UPLOGIX

UPLOGIX WHITE PAPER

Simplifying Remote Management with IT Automation: A Technical Overview of the Uplogix Secure Remote Management Platform

JULY 2008

WWW.UPLOGIX.COM

Quick Links

Contents

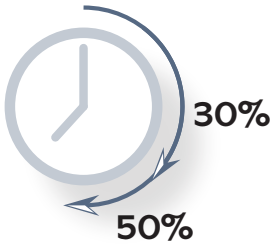
Executive Summary

Managing remote locations is costly, time-consuming and difficult to do with traditional, centralized management tools. This white paper outlines the requirements of managing a highly distributed IT environment and examines how new secure remote management solutions, using sophisticated automation, can uniquely address common challenges faced when managing remote locations as well as complement existing management solutions already in place.

The Challenges of Managing Remote Locations

Does this sound familiar? Users at a branch office halfway around the world are complaining that they can't get on the network, and you're getting paged in the middle of the night to find and fix the problem.

The greatest challenge to providing high service levels at remote locations, whether it's a lights-out data center or a branch office on another continent, is the lack of onsite IT support staff to monitor, troubleshoot and fix network and system-related problems when they occur. According to Nemertes Research, IT staff at large enterprises spend from 30–50% of their time troubleshooting and fixing problems at remote offices. If a problem does occur, a technician usually has to be dispatched on-site to fix it—which can be a costly, time-consuming and sometimes risky proposition. This same scenario repeats itself when extensive maintenance has to be performed on network devices and IT systems at a remote site.



IT staff at large enterprises spend from 30–50% of their time troubleshooting and fixing problems at remote offices.
—Nemertes Research

Managing remote locations presents a number of unique challenges:

- IT departments usually have to do more with less at remote locations where technical resources are often scarce.
- Remote users frequently experience poor application and network performance. However, IT staff is often unable to accurately measure end-user performance and cost-effectively resolve issues because they lack the tools that can autonomously find and fix problems at remote sites.
- During network outages and disruptions the centralized IT staff faces reduced visibility, control and security at remote sites because the monitoring and management tools they rely on are themselves dependent on the network being up and functional. As a result, managing remote locations has become increasingly complex. A simple task such as reconfiguring a router can turn into a major headache and expense if it requires deploying support personnel to hard-to-reach locations on the network.

Unfortunately, **a critical solutions gap exists between current technologies and the management needs of today's highly distributed enterprises**. Neither software-based monitoring nor remote access tools are able to reliably diagnose and fix problems, or automate ongoing operations, which forces IT staff to spend more time and expense doing routine administration and recovery tasks at remote locations.

The Need for Secure Remote Management

To effectively, efficiently and securely manage remote locations, a new approach and architecture is required. Solutions need to be deployed where they are needed most—at the edge of your network—becoming an integrated component of the IT infrastructure that they are designed to manage.

Uplogix has introduced an innovative approach to secure remote management (SRM) that not only fulfills the remote management checklist (See Appendix), but also overcomes the shortcomings of existing management tools to address the long-standing costs and challenges of managing a geographically distributed IT infrastructure. In short, Uplogix decreases the headaches and hassles of managing remote locations by eliminating routine, repetitive tasks.

Instead of having to dispatch an army of technicians in the field to sit in front of routers, switches, servers and firewalls, watch them for problems, and take action if something goes wrong or needs changing, Uplogix provides an intelligent remote management solution that essentially performs the same functions, but faster, error-free and at a fraction of the cost.

Uplogix' unique architecture uses an always-available, secure, direct connection to the remote devices it manages to provide integrated functionality that previously required multiple disparate solutions to deliver, including:

- **Access** | By co-locating and directly connecting to network devices, servers and communications equipment, Uplogix delivers uninterrupted connectivity, access, monitoring and control over remote devices—regardless of the state of the network.
- **Control** | By having the Uplogix appliance on-site at a remote location, it can perform a majority of the routine administration, maintenance and recovery tasks that an on-site technician would do today. The Uplogix appliance minimizes costly tech support calls and on-site visits to remote locations by diagnosing and fixing problems locally as well as automating routine maintenance tasks.
- **Enforcement** | Uplogix ensures that internal security and management policies are always enforced, even during a network outage. IT staff can control who has access to devices on the network, what they are doing while accessing the devices, and be able to accurately report on all user interactions in order to satisfy security and compliance requirements.

The Uplogix Secure Remote Management Platform

Uplogix solutions deliver the local access and control of a console server, the in-depth monitoring and diagnostics of systems management software, and the intelligence on an on-site technician into a single, integrated platform. The result is secure remote management required to control today's distributed infrastructures.

The Uplogix Secure Remote Management (SRM) Platform Components

- **Uplogix RMOS** | Uplogix' Remote Management Operating System which powers Uplogix SRM appliances to remotely automate hundreds of routine system maintenance, configuration, fault diagnosis and recovery operations. As part of the advanced version, service level verification module will monitor and manage the service levels of business critical applications. RMOS is available in both Standard and Advanced versions.
- **Uplogix SRM Appliances** | Secure remote management appliances, available in compact, affordable and integrated to enterprise scalable models, that are deployed at remote locations, branch offices and distributed datacenters to maintain, configure, and autonomously fix routine IT infrastructure issues
- **Uplogix Control Center** | A web-based, centralized point of control for all Uplogix SRM appliances and managed devices throughout your environment

A Look at the Uplogix SRM Platform

The Intelligence Behind SRM

RMOS | The Remote Management Operating System powers SRM appliances, automating hundreds of routine system maintenance, configuration, diagnosis and recovery operations

Enterprise Scalability and Performance

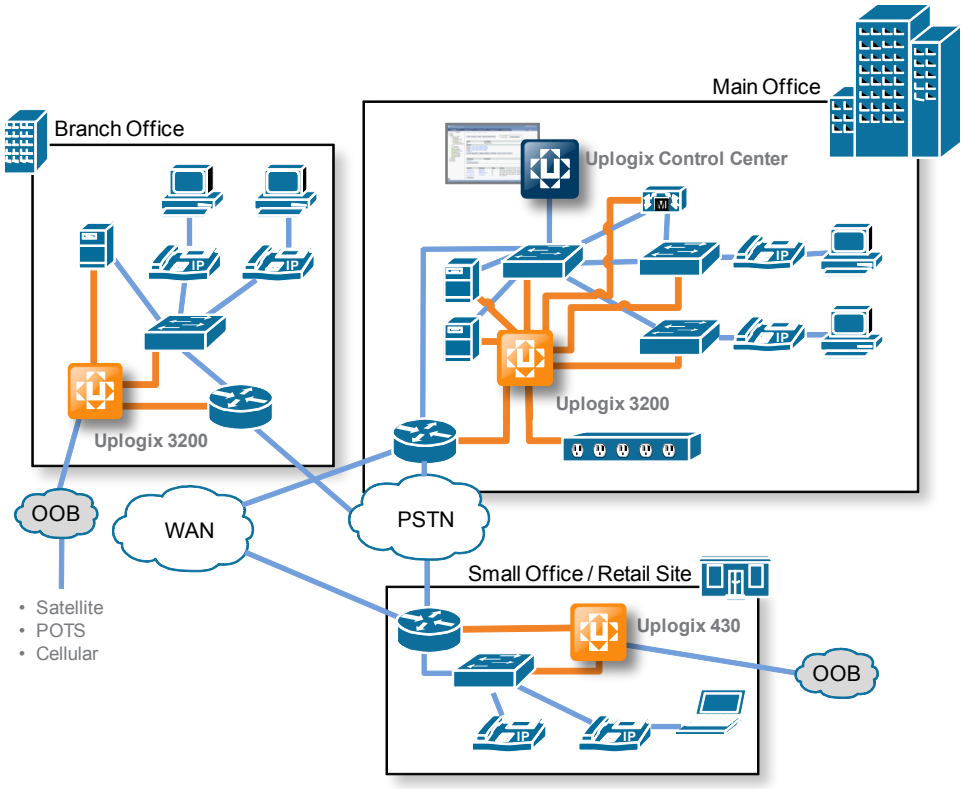
Uplogix 3200 | Our flagship SRM appliance, available in 4-, 8-, 16-, 24-, or 32-port models, delivers advanced remote management capabilities for data centers, branch offices and remote locations on a robust and flexible platform

Compact and Affordable

Uplogix 430 | Comprehensive functionality in a fixed 4-port SRM appliance designed for enterprises needing to monitor, manage and control four or fewer devices and their power supply at any distributed location

Managing SRM Across the Enterprise

Uplogix Control Center | The web-based, centralized point of control for all Uplogix SRM appliances and managed devices throughout your environment



Together, the components of the Uplogix SRM Platform deliver a comprehensive solution for effectively managing highly distributed IT environments that reduces management costs, complexity and risks while improving IT service levels in the process.

