

XRIO

UBM QUICK START GUIDE

V.2.0 Updated September 2009

Xrio UBM

Quick Start Guide

UBM QUICK START GUIDE

CONTENTS

1.0	Getting Started	Page 04
1.1	Connecting to Your UBM Appliance	Page 05
1.2	Navigating the Web User Interface	Page 07
2.0	Considerations for Installation	Page 08
2.1	In Transparent (Drop-in) Mode	Page 09
2.2	In Gateway Mode	Page 10
2.3	In Router Mode	Page 11
3.0	Common Configuration Steps	Page 12
3.1	Configuring Link Interfaces	Page 13
3.1.1	Configuring a Static Link	Page 14
3.1.2	Verifying Static Link Connectivity	Page 15
3.2.1	Configuring a Dynamic Link	Page 16
3.2.2	Verifying Dynamic Link Connectivity	Page 17
3.3.1	Configuring a ADSL Link	Page 18
3.3.2	Verifying ADSL Connectivity	Page 19
4.0	Configuring LAN Interfaces	Page 20
5.0	Configuring Transparent Interfaces	Page 21
6.0	Configuring Traffic Policies	Page 22
6.1	Outbound Load Balancing	Page 23
6.2	VPN Bonding	Page 27
6.3	Link Bonding	Page 30
7.0	Obtaining Support	Page 32
7.1	Xrio Support Process	Page 33
7.2	Other Support Resources	Page 35

Connecting to your **UBM** Appliance

CONTENTS

1.0	Getting Started	
1.1	Connecting to Your UBM Appliance	
1.2	Navigating the Web User Interface	

1.0 GETTING STARTED

On your desk right now sits a powerful and feature packed Unified Bandwidth Management Appliance. It represents a single device to control, monitor and tune connectivity for your organisation.

Although the complexity of what the UBM appliance provides is high, our core goal is to make the configuration and management as simple and as straight-forward as possible.

This Quick Start Guide aims to provide you with what you need to know to get your UBM appliance up and running quickly.

1.0 GETTING STARTED

1.1 Connecting to Your UBM Appliance

There are a number of ways to make initial connection to your UBM appliance depending on your preference.

Method 1 – Connect to the UBM's Management IP Address

Your UBM appliance comes preconfigured with an IP address of 172.31.3.1 on its last numbered Ethernet Port. You can connect your PC directly to this Port using a cross-over cable, or by connecting the UBM directly in to your network switch.

Note that if you have multiple UBM appliances on the same LAN segment, the second device to boot will use 172.31.3.2 and so on, until it finds a spare IP address.

Try to Ping the UBM, if you are successful, proceed to configure using the web user interface at <https://172.31.3.1>

Method 2 – Setting Initial IP address by Serial Port or by Virtual Machine Console

If you prefer to use the provided serial cable you can login to the UBM appliance using your favourite terminal emulator with the following settings:

Baud Rate	115200
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None

Once connected, you should see a login prompt.

If you are deploying a VBOND appliance or UBMv you may need to set the initial IP address using the Virtual Machine's VGA console.

1.0 GETTING STARTED

1.1 Connecting to Your UBM Appliance

The default username and password for the console is **admin** and **123**.

To set your initial IP address, use the following command:

```
set ip address [IP]/[Netmask] [Gateway] [Port]
```

for example:

```
set ip addresss 192.168.1.10/24 192.168.120.1 1
```

Now continue to configure your UBM appliance using the web user interface using the specified IP address.

1.0 GETTING STARTED

1.2 Navigating the Web User Interface

The Web User Interface is where you will spend most of your time configuring and monitoring your UBM appliance. It is accessible on the previously configured IP address using secure http (https). The default username and password is **admin** and **password**.

The web user interface is divided into 4 sections:

Dashboard – Provides a quick glance at the current status of your UBM, including the status of your connected links, any alerts, and supplementary information such as IP addressing and serial numbers.

Configure – This is where most of your time will be spent, here you'll create and modify the various configuration objects within the UBM appliance.

