

Quantum®

User's Guide

Quantum vmPRO



Quantum vmPRO User's Guide, 6-67535-06 Rev A, April 2015, Product of USA.

Quantum Corporation provides this publication "as is" without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability or fitness for a particular purpose. Quantum Corporation may revise this publication from time to time without notice.

COPYRIGHT STATEMENT

© 2015 Quantum Corporation. All rights reserved.

Your right to copy this manual is limited by copyright law. Making copies or adaptations without prior written authorization of Quantum Corporation is prohibited by law and constitutes a punishable violation of the law.

TRADEMARK STATEMENT

Be Certain (and the Q brackets design), DLT, DXi, DXi Accent, DXi V1000, GoVault, Lattus, NDX, the Q logo, the Q Quantum logo, Q-Cloud, Quantum (and the Q brackets design), the Quantum logo, Quantum Be Certain (and the Q brackets design), Quantum Vision, Scalar, StorageCare, StorNext, SuperLoader, Symform, and the Symform logo (and design) are either registered trademarks or trademarks of Quantum Corporation and its affiliates in the United States and/or other countries. All other trademarks are the property of their respective owners.

Products mentioned herein are for identification purposes only and may be registered trademarks or trademarks of their respective companies. All other brand names or trademarks are the property of their respective owners.

Quantum specifications are subject to change.



Contents

Preface	viii
Audience	viii
Chapter 1: Quantum vmPRO	1
Quantum vmPRO	1
Chapter 2: vmPRO Setup and Configuration	4
vmPRO Setup and Configuration	5
Quantum vmPRO Requirements	6
Configuring Network Settings for a vmPRO Appliance	8
Initially Configuring a vmPRO Appliance	13
vmPRO Licensing	14
Calculating Capacity Requirements for vmPRO Licensing	15
Adding Licenses to a vmPRO Appliance	19
vmPRO Servers	23
Configuring a vCenter Server for a vmPRO Appliance	24
Configuring ESX Servers for a vmPRO Appliance	33
Discovering Servers for a vmPRO Appliance	40

NAS Targets and File Sharing Protocols	41
Configuring a CIFS Protocol for a vmPRO Appliance	43
Configuring an NFS Protocol for a vmPRO Appliance	49
Configuring NAS Targets for SmartMotion Backups	53
vmPRO Group Configuration	57
Configuring vmPRO Groups	59
Managing vmPRO Groups	61
Importing vmPRO Group Configurations	62
vmPRO Folders	64
Configuring vmPRO Folders	65
vmPRO Emails, Reports, Alerts, and Autosupport	68
Configuring Email for a vmPRO Appliance	68
Configuring Reports, Alerts, and Autosupport for a vmPRO Appliance	70
vmPRO NTP Servers	73
Configuring an NTP Server for a vmPRO Appliance	73
vmPRO Users	75
Configuring Users for a vmPRO Appliance	76
vmPRO Upgrades	77
Checking for vmPRO Software Updates	78
Updating vmPRO Versions 2.X to 2.3.3 and 3.0.X to 3.X	79
Updating vmPRO Version 2.3.3 to vmPRO Version 3.X	80
Updating vmPRO Versions 3.1 or Newer	81
Installing vmPRO Software Updates Offline	82
vSphere Changed Block Tracking Support	84
Configuring CBT on a vmPRO Appliance	86
Quantum VSS Writer	88
Preparing a Windows System for VSS Backups	90
Using Log Truncation for VSS Backups	94
Uninstalling the VSS Writer	94

vmPRO Advanced Settings	95
Configuring Advanced Settings for a vmPRO Appliance	96
HotAdd Transport and Your vmPRO Appliance	98
Chapter 3: vmPRO GUI	103
vmPRO GUI	103
Accessing the vmPRO GUI	105
Embedding the vmPRO GUI in the vSphere Client	105
vmPRO GUI Menus	108
Navigating the vmPRO Home Console	115
Navigating the vmPRO VMs Console	117
vmPRO Auto-Export Feature	122
Modifying VM Settings from the vmPRO Appliance	123
Managing Servers and Nodes from the VMs Console	125
Navigating the vmPRO Alerts Console	130
Navigating the vmPRO Tasks Console	132
Chapter 4: vmPRO SmartMotion™ Backup	138
vmPRO SmartMotion Backup	138
Manually Activating a SmartMotion Backup	141
vmPRO SmartMotion Backup Policies	142
Retention Schedules for SmartMotion Backups	143
Creating SmartMotion Backup Policies	146
Modifying SmartMotion Backup Policies	155
Chapter 5: vmPRO Data Recovery	157
vmPRO Data Recovery	157
Recovering Virtual Machines	159
Recovering VMs Backed Up with a Third-Party Application	169
Manually Registering a Recovered VM	172

Preparing for Exchange Recovery	174
Recovering Mailboxes on an Exchange Server	180
Manually Cleaning Up the Exchange Server	188
iSCSI Export and Recovery	193
Recovering VM Disks Using iSCSI	195
Individual File Recovery	201
Recovering Individual Files	202
Appendix 1: vmPRO CLI Guide	205
vmPRO CLI Guide	206
Accessing the vSphere Client Console for vmPRO	207
vmPRO Console Commands – autosupport	211
vmPRO Console Commands – cbt	212
vmPRO Console Commands – config	212
vmPRO Console Commands – filesys	213
vmPRO Console Commands – group	214
vmPRO Console Commands – help	215
vmPRO Console Commands – import	215
vmPRO Console Commands – log	216
vmPRO Console Commands – nagios	217
vmPRO Console Commands – net	217
vmPRO Console Commands – ntp	219
vmPRO Console Commands – nw	220
vmPRO Console Commands – smartmotion	221
vmPRO Console Commands – snmp	222
vmPRO Console Commands – ssh	222
vmPRO Console Commands – system	223
vmPRO Console Commands – tsm	225
vmPRO Console Commands – vss	225

External Monitoring Support for a vmPRO Appliance226



Preface

This manual introduces the Quantum Quantum vmPRO and discusses:

- Configuration
- Appliance interface
- System Operations
- Basic troubleshooting

Audience

This manual is written for Quantum vmPRO operators and administrators. It is assumed that this audience has at least a basic understanding regarding the use and function of the following products and applications:

- Windows Operating Systems
- Linux Operating Systems
- VMware
- Backup and recovery systems

Document Organization

Following is a brief description of chapter contents.

- [Chapter 1](#) provides an overview of the vmPRO appliance.
- [Chapter 2](#) provides detailed instructions for configuring your vmPRO appliance.
- [Chapter 3](#) provides basic instructions for navigating through the vmPRO appliance graphical user interface (GUI).
- [Chapter 4](#) provides detailed instructions for backing up data with the vmPRO appliance.
- [Chapter 5](#) provides detailed instructions for recovering data with your vmPRO appliance.
- [Appendix A](#) provides information about basic vmPRO CLI commands.

Notational Conventions


This manual uses the following conventions:

Convention	Example
User input is shown in bold monospace font.	./DARTinstall
Computer output and command line examples are shown in monospace font.	./DARTinstall
User input variables are enclosed in angle brackets.	http://<ip_address>/cgi-bin/stats
For UNIX and Linux commands, the command prompt is implied.	./DARTinstall is the same as # ./DARTinstall
File and directory names, menu commands, button names, and window names are shown in bold font.	/data/upload
Menu names separated by arrows indicate a sequence of menus to be navigated.	Utilities > Firmware

The following formats indicate important information:

 **Note:** Note emphasizes important information related to the main topic.

 **Caution:** Caution indicates potential hazards to equipment or data.

 **WARNING:** Warning indicates potential hazards to personal safety.

- Right side of the system - Refers to the right side as you face the component being described.
- Left side of the system - Refers to the left side as you face the component being described.

- Data sizes are reported in base 1000 rather than base 1024. For example:
 - 1 MB = 1,000,000 bytes
 - 1 GB = 1,000,000,000 bytes
 - 1 TB = 1,000,000,000,000 bytes

Product Safety Statements

Quantum will not be held liable for damage arising from unauthorized use of the product. The user assumes all risk in this aspect.

This unit is engineered and manufactured to meet all safety and regulatory requirements. Be aware that improper use may result in bodily injury, damage to the equipment, or interference with other equipment.

⚡ WARNING: Before operating this product, read all instructions and warnings in this document and in the *Quantum Products System, Safety, and Regulatory Information Guide*.

⚡ ADVARSEL: Læs alle instruktioner og advarsler i dette dokument og i *Informationsvejledning vedrørende system-, sikkerheds- og lovbestemmelser for Quantum produkter, før produktet betjenes*.

⚡ AVERTISSEMENT : Avant d'utiliser ce produit, lisez toutes les instructions et les avertissements de ce document et du *Guide d'informations sur le système, la sécurité et la réglementation de Quantum*.


⚡ WARNUNG: Lesen Sie vor der Inbetriebnahme dieses Produkts alle Anleitungen und Warnungen in diesem Dokument und im *System-, Sicherheits- und Betriebsbestimmungen-Handbuch für Quantum-Produkte*.


⚡ ADVERTENCIA: Antes de hacer funcionar este producto, lea todas las instrucciones y advertencias de este documento y de la *Guía de información normativa, del sistema y de seguridad de los productos de Quantum*.

⚡ WARNING: Läs igenom alla instruktioner och varningar i detta dokument och i *Quantums produktsystem, säkerhet och reglerande informationsguide* innan denna produkt används.

⚡ ВНИМАНИЕ! Перед началом эксплуатации данного изделия прочтите все инструкции и предупреждения, приведенные в настоящем документе и в *Руководстве по системе, технике безопасности и действующим нормативам компании Quantum*.

⚡ 警告: 本製品を使用される前に、本書と『*Quantum製品システム、安全、規制情報ガイド*』に記載されているすべての説明と警告をお読みください。

 경고: 본 제품을 작동하기 전에 본 문서와 **Quantum 제품 시스템, 안전 및 규제 정보 설명서**에 있는 모든 지침과 경고를 참조합니다.

 警告：在操作本产品之前，请阅读本档和 **Quantum 产品系统、安全和法规信息指南**中的所有说明和警告。

 警告：操作此產品前，請閱讀本檔案及 **Quantum 產品系統、安全與法規資訊指南**中的指示與和警告說明。

אזהרה: לפני ההפעלה של מוצר זה, קרא את כל ההוראות והאזהרות הכלולות במסמך זה וכן במדריך המידע בנושא מערכת, בטיחות ותקינה עבור מוצרי **Quantum**.

Related Documents

The following Quantum documents are also available for Quantum vmPRO:

Document Number	Document Title	Document Description
6-67534	Quantum vmPRO Release Notes	Presents compatibility and support information about the latest release of Quantum vmPRO.
6-67728	Quantum vmPRO Open Source Licenses	Lists open source software components and associated licenses used in Quantum vmPRO.
6-66527	Quantum Vision User's Guide	Describes the Quantum Vision web-based user interface, management, configuration, and operation.
6-67612	Quantum DXi V-Series User's Guide	Describes Quantum's DXi V-Series appliances (DXi V1000 and DXi V4000) Web-based user interface, operations, and configuration.
6-67081	Quantum DXi-Series Command Line Interface (CLI) Guide	Describes the CLI commands for DXi V-Series Software.

For the most up to date information on Quantum vmPRO, see:

<http://www.quantum.com/serviceandsupport/index.aspx>

Contacts

For information about contacting Quantum, including Quantum office locations, go to:

<http://www.quantum.com/aboutus/contactus/index.aspx>

Comments

To provide comments or feedback about this document, or about other Quantum technical publications, send e-mail to:

doc-comments@quantum.com

Getting More Information or Help

StorageCare™, Quantum's comprehensive service approach, leverages advanced data access and diagnostics technologies with cross-environment, multi-vendor expertise to resolve backup issues faster and at lower cost.

Accelerate service issue resolution with these exclusive Quantum StorageCare services:

- **Service and Support Website** - Register products, license software, browse Quantum Learning courses, check backup software and operating system support, and locate manuals, FAQs, firmware downloads, product updates and more in one convenient location. Get started at:
<http://www.quantum.com/serviceandsupport/index.aspx>
- **eSupport** - Submit online service requests, update contact information, add attachments, and receive status updates via email. Online Service accounts are free from Quantum. That account can also be used to access Quantum's Knowledge Base, a comprehensive repository of product support information. Get started at:
<https://onlineservice.quantum.com>
- **StorageCare Guardian** - Securely links Quantum hardware and the diagnostic data from the surrounding storage ecosystem to Quantum's Global Services Team for faster, more precise root cause diagnosis. StorageCare Guardian is simple to set up through the internet and provides secure, two-way communications with Quantum's Secure Service Center. Learn more at:
<http://www.quantum.com/ServiceandSupport/Services/GuardianInformation/Index.aspx>

For further assistance, or if training is desired, contact the Quantum Customer Support Center:

Region	Support Contact
North America	1-800-284-5101 (toll free) +1-720-249-5700
EMEA	+800-7826-8888 (toll free) +49 6131 324 185
Asian Pacific	+800-7826-8887 (toll free) +603-7953-3010

For worldwide support:
<http://www.quantum.com/serviceandsupport/index.aspx>

Worldwide End-User Product Warranty

For more information on the Quantum Worldwide End-User Standard Limited Product Warranty:

<http://www.quantum.com/serviceandsupport/warrantyinformation/index.aspx>



Chapter 1: Quantum vmPRO

This chapter contains the following topics and sections:

Quantum vmPRO	1
---------------------	---

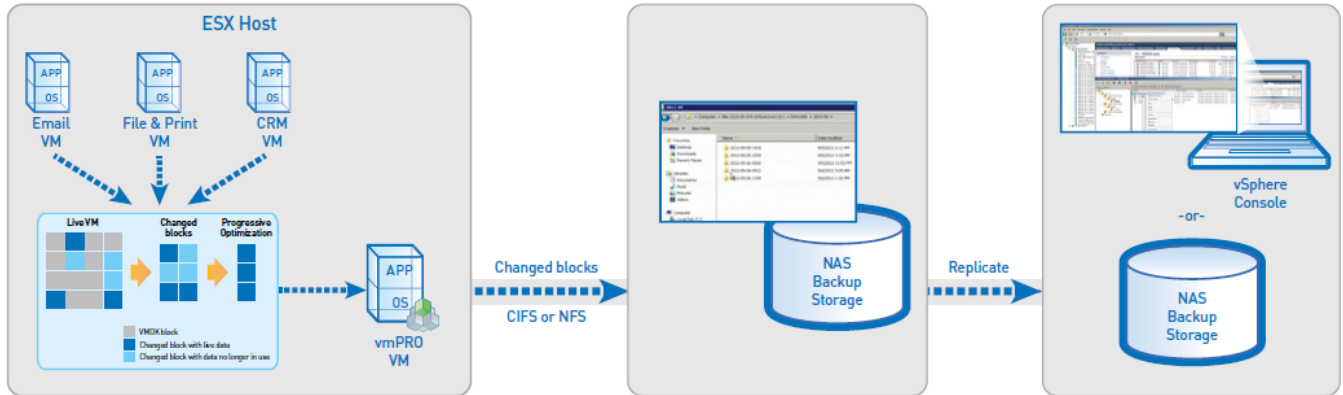
Quantum vmPRO

Quantum vmPRO is a lightweight, agentless backup and recovery application that protects data in its native format. Deployed as a virtual appliance on a VMware vSphere ESX or ESXi server, Quantum vmPRO works directly with the guest operating system (OS) of any virtual machine (VM) designated for data protection.

The vmPRO appliance backs up data in its native virtual machine disk (VMDK) file format to a Network Attached Storage (NAS) backup target. You can access the backed-up data down to the file level using any standard file browser. In addition, you can achieve easy drag-and-drop restores of whole VMs or individual files within seconds from a standard file browser.

You can also pair Quantum vmPRO with a Quantum DXi appliance to replicate backed-up data to another disk target or to the cloud. This replication allows for fast restores and bootable VMs from the data replication (DR) location, without the need of a backup application at a secondary location.

Figure 1: vmPRO Workflow Diagram



SmartMotion™

At the heart of vmPRO is SmartMotion. SmartMotion provides the backup services of vmPRO by initiating a scheduled push of specified VMDK files to any specified NAS target. The target can be resident on a plain NAS device or on a deduplication system such as the Quantum DXi.

SmartView™

SmartView can present the ESX environment as a virtual NAS file system in either a CIFS or NFS share format. Through this presentation, SmartView provides users easy access to VMs located on ESX servers.

Progressive Optimization

Progressive Optimization, a patented background application, runs on VMDK files whenever a read of the virtual file system is initiated. It filters out white space and deletes unused blocks of data, reducing the use of host, network, and storage resources by up to 75%.

Additional vmPRO Highlights

Quantum vmPRO provides the following additional functions and capabilities:

- Without the need for proprietary backup applications, recovers archived data from any medium, including disk, tape, and cloud
- Supports full manageability within a vCenter console, including Virtual SAN (VSAN) configurations
- Provides Volume Shadow Copy Service (VSS) support for Windows Shadow Services
- Auto-discovers VMs for better protection in dynamic environments
- Uses the vStorage API with Changed Block Tracking to access both running and idle VMs
- Supports vSphere 4.x, vSphere 5.x, and vSphere 6.0 environments



Chapter 2: vmPRO Setup and Configuration

This chapter contains the following topics and sections:

vmPRO Setup and Configuration	5
Quantum vmPRO Requirements	6
Configuring Network Settings for a vmPRO Appliance	8
Initially Configuring a vmPRO Appliance	13
vmPRO Licensing	14
vmPRO Servers	23
NAS Targets and File Sharing Protocols	41
vmPRO Group Configuration	57
vmPRO Folders	64
vmPRO Emails, Reports, Alerts, and Autosupport	68
vmPRO NTP Servers	73
vmPRO Users	75
vmPRO Upgrades	77
vSphere Changed Block Tracking Support	84
Quantum VSS Writer	88
vmPRO Advanced Settings	95

vmPRO Setup and Configuration

After installing your Quantum vmPRO appliance, you need to configure both network and appliance settings.

- Use the VMware vSphere Client console to configure network settings.
- Use the Quantum vmPRO Configuration Wizard in the vmPRO GUI to initially configure appliance settings.
- Use the vmPRO GUI to configure additional appliance settings, or to edit appliance settings, as needed.

Installation Notes

Refer to the following notes for information about installing your vmPRO appliance:

View step-by-step instructions

If you have not yet installed your Quantum vmPRO appliance, see the [Quantum vmPRO Download and Installation Guide](#). You need a valid email address and password to access the guide.

For Standard Edition users

Documentation, community support, and other resources are available through [Forum V](#) (Quantum's online support forum for virtualization products).

For Tivoli Storage Manager (TSM)

We recommend installing the TSM Linux agent after you install your Quantum vmPRO appliance. For more information, refer to [Installing and using the TSM Client on a Quantum vmPRO virtual appliance](#).

Configuration Tips

Use the following tips to configure your vmPRO appliance:

Group Configuration

If you plan to use more than one vmPRO appliance as part of your backup solution, set up the appliances in a group configuration. See [Configuring vmPRO Groups](#).

Multiple VLAN Configuration

If multiple virtual local area networks (VLANs) are present, configure the vmPRO network on the VLAN that has access to the ESX or vCenter server(s) to be protected.

If you use third-party backup software, its client that connects to the vmPRO network must be able to access the VLAN, as well.

DHCP Configuration

Although the vmPRO appliance automatically acquires a network address in environments with dynamic host configuration protocol (DHCP), we recommend configuring a static IP address during configuration. See [Configuring Network Settings for a vmPRO Appliance](#).

Active Directory Integration

On Windows backup servers, you can integrate the vmPRO appliance with an Active Directory (AD) domain to use any authenticated user ID for CIFS backups. When there is not an AD integration, you must use a local user ID with the same user context as the [vmPRO admin user](#)¹ for CIFS backups. See [Configuring a CIFS Protocol for a vmPRO Appliance](#).

Multiple ESX or ESXi Server Configuration

In environments with multiple ESX or ESXi servers and VMs, you can deploy multiple vmPRO appliances on more than one ESX or ESXi server to increase overall performance and throughput. See [Configuring ESX Servers for a vmPRO Appliance](#).

VSAN Configuration

In environments using VMware's Virtual SAN (VSAN) configuration, you must set up your vmPRO appliance to manage the configuration through a vCenter server rather than as opposed to managing individual ESX servers. VSAN is a cluster-wide resource that exists as datastores on a cluster of ESX servers. The vmPRO appliance manages VSAN through a vCenter server, which in turn manages the ESX servers housing the VSAN datastores.



Caution: Do not clone a vmPRO appliance. Cloned appliances are not supported.

Quantum vmPRO Requirements

Before installing your vmPRO appliance, make sure that your environment meets or exceeds the following system requirements.

¹Both the default user name and password are "sysadmin". The vmPRO administrator can change these credentials, as needed.

Component	Requirements
Virtual Server	At least one ESX/ESXi server, versions 4.0 update 2 or later, to host the vmPRO appliance and virtual machines (VMs) being backed up. <div style="background-color: #e6f2ff; padding: 10px;">Keep the following items in mind when configuring your ESX/ESXi servers:<ul style="list-style-type: none">• In environments with numerous ESX/ ESXi servers hosting multiple VMs, we recommend deploying a vmPRO appliance on each ESX/ESXi server.• We recommend using paid versions of VMware ESX or ESXi servers. Free versions have various API limitations that keep vmPRO from functioning as designed.• You can manage your ESX/ESXi server(s) directly or through VMware vCenter. If you have the option of using a vCenter server, we recommend that you do so.</div>
Hardware (Host Server)	<ul style="list-style-type: none">• 12 GB of free disk space• 1280 MB of free RAM• Gigabit NIC port for data movement on the vmPRO host server
Network (Host Server)	We recommend that you perform the following tasks in configuring your network: <ul style="list-style-type: none">• Configure a static IP address.• Configure your network on the VLAN that has access to the vCenter or ESX/ ESXi servers to be protected. If you use third-party backup software, its client that connects to the vmPRO network must be able to access the VLAN, as well.
Web Browser (Client)	Any modern Web browser that supports Adobe Flash Player plug-in 9.X or higher.
Flash Player plug-in (Client)	Adobe Flash Player plug-in 9.X or higher.
Microsoft Exchange Servers	One of the following versions of Microsoft Exchange for mailbox recovery: <ul style="list-style-type: none">• Windows 2008R2/Exchange 2010• Windows 2008R2/Exchange 2013• Windows 2012R2/Exchange 2013 For systems that use Microsoft Exchange servers running Windows 2008R2 and Exchange 2010, the Window Management Framework 3.0 must be installed.

Configuring Network Settings for a vmPRO Appliance

The vmPRO appliance installs with default network settings. You can edit these settings from the appliance's VMware vSphere Client console. Use the following tasks to help you access your appliance's **Network Configuration** screen on the Client console and configure network settings.

Access your vmPRO appliance's Network Configuration screen on the Client console

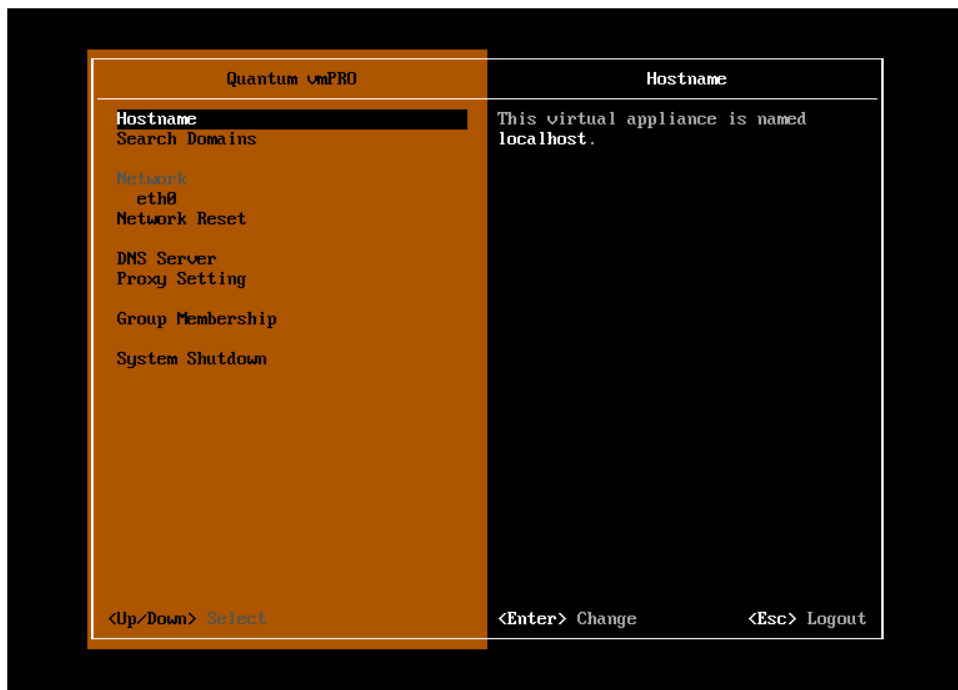
1. Access the vSphere Client console. See [Accessing the vSphere Client Console for vmPRO](#).
2. **Figure 2:** vSphere Client Console



3. Click inside the console and press **<Enter>** to display the **Login** prompt.
4. At the **Username** prompt, enter the vmPRO appliance's user name. The default user name is **sysadmin**.
5. At the **Password** prompt, enter the vmPRO appliance's password. The default password is **sysadmin**.

6. Press **<Enter>** to display the **Network Configuration** screen.

Figure 3: Network Configuration Screen



Configure your vmPRO appliance's network settings

1. Access your vmPRO appliance's **Network Configuration** screen on its client console.
2. Edit each of the following settings, as needed:

Setting	Description
---------	-------------

Hostname

The host name for the vmPRO appliance.
Edit the host name

- a. With **Hostname** selected, press **<Enter>** to display the **Change Hostname** prompt.

Figure 4: Change Hostname Prompt



- b. In the **Hostname** field, enter a new host name.
- c. Press **<Enter>** to save changes.

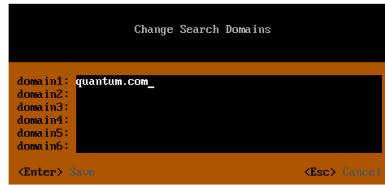
Setting	Description
---------	-------------

Search Domains

The search domains assigned to the vmPRO appliance.
The vmPRO appliance combines the search domain with the host name to create a fully qualified domain name (FQDN).
Edit search domains

- a. With **Search Domains** selected, press **<Enter>** to display the **Change Search Domains** prompt.

Figure 5: Change Search Domains Prompt



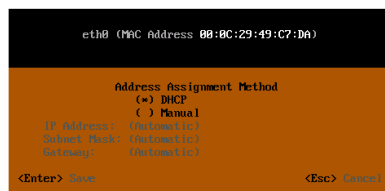
- b. In the **domain1-6** fields, enter search domains as needed. These fields are limited to 256 characters.
- c. Press **<Enter>** to save changes.

Network

The network interface for the vmPRO appliance.
Edit the method by which the appliance's IP addresses are assigned

- a. With **Network** selected, press **<Enter>** to display the **Address Assignment Method** prompt.

Figure 6: Address Assignment Method Prompt



- b. Select to assign the appliance's IP addresses by either **DHCP** or **Manual**.
- c. Press **<Enter>** to save changes.

Setting	Description
---------	-------------

Network Reset

Manually reset the network

- a. With **Network Reset** selected, press **<Enter>** to display a warning stating that resetting the network services may interrupt your data transfer.

Figure 7: Network Reset Warning



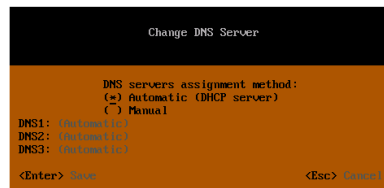
- b. To proceed with the network reset, press **<Enter>**; otherwise, press **<Esc>**.

DNS Server

The method by which the DNS servers are assigned.
Edit the DNS Server assignment method

- a. With **DNS Server** selected, press **<Enter>** to display the **Change DNS Server** prompt.

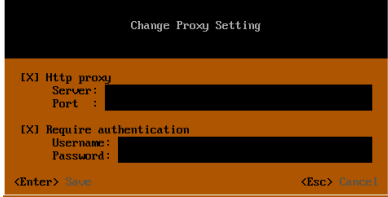
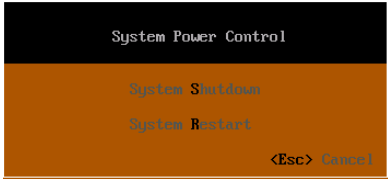
Figure 8: Change DNS Server Prompt



- b. Select either **Automatic** or **Manual** as the DNS server assignment method.

If you select **Manual**, enter the DNS servers in the **DNS1-3** fields, as needed.

- c. Press **<Enter>** to save changes.
-

Setting	Description
Proxy Setting	<p>The http proxy setting assigned to the vmPRO appliance. Use this proxy support to access the Internet.</p> <p>You can configure proxy support for vmPRO software upgrades only. See Updating vmPRO Versions 3.1 or Newer.</p> <p>Edit the http proxy setting for the vmPRO appliance</p> <ol style="list-style-type: none">With Proxy Setting selected, press <Enter> to display the Change Proxy Setting prompt. <p>Figure 9: Change Proxy Setting Prompt</p>  <ol style="list-style-type: none">Select Http proxy, and edit the values in the Server and Port fields to assign a new proxy server.Select Require authentication, and edit the values in the Username and Password fields to require login credentials when using the proxy server.Press <Enter> to save changes.
Group Membership	<p>The group membership assigned to the vmPRO appliance. See Configuring vmPRO Groups.</p>
System Shutdown	<p>Manually shut down or restart the system</p> <ol style="list-style-type: none">With System Shutdown selected, press <Enter> to display the System Power Control prompt. <p>Figure 10: System Power Control Prompt</p>  <ol style="list-style-type: none">Type <S> to shut down the system or type <R> to restart the system.

Initially Configuring a vmPRO Appliance

When you first access your vmPRO appliance's GUI, the **Quantum vmPRO Configuration Wizard** guides you through the setup of your appliance. The following task provides a road map for navigating this wizard. Refer to individual topics for detailed instructions on configuring each component of your vmPRO appliance.

Initially configure your vmPRO appliance using the Quantum vmPRO Configuration Wizard

1. Log in to your vmPRO GUI. See [Accessing the vmPRO GUI](#).

The first time you log in to your vmPRO GUI, the **End User License Agreement** dialog box displays.

2. Click **I Agree** to agree to the vmPRO licensing terms.

After you agree to the licensing terms, the **Quantum vmPRO Configuration Wizard** displays. If the wizard does not automatically display, access it from the **Configure > Config Wizard** menu.

3. Click **Next** to display the **Licenses** page, and install the license(s) for the vmPRO appliance. See [Adding Licenses to a vmPRO Appliance](#).