Uplogix RMOS

The Remote Management Operating System (RMOS) is the Uplogix software platform that powers our line of Uplogix secure remote management appliances. Utilizing the remote control capabilities of Uplogix appliances running RMOS, enterprises are able to dramatically reduce the cost, complexity and risk of managing their distributed IT infrastructures, and improve service levels in the process. RMOS increases network and system availability by directing Uplogix appliances to remotely automate hundreds of routine system maintenance, configuration, fault diagnosis and recovery operations. RMOS is available in both Standard and Advanced versions.

Uplogix SRM appliances running the Standard version of RMOS provide all of the remote access, control and enforcement features required to cost effectively and efficiently manage a highly distributed IT infrastructure.

The Advanced version of RMOS has all of the same robust, remote management capabilities as the Standard version of RMOS, but also includes advanced device

Key Features for Remote Management

ACCESS

- **Secure Access & Connectivity** | Maintains management connectivity with distributed locations, even when the network is down or degraded via a variety of backup communication options including dial-up modem, cellular network, or satellite communications
- **Local, In-depth Monitoring** | Continuously monitors and proactively diagnoses problems with network devices and servers, using data frequently collected on over 100 variables, with no impact to network performance

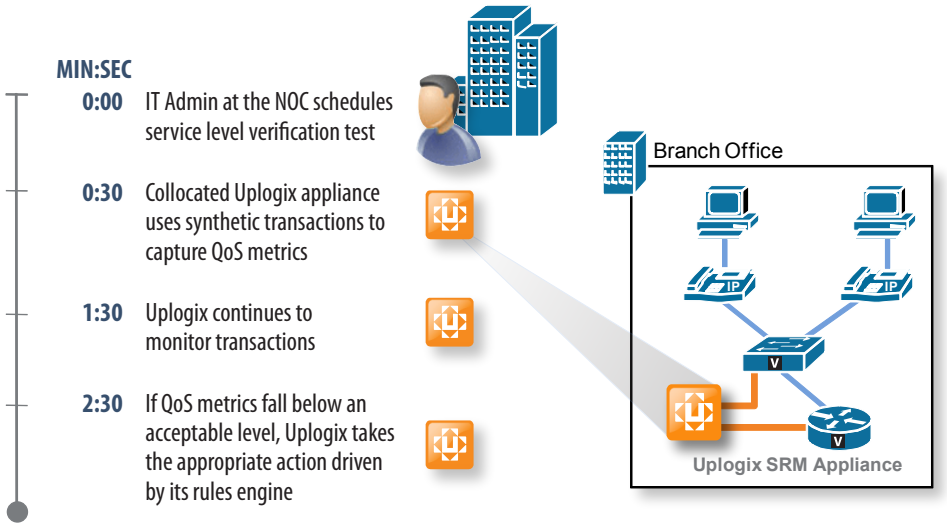
CONTROL

- **Proactive Maintenance** | Allows you to selectively choose which ongoing maintenance activities to automate including OS upgrades and patches, configuration changes, password resets, etc
- **Configuration Management & Recovery** | Enforces consistent operations by ensuring that change and configuration management tasks are done the right way, every time, minimizing human error and protecting availability
- **Automated Problem Resolution** | Lowers the cost and complexity of remote management by diagnosing and automatically fixing common problems within minutes, often before traditional monitoring tools even know there is a problem
- **Remote Power Management** | Allows you to securely access and control power to non-responsive remote devices, as well as execute more complex recovery actions requiring a power cycle such as quickly recovering from a failed configuration change to avoid an outage

ENFORCEMENT

- **IT Policy Enforcement** | Ensures that only the right users have the right level of access to devices and systems by providing very granular and customizable access, authorization and role-based permission controls, both in- and out-of-band
- **Compliance Reporting** | Captures, logs and reports all changes made by users and the results of those changes. Inspects logs in real-time for problems and can proactively take rules-based automated recovery actions based on log patterns

and application management features such as Service Level Verification (SLV) which monitors, measures and manages the performance of critical network services and applications from an end-user's perspective, including TCP/IP communications, web-based transactions and voice over IP telephony. Additionally, Advanced RMOS includes robust server management capabilities such as Service Processor Automation using IPMI and KVM over Service Processor. By upgrading Uplogix SRM appliances to Advanced RMOS, you can better monitor and manage the service levels of business critical applications, and extend Uplogix' industry-leading secure remote management capabilities to your distributed server infrastructure.

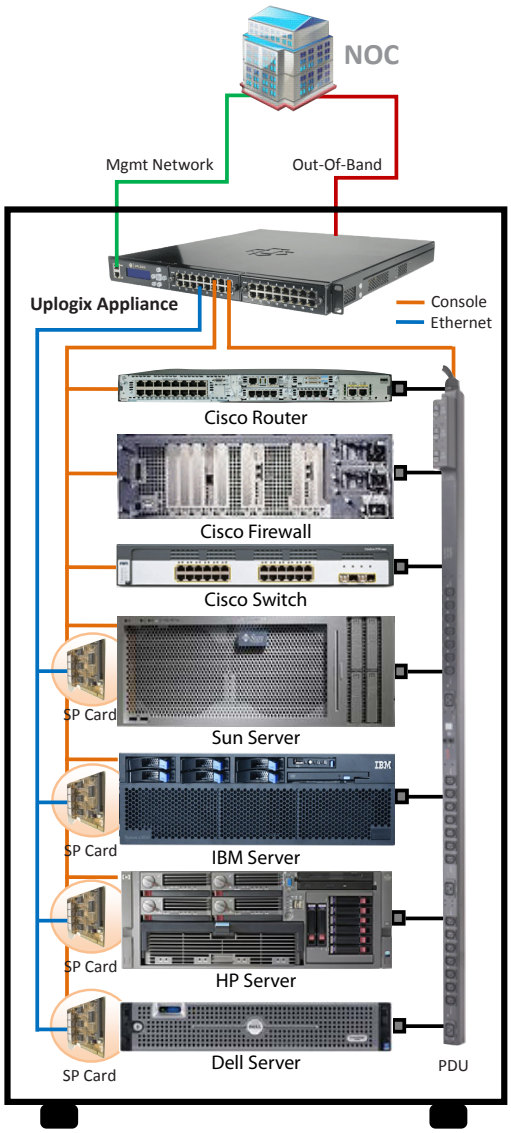


In a Service Level Verification (SLV) test of IP telephony performance at a remote location, the Uplogix appliance initiates a VoIP call from remote location and captures over 40 specific QoS metrics that reflect the health of the telephony system. Using standard Harvard sentences to gauge IPT performance, Uplogix monitors important metrics such as jitter, latency, packet loss, MOS scores, and R values. Using information received from the verification test, the SRM appliance reports service level data to the Uplogix Control Center and can take appropriate recovery actions.

Uplogix SRM Appliances

Uplogix secure remote management (SRM) appliances are the first fully-integrated remote management appliances that deliver a complete solution for cost-effectively managing a distributed IT infrastructure. Uplogix appliances are deployed at remote locations, branch offices and distributed datacenters to maintain and configure IT infrastructure, as well as autonomously fix routine issues.

Uplogix SRM appliances deliver remote management and control by interfacing directly through the console port of the devices they manage. This connection



The Uplogix SRM appliance connects to server and other network infrastructure via the console port, as well as the option to connect via Ethernet to servers over service processor.

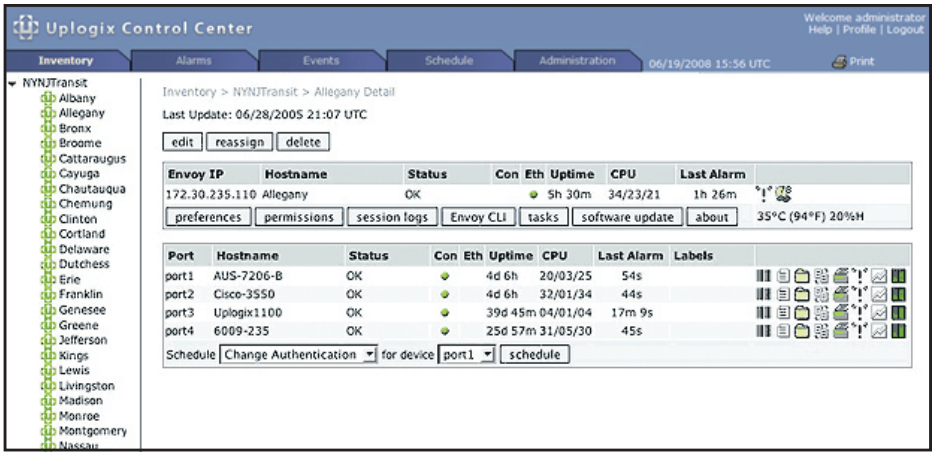
enables secure, always-on, round-the-clock management for your remote IT infrastructure. The Uplogix appliance can automate as much as 70% of routine remote IT support functions such as monitoring, configuration, fault and service level management, and autonomously address the majority of issues that cause network-related outages including configuration errors, wedged or hung devices, and telecom faults. Problems that today might require IT staff to resolve on-site are detected by the Uplogix SRM appliance in seconds, and fixed in minutes, avoiding costly downtime.

