and Exchange server.

Manage Microsoft IIS

To manage Microsoft IIS, Mobile Admin Server requires the IIS Common Files component be installed on the local host.

> You do not have to install the World Wide Web service, the FTP service, or any other components.

1. On the Start menu, click Control Panel.
2. On the Control Panel window, select Add/Remove Programs.
3. On the Add/Remove Programs window, click Add/Remove Windows Components.
   The Windows Components Wizard appears.
4. In the Windows Components Wizard, click Internet Information Services.
5. Click Details.
   The Internet Information Services window appears.
6. Make sure that Common Files is selected.
7. Click OK.
8. Follow the remaining prompts to complete the wizard and install the IIS Common Files.

Manage a Microsoft System Center Operations Manager 2007 server

To manage Operations Manager 2007 servers with Mobile Admin, the System Center Operations Manager 2007 SP1 Client Tools or the Operations Manager 2007 User Interface (32-bit) must be installed on the same machine as the Mobile Admin server. These tools are available from your System Center Operations Manager CD/DVD.

Manage a Microsoft System Center Operations Manager 2012 server

To manage Operations Manager 2012 servers with Mobile Admin, install the Operations console on the same machine as the Mobile Admin server. This is available from your System Center Operations Manager 2012 installer.

Manage a Microsoft System Center Mobile Device Manager server

The System Center Mobile Device Manager 2008 Administrator Tools must be installed on the same system as Mobile Admin to manage Mobile Device Manager servers with Mobile Admin.

Manage BlackBerry Enterprise servers

This section describes how to configure your BlackBerry Enterprise server so you can manage it with Mobile Admin.

Manage BlackBerry Enterprise Server 5.0.1 and above for the Exchange and Domino platforms

No additional tools or services are required to manage BlackBerry Enterprise Server 5.0.1, 5.0.2, and 5.0.3. However, some configuration is necessary. Management is performed through the BlackBerry Administration Service (BAS).

The BlackBerry Administration Service (BES 5.0.1) support may not be functional out of the box. Mobile Admin requires an additional configuration to properly detect the BlackBerry Administration Service.

The default BAS port must be set in the BAS server object properties. To set the BAS port property:

1. Access the Mobile Admin home page.
2. Selects the Manage Servers link.
3. Locate the BAS server object on the list and select it to reach the icons list of detected services.
4. Select the Server Properties actions link, or menu option.
   The properties page includes a BAS port setting which can be set to the corresponding port.
5. Change the zero default value to the port number in use by the BlackBerry Administration Service.

A BlackBerry Enterprise Server administrative roll must be assigned to each Mobile Admin user that will be responsible for managing the BlackBerry Enterprise Server.

BlackBerry Enterprise Server Express

No additional tools or services are required to manage BlackBerry Enterprise Server Express. However, some configuration is necessary. Management is performed through the BlackBerry Administration Service.

The BlackBerry Administration Service (BESX 5.0.1) support is not functional out of the box. Mobile Admin requires an additional configuration to properly detect the BlackBerry Administration Service. The default BAS port must be set in the BAS server object properties.

To set the BAS port property,

1. Access the Mobile Admin home page.
2. Locate the BAS server object on the list and select it to get the icons list of detected services.
3. Selects the Server Properties actions link, or menu option.
   The properties page includes a BAS port setting which can be set to the corresponding port.
4. Change the zero default value to the port number in use by the BlackBerry Administration Service.

A BlackBerry Enterprise Server administrative role must be assigned to each Mobile Admin user that will be responsible for managing the BlackBerry Enterprise server.

Manage BlackBerry Enterprise Server 4.x for the Exchange, Domino, and GroupWise platforms

You can download the BlackBerry Enterprise Server Resource Kit at:

https://www.blackberry.com/Downloads/entry.do?code=D736BB10D83A904AEFC1D6CE93DC54B8

This link may require registration at the BlackBerry.com site.

Ensure that you download the BlackBerry Enterprise Server Resource Kit version corresponding to the version of BlackBerry Enterprise Server. SolarWinds recommends installing only the BlackBerry Enterprise Server User Administration Service and not the entire resource kit.

Mobile Admin use the BlackBerry Enterprise Server User Administration Service included in the kit. Install the BlackBerry Enterprise Server User Administration Service on the BlackBerry Enterprise Server.

Use the following procedure to test your BlackBerry Enterprise Server User Administration Service installation.

