



Rove Mobile Admin Security

Introduction

Rove Mobile Admin is an enterprise-ready IT Management solution that generates significant cost savings by dramatically increasing the responsiveness of IT organizations facing outages and other issues. By enabling system administrators to access over 500 functions across dozens of different types of servers, platforms and devices through a convenient smartphone client, Mobile Admin provides a cost-effective means of increasing the availability of mission-critical business applications. The product enhances the efficiency of the IT team, which in turn has a direct positive impact on the productivity of the entire user population.

Security is a fundamental concern of all IT Management solutions, and it is of particular importance when mobile devices are used to access corporate information across the firewall. Mobile Admin's client-server architecture features a fully-integrated security model that provides both data encryption and user authentication.

Mobile control of your network

Mobile Admin is a client-server application. The Mobile Admin Server software is installed behind your corporate firewall on any one computer that has access to all other servers in your network that you want to manage. The Mobile Admin Client software is installed on your wireless device.

You can use Mobile Admin to manage a wide range of computers, servers, and systems in your network:

- Microsoft Windows computers and networks
- Microsoft Active Directory
- Microsoft Exchange 2000/2003
- Microsoft Exchange 2007
- Microsoft SQL Server
- Microsoft IIS
- Microsoft DHCP
- Microsoft DNS
- Microsoft Cluster Servers
- Microsoft SCOM
- Microsoft SCMDM
- IBM Lotus Domino
- Novell eDirectory/NDS
- BlackBerry Enterprise Server
- Blackberry Enterprise Server 5
- Oracle
- Citrix
- RSA Authentication Manager
- HP Integrated Lights Out (iLO)
- Backup Exec
- VMware ESX
- VMware Virtual Infrastructure
- Nagios

Mobile Admin allows you to use your wireless device to perform a full range of administrative tasks on these servers, including:

- managing users and groups, event logs, services, and print jobs
- rebooting servers
- resetting passwords
- editing server documents
- deleting mailbox messages.

Supported devices

Mobile Admin can be used with any of the following wireless handheld devices:

- BlackBerry smartphones
- Apple iOS devices
- Android devices

Mobile Admin can also be used on any computer with an Internet connection using the Mobile Admin Web Interface (Firefox and Internet Explorer are recommended).

Encryption

The types of data encryption available to you with Mobile Admin depend on the type of wireless handheld devices you use:

- BlackBerry smartphones, with or without a BlackBerry Enterprise Server
- Apple iOS devices, with or without a VPN
- Android devices, with or without a VPN

Encryption options for Mobile Admin on BlackBerry smartphone

You can choose to use Mobile Admin on BlackBerry smartphones with or without a BlackBerry Enterprise Server.

Mobile Admin with BlackBerry smartphones and a BlackBerry Enterprise Server

When you use Mobile Admin with a BlackBerry Enterprise Server, you are able to leverage the industry-leading security infrastructure of the BlackBerry network.

If you use a BlackBerry Enterprise Server, all your Mobile Admin data is sent over the Mobile Data Service (MDS), and is, by default, automatically encrypted using Triple Data Encryption Standard (TDES or 3DES). While TDES provides the highest industry standard encryption, you can also choose additional layers of encryption.

All versions of the BlackBerry Enterprise Server use TDES as the default encryption for all data. The BlackBerry Enterprise Server 4.1, however, allows you to choose between using TDES and Advanced Encryption Standard (AES), or both.

While TDES and AES are generally recognized as the most robust encryption methods available today, the US Government has also certified TDES and AES as compliant with Federal Information Processing Standards (FIPS).

The Mobile Admin Server is configured, by default, to add a layer of encryption with Hypertext Transfer Protocol – Secured (HTTPS). HTTPS is HTTP encrypted with Transport Layer Security (TLS). When Mobile Admin uses HTTPS, all Mobile Admin data transmitted between the Mobile Admin Server and the wireless handheld is encrypted.

