KerioControl AI

Hardware Transition Guide

This guide helps you migrate from legacy GFI KerioControl hardware to new generation appliances (NG120/320/520/521/700) with minimal downtime.

Hardware Platform Overview & Comparison

The new generation GFI KerioControl hardware (NG120, NG320, NG520/521, NG700) offers significant performance upgrades over legacy models (NG110, NG310, NG510/511) in CPU, RAM, storage, and throughput.

> ⚠ Critical Consideration
>
> A paramount consideration for any migration is the **physical port layout difference** between old and new appliances. This is especially critical when moving from models with more ports in use to models with fewer ports. Such reductions necessitate network redesign, often involving VLAN implementation, to consolidate network segments onto fewer physical interfaces while preserving existing network architecture and functionality.

Key Port Differences (Direct Successors)

Old Model - Port	New Model - Port	Port Differences
NG110 - 3xGbE	NG120 - 4xGbE	+1 port
NG310 - 6xGbE, 2xSFP	NG320 - 8x 2.5-GbE, 2x SFP	+2 ports
NG510 - 6xGbE	NG520 - 8x2.5GbE	+2 2.5GbE Ports, Faster Ports
NG511 - 14xGbE	NG521 - 8x2.5GbE, 8x 1GbE RJ45	+2 more ports
N/A	NG700 - 4x10GbE SFP	-

Prerequisites and Version Compatibility

Migration Planning Checklist:

- ☐ Verify Current Hardware & Software: Hardware model, software version, resource usage.
- ☐ Document Network Topology: Interface assignments, IP schemes (manual IPs import, DHCP IPs will change), VLANs, static routes.

> **Important:** IP addresses assigned to interfaces will only be imported to the new hardware if they are in manual configuration mode. Interfaces with automatic (DHCP) mode will receive new IP addresses from DHCP server.

- □ **Assess New Hardware:** Confirm suitability, compare port counts, plan for port reduction (VLANs) if needed.
- □ **Schedule Maintenance Window:** Communicate downtime.
- □ **Prepare Backup Strategy:** Full configuration backup stored securely.

GFI KerioControl v10

The new generation hardware models (NG120, NG320, NG520/521, NG700) leverage the GFI KerioControl v10 for enhanced compatibility and ensuring that GFI KerioControl remains future-proof and supports current and emerging network interface technologies.