Uplogix Control Center

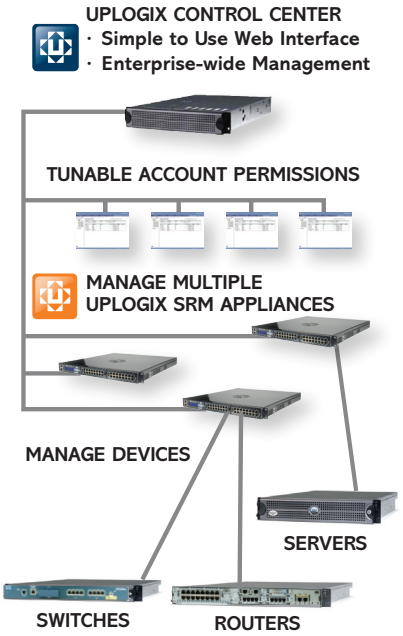
The Uplogix Control Center enables secure remote management through a centralized point of control for all Uplogix appliances and managed devices deployed throughout your distributed IT environment. With its web-based graphical user interface (GUI), Control Center puts IT administrators in control of real-time data to easily manage, configure, and control all network devices and servers connected to Uplogix appliances.

Deployed in the network operations center (NOC), 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 Uplogix SRM appliances, Control Center also serves as the gateway between the Uplogix appliances in the network and existing IT management systems. Control Center provides a simple, web-based point-and-click interface for executing enterprise-wide management tasks, such as distributing patches, resetting passwords or performing configuration changes. And it serves as a central reporting point providing both robust and customiz-

able reporting of event, alarm, and device statistics, as well as network service level measurements across the enterprise. Control Center scales to support even the most complex distributed networks and integrates easily with existing management systems.



Uplogix Control Center dashboard view of all SRM appliances and devices under management



Deployed at the NOC, the Uplogix Control Center provides a centralized point of control for all Uplogix appliances and managed devices.

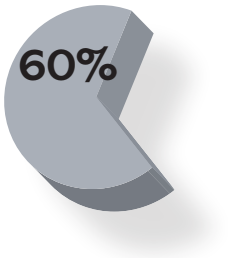
Interoperability with Existing Management Systems

The Uplogix SRM platform has been designed to work alongside and provide additional value to your existing management systems.

Network and System Management (NSM)

Centralized, SNMP-based NSM solutions provide rich diagnostic, fault management and reporting information. However, the majority of these solutions are network-dependent, so when the primary network connection is down or disrupted, they lose connectivity and visibility to devices in the field.

Uplogix solutions complement NSM solutions by providing persistent connectivity and control to remote devices. Since Uplogix appliances are directly connected to the devices being managed, they can continue to work even when the primary network connection is unavailable, performing system monitoring, maintenance, and recovery tasks locally, securely and efficiently. Uplogix solutions also seamlessly integrate with NSM solutions. System alarms, events and device performance data can be forwarded to NMS systems from the Uplogix Control Center via SNMP messages that appear as if they came from the managed device itself. Additionally, syslog messages can be sent in real-time to an NMS system or Syslog server for consolidation, auditing and analysis purposes. This persistent connectivity and in-depth monitoring capability can be especially useful during outages when your NSM solution may fail to capture data.



60% of network downtime is caused by human error during device configuration
—Enterprise Management Associates

Uplogix SRM appliances use Monitors to gather data on various aspects of network functionality as well as operation of the appliance itself. The appliance has a number of fixed based monitors for Chassis (temperature, power, SMART), RMOS (bad password attempts, log in/log out, user account activities, security, etc.) and Device Specific (ROMMON, password recovery, terminal access, etc.).

Rules give Monitors the added ability to assess the collected data and take appropriate action automatically. The monitor's syntax specifies the order in which the rules are executed and where they apply. In other words, the Monitor will collect the data every 30 seconds; compare the collected data against the Rules and take the appropriate action as defined in the rule.

Typically a rule consists of at least one condition ("if") and at least one action ("then"). Conditions provide the input to rules; each condition reads and evaluates a variable.

Actions are rule outputs. An action causes a change of some kind; for example, it may write a user-defined variable, trigger an automatic function, or generate an event to be logged. Conditions and actions may use predefined condition variables, which do not require initialization; or user-defined state variables, which must be created and initialized in an action statement.

Every 30 seconds, the Uplogix appliance will send heartbeat with all the currently triggered alarms to the Uplogix Control Center. System alarms, events and device performance data can be forwarded to NMS systems from the Uplogix Control Center via SNMP messages that appear as if they came from the managed device itself. Additionally, syslog messages can be sent in real time to an NMS system or Syslog server for consolidation, auditing and analysis purposes.

Here is how the Uplogix Control Center sends SNMP alarms/traps to the NMS tools:

1. Uplogix Control Center receives heartbeat from all Uplogix SRM appliances with all triggered alarms
2. The Uplogix Control Center trap receiver will send a SNMP v1.0 trap to the NMS with the source id as the device IP, management IP or Uplogix appliance IP
3. Within the trap, the Uplogix Control Center will provide the OID of the default constant (Uplogix MIB) or the device specific constant (e.g. Cisco MIB). If the Uplogix Control Center uses the device specific constant and IP address of the device, the NMS tool will think it is receiving traps/alerts from the device itself.

Configuration Management

Configuration management solutions enable you to track and control changes made in the IT environment as well as understand the relationship between IT components. Uplogix complements existing configuration management (CM) systems by performing four very important functions.

First, due to its direct connection, Uplogix can capture all changes made to managed devices, and send that data to a central CM system. By comparison, network-dependent configuration management systems may miss capturing system changes made during a network outage or disruption.

Second, Uplogix provides a built-in safety net feature called SurgicalRollback™ which can quickly recover and minimize the impact of a failed configuration change (See Configuration Recovery scenario below) by rolling a device back to its last known good state to avoid outages. Since Uplogix logs and reports all changes made to managed systems and the impacts of those changes, this information can be sent to an existing configuration management system via SNMP-based messages for enterprise-wide tracking and control.

Third, Uplogix can complement an existing CM solution by providing a trusted and consistent method to locally provision devices. Enterprise-wide provisioning can be scheduled centrally within the Uplogix Control Center and executed locally by Uplogix SRM appliances (See Centralized Push scenario), significantly reducing the time, effort and risk of provisioning or re-provisioning devices.

FInally, since Uplogix is constantly capturing, recording and reporting both change data and device performance data, it provides you with a more complete picture of the state of your IT infrastructure.

Security and Compliance Management

Uplogix solutions complement existing security and compliance management solutions such as identity access management (IAM) by serving as a constant, secure gateway for accessing and managing remote devices, as well as reporting on all user and device activity. By using the Uplogix appliance as your gateway to manage remote devices, your IT policies will always be enforced, whether working in-band or out-of-band. All user authentication can be directed to an existing RADIUS or TACACS server, in order to keep user passwords synchronized throughout your enterprise while authorization is maintained on the Uplogix appliance. User sessions can be controlled to avoid unauthorized access to systems, and authorization controls can be centrally defined and managed to enforce who has access to which systems.

In addition, Uplogix captures all changes made to systems and the results of those changes all the time to enable complete compliance reporting. Uplogix appliances record every user's keystrokes and output, unlike accounting tools (i.e. TACACS) or CM solutions that can fail to capture changes during a network outage. Complete log data including session, syslog and console data and can be forwarded to compliance management systems for analysis and customized compliance reporting. Uplogix also provides a unique, real-time log inspection capability. Logs are inspected in real-time for problems, and automated corrective actions can be taken based on

identified log patterns—a powerful, proactive feature that can save you a lot of time and effort over manually poring over logs after a problem has occurred.

Remote Power Management

The simple step of power cycling a failing or non-responsive device can often resolve a problem. Uplogix provides robust power management features that enable you to monitor and control power remotely. Uplogix appliances can be set to automatically manage power, or allow an authorized network administrator to manually control individual power outlets, create logical groupings, monitor current, and control power-up sequencing. This remote power management feature takes the headache out of power cycling devices in remote locations, eliminating truck rolls and saving you valuable time. Uplogix integrates with and manages power controllers from several leading vendors including Server Technology, APC and BayTech.

