UPLOGIX

> Solution Brief

Uplogix Local Management for Infrastructure Security

What Makes Uplogix Different?

We're turning network management inside out by deploying intelligent monitoring and automation to where network devices are to improve security, performance and availability. It's like having a virtual onsite technician.

Uplogix is a network independent management platform that is located with—and directly connected to—managed devices. It can stand alone or augment your existing centralized management tools providing the configuration, performance and security management automation functions that are best performed locally.

The benefits are reduced operational costs, faster resolution when issues arise and improved security and compliance vs. centralized only management. Our enhanced focus on network and communications devices hardens your infrastructure for increasing performance and availability requirements deriving from the use of applications like video conferencing, SaaS and VDI, and makes M2M applications economically feasible.

Locking down long-time vulnerabilities and remote site management weaknesses

Two forms of critical security vulnerabilities continue to plague mission critical network infrastructure and account for the majority of related security breaches:

- **Maintaining secure software and configurations** | Updating the software on, and configuration of, network and communications devices in the face of constantly evolving security threats
- **Securing Administrative Console Access** | Ensuring appropriate and audited access and compliance with policy by the technicians, sometimes employees sometimes not, that you rely on to maintain network and communications gear

Maintaining Secure Software and Configurations

Securing the network is an on-going battle that can never ultimately be won as new forms of attack are being developed and new vulnerabilities discovered every day in even the best software. For example in 2013 Cisco alone issued 42 Security Advisories typically recommending configuration changes or software patches.

> Network devices that cannot be frequently and easily configured and upgraded cannot be secured. "If it ain't broke don't fix it" is a hacker's dream.

When the network goes down users notice and the goals of the enterprise can be severely undermined. Given this, pushing upgrades and making changes to the network, over the network, using centralized tools is extremely risky. Applying upgrades and patches reliably can mean time consuming and expensive site visits, still with the risk of down-time, leading to infrequent change.

The local perspective of Uplogix brings new capabilities to network infrastructure security

Uplogix Configuration and Change Management makes it easy and safe to apply changes and updates to address new threats immediately as they become known.

Key Software and Configuration Change Management Capabilities

- Automatically and remotely push configuration changes and upgrades without the risk that the changes could result in network outages. Out-of-band automated SurgicalRollback™ restores valid configurations instantly and automatically, plus highlights issues when problems occur.
- Automate common, but complex, and therefore error-prone configuration tasks reducing error
- Securely update the access passwords on hundreds of managed devices in a single action
- Decrease the administrative complexity created by heterogeneous network infrastructures by providing a single consistent management interface
- Use configuration differencing to review recent changes to network and communications devices, easily discerning if either problematic or corrective changes have been made
- Ensure access to devices by skilled remote technicians even when the network is down via a completely out-of-band secure architecture

Securing Administrative Console Access

In the heat of the moment when network problems arise, urgency can prevail over security. Break-glass root passwords are issued to empower technicians to console connect to devices and resolve issues, any centralized administrative audit is off-line, and carefully crafted policies intended to protect data are quickly forgotten. This is precisely the circumstance that sets the stage for a serious breach, unintended or not.

Uplogix Local and Out-of-Band Management is console connected to managed devices, simultaneously enhancing technicians' ability to mount an effective response to issues while ensuring that security and audit is not compromised. By storing encrypted device credentials only on the Uplogix Local Manager, secure, policy compliant and audited administrative access can be ensured with complete logging of all transactions for compliance requirements.

Key Secure Administrative Access Capabilities

- Flexible and fine-grained role-based administrative access allows security policies to be precisely reflected and enforced in the form of user access privileges
- Rules prevent unauthorized user access by doing things like automatically closing idle console sessions, or intercepting and stopping noncompliant administrative commands, or even command sequences eliminating security gaps
- Maintenance of AAA (Authentication, Authorization and Accounting), regardless of the state of the network. Under normal circumstances, Uplogix Local Managers integrate with remote authentication mechanisms, such as TACACS and Radius, but if connectivity is lost, the LM can failover to other AAA servers before falling back on cached authentication data to maintain authorized access.
- Use multifactor authentication through integration with RSA SecureID and Secure Computing SafeWord even if the network is down
- Provide policy compliant audit by monitoring, measuring and reporting on all changes made to the managed IT infrastructure to satisfy internal and regulatory security standards. Capture, log and archive every keystroke and output regardless of network status. Allows for flexibility with customizable rules, policies, and reports to meet business- or industry-specific compliance requirements.
- Eliminate potential modem security issues with intelligent out-of-band access. Uplogix appliances can always "dial-out," never allowing in-bound dial-up requests and eliminating the potential for war-dialing or other external unauthorized access attempts.
- Improve overall security by restricting access to specific IP addresses and encrypting passwords stored in the database

