UPLOGIX

UPLOGIX WHITE PAPER

Cellular Strategies for Connecting Local Managers to the Control Center While Out-of-Band

WWW.UPLOGIX.COM

Contents

Introduction

A key feature of the Uplogix Local Manager is its ability to spin up an out-of-band connection when the primary in-band network connection fails. When using a cellular modem, a Local Manager can take advantage of high-speed LTE data transfer and compatibility with multiple carriers. In the design phase of an Uplogix deployment, considerations must be made for how the Local Manager(s) will communicate with the Uplogix Control Center once the out-of-band connection is established.

This document explores the most common strategies for creating robust out-of-band connections, to include:

- Private APN (may peer directly with corporate network via service provider)
- Virtual Private Network
- Reverse SSH Tunnel
- Publicly Routable IP Address

Also included is a discussion of network placement options for the Uplogix Control Center. The primary goal is to allow inbound communication to the Control Center, so the out-of-band strategy will ultimately depend on where the Control Center lives in your network.

When using a cellular modem, a Local Manager can take advantage of high-speed LTE data transfer and compatibility with multiple carriers.

Strategy 1: Private APN

An Access Point Name (APN) defines how the Local Manager connects to the service provider's network. Typically, this is a common APN that gives the Local Manager access to a network from which they can route or initiate a VPN connection back to the corporate network. A Private APN removes the VPN requirement by peering directly with the corporate network. This is accomplished through a joint effort between the service provider and your network team to create an always-on VPN tunnel that allows the Local Manager to communicate with the Control Center.

Key benefits of a Private APN:

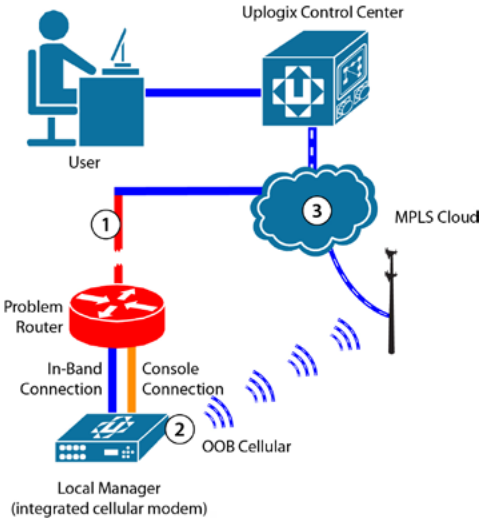
- Easier deployment of Uplogix Local Managers (no VPN settings to configure)
- No public internet component; Local Managers are directly connected to the corporate network
- Highly secure

Considerations:

- Expensive; setup and ongoing monthly costs
- May not be available with your service provider of choice
- If chosen, may prevent use of other service providers in locations
- Connectivity is dependent on service provider and internal peering

Diagram:

1. The in-band network connection fails due to a problem with a router.
2. The Local Manager detects the network outage and spins up its out-of-band connection to the cellular provider.
3. The service provider places the Local Manager in an MPLS cloud that peers with the corporate network where the Control Center is connected.



Strategy 2: Virtual Private Network

For customers with an existing VPN infrastructure, the Local Manager can act as a VPN client and create a secure tunnel back to the corporate network after spinning up its cellular connection. This allows the Local Manager to reach the Control Center as if it were still directly connected.

Key benefits of a Virtual Private Network:

- Uses existing VPN infrastructure
- Carrier-agnostic; connect from any routable provider network
- Secure, encrypted connection via IKEv2/IPSec
- Ability to whitelist incoming VPN connections from service provider network
- No recurring costs except for cellular data usage

Considerations:

- Initial setup required; Local Manager must be configured to access VPN server
- If VPN server is unavailable, isolation may occur

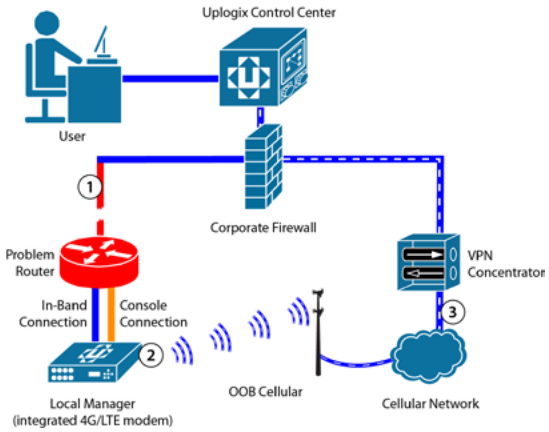


Diagram:

1. The in-band network connection fails due to a problem with a router.
2. The Local Manager detects the network outage and spins up its out-of-band connection to the cellular provider.
3. Once the PPP connection is built, a connection to the VPN server is established back to the corporate network.

Additional Resources: Click Here to Watch VPN Deep Dive

Strategy 3: Reverse SSH Tunnel

If a VPN connection is not available, either via a VPN server or Private APN, the Local Manager can still create a secure connection back to the Control Center using a Reverse SSH Tunnel. In this scenario, the Control Center would have to be reachable from outside the network, either through a NAT, firewall, or DMZ placement. After spinning up the out-of-band connection, the Local Manager creates a tunnel by initiating a reverse SSH connection to the Control Center. When a user opens an SSH connection to the Local Manager via the Control Center, the session is routed through the tunnel as well.

