



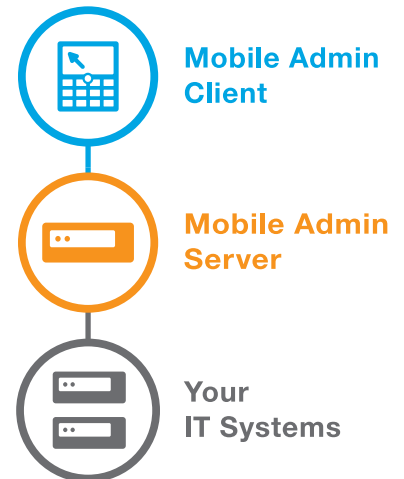
Rove Mobile Admin Architecture

Introduction

Rove Mobile Admin is an enterprise-ready IT Management solution that enables system administrators to monitor and manage their corporate IT infrastructure from a mobile device. When issues occur at inconvenient times, Mobile Admin enables administrators to respond immediately to determine the cause of the problem and take corrective action without having to get to a computer to access the corporate network. The product offers customers four key benefits:

- By reducing the amount of downtime when an issue occurs, Mobile Admin generates substantial direct cost savings.
- Mobile Admin provides a cost-effective means of increasing the availability of IT systems and services by reducing the Mean Time to Recovery (MTTR) rather than increasing the Mean Time Between Failures (MTBF), which generally involves expensive hardware duplication.
- By enabling system administrators to access a wide range of servers, services, systems and platforms from their smartphones, Mobile Admin increases the coverage and responsiveness of IT teams without the need for additional headcount.
- Mobile Admin gives system administrators unprecedented freedom and convenience, better enabling them to manage the demands, interruptions and urgent issues that occur both during office hours and while fulfilling on-call responsibilities. The result is measurably higher job satisfaction and greater employee retention on the IT team.

This white paper describes the Mobile Admin architecture, highlighting the breadth, security, scalability and reliability benefits that it provides. The document also describes a number of Mobile Admin deployment options.



Mobile Admin Architecture

Rove Mobile Admin features a client-server architecture engineered to scale cost-effectively from small, single-office networks to large global deployments. A single server can support up to forty clients, depending on the configuration. More servers can be added as required, based on the number of Mobile Admin clients, the number of geographic sites and the network topology.

The Mobile Admin Server

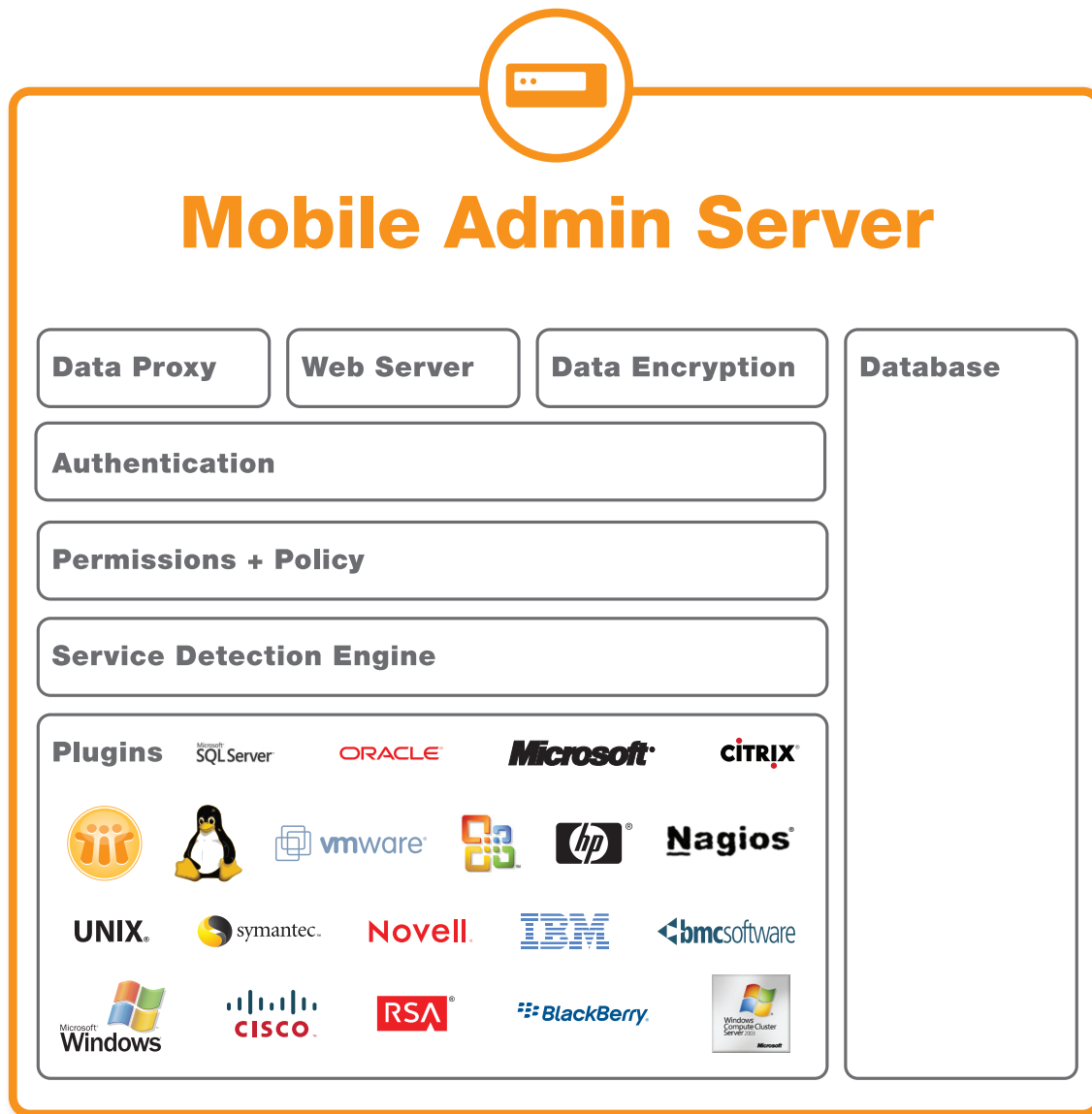
The Mobile Admin server runs on a Microsoft Windows server which can be either a dedicated physical machine or a virtual server. The server is installed behind the firewall centrally within the IT system that is to be managed. The server is then configured with the names of all of the servers and devices to which it will connect. Essentially, the Mobile Admin server sits in the network, extracts information from the IT infrastructure and relays commands from the system administrators to the systems and services. The Mobile Admin server is the heart of the solution, providing access to over 500 distinct functions spread across dozens of different types of servers and platforms.