4. Click **Next** to display the **Servers** page, and configure the appropriate vCenter or ESX server for your vmPRO appliance. See [Configuring a vCenter Server for a vmPRO Appliance](#) or [Configuring ESX Servers for a vmPRO Appliance](#).

i Note: When configuring a server for your vmPRO appliance, you can select either a single vCenter server to manage ESX servers, **OR** you can select one or more standalone ESX servers. You cannot manage both a vCenter server and ESX servers directly from your appliance. If the configuration includes a VSAN datastore, select the single vCenter server.

5. Click **Next** to display the **File Sharing** page, and configure the protocol — either CIFS or NFS — with which to export the vmPRO appliances file systems. See [NAS Targets and File Sharing Protocols](#).
6. Click **Next** to display the **Storage** page, and configure the network storage for your vmPRO appliance. See [Configuring NAS Targets for SmartMotion Backups](#).
7. Click **Next** to display the **Backup Policies** page, and configure the backup policies for your vmPRO appliance. See [Creating SmartMotion Backup Policies](#).
8. Click **Next** to display the **Email** page, and configure email for your vmPRO appliance. See [Configuring Email for a vmPRO Appliance](#).
9. Click **Next** to display the **Reports & Alerts** page, and configure report and alert settings for your vmPRO appliance. See [Configuring Reports, Alerts, and Autosupport for a vmPRO Appliance](#).
10. Click **Next** to display the **Time & NTP** page, and configure the time and NTP server for your vmPRO appliance. See [Configuring an NTP Server for a vmPRO Appliance](#).
11. Click **Next** to display the **vCenter Plugin** page, and register the vCenter plugin for your vmPRO GUI, as needed. See [Embedding the vmPRO GUI in a vSphere Client](#).
12. Click **Next** to display the **Summary** page, and review your configuration updates.

13. Click **Save** to save all configuration updates, and then click **Next** to display the final page of the wizard.
The final page provides next steps to take in using your vmPRO appliance.
14. Click **Finish** to exit the wizard.

vmPRO Licensing

Quantum vmPRO uses capacity-based licenses as its main licensing format. Target-based licenses are available to customers who purchase a Quantum vmPRO 4000 product bundle or customers of the Quantum Service Provider program.

Capacity-Based License

A capacity-based license is enforced based upon the total allocated capacity of all virtual machines (VMs) exported to a single vmPRO appliance.

When you configure your vmPRO appliance, you can retrieve your capacity-based license from the vmPRO support site. Upon retrieval, your license is automatically added to your vmPRO appliance. You can then set a capacity warning threshold, which triggers your vmPRO appliance to generate an alert when you are nearing your license's capacity.

Determining Maximum Allocated Capacity

VMware provides the information your vmPRO appliance needs to determine the maximum allocated size of each VM that has been selected for export. Even though the VM may only be using a percent of its allocated capacity, the vmPRO appliance uses the maximum allocated capacity for its calculations.

Example

A VM has a maximum allocated capacity of 250 GB, but it is only using 115 GB. The vmPRO appliance still uses the 250 GB for its capacity-based licensing calculations.

Because an exported VM's maximum allocated size counts toward your capacity license, we advise that you do not export a VM until you want to include it in your backups.

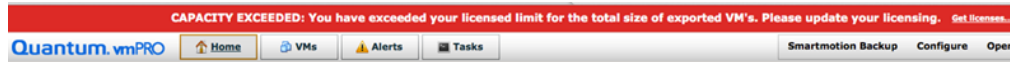
To better estimate your capacity needs, we recommend calculating your capacity requirements using VMware, Windows, or the vmPRO GUI. See [Calculating Capacity Requirements for vmPRO Licensing](#).

i Note: If you have configured your vmPRO to support **Upload a report to Quantum support site every day** (see [Configuring Reports, Alerts, and Autosupport for a vmPRO Appliance](#)), Quantum can tell you what capacity you are actually using.

Exceeding License Capacity

If you exceed your license capacity, the vmPRO GUI displays a warning banner. The vmPRO appliance continues to back up and restore data, but the warning banner remains until you increase your license capacity. Contact your Quantum sales representative to purchase additional capacity-based licenses, and then add the license(s) to your vmPRO appliance.

Figure 11: Capacity Exceeded Warning Banner



Target-Based License

A target-based license has no capacity limit or calculation, but is limited to using just a single Network Attached Storage (NAS) device as a target in backup policies.

Target-based licenses are available to customers who purchase a Quantum vmPRO 4000 product bundle or customers of the Quantum Service Provider program. If you qualify for a target-based license, you can retrieve it from the Web site where you received your initial contact email. You need to manually add your license to your vmPRO appliance.

Calculating Capacity Requirements for vmPRO Licensing

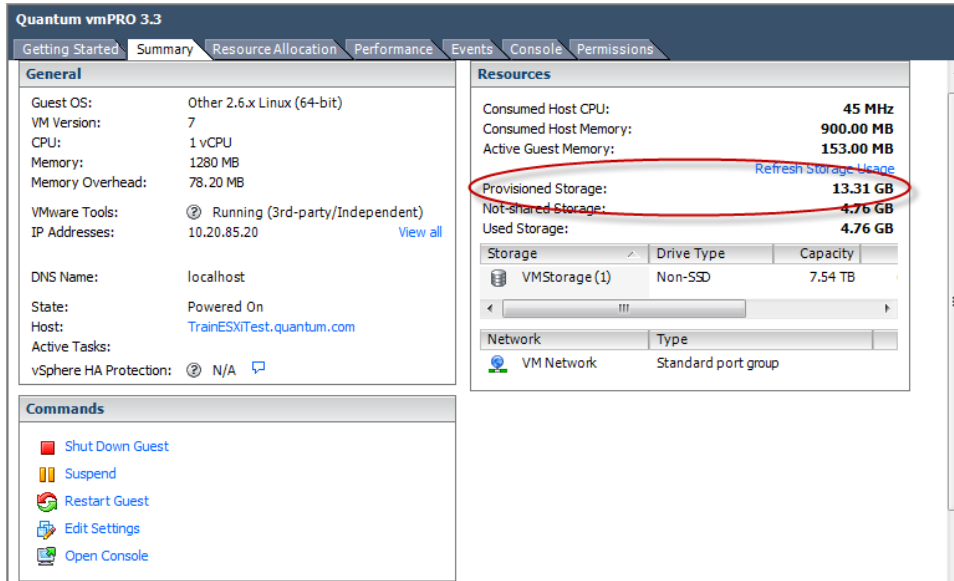
To better estimate your vmPRO appliance's capacity needs, we recommend calculating your capacity requirements using the vSphere Client or Web Client, a Windows or Linux operating system (OS), or the vmPRO GUI versions 3.1 and newer.

i Note: If you have configured your vmPRO to support **Upload a report to Quantum support site every day** (see [Configuring Reports, Alerts, and Autosupport for a vmPRO Appliance](#)), Quantum can tell you what capacity you are currently using.

Calculate your capacity needs using the vSphere Client

1. Open your vSphere Client.
2. In the left pane, select a virtual machine (VM) to be backed up by the vmPRO appliance, and then click the **Summary** tab in the right pane.

Figure 12: Summary Tab



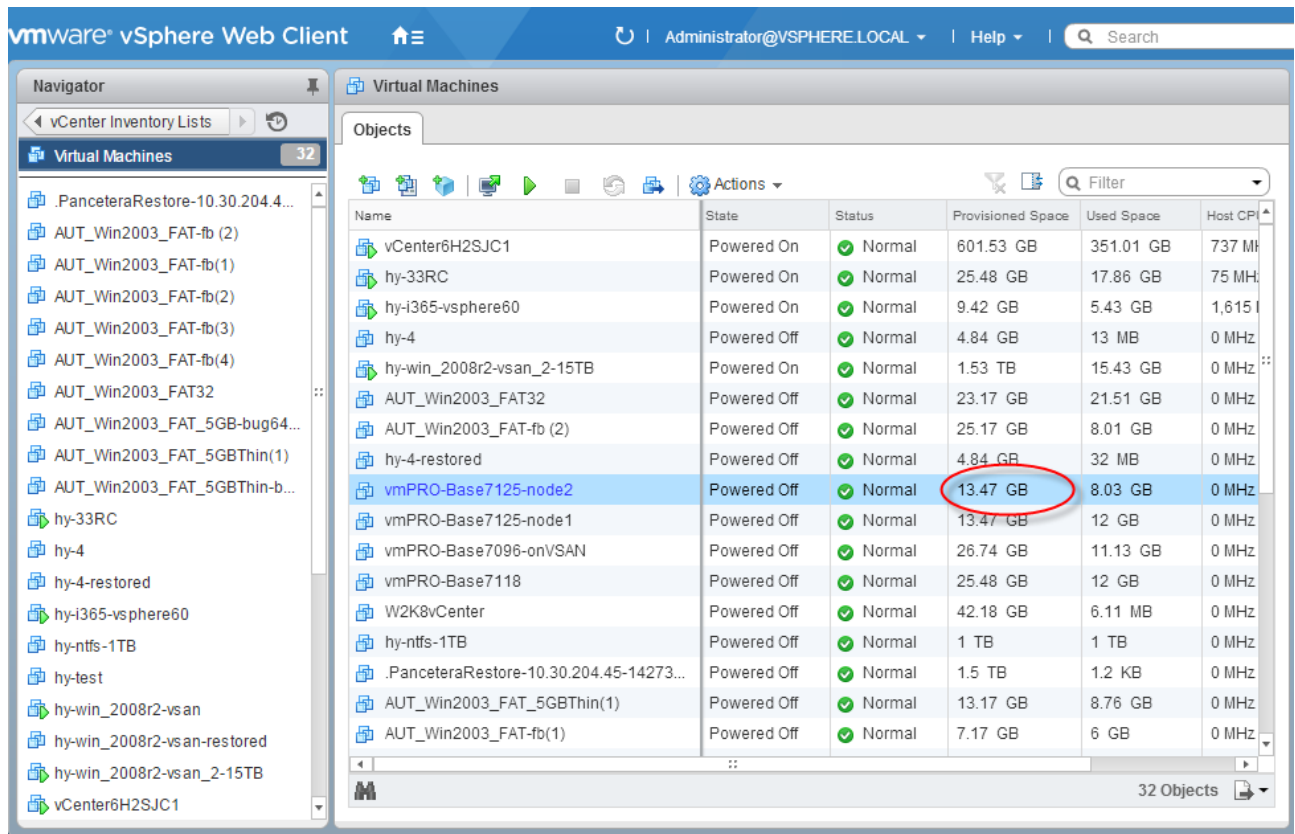
3. In the **Resources** pane, locate the **Provisioned Storage** field.
4. Record the value in the **Provisioned Storage** field. This value is the amount of provisioned storage for the VM.
5. Repeat this process to record the provisioned storage for each VM to be backed up by the vmPRO appliance.
6. Add all of the provisioned storage values together to calculate your vmPRO appliance's capacity needs.

Calculate your capacity needs using the vSphere Web Client

1. Open the vSphere Web Client.

- From **vCenter Inventory Lists**, select **Virtual Machines** to display the list of VMs within the vCenter.

Figure 13: Virtual Machines Grid



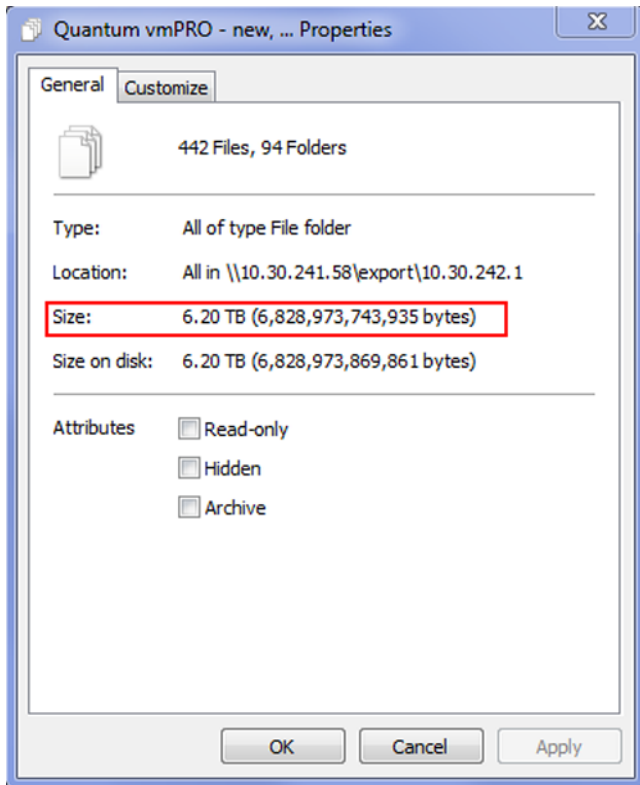
- For each VM to be backed up by the vmPRO appliance, record the value in the **Provisioned Space** column. This value is the amount of provisioned storage for the VM.
- Add all of the provisioned storage values together to calculate your vmPRO appliance's capacity needs.

Calculate your capacity needs using your machine's OS

Note: This task assumes you are using a Windows operating system.

- Browse to the export share on your vmPRO host.
- Select all the VMs that you are backing up.
- Right-click on the selected VMs and select **Properties** to display the **Properties** dialog box.
- In the **Size** field, record the value. This is the size of the capacity-based license you need for your vmPRO appliance.

Figure 14: Properties Dialog Box



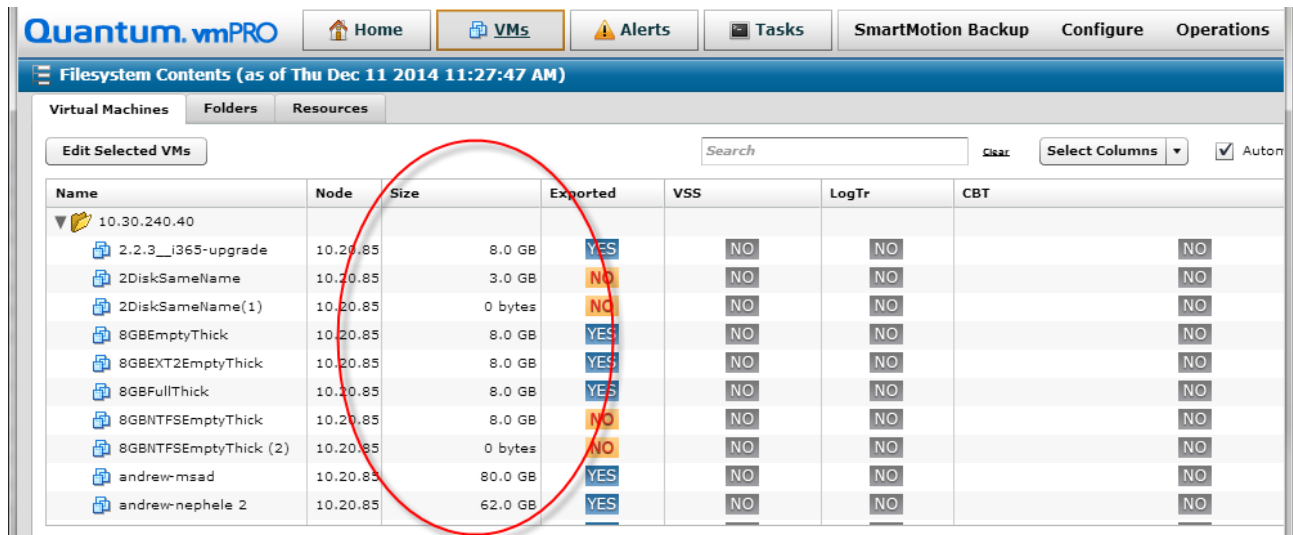
Calculate your capacity needs using your vmPRO GUI

i Note: This task only applies to vmPRO versions 3.1 and newer.

1. From your vmPRO GUI, click the **VMs** button to display the **VMs** console.
2. Click on each folder to display the associated list of VMs within the vmPRO appliance.

3. In the **Size** column, view the maximum allocated capacity of each VM.

Figure 15: VMs Console – Size Column



Name	Node	Size	Exported	VSS	LogTr	CBT
10.30.240.40						
2.2.3_i365-upgrade	10.20.85	8.0 GB	YES	NO	NO	NO
2DiskSameName	10.20.85	3.0 GB	NO	NO	NO	NO
2DiskSameName(1)	10.20.85	0 bytes	NO	NO	NO	NO
8GBEmptyThick	10.20.85	8.0 GB	YES	NO	NO	NO
8GBEXT2EmptyThick	10.20.85	8.0 GB	YES	NO	NO	NO
8GBFullThick	10.20.85	8.0 GB	YES	NO	NO	NO
8GBNTFSEmptyThick	10.20.85	8.0 GB	NO	NO	NO	NO
8GBNTFSEmptyThick (2)	10.20.85	0 bytes	NO	NO	NO	NO
andrew-msad	10.20.85	80.0 GB	YES	NO	NO	NO
andrew-nephele 2	10.20.85	62.0 GB	YES	NO	NO	NO

4. Use each VM's maximum allocated capacity to calculate your vmPRO appliance's capacity needs.

Adding Licenses to a vmPRO Appliance

Use the **Quantum vmPRO Configuration Wizard** to add licenses to your vmPRO appliance. Based on the type of license that you are installing, use one of the following methods.

Capacity-Based License

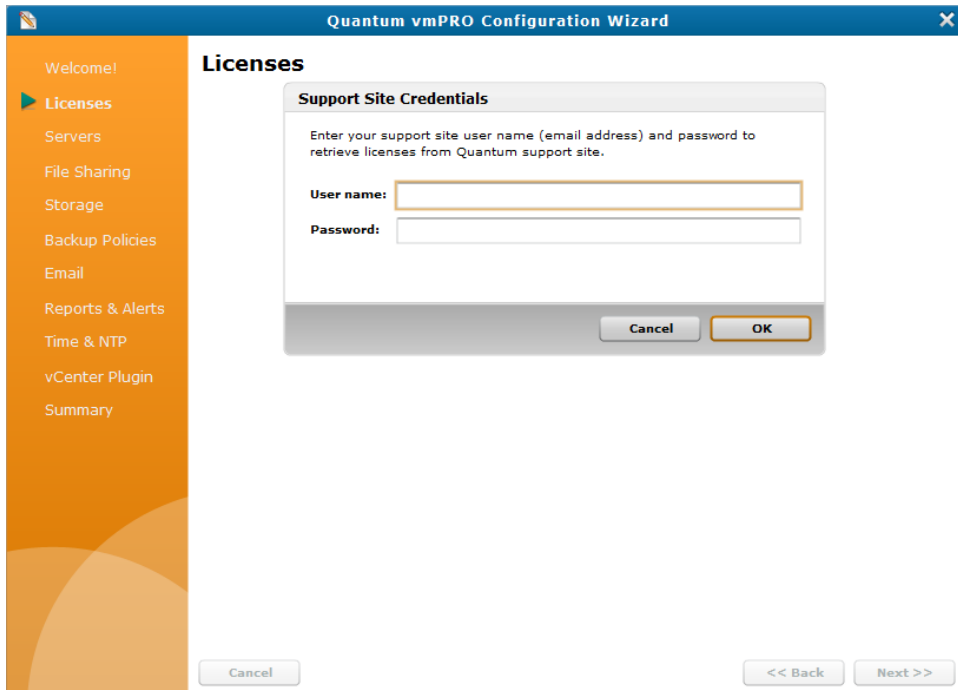
When you configure your vmPRO appliance, you can retrieve your capacity-based license from the vmPRO support site. Upon retrieval, your license is automatically added to your vmPRO appliance. You can then set a capacity warning threshold, which triggers your vmPRO appliance to generate an alert when you are nearing your license's capacity.

Add a capacity-based license to your vmPRO appliance

1. From the **Configure** menu, select **Config Wizard** to display the **Quantum vmPRO Configuration Wizard**.

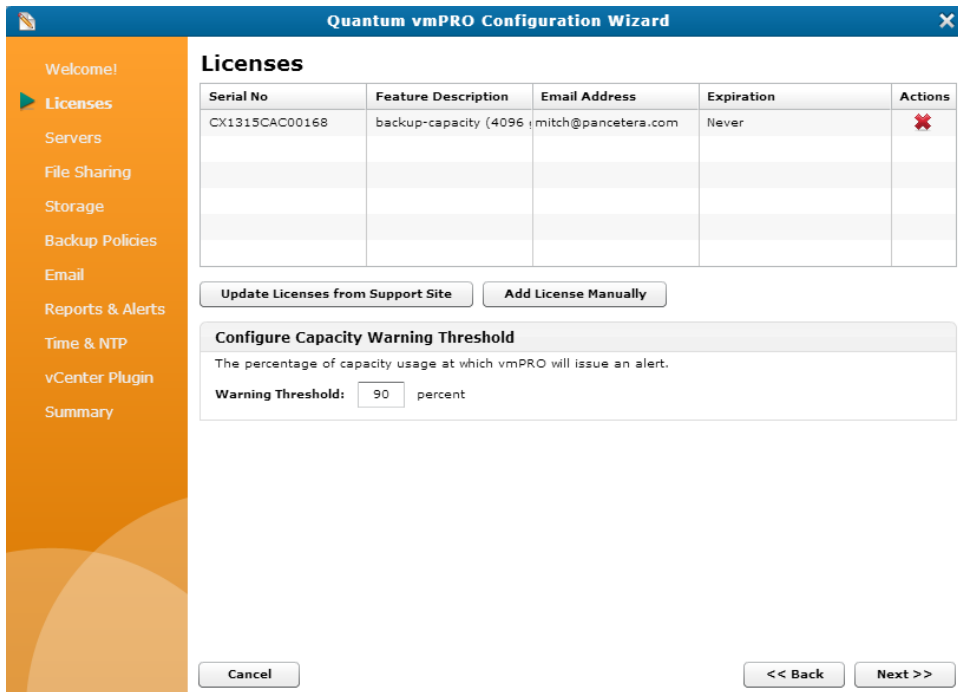
2. Click the **Licenses** tab to display the **Licenses: Support Site Credentials** page.

Figure 16: Licenses: Support Site Credentials Page



3. In the **User name** field, enter your Quantum support email address.
4. In the **Password** field, enter your Quantum support password.
5. Click **OK** to retrieve your license from the Quantum support site, and click **Next** to display any licenses currently added to your vmPRO appliance.

Figure 17: Licenses: Current Licenses Page



6. Click **Update Licenses from Support Site** to add any additional licenses to your vmPRO appliance.

Note: If necessary, you can use the **Add License Manually** option. [See below.](#)

7. In the **Warning Threshold** field, enter a percentage of capacity used. When the amount of the license being used reaches this percentage, the vmPRO appliance issues an alert.
8. Click the **Summary** tab to review your license updates on the **Summary** page.
9. Click **Save** to save updates, click **Next** to proceed to the final page of the wizard, and click **Finish** to exit the wizard.

Caution: Any time you make configuration updates from the **Quantum vmPRO Configuration Wizard**, you must exit the wizard using the **Summary** tab to save your updates. See [Initially Configuring a vmPRO Appliance](#).

Target-Based License

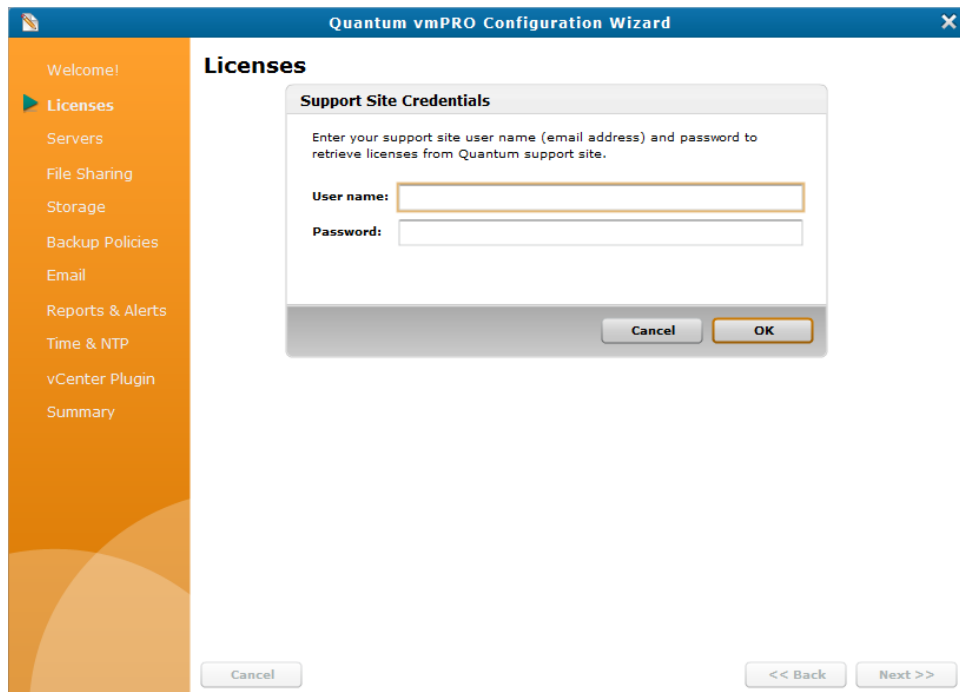
When you configure your vmPRO appliance, you can retrieve your target-based license from the Web site where you received your initial contact email. You need to manually add your license to your vmPRO appliance by copying the license key from the Web site and pasting it in the wizard.

Add a target-based license to your vmPRO appliance

1. From the **Configure** menu, select **Config Wizard** to display the **Quantum vmPRO Configuration Wizard**.

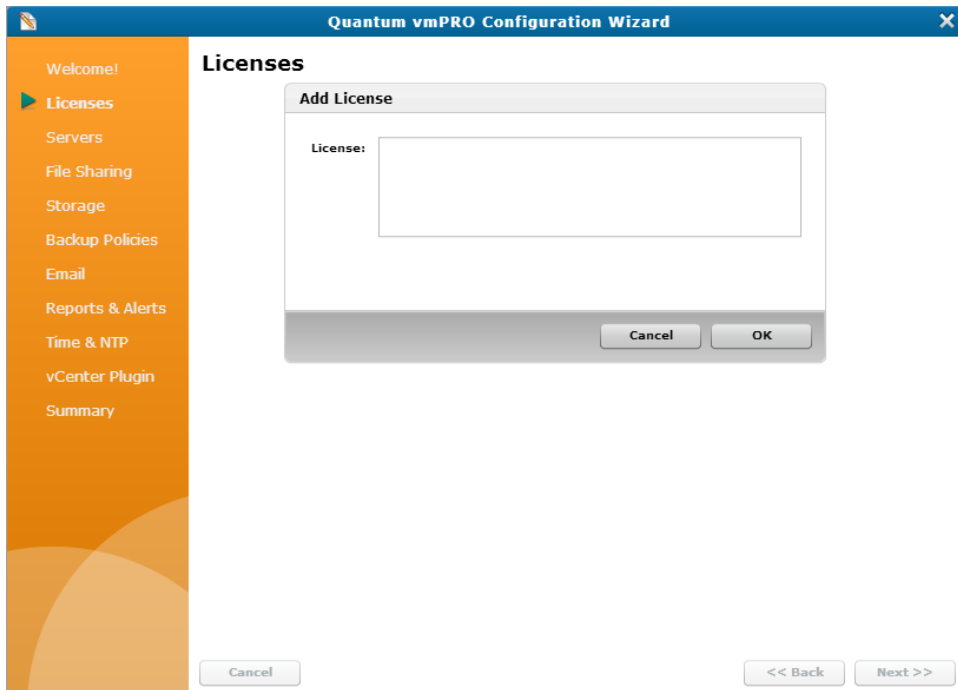
2. Click the **Licenses** tab to display the **Licenses: Support Site Credentials** page.

Figure 18: Licenses: Support Site Credentials Page



3. Click **Cancel** to display any licenses currently added to your vmPRO appliance, and click **Add License Manually** to display the **Licenses: Add License** page.

Figure 19: Licenses: Add License Page



4. In the **License** field, enter the license key.
5. Click **OK** to add the license to your vmPRO appliance.
6. Click the **Summary** tab to review your license updates on the **Summary** page.
7. Click **Save** to save updates, click **Next** to proceed to the final page of the wizard, and click **Finish** to exit the wizard.

Caution: Any time you make configuration updates from the **Quantum vmPRO Configuration Wizard**, you must exit the wizard using the **Summary** tab to save your updates. See [Initially Configuring a vmPRO Appliance](#).

vmPRO Servers

When you set up your vmPRO appliance, you must configure its server or servers.

Quantum vmPRO Supported Servers

Quantum vmPRO supports the following types of servers.

i Note: When configuring a server for your vmPRO appliance, you can select either a single vCenter server to manage ESX servers, **OR** you can select one or more standalone ESX servers. You cannot manage both a vCenter server and ESX servers directly from your appliance.

vCenter Server

Configure a single vCenter server hostname for VM discovery.

If you have the option of using a vCenter server, we recommend that you do so. Because vCenter servers auto-discover all ESX hosts, they allow for ease of use and reduced management overhead.

i Note: In environments using VMware's Virtual SAN (VSAN) configuration, you must set up your vmPRO appliance to manage the configuration through a vCenter server rather than as opposed to managing individual ESX servers. VSAN is a cluster-wide resource that exists as datastores on a cluster of ESX servers. The vmPRO appliance manages VSAN through a vCenter server, which in turn manages the ESX servers housing the VSAN datastores.

ESX Server

Configure one or more standalone ESX servers.

For information regarding vSphere ESX host datastore and storage considerations, see the "vSphere ESX Host Notes and Best Practices" section of the [Quantum vmPRO Best Practices Guide](#).

Discovering Servers

Before the vmPRO appliance can connect to newly added servers, it must discover the servers.

The discovery process is typically an automatic process. You can manually discover servers, as needed. When the discovery process is complete, you can view your configured servers and their virtual machines (VMs) on the VMs console. See [Navigating the vmPRO VMs Console](#).

Configuring a vCenter Server for a vmPRO Appliance

Configure a vCenter server from the **Quantum vmPRO Configuration Wizard**.

Considerations

Before configuring a vCenter server, consider the following items:

Single vCenter Server Support

You can only use a single vCenter server for your vmPRO appliance. If an existing vCenter server is configured for your appliance, you must delete it before adding a new vCenter server.