Business Service Management

Business Service Management (BSM) combines best practice IT processes (such as support for ITIL), automated technology management, and a shared view of how IT resources support the business, resulting in an effective approach for managing IT from the perspective of the business. Uplogix complements BSM initiatives and solutions by automating routine IT management operations so you can spend more time and effort proving the value of IT to the business.

Uplogix also improves the business value of IT services being delivered by providing unique service level monitoring and management capabilities. Many service level management (SLM) solutions monitor network and application service levels from a centralized perspective over the network. This approach does not give you a true perspective of what end users are experiencing and is dependent on the network's availability in order to function. Uplogix overcomes both of these limitations by measuring service levels locally and directly. And, the service level metrics gathered are fed into the Uplogix appliance's rules-based engine so that corrective actions can be automatically taken to proactively manage and improve service levels. This service level data as well as information about actions taken can be forwarded to an existing BSM solution for enterprise-level management.

Common Remote Management Challenges Resolved by Uplogix

Uplogix solutions move beyond the limitations of traditional monitoring and remote access tools to deliver the level of active, secure remote management required to manage a distributed IT infrastructures. Following are common challenges faced when managing remote locations that Uplogix can uniquely resolve.

Lost Connectivity to a Remote Device

One of the biggest challenges to managing remote locations is not always being able to securely connect to and access remote devices in order to perform maintenance tasks or troubleshoot and fix problems. Traditional, remote access solutions typically use network-based protocols, such as SNMP or Telnet, which can render them both unreliable in the case of a network outage and insecure due to a lack of encryption and authorization controls. Uplogix solutions don't rely on the network to manage the network. The Uplogix SRM appliance co-locates and directly connects to network devices and servers to deliver persistent connectivity, as well as localized management services – regardless of the state of the network or device. This means that you always have secure access to the distributed devices you need to manage.

When the network is functioning properly, an Uplogix appliance uses an Ethernet-based connection to connect to the centralized management server, Control Center. But when it's not, it will dial-out and immediately reestablish connectivity to Control Center via a secure out-of-band path using a variety of backup communication options including dial-up modem, cellular network, or satellite communications. This enables secure, always-on access and connectivity to the remote devices you need to manage.

Solution Timeline: Primary Path Failure

Situation

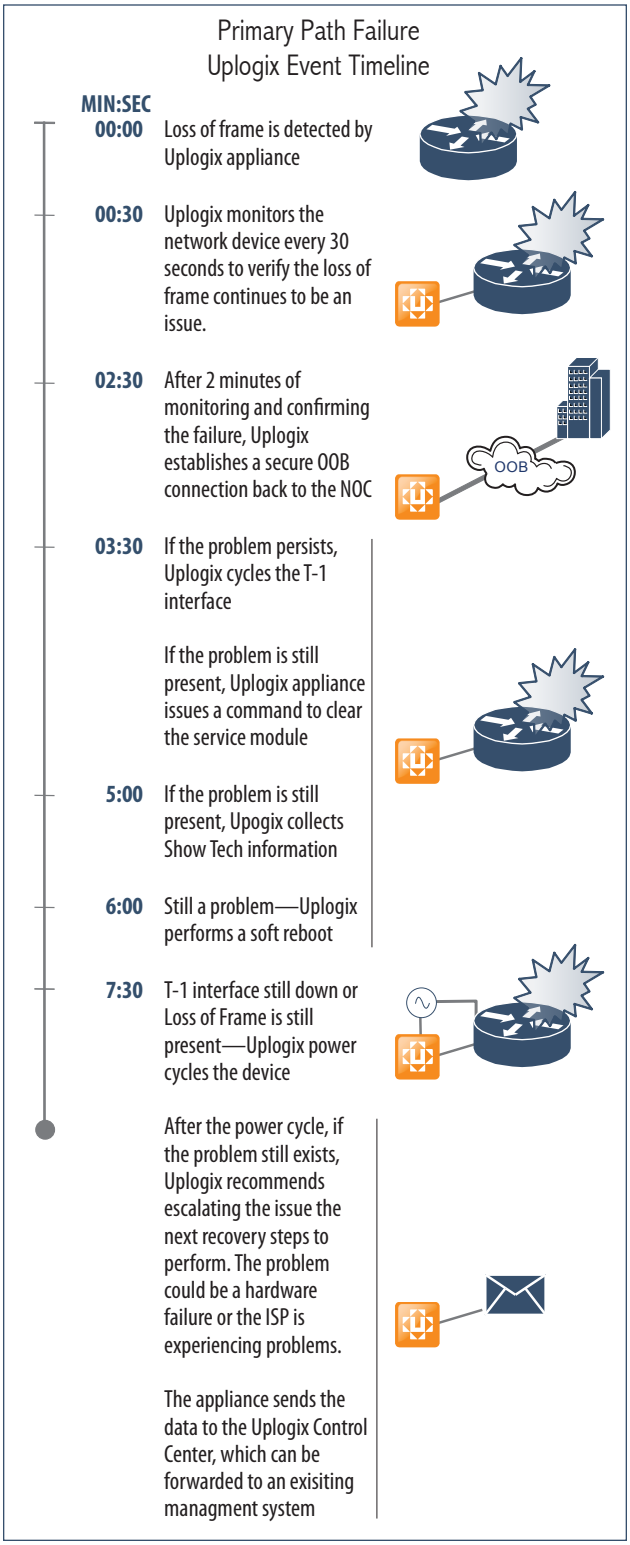
Whether located at a branch office or in a wiring closet at an enterprise headquarters, the need for remote access to network devices that are unresponsive or cannot be reached over the primary network infrastructure is critical. Regardless of where the business impact is greater, in either case a network device failure can disrupt operations, hamper revenue and decrease productivity.

Current Methods

The current solution is to wait for a central network monitoring tool to alert IT staff or the problem is discovered when the remote office employees complain of lost access to company resources. The loss of connectivity and visibility further hinders IT's ability to troubleshoot. Then there is also the problem of how to access the network device remotely and securely. A network engineer or an outsourced third party IT professional would be dispatched to try to diagnose and resolve the problem - costing time and money. Additionally, security policies are often lax, such as giving a third party contractor root-level access, in exchange for restoring service quickly.

Uplogix Solution-Secure Connectivity & Remote Power Management

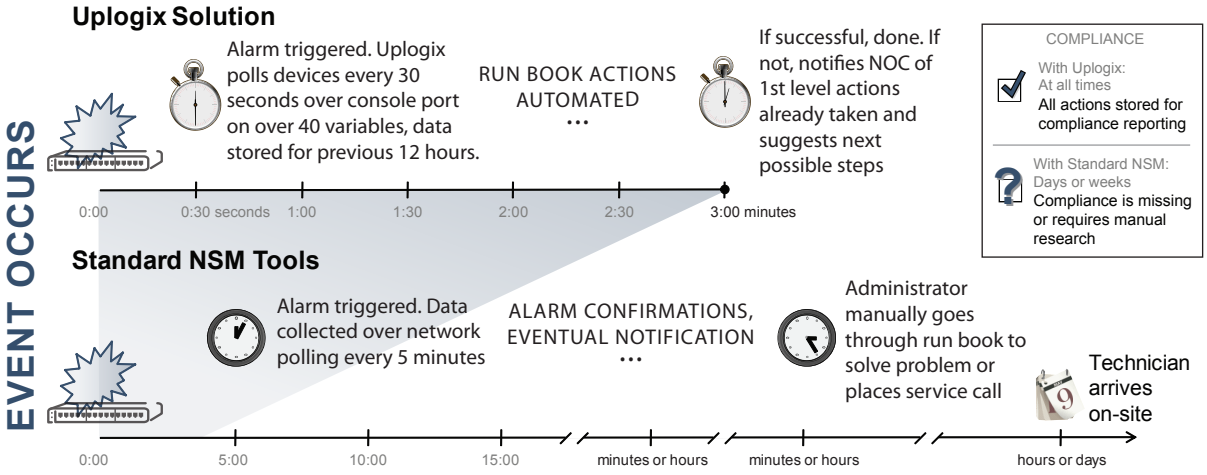
In the same time it takes traditional network monitoring tools to just discover a problem at a remote site, Uplogix can find it, fix it, and alert the NOC it has been resolved or needs escalation—eliminating costly site visits and dramatically reducing your Mean-Time-To-Resolution (MTTR).