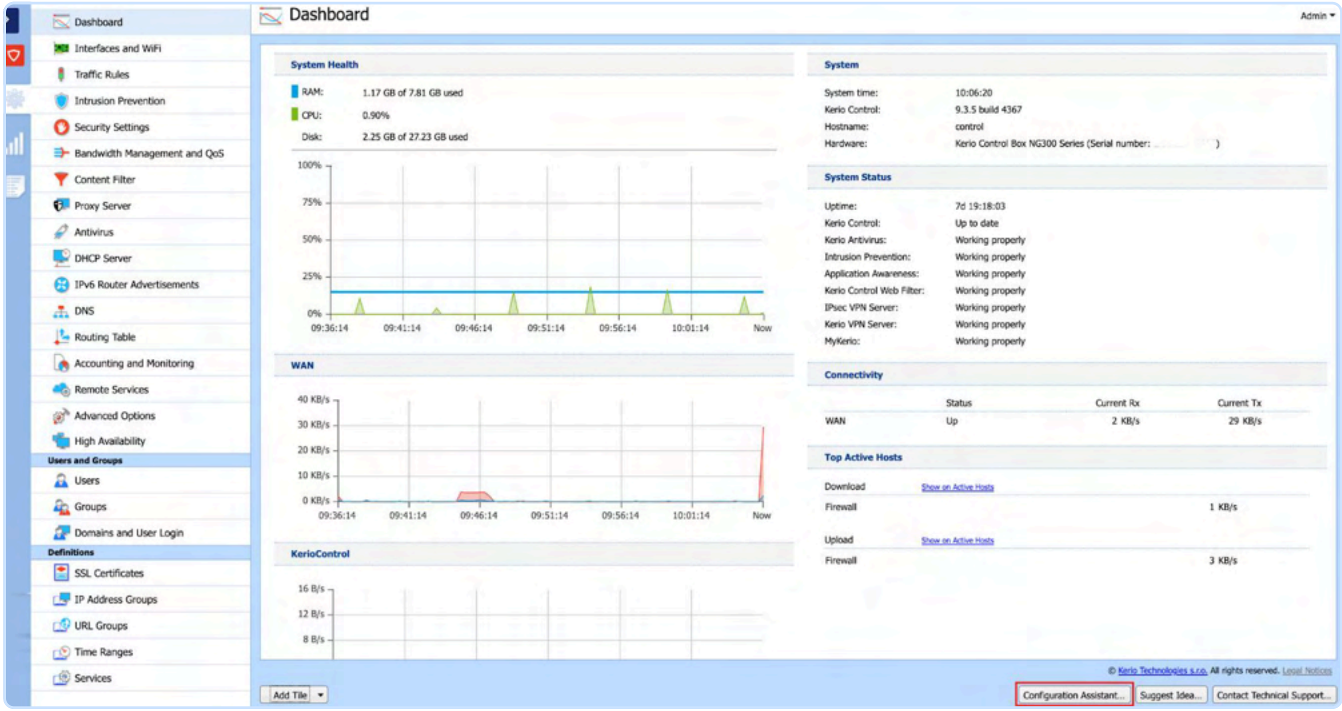
> **Critical Note:** If your current GFI KerioControl deployment is running a version earlier than version 9.4.5, you must upgrade your software version before attempting the hardware migration.

Configuration Backup Procedures

Creating a reliable and complete configuration backup is the most critical step before any hardware migration. This backup file will be used to restore your GFI KerioControl settings onto the new appliance.

Method 1: Web Administration Interface

This is a straightforward method for creating a full configuration backup.



System Health

RAM: 1.17 GB of 7.81 GB used
CPU: 0.90%
Disk: 2.25 GB of 27.23 GB used

WAN

KerioControl

System

System time: 10:06:20
Kerio Control: 9.3.5 build 4367
Hostname: control
Hardware: Kerio Control Box NG300 Series (Serial number: [redacted])

System Status

Uptime: 7d 19:18:03
Kerio Control: Up to date
Kerio Antivirus: Working properly
Intrusion Prevention: Working properly
Application Awareness: Working properly
Kerio Control Web Filter: Working properly
IPsec VPN Server: Working properly
Kerio VPN Server: Working properly
MyKerio: Working properly