Managing Through a vCenter Server

When configuring a server for your vmPRO appliance, you can select either a single vCenter server to

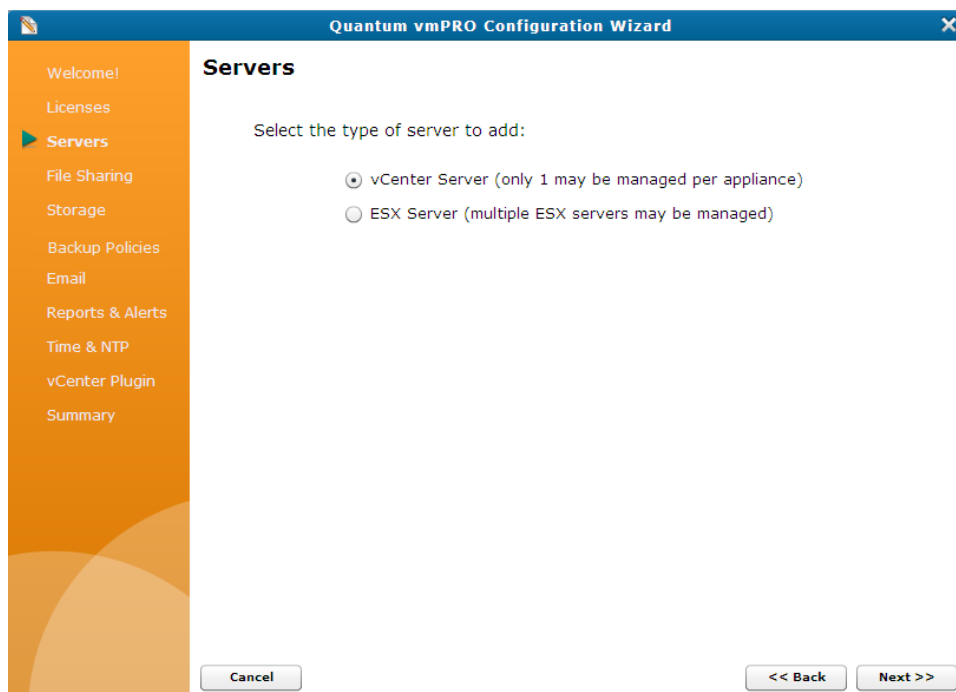
manage ESX servers, **OR** you can select one or more standalone ESX servers. You cannot manage both a vCenter server and ESX servers directly from your appliance. Before adding a new vCenter server, you must delete any ESX servers that are configured for your appliance.

In environments using VMware's Virtual SAN (VSAN) configuration, you must set up your vmPRO appliance to manage the configuration through a vCenter server, rather than managing individual ESX servers. VSAN is a cluster-wide resource that exists as datastores on a cluster of ESX servers. The vmPRO appliance manages VSAN through a vCenter server, which in turn manages the ESX servers housing the VSAN datastores.

Delete an existing vCenter server from your vmPRO appliance

1. From the **Configure** menu, select **Config Wizard** to display the **Quantum vmPRO Configuration Wizard**.
2. Click the **Servers** tab to display the **Servers** page.

Figure 20: Servers Page



3. Select **vCenter Server** and click **Next** to display one of the following:

If you currently have a vCenter server configured, the vCenter Server page displays:

- a. Click **Delete vCenter** to delete the current vCenter server.
- b. At the **No vCenter is configured** prompt, click **Add vCenter** to display the **Configure Server** page.

Figure 21: vCenter Server Page

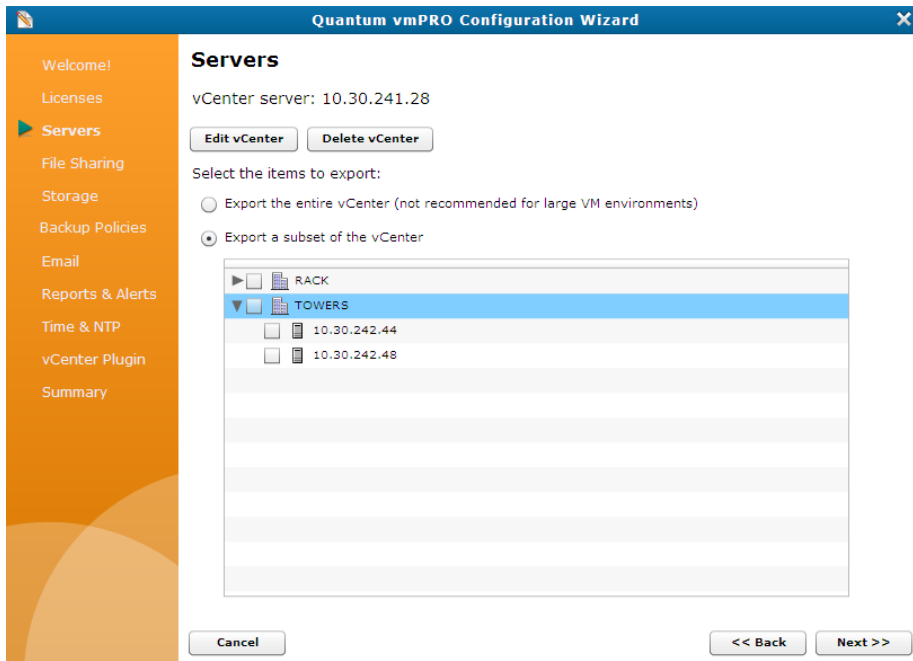
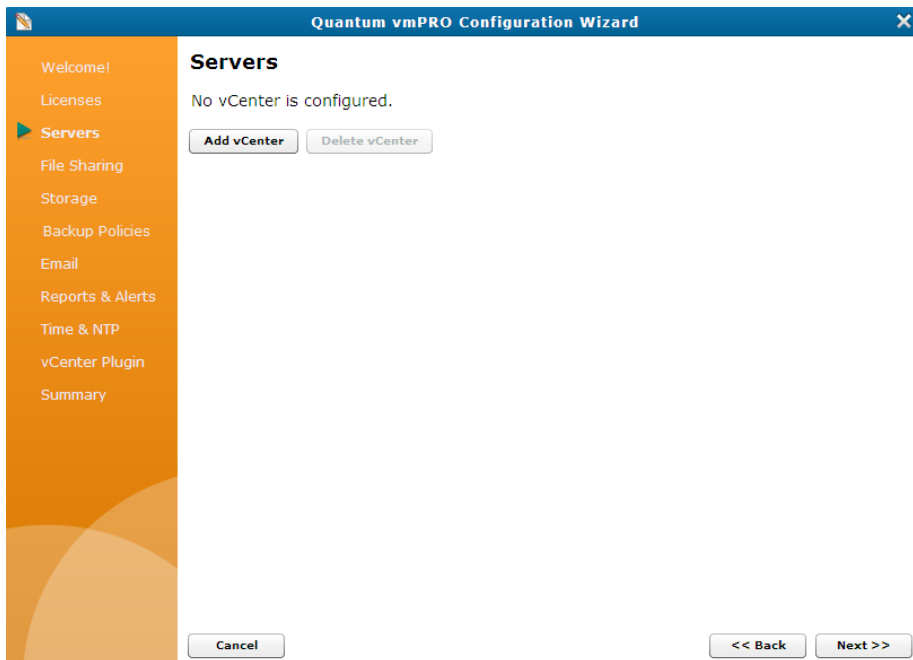


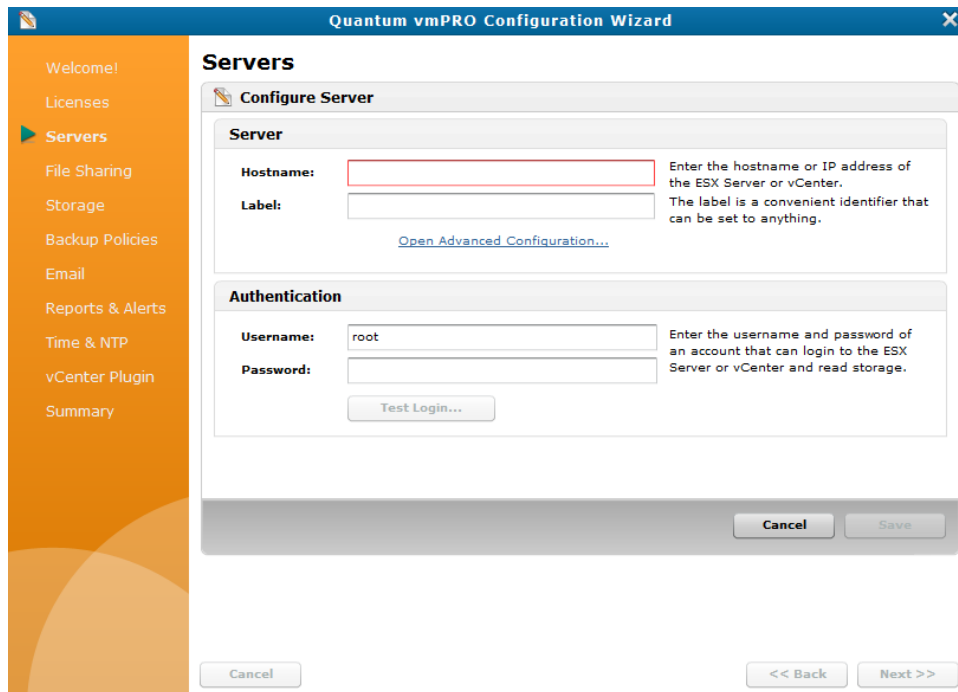
Figure 22: No vCenter Is Configured Page



i Note: If you are adding an ESX server, click **Back** to return to the **Servers** page. See [Configuring ESX Servers for a vmPRO Appliance](#).

If there is not another vCenter server configured, the Configure Server page displays.

Figure 23: Configure Server Page

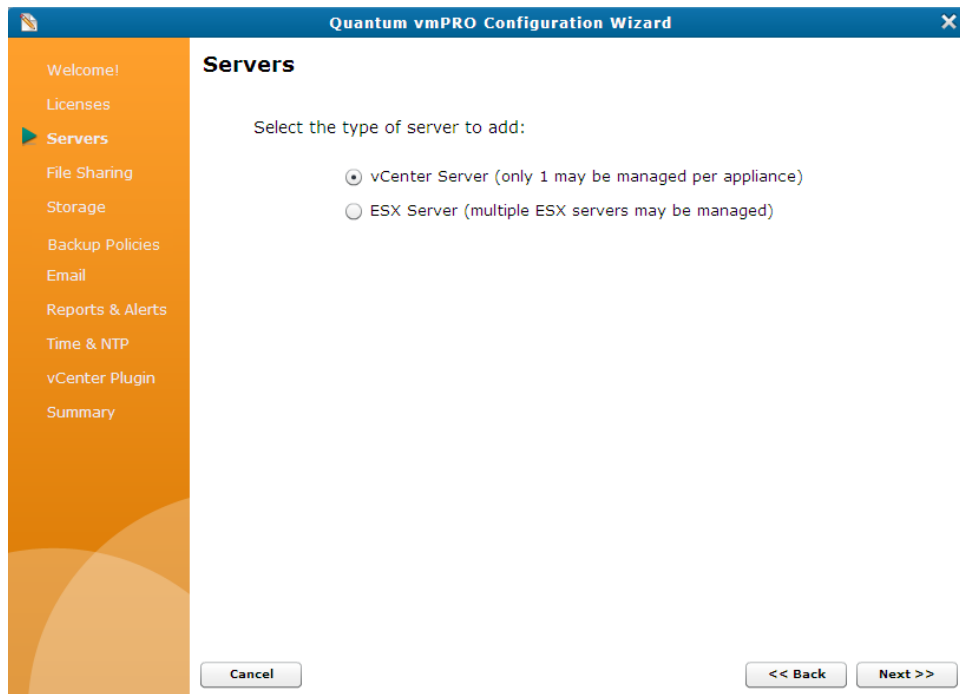


Delete existing ESX servers from your vmPRO appliance

1. From the **Configure** menu, select **Config Wizard** to display the **Quantum vmPRO Configuration Wizard**.

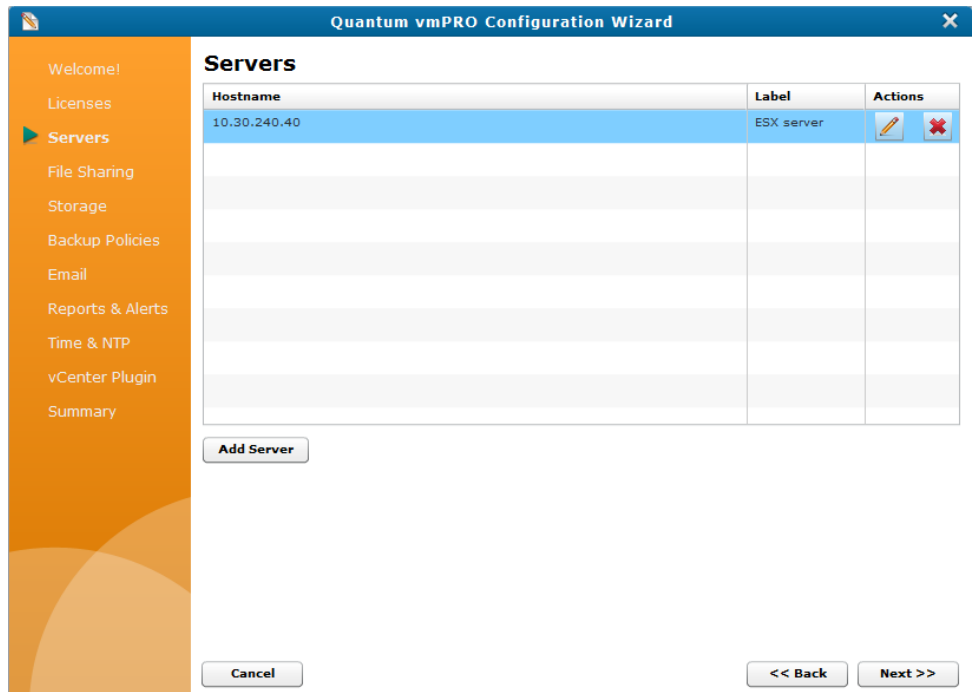
2. Click the **Servers** tab to display the **Servers** page.


Figure 24: Servers Page



3. Select **ESX Server**, and click **Next** to display a list of existing ESX servers configured for your appliance.

Figure 25: ESX Server List



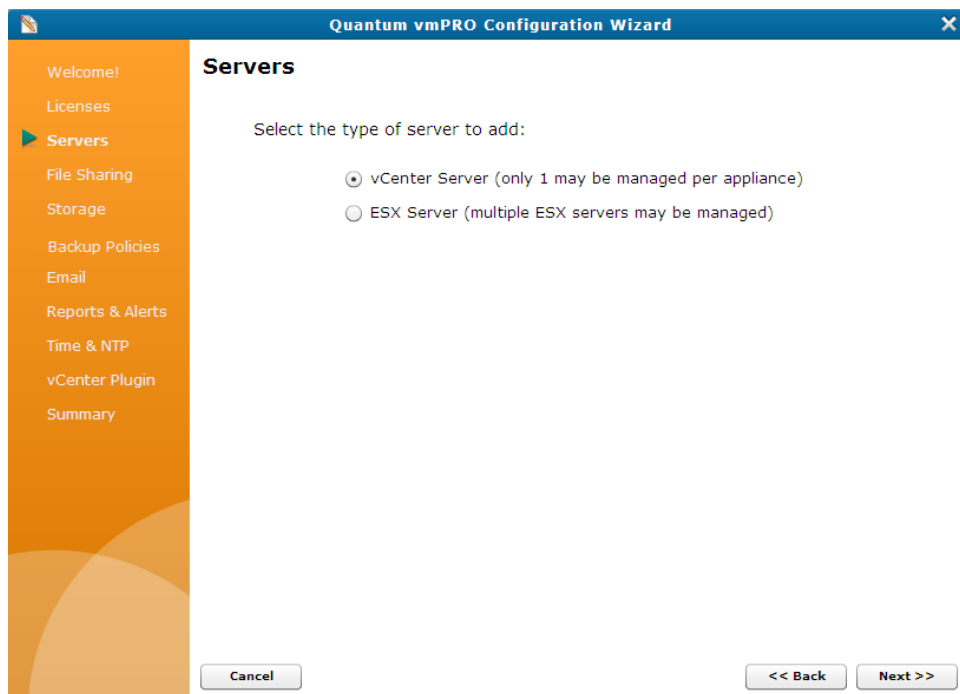
4. In the **Actions** column, click  to remove each server from your appliance.
5. Click **Back** to return to the **Servers** page.

Configure a vCenter Server

1. From the **Configure** menu, select **Config Wizard** to display the **Quantum vmPRO Configuration Wizard**.

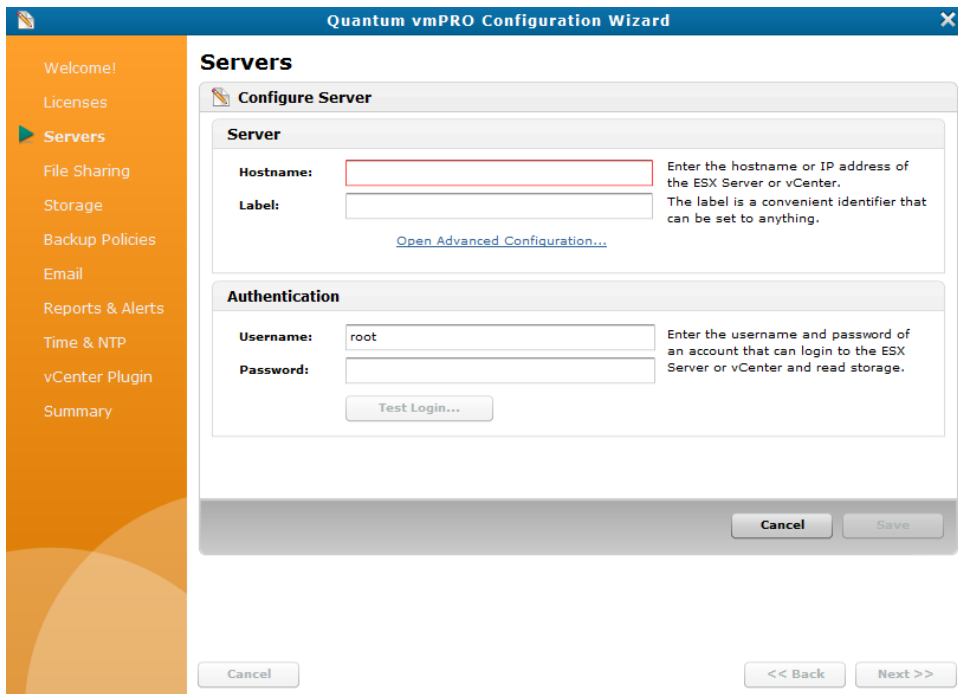
2. Click the **Servers** tab to display the **Servers** page.

Figure 26: Servers Page



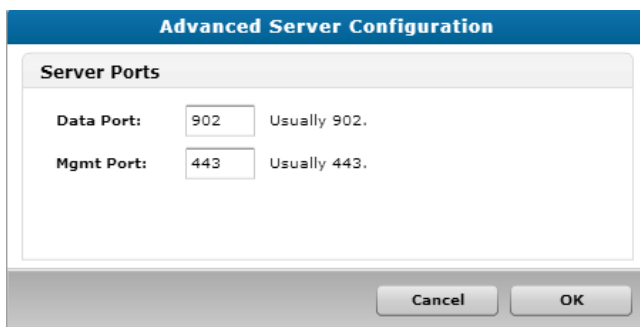
3. Select **vCenter Server** and click **Next** to display the **Configure Server** page.

Figure 27: Configure Server Page



4. In the **Hostname** field of the **Server** pane, enter the host name or IP address assigned to the server.
5. In the **Label** field of the **Server** pane, enter a label to assign to the server, as needed.
6. In the **Server** pane, click the **Open Advanced Configuration** link to display the **Advanced Server Configuration** dialog box.

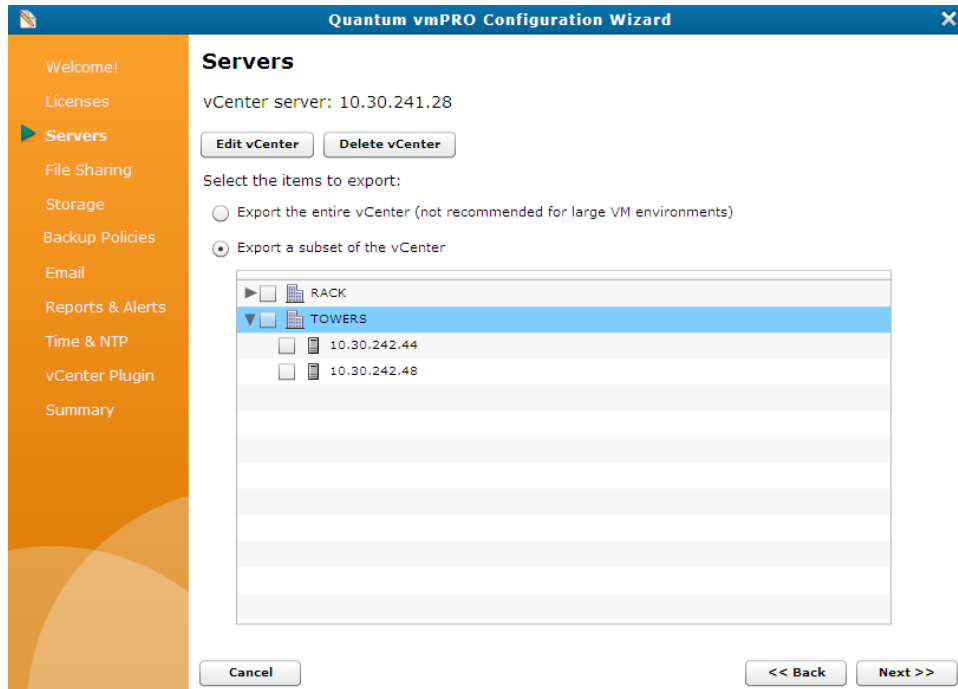
Figure 28: Advanced Server Configuration Dialog Box



7. In the **Data Port** and **Mgmt Port** fields, edit the server ports, as needed, and click **OK** to return to the **Configure Server** page.

8. In the **Username** and **Password** fields of the **Authentication** pane, enter the login credentials needed to access server read storage.
9. In the **Authentication** pane, click **Test Login** to verify that the login credentials work.
10. Click **Save** to save updates and display the **vCenter server** page.

Figure 29: vCenter Server Page



11. Select one of the following options:

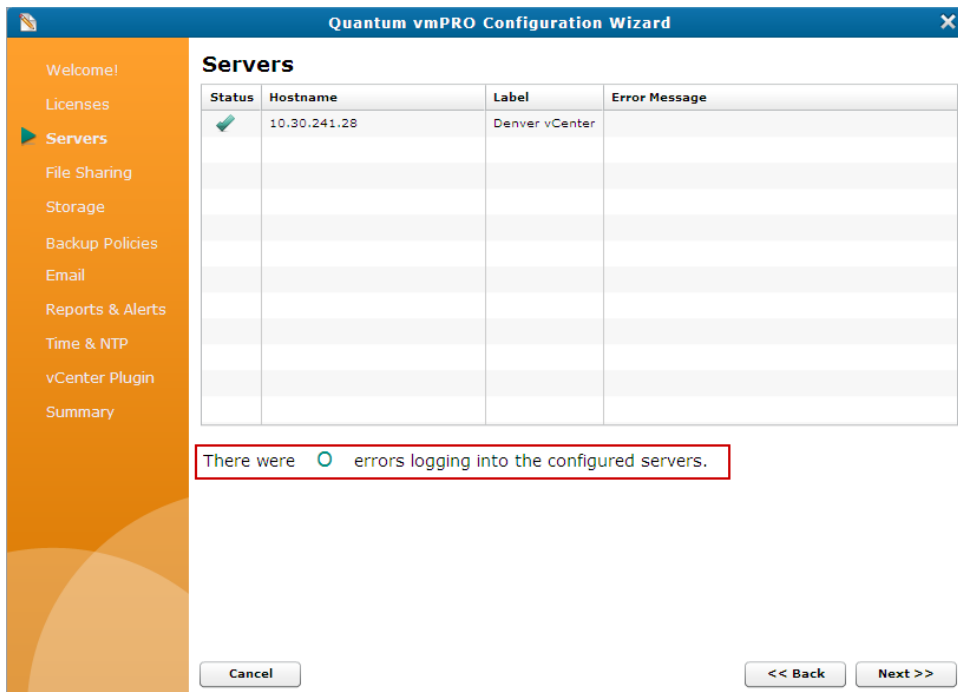
- **Export the entire vCenter** – Exports your entire vCenter server and all associated ESX hosts.

i Note: We do not recommend exporting entire vCenter servers as this type of export can exponentially increase backup times.

- **Export a subset of the vCenter** – Exports selected ESX hosts. Select the hosts to include in the export.

- Click **Next** to display the vCenter server in the **Servers** list.

Figure 30: Servers List



- Save changes and exit the wizard.

Caution: Any time you make configuration updates from the **Quantum vmPRO Configuration Wizard**, you must exit the wizard using the **Summary** tab to save your updates. See [Initially Configuring a vmPRO Appliance](#).

Configuring ESX Servers for a vmPRO Appliance

Configure ESX servers from one of the following locations in your vmPRO GUI:

- The **Configure Server** dialog box, which you can access from the **VMs** console or the **Configure** menu.
- The **Configure Server** page, which you can access from the **Quantum vmPRO Configuration Wizard**.

Considerations

Before configuring ESX servers, consider the following items:

Server Management

When configuring a server for your vmPRO appliance, you can select either a single vCenter server to manage ESX servers, **OR** you can select one or more standalone ESX servers. You cannot manage both a vCenter server and ESX servers directly from your appliance. If you currently have a vCenter server configured for your appliance, you need to delete it before adding an ESX server. See [Configuring a vCenter Server for a vmPRO Appliance](#).

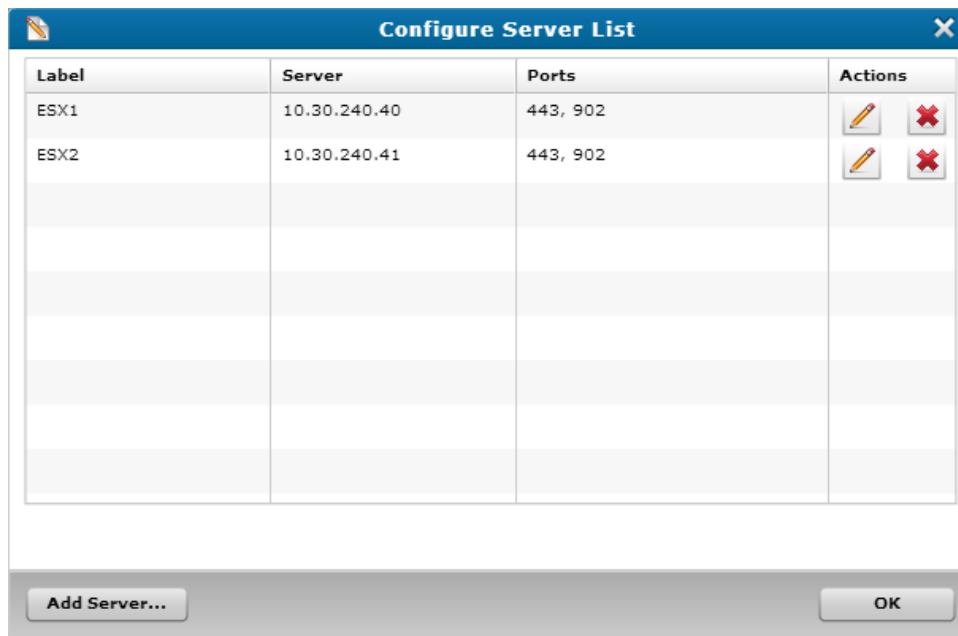
VMware VSAN

In environments using VMware's Virtual SAN (VSAN) configuration, you must set up your vmPRO appliance to manage the configuration through a vCenter server, rather than managing individual ESX servers. VSAN is a cluster-wide resource that exists as datastores on a cluster of ESX servers. The vmPRO appliance manages VSAN through a vCenter server, which manages the ESX servers housing the VSAN datastores.

Access the Configure Server dialog box from the VMs Console

1. On the vmPRO appliance GUI, click the **VMs** button to display the **VMs** console.
2. Click the **Resources** tab, as needed.
3. In the **Servers** pane, click **Configure** to display the **Configure Server List** dialog box.

Figure 31: Configure Server List Dialog Box



- Click **Add Server** to display the **Configure Server** dialog box.

Figure 32: Configure Server Dialog Box

Configure Server

Server

Hostname: Enter the hostname or IP address of the ESX Server or vCenter.

Label: The label is a convenient identifier that can be set to anything.

[Open Advanced Configuration...](#)

Authentication

Username: Enter the username and password of an account that can login to the ESX Server or vCenter and read storage.

Password:

Access the Configure Server dialog box from the Configure menu

- From the **Configure** menu, select **Servers** to display the **Configure Server List** dialog box.

Figure 33: Configure Server List Dialog Box

Configure Server List

Label	Server	Ports	Actions
ESX1	10.30.240.40	443, 902	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
ESX2	10.30.240.41	443, 902	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

2. Click **Add Server** to display the **Configure Server** dialog box.

Figure 34: Configure Server Dialog Box

Configure Server

Server

Hostname: Enter the hostname or IP address of the ESX Server or vCenter.

Label: The label is a convenient identifier that can be set to anything.

[Open Advanced Configuration...](#)

Authentication

Username: Enter the username and password of an account that can login to the ESX Server or vCenter and read storage.