False or Missed Alarms

IT administrators need to not only need to be able to constantly and securely access remote devices, but also need to be able to effectively monitor the distributed infrastructure in order to ensure its health and performance. Traditionally administrators have relied on network monitoring tools to provide this visibility. However, SNMP-based monitoring tools are limited by how much data they can collect and how often it can be collected in order to minimize the performance impact of these queries on the overall network. Additionally, these tools are network-dependent, so if the primary network connection is unavailable, IT administrators are literally "left in the dark." The end result is that critical alarms may be missed because the solution failed to capture performance data during an outage, or erroneous alarms may be presented because the monitoring system failed to gather the amount of data required to correctly diagnose a problem.

Uplogix solutions can gather much more granular diagnostic data and more frequently than SNMP-based systems without affecting the performance of the devices or the network. An Uplogix appliance leverages its serial connection to managed network devices and servers to collect data, either in-band or out-of-band, on network performance variables, every 5 to 30 seconds. More importantly this rich diagnostic data feeds Uplogix' rules-based policy engine which can determine if a parameter is in or out of specification. The Uplogix appliance can then either automatically resolve the incident based on pre-approved guidelines, or communicate the problem and recommended recovery steps back to centralized IT staff for resolution.



Uplogix provides local, in-depth monitoring, to find and fix problems faster than traditional management tools

Burdensome System Maintenance

The majority of your time is likely spent maintaining and making changes to the network, and the underlying IT infrastructure. Routine tasks like OS upgrades, patches, password resets, and configuration changes are ripe for automation, but remain largely manual, time-consuming and costly. Necessary changes like OS upgrades are often put off because of the fear and certainty that some percentage of changes will fail, leading to costly system downtime while someone tries to figure out which change failed, why, and how to restore service.

Uplogix provides proactive maintenance capabilities that you can control to speed changes, dramatically reduce the time and effort required, and minimize the risks of manual errors. The Uplogix SRM appliance allows customers to selectively choose which maintenance activities to automate and to what degree—and provides a built-in safety net to quickly recover from failed changes.

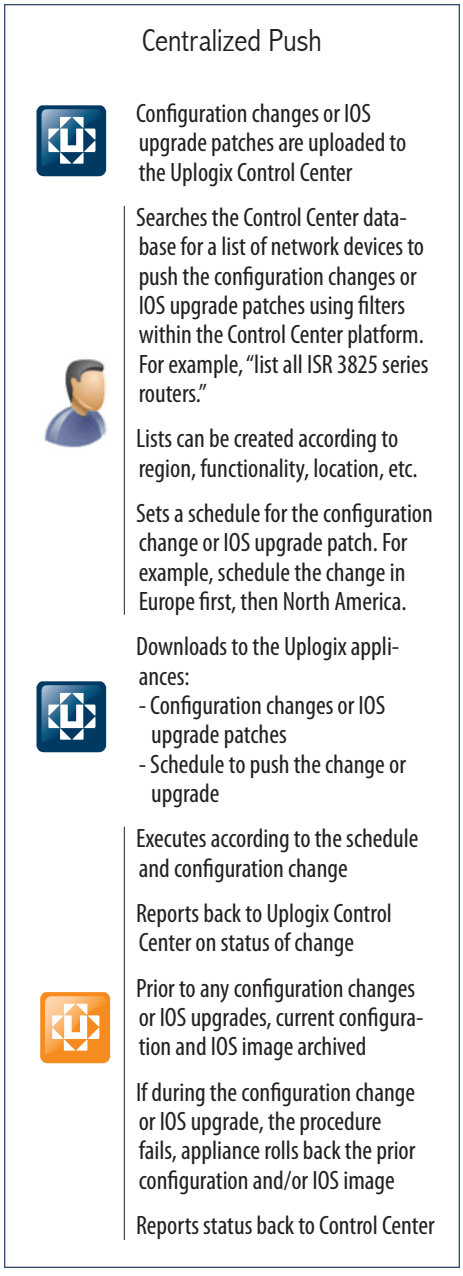
Solution Timeline: Mass Configuration / Password / OS Change

Situation

Situations arise where there is a requirement for a mass push to multiple devices. This can be a labor-intensive operation absorbing hours of manual cycles, and there are multiple opportunities for error or introduction of inconsistencies between devices.

Current Methods

In-band network management systems can perform mass changes, but risk increases by relying on the network's availability in order to execute the mass change. The expensive alternative is sending a technician to connect and update each device directly.



Uplogix Solution—Centralized Configuration Management

The Uplogix Control Center enables secure remote management through a centralized point of control for all Uplogix appliances and managed devices deployed throughout a distributed IT environment. With its web-based graphical user interface, Control Center puts IT administrators in control of real-time data to easily manage, configure, and control all network devices and servers connected to Uplogix appliances.

Control Center combines "one-click" administration of rules, policies, and changes across the entire network, with robust and flexible reporting of device statistics, alarms/events, user interactions and network service levels.

SurgicalRollback™: The Answer to a "Fat Fingered" Config Change

Situation

System or network admin makes a change that has caused an outage. Examples include typos, wrong patches, etc. that cause an errant configuration change in the Access Control List (ACL) for a network device. This causes the network to become inaccessible for all users in an office. Another example would be when an OS upgrade patch does not execute due to a corrupted file, flash sector or not enough RAM on the device. Situations like these create organizational downtime. In addition, the loss of connectivity and visibility hinders the ability for IT administrators to accurately troubleshoot the problem, prolonging downtime.

Current Methods

There isn't much you can do for this other than dispatch a network engineer to the site to access the device directly or contract with a third party technician to do so. The final option would be to locate, recruit and coach an on-site employee to perform the necessary recovery steps, which is both time-consuming and risky.

Uplogix Solution—Configuration Recovery

If a configuration change fails, Uplogix can immediately roll the device back to the last known good configuration using its unique SurgicalRollback™ feature—an automated safety net to recover from configuration errors without requiring an on-site visit.

How SurgicalRollback Works

- Connects and authenticates to Uplogix via secure (SSHv2) connection
- Connects to device via Uplogix
- Initiates a terminal connection to device

- During the terminal initialization to the connected device, a current running configuration is cached by the appliance
- Makes changes to the connected Cisco device

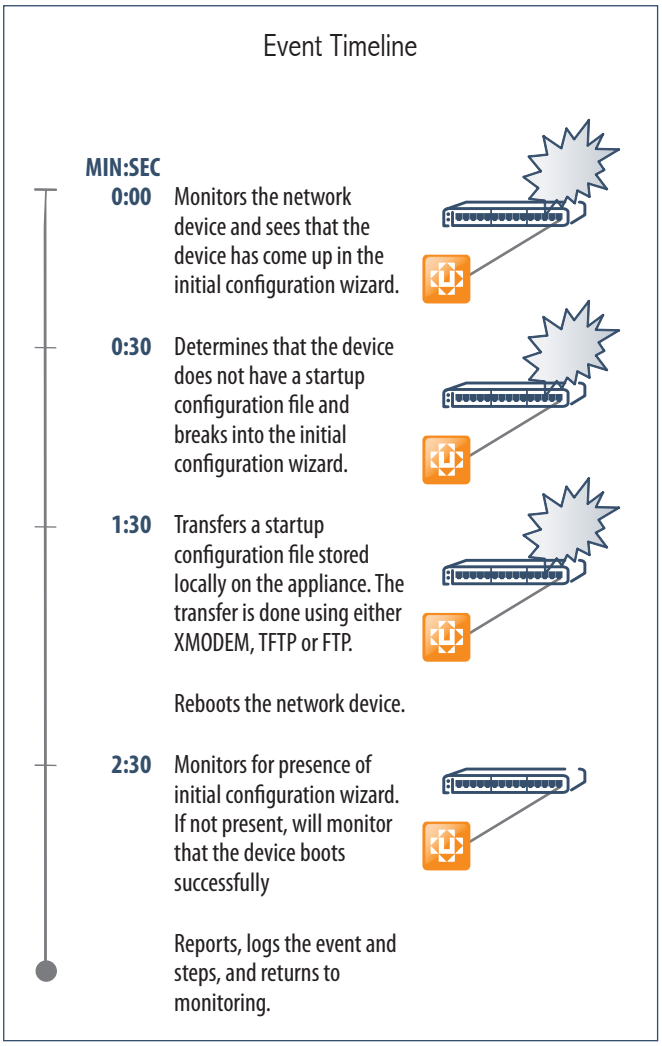
- Executes OS commands for the device
- If during the session the user logs out of the device or loses connection due to a configuration error, a running configuration is pulled again

- Generates a list of changes made during the session and prompts the user with a confirmation to accept, reject or delay the changes made. If the user session times out due to configuration error or general inactivity after a configurable amount of time, the appliance backs out all uncommitted changes made during that session.
- The default action is to rollback all uncommitted changes
- Starts countdown to SurgicalRollback
- If no response, Uplogix will rollback only changes made to the device
- Logs event and changes and sends data to Control Center for reporting purposes

Hung or Non-Responsive Device

Finding and fixing IT problems at remote sites remains a time-consuming, labor-intensive and expensive process. Existing management tools are good at monitoring devices and identifying problems, but lack the intelligence and local control to actively fix problems when they occur, forcing IT staff to go on-site to perform routine fault diagnosis and recovery tasks.