Architecture overview—BlackBerry smartphones with a BlackBerry Enterprise Server

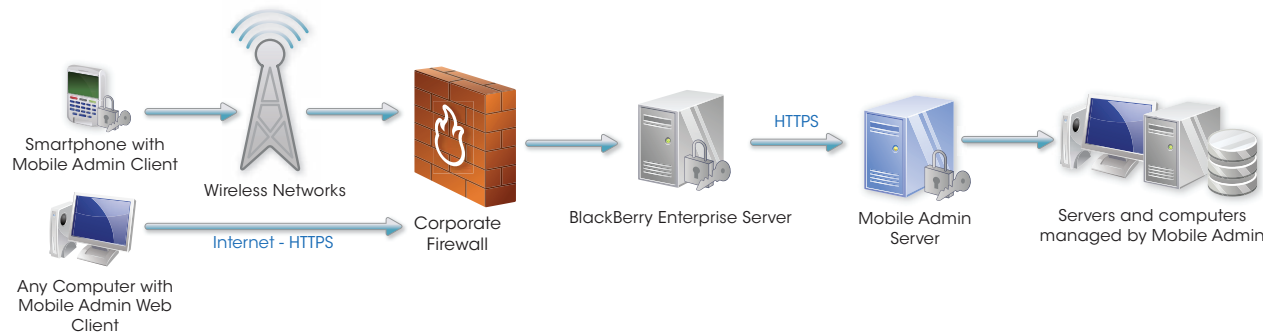
Figure 1-1 shows how Mobile Admin connects your wireless device to your network if you are using a BlackBerry Enterprise Server. The Mobile Admin Server is connected to the servers and computers that you want to manage with Mobile Admin. Information about these servers and computers is sent through the Mobile Admin Server to the BlackBerry Enterprise Server. The BlackBerry Enterprise Server encrypts the data with Triple Data Encryption Standard (TDES) or Advanced Encryption Standard (AES) and sends it over the Internet and the wireless network to the 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 then sent over the wireless network and the Internet to the BlackBerry Enterprise Server. The BlackBerry Enterprise Server decrypts the commands and sends them to the Mobile Admin Server, which then further decrypts the commands if required, and then performs the requested actions.

When Mobile Admin uses HTTPS, data is encrypted with TLS before it is transmitted between the Mobile Admin Servers and the BlackBerry smartphones.

Note Figure 1-1 shows the Mobile Admin Server and the BlackBerry Enterprise Server installed on separate computers. However, the Mobile Admin Server can be installed on the same computer as the BlackBerry Enterprise Server.

Figure 1-1
Architecture with BlackBerry smartphones
and a BlackBerry Enterprise Server



Protecting your network when a handheld device is lost

BlackBerry Enterprise Server 4.0 and above offers the ability to “kill” a lost BlackBerry device. The “kill” command disables the device, and deletes all of its stored information, including everything related to the Mobile Admin application. The “kill” command is one of the hundreds supported by Mobile Admin, enabling a system administrator to use one BlackBerry device to kill another one.

Mobile Admin with BlackBerry smartphones without a BlackBerry Enterprise Server

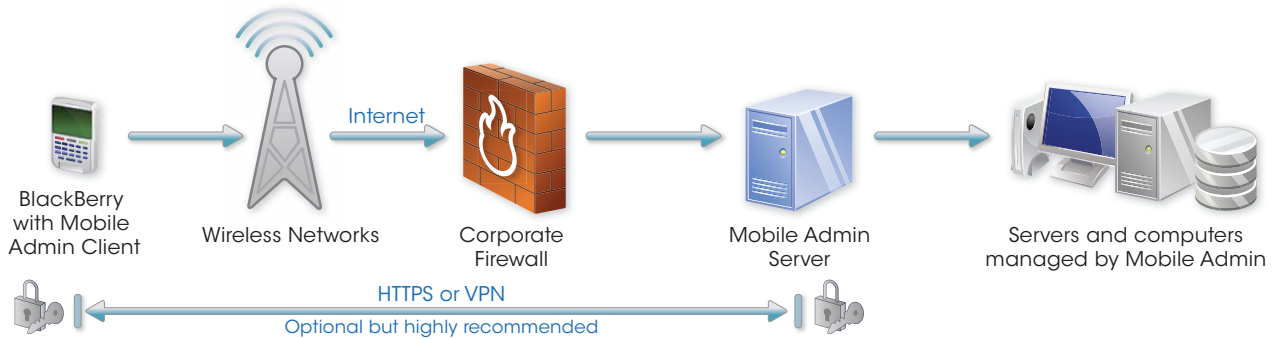
When you do not use a BlackBerry Enterprise Server, data sent between the Mobile Admin Server and BlackBerry smartphones can be encrypted using HTTPS. If you do not use a BlackBerry Enterprise Server with your BlackBerry smartphones, it is strongly recommended that Mobile Admin be configured to make HTTPS connections.