Connectivity

	Status	Current Rx	Current Tx
WAN	Up	2 KB/s	29 KB/s

Top Active Hosts

Download Show on Active Hosts
Firewall 1 KB/s

Upload Show on Active Hosts
Firewall 3 KB/s

© Kerio Technologies s.r.o. All rights reserved. Legal Notices

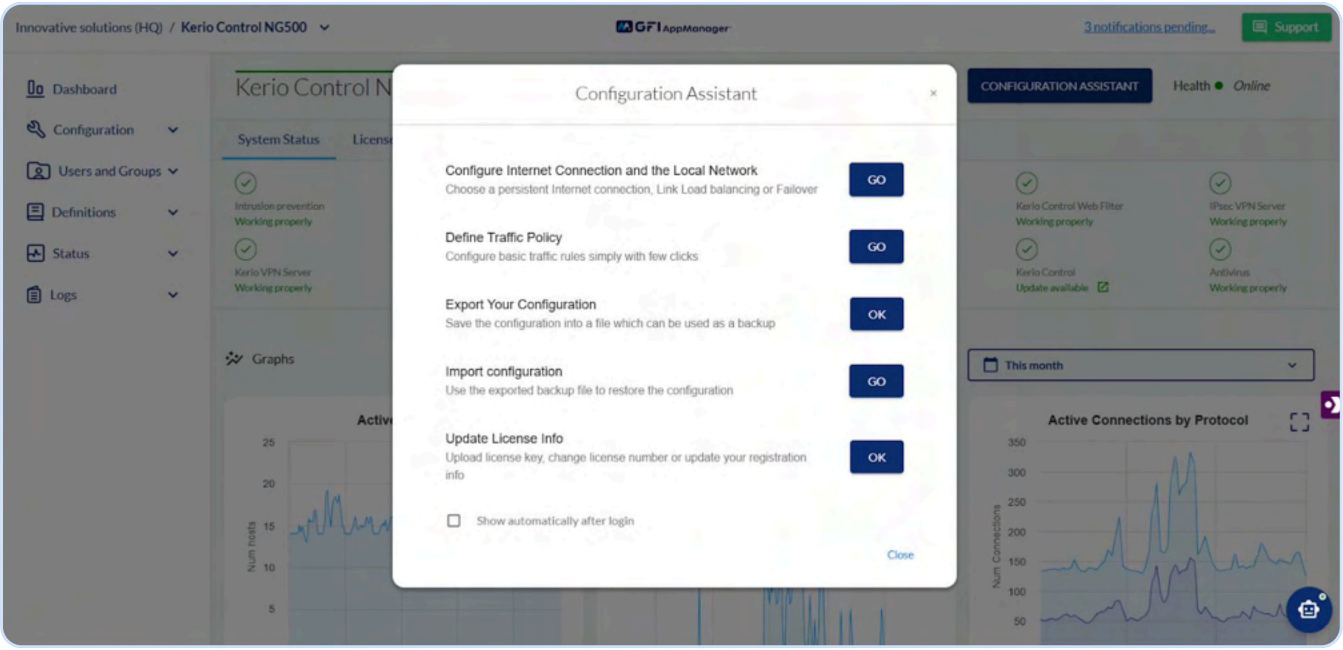
1. Log in to the administration interface of your original hardware appliance.
2. Go to the Dashboard.
3. Click “Configuration Assistant”.
4. In the Configuration Assistant dialog box, click “Export your configuration”.
5. In the Export Configuration dialog box, select all items.

   > **Note:** Ensure “Include traffic rules and user authentication data” is selected to capture all essential settings.

6. Click “Export”.
7. Your browser will download the GFI KerioControl backup file with the configuration. The backup file has the following format: ControlBackup_YYYY_MM_DD_HH_MM_SS.tar.gz.
8. Save this .tar.gz file to at least two secure, off-device locations (e.g., a network share, a USB drive, or cloud storage).

Method 2 GFI AppManager Backup *(Recommended)*

If your GFI KerioControl appliance is registered to GFI AppManager, you can essentially do the backup same way through the centralized management interface.


Innovative solutions (HQ) / Kerio Control NG500
GFI AppManager
3 notifications pending...
Support
Dashboard
Configuration
Users and Groups
Definitions
Status
Logs
Kerio Control N
System Status
License
CONFIGURATION ASSISTANT
Health Online
Intrusion prevention Working properly
Kerio VPN Server Working properly
Kerio Control Web Filter Working properly
IPsec VPN Server Working properly
Kerio Control Update available
Antivirus Working properly
Graphs
This month
Active Connections by Protocol
Num hosts
Num Connections

Configuration Assistant

Configure Internet Connection and the Local Network
Choose a persistent Internet connection, Link Load balancing or Failover
GO

Define Traffic Policy
Configure basic traffic rules simply with few clicks
GO

Export Your Configuration
Save the configuration into a file which can be used as a backup
OK

Import configuration
Use the exported backup file to restore the configuration
GO

Update License Info
Upload license key, change license number or update your registration info
OK

□ Show automatically after login

Close

Migration Process Overview

High-Level Migration Steps:

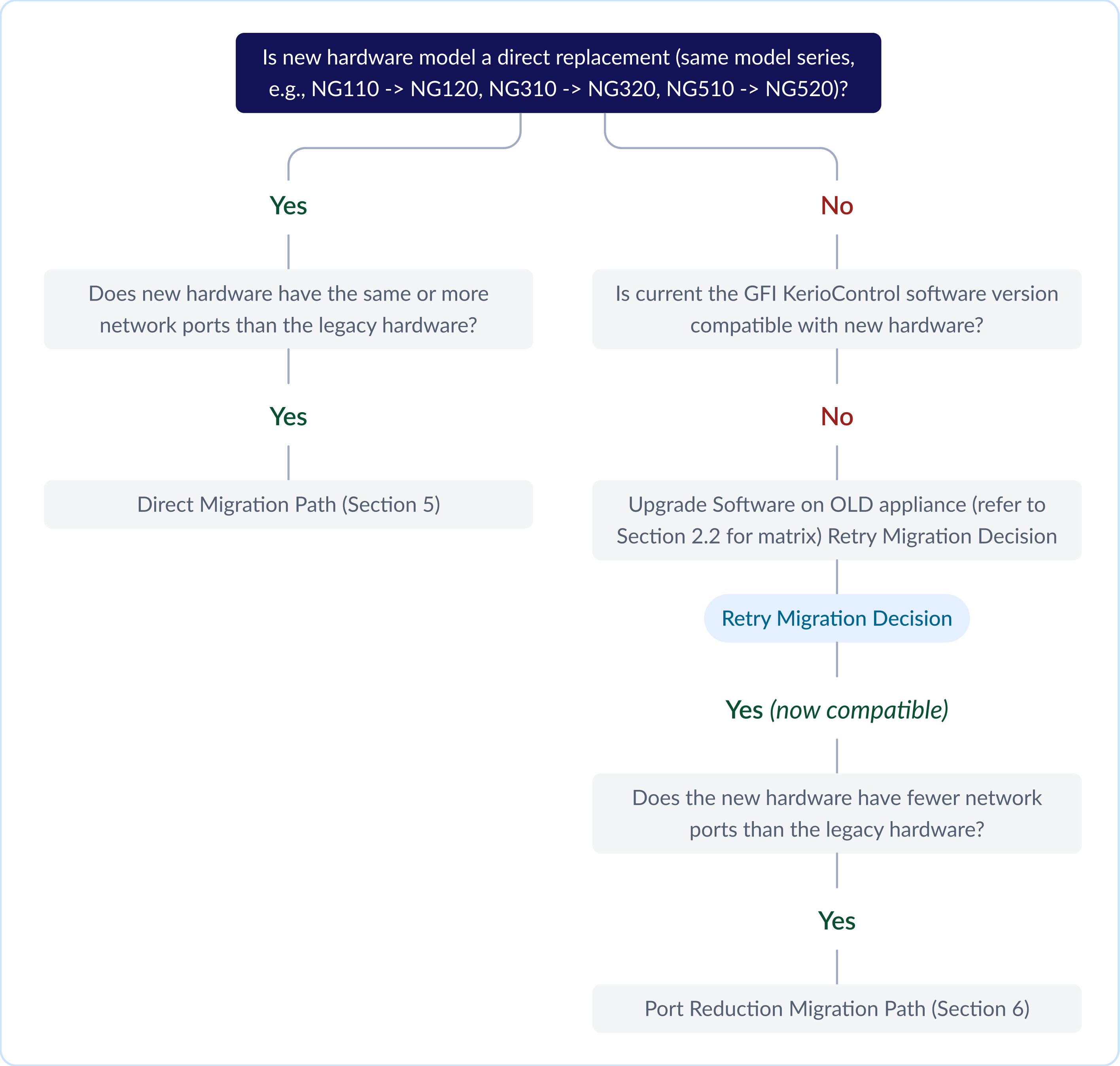
1. Export configuration from the original appliance (see section 3).
2. Connect the new appliance to the internet.
3. Activate the license on the new appliance.
4. Import the configuration to the new appliance.
5. Physically replace the original hardware appliance.