Monitor – Provides monitoring and status information such as utilisation, information about your Links and log files.

Settings – Various settings attributed to the device itself, such as user maintenance and configuration backup, restore and reset.

Finally, there are a number of important options always visible throughout the web user interface:

Commit Configuration – Send's the current changes that were made to the UBM appliance and commits. It is essential to perform this operation before closing your browser otherwise your changes will be lost.

Write to Flash – If you are happy that the previous changes you committed were good, you should write these to the UBM appliances flash. This will keep the configuration across reboots.

Refresh Configuration – Used to request the current configuration from the UBM appliance.

Logout – Closes the session and redirects to the login prompt.

2.0 CONSIDERATIONS FOR INSTALLATION

The UBM can be deployed in a number of configurations in order to meet the requirements of your business. Although the UBM appliance provides several functionalities, the actual deployment to the network can be simplified in 3 deployment scenarios:

Transparent Mode,
Gateway Mode and
Router Mode (UBMi only).

2.0 CONSIDERATIONS FOR INSTALLATION

2.1 IN TRANSPARENT (DROP-IN) MODE

Transparent Mode

It's a common requirement to install the UBM appliance in an existing environment that has a single router/modem and a firewall. In this environment the firewall has a public IP address within the range of allocated by the chosen ISP. Following deployment of the UBM, this is to become the 'Transparent Link'.

To implement a transparent link you'll need a block of public IP's from your ISP, a block of 8 is the minimum; this is a /29 or 255.255.255.248 subnet mask.

The default gateway for the firewall should remain set to the router.

The UBM appliance is allocated a spare IP within the same range.

Note that the directly connected router and firewall will remember the MAC addresses of each device they are currently connected to (ARP), so a reboot (or clear the ARP cache) on both the router and the firewall is required before the UBM appliance will route traffic.

One of the benefits of Transparent Mode installations is the ability to use the Wire-Pass-through feature in some models. If the UBM appliance itself fails, 2 of the Ethernet ports are hard-wired automatically allowing the firewall/gateway to pass traffic to the upstream router. Of course all the functionality of the UBM appliance will be no longer available however connectivity will be possible using the transparent link.

2.0 CONSIDERATIONS FOR INSTALLATION

2.2 IN GATEWAY MODE

Gateway Mode

Deploying a UBM appliance in Gateway Mode is used in 2 common deployment scenarios, the most common of which is Link Bonding where the UBM appliance is the gateway for your Firewall, however it is possible to deploy the UBM appliance to be directly connected to your LAN.

For Link Bonding, Gateway Mode is used to route the 'Bonded IP range' to the LAN side of the UBM. This is usually a publically routable address allocated in the core of the ISP network however it is also possible to use this for IPVPN or MPLS type private networks.

Gateway is also useful for small branch office deployments where a firewall installation may not be desired. Whilst the UBM provides firewalling features as standard, this deployment is not recommended beyond a small branch or home office. For this, the UBM will perform Network Address Translation (NAT) and all PCs and servers should use the specified IP address of the UBM as their default gateway in the network. The UBM can also act as a basic DHCP server.

2.0 CONSIDERATIONS FOR INSTALLATION

2.3 IN ROUTER MODE

Router Mode

Released January 2009, our flagship UBMi product was launched featuring integrated ADSL interfaces. This negates the requirement for the use of external modem/routers and allows the provisioning of PSTN telephones directly in to the UBM appliance. This offers several benefits outlined later in this guide.


In practice one of the above Transparent Mode or Gateway modes is used whilst using the UBMi appliance in Router Mode, however the actual deployment looks a little different.

If you are planning to connect the UBM in gateway mode, that is, routing an IP subnet to the LAN side of the UBM appliance or you wish to connect directly to your LAN and perform Network Address Translation (NAT), simply create a LAN Interface outlined in [4.0 Configuring LAN Interfaces](#).

However, if you are planning to connect a firewall directly to the UBM appliance and wish to make use of IP addresses you have been allocated on one of the connected links, you should create a Transparent Interface.

