UPLOGIX

> Technical Fact Sheet

Uplogix Local Management Capabilities

The Uplogix Local Management platform is located with, and directly connected to managed network devices and servers. This deployment allows Uplogix to perform the administrative functions that are best done locally, strengthening existing network management and lowering operational expenses, improving infrastructure performance and availability, and addressing significant security and regulatory compliance vulnerabilities.

Uplogix offers the most options for out-of-band connections including cellular (2G/3G/LTE), v.92, Ethernet, and Iridium satellites, ensuring you can reach your gear anywhere on Earth.

Local Connectivity Options

- RS-232 – the most reliable dedicated access method. RJ-45 wired as DCE to connect over standard CAT-5 patch cables to most networking equipment (adapters available)
- Console server option – SSH or RFC2217 (Serial over Telnet) TCP socket connection to a console server port that is already connected to a managed device
- SSH or Telnet connection to managed device – connect to device's management interface over TCP socketsSerial and TCP port forwarding back to the local workstation, enabling the use of vendor provided RS-232 tools and other interfaces
- HTTP(S) – ability to query an http interface to query web pages of devices; parse the results and trigger other HTTP(S) GET and POST types
- SSH-VTY virtual ports establish secure connections to simplify management for devices like service processors where users simply desire to use the SSH TCP port-forwarding feature to forward the GUI and other application ports without making an actual SSH or telnet virtual connection to the device.

Local Configuration Management

- Automatically retrieve and store device OS – includes six named versions, the current, previous, and candidate versions per managed device
- Automatically retrieve and store device startup configuration files – includes five named versions, the current, previous, candidate and up to 19 archived versions per managed device
- Automatically retrieve and store device running configuration files – includes five named versions, the current, previous, candidate and up to 19 archived versions per managed device
- Support scheduled recurring jobs that automatically retrieve the current OS, startup and running configuration files per managed device
- Support scheduling a job to update a startup or running configuration file for one or multiple devices across the network, where the device configurations to be updated are specified through advanced filtering that operates on hierarchical groups, Local Managers, managed devices, device make, device model, OS name and the OS version
- Support scheduling a job to upgrade the operating system for one or multiple devices across the network where the devices to be upgraded are specified through advanced filtering that operates on hierarchical groups, Local Managers, managed devices, device make, device model, OS name and OS version
- Display configuration changes made during a user session to a managed device when the session is complete so the user can confirm the changes are accurate and commit the changes.
- Automatic rollback of configuration changes made during a user terminal session to a managed device if the session times out and user does not commit changes
- Display configuration changes made during a user terminal session to a managed device and enable the user to automatically rollback the changes
- Support bare metal restore on a replacement device by installing OS and configuration files
- Support the ability to independently recover a configuration on a managed device for the case where the configuration is corrupted

Deploying Uplogix

Uplogix Local Managers (LMs)
Available in both scalable and smaller fixed-port formats, Uplogix LMs manage up to 38 devices including networking and satellite communications gear, servers and other IT infrastructure located at data centers, branch locations... wherever you have equipment that needs management.

Uplogix Control Center (UCC)
Deployed in the NOC, the Uplogix Control Center delivers real-time monitoring and management capabilities, offering a unified view of what's occurring in your distributed infrastructure. As an element manager for up to 3,000 Uplogix Local Managers, the Control Center also serves as the gateway between the LMs in the network and existing IT management systems.

Custom Deployments
All Uplogix custom solutions are based on the patented Local Management Software (LMS), originally developed for use on specialized Uplogix hardware (Uplogix Local Managers). Uplogix LMS is now available, in its entirety, packaged as a virtual machine. Virtual Local Managers of all kinds can be mixed and matched in the same deployment with Uplogix Local Managers and other kinds of Local Managers. This creates the opportunity for tremendous flexibility in the way that customers create Local Managers for use in their Uplogix deployment.