Post-Import Verification

After importing the configuration, verify that all critical components have been successfully transferred:

- **Policies:** Ensure all firewall rules, VPN settings, and user accounts are present and functional.
- **VPN Connections:** Test client-to-site and site-to-site VPN tunnels to confirm connectivity.
- **Active Directory (AD) Integration:** If using AD, ensure the new appliance is connected to the LAN port and can communicate with the AD server.

Migration Decision Tree:



Is new hardware model a direct replacement (same model series, e.g., NG110 -> NG120, NG310 -> NG320, NG510 -> NG520)?

Yes

Does new hardware have the same or more network ports than the legacy hardware?

Yes

Direct Migration Path (Section 5)

No

Is current the GFI KerioControl software version compatible with new hardware?

No

Upgrade Software on OLD appliance (refer to Section 2.2 for matrix) Retry Migration Decision

Retry Migration Decision

Yes *(now compatible)*

Does the new hardware have fewer network ports than the legacy hardware?

Yes

Port Reduction Migration Path (Section 6)

Detailed Migration Steps Direct Migration 🔗

This path is suitable when the new hardware has an equal or greater number of network ports compared to the old appliance, allowing for a straightforward configuration transfer.

Physical Installation of New Hardware

1. Unpack and Install the new GFI KerioControl hardware appliance.
2. DO NOT connect network cables to the new appliance yet. This is crucial to prevent IP conflicts or network disruption.
3. Connect only the power cable and the console/management port (if applicable for initial setup).
4. Power on the new device and allow it to complete its initial boot sequence.

Connecting and Registering the New GFI KerioControl

The DHCP server in the GFI KerioControl hardware appliance is enabled by default.

1. Connect a laptop directly to the LAN port of the new appliance (typically eth0 or LAN1). The default IP address for management is usually https://10.10.10.1/admin.
2. Access the administration interface via your web browser.
3. Log in with the default credentials (Username: Admin, Password: admin). You will be prompted to change the password immediately.
4. Complete with the Activation Wizard that will appear automatically. If the new appliance does not have internet access, the license activation will fail. In such cases, you can obtain a license key file from GFI Customer Care and manually upload it during the activation process.
5. At this point, the hardware appliance is running, and users connected in the GFI KerioControl network will see a notification page every 2 minutes until you activate GFI KerioControl.

Importing Configuration to the New GFI KerioControl

Now you can import the previously exported configuration:

1. Go to the Dashboard, click “Configuration Assistant”.
2. In the Configuration Assistant dialog box, click “Import configuration”.
3. In the Import Configuration wizard, click “Upload configuration file”.