Usually firewalls or gateway devices do not understand the use of multiple IP subnets or gateways and so it is a requirement to present an IP and gateway as if there was just a single link.

Now, when the firewall tries to route traffic to its gateway, the UBM will intercept and apply the traffic policies that were specified later in this guide. This could be bonding or load balancing over multiple links or even redirect to another link, whilst appearing to the firewall that there is a single link and gateway.



The First Steps In Your **UBM** Deployment

CONTENTS

3.0 Common Configuration Steps

3.1 Configuring Link Interfaces

3.0 Common Configuration Steps

3.1 Configuring Link Interfaces

The first step in any UBM deployment should be to configure Link Interfaces. These are the Wide Area Network Circuits that are connected to your UBM appliance.

There are 5 types of Link available to configure:

Static

- These are statically assigned IP addresses, usually publicly routable IP's assigned by the Service Provider.

Dynamic

- IP addresses that are assigned via DHCP, should only be used if required by the Service Provider.

PPPoE

- Dynamic Dial Link that require the UBM to authenticate itself before an IP address is assigned.

ADSL

- Links that use the UBM's built-in ADSL interfaces, properties vary depending on the type of ADSL link.

Mobile

- 3G Links connected to the UBM's USB ports.

To Access the Link configuration go to the Configure Tab and choose Link in the Interfaces group.

3.1 Configuring Link Interfaces

3.1.1 Configuring a Static Link

1. From the Operations Toolbar, click Add a Link, the properties for this Link will appear.
2. Choose the Port of which this Link is connected to, this is the physical port on the UBM appliance. Depending on the model, Port1 may be labelled as eth0.
3. Enter the download and upload bandwidth for this link. For example a 1mbps Link should be entered as 1024.
4. Enter the Health check IP for this Link this is the IP address the UBM appliance will use to verify status. Usually this is a DNS server or a core router within the ISP network.
5. From the Interface Type list select Static.
6. For Static Links, we must finally assign the IP addresses. The Endpoint IP should be the address you are allocating the UBM appliance itself. This is entered using CIDR notation for example 80.0.0.2/29. The UBM will calculate what it thinks should be the Gateway address based on the Endpoint IP you entered, if it appears incorrect, you should change it.
7. Apply this Link, Commit Configuration and Write to Flash.

3.1 Configuring Link Interfaces

3.1.2 Verifying Static Link Connectivity

At this stage we should verify that connectivity is established by following the steps outline below.

- a. If you configured the Port and IP addressing correctly there is a good chance that the Link will be ready and working. Go to the Monitor tab and choose the Link Monitor. Verify the Link is showing a Green traffic light, you are ready to proceed with the rest of the configuration. If you have a Red traffic light, continue with the following steps.
- b. SSH to the UBM appliance and login with the admin user.
- c. Type 'show arp' and verify you have an ARP entry for your router. If you don't you probably don't have physical connectivity.
- d. Now type 'show status ports' and verify the port shows 'Link detected: yes'. If it does not, it's likely you have a problem with the cabling to the router. If the router has an integrated switch then you should use a standard CAT5 cable between the UBM's Ethernet port and the router, however if the router has just a single LAN port, it's likely you'll need a cross-over CAT5 cable.
- e. Once you have physical connectivity and have an ARP entry for the router, you should proceed to verify the Link has IP connectivity by using the 'show status links' command.

If all these checks are successful you are then ready to proceed with the rest of the configuration.

3.0 Configuring Link Interfaces

3.2.1 Configuring a Dynamic Link

1. From the Operations Toolbar, click Add a Link, the properties for this link will appear.
2. Choose the Port of which this Link is connected to, this is the physical port on the UBM appliance. Depending on the model, Port1 may be labelled as eth0.
3. Enter the download and upload bandwidth for this link. For example a 1mbps Link should be entered as 1024.
4. Enter the Health check IP for this Link, this is the IP address the UBM appliance will use to verify status. Usually this is a DNS server or a core router within the ISP network.
5. From the Interface Type list select Dynamic.
6. Apply this Link, Commit Configuration and Write to Flash.

