Feature Guide: SSH Port Forwarding
Introduced in RMOS 4.0

Description
This document describes the capabilities and configuration of the SSH Port Forwarding feature in RMOS 4.0.

Features
- Access network services running on the dedicated or management IP addresses of a managed device.
- Multiple users on multiple workstations can use SSH Port Forwarding concurrently.

Required Privileges
Certain privileges are required to edit or view a port’s forward configuration.

- `show protocols forward` – Views the forwarding settings.
- `config protocols forward` – Configures the forwarding settings.
- `forward` – Allows the user to open an SSH session with a tunnel to the forwarded port.

Other Requirements
The Uplogix appliance will attempt to forward incoming TCP traffic regardless of whether the destination is configured properly or not. Ensure the managed device is configured to listen on the port specified.

If you will be using the CLI Applet on the Uplogix Control Center, a Java JRE must be installed.

Usage
Complete the following steps to configure SSH port forwarding for your managed device.

Configure IP Addresses
The managed device’s management or dedicated IP address must be configured on the Uplogix appliance. This can be configured using `config init` or `config info`.

```
[admin@UplogixAppliance (port1/1)]# config init
--- Enter New Values ---
description: []:
/////
management IP: []: 10.10.5.200
Configure dedicated ethernet port? (y/n) [y]:
Use DHCP? (y/n) [n]:
dedicated device IP []: 192.168.1.2
dedicated port IP []: 192.168.1.1
dedicated netmask: []: 255.255.255.252
speed/duplex: [auto]:
/////
Do you want to commit these changes? (y/n): y
```
Configure Port Forwarding

Use the `config protocols forward` command to open the port forwarding configuration editor.

```
[admin@UplogixAppliance (port1/1)]# config protocols forward
[forward]#
```

Once in the editor, you can use the `?` command to view a list of possible options.

```
[forward]# ?
Forward options are:
[no] management {port}
[no] dedicated {port}
[no] events
show
exit
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>[no]</code> management <code>{port}</code></td>
<td>Enables forwarding to the management IP address and the port specified. The <code>no</code> prefix will remove the forward. Example: To enable traffic forwarding to port 80 on the managed device’s management IP address, use <code>management 80</code>.</td>
</tr>
<tr>
<td><code>[no]</code> dedicated <code>{port}</code></td>
<td>Enables forwarding to the dedicated IP address and the port specified. The <code>no</code> prefix will remove the forward. Example: To enable traffic forwarding to port 80 on the managed device’s dedicated IP address, use <code>dedicated 80</code>.</td>
</tr>
<tr>
<td><code>[no]</code> events</td>
<td>Turns on event logging for traffic forwarding. The <code>no</code> prefix will turn off event logging.</td>
</tr>
<tr>
<td><code>show</code></td>
<td>Displays the current configuration.</td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Exits the configuration editor.</td>
</tr>
</tbody>
</table>

Note that the port specified should match the listening port on the managed device. If the managed device is running an SSH server on its management IP address, forwarding should be configured as `management 22`.

Creating a Tunnel

When connecting with an SSH client, you can specify an IP address or hostname and a port to create a tunnel. With forwarding enabled, the Uplogix appliance will allowing incoming users to establish a tunnel for which they have the `forward` privilege.

Hostnames will take the form of `portx_y`. For example, “port1/1” will specified as “port1_1” when creating the tunnel. This hostname will point to whichever IP address is configured for forwarding, either management or dedicated. If both addresses are configured for forwarding, an IP address should be used to avoid ambiguity.
SSH Client Examples

Uplogix Control Center CLI Applet

To use the CLI Applet on the Control Center, navigate to an appliance in the Inventory tree and click on the CLI button. Once the applet has loaded, click on Terminal in the menu bar and select Forward.

![Forward Settings](image)

In this example, the Uplogix appliance has already been configured to forward traffic to port 80 at the management IP address for the device on port 1/2. The window above allows you to select which tunnels to create. On an appliance with multiple forwards configured, the above list would be longer.

To create a tunnel, check the box next to the port forwards you wish to enable. Then, select a local port to use for forwarding. If random is selected, the applet will select a random port on the workstation.

Click Apply to save your settings.

![Forward Settings](image)

If the forward was successful, the drop down box will turn green. If a random port was requested, it will be displayed.

If the drop-down menu turns red, then the tunnel was not created. Double-check the forwarding settings on the target appliance. Ensure that forwarding is enabled and that the user has permission to forward to that port.

OpenSSH (Linux/Unix)

The ssh command on most Linux platforms provides for port forwarding with the –L option. For example, if port 1/3 is forwarding port 80 on its dedicated IP address and you want to map it locally to port 1080, use the following command:

```
# ssh -L 1080:port1_3:80 username@uplogixappliance
```

An IP address can also be used:

```
# ssh -L 1080:192.168.1.40:80 username@uplogixappliance
```
PuTTY 0.60:

To use PuTTY with SSH Port Forwarding, run the program and view the PuTTY Configuration window. On the left side of the window, select the Tunnels section under Connection -> SSH.

Configure port forwarding with the following options:

**Source Port:** A local port on the user’s workstation to forward the remote port to. For example, to make the remote port 80 appear locally as 1080, use 1080 as the source port.

**Destination:** A combination of the destination hostname (or IP address) and the remote port. For example, to create a tunnel to port 80 on port 1/1, use port1_1:80. If you would like to specify the IP address, use 192.168.1.1:80 (where 192.x.x.x is the management or dedicated IP address of the managed device).

The default options of **Local** and **Auto** will be sufficient for creating the tunnel.

Click **Add** to save the configuration for use with the next SSH connection. Once you click **Open** and establish a session, the tunnel will be created.

In this example, you would then be able to open a web browser to http://127.0.0.1:1080. Your request will be forwarded through the tunnel to the managed device on port 1/1.

**Notes**

- Access to forwarded ports is secured by mapping the requested hostname or IP address to a managed device on the appliance. If forwarding is enabled for two ports that have the same management or dedicated IP addresses, it may be possible for a user to access the forwarded port of a device that they do not have explicit permission for.
- If port forwarding is enabled on the Uplogix appliance CLI, a full heartbeat must occur before the forward menu will be available in the CLI applet.
- Any tunnels created with an SSH session will be destroyed if the session times out or is exited. To regain access to the tunnel, initiate another SSH session.
Receiving technical support

The Uplogix technical support website allows you to open support requests, browse the knowledge base and download software updates. You must have a user account to view this site. To create an account, send an email to support@uplogix.com with the subject line create account. Include this information:

- Organization name
- Account user’s email address
- User’s general contact information

You may request up to 10 accounts.

If you need to contact Uplogix customer support, please provide this information:

- Product model
- Serial number and software version (use the show version command from the RMOS command line)

Phone: 512-857-7070
Fax: 512-857-7002
Email: support@uplogix.com
URL: www.uplogix.com/support

Trademark and copyright information

Information in this document is subject to change without notice.

© 2009 Uplogix, Inc. All Rights Reserved. Uplogix, the Uplogix logo, and SurgicalRollback are trademarks of Uplogix, Inc. in the United States and other jurisdictions. All other marks referenced are those of their respective owners.