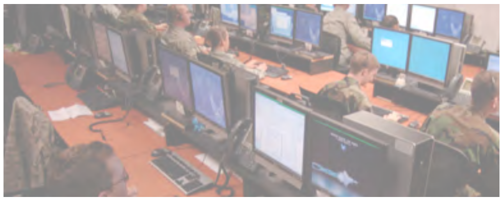
UPLOGIX WHITE PAPER

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

Annotated with Solutions for the DISA Network Infrastructure STIG

WWW.UPLOGIX.COM/FEDERAL



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 Local Management from Uplogix, using sophisticated automation, can uniquely address common challenges faced when managing remote locations as well as complement existing management solutions already in place.

Uplogix and the DISA STIG

The security features inherent in the Uplogix platform meet many of the requirements of the Network Infrastructure STIG outlined in Section 5 - Device Management, Section 6 - Authentication, Authorization, and Accounting (AAA), and Section 7 - Passwords. Features described in this document that meet STIG requirements are called out in the margins and highlighted in blue. A complete discussion of the portions of the STIG met by Uplogix is available in the appendix.

The Challenges of Managing Distributed Networks

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 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

DISA STIG
5.2 Out-of-band Management (OOB)

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 Local 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 local management that not only fulfills the local 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 local 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 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 managed devices—regardless of the state of the network.

DISA STIG

5.2	Out-of-band Management (OOB)
5.2.1	Console Port Access
5.2.2	Terminal Server Implementation
5.4.3	Network Management Station

- **Control** | By having the Uplogix platform on-site, it can perform a majority of the routine administration, maintenance and recovery tasks that an on-site technician would do today. Uplogix 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.

DISA STIG

5.4.2	Network Management Security Implications
5.5	Logistics for Configuration Loading and Maintenance
5.6	Change Management and Configuration Management

- **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.

DISA STIG

6.1	AAA Implementation
6.2	Administrator Accounts
6.3	Emergency Account
6.4	Two-factor Authentication
6.5	Auditing

The Uplogix Local Management Platform

DISA STIG
5.2.1 Console Port Access
5.2.2 Terminal Server Implementation

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 local management required to control today's distributed infrastructures.

DISA STIG
5.4.2 Network Management Security Implications
5.5 Logistics for Configuration Loading and Maintenance
5.6 Change Management and Configuration Management

The Uplogix platform components:

- **Uplogix LMS** | Uplogix' Local Management Software which powers the Uplogix devices to locally 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. LMS is available in both Standard and Advanced versions.
- **Uplogix Platform** | Available in form factors that scale from 5 to 48 managed devices, Uplogix is 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 devices and managed infrastructure throughout your environment

A Look at the Uplogix Platform Options

Scalability and Performance

Uplogix 5000 | A configurable and robust platform for enterprises that need to locally manage a large or growing infrastructure of networking gear, servers and other devices located at data centers and branch locations. Able to manage up to 21 devices and a managed power source.

Compact and Capable

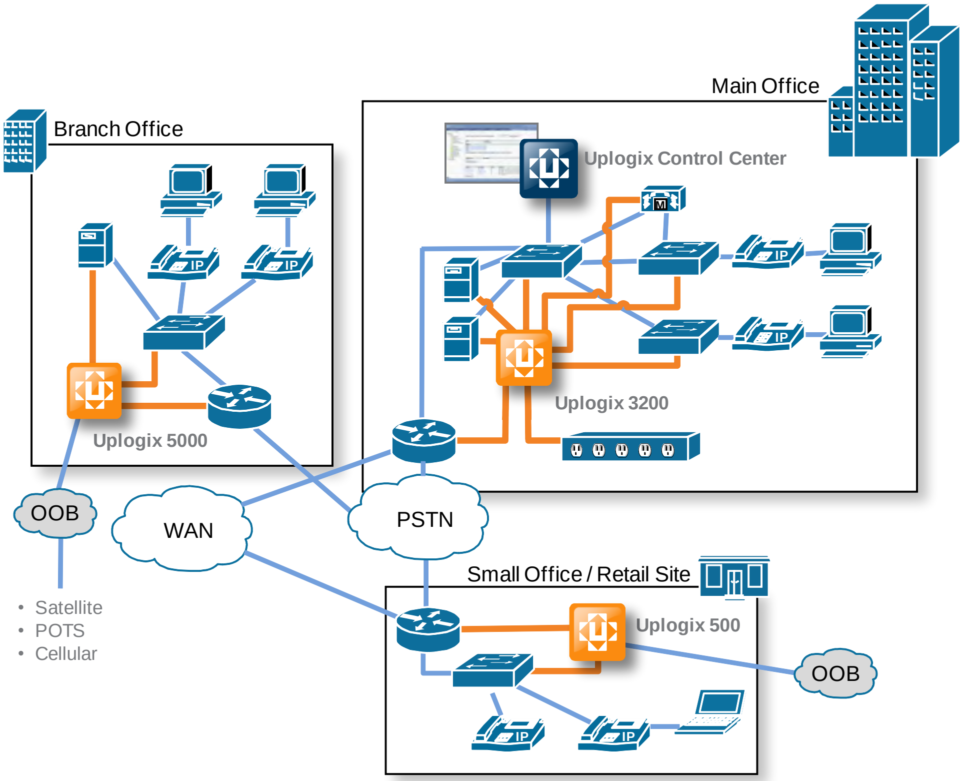
Uplogix 500 | Ideal for branch offices and remote sites where the requirement is to monitor, manage and control five or fewer devices and their power supply. The Uplogix 500 delivers local management in a compact, low cost format.

Uplogix on Cisco UCS Express

By hosting the Local Management Software on a blade in a Cisco ISR with HWIC serial port cards, the router becomes a full-featured Uplogix Local Manager configurable up to 48 managed devices.

Local Management Fit to Your Environment

Uplogix Custom Solutions | Uplogix Local Management Software deployed virtually on select platforms using in-place console servers



Together, the components of the Uplogix 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 Local Management Software

The Local Management Software (LMS) is the Uplogix software platform that powers the Uplogix platform. Utilizing LMS, enterprises are able to dramatically reduce the cost, complexity and risk of managing their distributed IT infrastructures, and improve service levels in the process. LMS increases network and system availability by automating hundreds of routine system maintenance, configuration, fault diagnosis and recovery operations. LMS is available in both Standard and Advanced versions.

The Standard version of LMS provides 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 LMS has all of the same robust, local management capabilities as the Standard version of LMS, but also includes advanced device and application management features such as Service Level Verification (SLV) which monitors, measures and manages the performance of critical network services and

DISA STIG

5.4.2	Network Management Security Implications
5.5	Logistics for Configuration Loading and Maintenance
5.6	Change Management and Configuration Management

DISA STIG

5.2	Out-of-Band Management
5.2.1	Console Port Access
5.2.2	Terminal Server Implementation
5.3	In-Band Management
5.3.1	Secure Shell Implementation
5.4.2	Network Management Security Implications
5.4.3	Network Management Station

Key Features of Local 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

DISA STIG

5.5	Logistics Configuration Loading and Maintenance
5.6	Change Management and Configuration Management
5.4.2	Network Management Security Implications