Architecture overview—BlackBerry smartphones without a BlackBerry Enterprise Server

Figure 1-2 shows how Mobile Admin connects your wireless device to your network if you are not using a BlackBerry Enterprise Server. The Mobile Admin Server is connected to the servers and computers that you want to manage with Mobile Admin. The Mobile Admin Server encrypts the data with HTTPS and sends it over the Internet and the wireless network to the 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 using HTTPS, and then sent over the wireless network and the Internet. The Mobile Admin Server decrypts the commands if required, and then performs the requested actions.

Figure 1-2
Architecture with BlackBerry smartphones



Other considerations

If you do not have a BlackBerry Enterprise Server, you can choose to either rent a BlackBerry Enterprise Server from a hosting company for a monthly fee, or to use Mobile Admin without one.

To use Mobile Admin without a BlackBerry Enterprise Server, you must:

- use a BlackBerry smartphones meeting Mobile Admin's minimum system requirements
- connect from the Mobile Admin Client handheld 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

Encryption options for Mobile Admin on Apple iOS and Android devices

You can choose to use Mobile Admin on Apple iOS and Android devices with or without a Virtual Private Network (VPN). If you use a VPN, all your Mobile Admin data is sent over the VPN, and is, by default, automatically encrypted.

By default, the Mobile Admin Server is configured to add a layer of encryption with HyperText Transport Protocol – Secured (HTTPS). HTTPS is HTTP encrypted with Transport Layer Security (TLS). When Mobile Admin uses HTTPS, all data transmitted between the Mobile Admin Server and the wireless handheld is encrypted.

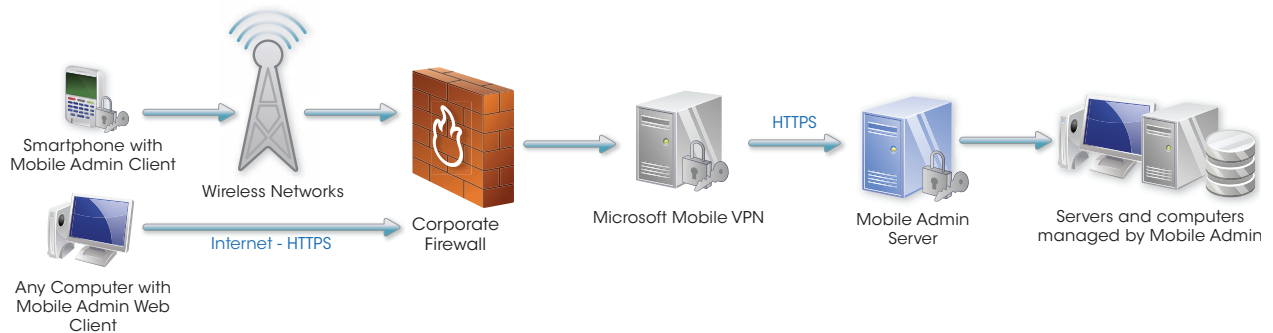
If you are using Apple iOS devices and Android devices with Mobile Admin, it is strongly recommended that you connect to your network through a VPN. If you cannot use a VPN, it is strongly recommended that Mobile Admin be configured to make HTTPS connections.

Architecture overview—Apple iOS and Android devices

Figure 1-3 shows how Mobile Admin connects your wireless handheld device to your network using a VPN and/or HTTPS. The Mobile Admin Server is connected to the servers and computers that you want to manage with Mobile Admin through a Virtual Private Network (VPN), which encrypts network data. The Mobile Admin Server encrypts the data with HTTPS and sends it over the Internet and the wireless network to the wireless handheld device. The Mobile Admin Client decrypts the data on the wireless handheld device so that it can be viewed.