For more, please go to uplogix.com

> Technical Fact Sheet

Device Monitoring

- Regularly monitor a device and automatically restore the startup configuration and standard/certified OS for the device if the device is replaced (due to RMA) or found without its configuration
- Regularly monitor a device and automatically recover the device if the OS is missing or corrupted, or if the device is stuck in a boot loader state
- Monitor and save device CPU and memory utilization
- Monitor and save device interface status and statistics
- Monitor and save device log messages
- Monitor and save power on self test (POST) messages when managed device powers up
- Monitor commands typed by user in a terminal session
- Monitor device connectivity using ICMP Ping

Service Level Monitoring

- Represent interfaces on multiple networks, QOS tagged, performed just as end user devices
- Regularly monitor network based services to validate availability
- Execute tests ad-hoc for troubleshooting
- Available types include Voice, Web Transaction and TCP:
  - Voice – executes a synthetic call using similar codecs of humans speaking phonetically balanced "Harvard" sentences – provides 47 RTCP elements.
  - Web Transaction – executes a HTTP(S) transaction including DNS lookup, SYN/ACK round trip time, time to first/last byte, HTTP result codes, and includes the ability to parse the first 1000 bytes for a keyword or phrase
  - TCP Port – Executes a SYN/ACK round trip to measure network latency and availability for any TCP-based application

Flexible Automation

- Support a customizable rules engine that takes action when collected data meets specified conditions, allowing users to create specialized, automated operations based on their run book and best practices
- Support following actions:
  - Execute any CLI command on device
  - Generate alarms
  - Generate events
  - Power on/off/cycle device
  - Initiate out-of-band connection
  - Push configuration file to device
  - Pull configuration file from device
  - Reboot device
  - Issue "show tech" on device
- Send email alerts for device and system alarms
- Temperature and humidity can be monitored by an optional USB-connected sensor. Data can be used by the rules engine.

Secure Operations

- FIPS 140-2 Level 2
- On-board storage: SSDs available with 256-bit AES compliant data encryption
- Encrypt all data transferred to centralized management server
- Support local authentication and authentication to RADIUS, TACACS and Microsoft Active Directory servers (LDAP)
- Support local authentication and authorization to TACACS and RADIUS servers (AD/LDAP proxy via Uplogix Control Center)
- Support specification of preferred and allowed ciphers, hashing, compression and key exchange algorithms for SSH
- A robust granular authorization model:
  - Access can be defined by groups, with users only able to see devices they have proper credentials for
  - Limit the functions a user is able to implement based on their role
  - Roles and responsibilities can be broken down by user, device, location and label
- SSH certificate authentication
- LM can establish a reverse SSH tunnel back to the UCC over in- or out-of-band connections that carry SSH terminal connections with the UCC acting as a proxy to overcome network address translation (NAT) and other issues

Out-of-Band Management

- With the loss of the primary WAN connection, Uplogix can provide a tethered WAN traffic failover option by sharing its cellular out-of-band connection with the local router
- With a secure out-of-band connection back to the NOC, administrators can connect to remote managed devices during the network outage, and Uplogix continues to forward alarms, events, alerts and SYSLOG messages.
- Monitor primary network connectivity during an outage and automatically tear down the out-of-band network connection when primary network connectivity is restored.
- Support encrypted dial-in access with caller-ID filtering

Logging

- Log all keystrokes typed by a user while logged into the Local Manager to a session file that is stored locally and on the Uplogix Control Center
- Send SYSLOG message for all Local Manager alarms and events to a designated SYSLOG server
- Forward log messages collected from a managed device to a SYSLOG server on behalf of the managed device
- Generate and store events for the Local Manager and its managed devices that are viewable locally and on the centralized management server
- Store device changes made by users in terminal sessions to managed devices locally and to the Uplogix Control Center

Reporting

- Provide hourly, daily, weekly and monthly reports for configuration changes, alarms, events, and logins

Integration

- Full multi-tenant support – granular authorization and roles allow multiple tenants to share the same Uplogix Control Center
- Send SNMP messages to northbound management system for all alarms/events
- Send Console log entries to SYSLOG servers
- User interface integration with centralized management tools