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

DISA STIG

5.6	Change Management and Configuration Management

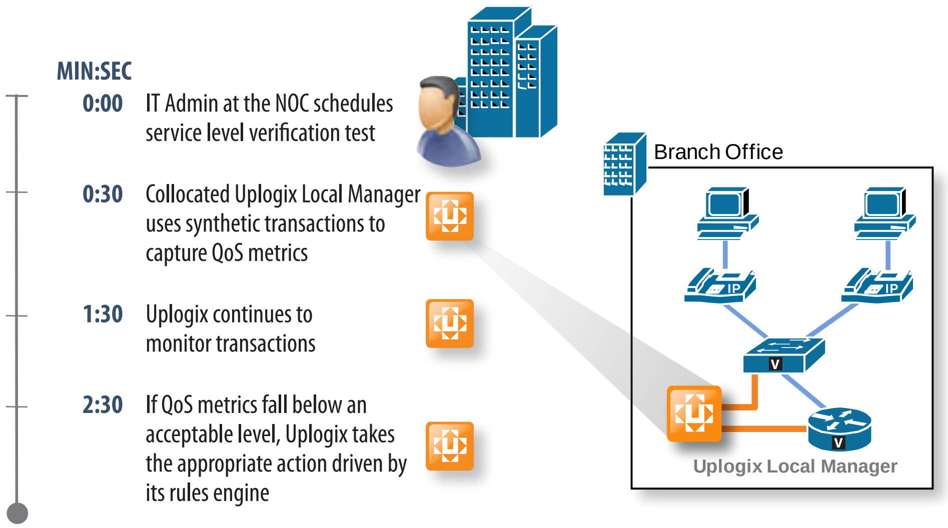
ENFORCEMENT

- **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

applications from an end-user's perspective, including TCP/IP communications, web-based transactions and voice over IP telephony.

DISA STIG
5.4.2 Network Management Security Implications

Uplogix Devices


MIN:SEC

0:00 IT Admin at the NOC schedules service level verification test

0:30 Collocated Uplogix Local Manager uses synthetic transactions to capture QoS metrics

1:30 Uplogix continues to monitor transactions

2:30 If QoS metrics fall below an acceptable level, Uplogix takes the appropriate action driven by its rules engine

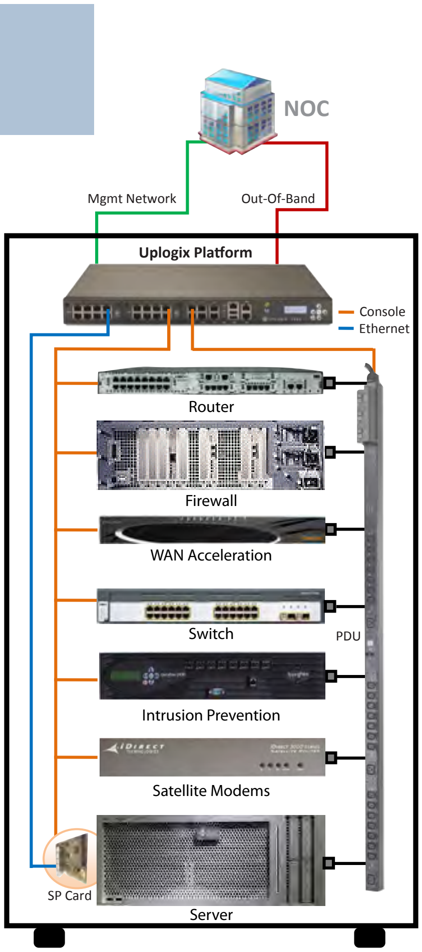
In a Service Level Verification (SLV) test of IP telephony performance at a remote location, Uplogix initiates a VoIP call from remote location and captures over 40 specific QoS metrics that reflect the health of the telephony system. Using standard Harvard sentences to gauge IPT performance, Uplogix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

Uplogix is the first fully-integrated local management platform that delivers a complete solution for cost-effectively managing a distributed IT infrastructure. Uplogix devices are deployed at remote locations, branch offices and distributed datacenters to maintain and configure IT infrastructure, as well as autonomously fix routine issues.

Uplogix delivers local management and control by interfacing directly through the console port of the devices they manage. This connection enables secure, always-on, round-the-clock management for your remote IT infrastructure. Uplogix can automate as much as 70% of routine 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 Uplogix in seconds, and fixed in minutes, avoiding costly downtime.

DISA STIG
5.2.1 Console Port Access
5.4.2 Network Management Security Implications
5.6 Change Management and Configuration Management

DISA STIG
5.4.2 Network Management Security Implications



The Uplogix LM manages IP and hybrid networks using a patented solution that delivers the local access and control of a console server, the in-depth monitoring and diagnostics of systems management software, and the intelligence of an on-site technician into a single, integrated platform.

DISA STIG
5.4.3 Network Management Station

Uplogix Control Center

The Uplogix Control Center enables local management through a centralized point of control for all deployed Uplogix devices and managed infrastructure 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 managed network devices and servers.

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, Control Center also serves as the gateway between the deployed Uplogix devices 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 customizable 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.

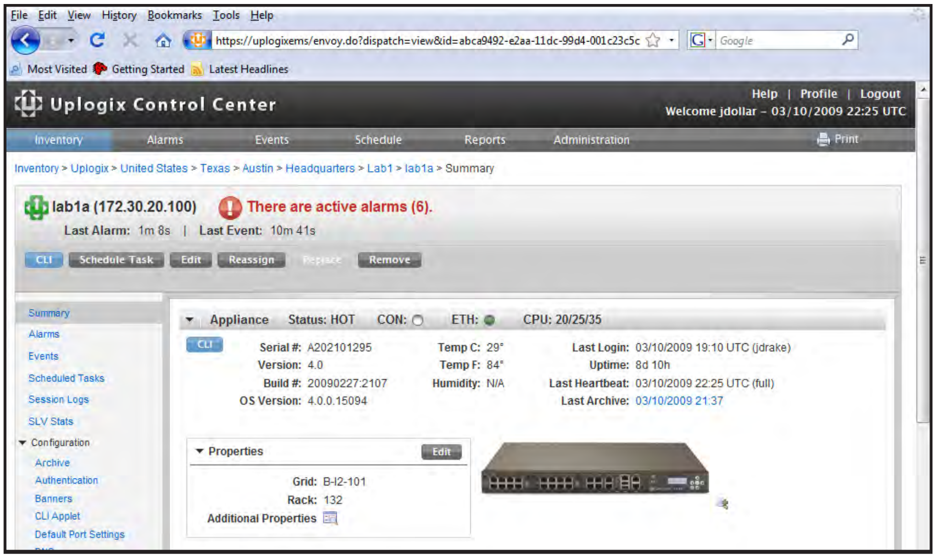
Interoperability with Existing Management Systems

The Uplogix 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-de-

DISA STIG
5.4.2 Network Management Security Implications



https://uplogixems/envoy.do?dispatch=view&id=abca9492-e2aa-11dc-99d4-001c23c5c

Welcome jdollar – 03/10/2009 22:25 UTC

Inventory > Uplogix > United States > Texas > Austin > Headquarters > Lab1 > lab1a > Summary

lab1a (172.30.20.100) There are active alarms (6).

Last Alarm: 1m 8s | Last Event: 10m 41s

Appliance Status: HOT CON: ○ ETH: ● CPU: 20/25/35

Serial #: A202101295
Version: 4.0
Build #: 20090227:2107
OS Version: 4.0.0.15094

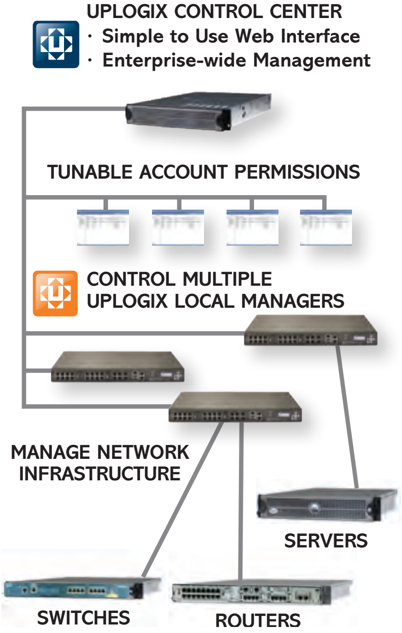
Temp C: 29°
Temp F: 84°
Humidity: N/A

Last Login: 03/10/2009 19:10 UTC (jdrake)
Uptime: 8d 10h
Last Heartbeat: 03/10/2009 22:25 UTC (full)
Last Archive: 03/10/2009 21:37

Properties

Grid: B-I2-101
Rack: 132
Additional Properties

Uplogix Control Center dashboard view of all Uplogix devices

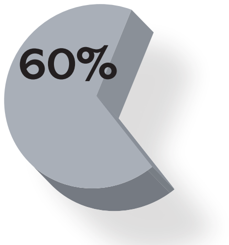


Deployed at the NOC, the Uplogix Control Center provides a centralized point of control for all Uplogix devices and managed infrastructure pendent, so when the primary network connection is down or disrupted, they lose connectivity and visibility to devices in the field.