3.0 Configuring Link Interfaces

3.2.2 Verifying Dynamic Link Connectivity

At this stage we should verify that connectivity is established by following the steps outline below.

- a. Go to the Monitor tab and choose the Link Monitor. Verify the Link is showing a Green traffic light, you are ready to proceed with the rest of the configuration. If you have a Red traffic light, follow the steps outlined in [3.1.2 Verifying Static Link Connectivity](#).

3. Configuring Link Interfaces

3.3.1 Configuring a ADSL Link

1. First we must configure the ADSL Interface by choosing ADSL from the Interfaces group in the left navigation.
2. Hover over the ADSL link you wish to configure and click Edit. The ADSL Interface properties will appear.
3. Choose the Protocol, Modulation, Encapsulation, VPI and VCI used by the Service Provider.
4. Now you have configured your ADSL ports, we can now create the associated Link. Choose Link from the Interfaces group in the left navigation and add a Link.
5. For the Port choose the ADSL Interface you just configured. Depending on the type of ADSL port you configured, you will be presented with different options when creating the Link.

If the ADSL port type is PPPoA or PPPoE, you'll be asked to enter the username and password to authenticate with the providers RADIUS server.

If the ADSL port type is Bridged Ethernet or Routed IP, you'll be asked to enter the IP address and gateway that is allocated by the provider.

6. Now complete the rest of the required configuration for the Link, including the expected download/upload speed, and Health check IP.
7. Apply this Link, Commit Configuration and Write to Flash.

3.0 Configuring Link Interfaces

3.3.2 Verifying ADSL Connectivity

At this stage we should verify that connectivity is established by following the steps outline below.

a. **Do we have ADSL line sync?**

On the Monitor tab, click ADSL Port Status, and verify that the ADSL port reports 'connected' and the various information is in order such as the actual sync speeds.

b. **Does PPP establish?**

On the Monitor tab, click Dynamic Link Status. Here you should verify that the Link is 'Active' and if you are using PPPoA or PPPoE that you have received an IP address and gateway from the provider.

c. **Does the Link have IP connectivity?**

On the Monitor click Dynamic Link Status. The final check here is to verify that you have a green traffic light in the top right hand corner of each Link. If you have both ADSL line sync and PPP is established the UBM appliance will then check that it can reach IP connectivity further into the network. This is done using the Health-check IP specified in the Link configuration and the global Health-check settings specified in the System Parameters screen.

If all 3 checks are successful you are then ready to proceed with the rest of the configuration.

4.0 Configuring LAN Interfaces

LAN Interfaces are required when the UBM appliance is to be used as a gateway device by a Local Area Network or an upstream firewall or router. Uses of LAN Interfaces are explained earlier in this guide.

To Access the LAN Interface configuration, go to the Configure Tab and choose LAN in the Interfaces group.

1. From the Operations Toolbar, click Add an Interface, the properties for this Interface will appear.
2. Choose the Port of which this LAN Interface is connected to, this is the physical port on the UBM appliance. Depending on the model, Port1 may be labelled as eth0.
3. Now enter the Endpoint IP, this is the IP address you want to assign to the LAN port itself and is entered using CIDR notation for example 192.168.1.254/24.
4. Apply this Interface.

5.0 CONFIGURING TRANSPARENT INTERFACES

Transparent Interfaces provide the ability to install the UBM appliance in an existing network, essentially passing through an IP address range that resides on a Link to a device connected on the UBM's LAN.

To Access the Transparent Interface configuration, go to the Configure Tab and choose Transparent in the Interfaces group.

1. From the Operations Toolbar, click Add an Interface, the properties for this Interface will appear.
2. Choose the Link that you are allocating as the transparent link.
3. Choose the Port of which this LAN Interface is connected to, this is the physical port on the UBM appliance. Depending on the model, Port1 may be labelled as eth0.
4. Finally you must now choose the IP addresses residing on this Port that is the IP addresses that the UBM will pass-through to the Port you selected in Step 3.
5. Apply this Interface.