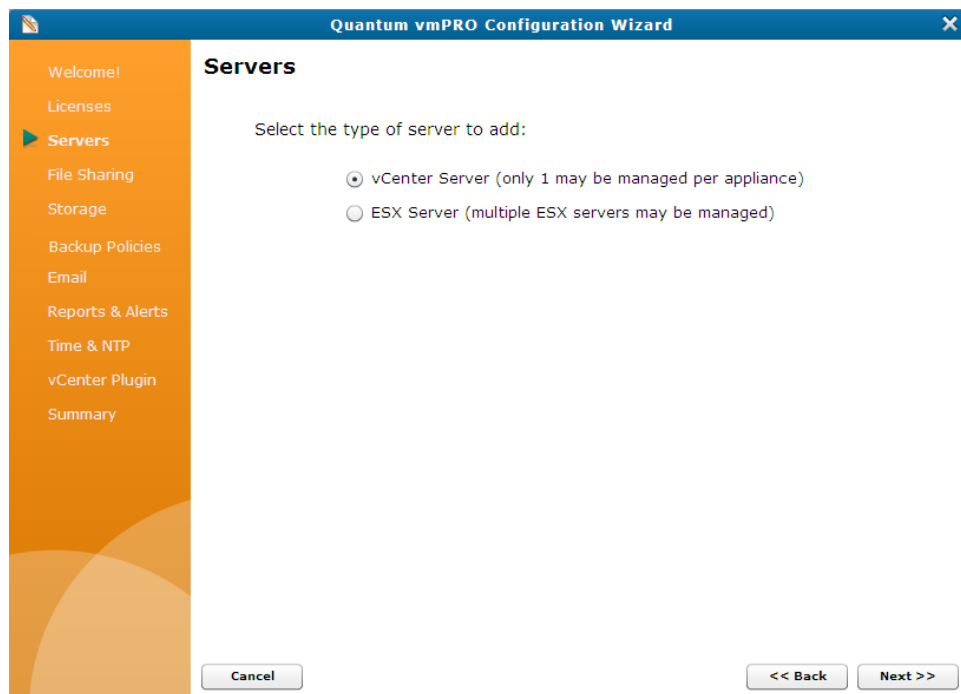
Password:

Access the Configure Server page for ESX servers from the Quantum vmPRO Configuration Wizard

1. From the **Configure** menu, select **Config Wizard** to display the **Quantum vmPRO Configuration Wizard**.

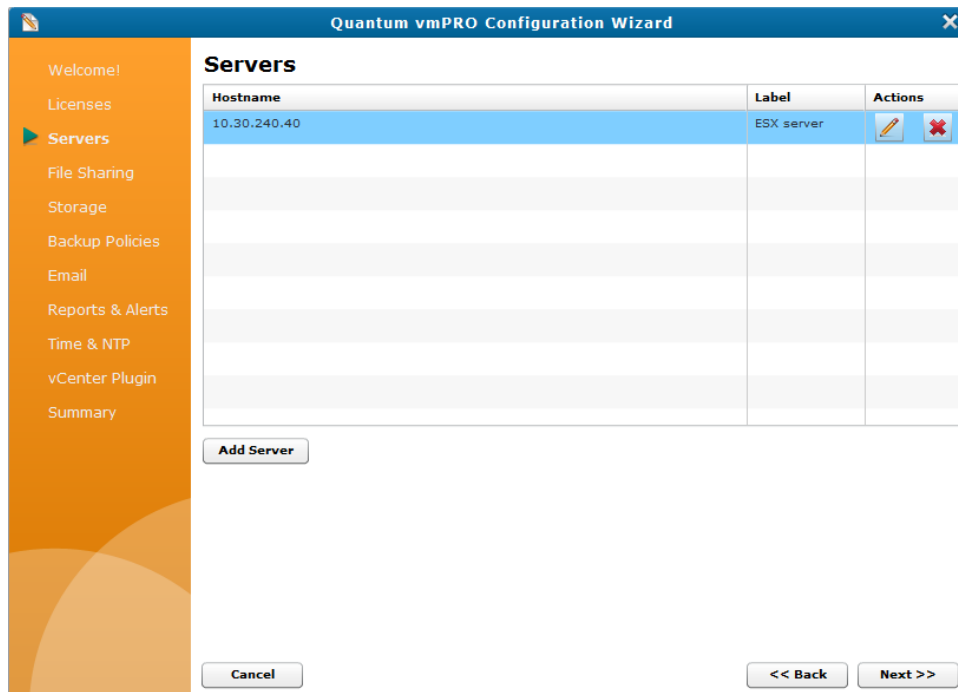
2. Click the **Servers** tab to display the **Servers** page.

Figure 35: Servers Page



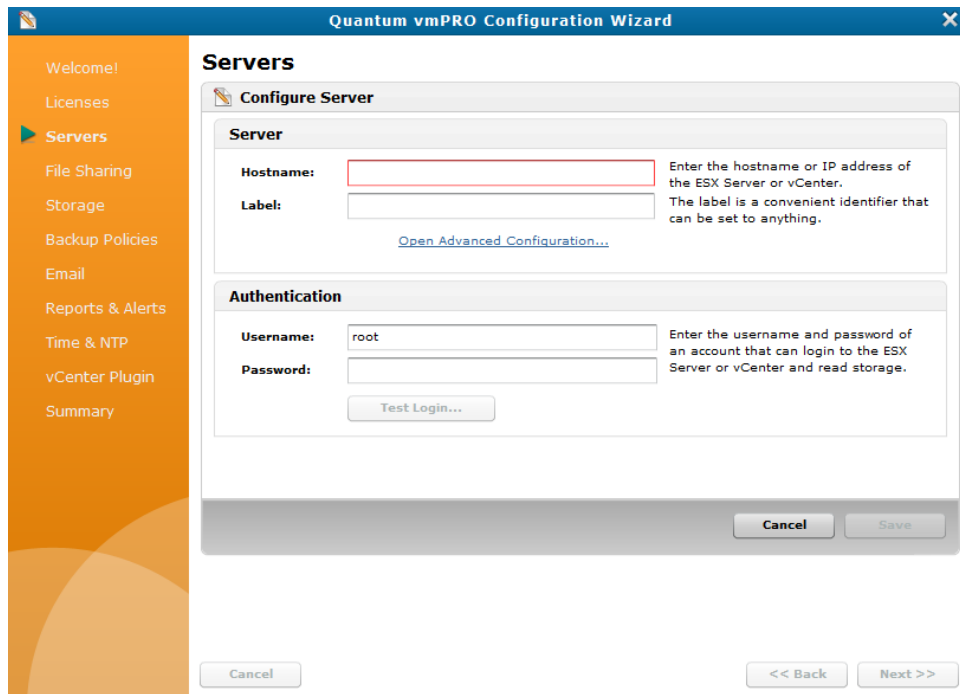
3. Select **ESX Server** and click **Next** to display the **Server** list.

Figure 36: Server List



4. Click **Add Server** to display the **Configure Server** page.

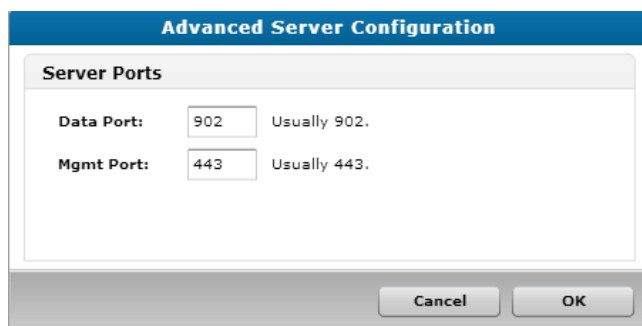
Figure 37: Configure Server Page



Configure an ESX server for your vmPRO appliance

1. Display the **Configure Server** dialog box or the **Configure Server** page, as appropriate.
2. In the **Hostname** field of the **Server** pane, enter the host name or IP address to assign to the server.
3. In the **Label** field of the **Server** pane, enter a label to assign to the server, as needed.
4. In the **Server** pane, click the **Open Advanced Configuration** link to display the **Advanced Server Configuration** dialog box.

Figure 38: Advanced Server Configuration Dialog Box



5. In the **Data Port** and **Mgmt Port** fields, edit the server ports, as needed, and click **OK** to return to the **Configure Server** dialog box.
6. In the **Username** and **Password** fields of the **Authentication** pane, enter the login credentials needed to access server read storage.
7. In the **Authentication** pane, click **Test Login** to verify that the login credentials work.
8. Depending on where you configured the ESX server, do the following:

From the Configure Server dialog box:

- a. Click **Save** to save updates and return to the **Configure Server List** dialog box.
- b. Verify that the server has been added to your appliance, and click **OK** to exit the dialog box.

From the Configure Server page:

- a. Click **Save** and click **Next** to return to the **Configure Server List**.
- b. Verify that the server has been added to your appliance.
- c. Save your changes and exit the wizard.

⚠ Caution: Any time you make configuration updates from the **Quantum vmPRO Configuration Wizard**, you must exit the wizard using the **Summary** tab to save your updates. See [Initially Configuring a vmPRO Appliance](#).

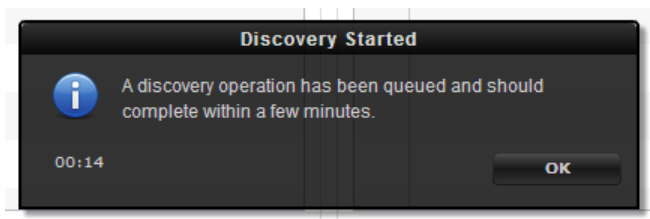
Discovering Servers for a vmPRO Appliance

The vmPRO appliance must discover all servers before using them. This discovery process usually occurs automatically. If the automatic discovery process does not discover a new server, you can manually discover servers.

Manually discover servers

- From the **Operations** menu, select **Discover Now** to display the **Discovery Started** alert box.

Figure 39: Discovery Started Alert Box



When the discovery process is complete, the alert box no longer displays.

NAS Targets and File Sharing Protocols

Your vmPRO appliance uses Network Attached Storage (NAS) targets, as follows.

User-Accessible Shares

The vmPRO appliance exports the **/export** and **/recover** directories as Network Attached Storage (NAS) targets. After being exported, [pre-configured users](#) can access the **/export** and **/recover** directories as mounted shares.

Use these directories to access the following:

/export

The **/export** directory gives you direct access to the virtual machines (VMs) running on the ESX server.

/recover

The **/recover** directory gives you access to the VMs' backed-up data.

File Sharing Protocols

For users to access exported data, you must first configure file sharing protocols to present the directories in a format that you and other network users can access. Configure one or both of the following file sharing protocols:

Protocol	Description
CIFS	A Common Internet File System (CIFS) file sharing protocol is typically used with Windows-based servers. When you configure a CIFS file sharing protocol, define the users who can access the CIFS share.
NFS	A Network File System (NFS) file sharing protocol is typically used with Linux-based servers. When you configure an NFS file sharing protocol, define the file systems and hosts that can access the NFS share.

Consideration

Keep in mind that the operating system (OS) running on the VMs could dictate the best file sharing protocol to use.

Example

In cases where Windows systems need to directly access backed-up files from a CIFS share, select a CIFS protocol.

Or

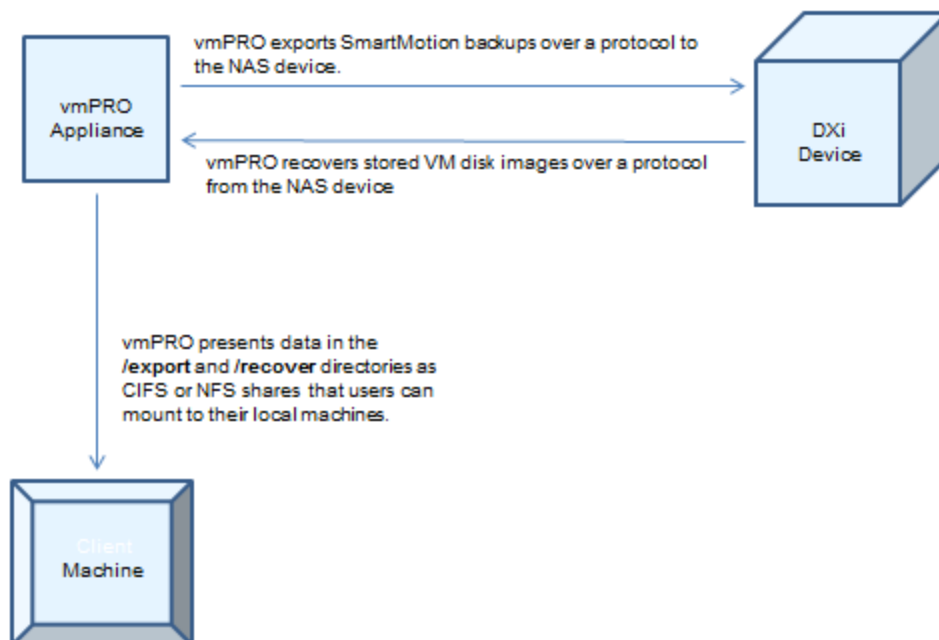
In cases where Linux host integration is a priority, select an NFS protocol.

i Note: We strongly recommend using the NFS protocol for Linux client machines accessing the vmPRO **/export** directory. If a Linux client machine uses the CIFS protocol, specify the **directio** mount option at the **mount** command. For example: `# mount.cifs -o ..,directio <share> <mount point>`

Back-End Storage

The vmPRO appliance exports SmartMotion™ backups to NAS devices, such as a Quantum DXi device. This data is stored in the NAS device as a VM disk image. Users cannot directly access this stored data. Instead, the vmPRO appliance communicates to the device over a CIFS or NFS protocol, both to store backed-up VM disk images and to recover the stored VM disk images. The vmPRO appliance presents the stored data to authorized users and machines in the **/recover** directory as CIFS or NFS shares (see above).

Figure 40: NAS Presentation Example



Before performing SmartMotion backups, you need to configure NAS target devices to which to export data.

Configuring a CIFS Protocol for a vmPRO Appliance

When you configure a CIFS protocol for your vmPRO appliance, you are defining who can access the exported data in the CIFS share. Use Workgroup or Active Directory (AD) Authentication to define user access. Authenticated users can mount the CIFS share as a Windows network drive on their local machine.

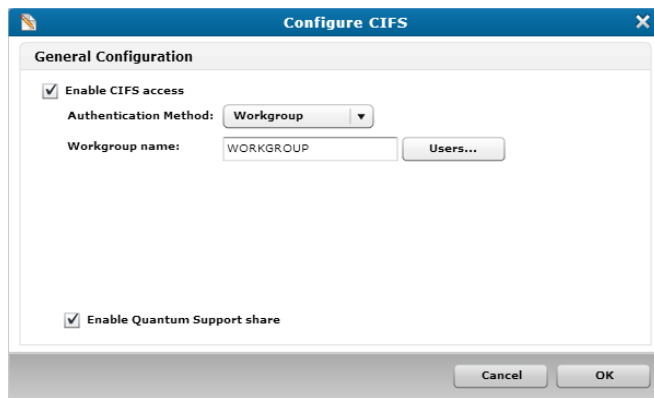
Accessing CIFS Authentication Configuration

You can configure authentication for a CIFS protocol from the **Configure** menu or the **Quantum vmPRO Configuration Wizard**.

Display the Configure CIFS dialog box

- From the **Configure** menu, select **CIFS**.

Figure 41: Configure CIFS Dialog Box

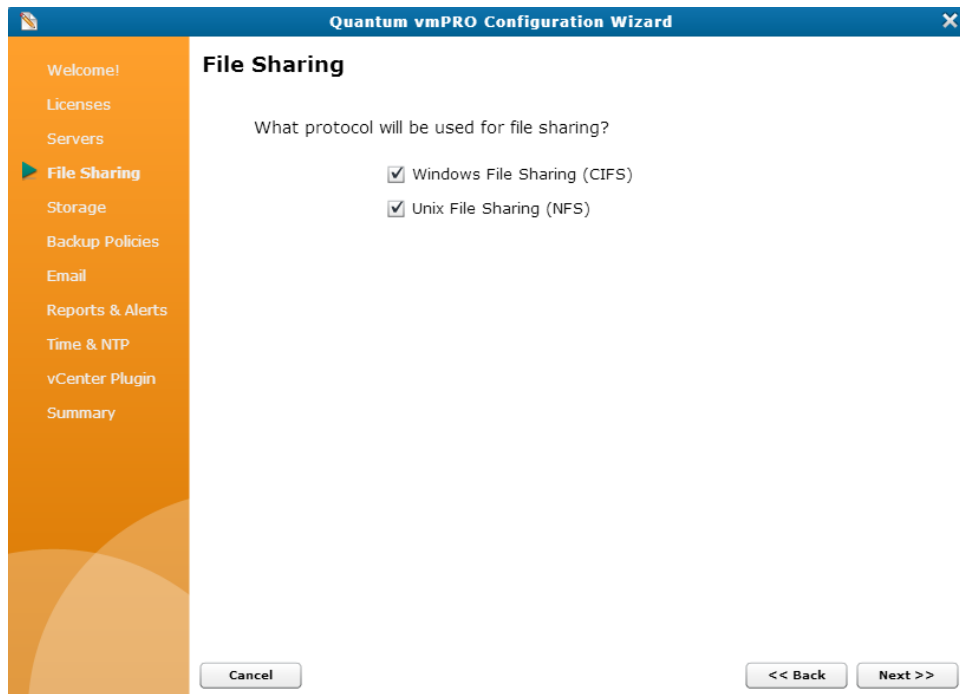


Display the CIFS General Configuration page

1. From the **Configure** menu, select **Config Wizard** to display the **Quantum vmPRO Configuration Wizard**.

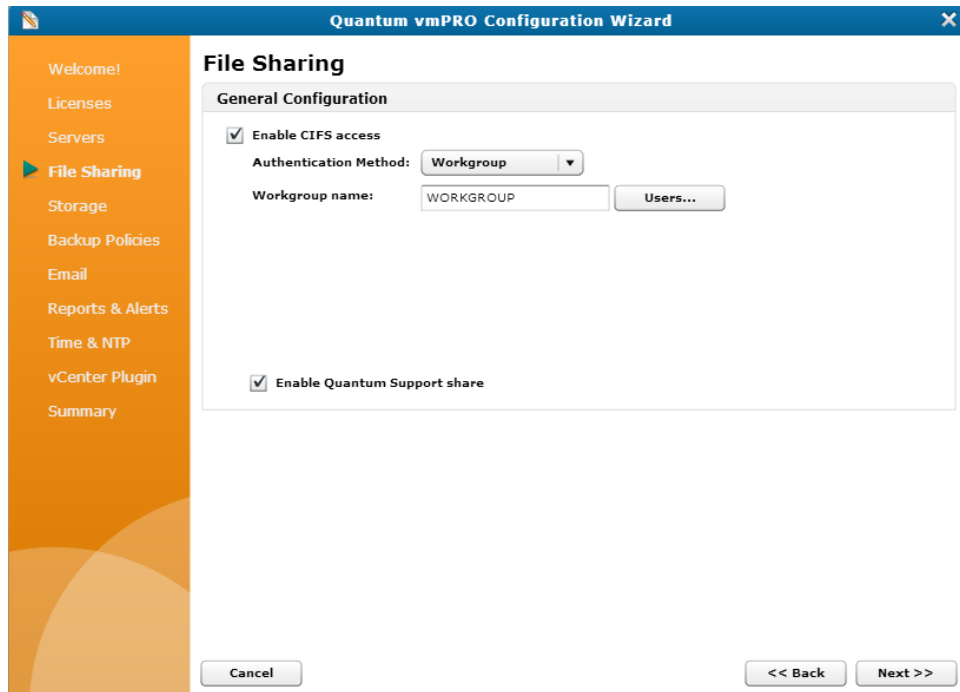
2. Click the **File Sharing** tab to display the **File Sharing** page.

Figure 42: File Sharing Page



3. Select the **Windows File Sharing (CIFS)** check box, as needed, and click **Next** to display the CIFS **General Configuration** page.

Figure 43: CIFS General Configuration Page



WorkGroup Authentication

Configure Workgroup Authentication for your CIFS protocol to authorize user access based on [credentials](#)¹ defined in the **Configure User** dialog box. When you add users to a work group created for the CIFS protocol, you authorize them to access the exported data on the CIFS share.

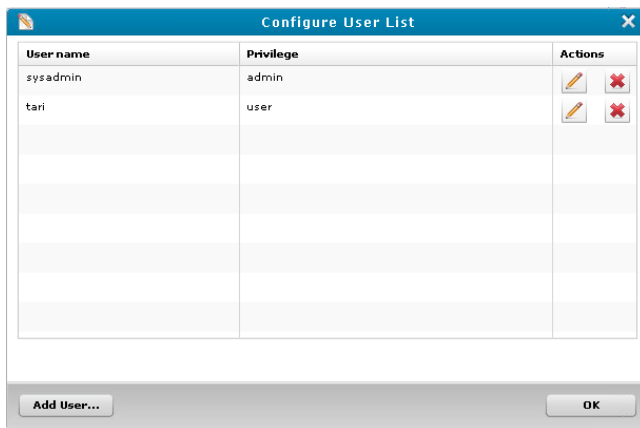
Configure Workgroup Authentication for a CIFS protocol

1. On the **Configure CIFS** dialog box or **CIFS General Configuration** page, select the **Enable CIFS access** check box, as needed.
2. In the **Authentication Method** drop-down list, select **Workgroup**.
3. In the **Workgroup name** field, edit the work group name, as needed.

¹User name and password

- Click **Users** to display **Configure User List** dialog box.

Figure 44: Configure User List Dialog Box



- Select the users to add to the work group, and click **OK** to return to the **Configure CIFS** dialog box or **CIFS General Configuration** page.

Note: User credentials must be configured before you can add a user to a work group. See [Configuring Users for a vmPRO Appliance](#).

- Select the **Enable Quantum Support share** check box to enable the Quantum support team to access the CIFS share when support is needed.
- Click **OK** to save changes and exit the dialog box, or save changes and exit the wizard.

Caution: Any time you make configuration updates from the **Quantum vmPRO Configuration Wizard**, you must exit the wizard using the **Summary** tab to save your updates. See [Initially Configuring a vmPRO Appliance](#).

AD Authentication

Configure AD Authentication for your CIFS protocol to authorize user access based on AD domain controllers. Users who are authenticated against these domain controllers can access the exported data on the CIFS share.

Requirements

To use authentication with your vmPRO appliance:

- You must use a server with Windows 2003 or 2008.
- Your vmPRO appliance's main DNS server must be in the same domain as the vmPRO appliance. See [Configuring Network Settings for a vmPRO Appliance](#).

Configure AD Authentication for a CIFS protocol

1. On the **Configure CIFS** dialog box or **CIFS General Configuration** page, select the **Enable CIFS access** check box, as needed.
2. In the **Authentication Method** drop-down list, select **Active Directory** to display additional authentication fields, in the **CIFS General Configuration Page**.

Figure 45: Configure CIFS Dialog Box – Authentication Method

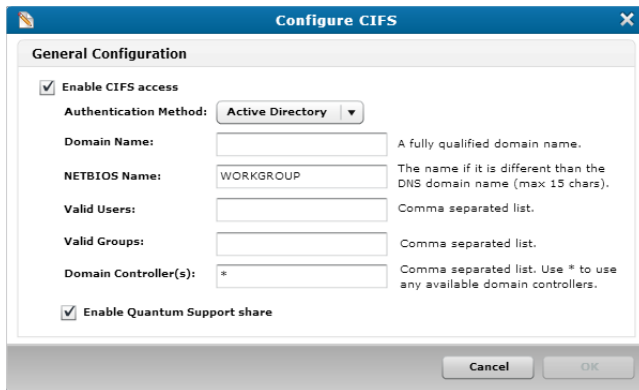
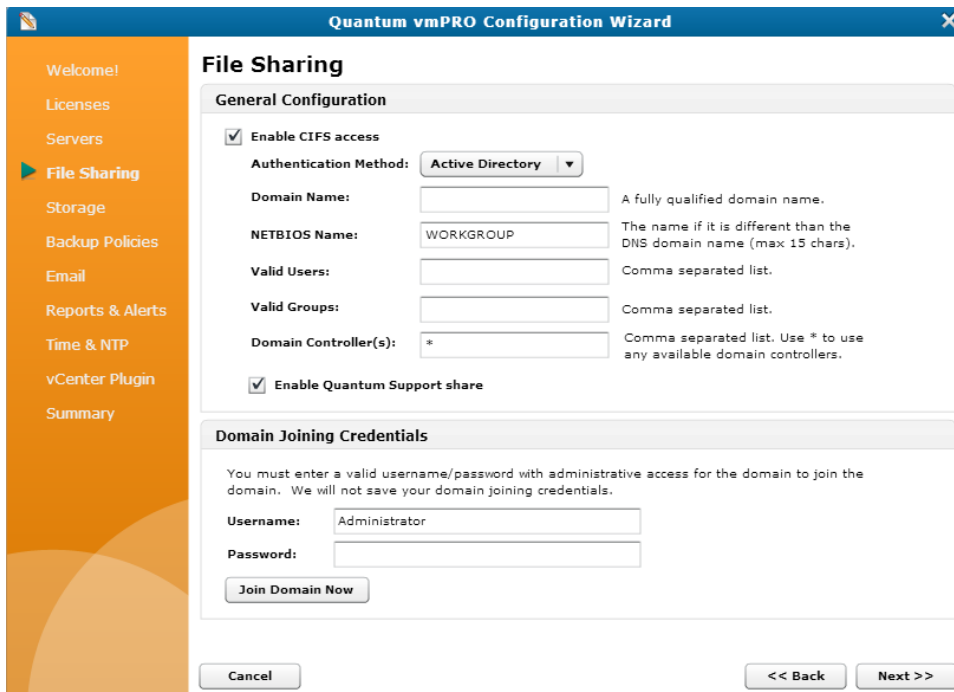



Figure 46: CIFS General Configuration Page – Active Directory Authentication Fields



3. In the **Domain Name** field, enter the fully qualified domain name for your AD's host.

4. In the **NETBIOS Name** field, enter the NetBIOS name of the AD.
5. In the **Valid Users** field, enter a list of AD-defined users who can access the CIFS share. Separate each user with a comma.
6. In the **Valid Groups** field, enter a list of AD-defined groups that can access the CIFS share. Separate each group with a comma.
7. In the **Domain Controller(s)** field, do one of the following:
 - Enter a list of domain controllers to use in authenticating access. Separate each domain controller with a comma, **OR**.
 - Enter an asterisk (*) to use any available domain controllers to authenticate access.

 **Note:** If you need to remove a vmPRO appliance from a domain controller, you must do so manually.


8. Select the **Enable Quantum Support share** check box to enable the Quantum support team to access the CIFS share when support is needed.
9. Do one of the following:

From the Configure CIFS dialog box:

- a. Click **OK** to display the **CIFS Change** popup reminding you that active connections will be disconnected if you continue.
- b. Click **OK** to display the **Join Domain** dialog box.
- c. In the **Username** field, enter a user name for an account with authority to join the domain.
- d. In the **Password** field, enter the password for the account.
- e. Click **Join** to join the domain and exit the dialog box.

From the CIFS General Configuration page:

- a. In the **Username** field of the **Domain Joining Credentials** pane, enter a user name for an account with authority to join the domain.
- b. In the **Password** field of the **Domain Joining Credentials** pane, enter the password for the account.
- c. Click **Join Domain Now** to join the domain.
- d. Save changes and exit the wizard.

 **Caution:** Any time you make configuration updates from the **Quantum vmPRO Configuration Wizard**, you must exit the wizard using the **Summary** tab to save your updates. See [Initially Configuring a vmPRO Appliance](#).

Mounting a CIFS Share as a Windows Network Drive

Mount a CIFS share as a Windows network drive to access the **/export**, **/recover/images**, and **/recover/files** directories through Windows. In addition, you can use drag-and-drop functionality to copy data from the share to your local machine.

i Note: We strongly recommend using the NFS protocol for Linux client machines accessing the vmPRO **/export** network file system. If a Linux client machine uses the CIFS protocol, specify the **directio** mount option at the **mount** command. For example: `# mount.cifs -o ..,directio <share> <mount point>`

i Note: A system administrator must first configure the NAS target to enable client CIFS mounting. See [Configuring NAS Targets for SmartMotion Backups](#).

To mount your CIFS share as a Windows network drive:

1. Display Windows Explorer.
2. Click **Map network drive** to display the dialog box.
3. In the **Drive** field, select the drive letter to which to map the CIFS share.
4. In the **Folder** field, enter `\\<vmPRO-Host_IP>\<directory>`, where **vmPRO-Host_IP** is the IP address for your vmPRO appliance and **directory** is the name of the directory that you mount as the CIFS share.
5. Select the **Reconnect at logon** and **Connect using different credentials** check boxes, as needed.
6. Click **Finish** to mount the CIFS share as a network drive.

Configuring an NFS Protocol for a vmPRO Appliance

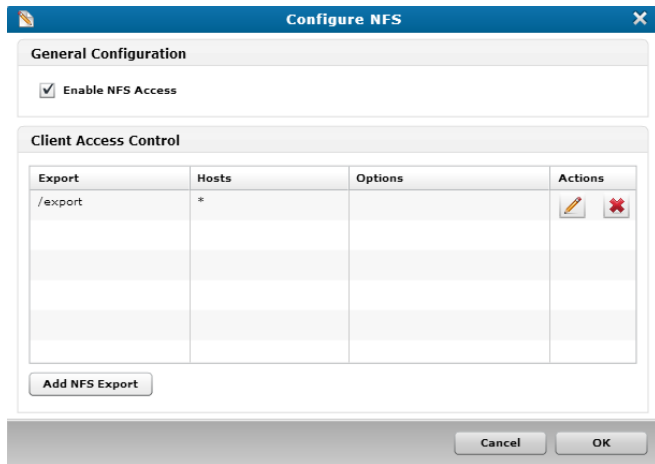
When you configure an NFS file sharing protocol for your vmPRO appliance, you are defining the file systems and hosts that can access the exported vmPRO data.

You can configure an NFS file sharing protocol from the **Configure** menu or the **Quantum vmPRO Configuration Wizard**. In addition, you can edit or delete NFS protocols from these locations.

Display the Configure NFS dialog box

- From the **Configure** menu, select **NFS**.

Figure 47: Configure NFS Dialog Box



Display the NFS General Configuration page

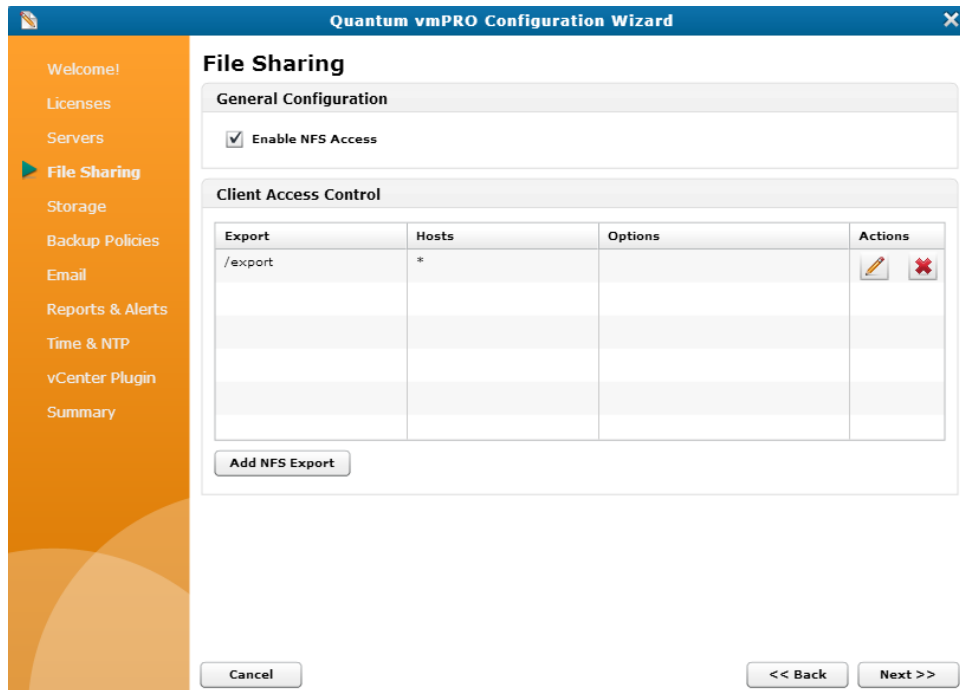
1. From the **Configure** menu, select **Config Wizard** to display the **Quantum vmPRO Configuration Wizard**.
2. Click the **File Sharing** tab to display the **File Sharing** page.