Uplogix solutions complement NSM solutions by providing persistent connectivity and control to managed devices. Since Uplogix is 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.

Uplogix uses Monitors to gather data on various aspects of network functionality as well as operation of the Uplogix device itself, with a number of fixed based monitors for chassis (temperature, power, SMART), LMS (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.



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

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, Uplogix will send heartbeat information 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 devices 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 device 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.

DISA STIG
5.5 Logistics for Configuration Loading and Maintenance
5.6 Change Management and Configuration Management

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 (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 Uplogix 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 by Uplogix. 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.

DISA STIG

6.1	AAA Implementation
6.2	Administrator Accounts
6.3	Emergency Account
6.4	Two-factor Authentication
6.5	Auditing

In addition, Uplogix captures all changes made to systems and the results of those changes all the time to enable complete compliance reporting. Uplogix records 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 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 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.

DISA STIG
5.4.2 Network Management Security Implications

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 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 Network Management Challenges Resolved by Uplogix

Uplogix solutions move beyond the limitations of traditional monitoring and remote access tools to deliver the level of active, Local 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

DISA STIG

5.2	Out-of-Band Management
5.2.1	Console Port Access
5.2.2	Terminal Server Implementation
5.4.2	Network Management Security Implications

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 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. Uplogix co-locates and directly connects to network devices and servers to deliver persistent connectivity, as well as local 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, Uplogix 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

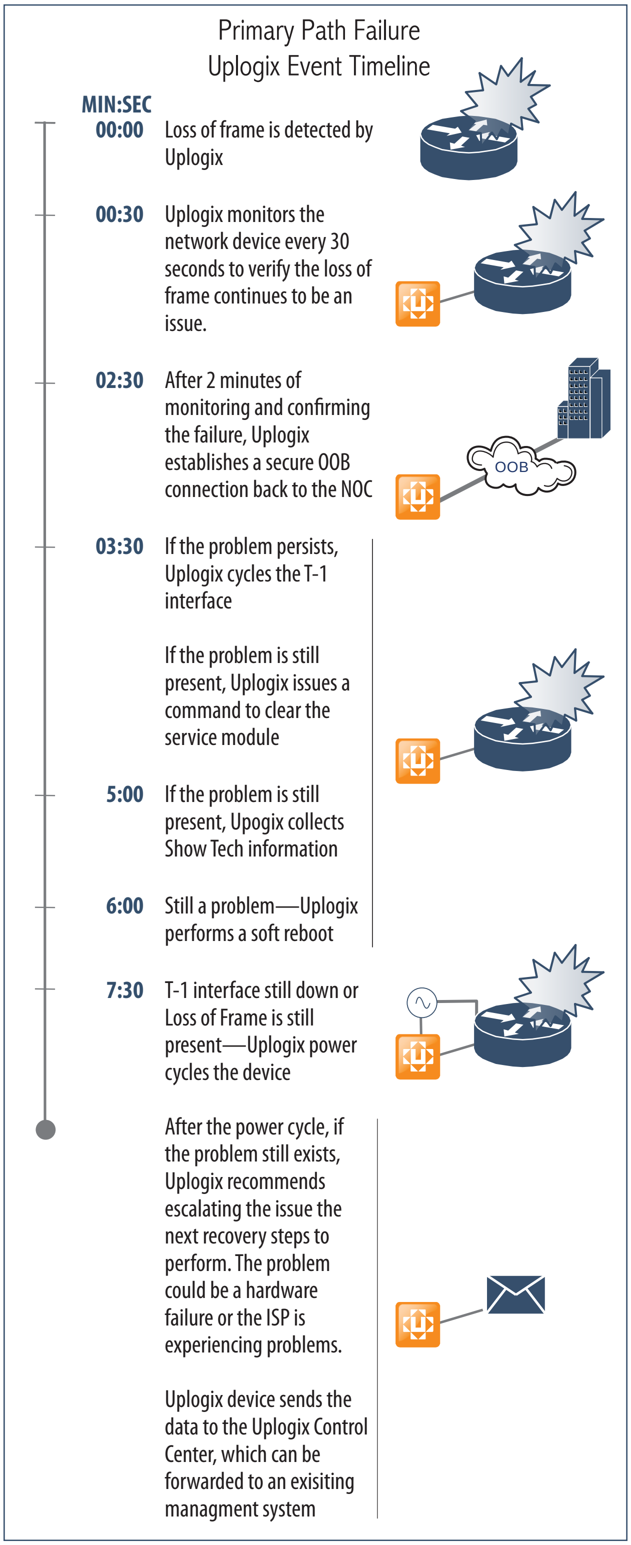
Whether located at a branch office or in a wiring closet at an enterprise headquarters, the need for remote access to network devices that are unresponsive or cannot be reached over the primary network infrastructure is critical. Regardless of where the business impact is greater, in either case a network 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).



Primary Path Failure
Uplogix Event Timeline

MIN:SEC

00:00 Loss of frame is detected by Uplogix

00:30 Uplogix monitors the network device every 30 seconds to verify the loss of frame continues to be an issue.

02:30 After 2 minutes of monitoring and confirming the failure, Uplogix establishes a secure OOB connection back to the NOC

03:30 If the problem persists, Uplogix cycles the T-1 interface

If the problem is still present, Uplogix issues a command to clear the service module

5:00 If the problem is still present, Upogix collects Show Tech information

6:00 Still a problem—Uplogix performs a soft reboot

7:30 T-1 interface still down or Loss of Frame is still present—Uplogix power cycles the device

After the power cycle, if the problem still exists, Uplogix recommends escalating the issue the next recovery steps to perform. The problem could be a hardware failure or the ISP is experiencing problems.

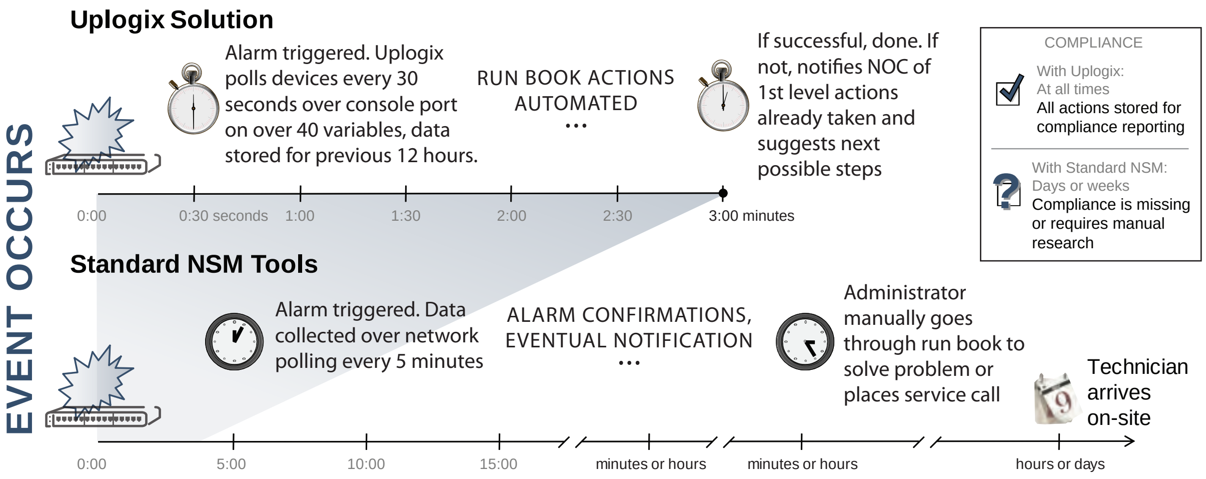
Uplogix device sends the data to the Uplogix Control Center, which can be forwarded to an exisiting managment system

False or Missed Alarms

DISA STIG
5.4.2 Network Management Security Implications

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. Uplogix 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. Uplogix 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.