1. Open a command prompt.
2. Navigate to the install directory for the BlackBerry Enterprise Server User Administration Service.
3. Enter the following to see a list of BES statistics:
   ```
   BESUserAdminClient -p yourpassword -stats -servers
   ```

A BlackBerry Enterprise Server administrative role must be assigned to the Mobile Admin user that will be responsible for managing BlackBerry Enterprise Server.

For Exchange Server, you will be prompted for the MAPI profile during the installation. In most cases, (the default setting) is BlackBerryServer. If you or someone else changed the MAPI profile before installing Mobile Admin, you must enter this custom MAPI profile instead.

For Domino, you will be prompted for the path to specified Domino files. These paths must be entered correctly.

Manage Backup Exec servers

To manage Backup Exec servers, install Windows PowerShell version 2.0 on each managed Backup Exec server and make some additional configuration changes on the Backup Exec and Mobile Admin servers.

PowerShell is included with Windows 2008 R2 and above. To install PowerShell 2.0 on Windows 2003 and 2008 R1, download PowerShell 2.0 from Windows Management Framework, and then run the installer.

Configure the Backup Exec server

To manage Backup Exec servers that are not installed on the same computer as Mobile Admin, enable PowerShell remoting on each server.

1. Open a command prompt with administrative privileges on the Backup Exec server.
2. Run the following command:
   ```
   winrm quickconfig
   ```
3. Follow the onscreen instructions.
4. If your Backup Exec server is installed on Windows 2003, increase the PowerShell session size by entering the following command:
   ```
   winrm s winrm/config/winrs @{MaxMemoryPerShellMB="256"}
   ```

Configure the Mobile Admin server

If Mobile Admin Server is not installed on the same computer as Backup Exec, add each server to the trusted hosts list In Mobile Admin Server.

1. Open a command prompt with administrative privileges on the Backup Exec server.
2. Run the following command for each Backup Exec server:
   `winrm set winrm/config/client @{TrustedHosts="RemoteHostName,IP"}`
   where `RemoteHostName` and `IP address` are the Backup Exec server's remote name and IP address.
3. If you encounter a WSManFault error, enter the following command and follow the onscreen instructions:
   `winrm quickconfig`

Manage IBM Lotus Domino servers

You can use Mobile Admin to manage IBM® Lotus Domino R5, R6, and R6.5, partitioned or unpartitioned servers.

> ⚠ To use Mobile Admin to manage IBM Lotus Domino 5.0 or later (partitioned or unpartitioned servers), Mobile Admin Server must be installed on the same computer as an IBM Lotus Domino 6.0 (or later) server. It is strongly recommended that you install the Domino server first, then install the Mobile Admin Server on the same computer. Do not install the Mobile Admin Server on a partitioned Domino server or a computer that has the Domino Client installed.

To manage Lotus Domino servers:

1. Log in to the Domino server where the Mobile Admin Server was installed.
2. Open the Current Server Document.
3. Click Edit Server.
4. On the Security tab, edit Run unrestricted methods and operations and add all administrators who will be using Mobile Admin.
5. Click Save & Close.

On each Domino server that you want to manage with Mobile Admin, do the following:

1. Open the Server Document.
2. Click Edit Server.
3. Under Administrators, add the Domino server where the Mobile Admin Server was installed.
4. Under Trusted Servers, (at the bottom of the screen) add the Domino server where the Mobile Admin Server was installed.
5. Click Save & Close.

   ⓘ This process may require up to 30 minutes for these settings to propagate and take effect.

Manage Citrix servers

The Enterprise version of Citrix® MetaFrame, Presentation, or XenApp server is required for Mobile Admin to manage a Citrix installation. To manage Citrix servers with Mobile Admin, install the Citrix WMI Provider on the Citrix MetaFrame, Presentation or XenApp servers that you want to manage.

Manage Novell servers

Mobile Admin uses Lightweight Directory Access Protocol (LDAP) to manage eDirectory and NDS on Novell servers. To use Mobile Admin to manage a Novell server, configure LDAP on your Novell server to allow anonymous binds.

To manage Novell eDirectory/NDS servers:

1. Make sure the LDAP server on the Novell server is enabled.
2. In Console One, select the LDAPServer object.
3. Right-click and select Properties.
4. Make sure that `ldapbindrestrictions` is set to `0`.