Similarly, Mobile Admin Client commands from the wireless handheld are encrypted by with HTTPS, and can be encrypted with a VPN, then sent over the wireless network and the Internet. The Mobile Admin Server decrypts the commands if required, and then performs the requested actions.

Figure 1-3



Mobile Admin proxy

The Mobile Admin proxy is a service that runs on the same computer as Mobile Admin and proxies SSH/Telnet and RDP/VNC traffic. The Mobile Admin clients authenticate transparently to the proxy if the appropriate rights and permissions have been configured.

The Mobile Admin proxy enables access to SSH/Telnet and RDP/VNC servers through a central port, rather than having to configure access to each individual server.

If the Mobile Admin proxy is not used, then all SSH/Telnet and RDP/VNC servers must have the appropriate firewall configuration.

Other considerations

A VPN client is provided by default on all Apple iOS and Android devices.

Port and firewall configurations

Mobile Admin can use ports 4054 (the HTTP port), 4055 (the HTTPS port) or 4056 (the proxy port for SSH/Telnet and RDP/VNC connections) 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, you will have to make sure that the gateway you use is able to contact your Mobile Admin Server through these ports, which may require firewall configuration. You can also choose to configure the ports that Mobile Admin uses; if you change these ports used by Mobile Admin, you must make sure that your gateway is still able to contact your Mobile Admin Server.

Authentication

As well as data encryption, Mobile Admin supports three different levels of authentication:

- 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/RADIUS (optional)

Primary login authentication

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) that you may have configured for the user.

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 after time-out intervals that you specify.

Windows user name and password authentication

Administrative access to servers with Mobile Admin can be configured to use the Windows user settings for your network. With this option, users must always provide their Windows network user name and password to login to Mobile Admin.

If you choose to use the Windows network settings, you can configure Mobile Admin users to have access to either:

- exactly 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

Administrative access to servers with Mobile Admin can be configured to be specific to Mobile Admin, if you would rather not use Windows login data for Mobile Admin.

Because Mobile Admin is fully integrated with Windows security, you must specify at least one Windows account for the Mobile Admin Server to use to authenticate Mobile Admin users when they login with their Mobile Admin-specific username and password.

If you specify one Windows account, Mobile Admin will use that as the default Windows authentication for all Mobile Admin users when they enter their Mobile Admin-specific username password. However, for each user, you can choose to:

- use the default Windows account, or use any other Windows account
- further 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

Because of the many available choices, there are several ways to configure user access to your network if you choose to use Mobile Admin-specific passwords. The following three examples are provided to illustrate some of the possibilities.

Sample configuration #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.
- In Mobile Admin, add users, and set up Mobile Admin specific passwords for each user.
- In Mobile Admin, configure access for each user to an appropriate subset of network servers.

Sample configuration #2:

- In Windows, create a specific Windows account that has the permissions that you want all Mobile Admin users to have.
- In Mobile Admin, set up the new Windows account as the default account for Mobile Admin.
- In Mobile Admin, add users, and set up Mobile Admin specific passwords for each.

Sample configuration #3:

- In Windows, create a specific Windows account that has the permissions that you want most Mobile Admin users to have.
- In Mobile Admin, set up the new account as the default account for Mobile Admin.
- In Mobile Admin, add users and set up Mobile Admin specific passwords for each.
- For the small number of users who you want to have different permissions than the default Windows account, configure them to use different appropriate Windows accounts to authenticate with Mobile Admin.

Device-level password authentication

Most wireless handheld devices and phones provide optional device-level authentication. When the device password feature is enabled, you must enter a password before you can use the device and Mobile Admin.

Device-level passwords for BlackBerry smartphones

The BlackBerry smartphone password provides device-level authentication on BlackBerry smartphones. After ten failed attempts to enter the handheld password, all information on the handheld is erased for security purposes.