Alarm triggered. Uplogix polls devices every 30 seconds over console port on over 40 variables, data stored for previous 12 hours.

If successful, done. If not, notifies NOC of 1st level actions already taken and suggests next possible steps

With Uplogix: At all times
All actions stored for compliance reporting

With Standard NSM: Days or weeks
Compliance is missing or requires manual research

Alarm triggered. Data collected over network polling every 5 minutes

Administrator manually goes through run book to solve problem or places service call

Technician arrives on-site

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

Burdensome System Maintenance

DISA STIG
5.5 Logistics for Configuration Loading and Maintenance
5.6 Change Management and Configuration Management

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. Uplogix 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.

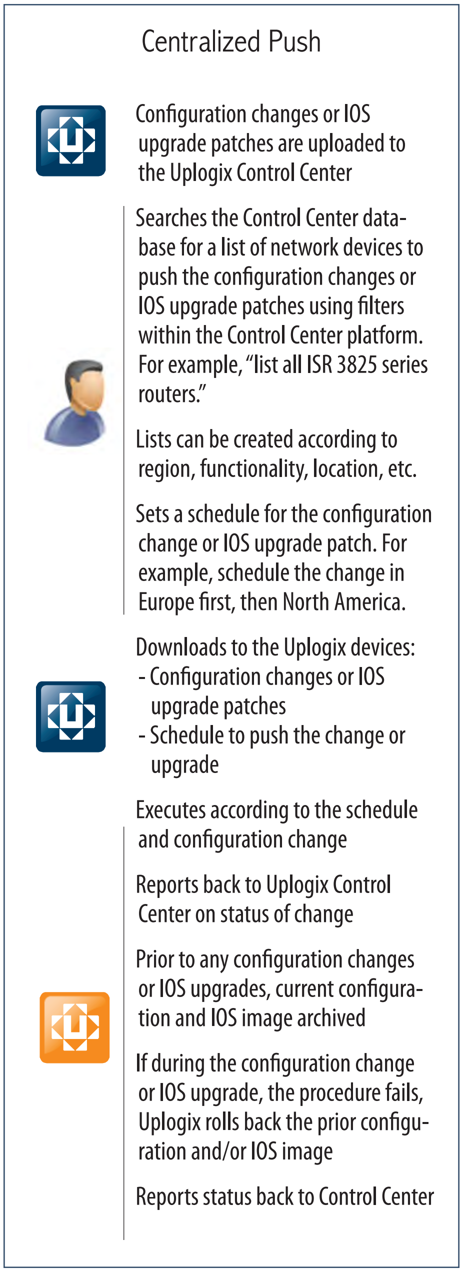
Solution Timeline:
Mass Configuration / Password / OS Change

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.



Centralized Push

Configuration changes or IOS upgrade patches are uploaded to the Uplogix Control Center

Searches the Control Center database for a list of network devices to push the configuration changes or IOS upgrade patches using filters within the Control Center platform. For example, "list all ISR 3825 series routers."

Lists can be created according to region, functionality, location, etc.

Sets a schedule for the configuration change or IOS upgrade patch. For example, schedule the change in Europe first, then North America.

Downloads to the Uplogix devices:
- Configuration changes or IOS upgrade patches
- Schedule to push the change or upgrade

Executes according to the schedule and configuration change

Reports back to Uplogix Control Center on status of change

Prior to any configuration changes or IOS upgrades, current configuration and IOS image archived

If during the configuration change or IOS upgrade, the procedure fails, Uplogix rolls back the prior configuration and/or IOS image

Reports status back to Control Center

Uplogix Solution—Centralized Configuration Management

The Uplogix Control Center enables Local Management through a centralized point of control for all Uplogix devices and managed infrastructure 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 the Uplogix platform.

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 locally by Uplogix

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, Uplogix backs out all uncommitted changes made during that session.

The default action is to rollback all uncommitted changes

Starts countdown to SurgicalRollback

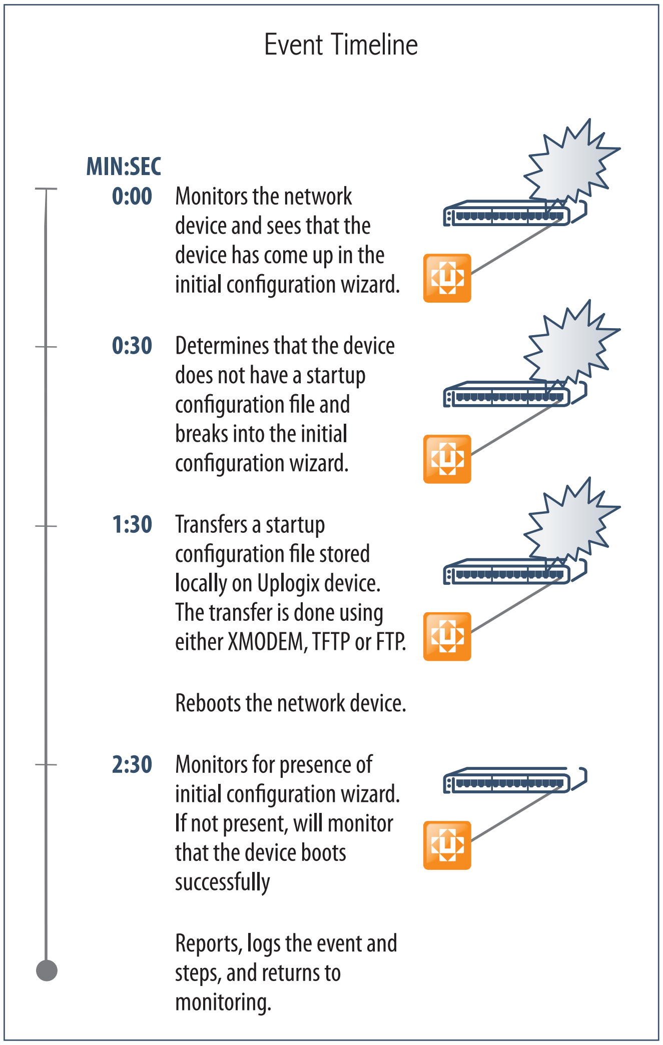
If no response, Uplogix will rollback only changes made to the device

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 local 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 take action when certain conditions occur. For example, Uplogix 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.



Event Timeline

MIN:SEC

0:00 Monitors the network device and sees that the device has come up in the initial configuration wizard.

0:30 Determines that the device does not have a startup configuration file and breaks into the initial configuration wizard.

1:30 Transfers a startup configuration file stored locally on Uplogix device. The transfer is done using either XMODEM, TFTP or FTP.

Reboots the network device.

2:30 Monitors for presence of initial configuration wizard. If not present, will monitor that the device boots successfully

Reports, logs the event and steps, and returns to monitoring.

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 take action when certain conditions occur.

