



Application Note:

Gateway Management Program

The Gateway Management program provides command and control of remote Gateways.

Overview

JBM Electronics has developed a Gateway Management System (GMU) to complement the Gateway Product Family. The system provides monitoring and updating of a remote Gateway's operating system, application, configuration and status. The Management system consists of a JBM supplied central site server with the Management database and Web-GUI interface. Each remote unit also contains a custom Management Client to interface with the central site component. The Client uses a check-in, pull-based method of reporting and obtaining updates.

Key Benefits and Features

- Provides simple management of remote Gateways
- Centralized tracking of all remote JBM Units
- Consolidated Command and Control of all Gateways
- Summary and detail displays of all units
- Unit Status and Event summary with at-a-glance color coding
- Detailed history of individual Gateway's behavior over time
- Patch Management to update remote units
- Alerts when a Gateway report errors or have trouble communicating
- Support Static and Dynamic DNS Connections

Operation

First-time installation and configuration of Gateways is now much easier. Once a Gateway has network access and is configured to communicate to a specific central site Management Server, almost all other updating and configuration can be controlled from the central site.

When the remote Gateway is installed, a connection script can be enabled. This script is used to implement communications between the remote edge Gateway and the central site management Server. The communication path is used for heartbeats, retrieving new configurations, operating system and application patches and for regular management tasks. The connection interval is configurable and is controlled by the script on the remote Gateway.

The remote Gateway uses a separate TCP session to communicate with the GMU. At connection, the Gateway provides the GMU with the signal strength (for cellular units), the number of bytes transferred since the last connection and the unit's IP Address. If the Gateway is assigned a Dynamic IP Address, this capability allows the GMU to imitate a connection to the remote unit. The GMU maintains a MySQL database of all of the authorized Gateways. An operator can select a specific Gateway from the list and with a simple mouse click, establish a session with the Gateway.

The remote Gateway pulls files and commands from the central server. This architecture supports both Static and Dynamic DNS connections by allowing the remote Gateway to initiate access to the central site. Triggering remote units to force an expedited check-in is also supported. Furthermore, units with Dynamic IP Addresses can be configured to check in every time their IP Address changes.

Units can be manually pre-added to the central site database, or simply be allowed to check-in for the first time and then be manually authorized. Units are keyed by their unique serial number, but provisions are available to store associated unit information unique to your specific corporate unit organization. Searching for units by corporate organizational identifiers is an integral feature, so you do not need to convert from your current method of tracking units.

The central site server manages all patches and files to be sent to remote units. Sending a patch is as easy as creating a “job” for the unit, and choosing the serial number and a specific patch file. Then simply wait for the unit to check-in, or trigger the unit manually. While waiting, you can check the list of pending jobs to be sent to remote units. After the job has been issued to the remote unit, you can watch for the unit to report back on the status of the application of the patch. The cycle of checking for jobs will be repeated by the remote unit until it has finished all pending jobs and applied all updates.

In addition to sending updates to programs and configurations, jobs may also be configured to send commands. Using this feature will allow a level of remote control over units, commanding them to reboot, transfer logfiles off to a repository, or other automated processes.

Security

Keeping remote units safe and secure from unauthorized updates is vital. For this reason, an update or command can never be pushed to a remote unit. Instead, the remote unit must first contact a known and trusted central site JBM Management Server. In addition, the communication between the central site and remote units is validated by an encrypted key exchange.

Each user session that accesses the Management Server database is protected by accounts with individual permission levels and passwords. The Management Server can control access of a remote unit based upon any combination of the following:

- Gateway’s IP Address
- Gateway’s Serial Number
- Customer-selected Identifier

The access control provides an additional level of security to enhance the Gateway’s integrity.

Central Site Command and Control

For additional control, an operator at the central site can access the Gateway through Telnet or SSH to execute scripts or configuration changes. The operator can retrieve logs and statistics or perform other diagnostic functions. On connections without bandwidth limitation, the Gateway’s Web menus can be used to perform these functions.