Figure 48: File Sharing Page



3. Select the **Unix File Sharing (NFS)** check box, as needed, and click **Next** to display the **NFS General Configuration** page.

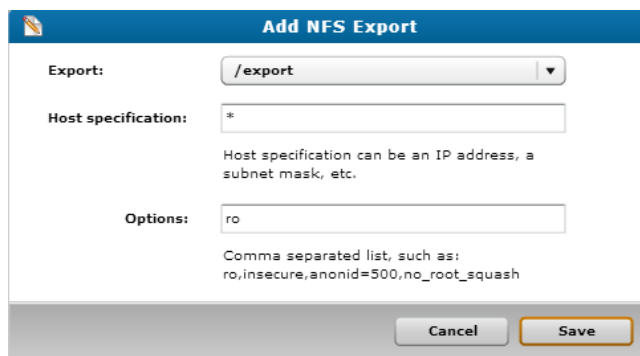
Figure 49: NFS General Configuration Page



Configure an NFS protocol


1. On the **Configure NFS** dialog box or NFS **General Configuration** page, select the **Enable NFS Access** check box, as needed.
2. Click **Add NFS Export** to display the **Add NFS Export** dialog box or page.

Figure 50: Add NFS Export Dialog Box




3. In the **Export** drop-down list, select one of the following directories that can be mounted as an NFS share:
 - **/export** – Only data in the **\export** directory can be mounted by the host defined in the **Host specification** field.

- **/recover/images** – Only data in the **\recover\images** directory can be mounted by the host defined in the **Host specification** field.
4. In the **Host specification** field, enter the IP address or host name for the host that can mount the specified data in the NFS share.
 5. In the **Options** field, enter actions that users can take with the data in the NFS share, such as **ro** for read-only access or **rw** for read-and-write access. Separate each option with a comma.
 6. Click **Save** to add the NFS protocol to the **Client Access Control** list on the **Configure NFS** dialog box or NFS General Configuration page.
 7. Click **OK** to save changes and exit the dialog box, or save changes and exit the wizard.

 **Caution:** Any time you make configuration updates from the **Quantum vmPRO Configuration Wizard**, you must exit the wizard using the **Summary** tab to save your updates. See [Initially Configuring a vmPRO Appliance](#).



Mounting Options

Users can mount NFS shares from the NAS as a Linux network drive using **<vmPRO-Host:/directory>**, where **vmPRO-Host** is the name of the host on which to mount the directory and **/directory** is the directory to mount.

 **Note:** We strongly recommend using the NFS protocol for Linux client machines accessing the vmPRO **/export** network file system. If a Linux client machine uses the CIFS protocol, specify the **directio** mount option at the **mount** command. For example: `# mount.cifs -o ..,directio <share> <mount point>`

Additional Functions

In addition to configuring NFS protocols, you can also use the following icons on the **Configure NFS** dialog box or **NFS General Configuration** page:

Icon	Function
	Displays the Edit NFS Export dialog box or page. Use this page to edit the NFS protocol's settings.
	Deletes the NFS protocol from the vmPRO appliance.

Configuring NAS Targets for SmartMotion Backups

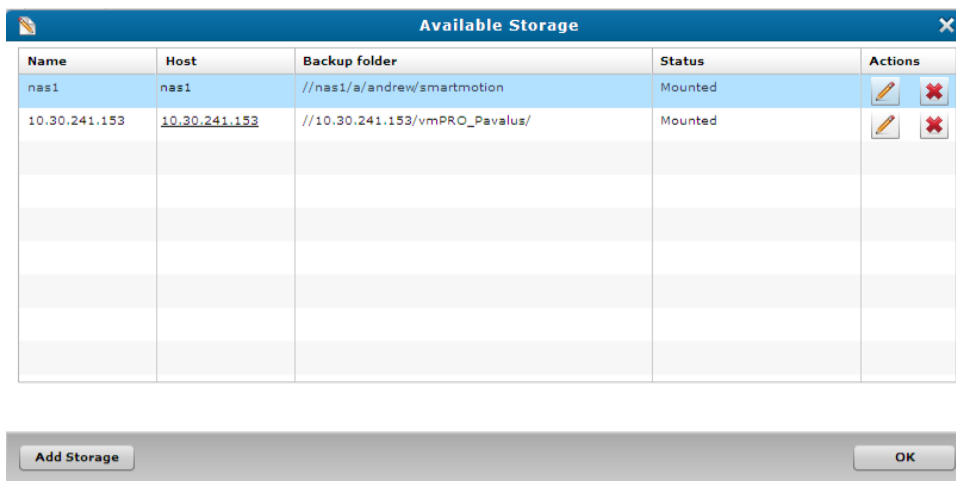
To perform SmartMotion™ backups, you need to configure NAS targets to which to export data. When configuring NAS targets, define a device to use as the NAS target, along with the protocol, share, sub-folder, and mount options.

You can configure NAS targets from the **SmartMotion Backup** menu or the **Quantum vmPRO Configuration Wizard**.

Display the Configure Storage dialog box

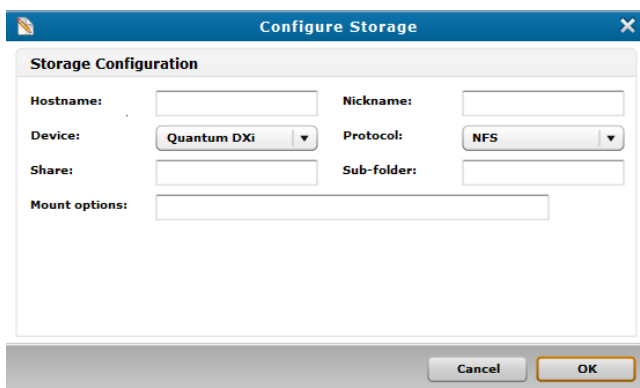
1. From the **SmartMotion Backup** menu, select **Storage** to display the **Available Storage** dialog box.

Figure 51: Available Storage Dialog Box



2. Click **Add Storage** to display the **Configure Storage** dialog box.

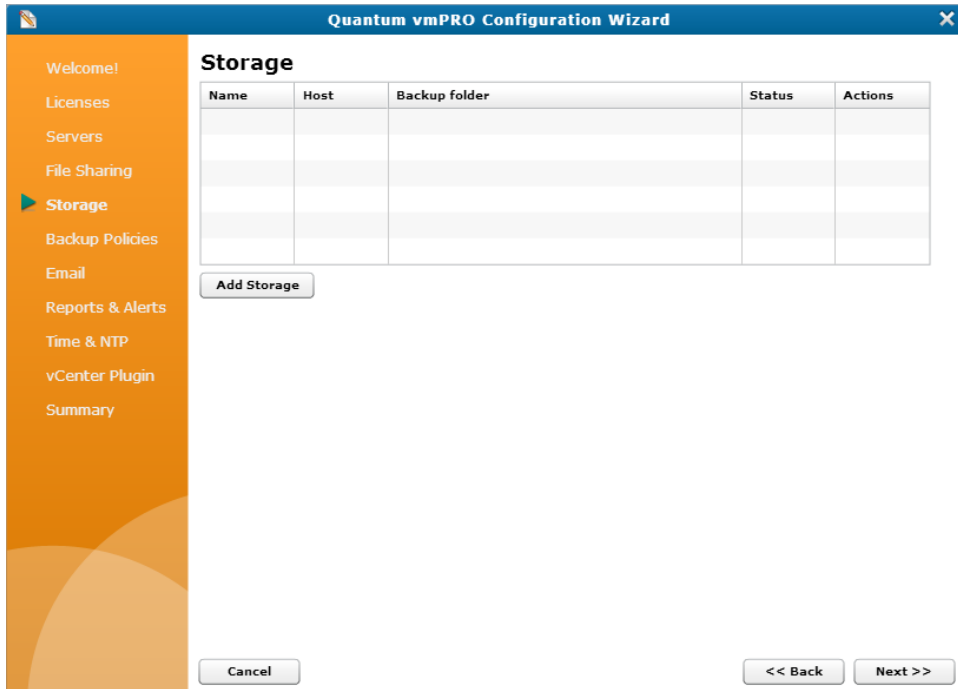
Figure 52: Configure Storage Dialog Box



Display the Storage Configuration page

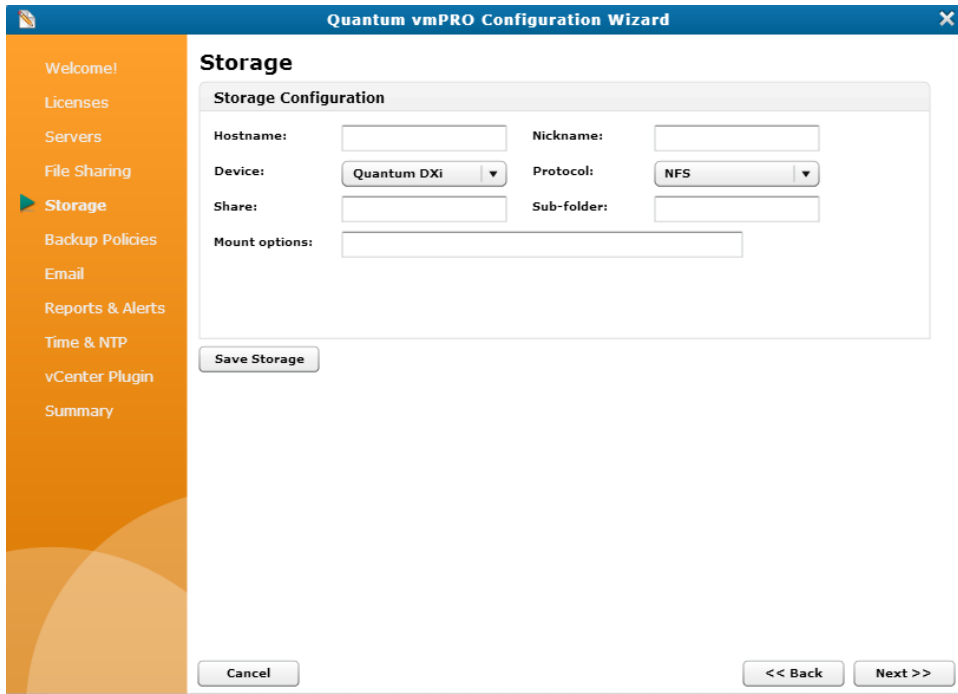
1. From the **Configuration** menu, select **Config Wizard** to display the **Quantum vmPRO Configuration Wizard**.
2. Click the **Storage** tab to display the **Storage** page.

Figure 53: Storage Page



3. Click **Add Storage** to display the **Storage Configuration** page.

Figure 54: Storage Configuration Page



Configure NAS targets for SmartMotion backups

1. Display the **Configure Storage** dialog box or the **Storage Configuration** page.
2. In the **Hostname** field, enter the NAS target's IP address or host name.

Caution: Take care to enter the correct host name or IP address for the target. If you enter an incorrect target identifier, the exported data may not be stored.

3. In the **Nickname** field, enter a more easily identifiable name for the NAS target, as necessary.

4. In the **Device** drop-down list, select one of the following NAS targets:

NAS Target	Description
Quantum DXi	<p>Use a Quantum DXi device as your NAS target. Before you can use a DXi device as a NAS target</p> <p>The DXi appliance must be configured with either a CIFS or NFS share that is accessible to your vmPRO appliance. See the Quantum DXi User's Guide for your DXi system for information about configuring your DXi device.</p> <p>If you are using the CIFS protocol with your DXi device</p> <p>Populate the following fields:</p> <ol style="list-style-type: none"> CIFS User – The user name defined for the DXi device's NAS configuration settings. CIFS Password – The password defined for the DXi device's NAS configuration settings.
Data Domain	<p>Use a Data Domain appliance as your NAS target. If you select this option</p> <ul style="list-style-type: none"> The Fastcopy user field and Show SSH Key button display. vmPRO assigns sysadmin as the fast copy user. <p>Do the following to add the SSH key to your Data Domain appliance</p> <ol style="list-style-type: none"> Click Show SSH Key to display the SSH Key popup. Copy the SSH key. Use the adminaccess add ssh-keys command on your Data Domain appliance.
Generic	Use a generic NAS as your storage target.

- In the **Protocol** drop-down list, select a [file sharing protocol](#) — either CIFS or NFS — to assign to your NAS storage target.
- In the **Share** field, enter the name of the exported file system being accessed from the NAS target.
- In the **Sub-folder** field, enter a directory within the file system, as needed.
- In the **Mount options** field, enter the location to which you are mounting the NFS or CIFS shares.
 - To provide file-level access to the backups at the `\\<vmPRO-Host_IP>\recover\files` directory on a CIFS share, enter the IP address or host name of the NAS target. See [Individual File Recovery](#).
 - If you are using a Scalar LTFS appliance with an NFS share, enter the following NFS mount option: `rsize=1048576, wsize=1048576, timeo=12000`.

i Note: For recommendations regarding Linux system mount options, see [Configuring an NFS Protocol for a vmPRO Appliance](#). For mounting CIFS shares, see [Configuring a CIFS Protocol for a vmPRO Appliance](#).

9. Do one of the following to save the NAS target:

From the Configure Storage dialog box:

- a. Click **OK** to add the NAS target to the **Available Storage** dialog box.
- b. Click **OK** to save changes and exit the dialog box.



From the Storage Configuration page:

- a. Click **Save Storage** to add the NAS target to the **Storage** page.
- b. Save changes and exit the wizard.

! Caution: Any time you make configuration updates from the **Quantum vmPRO Configuration Wizard**, you must exit the wizard using the **Summary** tab to save your updates. See [Initially Configuring a vmPRO Appliance](#).

Additional Functions

In addition to configuring NAS targets, you can also use the following icons on the **Available Storage** dialog box or **Storage** page.

Icon	Function
	Displays the Configure Storage dialog box or Storage Configuration page. Use this dialog box or page to edit the NAS target's settings.
	Deletes the NAS target from the vmPRO appliance.

vmPRO Group Configuration

If a single vmPRO appliance does not provide enough throughput to complete backups in the desired window of time, you can deploy additional vmPRO appliances in the network to provide the necessary throughput. To deploy multiple vmPRO appliances within a single network, configure the vmPRO appliances as a group.

Group configuration streamlines the management of multiple vmPRO appliances and the virtual machines (VMs) backed up by the appliances. You can configure and manage all appliances and VMs in a group from the assigned master appliance.

Keep in mind that the vmPRO appliances in a group relationship can export only one vCenter server. If two standalone appliances are joined together, the appliance in the master role is given export priority over its assigned appliances.

Configure groups from your VMware vSphere Client console. You can then manage groups and backups from the master vmPRO appliance's GUI.

Prerequisites

Before configuring groups, do the following to ensure that the group deployment of virtual machines (VMs) works correctly.

Network Connectivity and DNS Resolution Confirmation

Confirm that each vmPRO appliance being assigned to the group has network connectivity and DNS resolution. If IP routing issues or DNS resolution failures occur in a group deployment, backups can fail.

Confirm that a vmPRO appliance can communicate with the other appliances in the group

1. Open the VMware vSphere Client console.
2. At the command line, enter the `net ping` command, or enter the `ping <appliance name>` command if using DNS.
3. Repeat steps 1 and 2 for each appliance.

vmPRO Version Confirmation

Verify that all vmPRO appliances in the group are upgraded to the same version of Quantum vmPRO, such as 3.2.

Folder Configuration

Set up folders on your master vmPRO appliance to use in organizing VMs and backup policies. See [Configuring vmPRO Folders](#).

Group Mode Licensing

Group Configuration is also advantageous because it allows you to use a single capacity-based license for the entire group of vmPRO appliances. The exported capacity of all appliances counts toward the capacity of the license.

Use Group Mode Licensing

1. Install the capacity-based license on the vmPRO appliance that is the master for the group. See [Adding Licenses to a vmPRO Appliance](#).
2. Configure the vmPRO appliance as the group master. See [Configuring vmPRO Groups](#).

3. Add vmPRO appliances to the group. See [Configuring vmPRO Groups](#).

The capacity-based license is applied to all vmPRO appliances in the group.

Configuring vmPRO Groups

When you configure a group for your network's multiple vmPRO appliances, you need to first assign a vmPRO appliance as the master from which to manage all other appliances. Once a master is defined, you can add appliances to the group.

Configure groups from your VMware vSphere Client console.

Assign a vmPRO appliance as the group's master appliance

1. Log in to the VMware vSphere Client console for the vmPRO appliance to assign as the group's master.
2. Display the **Network Configuration** screen. See [Configuring Network Settings for a vmPRO Appliance](#).
3. Select **Group Membership**, and press **Enter** to display the **Change Group Membership** screen.

Figure 55: Change Group Membership Screen - Create Group



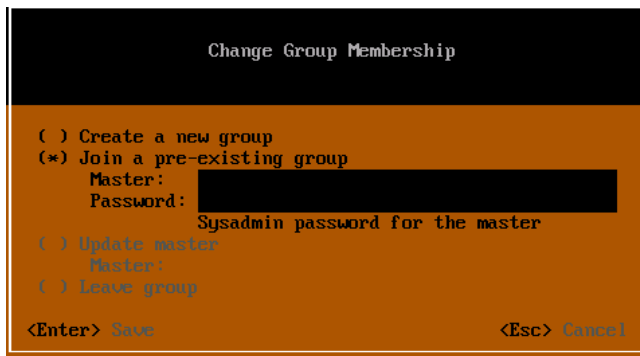
4. Arrow to **Create a new group**, and press the **spacebar** to assign the current vmPRO appliance as the group master.
5. Press **Enter** to save the assignment and exit the screen.

Assign vmPRO appliances to a group

1. Log in to the VMware vSphere Client console for the vmPRO appliance to assign to a group.
2. Display the **Network Configuration** screen. See [Configuring Network Settings for a vmPRO Appliance](#).

3. Select **Group Membership**, and press **Enter** to display the **Change Group Membership** screen.

Figure 56: Change Group Membership Screen – Join Group



4. Arrow to **Join a pre-existing group**, and press the **spacebar** to assign the current vmPRO to a group.
5. In the **Master** field, enter the IP address or resolvable host name for the group's master appliance.
6. In the **Password** field, enter the master appliance's password.
7. Press **Enter** to save changes and exit the screen. The vmPRO appliance is now part of the master appliance's group.

Additional Configuration Options

Use the following options on the **Change Group Membership** screen of your vmPRO appliance's VMware vSphere Client console to further configure groups.

Configuration Option	Description
Update master	<p>If a master appliance's IP address or host name changes, use this option to update that information for each VM appliance in the group.</p> <p>After updating the master appliance's information for an assigned vmPRO appliance, you must reboot the appliance for the change to take effect.</p> <p>Update a master appliance's information for each subordinate appliance in the group</p> <ol style="list-style-type: none">1. Log in to the VMware vSphere Client console for each subordinate vmPRO appliance.2. Display the Network Configuration screen. See Configuring Network Settings for a vmPRO Appliance.3. Select Group Membership and press Enter to display the Change Group Membership screen.4. Arrow to Update Master, and press the spacebar to update the master appliance's information.5. In the Master field, enter the IP address or resolvable host name of the group's new master appliance.6. Press Enter to save changes and exit the screen.7. Reboot each vmPRO appliance. See vmPRO Console Commands – system.
Leave group	<p>Use this option to remove a vmPRO appliance from its current group.</p> <p>When you remove a vmPRO appliance from a group, it no longer uses the group's backup policies. You must configure new backup policies for the appliance, either from its new master appliance or as a standalone appliance. If you are going to use the vmPRO appliance as a standalone appliance, you need to provide its own license.</p> <p>You cannot remove a master appliance from a group until all other appliances have been removed.</p> <p>Remove a vmPRO appliance from a group</p> <ol style="list-style-type: none">1. Log in to the VMware vSphere Client console for each subordinate vmPRO appliance.2. Display the Network Configuration screen. See Configuring Network Settings for a vmPRO Appliance.3. Select Group Membership and press Enter to display the Change Group Membership screen.4. Arrow to Leave group, and press the spacebar to remove the appliance from its current group.5. Press Enter to save changes and exit the screen.

Managing vmPRO Groups

When you have a vmPRO group configured, you can increase your backup throughput by assigning virtual machines (VMs) to the vmPRO appliances – or nodes – within the group. Your backup throughput increases

by using multiple nodes to perform your network's VM backups, rather than using a single appliance to perform the entire network's VM backups.

You must manage all vmPRO appliances in a group from the master appliance's GUI:

- View all nodes assigned to the master appliance on the **VMs Console > Resources** tab. See [Navigating the vmPRO VMs Console](#).
- View VM node assignments on the **VMs Console > Virtual Machines** tab. See [Navigating the vmPRO VMs Console](#).

Assign VMs to nodes

1. From the master vmPRO appliance's GUI, click the **VMs** button to display the **VMs** console.

i Note: If you access a subordinate vmPRO appliance's GUI, it displays a warning reminding you to use the master appliance's GUI to manage the appliance. Click **Go to master** to access the master vmPRO appliance's GUI.
2. Select the **Virtual Machines** tab, as needed.
3. In the **VMs** table, locate and select one or more VMs to which to assign a node.
4. Click **Edit Selected VMs** to display the **Configure Virtual Machine** dialog box. See [Modifying VM Settings from the vmPRO Appliance](#).
5. In the **Node** drop-down list, select a node to assign to the selected VM(s).
6. Click **Save** to save changes and exit the dialog box.

Importing vmPRO Group Configurations

You can transfer the configuration settings of an existing vmPRO appliance group to a new vmPRO appliance group. After the transfer, the new group functions as the original group did.

Import group configurations

1. Export the group's configuration file by doing the following:
 - a. From the **Operations** menu of the master appliance's GUI, select **Export vmPRO Configuration** to display the **Quantum vmPRO Configuration Save and Import** page.

Figure 57: Quantum vmPRO Configuration Save and Import Page

Quantum vmPRO Configuration Save and Import

Save a copy of your configuration

Provided below is a link to a file containing configuration information for this vmPRO. Please note, this package contains password information and should only be provided to administrators.

- [db-package.tar.bz2.enc](#)

Import a saved configuration

In the box below select a saved configuration file that you would like to import, and then click 'Import'. The configuration of this vmPRO will be set to the saved copy, including login information. The update may take a few minutes to complete.

WARNING: Before importing a configuration, the vmPRO from which the configuration package originated must no longer be in use. Importing the same configuration to multiple vmPRO appliances is not supported and can cause undesired results.

Importing is only supported to vmPRO appliances with factory default settings.

Select the package: No file chosen

[Quantum vmPRO](#)
Thu Nov 13 15:01:32 2014

- b. Follow the instructions on the displayed **Quantum vmPRO Configuration Save and Import** page to download the configuration file. Make sure to note the name and location of the group's configuration file when you download it.
2. Import the group's configuration file into the new master vmPRO appliance by doing the following:
 - a. From the **Operations** menu of the new master appliance's GUI, select **Import vmPRO Configuration** to display the **Quantum vmPRO Configuration Save and Import** page.
 - b. Click **Choose File** to navigate to the original group's exported configuration file.
 - c. Select the file and click **Open** to return to the **Quantum vmPRO Configuration Save and Import** page with the file displayed next to the **Choose File** button.
 - d. Click **Import** to import the configuration file to the new master appliance.
3. For each node in the original group that needs to be replaced, deploy a new vmPRO appliance. See the [Quantum vmPRO Installation Guides](#).

i Note: You need a valid email address and password to access the [Quantum vmPRO Installation Guide](#).

4. Add each new vmPRO appliance to the new group. See [Configuring vmPRO Groups](#).
5. Reassign the VMs from the original group to the new group nodes. See [Managing vmPRO Groups](#).
6. Remove the original nodes from the new master appliance's **VMs Console > Resources** tab. See [Managing Servers and Nodes from the VMs Console](#).

7. Reboot all new nodes, either from the VMware vSphere console or from each appliance's console command line interface (CLI). See [vmPRO Console Commands – system](#).

vmPRO Folders

By default, your vmPRO appliance organizes virtual machines (VMs) in folders named for their respective vSphere ESX hosts. These folders are separate from the existing folders within the vSphere Client. The separate folders in your vmPRO appliance's GUI allow you to refine and optimize the backup loads across your appliance or group of appliances.

- If you add a vCenter server, your VMs appear in a single initial folder with the name of that vCenter server.
- If you add one or more ESX servers, your VMs appear in folders corresponding to the ESX hosts on which they reside.

You can also configure your own folders on the vmPRO appliance to do the following:

Manage multiple backup policies to facilitate higher throughput

Divide your VMs among several folders to assign multiple backup policies to a single VM. Although VMs can only belong to one folder, folders can have multiple policies, enabling multiple policies to apply to a single VM.

You can also use folders to stagger full backups across different weeks to avoid having full backups running close together.

Manage the distribution of backups across multiple vmPRO appliances within a group

Assign folders – and the VMs residing within them – to be managed by the different appliances within a group, distributing the backup load. Folders that you create on the master appliance display for all appliances within the group.

Manage multiple differential Changed Block Tracking (CBT) backup rotation schedules

Changed Block Tracking (CBT) enables differential backups, or backing up of only new or changed information to significantly reduce the amount of data read from the VM and written to the Network Attached Storage (NAS) target.

Configuring vmPRO Folders

Configure folders to better organize virtual machines (VMs) and the schedule on which they are backed up. You can assign SmartMotion™ backup policies to folders, which in turn dictates the schedule for backing up the VMs in the folder.

Create Folders

When creating folders, you can assign a unique Changed Block Tracking (CBT) schedule to a folder. In addition, select the transport method for the vmPRO appliance to use in transferring VMDKs.

Create a folder on the vmPRO GUI

1. Click the **VMs** button to display the **VMs Console**.
2. Click the **Folders** tab to display the **Folders Tab** view.
3. Click **Add Folder** to display the **Configure Folder** dialog box.

Figure 58: Configure Folder Dialog Box

Folder

Name:

Changed Block Tracking Reset Schedule

The time and frequency which the 'last modified time' of each CBT-enabled VM's base disk is reset to the current time. The default schedule is Sundays at 03:30.

Time: 03 : 30

Frequency: Every Sunday of the month

On the 1 st of each month

Transport Method

Select the transport method to use for VMs in this folder.

[View the HotAdd Transport warning.](#)

Use the global default (set using 'Configure > Advanced Settings...')

Cancel Save

4. In the **Name** field, enter a name for the folder.
5. In the **Changed Block Tracking Reset Schedule** area, edit the CBT schedule, as needed. See [Configuring CBT on a vmPRO Appliance](#).
6. In the **Transport Method** area, select one of the following methods to use in transferring the VM disks (VMDKs) within the folder:

Transport Method	Description
<p>Use the global default</p>	<p>The vmPRO appliance uses transport method settings defined in the Configure Advanced Settings dialog box. See Configuring Advanced Settings for a vmPRO Appliance.</p>
<p>Attempt to use HotAdd, fall back to NBD</p>	<p>The vmPRO appliance uses the HotAdd transport method to transfer VMDKs. HotAdd provides a non-network-based method of transferring VMDKs from the source VM to the vmPRO appliance. If HotAdd cannot be used for transporting data, such as when the target VMs are not on the same ESX server as the vmPRO appliance, the vmPRO appliance uses the network block device (NBD) transport method. If you select this option, click the View the Hot Add Transport warning link to display the HotAdd Warnings pop-up. We recommend reviewing the displayed information.</p> <p>Figure 59: HotAdd Warnings Pop-up</p> <div data-bbox="610 842 1032 1075" data-label="Image"> </div> <p>For more information about HotAdd Transport, see Configuring Advanced Settings for a vmPRO Appliance.</p>
<p>Use NBD only</p>	<p>The vmPRO appliance uses the NBD transport method to transfer VMDKs. The NBD transport method reads a VM's disk over a network interface. This transport method adds to your network's traffic. If the VMDK holds large amounts of data, transfer times can be long. The NBD transport method is the default, and the vmPRO appliance uses it when HotAdd is not available.</p>

7. Click **Save** to exit the dialog box and add the new folder to the **Folders** table.

Assign VMs To Folders

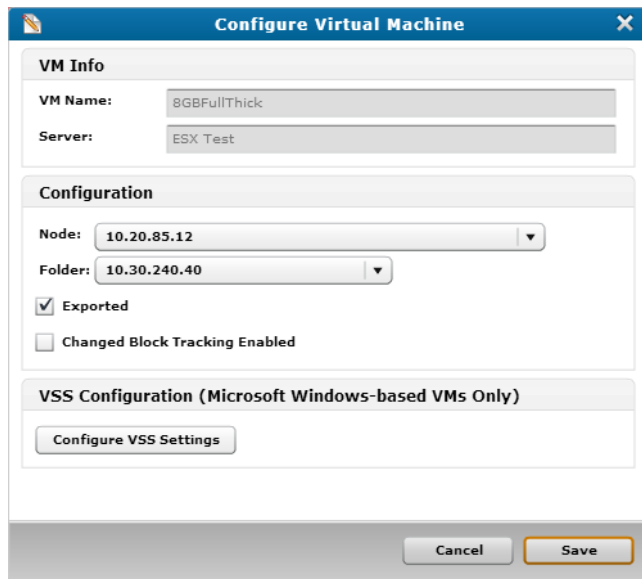
After creating folders, assign VMs to them from the **Virtual Machines** tab on the **VMs** Console. You can assign more than one VM at a time to a folder.

To assign VMs to folders:

1. Click the **VMs** button to display the **VMs** Console.

2. Click the **Virtual Machines** tab to display the **Virtual Machines Tab** view.
3. In the **VMs** table, locate and select one or more VMs to add to a folder.
4. Click **Edit Selected VMs** to display the **Configure Virtual Machine** dialog box.



Figure 60: Configure Virtual Machine Dialog Box



5. In the **Folder** drop-down list, select the folder to which to assign the VMs.
6. Click **Save** to exit the dialog box and add the VMs to the folder.

Additional Functions

In addition to configuring folders, you can also use the following icons on the **VMs Console – Folders Tab** view.

Icon	Function
	Displays the Configure Folder dialog box, in which you can edit the folder's settings.
	Deletes the folder. At the prompt, confirm the deletion. You cannot delete folders that contain VMs. You must first move the VMs to another folder.

vmPRO Emails, Reports, Alerts, and Autosupport

Use Quantum vmPRO's Email, Reports, and Alerts features to send daily reports and alerts to recipients who need to stay informed about the vmPRO appliance.

Use the Quantum vmPRO Autosupport feature to include the Quantum support team on daily report and alert emails, as well as to upload a daily report to the Quantum support site. Uploading reports to the Quantum support site enables SmartRead statistical analysis, and facilitates pro-active support from the Quantum support team.

To take advantage of daily reports and email alerts, as well as Autosupport, configure both the Email feature and the Reports and Alerts feature on your vmPRO appliance.

i Note: Standard edition customers can upload reports, but they cannot access the support site. To take full advantage of the Autosupport feature, either purchase additional capacity or purchase a service contract. For more information, go to www.quantum.com.