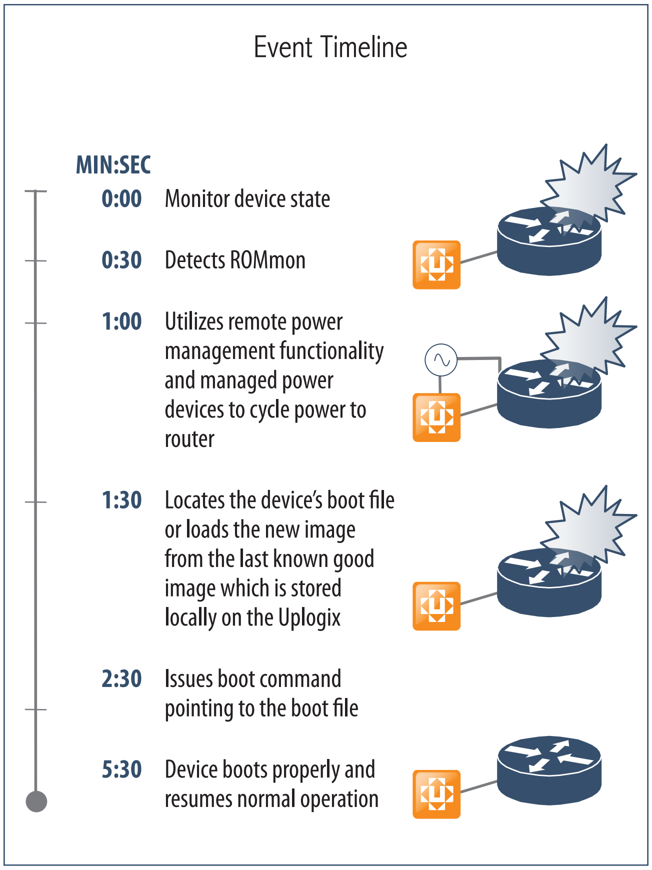
Cycling Power to a Remote Device

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, Uplogix 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



Event Timeline

MIN:SEC	
0:00	Monitor device state
0:30	Detects ROMmon
1:00	Utilizes remote power management functionality and managed power devices to cycle power to router
1:30	Locates the device's boot file or loads the new image from the last known good image which is stored locally on the Uplogix
2:30	Issues boot command pointing to the boot file
5:30	Device boots properly and resumes normal operation

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 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 operates 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 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.

DISA STIG

5.3	In-Band Management
5.3.1	Secure Shell Implementation
6.1	AAA Implementation
6.2	Administrator Accounts

Current Methods

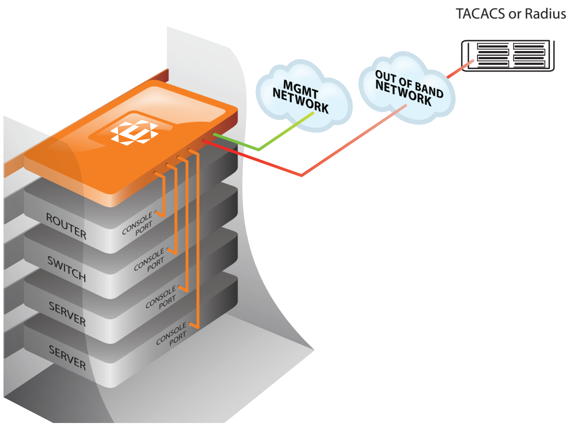
Software-based tools often cannot enforce security policies during a network outage, plus they often require the opening of additional ports to both receive and send data, which increases exposure. Remote access tools such as console servers are usually limited to only enforcing port-level permissions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

DISA STIG
5.6 Change Management and Configuration Management

Leveraging its dedicated serial connection with managed devices and servers, Uplogix 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 continues 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

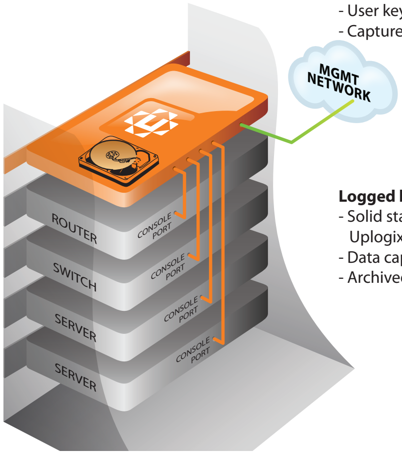
Uplogix audits all user interactions with managed systems to aid in compliance reporting.

DISA STIG
5.6 Change Management and Configuration Management

How It Works

The Uplogix Platform:

- 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. Uplogix 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



Persistent Logging
- User keystroke and response
- Captures both up and down network

Logged locally
- Solid state hard drive inside Uplogix Local Manager
- Data captured for analysis
- Archived via Uplogix Control Center

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 Local 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 Platform

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 securely relays 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
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) – 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 LMs – 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
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 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
- **Power strips** from APC, Servertech, and Baytech

Supported Technologies

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

RADIUS & TACACS

User authentication for Uplogix can be directed to a RADIUS or TACACS server, keeping user passwords synchronized throughout the enterprise while authorization is maintained on the LM. Uplogix can optionally cache TACACS ACLs, passwords locally in case authentication server cannot be reached. Some TACACS accounting features are supported by Uplogix. 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 devices. Users may authenticate using passwords, certificates, or a combination of both. Uplogix recognizes 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. Uplogix facilitates communication between managed devices (e.g. Cisco router) connected to the Uplogix device via serial connection and the RSA Authentication Manager. Uplogix 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 can be configured to notify administrators of certain situations via email. Uplogix aggregates alarms and sends alerts by SMTP-based email every two minutes during an outage. Uplogix' 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 devices. 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 LM. Uplogix 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 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 Upogix' management traffic on the network.

Syslog

Uplogix 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.

A detailed discussion of the Uplogix Platform for STIG Requirements for Device Management, AAA and Passwords

The DISA Network Infrastructure Security Technical Implementation Guide (STIG) is designed to help sites meet the minimum requirements, standards, controls, and options that must be in place for secure network operations. To read the full STIG, please go to: http://iase.disa.mil/stigs

5. Device Management

5.1 Vulnerability & Asset Management

(NET1621: CAT II) The IAO will properly register all network components in VMS.

5.2 Out-of-band Management (OOB)

(NET1622: CAT II) The IAO/NSO will ensure an OOB management network is in place for MAC I systems or 24x7 personnel have immediate console access (direct connection method) for communication device management.

- By using the Uplogix Local Manager (LM) 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 LM—even during outages. 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.

  Provides constant, secure connectivity, access and control over remote devices

  By default Uplogix LMs "Dial-out", not in, to restore secure connectivity to managed devices when primary connection is lost, eliminating potential security threats

  Functions securely both in-band and out-of-band, providing multiple backup connectivity options including PPP/dial-up, cellular, and satellite with secure VPN connectivity

5.2.1 Console Port Access

- Uplogix LMs have a dedicated console port. A user must properly authenticate to gain access to the system via the console port via local, TACACS or RADIUS authentication methods. Even if the network is down, authentication will occur over the out-of-band connection that is automatically established.

5.2.2 Terminal Server Implementation

- Uplogix LMs provide up to 32 serial ports for Terminal Server functionality. Each port supports RS-232 and can only be accessed if the user is authorized via local, TACACS or RADIUS authentication methods.

5.2.3 Juniper Implementation

- Uplogix provides a "driver" that supports Juniper devices. Uplogix can log in, log off, manage, and monitor Juniper Devices. Uplogix maintains 21 versions of previous configurations and 3 versions of OS. Each LM logs all actions and output users execute during entire length of the session.

5.2.4 WAN Implementation

(NET1623: CAT I) The IAO/NSO will ensure all OOB management connections to the device require passwords.