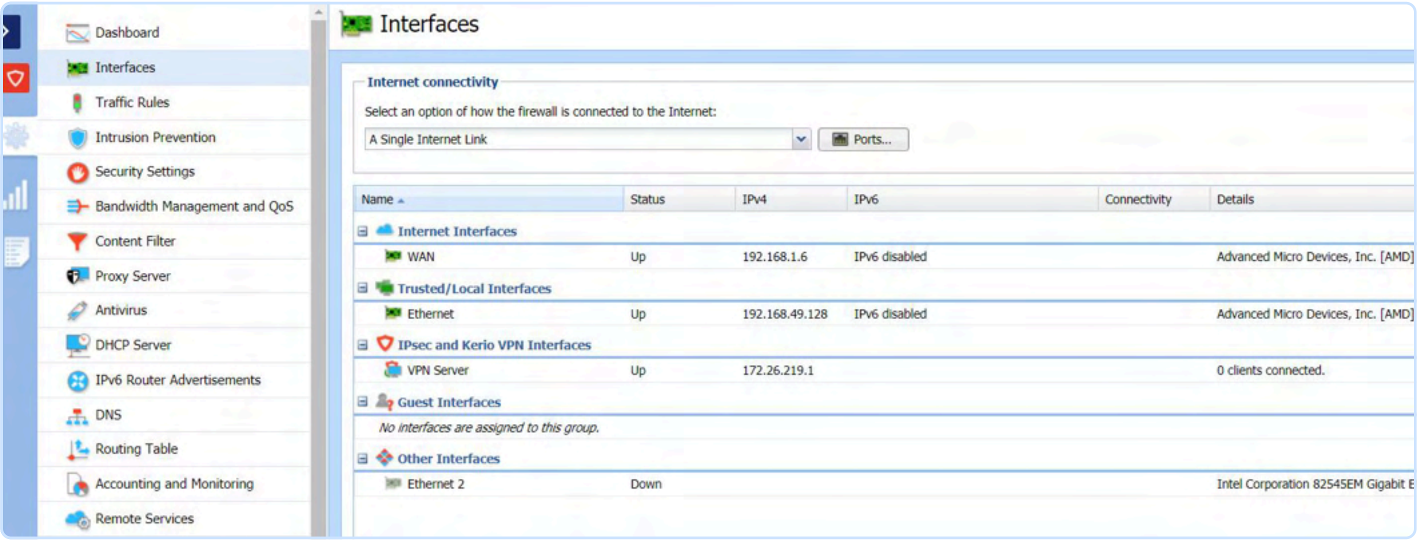
4. Select your backup file (e.g., ControlBackup_2016_03_03_14_44_45.tar.gz) and click “Open”.
5. Select “Restore from backup to completely replace all the configuration files”.
6. Click “Next”.

The system will now pair the imported network interfaces with the real interfaces on the appliance. If you need to change the pairing:

1. Double-click the interface you want to change.
2. In the Select Interface dialog box, double-click the interface you want to pair. From now on, the interface from the original appliance is paired with the new one.
3. If you cannot pair the interfaces during this process, you can edit them later in the Interfaces section of the administration interface.
4. Click “Next” to proceed.
5. Read the notes in the last step of the wizard and click “Finish”. GFI KerioControl imports the configuration and restarts.
6. More information on setting up interfaces.

Handling Port Mismatches and VLANs *(Port Reduction Migration)*

This path is necessary when the new hardware has fewer physical network ports than the original appliance. This scenario requires a more involved network redesign and often relies on VLAN implementation.



Internet connectivity

Select an option of how the firewall is connected to the Internet: A Single Internet Link

Name	Status	IPv4	IPv6	Connectivity	Details
Internet Interfaces					
WAN	Up	192.168.1.6	IPv6 disabled		Advanced Micro Devices, Inc. [AMD]
Trusted/Local Interfaces					
Ethernet	Up	192.168.49.128	IPv6 disabled		Advanced Micro Devices, Inc. [AMD]
IPsec and Kerio VPN Interfaces					
VPN Server	Up	172.26.219.1			0 clients connected.
Guest Interfaces					
No interfaces are assigned to this group.					
Other Interfaces					
Ethernet 2	Down				Intel Corporation 82545EM Gigabit E

Network Redesign Planning

Before touching any hardware, you must develop a detailed port mapping strategy. This typically involves consolidating multiple physical network segments onto fewer physical interfaces using VLANs.

Example: 14 ports to 8 ports Port Mapping Strategy

Original Port	Original Network/Purpose	New Port	New Network Configuration (Example)
eth0 (WAN)	Public Internet (DHCP)	eth0 (WAN)	Public Internet (DHCP)
eth1 (LAN)	192.168.1.0/24 (Main LAN)	eth1 (LAN)	192.168.1.0/24 (Main LAN)
eth2 (DMZ)	10.0.0.0/24 (Servers)	eth2 (DMZ)	10.0.0.0/24 (Servers)
eth3 (Guest WiFi)	192.168.2.0/24	eth3 (Trunk Port)	VLAN 10: 192.168.2.0/24 (Guest)
eth4 (IoT Devices)	192.168.3.0/24	eth3 (Trunk Port)	VLAN 20: 192.168.3.0/24 (IoT)
eth5 (VoIP Phones)	192.168.4.0/24	eth3 (Trunk Port)	VLAN 30: 192.168.4.0/24 (VoIP)
eth6-eth13 (Other Segments)	Various networks	eth4-eth7 (Trunk Ports)	Consolidated via additional VLANs or retired.