Configuring Email for a vmPRO Appliance

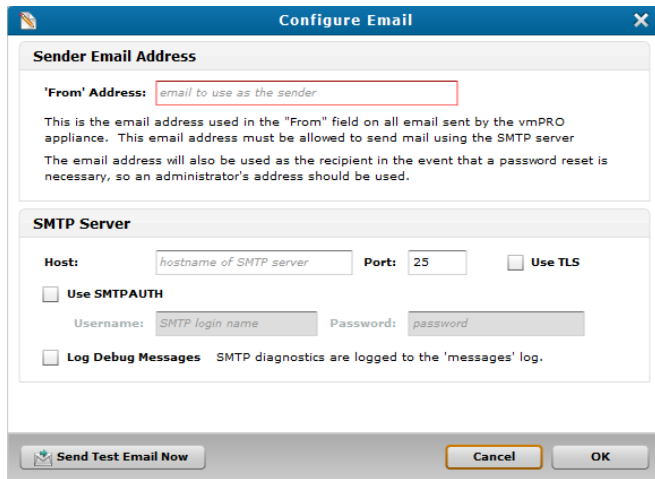
Configure your vmPRO appliance's Email feature to send daily reports and alerts to recipients who need to stay informed about the vmPRO appliance. You can configure your appliance's Email feature from the **Configure** menu or the **Quantum vmPRO Configuration Wizard**.

After entering credentials for your appliance's Email feature, you can verify that the credentials are correct by sending a test email.

Display the Configure Email dialog box

- From the **Configure** menu, select **Email**.

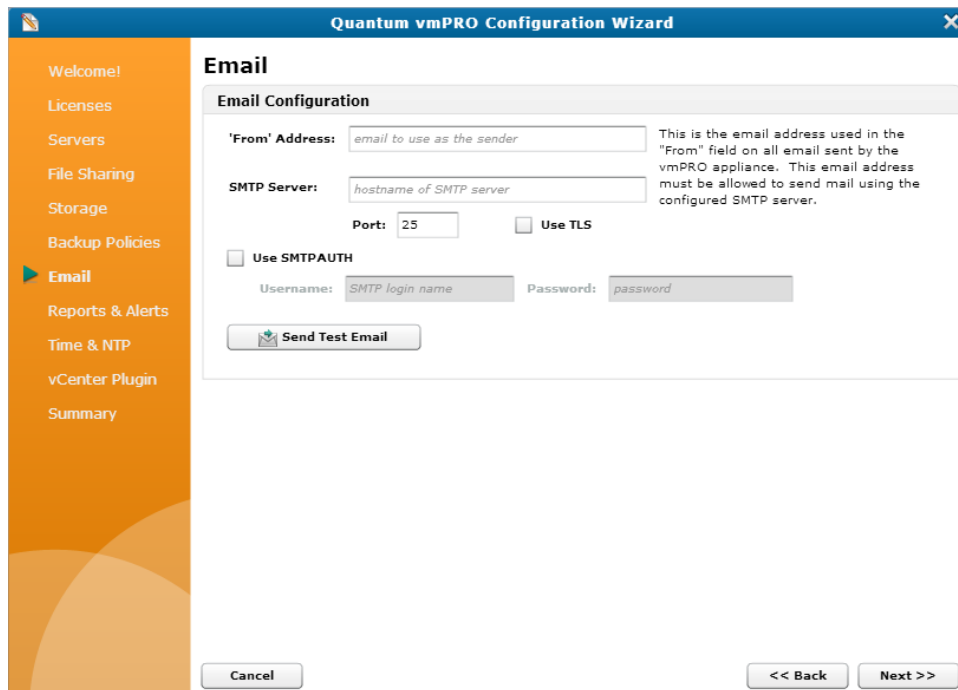
Figure 61: Configure Email Dialog Box



Display the Email Configuration page

1. From the **Configure** menu, select **Config Wizard** to display the **Quantum vmPRO Configuration Wizard**.
2. Click the **Email** tab to display the **Email Configuration** page.

Figure 62: Email Configuration Page



Configure the Email feature for your vmPRO appliance

1. Display the **Configure Email** dialog box or the **Email Configuration** page.
2. In the **'From' Address** field, enter the email address from which to send the vmPRO appliance's reports and alerts.

i Note: We recommend entering an administrator's address in the **'From' Address** field, since the address entered in this field is also used as the recipient address when a password reset is needed.

3. In the **Host** or **SMTP Server** field, enter the host for the vmPRO appliance's SMTP server.
4. In the **Port** field, enter the port for the vmPRO appliance's SMTP server.
5. Select the **Use TLS** check box to use transport layer security (TLS) when sending emails over the Internet, as needed.
6. Select the **Use SMTPAUTH** check box to use SMTP authentication in accessing the email server, as needed.

If you select this option, do the following:

- a. In the **Username** field, enter the login name for accessing the SMTP server.
 - b. In the **Password** field, enter the password for accessing the SMTP server.
7. Select the **Log Debug Messages** check box to log debugged emails in the Support Logs. See [vmPRO GUI Menus](#).

i Note: This field only displays on the **Configure Email** dialog box.

8. Click **Send Test Email Now** to send a test email from the email address entered in the **'From' Address** field.
9. Click **OK** to save changes and exit the **Configure Email** dialog box, or save changes and exit the wizard.

⚠ Caution: Any time you make configuration updates from the **Quantum vmPRO Configuration Wizard**, you must exit the wizard using the **Summary** tab to save your updates. See [Initially Configuring a vmPRO Appliance](#).

Configuring Reports, Alerts, and Autosupport for a vmPRO Appliance

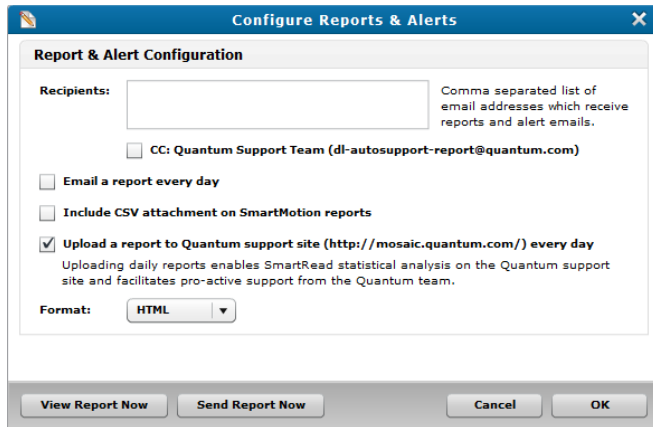
Configure your vmPRO appliance to send daily reports and alerts to recipients who need to know about the status of the appliance. In addition, enable Autosupport to facilitate pro-active support from the Quantum support team.

i Note: Make sure your firewall allows access to support.Quantum.com on port 443.

Display the Configure Reports & Alerts dialog box

- From the **Configure** menu, select **Reports & Alerts** to display the **Configure Reports & Alerts** dialog box.

Figure 63: Configure Reports & Alerts Dialog Box

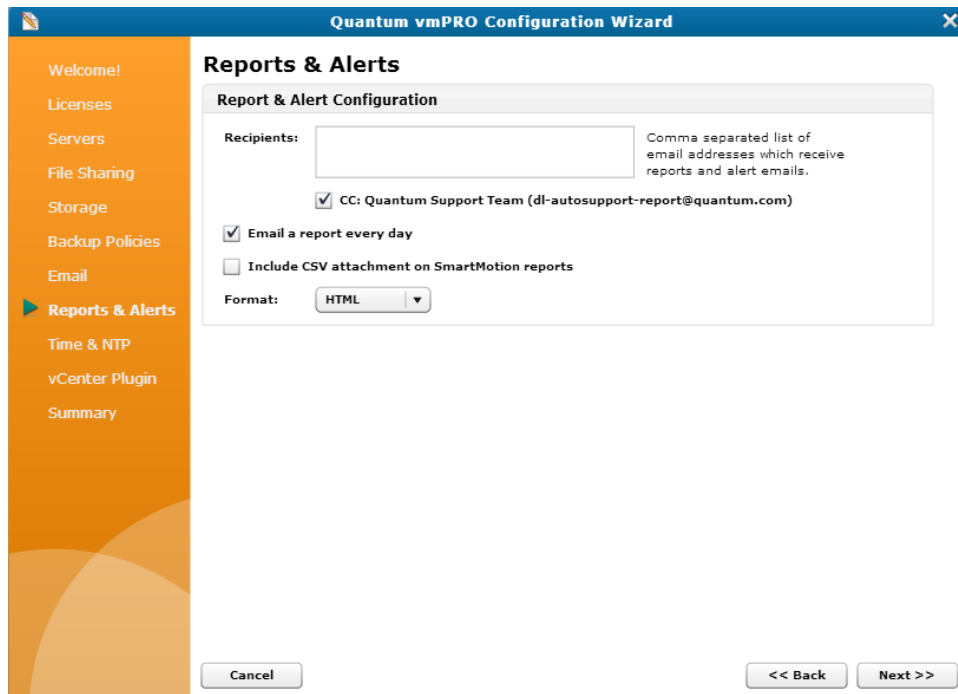


Display the Report & Alert Configuration page

1. From the **Configure** menu, select **Config Wizard** to display the **Quantum vmPRO Configuration Wizard**.

2. Click the **Reports & Alerts** tab to display the **Report & Alert Configuration** page.

Figure 64: Report & Alert Configuration Page




Configure reports, alerts, and Autosupport for a vmPRO appliance

1. Display the **Configure Reports & Alerts** dialog box or the **Report & Alert Configuration** page.
2. In the **Recipients** field, enter the email addresses to which to send reports and alerts. Separate each email address with a comma.
3. Select the **CC: Quantum Support Team** check box to include the Quantum support team on all report and alert emails.
4. Select the **Email a report every day** check box to send daily report and alert emails.
5. Select the **Include CSV attachment on SmartMotion reports** check box to include a plain-text form of the SmartMotion reports, which can be read by programs such as Microsoft Excel.
6. Select the **Upload a report to Quantum support site every day** check box to upload a daily report to the Quantum support site.

i Note: This check box is available only on the **Configure Reports & Alerts** dialog box.

7. In the **Format** drop-down list, select the format in which to send the email, either **HTML** or **plain text**.

8. Click **OK** to save changes and exit the dialog box, or save changes and exit the wizard.

 **Caution:** Any time you make configuration updates from the **Quantum vmPRO Configuration Wizard**, you must exit the wizard using the **Summary** tab to save your updates. See [Initially Configuring a vmPRO Appliance](#).

Additional Functions

Use the following buttons on the **Configure Reports & Alerts** dialog box, as needed.

Button	Function
View Report Now	Use to view the Quantum vmPRO Report. See vmPRO GUI Menus .
Send Report Now	Use to send the report immediately. The vmPRO appliance sends the report to all recipients entered in the Recipients field, and posts it on the Quantum support site if you enabled the auto support feature.


vmPRO NTP Servers

Use Network Time Protocol (NTP) servers with your vmPRO appliance to control the system date and time.

Configuration Considerations

Set up NTP servers for your vmPRO appliance based on your environment.

- The vmPRO appliance and all ESX or ESXi hosts should have their date and time synchronized to an NTP server.
- The vmPRO appliance and the vCenter server **must** have their date and time synchronized to the same NTP server.

 **Note:** The time zone of your vmPRO appliance **must** be the same as the time zone of the vCenter or ESX server(s).

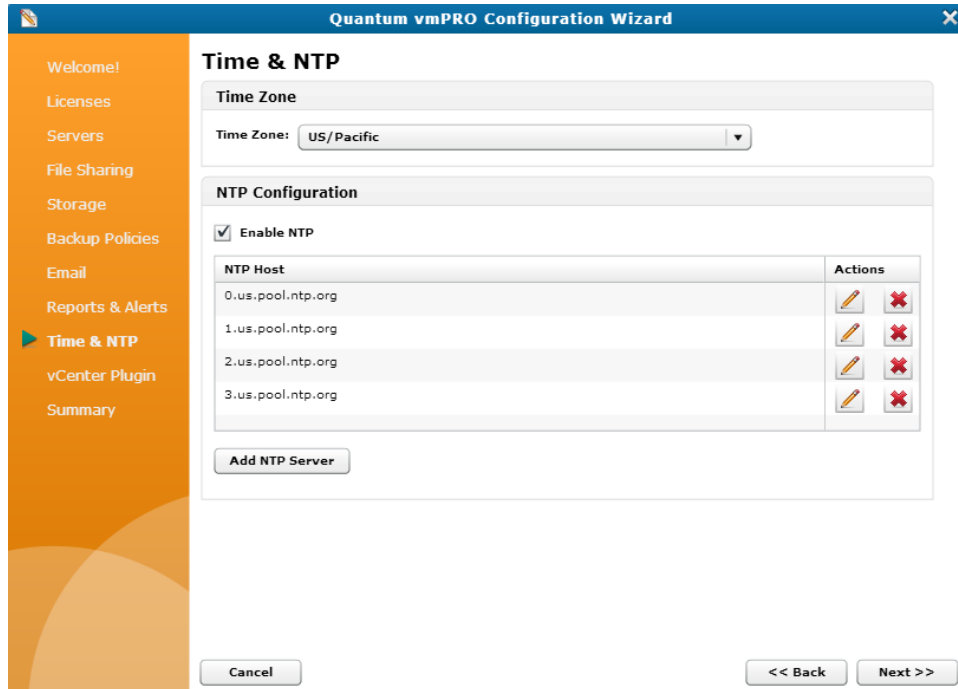
Configuring an NTP Server for a vmPRO Appliance

Use the **Time & NTP** page of the **Quantum vmPRO Configuration Wizard** to configure an NTP server for the vmWare environment in which your vmPRO appliance resides.

Configure an NTP server for your vmPRO appliance

1. From the **Configure** menu, select **Config Wizard** to display the **Quantum vmPRO Configuration Wizard**.
2. Click the **Time & NTP** tab to display the **Time & NTP** page.

Figure 65: Time & NTP Page





3. In the **Time Zone** drop-down list, select the appropriate time zone for the vmPRO appliance.

Note: The time zone of your vmPRO appliance must be the same as the time zone of the vCenter or ESX server(s).


4. Select the **Enable NTP** check box to enable an NTP server for your vmPRO appliance.
5. Select an NTP server for your vmPRO appliance by doing one of the following:

Select an existing NTP server:

- In the **NTP Host** field, select the NTP server to use with your vmPRO appliance.
- Use the **Actions** column icons to do the following, as needed:
 -  – Use to edit the NTP server.
 -  – Use to delete the NTP server from the list of NTP hosts.

Add a new NTP server:

- a. Click **Add NTP Server** to display the **Add NTP Server** page.
 - b. In the **NTP Server** field, enter the NTP Server to use with your vmPRO appliance.
 - c. Click **Save** to return to the **Time & NTP** page with the new NTP server displayed in the **NTP Host** field.
 - d. Select the NTP server to use with your vmPRO appliance.
6. Save changes and exit the wizard.

 **Caution:** Any time you make configuration updates from the **Quantum vmPRO Configuration Wizard**, you must exit the wizard using the **Summary** tab to save your updates. See [Initially Configuring a vmPRO Appliance](#).

vmPRO Users

Configure users, both to define the level of access they have to the vmPRO appliance, and to assign them authentication credentials for accessing the appliance.

Access Levels

When you configure new users for your vmPRO appliance, you can assign them one of the following access levels.

Access Level	Description
User	Limits users to basic operations, and revokes configuration privileges.
Admin	Grants full access to and use of the vmPRO appliance. You cannot edit the sysadmin user's access level.

Authentication Credentials

Assign users authentication credentials to give them access to both the vmPRO Command Line Interface (CLI) Console and the vmPRO GUI.

How the vmPRO appliance authenticates users

- a. When logging into the vmPRO GUI and CLI, a user enters assigned credentials – a user name and password.
- b. The vmPRO appliance compares the credentials the user enters to the credentials assigned in the **Configure User** dialog box.

- c. If the credentials match, the user is authenticated and given access to the vmPRO CLI Console and vmPRO GUI.

In addition to granting access to the vmPRO CLI Console and vmPRO GUI, you can use authentication credentials to grant access to exported CIFS shares. See [Configuring a CIFS Protocol for a vmPRO Appliance](#).

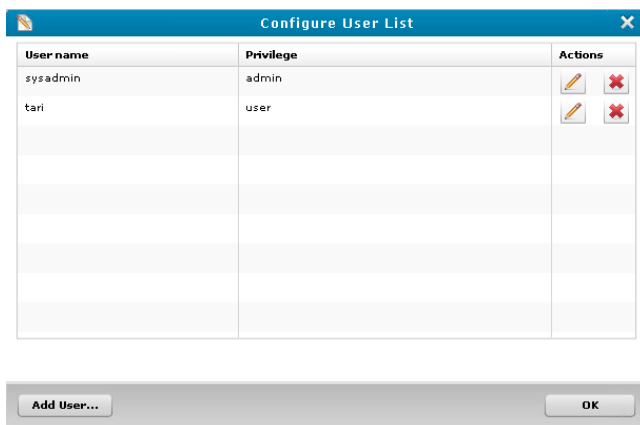
Configuring Users for a vmPRO Appliance

Configure users, both to define the level of access they have to the vmPRO appliance, and to assign them authentication credentials for accessing the appliance.

Configure a new user for a vmPRO appliance

1. From the **Configure** menu, select **Users** to display the **Configure User List** dialog box.

Figure 66: Configure User List Dialog Box



2. Click **Add User** to display the **Configure User** dialog box.
3. In the **User name** field, enter a user ID to assign to the user.
4. In the **Password** field, enter a password to assign to the user.

Note: Users enter these credentials to access both the vmPRO CLI console and the vmPRO GUI.

5. In the **Confirm** field, re-enter the user's password to confirm that you entered it correctly.



6. In the **Privilege** drop-down list, select one of the following access levels to assign to the user:

Access Level	Description
user	Limits users to basic operations, and revokes configuration privileges.
admin	Grants users full privileges for accessing and using the vmPRO appliance.

7. Click **Save** to return to the **Configure User List** dialog box, with the new user's ID displayed.

Additional Functions

In addition to configuring new users, you can also use the following icons in the **Configure User List** dialog box.

Icon	Function
	Displays the Configure User dialog box, in which you can edit the user's password and access level. i Note: You cannot edit the sysadmin user's access level. i Note: You can also access this dialog box from the Operations > Change My Password menu.
	Deletes the user. At the prompt, confirm the deletion. i Note: You cannot delete the sysadmin user.

vmPRO Upgrades

You can upgrade your Quantum vmPRO software either online or offline.

- i Note:** When upgrading to vmPRO versions 3.0 or newer, you must upgrade all vmPRO appliances within a group together.
- i Note:** When upgrading from 2.1.4 or prior to 2.3 and newer, we recommend increasing the memory allocation on the vmPRO appliance to 1280 MB. You can increase memory by editing the Quantum vmPRO VM settings in the VI Client.

Online Upgrades

- If you are upgrading from vmPRO versions 3.0 or older, you can perform the upgrade from your vmPRO appliance's Client console. See [Updating vmPRO Versions 2.X to 2.3.3 and 3.0.X to 3.X.](#)

- If you are upgrading from vmPRO version 2.3.3 to vmPRO 3.X, you need to deploy a new vmPRO version 3.X appliance first. You can then import your current configuration file from your vmPRO version 2.3.3 appliance into the newly deployed 3.X appliance. See [Updating vmPRO Version 2.3.3 to vmPRO Version 3.X](#).
- If you are upgrading from vmPRO versions 3.1 or newer, you can perform the upgrade from your vmPRO appliance's GUI. See [Updating vmPRO Versions 3.1 or Newer](#).

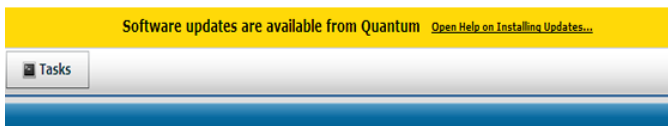
Offline Upgrades

If you do not have access to the Internet, you can perform offline upgrades. Before performing an offline upgrade, you need to access and download the correct zip file containing the upgrade RPMs. See [Installing vmPRO Software Updates Offline](#).

Checking for vmPRO Software Updates

You can configure your vmPRO appliance to automatically check for software updates. When software updates are available, a **Software Updates Available** bar displays above the main buttons of the vmPRO GUI.

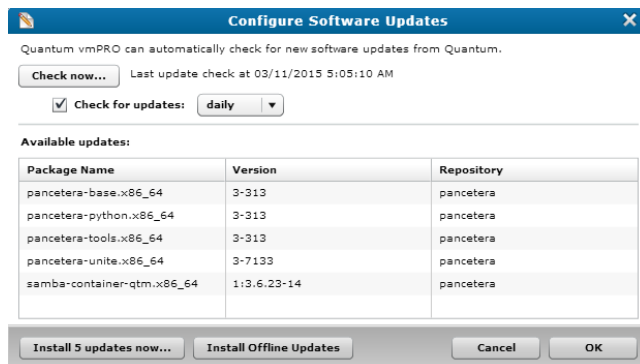
Figure 67: Software Updates Available Bar



Check for vmPRO software updates

1. From the **Configure** menu, select **Software Updates** to display the **Configure Software Updates** dialog box.

Figure 68: Configure Software Updates Dialog Box



2. Do one of the following to check for updates:

Check for updates now:

- Click **Check now**. The vmPRO appliance checks for software updates and lists new updates in the **Available updates** list.

Configure the vmPRO appliance to automatically check for updates:

- a. Select the **Check for updates** check box.
- b. In the drop-down list, select **daily** or **weekly** to indicate how often the appliance checks for updates.

3. Update the vmPRO software, as needed.

Updating vmPRO Versions 2.X to 2.3.3 and 3.0.X to 3.X

Use your vmPRO appliance's VMware vSphere Client console command line interface (CLI) to perform software updates for vmPRO versions 2.X to 2.3.3 and 3.0.X to 3.X.

Upgrade Notes

Before you upgrade your current vmPRO appliance, review the following notes:

Firewalls and Ports

This online upgrade process uses port 443 and opens [updates.Quantum.com](https://updates.quantum.com). If your system uses a firewall, you may need to change your port settings, as appropriate. The process uses signed, private key/public key encryption to verify and authenticate the updates.

Upgrade Size

Updates are typically no smaller than 17 MBs and no larger than 284 MBs.

Proxy Support

Configure proxy support to access the Internet, as needed. See [Configuring Network Settings for a vmPRO Appliance](#).

Group Upgrades

When upgrading to vmPRO versions 3.0 or newer, you must upgrade all vmPRO appliances within a group together.

Update vmPRO versions 2.X to 2.3.3 and 3.0.X to 3.X

1. Close your vmPRO appliance's GUI. The process does not update an open GUI.
2. Access the vmPRO Client console. See [Accessing the vSphere Client Console for vmPRO](#).

3. At the command line, enter **system upgrade**.

4. Confirm the upgrade.

The upgrade process automatically downloads and installs updates.

5. To see updates in your vmPRO appliance's GUI, start a new instance of the vmPRO appliance GUI.

Updating vmPRO Version 2.3.3 to vmPRO Version 3.X

Upgrading from vmPRO version 2.3.3 to vmPRO version 3.X allows you to keep your vmPRO appliance's current configuration. To perform this upgrade, do the following:

1. Deploy a vmPRO version 3.X appliance. See [vmPRO Setup and Configuration](#).
2. Use the vmPRO Import Configuration feature from your current vmPRO version 2.3.3 appliance to save your current vmPRO configuration.
3. Import your current vmPRO version 2.3.3 appliance's configuration file into your new vmPRO version 3.X appliance.

Upgrade Notes

Before you upgrade your current vmPRO appliance, review the following notes:

Group Upgrades

When upgrading to vmPRO versions 3.0 or newer, you must upgrade all vmPRO appliances within a group together.

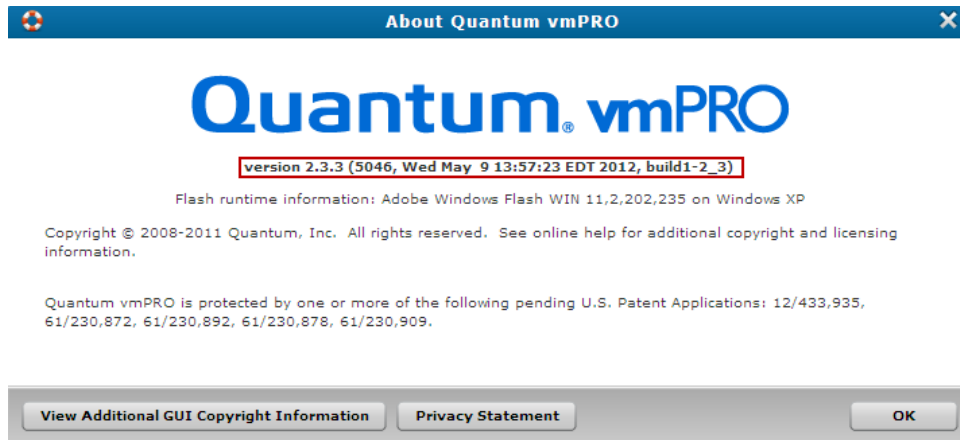
Configuration Files

- Before you import a configuration file, the vmPRO appliance from which the configuration file originated must no longer be in use.
- We do not recommend importing the same configuration file to more than one vmPRO appliance.
- You can import configuration files only to vmPRO appliances with factory default settings.

Import your vmPRO version 2.3.3 appliance's configuration file to your vmPRO version 3.X appliance

1. From your vmPRO 2.3.3 appliance's GUI, select **Help > About** to display the **About Quantum vmPRO** dialog box.
2. Verify that your vmPRO software is version 2.3.3.

Figure 69: About Quantum vmPRO Dialog Box



3. From the **Operations** menu, select **Save vmPRO Configuration** to display the **Quantum vmPRO Configuration Save and Import** window.
4. Review the information displayed on the window.
5. Click the **db-package.tar.bz2** link to download the upgrade file.

Note: Remember the location to which you download the upgrade file.

6. Access your vmPRO version 3.X appliance's GUI.
7. From the **Operations** menu, select **Import vmPRO Configuration** to display the **Quantum vmPRO Configuration Save and Import** window.
8. Review the information displayed on the window.
9. Click the **Browse** button to display the **Choose file** dialog box.
10. Navigate to the configuration file from your vmPRO version 2.3.3 appliance.
11. Select the file and click **Open** to import the configuration file into your vmPRO version 3.X appliance.
The vmPRO appliance automatically configures all settings using the imported configuration file.

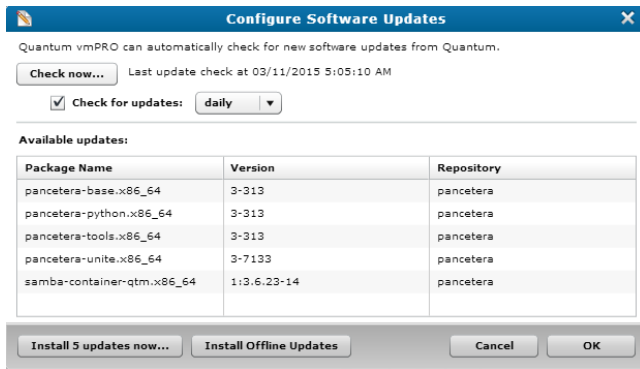
Updating vmPRO Versions 3.1 or Newer

If you are using vmPRO versions 3.1 or newer, you can install software updates from your vmPRO appliance's GUI. Use the **Configure Software Updates** dialog box to perform the update.

Update vmPRO versions 3.1 or newer

1. From the **Configure** menu, select **Software Updates** to display the **Configure Software Updates** dialog box.

Figure 70: Configure Software Updates Dialog Box



2. In the **Available updates** list, review the following information for available software updates:

Column	Description
Package Name	The name of the software update package.
Version	The version of the software update package.
Repository	The repository in which the software update package is located.

3. Click one of the following buttons to update your vmPRO software:

Button	Function
Install x updates now	Installs updates online from the Quantum repository. To use this option, your vmPRO appliance must have direct access to the Quantum repository.
Install Offline Updates	Installs updates in offline mode. See Installing vmPRO Software Updates Offline . If your vmPRO appliance is located at a dark site, use this option.

4. At the reboot prompt, click **OK** to begin the update.
After the software update has completed, the vmPRO appliance reboots.
5. After the vmPRO appliance reboots, log off the vmPRO GUI and close the browser.
6. Log back on to the vmPRO GUI for the software updates to take effect.

Installing vmPRO Software Updates Offline

If your vmPRO appliance does not have Internet access, you can perform an offline upgrade.

Requirements

Before performing an offline upgrade, make sure of the following:

Read and Write Access

The vmPRO appliance must have read and write access to `\\<vmpro-host>\quantum-upgrade`.

Note: At this time, you must use CIFS shares for exporting `\quantum-upgrade`.

RPMs

Download the appropriate zip file containing the upgrade RPMs:

- If you are upgrading from a 2.x appliance, download the zip file from <http://mosaic.quantum.com/downloads/QuantumvmPROUpgrade-2.X.zip>.
- If you are upgrading from a 3.0.x appliance, download the two zip files from <https://mosaic.quantum.com/downloads/QuantumvmPROUpgrade-from30x-1-of-2.zip> and <https://mosaic.quantum.com/downloads/QuantumvmPROUpgrade-from30x-2-of-2.zip>
- If you are upgrading from a 3.1.x appliance, download the zip file from <https://mosaic.quantum.com/downloads/QuantumvmPROUpgrade.zip>

Note: The upgrade zip file will contain one or more of these Quantum vmPRO upgrade RPMs: -**unite**, -**base**, -**python**, and -**tools**. The zip file may also contain third party RPMs.

Install vmPRO software updates for a 2.X or 3.1.X appliance

1. Extract the RPM files from the zip file and place them in the vmPRO appliance's `\quantum-upgrade` folder.
2. Access the vmPRO appliance's VMware vSphere Client console. See [Accessing the vSphere Client Console for vmPRO](#).
3. At the command line, enter **system upgrade local**.
4. Confirm the upgrade, which starts automatically after confirmation.
5. Start a new instance of the vmPRO appliance's GUI to see the updates.

Install vmPRO software updates for a 3.0.X appliance

1. Extract the RPM files from the **1-of-2** zip file and place them in the vmPRO appliance's `\quantum-upgrade` folder.
2. Access the vmPRO appliance's VMware vSphere Client console. See [Accessing the vSphere Client Console for vmPRO](#).
3. At the command line, enter **system upgrade local**.
4. Confirm the upgrade, which starts automatically after confirmation.