By default, the handheld password feature is not enabled. The handheld password can be enabled at the device level by each user. Alternatively, your BlackBerry Enterprise Server administrator can edit the IT Policy for the BlackBerry Enterprise Server to require a handheld password for some or all users.

Security time-out settings define how long a handheld device must be inactive before a user is required to enter the handheld password. These settings can also be configured at the device level by individual users, or by modifying the IT Policy on the BlackBerry Enterprise Server for some or all users.

For extra security, it is recommended that you enable the BlackBerry smartphone password for all Mobile Admin users.

For more information about how to enable the handheld password and to configure the security time-out, please refer to the user documentation for your BlackBerry smartphone.

Device-level passwords for Apple iOS and Android devices

By default, device-level passwords are not usually enabled, and must be enabled at the device level by each user.

For extra security, it is recommended that all Mobile Admin users enable the device-level password.

For more information about how to enable the device-level password for your device, please refer to the user documentation that was provided with your device.

RSA SecurID and RADIUS authentication

Mobile Admin also supports the option of using RSA SecurID authentication, and has been officially approved as an RSA-Certified application. RSA SecurID provides “twofactor” authentication, which requires a user to enter a combination of a secret, personal identification number (PIN) and a code from a SecurID token. The token generates a new, unpredictable code every 60 seconds. These PIN and code combinations are synchronized with the RSA Authentication Manager, which is installed on your network and controls access to RSA-protected applications and devices.

If you choose to use RSA SecurID authentication with Mobile Admin, users will have to enter their PIN and token code before they can log in to Mobile Admin. For more information about using RSA SecurID authentication, please see www.rsasecurity.com.

Mobile Admin also supports RADIUS authentication, which means that Mobile Admin can act as a RADIUS client or RADIUS device for whatever type of RADIUS server and authentication system you are using, such as SafeWord.

Credential and Information Logging in Mobile Admin

Client(Mobile User)

If a login to the network is required, the user is prompted for authentication information. This authentication information takes the form of

- (optionally) RADIUS or RSA SecurID 2-factor authentication
- (optionally) device-level authentication
- (required) Windows credentials

If the authentication is successful, the server passes back a token to the client that is required in subsequent transactions between the client and server. This token is not stored on the mobile device between sessions.

The sessions can be configured from the server – the server can be configured to ensure that the token expires after a period of time. The default token length is 10 minutes.

When overriding credentials are used for individual managed servers, this information is sent directly to the Mobile Admin server (within your data center) and stored securely on it. This information is not used in a token, nor is it stored on the mobile device in any way.

As well, on all mobile platforms, any state information stored by the Mobile Admin client is stored in common persistent storage areas – if a device for any reason becomes compromised, wiping the devices will remove all of this state information. The only state information stored persistently is configuration and preference information – not credentials.

Server

During the authentication process, once the server securely receives the credentials, they are passed onto the relevant subsystems for validation.

The server stores two types of data:

- Configuration data (user and server preferences, Mobile Admin policy information, etc)
- Server characteristics (port settings, etc)

Any sensitive data related to credentials (usernames and passwords) are encrypted using Triple-DES encryption before being placed in a SQLite back-end that is embedded in the Mobile Admin server. Strong key management is handled by the OS and .NET APIs, not Mobile Admin. Users on the Mobile Admin server that have file access rights to the Mobile Admin installation folder can access the back-end data. This data is extremely well protected, as long as routine and prudent measures are taken to secure the Mobile Admin server from unauthorized entry (as with any other server host).

Audit and Debug Logging

There are two categories of information stored by the Mobile Admin server:

- Audit Logs
- Debug Logs

Audit log information is maintained inside the database, but this information does not contain any identifying data other than the user login name that performed the action. This information is kept indefinitely to satisfy compliance and regulation-related requirements of our users. It can be browsed and searched from within the administration interface of the Mobile Admin server.

Debugging and diagnostic information is stored on the server in a text file in the Mobile Admin directory – by default, the server only logs for debugging purposes information related to server activity and events. This information can be configured to be more detailed, but this is usually only done to diagnose a support issue. Great care and testing have taken place to ensure no sensitive information enters debug logs. These logs are not rotated or deleted unless the user removes them manually.