Key Considerations for Port Reduction

- ✓ **Network Segmentation:** Identify which networks can be consolidated onto a single physical interface using VLANs.
- ✓ **Switching Infrastructure:** Ensure your network switches support VLAN tagging and can be configured as trunk ports.
- ✓ **Traffic Volume:** Consider the combined traffic volume of consolidated segments to ensure the single physical interface can handle the load.
- ✓ **Security Implications:** Review security rules to ensure they correctly apply to the new VLAN interfaces.

Modified Configuration Import / Manual Reconfiguration

For port reduction scenarios, a direct configuration import is not recommended. Instead, a partial or manual reconfiguration approach is required.

1. Perform the Physical Installation (Section 5.1) and Connecting and Registering (Section 5.2) on the new appliance.
2. Do not directly import the full configuration backup from the old appliance.
3. Instead, you will manually configure the interfaces on the new appliance, starting with the planned VLAN structure.
4. Once the basic network interfaces (including VLANs) are configured, you can then selectively re-create or import specific configuration elements (e.g., traffic rules, VPN tunnels, user accounts) from your documented old configuration or by using a partial import.

VLAN Configuration Procedure on New Hardware

This procedure assumes you have identified which physical ports will act as VLAN trunks and which VLANs will be configured on them.

1. From the new appliance's administration interface, navigate to Interfaces.
2. Configure the physical interfaces that will serve as VLAN trunks (e.g., eth3 and eth4 in the example above) with appropriate settings (e.g., set to "LAN" or "Other," assign a management IP if desired, or leave unassigned if purely for VLANs).
3. To add a VLAN interface:
   - Click "Add" (or the + button) and select "VLAN Interface."
   - In the "New VLAN Interface" dialog:
     - **Name:** Give it a descriptive name (e.g., "Guest-VLAN10")
     - **VLAN ID:** Enter the VLAN ID (e.g., 10 for Guest, 20 for IoT, 30 for VoIP)
     - **Parent Interface:** Select the physical interface that will carry this VLAN traffic (e.g., eth3)
     - **Type:** Select "LAN" or "Other" as appropriate
     - **IP Address:** Configure the IP address and subnet mask for this VLAN interface (e.g., 192.168.2.1/24)
     - **DHCP Server:** Enable and configure the DHCP server for this VLAN if needed.
   - Click "OK" to save the VLAN interface.

4. Repeat for each required VLAN.

5. **Update Traffic Rules:** After configuring the VLAN interfaces, you must review and update your existing traffic rules to reference the new VLAN interfaces instead of the original physical interfaces they replaced. This ensures traffic is correctly filtered and routed.

Network Switch Configuration for VLANs

For VLANs to function correctly, your downstream network switches must be configured to support VLAN tagging.

1. Configure the switch port connected to the GFI KerioControl's VLAN trunk interface as an 802.1Q trunk port. This port should be configured to allow all necessary VLANs.

2. Configure access ports on the switch for devices on specific VLANs. For example, a port for a guest Wi-Fi access point would be configured as an access port for VLAN 10.

3. Ensure that the native VLAN (if any) on the switch trunk port matches the native VLAN configuration on the GFI KerioControl interface (if not using tagged VLANs for all traffic).

GFI AppManager Integration and Management

GFI AppManager plays a vital role in centralizing the management, monitoring, and backup of your GFI KerioControl deployments. During a hardware transition, it can simplify the process and ensure continuity of management.