Uplogix lowers the cost and complexity of remote management by proactively finding and automatically fixing common problems throughout your infrastructure. In fact, Uplogix can address and resolve the majority of the issues that commonly impact distributed networks such as configuration errors, nonresponsive devices and telecom hardware failures. Using device manufacturers' best practices, Uplogix has automated hundreds of management procedures that enable the appliances to take action when certain conditions occur. For example, an Uplogix appliance can automatically recover a device from ROMmon state or power cycle a frozen console. Uplogix' ability to automatically fix problems locally, quickly and consistently reduces downtime incidents and lowers your support burden by eliminating the need for manual intervention.



Solution Timeline: Remote Device Loses Startup Configuration

Situation

There are times when a brand new router is sent to a remote office, a network device loses the startup configuration, or an IT admin accidently erases the startup configuration file. The result is the network device will boot up in its initial configuration wizard waiting for a human to input the parameters. This causes downtime in an organization resulting in inability to complete mission critical work and possibly a mass business disruption caused by a bad rollout that affects multiple sites.

Current Methods

The best you can do is dispatch a technician, or call in a third party technician to restore the device. Both options can be costly in terms of time, money and risk.

Uplogix Solution - Automated Problem Resolution

Using device manufacturers' best practices, Uplogix has hundreds of built-in management procedures that enable the appliances to take action when certain conditions occur.

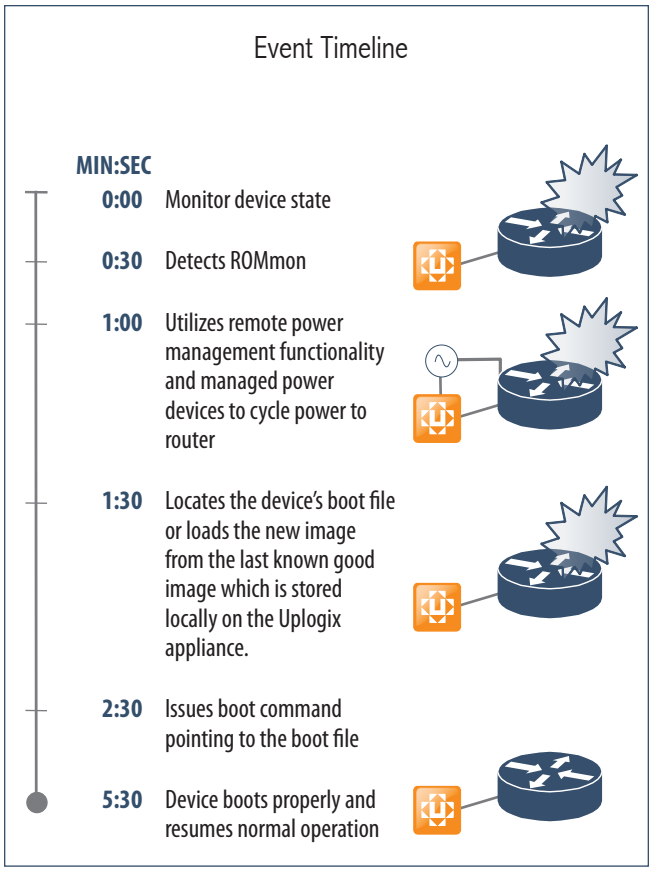
Cycling Power to a Remote Device

Complex IT infrastructure devices such as servers, networking and telecom equipment are prone to entering states that are not recoverable through normal remote administrative commands even at the BIOS level. This often leads to the inevitable step of a hard reboot, which requires an administrator to physically power cycle the device. This is not only an inconvenience, especially if it is remotely located or if it happens in the middle of the night, but it can lengthen downtime, disrupt business continuity and increase support costs.

Not only will you be able to securely access and control power to non-responsive remote devices, but by using Uplogix' best-in-class automation engine, more complex recovery actions can be executed such as recovering from a failed configuration change. For example, an Uplogix appliance can power cycle a remote server, break into the reboot sequence at just the precise moment, and restore the last known good configuration file for the device—all within seconds and without ever having to dispatch a support technician on-site.

Using the Uplogix remote power management feature will allow you to monitor, manage and control power to nearly every device in your distributed IT infrastructure—regardless of network availability.

Solution Timeline: Router Enters ROMmon State



Situation

A hung or unresponsive router can enter ROMmon mode for various reasons such as a boot failure, settings in the virtual configuration register that force the router to stop in ROMmon mode during the boot, or a break sequence sent to the console. Whatever the cause, the device isn't available for business use, which likely means that the site is down and productivity comes to a halt.

Current Methods

Send a trained technician, call in a third party service provider, or try to talk on-site personnel through the repair routine, which are all costly and time-consuming options.

Uplogix Solution—Remote Power Management

The intelligence built into Uplogix appliances makes it possible to automatically detect, diagnose and sequence events to restart and recover a device to a working state with the last known good configuration.

Internal Security Breach

According to the FBI, two of the top four types of information security attacks are related to insider abuse or unauthorized access to systems. Uplogix helps you eliminate internal security threats before they impact the network, overcoming the security risks of traditional management protocols used today, such as SNMP and Telnet, and setting a new standard for enforcing IT policies. Uplogix appliances operate on a secure management platform that supports the industry's most stringent AAA requirements, ensuring that security and management policies are always enforced, even during a network outage. Additionally, Uplogix utilizes the strongest security, encryption and authentication standards on the market such as SSHv2 to access and communicate with managed devices.

Uplogix solutions ensure that only the right users have the right access to devices and systems by providing very granular and customizable authorization controls as well as role-based permissions. Uplogix appliances can even be setup to accommodate additional security precautions, such as restricting access to specific IP addresses and encrypting passwords stored in the database, or automate management functions related to security enforcement, like updating the access passwords on hundreds of managed devices at once.

Unauthorized Device Access

Situation

It's getting harder to know and control who has access to internal systems. Unauthorized access to internal systems, whether malicious or not, can result in significant financial losses for a company, including stiff penalties for non-compliance by regulatory bodies.

Current Methods

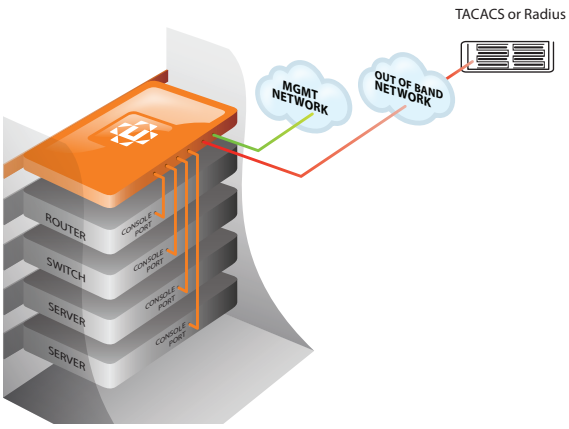
Software-based tools often cannot enforce security policies during a network outage, plus they often require the opening of additional ports to both receive and send data, which increases exposure. Remote access tools such as console servers are usually limited to only enforcing port-level permissions on devices being accessed, which is often not granular enough.

Uplogix Solution—IT Policy Enforcement

Uplogix maintains constant, secure management access and control over connected devices, even when the network is down.

How It Works

- IT admins can provide users different levels of access privileges at device, port or even command level
- Users can be grouped by role, function, department, geography, etc. and monitored centrally via web-based portal (Control Center)



Uplogix maintains and enforces AAA, regardless of network state

- Uplogix appliance cleans up and closes down a session before other users are permitted access, or can lock down the port if unable to close the session, eliminating the threat of unauthorized users "ghosting" or "piggybacking" idle sessions left open. Can be configured to timeout sessions automatically according to internal security policies
- Uplogix supports the same AAA settings irrespective of the state of network. Uplogix appliances can be configured to fail-over to SSH certificates, RADIUS servers, and finally a local user account when the connection to the primary authentication server is broken.

Incomplete Compliance Reporting

In today's world, you need complete reporting data in order to satisfy both internal and external auditors. However, during network disruptions and outages, reporting data on who has accessed devices and what was done to those devices often goes uncaptured and unrecorded.

Leveraging its dedicated serial connection with managed devices and servers, an Uplogix appliance logs all changes made by users and the results of these changes. This information is saved locally and then transmitted to the Uplogix Control Center for analysis and long-term storage. Logging, recording and reporting are unaffected by the state of the network—Uplogix appliances continue to satisfy compliance reporting requirements even during downtime. Uplogix can also inspect the log files in real-time for problems and can proactively take automated recovery actions based on log patterns—a unique feature that can put an end to the laborious, and time-consuming process of manually sifting through log data trying to find the proverbial "needle in the haystack."