- Any connection to an Uplogix LM or Control Center requires the proper Authentication and based on the user the proper authorizations are applied. Uplogix also may use TACACS or RADIUS for both authentication and authorization. A user only has access to what they are authorized.

(NET1624: CAT II) The system administrator will ensure the console port is configured to time out after 10 minutes or less of inactivity.

- Both the Uplogix Control Center and LMs have the ability to set the inactivity timer of each port and the LM itself.

(NET1628: CAT II) The IAO/NSO will ensure modems are not connected to the console port.

- Uplogix has multiple connection methods for OOB (PPP/POTS, Cellular, Satellite or Ethernet). Once the OOB connection is established and secured, a user must authenticate and only has access to what they are authorized. This is granular to the port and command level. The OOB technolgy is connected to Uplogix LMs instead of the managed devices to ensure this level of security. Even during out of band situations, TACACS or RADIUS would still be functional as the OOB implementation ensures that a proper secure network is established to these systems.

(NET1629: CAT III) The system administrator will ensure the device auxiliary port is disabled if a secured modem providing encryption and authentication is not connected.

- Since the Uplogix LMs would facilitate the OOB connection instead of the network components, the network and the devices supporting the network inherently become more secure even during outages.

5.3 In-Band Management

(NET1635: CAT II) The network administrator will limit the use of in-band management to situations where the use of OOB management would hinder operational commitments or when emergency situations arise. IAO/NSO will approve the use of in-band management on a case-by-case documented basis.

- All in-band traffic is secure via SSHV2 and HTTPS (port 8443). SNMP is not used for management of end components such as routers, switches, etc. All monitoring is done via the CLI of the connected device via the console/serial port. SNMP may be used from the Uplogix Control Center to an NMS system via the management network. In essence this is Secure Monitoring. Via the CLI of a device, we find incidents based on known errors (conditions). This information is relayed via the secure traffic via port 8443 to the Uplogix Control Center.

(NET1636: CAT I) The IAO/NSO will ensure all in-band management connections to the device require passwords.

- Any connection to an Uplogix LM or Control Center requires the proper Authentication and based on the user the proper authorizations are applied. Uplogix also may use TACACS or RADIUS for both authentication and authorization. A user only has access to what they are authorized.

(NET1637: CAT II) The system administrator will ensure the device only allows in-band management sessions from authorized IP addresses from the internal network.

- An IP filter may be used within the Uplogix LM to dictate an ACL based restriction.

(NET1638: CAT II) The system administrator will ensure in-band management access to the device is secured using an encryption such as AES, 3DES, SSH, or SSL.

- Uplogix LMs support SSHv2 for in-band and out of band access. The Uplogix Control Center uses SSL certs between LMs and Users.

(NET1639: CAT II) The system administrator will ensure the timeout for in-band management access is set for no longer than 10 minutes.

- Both the Uplogix Control Center and LMs have the ability to set the inactivity timer of each port and the LM itself.

(NET1640: CAT III) The system administrator will configure the ACL that is bound to the VTY ports to log permitted and denied access attempts.

- Using Uplogix, there is no longer a need to enable VTY port on network components. Having users connect to the Uplogix LM via SSHv2 creates a more secure solution. This process also enables the tracking of everything a user executes and is displayed as output from the user perspective. A user is only given permission to see and do on a per port and per command basis via local, TACACs or RADIUS authentication/authorization.

5.3.1 Secure Shell Implementation

(NET1645: CAT II) The system administrator will ensure SSH timeout value is set to 60 seconds or less, causing incomplete SSH connections to shut down after 60 seconds or less.

- The FIPS 140-2 version of Uplogix has implemented this timeout.

(NET1646: CAT II) The system administrator will ensure the maximum number of unsuccessful SSH login attempts is set to three, locking access to the router.

- The Uplogix LMs support locking access after a configureable threshold is met.

(NET1647: CAT II) The system administrator will ensure SSH version 2 is implemented.

- Uplogix LMs and Control Center both support SSHv2. Telnet is disabled by default.

5.4 Simple Network Management Protocol (SNMP)

5.4.1 The IP Management Model

5.4.2 Network Management Security Implications

(NET1650: CAT II) The IAO/NSO will ensure IPSec is used to secure traffic between the network management workstation on DoD-managed LANs and all monitored devices sent via the Internet, NIPRNet, SIPRNet, or other external network.

- Uplogix supports SSHv2 between client and LM via in-band and out-of-band. When Out of band a secure VPN is established back to the management network.

(NET1660: CAT I) The IAO/NSO will ensure the SNMP Version 3 Security Model (both MD5 packet authentication and DES encryption of the PDU) is used across the entire network infrastructure.

NOTE: If the site is using Version 1 or Version 2 with all of the appropriate patches and has developed a migration plan to implement the Version 3 Security Model, this finding can be downgraded to a Category II.

- Uplogix uses SNMP V3.

(NET1665: CAT I) The IAO/NSO will ensure all SNMP community strings are changed from the default values.

- By default SNMP is disabled and must be enabled to work. There is no default community string.

(NET1666: CAT II) The IAO/NSO will ensure all SNMP community strings and usernames are protected via technology that secures using an encryption such as AES, 3DES, SSH, or SSL.

- Uplogix LMs support AES128, AES192 and AES256 for encryption.

(NET1670: CAT III) The IAO/NSO will establish and maintain a standard operating procedure managing SNMP community strings and usernames to include the following:
- Community string and username expiration period
- SNMP community string and username distribution including determination of membership

- Uplogix incorporates a hierarchy model and a query model to modify SNMP settings. This allows a mass change on-demand of any SNMP setting for all LMs. Uplogix can also schedule SNMP configuration changes on a mass scale to all managed devices that are supported by an Uplogix driver.

(NET1675: CAT II) The IAO/NSO will ensure if both privileged and non-privileged modes are used on all devices. Different community names will be used for read-only access and read-write access.

- Only one mode is allowed on the LM therefore this is not applicable.

(NET1710: CAT III) The IAO/NSO will ensure security alarms are set up within the managed network's framework. At a minimum, these will include the following:

- Integrity Violation: Indicates that network contents or objects are illegally modified, deleted, or added.

- Uplogix LMs do not inspect packets on the network. The LM sits on the network to provide in-band and out-of-band access via SSHv2. This access allows the northbound monitoring of devices via an Uplogix driver by interfacing with the CLI. This access also provides end users whom are authorized access similar to a terminal server.

- Operational Violation: Indicates that a desired object or service cannot be used.

- The Uplogix LMs can monitor many components on the network. By using the managed device (Router, Switch, Power, etc) Command Line Interface (CLI) Uplogix LMs can isolate and possibly resolve many types of incidents.

- Physical Violation: Indicates that a physical part of the network (such as a cable) is

damaged or modified without authorization.

- The Uplogix LM can monitor anything that the managed component detects via the CLI. If there is a Layer 1 incident on a router or switch and Uplogix monitors that particular port, an alarm will be generated.

- Security Mechanism Violation: Indicates that the network's security system is compromised or breached.

- Uplogix LMs do not inspect packets on the network. The LM sits on the network to provide in-band and out-of-band access via SSHv2. This access allows the northbound monitoring of devices via an Uplogix driver by interfacing with the CLI. This access also provides end users whom are authorized access similar to a terminal server.

- Time Domain Violation: Indicates that an event is happening outside its allowed or typical time slot.

- Uplogix LMs can perform both monitoring and alerting based on time and schedules.

(NET1720: CAT III) The IAO/NSO will ensure alarms are categorized by severity using the following guidelines:

- Critical and major alarms are given when a condition that affects service has arisen. For a critical alarm, steps must be taken immediately in order to restore the service that is lost completely.

- A major alarm indicates that steps must be taken as soon as possible because the affected service has degraded drastically and is in danger of being lost completely.