When implementing Transparent Interfaces for use in an existing network, it is very important to clear to ARP cache on the Gateway Router of the Link you specified and also the devices that are connected to the Port you specified, usually this is a Firewall. Some routers and firewalls do not have an ARP reset option and so a reboot will be required. If ARP cache is not cleared, traffic will not route out of the UBM appliance.

Engine Room Of Your **UBM** Appliance

CONTENTS

6.0	Configuring Traffic Policies
6.1	Outbound Load Balancing
6.2	VPN Bonding
6.3	LINK Bonding

6.0 Configuring Traffic Policies

Traffic Policies are the engine room of the UBM appliance. They are used to tell the UBM appliance how it should route traffic in and out of the network. In-depth detail regarding Traffic Policies is beyond the scope of this guide, however here we will describe the most common deployment scenarios you are likely to require.

When building Traffic Policies you'll need to become familiar with the following configurations objects:

Address Aliases – Used to map IP addresses to names to provide enhanced readability. They have an associated type such as Source Subnet or Destination Subnet.

Interface Teams – Used to group together multiple Links or Virtual Tunnels using a specific Traffic Distribution Algorithm.

Traffic Distribution Algorithms

Distribute Connections – An intelligent load balancing algorithm that distributes outbound connections as they arrive at the UBM appliance.

Sticky Connections – Similar to Distribute Connections, but will remember the destination IP and port number and ensure they are always directed to the same link. This is useful for applications such as online banking which require IP persistence.

6.0 Configuring Traffic Policies

Static Bonding – Distributes traffic on a per packet basis, effectively joining multiple links together to function as one. Bonding requires Virtual Tunnels to be created and will not be visible for Teams that use Links.

Dynamic Bonding – Similar to Static Bonding however the UBM appliance (the Central and CPE) actively monitor the performance of each link and notifies the other side in order to adjust the packet flow. This is useful for Links that fluctuate regularly.

Service Definitions – These are used to define application protocols. Any combination of TCP, UDP or custom protocols can be used.

Traffic Policies – Bring together all the objects listed above to define traffic flow. This can be any combination of load balancing, bonding or forcing traffic to a specific link. Policies are built up with the following properties:

Source – The local IP subnet from where traffic originates. These are defined by creating a Source Subnet Address Alias.

Destination – The remote IP subnet where traffic is destined. These are defined by creating a Remote Subnet or Remote IP Address Alias.

Service – The name of the Service Definition object that you want to match.

Team – The name of the Interface Team or Link you want to direct the traffic to.

Translate – Specifies if Network Address Translation (NAT) is applied to this traffic using the following modes:

Auto – Translates using the Endpoint IP specified in each Link specified in the Team

Off – No translation is done, mostly required for bonded Teams.

Manual – Allows specific control of which Links are translated and using which IP addresses. This is only used in advanced deployments.

6.0 Configuring Traffic Policies

6.1 **Outbound Load Balancing**

This is the simplest functionality that your UBM appliance can provide and consists of building a Team of Links that you want to load balance across. Outbound Load Balancing can be used together with Gateway, Router or Transparent Mode.

In Load Balancing mode the UBM appliance distributes traffic across multiple Links on a connection by connection basis. That is, when a client on the Local Area Network attempts to establish a new connection to a host on the Internet (or Wide Area Network) the UBM will use its traffic distribution algorithms to decide the best Link in which to direct this connection to. It is important to note that this connection can only consume the maximum bandwidth available to the Link of which the traffic is directed.