The Mobile Admin Client

The Mobile Admin server is accessed through the Mobile Admin client, which runs on a wide range of smartphones. The clients register with one or more Mobile Admin servers, and then communicate securely with those servers to access information from the network, and to issue commands, modify configuration files, and perform other actions that control the behavior of the network and systems. In

in addition to the Mobile Admin user interface, which provides direct intuitive access to numerous different servers and services, Mobile Admin supports Telnet, Secure Shell (SSH), Virtual Network Computing (VNC) and Remote Desktop Protocol (RDP) for access to virtually any device on the network.

The Mobile Admin client can also be accessed through a web interface from any computer, or from any browser-enabled smartphone.



Breadth

The Mobile Admin server supports a plug-in architecture that enables connections to multiple back-end servers, platforms, systems and devices to be discretely introduced and managed. The product is designed to support complete corporate IT infrastructures, and new plug-ins are introduced with each new release of the product. Mobile Admin supports:

- Monitoring systems such as Microsoft System Center Operations Manager and Nagios;
- Email systems such as Microsoft Exchange and IBM Lotus Notes/Domino;
- Mobile systems such as BlackBerry Enterprise Server and Microsoft System Center Mobile Device Manager;
- Database systems such as Microsoft SQL Server and Oracle;
- Network servers such as Dynamic Host Configuration Protocol (DHCP), Internet Information Services (IIS) and Domain Name System (DNS);
- Virtualization such as Citrix and VMWare;
- Specific third party solutions, such as HP iLO, Symantec Backup Exec and RSA SecurID
- Microsoft Windows, Novell, UNIX, Linux and AS/400 servers
- IBM Mainframes

Mobile Admin supports over 500 distinct functions across these servers, platforms and systems. Together, these functions enable system administrators to monitor the IT infrastructure, identify and diagnose any issues that occur, and then take corrective action. Mobile Admin can also be used proactively to monitor and manage the network at times when it is inconvenient to access a computer. For example, when running processor or network intensive jobs during off hours, Mobile Admin provides a convenient and powerful means of checking the status of the work and addressing any issues that occur.

Reliability

Mobile Admin communicates with the IT Infrastructure using well-defined interfaces and connectors. The product does not require the installation of software agents on the managed servers, platforms and devices, which enables the IT infrastructure to continue to operate with undiminished performance and reliability. Indeed, the availability of the infrastructure is significantly improved because the addition of Mobile Admin enhances the overall responsiveness of the IT team when some element of the infrastructure does require attention. The Mobile Admin server itself can be deployed in redundant configurations. If a Mobile Admin server becomes unavailable for any reason, the clients can simply connect to an alternate Mobile Admin server that has access to the same back-end servers and services.

Scalability

The Mobile Admin client-server architecture is engineered to cost-effectively scale up to support the largest global installations. Any number of Mobile Admin servers can be independently added to the network and configured to support a specified number of clients (Rove provides a deployment guide which contains recommendations for the number of clients per server depending on the server configuration). In smaller installations, each Mobile Admin server might be configured to see the entire infrastructure, but as organizations grow, the Mobile Admin servers are typically configured to focus on a specific part of the infrastructure. In either case, the server includes a “Service Detection Engine” which enables it to automatically detect the services that are running within its configured realm. This automatic detection greatly simplifies the deployment of the product in large networks.