- A minor alarm indicates a problem that does not yet affect service, but may do so if the problem is not corrected.

- A warning alarm is used to signal a potential problem that may affect service.

- An indeterminate alarm is one that requires human intervention to decide its severity.

- ▶ Uplogix LMs use a ruleset to monitor specific conditions and take automated action based on these conditions. Based on the severity, time, thresholds, etc, these automated actions work as a standard troubleshooting methodology. This allows for a standard practice for incident management with the potential to resolve the incident within minutes or at the very least isolate the problem.

5.4.3 Network Management Station

(NET1730: CAT II) The IAO/NSO will ensure the management workstation is located in a secure environment.

- ▶ N/A

(NET1740: CAT II) The IAO/NSO will ensure only those accounts necessary for the operation of the system and for access logging are maintained.

- ▶ Any connection to an Uplogix LM or Control Center requires the proper Authentication and based on the user the proper authorizations are applied. Uplogix also may use TACACS or RADIUS for both authentication and authorization. A user only has access to what they are authorized.

(NET1750: CAT III) The IAO/NSO will ensure a record is maintained of all logons and transactions processed by the management station.

NOTE: Include time logged in and out, devices that were accessed and modified, and other activities performed.

- ▶ Uplogix LMs log all interactions including Time stamp of all logon/logoff activities. Furthermore, all commands executed and output displayed to user is logged. This is true for both interactions on the LM itself and via the managed device CLI.

(NET1760: CAT I) The IAO/NSO will ensure access to the NMS is restricted to authorized users with individual userids and passwords.

- ▶ Any connection to an Uplogix LM or Control Center requires the proper Authentication and based on the user the proper authorizations are applied. Uplogix also may use TACACS or RADIUS for both authentication and authorization. A user only has access to what they are authorized.

(NET1762: CAT II) The IAO/NSO will ensure all in-band sessions to the NMS is secured using an encryption such as AES, 3DES, SSH, or SSL.

- Uplogix LMs support SSHv2 for in-band and out of band access. The Uplogix Control Center uses SSL certs between LMs and Users.

(NET1770: CAT II) The IAO/NSO will ensure connections to the NMS are restricted by IP address to only the authorized devices being monitored.

- An IP filter may be used within the Uplogix LM to dictate an ACL based restriction.

(NET1780: CAT II) The IAO/NSO will ensure all accounts are assigned the lowest possible level of access/rights necessary to perform their jobs.

- Uplogix LMs and Control Center support granularity to the command level on each resource such as port, modem, etc.

5.5 Logistics for Configuration Loading and Maintenance

(NET1030: CAT III) The router administrator, when saving and loading configurations will ensure that the running and startup configurations are synchronized.

- Uplogix LMs have the ability to save the running configuration to startup configuration both ad-hoc or on a scheduled/reoccurring basis. By default the LM stores 21 previous versions and the current of both the running and startup configurations. These also may be pushed ad-hoc or on a scheduled/reoccurring basis.

(NET1040: CAT III) The router administrator will ensure at least the current and previous router configurations are stored in a secured location to ensure a proper recovery path.

- By default the LM stores 21 previous versions and the current of both the running and startup configurations. These also may be pushed ad-hoc or on a scheduled/reoccurring basis. This data is stored at the port level in a secure encrypted database on the Uplogix LM.

(NET1050: CAT III) The IAO/NSO will ensure that on the system where the configuration files are stored, the administrator uses the local operating system's security mechanisms for restricting access to the files (i.e., password restricted file access).

- Since Uplogix LMs and Control Center support granularity to the command level on each resource such as port, modem, etc, restricting the viewing of these configurations is easily accomplished.

(NET1060: CAT I) The router administrator will not store unencrypted router passwords in an offline configuration file.

- The Uplogix LM does not store any passwords to any device outside of its database. These passwords are stored in a 3DES encrypted SHA-1 salted hash.

(NET1070: CAT II) The IAO/NSO will authorize and maintain justification for all TFTP implementations.

- Uplogix LMs support the use of FTP instead of TFTP collecting device images such as JUNOS and/or Cisco IOS. Files sent between the LMs and the Control Center are all encrypted via SSL on port 8443. Files between clients and the LM may useSCP as well as FTP.

(NET1071: CAT II) If TFTP implementation is used, the router administrator will ensure the TFTP server resides on a controlled managed LAN subnet, and access is restricted to authorized devices within the local enclave.

- Uplogix LMs solve this in a couple ways. First, the TFTP server is only enabled when necessary. Unless a file is needing transferred between LM and managed device, TFTP is turned off. TFTP only works if the managed device IP is the source of the TFTP transfer, otherwise the transfer fails. The LM also has an optional "dedicated" Ethernet module that enables a 2 node network isolated between the LM and managed device if more security is needed. Manual TFTP transfers are only allowed on an ad-hoc basis if the user has been given that privilege. Once exiting the port, the TFTP server is automatically disabled.

(NET1080: CAT II) The router administrator will ensure the FTP username and password are configured.

- Uplogix LMs support the use of FTP instead of TFTP collecting device images such as JUNOS and/or Cisco IOS. Files sent between the LMs and the Control Center are all encrypted via SSL on port 8443. Files between clients and the LM may useSCP as well as FTP.

5.6 Change Management and Configuration Management

(NET1110: CAT II) The IAO/NSO will ensure all changes and updates are documented in a manner suitable for review and audit.

- All interactions through and on the Uplogix LM are logged. Auditing is also possible based on user privilege. Reports may be sent on a hourly, daily, weekly or monthly basis based on changes, events, alarms, among others.

(NET1111: CAT II) The IAO/NSO will ensure request forms are used to aid in recording the audit trail.

- N/A

(NET1113: CAT II) The IAO/NSO will ensure current paper or electronic copies of configurations are maintained in a secure location.

- By default the LM stores 21 previous versions and the current of both the running and startup configurations. These also may be pushed ad-hoc or on a scheduled/reoccurring basis. This data is stored at the port level in a secure encrypted database on the Uplogix LM.

(NET1114: CAT II) The IAO/NSO will ensure only authorized personnel, with proper verifiable credentials, are allowed to request changes to routing tables or service parameters.

- N/A

6. AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING

6.1 AAA Implementation

Table 6-1. Authentication Parameters

(NET0430: CAT II) The IAO/NSO will ensure an authentication server is used to gain administrative access to all network devices.

- Uplogix Supports authentication, authorization and accounting locally on an encrypted database, TACACS and Radius.

(NET0431: CAT III) The IAO/NSO will ensure all AAA authentication services are configured to use two-factor authentication during normal operation.

- Uplogix LMs support two-factor authentication

(NET0432: CAT III) The IAO/NSO will ensure the device is configured to use AAA tiered authorization groups for management authentication.

- Uplogix LMs support tiered groups within its local authentication mechanism. Support for TACACS and RADIUS for AAA may be configured individually on specific LMs, groups of LMs and the Control Center.

(NET0433: CAT II) The IAO/NSO will ensure an authentication method list is applied to all interfaces via an explicit definition or by use of default key word.

- N/A

(NET0434: CAT II) The IAO/NSO will ensure the AAA authentication method implements user authentication.

- Users who access the Uplogix LMs and/or Control Center must be authenticated first via local, TACACS or Radius authentication. A user is assigned privileges based on role.

6.2 Administrator Accounts

(NET0460: CAT I) The IAO/NSO will ensure each user accessing the device locally have their own account with username and password.

- Managed devices console username and passwords when applicable may forever be kept secret. The Uplogix LM understands the concept of secondary authentication means when a device cannot connect to the AAA servers. With the ability to use the Uplogix LM whether in-band or out-of-band, a user must authenticate to the LM to gain authorized access to a device. There are multiple options to logging into the console port. It may be done for the user to keep the username/password safe, or a user may authenticate manually.