5. After the upgrade completes, extract the RPM files from the **2-of-2** zip file and place them in the vmPRO appliance's **quantum-upgrade** folder.
6. Access the vmPRO appliance's VMware vSphere Client console.
7. At the command line, enter **system upgrade local**.
8. Confirm the upgrade, which starts automatically after confirmation.
9. Start a new instance of the vmPRO appliance's GUI to see the updates.

vSphere Changed Block Tracking Support

vSphere's Changed Block Tracking (CBT) identifies the disk blocks that have changed on a virtual machine (VM) since the previous backup, allowing the vmPRO appliance to back up VMs at a differential level. Differential-level backups export only the data that has changed since the last full backup, as opposed to backing up the entire VM disk. When you use CBT with SmartMotion backups, both network I/O and backup times are reduced.

CBT Cycle

When CBT is enabled for a VM, the vmPRO appliance creates two kinds of files in the /export file system:

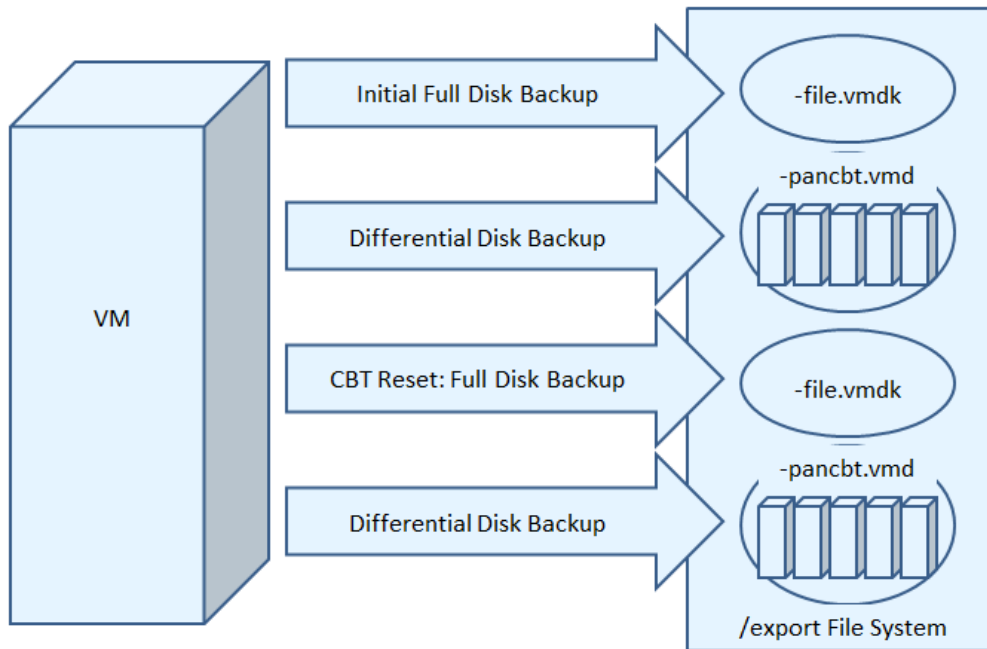
- A file for each base disk (identified by **-flat.vmdk**), which contains the full disk backup.
- A CBT file (identified by **-pancvt.vmdk**) for each base disk. The CBT file contains the changed blocks for the corresponding base disk.

The vmPRO appliance performs differential-level backups with CBT as follows:

1. Using SmartMotion backups, the vmPRO appliance performs a full disk backup following the CBT reset time. The CBT reset time indicates when to initiate a full disk backup, thus resetting the CBT cycle. For more information about CBT reset times, see [Configuring CBT on a vmPRO Appliance](#).
2. After the full backup, the vmPRO appliance runs differential backups on the disk until the next reset time, at which point the vmPRO appliance runs another full disk backup to replace the previous full disk backup.

i Note: Keep in mind that the base disk's modification time is the start of the reset time, while the CBT files have newer modification times.

Figure 71: CBT Cycle



i Note: The CBT files are not complete disk images because they contain only the disk's changed data. You cannot access the data in CBT files until you perform a full recovery of these files using the **Recover Virtual Machines Wizard**.

CBT Considerations

Keep the following in mind when using CBT:

Versions

- VMs must be running virtual hardware versions 7 or higher.
- We recommend using only paid versions of VMware ESX or ESXi servers. Free versions have various application programming interface (API) limitations that keep the vmPRO appliance from functioning as designed.
- The ESX server must be version 4.0 update 2 or above.

If you are using ESX 4.1, reverting a snapshot resets CBT for that VM.

Resolve the reset

- a. Remove all snapshots from the appliance.
- b. On the VMware vSphere Client console, enter the following command:

```
cbt reset <hypervisor> <VM>
```

VM Transfers

Transferring a VM with Storage vMotion disables CBT.

Standard vMotion (when only the ESX host changes for the VM, but the VM disk stays in the same storage location) does *not* disable CBT.

Load Balancing

Using vMotion on VMs for load balancing during a backup can cause the backup to fail if you do not have one of the following:

- vmPRO 3.0.1 and newer
- vCenter Server version 5

In these versions, vMotion is disabled on the VMs prior to the start of the backup process.

For vCenter 4.x, you need to configure the VMs so that vMotion does not run during a backup.

Multiple vmPRO Appliances

Multiple appliances cannot manage the same VM using CBT.

Activating and Deactivating CBT

Activating or deactivating CBT on a VM triggers the immediate and simultaneous creation and removal of a VM snapshot. This function is required by the VMware API.

The removal and creation of a snapshot for each VM can be a time-consuming process when activating or deactivating CBT on multiple VMs.

CBT and Retention Schedules

During differential disk backups, CBT needs to access data from the **flat.vmdk** file and the corresponding database entry. For this reason, the retention schedule for the backup policy does not initiate partial deletions of full backups. Instead, full backups, differential backups, and associated database entries are deleted at same time by the same retention schedule.

Configuring CBT on a vmPRO Appliance

Do the following to configure Changed Block Tracking (CBT) on your vmPRO appliance:

Enable CBT for Virtual Machine (VMs)

You must enable CBT for each VM on which you are performing differential backups from the **VMs Console – Virtual Machines** tab.

For detailed steps on how to enable CBT for VMs, see [Modifying VM Settings from the vmPRO appliance](#).

Schedule a CBT Cycle Reset

By default, the CBT cycle is reset each Sunday at 03:30. At this point, the vmPRO appliance performs a full backup of all CBT-enabled VMs. After the full disk backups complete, the vmPRO appliance performs differential backups of the VMs until the next Sunday at 03:30.

If needed, you can modify the CBT reset schedule from the **Configure Folders** dialog box. In addition, after CBT is enabled for a VM, you can perform a one-time, immediate reset of a base disk's modified time from the appliance's VMware vSphere Client console. A base disk's modified time is the last time the vmPRO appliance completed a full disk backup for the VM.

Note: Do not reset your CBT cycle to the same time at which backups are occurring. Instead, reset your CBT cycle to start a few hours before your backups to ensure that all CBT-enabled VMs have been reset before backups begin.

Modify a CBT reset schedule


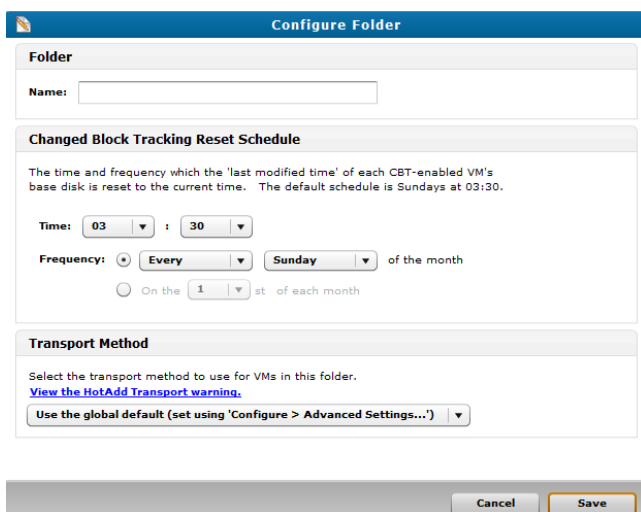
1. Click the **VMs** button to display the **VMs Console**.
2. Click the **Folders** tab to display the **Folders Tab** view.
3. In the **Folders** table, locate the folder that contains the VM for which to modify the CBT reset schedule.
4. For the appropriate folder, click  to display the **Configure Folder** dialog box.

Figure 72: Configure Folder Dialog Box



5. In the **Time** drop-down lists, select the hour and minute at which to reset the CBT schedule.

6. In the **Frequency** field, select one of the following options:

First Radio Button



Reset the CBT schedule for a selected interval and day of the month.

- a. In the first drop-down list, select one of the following intervals at which to reset the CBT schedule: **Every, First, Second, Third, Fourth, or Last**.
- b. In the second drop-down list, select the day of the month on which to reset the CBT schedule for the chosen interval.

Example

If you select **First** and **Sunday**, the CBT schedule is reset on the first Sunday of every month.

Second Radio Button



Reset the CBT schedule to a specific day each month.

- In the drop-down list, select the date (**1st–31st**) of each month on which to reset the CBT schedule.

7. Click **Save** to save changes and exit the dialog box.

Perform a one-time, immediate reset of a base disk's modified time

1. Access your appliance's Client console. See [Accessing the vSphere Client Console for vmPRO](#).
2. At the command line, enter `cbt reset [all | <hypervisor> <vm name> | folder <folder>]`.

The base disk's last modified time is reset to the current time.

Quantum VSS Writer

Enable the Quantum Volume Shadow Copy Service (VSS) Writer to perform VSS backups for Windows-based virtual machines (VMs) on an Active Directory (AD) Domain Controller.

The VSS Writer prepares Windows for a VMware snapshot to back up the VM's data. It then automates a non-authoritative restore of the Windows AD Domain Controller when the VM is restored.

When you restore a Windows AD Domain Controller from a snapshot image, the vmPRO appliance automatically boots the VM in the restore mode and performs necessary steps to prevent an update sequence number (USN) rollback. These steps ensure that directory replication works correctly.

Supported Systems

You can perform VSS backups only on systems for which the vmPRO appliance and Quantum VSS Writer support application-consistent quiescing and non-authoritative recovery from snapshot images.

Application-Consistent Quiescing

vmPRO supports application-consistent quiescing of the following Windows systems:

- Windows 2003 32bit/64bit
- Windows 2008 32bit/64bit
- Windows 2008 R2
- Windows 2012

Non-Authoritative Recovery

The VSS Writer supports automating non-authoritative recovery from a snapshot image of the following:

- AD
- Exchange 2007
- Exchange 2010
- Windows Server 2012
- SQL Server 2008
- SQL Server 2012

Troubleshooting Failed VSS Backups

If a VSS backup fails, make sure that the VMs being backed up are configured correctly. In addition, make sure of the following:

- The system to which you are backing up the VM must have enough free disk space. If the system does not have enough free disk space, the VSS backup will fail. For more information, see [http://technet.microsoft.com/en-us/library/cc708051\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc708051(v=ws.10).aspx).
- Each of the Windows system's VMs have the most up-to-date version of VMware Tools installed.
- VSS requires VMware Tools to be current. If a VM is configured for VSS but does not have a current version of VMware Tools, the following warnings appear on the vmPRO GUI:

Warnings

VMs Console

- The **VSS** column displays a red **YES** for the VM.

- An error message displays when you mouse over a VM with a red **YES** in the **VSS** column.

Alerts Console

An alert message displays for a VM that does not have a current version of VMware Tools. The message continues to display until you do one of the following:

- Update VMware Tools for the VM, and rediscovers the VM.
- Disable VSS for the VM.

VSS Resources

Use the following links to learn more about VSS:

- For more information how VMware can use VSS, see [Designing Backup Solutions for VMware vSphere](#).
- For more information about AD recovery, see [How to detect and recover from a USN rollback in Windows Server 2003, Windows Server 2008, and Windows 2008 R2](#) or [Active Directory Backup and Restore](#).

Preparing a Windows System for VSS Backups

Before beginning a Volume Shadow Copy Service (VSS) backup, you must prepare the Windows system on which a VSS backup is being performed by installing the Quantum VSS Writer, and configuring the system's virtual machines (VMs).

Install the Quantum VSS Writer

On each Windows system for which you are enabling VSS backups, you must install the Quantum VSS Writer. You can manually install the Quantum VSS Writer, or you can configure the vmPRO appliance to automatically install the VSS Writer. See [Configure virtual machines \(VMs\) being backed up with VSS on the next page](#)

-
- i Note:** Manually installing the VSS Writer does not require the Windows system's credentials. However, you will need to supply the Windows system's user name and password to have the vmPRO appliance automatically install the VSS Writer.

Manually install the Quantum VSS Writer

1. From the Windows system on which you are installing the VSS Writer, open a Web browser and navigate to `\\<vmPRO IP>\quantum-support\vss`.

2. Navigate to one of the following folders, as appropriate:

Folder	Description
2003	Contains the QuantumVSS.exe file that supports Windows 2003.
2008 and higher	Contains the following two sub-folders: <ul style="list-style-type: none">• 32bit – Contains the QuantumVSS.exe file that supports 32-bit servers of Windows 2008 or higher.• 64bit – Contains the QuantumVSS.exe file that supports 64-bit servers of Windows 2008 or higher.

3. Double-click the appropriate **QuantumVSS.exe** file to open the installer.
4. Follow the installer's instructions to complete the installation of the Quantum VSS writer.

Configure virtual machines (VMs) being backed up with VSS

For each VM being backed up using VSS, you must first enable quiesce for file system consistency. In addition, you can select to enable log truncation, as well as to configure the vmPRO appliance to automatically install and upgrade the VSS writer onto each VM.

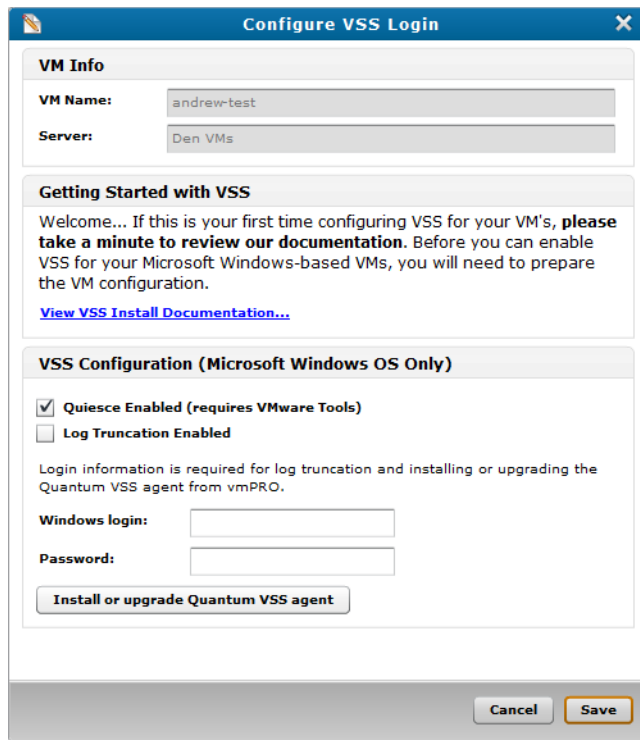
You can enable quiesce and test the VSS configuration for multiple VMs at the same time; however, you can only install or upgrade the Quantum VSS agent on one VM at a time.

To configure a single VM being backed up with VSS:

1. On the vmPRO appliance GUI, click the **VMs** button to display the **VMs Console**.
2. Click the **Virtual Machines** tab to display the list of VMs, as needed.
3. Select a VM for which to enable quiesce, and click **Edit Selected VMs** to display the **Configure Virtual Machine** dialog box.

4. Click **Configure VSS Settings** to display the **Configure VSS Login** dialog box.

Figure 73: Configure VSS Login Dialog Box – Single VM



5. Select the **Quiesce Enabled** check box.
6. Select the **Log Truncation Enabled** check box, as needed. For more information about log truncation, see [Using Log Truncation for VSS Backups](#).
7. Populate the following fields if you enabled log truncation, or to automatically install or upgrade the VSS writer:
 - a. **Windows login** – Enter the user name to access the Windows system on which log truncation or an automatic install/upgrade is occurring.
 - b. **Password** – Enter the password to access the Windows system on which log truncation or an automatic install/upgrade is occurring.
8. Click **Install or upgrade Quantum VSS agent** to install the VSS Writer onto the VM, as needed.

i Note: The installation or upgrade process can take some time if you are configuring a large number of VMs.

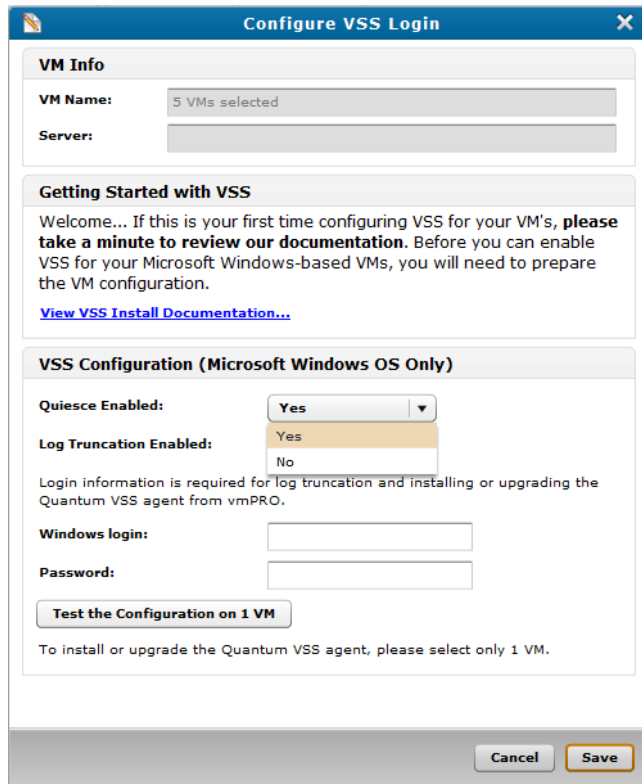
9. Click **Save** to save changes and exit the dialog box.

To enable quiesce for multiple VMs:

1. On the vmPRO appliance GUI, click the **VMs** button to display the **VMs Console**.

2. Click the **Virtual Machines** tab to display the list of VMs, as needed.
3. Select the VMs for which to enable quiesce, and click **Edit Selected VMs** to display the **Configure Virtual Machine** dialog box.
4. Click **Configure VSS Settings** to display the **Configure VSS Login** dialog box.

Figure 74: Configure VSS Login Dialog Box – Multiple VMs



5. From the **Quiesce Enabled** drop-down list, select **Yes**.
6. From the **Log Truncation Enabled** drop-down list, select **Yes**, as needed. For more information about log truncation, see [Using Log Truncation for VSS Backups](#).
7. Populate the following fields if you enabled log truncation:
 - a. **Windows login** – Enter the user name to access the Windows system on which log truncation or an automatic install/upgrade is occurring.
 - b. **Password** – Enter the password to access the Windows system on which log truncation or an automatic install/upgrade is occurring.
8. Click **Test the Configuration on 1 VM** to validate that the VSS configuration is compatible with the selected VMs.

-
- i Note:** The system tests the configuration on one of the selected VMs. After you save the configuration, the system will then test the configuration on all selected VMs and notify you of any errors.
9. After receiving confirmation that the VSS configuration is compatible with one VM, click **Save** to enable quiesce for the VMs and save changes.

Using Log Truncation for VSS Backups

To avoid overfilling a Windows system disk or partition with log files, which can lead to application downtime, it is important to truncate transaction logs after a VSS backup completes.

Enable log truncation on the **Configure VSS Login** dialog box (see [Preparing a Windows System for VSS Backups](#)). After log truncation is enabled, SmartMotion™ automatically truncates logs after a backup has completed successfully.

If you are not using SmartMotion, you need to manually initiate log truncation after a backup completes. Use the vmPRO appliance's GUI (see below) or the vmPRO appliance's VMware Console (see [vmPRO Console Commands – vss](#)) to manually initiate log truncation.

Manually initiate log truncation from the vmPRO appliance's GUI

1. On the vmPRO appliance GUI, click the **VMs** button to display the **VMs Console**.
2. Click the **Virtual Machines** tab to display the Virtual Machines tab view, as needed.
3. Click **Complete Backup (VSS)** to truncate the transaction logs.

-
- i Note:** The **Complete Backup (VSS)** button displays only after backups are run for VMs that have log truncation enabled. It can take up to an hour after the backup starts before the button displays.

Uninstalling the VSS Writer

If you need to uninstall the Quantum VSS Writer, use **Add/Remove Programs** on the Windows Control Panel. If you encounter an error uninstalling the VSS Writer, update the Uninstall key in the Registry Editor.