6.0 Configuring Traffic Policies

6.1 Outbound Load Balancing

To deploy the UBM appliance to perform Outbound Load Balancing you are required to follow these steps:

1. Configure the Interfaces described in the sections above.
2. Create an Interface Team, choosing the Links you want to include and the desired algorithm.
3. Create a Policy, specifying the following properties:

Source	The source subnet of your LAN/Firewall
Destination	Any
Service	Any
Team	The name of the Team you created in step 2
Translate	Auto

4. Apply the Team, Commit Configuration and Write to Flash.

6.0 Configuring Traffic Policies

6.2 VPN Bonding

VPN Bonding - Used to implement increased bandwidth and failover capability for site-to-site VPN's such as IPSEC or L2TP. VPN Bonding has been designed to be deployed into an existing VPN infrastructure without the need to reconfigure Firewall/VPN appliances. The UBM appliance is installed in Transparent Mode enabling the Firewall/VPN appliance to maintain its existing IP addressing and default gateway.

The UBM appliance is then configured to intercept the VPN traffic through configuration of Policies and distribute traffic over multiple links simultaneously. This results in the combined bandwidth of all specified links being available to the VPN connection for both incoming and outgoing traffic.

To enable 'bonding', Virtual Tunnels are created between the local and remote UBM appliances to encapsulate the bonded packets. Usually in a VPN bonding deployment, the remote appliance has the same amount of links as the local appliance, this is not a requirement however there are some rules you need to follow.

6.0 Configuring Traffic Policies

6.2 VPN Bonding

Bonding Configuration Recommendations

- ✓ It is common for a central site to have a single large Link, and remote sites to have multiple, this is supported.
- ✓ You may want to bond 2 Links at one site, with 4 Links at another, this is supported.
- × It is not recommended to bond an odd number of Links such as 3 Links to 2 Links. This will cause contention of bandwidth and impact overall performance.

Required Steps

1. Create Virtual Tunnels for each of the Link you want to bond specifying the following properties:

Local Endpoint	The Link from which to create the Tunnel
Remote Endpoint	The Endpoint IP address of the Remote Link
Local Virtual IP	An IP address used for verifying the Tunnel status
Remote Virtual IP	The IP address specified as the Local Virtual IP on the Remote appliance
Bandwidth	The download and upload speed across the Tunnel
Encrypt Tunnel	Don't use if you encryption is done on the Firewall.

2. Create an Interface Team, choosing the Virtual Tunnels you want to include and the desired algorithm, Static Bonding or Dynamic Bonding.

6.0 Configuring Traffic Policies

6.2 VPN Bonding

3. Create a Policy, specifying the following properties:

Source	The source subnet of your LAN/Firewall
Destination	The IP address of the Remote Firewall
Service	Any
Team	The name of the Team you created in step 2
Translate	Off

3. Apply the Team, Commit Configuration and Write to Flash.

6.0 Configuring Traffic Policies

6.3 Link Bonding

Link Bonding is used by Service Providers, Telco's and ISP's to provide increased bandwidth and reliability to a customer site through the provisioning of multiple, individual circuits. To the network, this bonded circuit has the characteristics of a single link, a single IP address range and a single cable connecting to the customers' network or firewall. All available bandwidth is multiplied both downstream and upstream.

Just as VPN Bonding, Virtual Tunnels are created for each Link you want to bond however the remote end is located in a datacenter with adequate bandwidth to support the requirements of the remotes sites of which it is connected.

6.0 Configuring Traffic Policies

6.3 Link Bonding

Required Steps

1. Create Virtual Tunnels for each of the Links you want to bond specifying the following properties:

Local Endpoint	The Link from which to create the Tunnel
Remote Endpoint	The IP address of the datacenter appliance
Local Virtual IP	An IP address used for verifying the Tunnel status
Remote Virtual IP	The IP address specified as the Local Virtual IP on the Remote appliance
Bandwidth	The download and upload speed across the Tunnel
Encrypt Tunnel	Not recommended for performance

2. Create an Interface Team, choosing the Virtual Tunnels you want to include and the desired algorithm, Static Bonding or Dynamic Bonding.
3. Create a Policy, specifying the following properties:

Source	The subnet allocated to the customer premise.
Destination	Any
Service	Any
Team	The name of the Team you created in step 2
Translate	Off

4. Apply the Team, Commit Configuration and Write to Flash.

Xrio Offers Professional Support Services

CONTENTS

7.0	Obtaining Support
7.1	Xrio Support Process

7.0 Obtaining Support

7.1 Xrio Support Process

Technical Support is provided exclusively via our online ticket system at <http://helpdesk.xrio.com>
In order to create a ticket, you are first required to create a login. All open and closed tickets are logged under your account.