Key benefits of a Reverse SSH Tunnel:

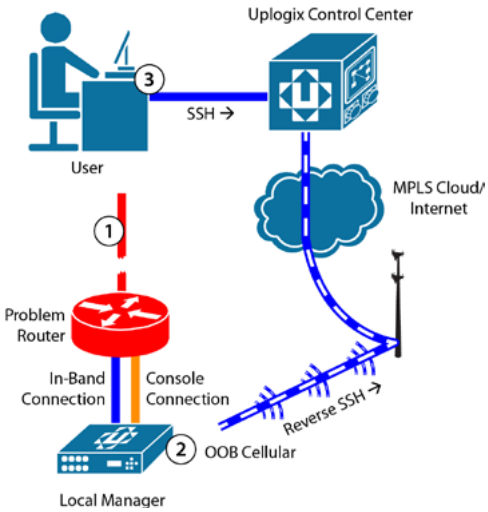
- Provides security without need for VPN or APN
- Incoming SSH connections can be limited to tunnel
- SSH sessions to Local Manager are twice-encrypted
- SSH/RSSH security
- SSH key management

Considerations:

- Control Center must be accessible from outside the network on TCP 8443 and TCP 2222, usually protected by an ACL or firewall whitelist
- VPN/APN would allow Control Center to remain inside corporate network without exposing public ports

Diagram:

1. The in-band network connection fails due to a problem with a router.
2. The Local Manager detects the network outage and spins up its out-of-band connection to the cellular provider. Once the PPP connection is built, a Reverse SSH Tunnel is established back to the Control Center.
3. The user initiates an SSH session via the SSH button on the Control Center, which connects them to the Local Manager over the established Reverse SSH Tunnel.



Additional Resources: [Click Here to Watch Reverse SSH Tunnel Deep Dive]

Strategy 4: Publicly Routable IP Address

If the Local Manager will not be able to communicate directly with the Control Center, it must find another way to inform users of its new IP address. Static IP addresses are recommended, as they can be stored on the Control Center for easy reference. If IP addresses are dynamically assigned, the Local Manager can be configured to send an email or SMS to subscribed users/groups. The built-in firewall can be used to limit incoming connections to those sourced from the corporate network, if desired.

Key benefits of a Publicly Routable IP Address:

- Operates regardless of corporate network status
- Access the Local Manager from anywhere
- Firewall can limit incoming connection sources
- SSH security

Considerations:

- Not as secure as other options
- Must know out-of-band IP address ahead of time or configure notifications

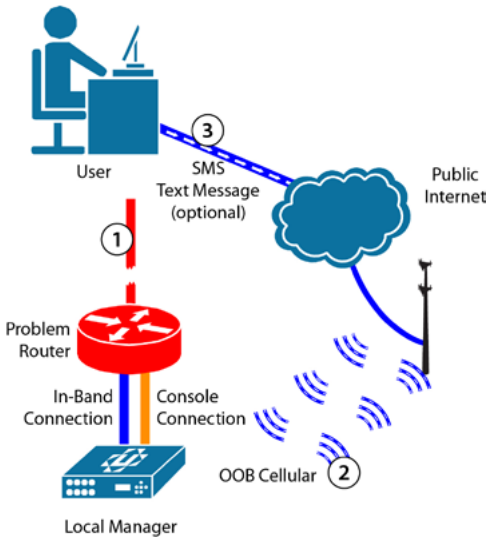


Diagram:

1. The in-band network connection fails due to a problem with a router.
2. The Local Manager detects the network outage and spins up its out-of-band connection to the cellular provider. Once the PPP connection is built, a notification is sent to inform users of out-of-band IP address.
3. (OPTIONAL) An SMS text message can be sent from the Control Center to initiate the out-of-band connection.

Additional Resources: Click Here to Watch Cellular OOB via SMS

Control Center Placement

The location of the Control Center inside your network will help decide which out-of-band strategy you'll need to use. Listed below are

- **Private Internal Network** | The most common placement of the Control Center is inside the corporate network. Outside traffic is not allowed, and the Local Manager must create a VPN connection or use a Private APN.

  Ideal for: Private APN, Virtual Private Network

- **NAT** | Network Address Translation is used to forward traffic from an outside IP address to the internal network where the Control Center sits. TCP port 8443 is used for heartbeat, while TCP port 2222 is used for Reverse SSH Tunnels. Incoming traffic can be limited to service providers' networks or specific IP addresses.

  Ideal for: Reverse SSH Tunnel

- **DMZ** | The Control Center is placed in a DMZ to separate it from the internal network. Outside traffic can still reach the Control Center on ports 8443 and 2222. Incoming traffic can be limited to service providers' networks or specific IP addresses.

  Ideal for: Reverse SSH Tunnel

- **Colocation Facility / Cloud** | Placing the Control Center at a colocation facility or in the cloud provides a safeguard against the loss of the corporate network. Local Managers operating out-of-band would still be able to communicate with the Control Center, and users would be able to access them from outside the corporate network.

  Ideal for: Reverse SSH Tunnel, Publicly Routable IP Address

ABOUT UPLOGIX // Uplogix provides the industry's most evolved out-of-band management solution. Our co-located 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 takes you beyond out-of-band.

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