Each Mobile Admin user accesses the functionality through a client running on a mobile device. Each client can register with one or more servers, as required. Smaller organizations tend to enable every client to access the complete infrastructure, while larger organizations tend to introduce IT specializations which focus each administrator’s responsibility on a specific part of the overall infrastructure. In either case, the Mobile Admin client can show all of the servers, services, platforms and devices that are configured on the server, or it can be customized to show only a selected subset, for convenient access. In all cases, the system administrator’s ability to monitor and manage is controlled by the permissions that have been established within each of the back-end servers and systems.

Security

Security is a fully integrated feature of the Mobile Admin server, which offers intrinsic support for both encryption and authentication. In addition, the product is designed to take advantage of the BlackBerry Enterprise Server (BES) security model.

Encryption

When Mobile Admin is used with BES security, all Mobile Admin data is sent over the Mobile Data Service (MDS) which uses Triple Data Encryption (Triple DES), Advanced Encryption Standard (AES) or both. If the BES server is not used, Mobile Admin supports connections through a Virtual Private Network (VPN), in which case the data is encrypted by definition. In all cases (BES, VPN or neither), Mobile Admin supports HTTPS connections, which encrypt the data using Transport Layer Security (TLS).

Authentication

The Mobile Admin server authenticates every client before providing access to any monitoring or management functionality. The mandatory authentication can be achieved in one of two ways:

- Microsoft Active Directory username and password
- Mobile Admin-specific username and password

When using the Microsoft Active Directory authentication, the Mobile Admin permissions and policy engine can either provide access to exactly the same servers and services that are available to this user directly through the network, or it can restrict the user's Mobile Admin access to a subset of these. When using a Mobile Admin-specific username and password, it must be associated with

an Active Directory account for security purposes. One or more default Active Directory accounts can be created for this purpose, with the desired access permissions. Each Mobile Admin user account can be tied to one of the default accounts or any other Active Directory account. The Mobile Admin permissions and policy engine can then be individually configured to allow each user access to the full set of servers and services that the associated Windows account allows, or to a subset of those. In no case will Mobile Admin enable access to any server or service that is unauthorized for the associated Active Directory user account.

IT Infrastructures often include servers and services that are independent of Microsoft Active Directory. For example, UNIX server permissions are beyond the scope of Active Directory. In such cases, Mobile Admin users will be prompted to enter their credentials before accessing the server or service in question. In every case, Mobile Admin will require that the user is successfully authenticated before providing access to any monitoring or management functionality.

In addition to the mandatory authentication described above, three optional authentication steps can be used for further security. These are:

- Device level authentication, which causes the mobile device to require a username and password upon startup, and after a configurable period of inactivity. The details and usage of device level authentication is dependent on the specific device.
- RSA SecurID two factor authentication, which requires both a username/ password and a dynamically generated secure token.
- Remote Authentication Dial-In User Service (RADIUS), which is a centralized authentication model.

Data Proxy

One final security measure is the Data Proxy server that is included in the Mobile Admin server. This feature enables Mobile Admin to support Telnet, SSH, VNC and RDP connections to send and receive data through the Mobile Admin ports, rather than forcing separate ports to be opened for those connections. Mobile Admin will examine all of the information sent through these ports to confirm that it is valid Mobile Admin data. This careful use of communication ports is consistent with standard best practices for security.

Web Server Support

The Mobile Admin server incorporates a web server that manages all client and browser communications with Mobile Admin. The web server enables Mobile Admin to be deployed without dependence or additional load on existing Microsoft IIS servers.

Database

The Mobile Admin server includes a database that is used to securely store information specific to the Mobile Admin solution. This information includes:

- Configuration settings
- Mobile Admin account information
- Audit tables
- Log files

Authorized administrators can examine the data in the Mobile Admin database in real time, or can generate reports.

Deployment Options

The specific details of any Mobile Admin deployment are heavily dependent on the unique aspects of the network on which it is installed. Apart from these specific differences that can exist, there are three fundamental deployment options for Mobile Admin:

- Using BlackBerry devices and connecting through the BES
- Using any supported devices and connecting through a VPN
- Using any supported devices and connecting without a VPN

In all cases, the Mobile Admin server must be installed within the network that is to be managed, where it can establish the necessary connections with the back end infrastructure. The Mobile Admin server should never be installed in a DMZ, where it would be unable to establish those connections. The security model for each of these deployments is different as described above, although encryption is used to protect the data in every case. And in every case, the full power of the Mobile Admin server is available through the mobile device, enabling the generation of substantial cost savings, providing cost-effective increases to network availability, enhancing the efficiency of the IT team and improving employee retention.