Incomplete or Insufficient Audit Logs

Situation

Being able to always answer, "Who did what? When? What was the impact?" is a must to meet security and compliance reporting requirements.

Current Methods

Network-dependent tools only log changes made to systems when the network is active and accessible, meaning logging is interrupted and incomplete during an outage. Additionally, most are limited to keystroke logging which captures a user's input but not the output from the actions taken. SNMP-based tools lack adequate storage to capture complete log data, which can result in insufficient data for compliance reporting.

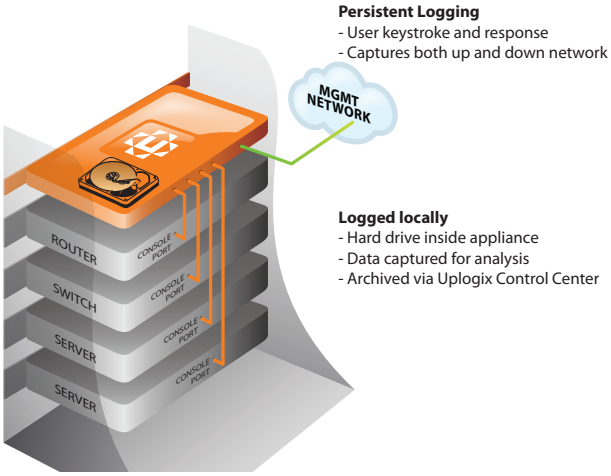
Uplogix Solution—Audit & Compliance Reporting

Uplogix audits all user interactions with managed systems to aid in compliance reporting.

How It Works

The Uplogix Appliance:

- Audits and reports all user access, device changes, and session activity (syslog, console and session logs)
- Stores logs locally and sends archives to Control Center for long-term storage, retrieval and analysis
- Examines session and console logs inline for pre-defined patterns. Alarms are generated based on log patterns. The appliance can take automated corrective action based on log patterns—avoiding the tedious, cumbersome task of manually poring over log data after a problem has occurred.
- Rules, policies and reporting can be customized in the Uplogix Control Center to meet business- or industry-specific compliance requirements



Uplogix captures, logs and archives every keystroke and output locally

Conclusion

Your role has never been more important or challenging. Your company has invested in the technology you're tasked to manage in order to gain a competitive edge in the global marketplace. However, managing this technology has grown increasingly more difficult as the IT infrastructure has become more widely distributed, more complex and more susceptible to availability and security breaches. You are stretched thin just trying to stay on top of everything that needs managing, and are constantly being asked to do more with less, leaving little time to focus on strategic initiatives.

However, a new approach for managing remote locations has emerged that overcomes the limitations of traditional management tools. The Uplogix secure remote management solution takes the headaches and hassles out of managing remote locations, greatly reducing the costs and risks that have saddled enterprise IT staff for years. To learn more about how Uplogix can solve your toughest remote management challenges, visit www.uplogix.com or contact Uplogix today.

Appendix

Key Features & Capabilities of the Uplogix SRM Solution

Access		
Heterogeneous Device Access	Serves as an secure gateway to remotely connect and access any device that supports serial management	– Native access to and support for any console-managed device – Collects console log messages from serial-connected device
Secure Remote Access	Provides multiple in-band methods to securely access and manage remote devices	– Converts unsecure serial access to secure SSHv2 access – Uplogix appliances securely relay info to the Uplogix Control Center via out-bound communications over management Ethernet connection – Supports additional security features such as source address (IP and caller ID) filtering
Out-of-Band Connectivity	Offers numerous secure out-of-band connectivity and management methods when primary network path is unavailable	– Integrated internal model dials out to POTS, Cellular or LEO Satellite connection to re-establish connectivity – Supports dial-in/ PPP dial-out (with VPN support) via embedded, Iridium or GlobalStar modems
KVM over Service Processor	Enables local access and control to a remote server for provisioning, monitoring, troubleshooting, etc.	– Functions independent of the availability of server's OS or network connection – Connects to the service processor of a remote server and exports KVM of the server to client's desktop
Remote Web Access	Offers secure access to remote devices with web-only management interfaces	– Does not require additional overhead to be managed (i.e. switch port, VLAN, user access) – Connects to remote web servers and exports the web pages to client's desktop
In-depth Device Monitoring	Continuously monitors and proactively diagnoses problems with network devices and servers, using data frequently collected on over 100 variables, with no impact to network performance	– Leverages serial connection to managed device to collect data, either in-band or out-of-band, on performance variables every 5 to 30 seconds including device interface data, CPU and memory utilization – Collects and reports device environmental data (power, temperature and humidity) to be used for trending and root cause analysis

Control		
Heterogeneous Device Management	Advanced drivers automate numerous monitoring, maintenance, configuration and recovery operations for a variety of critical IT infrastructure devices	– Advanced drivers for remotely managing: – Networking Equipment (Cisco, Nortel, 3COM, Juniper, Alcatel, NetScreen, and Tasman routers, switches, and firewalls, TippingPoint intrusion prevention systems (IPS) – Satellite Communications (Garmin GPS devices; Comtech, ND SatCom, and iDirect satellite modems; Iridium and GlobalStar external data modems) – Servers (Solaris, Linux and Windows servers (console port); Sun, Dell, IBM, HP servers (service processor port) – Power Controllers (APC, ServerTech, and Baytech)
Proactive Maintenance	Selectively choose which ongoing maintenance activities to automate including OS upgrades and patches, configuration changes, password resets, etc	– Supports OS upgrade with verification – Locally archives OS images with full rollback support – Locally stores Power-On-Self-Test (POST) data and diagnosis data (e.g. – Cisco "show tech") – Enables password recovery for devices through combination of device boot and power management procedures
Configuration Management & Recovery	Enforces consistent operations by ensuring that change and configuration management tasks are done correctly, minimizing human error and protecting availability	– Enterprise-wide configuration changes can be centrally scheduled via the Uplogix Control Center and consistently executed locally by Uplogix appliances – Device recovery with SurgicalRollback™ - If a config change fails, immediately rolls the device back to the last known good configuration
Automated Problem Resolution	Provides automation of routine fault diagnosis and recovery tasks through rule-based engine	– Proactively diagnoses non-standard operational state based on configurable thresholds – Executes best-practice recovery procedure locally to restore normal operational state – Notifies IT staff of the problem and recovery action(s) taken
Real-Time Log Inspection & Management	Shortens mean-time-to-recover by inspecting device log data in real-time and taking corrective actions based on log patterns	– Collects and inspects device console data in real-time – Sends alarm or takes predefined recovery action based on specific log messages
Service Processor Automation	Provides the ability to remotely monitor, manage, diagnose and recover servers, even if operating system has hung or the server is powered down	– Connects to service processor of remote server over IPMI and manages the server's power, system event log and sensor information without relying on the server OS

Remote Power Management	Monitors power utilization and controls power to remotely restart a managed device	– Collects power draw at regular intervals to provide an accurate view of power consumption that can be used for capacity planning – Supports daisy-chained power units, providing redundancy in the remote power management solution – Automates hardware-specific tasks that often require sub-second specialized commands and interactions during the power-on self test cycle to facilitate complicated recovery interactions
Service Level Verification	Monitors, measures and manages the performance of critical network services and applications from an end-user's perspective	– Collects performance data for the TCP/ IP based networked services and IP Telephony – Enables access to correlated device data for faster diagnostic and troubleshooting of network issues – Notifies administrators when the performance data violates threshold values – Rules-based automated procedures facilitate instant recovery for service anomalies or interruptions
Alerting & Reporting	Robust and customizable reporting of event, alarm, and device statistics, as well as network service level measurements across the enterprise	– Aggregates alarms and sends alerts via SMTP-based email to users based on their access privileges – Generates detailed reports using built-in templates or using customized templates based on organizational requirements – Provides on-demand reports and/or sends auto-generated, scheduled reports via email
Integration	Allows for flexible integration with other management systems and solutions	– Sends alarms and events via SNMP messages to other management systems as if they came from the managed device itself
Enforcement		
IT Policy Enforcement	Ensures that only the right users have the right level of access to devices and systems by providing very granular and customizable access, authorization and role-based permission controls	– AAA Enforcement – Maintains and enforces AAA (Authentication, Authorization and Accounting) model, regardless of the state of the network – Session Management – Automatically closes idle sessions to prevent unauthorized access to systems – Granular Authorization – supports and enforces role-based permissions – Authentication Standards – Integrates with remote authentication and accounting standards such as TACACS and Radius; Multifactor authentication support through integration with RSA SecureID and Secure Computing Safeword
Compliance Reporting	Audits and reports on all user access, device changes, and session activity to enable compliance	– Logs, archives and reports all console, user session, and syslog data for each managed device, even during network outages