(NET0465: CAT II) The IAO/NSO will ensure all user accounts are assigned the lowest privilege level that allows them to perform their duties.

- Uplogix LMs and Control Center support granularity to the command level on each resource such as port, modem, etc.

(NET0470: CAT II) The IAO/NSO will immediately have accounts removed from the authentication server or device, which are no longer required.

- N/A

6.3 Emergency Account

(NET0440: CAT II) The IAO/NSO will ensure only one account is defined locally for use in an emergency (i.e., authentication server or connection to the device is down).

- Managed devices console username and passwords when applicable may forever be kept secret. The Uplogix LM understands the concept of secondary authentication means when a device cannot connect to the AAA servers. With the ability to use the Uplogix LM whether in-band or out-of-band, a user must authenticate to the LM to gain authorized access to a device. There are mulitple options to logging into the console port. It may be done for the user to keep the username/password safe, or a user may authenticate manually.

(NET0441: CAT I) The IAO/NSO will ensure the emergency account defaults to the lowest authorization level and the password is in a locked safe.

- The Uplogix LM does not store any passwords to any device outside of its database. These passwords are stored in a 3DES encrypted SHA-1 salted hash.

(NET0340: CAT II) The IAO/NSO will ensure warning banners are deployed on all network devices allowing SSH, Telnet, FTP, or HTTP access in accordance with DoDI 8500.2 ECWM-1.

- Uplogix provides the ability to configure a Login (Warning) banner and a Welcome message for clients accessing the LMs and/or Control Center.

6.4 Two-factor Authentication

(NET0445: CAT II) To ensure the proper authorized network administrator is the only one who can access the device, the IAO/NSO will ensure device management is restricted by two- factor authentication (e.g., Secure ID, DoD PKI, or alternate token logon).

- Uplogix LMs support two-factor authentication

6.5 Auditing

6.5.1 Syslog Server

Table 6-2. Logging

(NET1020: CAT III) The IAO/NSO will ensure all attempts to any port, protocol, or service that is denied is logged.

- Uplogix LMs log all interactions including Time stamp of all logon/logoff activities. Furthermore, all commands executed and output displayed to user is logged. This is true for both interactions on the LM itself and via the managed device CLI. All failed attempts are also logged.

(NET1021: CAT III) The IAO/NSO will configure all devices to log severity levels 0 through 7 and send log data to a syslog server.

- Uplogix LMs support forwarding of all syslogs to a designated syslog server. The LMs collect the syslogs from the managed device and stores them on the LM. This information can update an NMS system despite the state of the network due to the out-of-band capabilities.

(NET1022: CAT III) The IAO will ensure the syslog server is only connected to the management network.

- N/A

(NET1023: CAT II) The IAO will ensure the syslog servers are configured IAW the appropriate OS STIG.

- N/A

(NET1025: CAT III) The IAO/NSO will ensure a centralized syslog server is deployed and configured by the syslog administrator to store all syslog messages for a minimum of 30 days online and then stored offline for one year.

- The Uplogix LM can forward all SYSLOGs to a centralized server in-band or out-of-band.

(NET1027: CAT III) The syslog administrator will configure the syslog sever to collect syslog messages from levels 0 through 7.

- N/A

(NET1028: CAT III) The syslog administrator will configure the syslog server to accept messages only from authorized devices (restricting access via source and destination IP address).

- Uplogix LMs only collect the SYSLOG data from the managed device via the console port.

(NET1280: CAT III) The IAO/NSO will ensure there is a review on a daily basis, of the firewall log data by the Firewall Administrator (FA), or other qualified personnel, to determine if attacks or inappropriate activity has occurred.

- N/A

(NET1281: CAT III) The IAO will ensure an HIDS is implemented on the syslog server to provide access control for the syslog data as well as provide the necessary protection against unauthorized user and service access.

- N/A

(NET1284: CAT III) The IAO/NSO will ensure the firewall configuration data are backed up weekly and whenever configuration changes occur.

- If the Uplogix LM is managing a supported firewall with the appropriate Uplogix driver, 21 versions of previous configurations are stored. If the current configuration is different than the stored current, the Uplogix LM automatically updates it's database and stores the older configuration.

(NET1286: CAT III) The IAO/NSO will ensure the audit log data is backed up weekly.

- N/A

(NET1287: CAT II) The IAO/NSO will ensure audit logs are protected from deletion.

- Events are not stateful and cannot be deleted from the database. All logs are kept on the LM and stored/archived to the Control Center.

(NET1288: CAT III) The IAO/NSO will ensure the audit trail events are stamped with accurate date and time.

- NTP is the preferred method of ensuring times are accurately reported for all stamped events/logs.

(NET1289: CAT III) The IAO/NSO will ensure the audit trail events include source IP, destination IP, protocol used and action taken.

- Based on the interactions, this information is stored in log

(NET1300: CAT III) The IAO/NSO will ensure administrator logons, changes to the administrator group, and account lockouts are logged.

- All interactions on the Uplogix LMs are logged and archived on the Control Center. Any executed command and the output is also stored and archived.

(NET1299: CATIII) The IAO will ensure the firewall provides the ability to perform searches and sorting of audit data, based on user identity, source identity, destination identity, and provides ranges of one or more of the following: dates, times, user identities, service identifiers, or transport layer protocol, rule identity, and network interfaces.

- N/A

7. PASSWORDS

7.1 Password Encryption

(NET0230: CAT I) The IAO/NSO will ensure all communications devices are password protected.

- The Uplogix LM does not store any passwords to any device outside of its database. These passwords are stored in a 3DES encrypted SHA-1 salted hash.

(NET0240: CAT I) The IAO/NSO will ensure all default manufacturer passwords are changed.

- N/A

(NET0260: CAT II) The IAO/NSO will ensure all passwords are created and maintained in accordance with the rules outlined in DoDI 8500.2, IAIA-1, and IAIA-2. http://www.dtic.mil/whs/directives/corres/html/85002.htm

- The local authentication mechanism has the option to enforce the following:
  Use strong passwords
  Require mixed case
  Require numbers and punctuation
  Reject variation of login id
  Reject word in dictionary
  Reject standard substitutions (@ for a, 3 for e, etc)
  Reject sequences in numbers or letters (qwerty)
  Reject previous password
  Number of previous passwords to check
  Reject single character difference from previous password
  Enforce minimum password length
  Minimum password length
  Expire password
  Number of valid days
  Number of invalid attempts before lockout

  Lockout duration in minutes

(NET0270: CAT II) The IAO/NSO will record the locally configured passwords used on communications devices and store them in a secured manner.

- The Uplogix LM does not store any passwords to any device outside of its database. These passwords are stored in a 3DES encrypted SHA-1 salted hash.

(NET0590: CAT III) The router administrator will ensure the CISCO enable secret password does not match any other username password, enable password, or any other enable secret password.

- N/A

(NET0600: CAT I) The router administrator will ensure passwords are not viewable when displaying the router configuration. Type 5 encryption must be used for the enable mode password (i.e., enable secret password).

- The Uplogix LM does not display the passwords when viewing any configuration.

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 Local Management from Uplogix, please visit us online or contact us for a technical demo and free evaluation of the benefits of Uplogix in your infrastructure:

- **uplogix.com/federal**
- Marco Martinez
mmartinez@uplogix.com

ABOUT UPLOGIX // **Uplogix provides the industry's first local management solution. Our co-located management platform automates routine administration, maintenance and recovery tasks—securely and regardless of network availability. In comparison, traditional network and systems management depends on the network, uses multiple tools, 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. For more information, please visit www.uplogix.com.

www.uplogix.com | Headquarters: 7600B N. Capital of Texas Hwy.
Suite 220, Austin, Texas 78731 | Sales 877.857.7077

UPLOGIX