If you have a System Assurance Contract your ticket will be responded to within 4 working hours between 9.00am to 5.00pm GMT Monday to Friday.

If you do not have a System Assurance Contract, you will be required to purchase a pay-as-you-go support pack from our online store at <http://store.xrio.com>

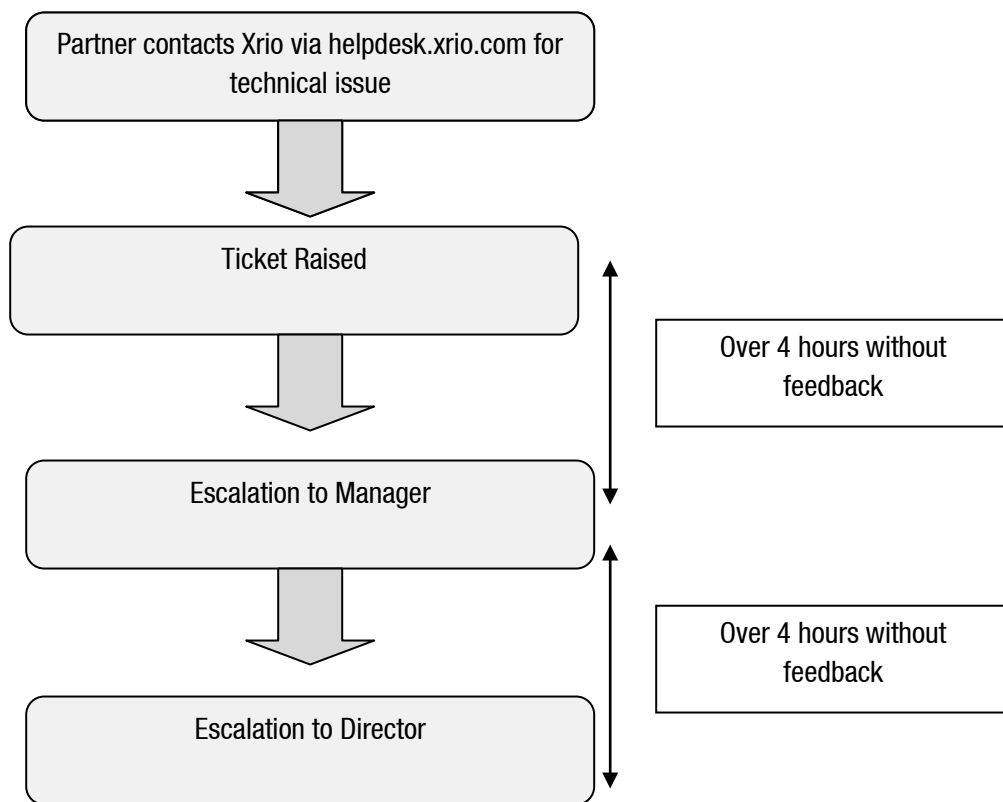
7.0 Obtaining Support

7.2 Xrio Support Process

This section describes the procedure followed by the partner support when responding to a fault and the escalation measures that may result from that.

We have strict procedures in place to ensure we are effective in dealing with such situations and to reassure our customers that there is a defined plan of action should a fault occur.

We employ a twin stream approach whereby minor incidents are dealt with by one layer of Support Technicians and more serious and urgent incidents are the responsibility of a second group who will escalate within the specific Technical Support functions as appropriate.



7.0 Obtaining Support

7.3 Other Support Resources

Xrio Knowledgebase

Online self-help resources are available from our Knowledgebase at <http://kb.xrio.com> Here you can find documents answering the most commonly asked questions.

Setup Videos

<http://www.xrio.com/support/videos/>