Managed Devices & Supported Technologies

Managed Devices

Native IP

For any console-connected device, Uplogix SRM solutions can provide:

- Secure, remote access to the device, both in-band and out-of-band
- Constant and consistent IT policy enforcement including AAA enforcement, session management, and role-based permissioning
- Complete device logging (console, session, syslog) and reporting

Advanced Drivers

Beyond the level of remote management that Uplogix can provide for any console-connected device, Uplogix delivers advanced support via automated capabilities for the following devices:

- **Routers, switches, and firewalls** from Cisco, Nortel, 3COM, Juniper, Alcatel, NetScreen, and Tasman
- **Intrusion prevention systems** (IPS) from TippingPoint
- **GPS devices** from Garmin
- **Satellite modems** from Comtech, ND SatCom, and iDirect
- **External data modems** from Iridium and GlobalStar
- **Servers (console port)** from Solaris, Linux, and Windows
- **Servers (service processor port)** from Sun, Dell, IBM, and HP
- **Power strips** from APC, Servertech, and Baytech

Supported Technologies

Uplogix solutions support and integrate with the following technologies in order to provide enterprise-class secure remote management:

RADIUS & TACACS

User authentication for Uplogix SRM appliances can be directed to a RADIUS or TACACS server, keeping user passwords synchronized throughout the enterprise

while authorization is maintained on the appliance. Uplogix appliances can optionally cache TACACS ACLs, passwords locally in case authentication server cannot be reached. Some TACACS accounting features are supported by Uplogix appliances. Accounting events can be sent to a configured TACACS server using the start-stop (before and after each command) or the stop-only (after each command) model. Uplogix Control Center user authentication can also be directed to a RADIUS or TACACS server.

SSHv2

Secure Shell version 2 is the default method of communicating with Uplogix SRM appliances. Users may authenticate using passwords, certificates, or a combination of both. Uplogix appliances recognize both DSA and RSA encryption methods with key length up to 2048 bytes.

RSA SecurID Hardware Authentication

An RSA SecurID® SID800 hardware authenticator can be used with Uplogix SRM appliances. Uplogix appliances facilitate communication between managed devices connected to the appliance (e.g. Cisco router) via serial connection and the RSA Authentication Manager. The appliance reads the current authentication code from the attached RSA SecurID device and passes it on to the managed device. The managed device can then use the credentials with the RSA Authentication Manager to enforce two factor authentication.

SMTP

Uplogix SRM appliances can be configured to notify administrators of certain situations via email. The appliances aggregate alarms and sends alerts by SMTP-based email every two minutes during an outage. The Uplogix appliance's mail system supports separate email servers for use in- and out-of-band. IP addresses are used in place of hostnames to minimize dependence on DNS servers. SSL connections and SMTP authentication are both supported.

SNMP

During normal operation, the Uplogix Control Center receives SNMP trap information from managed Uplogix SRM appliances. If you are using a third-party SNMP management tool, Control Center server can be configured to forward any traps it receives. SNMP messages will be sourced with the IP address of the managed appliance. Uplogix appliances can report back SNMP information to snmp-get or snmp-walk requests.

HTTPS/SSL

Communicating to the Uplogix Control Center over a two-way SSL-Certificate secured HTTPS stream, the Uplogix SRM appliance regularly updates the server with current device status, status of scheduled jobs, alarm and event information, and other status variables. Using TCP port 8443 by default on 30-second increments, this data is compressed to reduce impact of the appliance's management traffic on the network.

Syslog

Uplogix SRM appliances can be configured to send alarm and event info to a syslog server.

CSV

Interactive views of statistics for Interfaces, CPU, Events, and more can be easily exported to .csv files for use in graphing or analysis applications. Reports also can be configured to be sent as .csv files.

Remote Management Checklist

How can you determine if a management solution can truly and actively address the challenges of managing remote locations? With so many vendors claiming "management" capabilities, it's important to separate fact from fiction. A solution that provides active, remote control of network devices and IT systems should be able to address the following questions:

- ❑ **How can I securely access and manage a device that I can't physically touch?**
  IT staff need to be able to connect to and control remote devices even when the network is down. All access, communications and actions taken need to be done securely, and audited for reporting purposes. When the primary in-band network connection is unavailable, a secure, out-of-band path is required for accessing and managing devices.

- ❑ **How does the product perform when there is a network outage or disruption?**
  All remote management tasks, including remote access, monitoring, configuration, fault and service level management needs to be performed securely and consistently, regardless of network availability.

- ❑ **How are problems with remote devices detected and fixed?**
  This is what separates monitoring from true management solutions. When common problems arise with network devices or systems, the remote management solution should be able to quickly pinpoint the root cause of an issue and offer the capability to automatically fix it without requiring manual intervention or costly on-site repair. These automated problem diagnosis and recovery abilities should be administrator-controlled, so IT staff can determine which automated features to activate and which to keep manual control over.

- ❑ **How does the product recover when a change fails?**
  Since the majority of unplanned outages are caused by human error while making changes to IT systems, it is imperative that a remote management solution provide some sort of safety net that can quickly recover from failed changes to minimize the risk of human errors and associated downtime.

- ❑ **How does the product enforce security policies?**
  Access and communications with remote devices need to be secure, authenticated and encrypted at all times. User access controls need to be enforced and user sessions managed to ensure that only the right people have the right access to the right systems. And all IT security policies need to be not only always-enforced, but also audited for compliance reporting purposes, even during network outages.

- ❑ **How much automation is built into the product?**
  Routine system maintenance, configuration, and recovery tasks should be automated whenever and wherever possible. It's just too costly and risky to send scarce, trained IT staff, or recruit untrained local staff, to perform these time-consuming tasks. Administrators should be able to control the level of automation desired in order to reduce downtime, speed changes, reduce labor requirements and minimize the risk of unplanned outages.

- ❑ **How complete is the logging data that the product provides?**
  Enterprises need complete reporting data to pass today's stringent compliance audits. This means every user interaction with network devices and systems must be logged and securely stored to comply with data control requirements found in laws such as Sarbanes-Oxley, PCI DSS (Payment Card Industry's Data Security Standards) and HIPAA (Health Insurance Portability and Accountability Act). However, when a network outage or disruption occurs, reporting data on who has accessed devices and what was done to those devices often goes un-captured and unrecorded, which can lead to stiff financial penalties as a result of incomplete reporting information.

- ❑ **How are service levels monitored and managed?**
  Existing service level monitoring and management tools have been designed to measure performance from a central location, not the end user's perspective, so they do not accurately capture and relay the quality of service that a remote user is experiencing. Additionally, these tools usually depend on the network to perform and lack the automation to proactively find and fix service-related issues. To protect SLA's, IT staff needs better visibility and control throughout the distributed infrastructure to accurately measure and manage the application and network service levels being delivered.

- ❑ **How resource-intensive (i.e. performance impact) is the product?**
  SNMP-based tools are limited by how much data they can collect and how often it can be collected in order to minimize the performance impact of these queries on the overall network. Since these tools are network-dependent, they fail to capture diagnostic data during network outages or disruptions—literally leaving IT staff "in the dark" and unable to determine the root cause of a problem, or how to fix it. Local, in-depth monitoring of devices is needed that can gather data on hundreds of diagnostic variables every few seconds without impacting network performance, which means problems at remote sites can be identified and resolved faster before leading to costly downtime that can impact business performance.

- ❑ **How easy is the product to deploy, use and manage?**
  Managing a widely distributed IT infrastructure is hard enough. It doesn't need to be made more challenging and expensive by having to buy, deploy and manage multiple non-integrated, point management tools. An integrated remote management solution is needed that deploys quickly, begins working immediately, is simple to use and manage, and integrates seamlessly with existing IT management systems.

To learn more about secure remote management from Uplogix, please visit us online or contact us for a technical demo and free evaluation of the benefits of SRM in your infrastructure:

- **uplogix.com**
- sales@uplogix.com
- 877.857.7077 (North America)
- 44(0)207 193 2798 (EMEA)

ABOUT UPLOGIX // Uplogix provides the first fully-integrated remote management solution. Our collocated management appliances automate routine administration, maintenance and recovery tasks—securely and regardless of network availability. In comparison, traditional network and systems management requires multiple tools, relies on the network, and remains labor intensive. Uplogix puts the power of your most trusted IT administrator everywhere, all the time.

Uplogix is privately held and headquartered in Austin, Texas with European offices in London.
For more information, please visit **www.uplogix.com**.

UPLOGIX