GFI AppManager's Role in Migration

GFI AppManager provides several benefits for migration:

- ✓ **Centralized Overview:** Provides a single pane of glass for managing GFI KerioControl devices.
- ✓ **Automated Configuration Backup:** GFI AppManager can store automated configuration backups in the cloud, offering an off-site recovery point.
- ✓ **Status Monitoring and Alerts:** Allows you to monitor the status of your new appliance and receive alerts post-migration.
- ✓ **Remote Configuration:** Enables remote configuration adjustments if needed after the appliance is online.

Important: If you encounter a license error in GFI AppManager after importing the configuration, you may need to reset the AppManager agent on the GFI KerioControl appliance. See detailed steps here.

Configuration Backup via GFI AppManager

As mentioned in Section 3.2, GFI AppManager can be used to store configuration backups. This is particularly useful for MSPs managing many devices, providing an additional layer of security and convenience during migration.

Post-Migration GFI AppManager Reconnection

After successfully importing the configuration and bringing the new hardware online, you may need to verify or re-establish its connection to GFI AppManager.

1 Verify GFI AppManager Connectivity

- Log in to your GFI AppManager account.
- Check the status of the newly migrated GFI KerioControl appliance. It should show as "Online."
- If the device shows as "Offline" or "Disconnected," proceed to re-registration.

2 Re-registration Procedure

- Log in to the GFI KerioControl administration interface of the new appliance.
- Navigate to Dashboard.
- Locate the "GFI AppManager" tile.
- If the device is not connected, click "Add to GFI AppManager" or "Update registration info" if a previous connection attempt failed.
- Follow the on-screen prompts to register the device with your GFI AppManager account. This typically involves entering your GFI AppManager login credentials.

3 Verification

- Once registered, the device's status in AppManager should change to "Online," and you should see its details and status updates.
- Confirm that automated backups are scheduled and functioning correctly via AppManager.

Troubleshooting and Common Issues

Despite careful planning, issues can arise during hardware migration. This section outlines known challenges and provides troubleshooting decision trees and recovery procedures.

Troubleshooting Decision Trees:

Problem: Configuration Import Fails / Interfaces are Incorrectly Mapped

Check 1: Is new hardware running the minimum required GFI KerioControl version?

Yes: Continue.

No: Upgrade firmware on new hardware first.

Check 2: Does the imported configuration have more physical interfaces than the new hardware?

Yes: This is a port reduction scenario. Do NOT use direct import. Proceed with Port Reduction Migration Path.

No: Continue.

Check 3: Is the backup file corrupted or incomplete?

Yes: Use an alternative, verified backup file.

No: Continue.

Check 4: Did you carefully review and adjust interface pairings during import wizard?

Yes: Contact GFI Support with error logs.

No: Perform factory reset on new appliance, then retry import.

Problem: No Network Connectivity After Migration

Check 1: Is the new appliance powered on and fully booted?

Yes: Continue.

No: Power on, wait for boot.

Check 2: Are network cables connected to the CORRECT ports on the new appliance?

Yes: Continue.

No: Correct cabling.

Check 3: Can you access the GFI KerioControl web UI on the new appliance's LAN IP?

Yes: Continue.

No: Check physical connection to PC, PC's IP config (DHCP/static), console for boot errors.

Check 4: In GFI KerioControl UI, check "Interfaces" section. Are all interfaces "Connected" and have correct IP addresses?

Yes: Continue.

No: Correct interface settings (IP, DHCP, VLANs). Ensure physical link lights are on.

Check 5: Check "Traffic Rules." Are essential rules (e.g., LAN to Internet, VPN) correctly configured and enabled?

Yes: Continue.

No: Correct/enable rules.

Check 6: Check "DNS Forwarding." Is it configured correctly, and are DNS servers reachable from GFI KerioControl?

Yes: Continue.

No: Correct DNS settings.

Check 7: If using VLANs, is the downstream network switch configured with correct 802.1Q trunking and access ports?

Yes: Contact GFI Support with Connection log and Filter log.

No: Configure switch VLANs (Section 6.4).