Update the Uninstall key

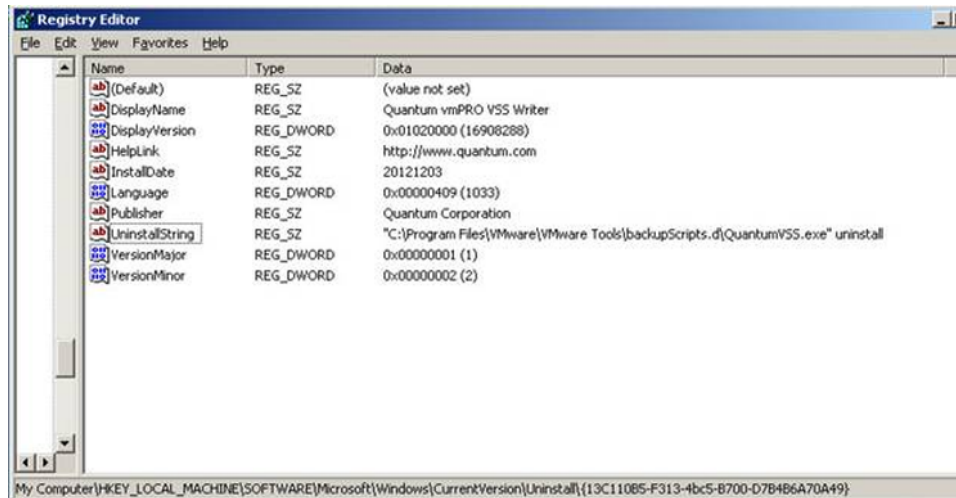
1. From the VM's Windows **Start** menu, select **Run** to open the **Run** dialog box.
2. In the **Open** field, enter **regedit** and click **OK** to display the **Registry Editor**.
3. Navigate to the following key:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{13C110B5-F313-4bc5-B700-D7B4B6A70A49}
```

4. Change the value of **UninstallString** to the following, including the quotes:

"C:\Program Files\VMware\VMware Tools\backupScripts.d\QuantumVSS.exe" uninstall

Figure 75: Registry Editor Window



Note: If the **Program Files** directory is not located at **C:\Program Files**, enter the actual location of the directory.

5. Return to **Add/Remove Programs**, and uninstall the VSS Writer.

vmPRO Advanced Settings

Use the following settings in the **Configure Advanced Settings** dialog box to configure additional settings for Progressive Optimization, HotAdd Transport methods, and SmartMotion™ backups.

vmPRO Advanced Settings

Enable the file system integrity check during backup

For Progressive Optimization to work correctly during SmartMotion backups, you need to allow your vmPRO appliance to execute file system integrity checks on virtual machine (VM) disks prior to the backup. Otherwise, recovery issues could occur.

Select this setting to allow your vmPRO appliance to execute a file system integrity check on VM disks before performing a backup.

Enable HotAdd Transport for all folders by default

Quantum vmPRO supports vSphere's HotAdd Transport feature. With HotAdd Transport, you can add and remove SCSI virtual hard disks while your vmPRO appliance is running. SCSI HotAdd provides a convenient method for transporting virtual disk data from guest virtual machines (VMs) directly to the ESX/ESXi host on which they are running. HotAdd improves performance and provides a non-network-based method of transferring data from the source VM to your vmPRO appliance for backup purposes.

Select this setting to enable HotAdd Transport for all folders within your vmPRO appliance.

Skip reading of page file and swap partitions during backup

For improved overall disk I/O savings during a SmartMotion backup, select this setting to enable Progressive Optimization to skip reading blocks of data associated with [temporary, transitional files](#)¹ on VMs.

Temporary and transitional files are not required for a full system restore, and so it is safe not to back up these files.

Allow a SmartMotion backup to run even if the same policy is already running

Select this setting to do the following:

- Start another scheduled SmartMotion backup of a policy, even if that same policy is currently running.
- Start another SmartMotion backup immediately after a long running backup – more than 24 hours – has completed.

This method is not the preferred backup method, and is not enabled by default.

Disallow backups when there is not enough datastore space for snapshot

Select this option to enable the vmPRO appliance to display an alert and stop a backup when the datastore is at a certain percentage of its total accessible capacity.

Configuring Advanced Settings for a vmPRO Appliance

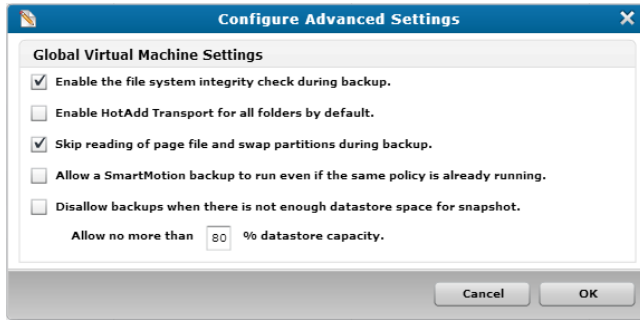
Use the settings in the **Configure Advanced Settings** dialog box to configure additional settings for Progressive Optimization, the HotAdd Transport method, and SmartMotion™ backups.

Configure advanced settings for a vmPRO appliance

1. From the **Configure** menu, select **Advanced Settings** to display the **Configure Advanced Settings** dialog box.

¹Examples include virtual memory paging files and temporary files created during software installation.

Figure 76: Configure Advanced Settings Dialog Box



2. Select the check box next to any of the following settings, as appropriate:

Settings

Enable the file system integrity check during backup

Select this setting to allow your vmPRO appliance to execute a file system integrity check on VM disks before performing a backup. See [About vmPRO Advanced Settings](#).

Enable HotAdd Transport for all folders by default

Select to enable HotAdd Transport for all folders within your vmPRO appliance. See [HotAdd Transport and Your vmPRO Appliance](#).

Skip reading of page file and swap partitions during backup

For improved overall disk I/O savings during a SmartMotion backup, select this setting to enable Progressive Optimization to skip reading blocks of data associated with [temporary, transitional files](#)¹ on VMs. See [About vmPRO Advanced Settings](#).

Allow a SmartMotion backup to run even if the same policy is already running

Select this setting to do the following:

- Start another scheduled SmartMotion backup of a policy even if that same policy is currently running.
- Start another SmartMotion backup immediately after a long running backup – more than 24 hours – has completed.

This method is not the preferred backup method, and is not enabled by default.

¹Examples include virtual memory paging files and temporary files created during software installation.

Settings

Disallow backups when there is not enough datastore space for snapshot

Select this setting to enable the vmPRO appliance to display an alert and stop a backup when the datastore is at a certain percentage of its total accessible capacity.

In the **Allow no more than <x> % datastore capacity** field, enter the percentage at which the vmPRO needs to display the alert and stop the backup.

3. Click **OK** to save settings and exit the dialog box.

HotAdd Transport and Your vmPRO Appliance

Quantum vmPRO supports vSphere's HotAdd Transport feature. With HotAdd Transport, you can add and remove SCSI virtual hard disks while your vmPRO appliance is running. SCSI HotAdd provides a convenient method for transporting virtual disk data from guest virtual machines (VMs) directly to the ESX/ESXi host on which they are running. HotAdd improves performance and provides a non-network-based method of transferring data from the source VM to your vmPRO appliance for backup purposes.

Enable HotAdd Transport in the **Advanced Settings** dialog box. See [Configuring Advanced Settings for a vmPRO Appliance](#).

- Note:** For hypervisors under moderate to heavy system loads, Quantum tests show significant performance improvement for backup throughput when HotAdd Transport is enabled.

Prerequisites

Ensure that the following prerequisites are met before enabling HotAdd Transport:

VM Conditions

Before enabling HotAdd Transport, keep in mind that the HotAdd Transport feature can only access VMs if one of the following conditions is met. If neither condition is met, the transport method automatically reverts to the network block device (NBD) transport method.

Condition 1

Target VMs that are on the same ESX server as the vmPRO appliance.

Condition 2:

Target VMs that are managed by the same vCenter server configured for the vmPRO appliance. In this case, the vmPRO must manage the ESX server through the vCenter server.

Target VMs under a vCenter server must also share the same storage, and the ESX server hosting the vmPRO appliance must also have access to the shared storage set up for the VMs.

vSphere's HotAdd Licensing Requirements

You must meet the following licensing requirements for your version of vSphere.

vSphere Version	Licensing Required
5.1 and newer	Does not require special licensing to use HotAdd Transport.
5.0	Requires Enterprise editions and higher with HotAdd licensing enabled.
4.1	Does not require special licensing to use HotAdd Transport.
4.0 update 2	Requires an Advanced, Enterprise, or Enterprise Plus license.

Verification

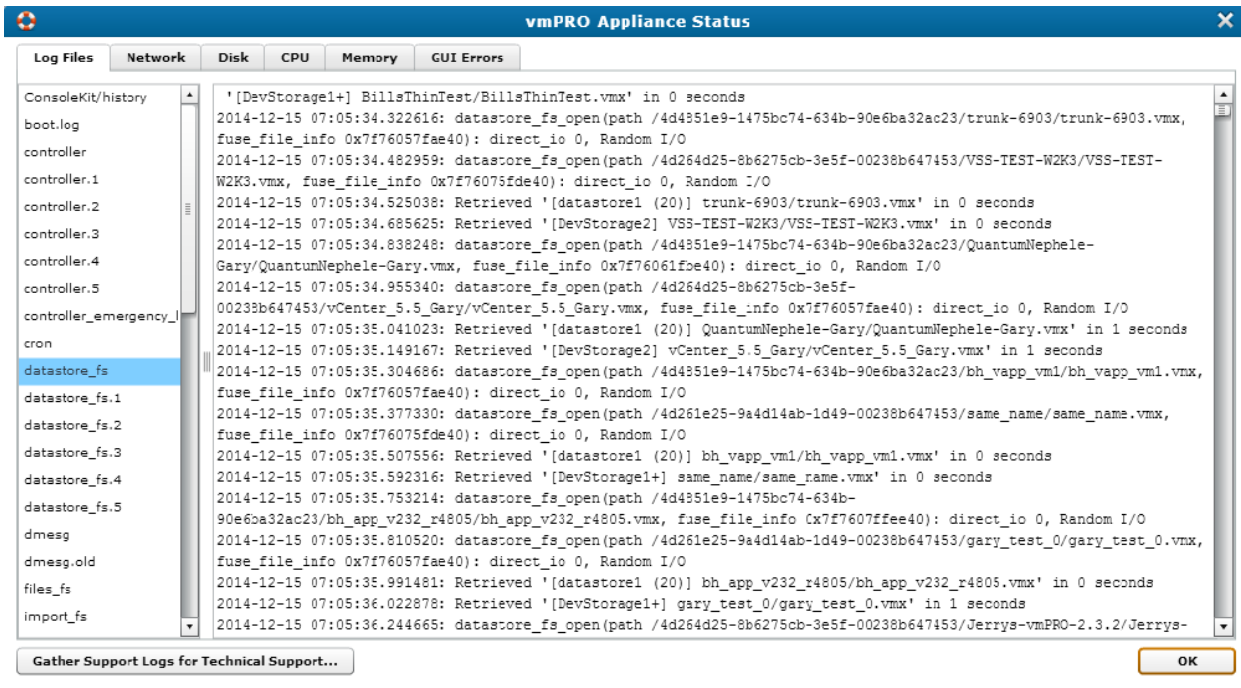
When you enable HotAdd Transport in the Advanced Configuration dialog box, you are *only requesting* that the vmPRO appliance use this transport method. Enabling HotAdd does not guarantee that the vmPRO appliance will use it.

Verify that the vmPRO appliance used HotAdd Transport

Use one of the following verification options:

- From your vmPRO appliance's GUI, select **Help > vmPRO System** to display the **vmPRO Appliance Status** dialog box.

Figure 77: vmPRO Appliance Status Dialog Box



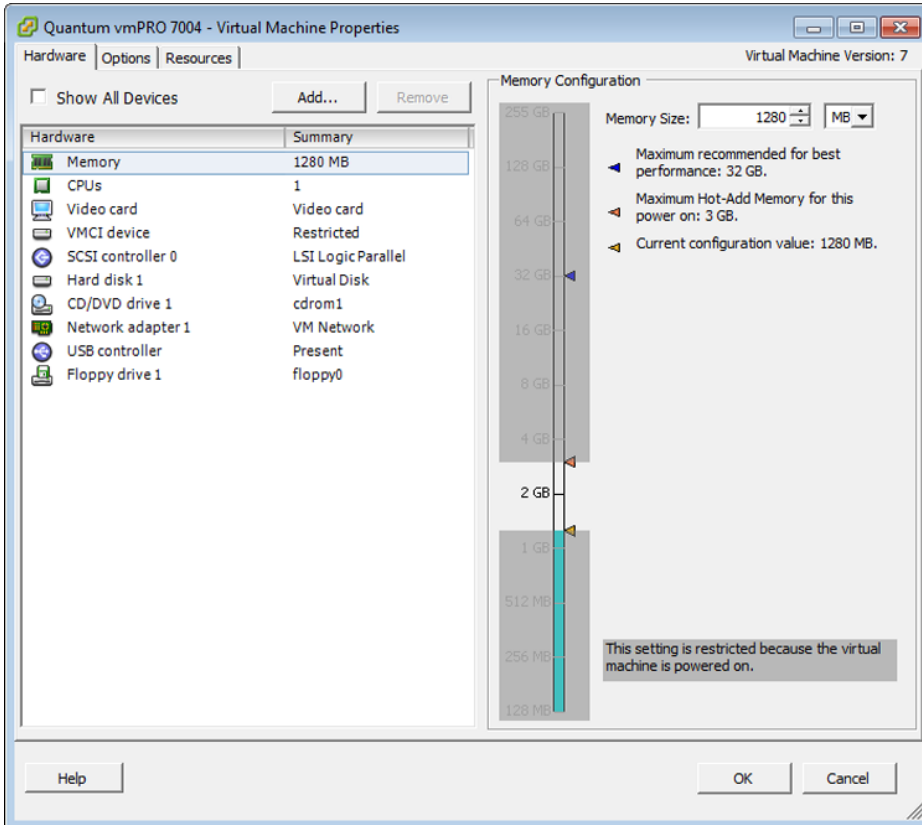
- Select the **Log Files** tab, as needed.
- Click **datastore_fs**, and look for **Obtained (and using) Transport Mode: hotadd** in the viewing pane.

If you see this message, the vmPRO appliance used HotAdd Transport.

Use one of the following verification options:

- a. Log in to your VMware vSphere Client.
- b. In the vSphere client's left pane, right-click on your vmPRO appliance and select **Edit Settings** to display the **Virtual Machine Properties** dialog box.

Figure 78: Virtual Machine Properties Dialog Box

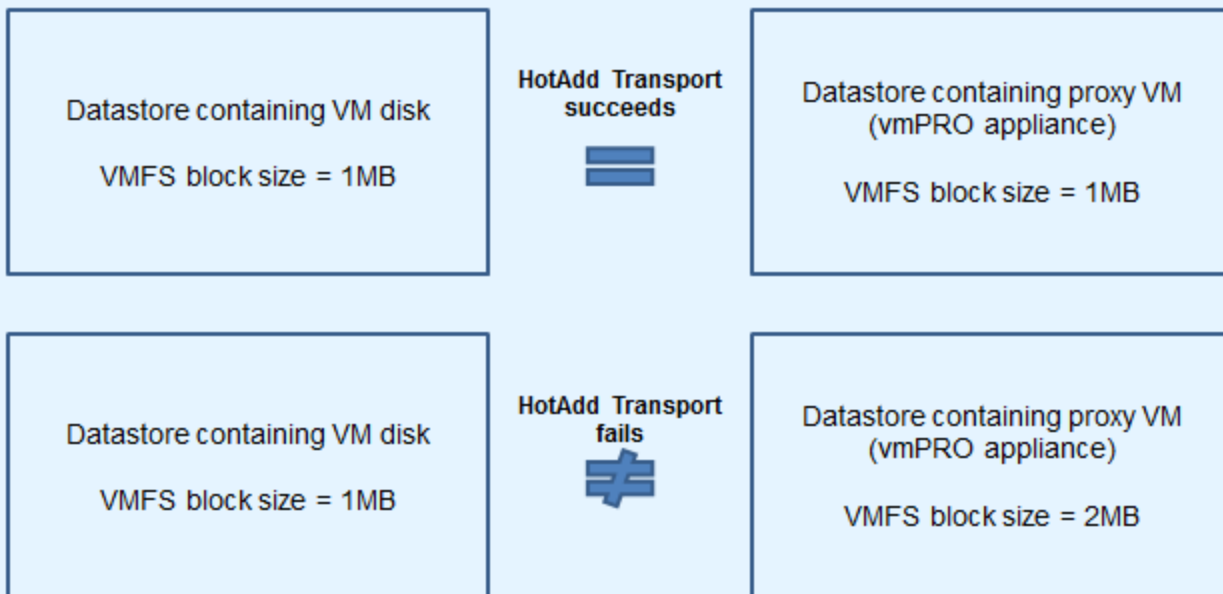


- c. Select the **Hardware** tab as needed, and verify that a new virtual disk is added each time a VM disk is backed up.

Limitation with Mismatched Block Size

When using HotAdd Transport, the Virtual Machine File System (VMFS) block size must be the same in both the datastore containing the backed-up VM disk and the datastore containing the proxy VM. Keep in mind that your vmPRO appliance is standing in as the proxy for the original VM from which the disk is backed-up.

Example





Chapter 3: vmPRO GUI

This chapter contains the following topics and sections:

vmPRO GUI	103
Accessing the vmPRO GUI	105
Embedding the vmPRO GUI in the vSphere Client	105
vmPRO GUI Menus	108
Navigating the vmPRO Home Console	115
Navigating the vmPRO VMs Console	117
vmPRO Auto-Export Feature	122
Modifying VM Settings from the vmPRO Appliance	123
Managing Servers and Nodes from the VMs Console	125
Navigating the vmPRO Alerts Console	130
Navigating the vmPRO Tasks Console	132

vmPRO GUI

The following is an overview of the functions and options you can access from the Quantum vmPRO GUI.

Home Console

The [Home console](#) displays a general status of the appliance, including active alerts, activity over the last 24 hours, summaries of the servers and virtual machines (VMs) that the vmPRO device is managing, and network throughput.

VMs Console

The [VMs console](#) displays status information about the VMs that are resident on the appliance. From this console, you can modify a VM's settings, select to use the Auto-Export feature, manage folders, and manage servers and nodes.

Alerts Console

The [Alerts console](#) displays a list of current and past alerts. Use this console to manage vmPRO alerts.

Tasks Console

The [Tasks console](#) displays backup and recovery information, as well as history for these tasks. From this console, you can manage backup and recovery tasks and backup policies.

vmPRO GUI Menus

Use the [vmPRO GUI menus](#) to access your appliance's SmartMotion features and operational controls, to configure your appliance, and to access help topics.

Refresh Button

Click  to update the vmPRO GUI display to the most current information.

Accessing the vmPRO GUI

Your primary means of interacting with the Quantum vmPRO appliance is through its GUI. Use the following task to assist you in accessing the vmPRO GUI.

Access the vmPRO GUI:

1. In a Web browser's address field, enter the IP address of the vmPRO appliance to display the **Quantum vmPRO Login** page.

Figure 79: Quantum vmPRO Login Page



2. In the **User name** field, enter the user name for the appliance. The default user name is **sysadmin**.
3. In the **Password** field, enter the password for the appliance. The default password is **sysadmin**.
4. Click **OK** to display the vmPRO GUI.

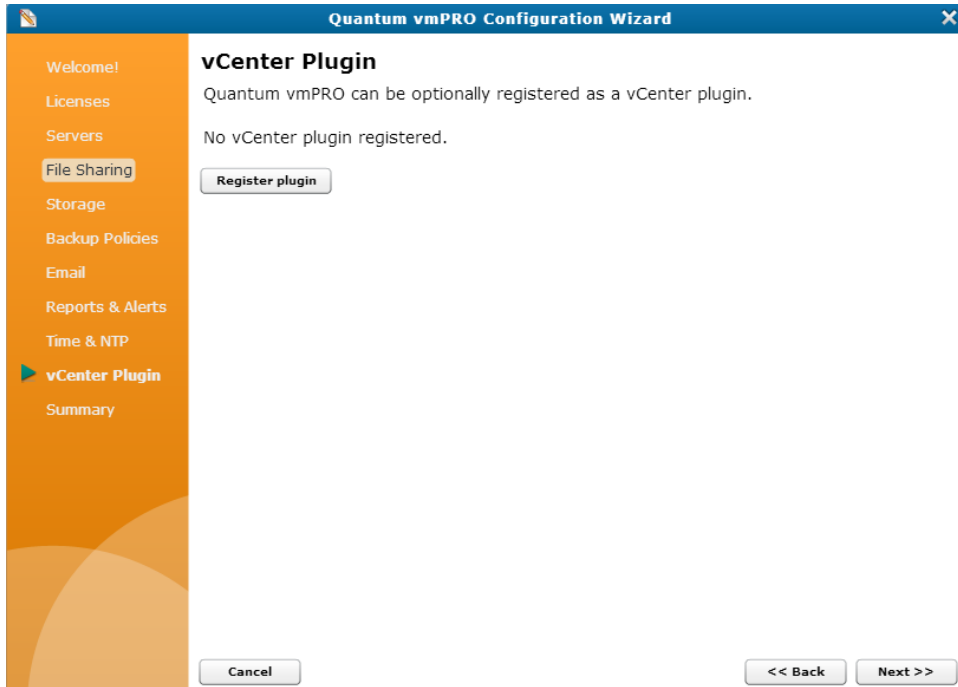
Embedding the vmPRO GUI in the vSphere Client

If you use a vCenter server for your vmPRO appliance, you can embed the vmPRO GUI directly into your vSphere Client. To use this feature, a Quantum plugin must be registered with the vCenter server.

Register the vmPRO appliance as a vCenter plugin

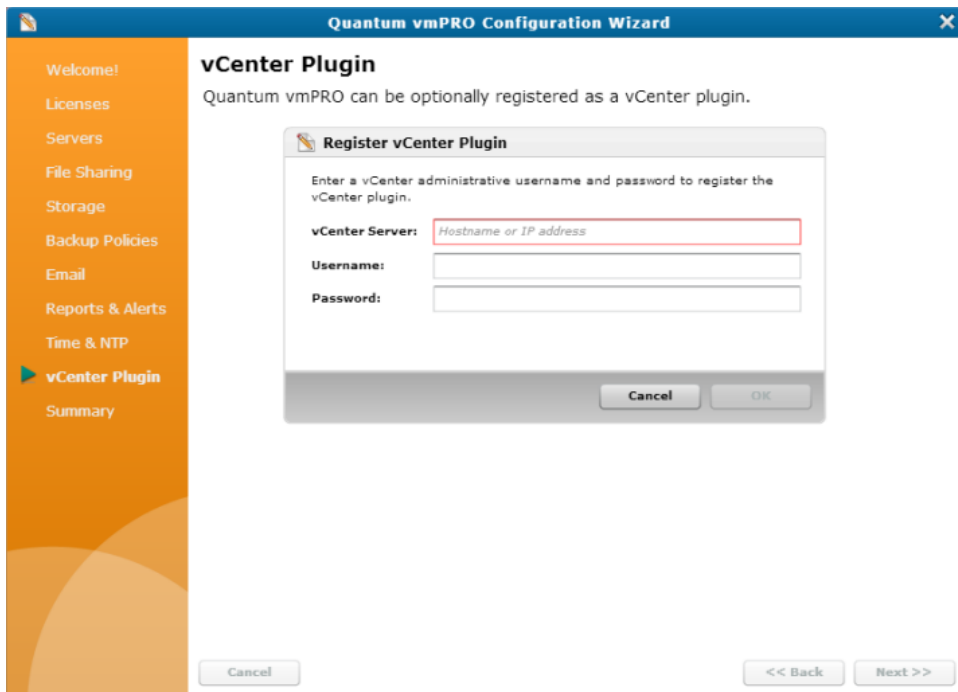
1. From the **Configure** menu, select **Config Wizard** to display the **Quantum vmPRO Configuration Wizard**.
2. Click the **vCenter Plugin** tab to display the **vCenter Plugin** page.

Figure 80: vCenter Plugin Page



3. Click **Register plugin** to display the **Register vCenter Plugin** page.

Figure 81: Register vCenter Plugin Page



4. In the **vCenter Server** field, enter the IP address or resolvable host name of your vCenter server.
If you need to register your vCenter plugin using an alternate port, enter the IP address and port number using the following format:

<IP_address:port_number>

5. In the **Username** field, enter the administrative user name for accessing the vSphere Client.
6. In the **Password** field, enter the administrative password for accessing the vSphere Client.
7. Click **OK** to register the vmPRO plugin with the vCenter server.
8. Save changes and exit the wizard.

⚠ Caution: Any time you make configuration updates from the **Quantum vmPRO Configuration Wizard**, you must exit the wizard using the **Summary** tab to save your updates. See [Initially Configuring a vmPRO Appliance](#).

9. Restart your vCenter server.

Access the vmPRO appliance from your vSphere Client:

1. Log in to your vSphere Client.
2. In the left pane, select the vmPRO appliance.
3. Select the **Quantum vmPRO <IP address>** tab to display the vmPRO GUI in the tab.

4. Log in to the vmPRO GUI. See [Accessing the vmPRO GUI](#).

i Note: If the vmPRO GUI does not load, make sure Adobe Flash Player is installed on the system running the vSphere Client.

vmPRO GUI Menus

Use the vmPRO GUI menus to access the following features.

SmartMotion Backup Menu

Use the **SmartMotion Backup** menu to access the following features:

Menu Item	Feature
Backup	Run SmartMotion Backup Use this feature to run a SmartMotion backup. In addition, you can edit a backup policy before running a SmartMotion backup. See vmPRO SmartMotion Backup .
Recover	Recover Virtual Machines Wizard Use this feature to recover virtual machines (VMs), or mailboxes on an exchange server. See vmPRO Data Recovery .
iSCSI Targets	iSCSI Targets Use this feature to view and manage virtual disk backups that you have exported as iSCSI targets. See Recovering VM Disks Using iSCSI .
Backup Policies	Available Backup Policies Use this feature to create a new policy, set a default policy, edit an existing policy, edit the folder assignments for the policy, or delete a policy. See vmPRO SmartMotion Backup Policies .
Storage	Available Storage Use this feature to add, edit, or delete storage. See Configuring NAS Targets for SmartMotion Backups .

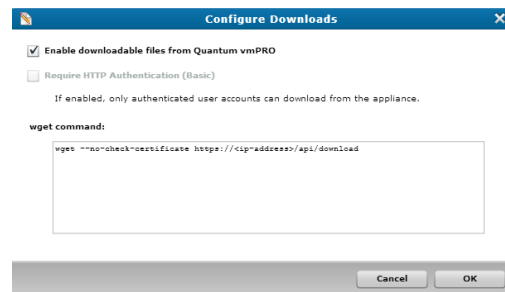
Configure Menu

Use the **Configure** menu to access the following features:

Menu Item	Feature
Servers	Configure Server List Use to add an ESX server to the vmPRO appliance, modify an existing server's configuration, or delete a server from the appliance. You must add vCenter servers using the Configuration Wizard . See Configuring a vCenter Server for a vmPRO Appliance . See Configuring ESX Servers for a vmPRO Appliance or Managing Servers and Nodes from the VM Tab .
CIFS	Configure CIFS Use to configure a CIFS file sharing protocol for the /export and /recover directories exported by the vmPRO appliance. See Configuring a CIFS Protocol for a vmPRO Appliance .
NFS	Configure NFS Use to configure an NFS file sharing protocol for the /export and /recover directories exported by the vmPRO appliance. See Configuring an NFS Protocol for a vmPRO Appliance .
iSCSI	Configure iSCSI Use to configure the iSCSI write area by defining the following: <ul style="list-style-type: none">• The storage target for the iSCSi backup.• The maximum size of each iSCSI target's write area. See Preparing For Exchange Recovery .
Email	Configure Email Use to configure email sent from your vmPRO appliance. See Configuring Email for a vmPRO Appliance .
Reports & Alerts	Configure Reports & Alerts Use to create a list of recipients for emailed reports and alerts, as well as to view reports and send reports. See Configuring Reports, Alerts, and Autosupport for a vmPRO Appliance .
Advanced Settings	Configure Advanced Settings Use to enable advanced features for your vmPRO appliance. See Configuring Advanced Settings for a vmPRO Appliance .

Menu Item	Feature
Users	Configure User List Use to configure user access to your vmPRO appliance. See Configuring Users for a vmPRO Appliance .
Downloads	Configure Downloads Use to configure file download settings to accomplish the following: <ul style="list-style-type: none">• Enable the vmPRO appliance to download files.• Define who can access downloaded files.• Define wget commands for downloading files. When the vmPRO appliance downloads files, you can access the files at http://<vmPRO_appliance_IP-address>/api/download . Configure downloads for a vmPRO appliance <ol style="list-style-type: none">a. Select the Enable downloadable files from Quantum vmPRO check box to allow files to be downloaded from the vmPRO appliance.b. Select the Require HTTP Authentication (Basic) check box to require user authentication to access downloaded files from the vmPRO appliance.c. In the wget command field, enter additional wget commands, or edit existing ones, as needed.d. Click OK to save changes and exit the dialog box.
Software Updates	Configure Software Updates Use both to schedule and check for vmPRO software updates. See Updating vmPRO Versions 3.1 or Newer .
Config Wizard	Quantum vmPRO Configuration Wizard Use to access a wizard to guide you through configuration steps for licenses, servers, file sharing, storage, backup policies, email, reports and alerts, time and NTP, and vCenter plugins. See Initially Configuring a vmPRO Appliance .

Figure 82: Configure Downloads Dialog Box

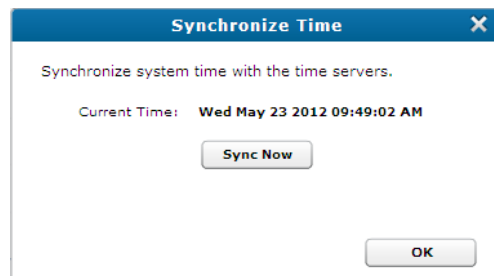


Operations Menu

Use the **Operations** menu to access the following features:

Menu Item	Feature
Discover Now	Discovery Use to initiate the vmPRO Discovery feature, in which the appliance automatically finds all VMs that are candidates for export. See Discovering Servers for a vmPRO Appliance .
View Report	Quantum vmPRO Report Use to view a report of your vmPRO appliance's daily activity. Report Contents <ul style="list-style-type: none">• Current alerts for the vmPRO appliance.• Licenses configured for the vmPRO appliance.• Servers configured for the vmPRO appliance.• VMs discovered by the vmPRO appliance.• SmartMotion™ statistics for the vmPRO appliance.• History of commands given to the vmPRO appliance.• Performance history for the vmPRO appliance.• Statistics for VMs on the vmPRO appliance.• Status of the vmPRO appliance.• Log files for the vmPRO appliance.
Synchronize With Time Server	Synchronize Time Use to synchronize your vmPRO appliance with the time server. Synchronizing your vmPRO appliance with the time server <ol style="list-style-type: none">a. In the Synchronize Time dialog box, click Sync Now.b. After the synchronization has completed, click OK to exit the dialog box.

Figure 83: Synchronize Time Dialog Box



Menu Item	Feature
Gather Support Logs	Gather Support Logs Use to create and upload support packages to assist Quantum technical support. Creating and uploading support packages <ol style="list-style-type: none">Click Create Support Package to automatically bundle system logs into a support package.Click Download Support Package to download the system logs to a local server.Click Upload Support Logs to Quantum to send the bundled system logs to Quantum technical support.

Figure 84: Gather Support Logs Dialog Box



Menu Item	Feature
Export vmPRO Configuration	<p>Export vmPRO Configuration</p> <p>Use to save a copy of your vmPRO appliance's current XML configuration file. Use this file to do the following:</p> <ul style="list-style-type: none">• Restore your vmPRO appliance's configuration in the event of a disaster recovery scenario.• Transfer the configuration settings of an existing vmPRO appliance group to a new vmPRO appliance group. <p>Export the XML configuration file</p> <ol style="list-style-type: none">a. Follow the instructions on the displayed Quantum vmPRO Configuration Save and Import page.b. Note the name and location of the group's configuration file when you download it.

Figure 85: Quantum vmPRO Configuration Save and Import Page

Quantum vmPRO Configuration Save and Import

Save a copy of your configuration

Provided below is a link to a file containing configuration information for this vmPRO. *Please note, this package contains password information and should only be provided to administrators.*

- [db-package.tar.bz2.enc](#)

Import a saved configuration

In the box below select a saved configuration file that you would like to import, and then click 'Import'. The configuration of this vmPRO will be set to the saved copy, including login information. The update may take a few minutes to complete.

WARNING: Before importing a configuration, the vmPRO from which the configuration package originated must no longer be in use. Importing the same configuration to multiple vmPRO appliances is not supported and can cause undesired results.

Importing is only supported to vmPRO appliances with factory default settings.

Select the package: No file chosen

[Quantum vmPRO](#)
Thu Nov 13 15:01:32 2014

Menu Item	Feature
Import vmPRO Configuration	<p>Import vmPRO Configuration</p> <p>Use to import a previously saved XML configuration file into the current vmPRO appliance.</p> <p>Only vmPRO appliances with factory default settings support importing XML configuration files.</p> <p>Import an XML configuration file</p> <ol style="list-style-type: none">Follow the instructions on the displayed Quantum vmPRO Configuration Save and Import page.Browse to the location of the exported configuration file, and double-click it to import the configuration settings.

Figure 86: Quantum vmPRO Configuration Save and Import Page

Quantum vmPRO Configuration Save and Import

Save a copy of your configuration

Provided below is a link to a file containing configuration information for this vmPRO. *Please note, this package contains password information and should only be provided to administrators.*

- [db-package.tar.bz2.enc](#)

Import a saved configuration

In the box below select a saved configuration file that you would like to import, and then click 'Import'. The configuration of this vmPRO will be set to the saved copy, including login information. The update may take a few minutes to complete.
WARNING: Before importing a configuration, the vmPRO from which the configuration package originated must no longer be in use. Importing the same configuration to multiple vmPRO appliances is not supported and can cause undesired results.

Importing is only supported to vmPRO appliances with factory default settings.

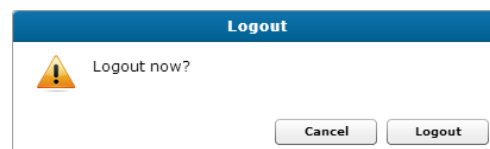
Select the package: No file chosen

*Quantum vmPRO
Thu Nov 13 15:01:32 2014*

Change My Password	<p>Configure User</p> <p>Use to change the password for the currently logged-in user.</p> <p>This function changes the user's password for both the vmPRO GUI and the vmPRO's Console Command Line (CLI) interface.</p> <p>See Configuring Users for a vmPRO Appliance.</p>
---------------------------	--

Logout	<p>Logout</p> <p>Use to log out of the vmPRO GUI.</p>
---------------	--

Figure 87: Logout Dialog Box



Help Menu

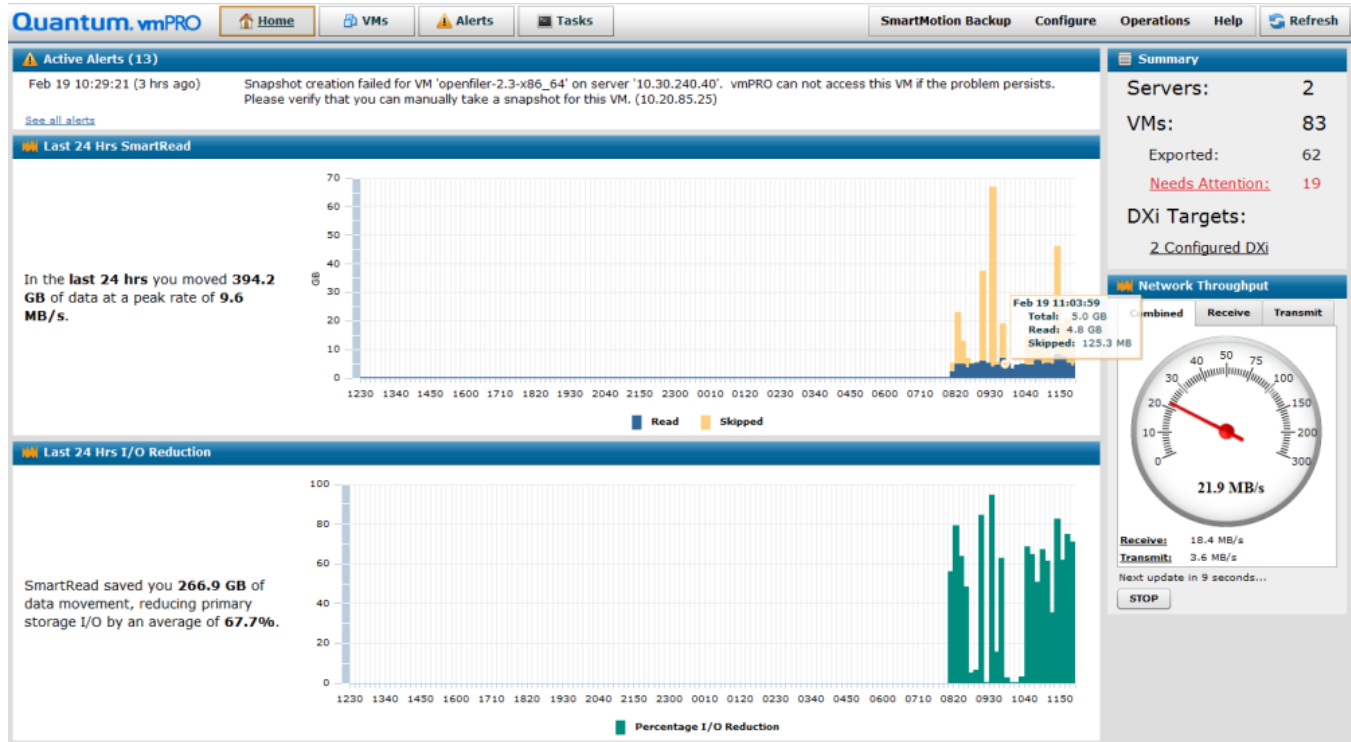
Use the **Help** menu to access the following features:

Menu Item	Feature
Help Contents	Quantum vmPRO Online Help Use to access the Quantum vmPRO Help.
Online Help	Quantum vmPRO Knowledge Base Use to access Knowledge Base articles addressing vmPRO functionality, installation, and other topics.
About	About Quantum vmPRO Use to access information about your vmPRO appliance, such as the privacy statement, copyright and patent information, version, and Flash runtime version.
Licensing	Quantum vmPRO Licensing Use to view information about the vmPRO appliance's license. Displayed Information <ul style="list-style-type: none">• Type of license.• Total licensed capacity.• Current capacity usage.• Expiration date.• Number of days remaining until the expiration date.
End User License	Quantum vmPRO End User License Agreement Use to access and accept the Quantum vmPRO End User License Agreement.
vmPRO System	vmPRO Appliance Status Use to view your vmPRO appliance's log files, network information, disk information, CPU information, memory statistics, and GUI errors. From this dialog box, you can also access the Gather Support Logs dialog box.

Navigating the vmPRO Home Console

Use the vmPRO **Home** console to view a general status of the appliance, including active alerts, activity over the last 24 hours, summaries of the servers and virtual machines (VMs) that the vmPRO device is managing, and network throughput.

Figure 88: Home Console



Navigate the vmPRO Home console

1. Log in to the vmPRO appliance GUI to display the **Home** console. If you are on a different tab, click the **Home** button to display the **Home** console.
2. In the **Active Alerts** pane, review the following information:
 - Total number of active alerts.
 - The date and time of the most recent alert.
 - A short description of the most recent alert.

To view all alerts for your vmPRO appliance, click the **See all alerts** link.

3. In the **Last 24 Hrs SmartRead** pane, view the amount of data that has been backed up within the past 24 hours.

Hold the cursor over a line or bar on the chart to see the date and time the data was backed up, along with the total amount of data, the total amount of data read (backed up), and the total amount of data skipped on the associated VMs.

4. In the **Last 24 Hrs I/O Reduction** pane, view the amount of data reduction achieved within the past 24 hours.

5. In the **Summary** pane, review the following information:

Field	Description
Servers	The total number of servers that the vmPRO appliance is managing.
VMs	The total number of VMs that the vmPRO appliance is managing, along with the number of VMs that are exported, and the number of VMs requiring attention. Click the Needs Attention link to display the Resources tab to access additional information regarding the VMs. See Navigating the vmPRO VMs Console .
DXi Targets	If DXi devices are configured for storage with CIFS or NFS shares, displays the IP address for each DXi target. Click this link to open the native management interface for the DXi device. If more than one DXi device is available for extra storage, the x Configured DXi link displays. Click this link to display the Available Storage dialog box. See Configuring NAS Targets for SmartMotion Backups .

6. In the **Network Throughput** pane, review the speed at which the current session is processing the following data:

Data Type	Description
Combined	A combination of both received and transmitted data.
Received	Received data, such as data being recovered.
Transmit	Transmitted data, such as data being backed up.

- Click the appropriate tab or link to display the corresponding data type.
- Click **Stop** to stop the data refresh feature.
- Click **Start** to restart the data refresh feature.

Navigating the vmPRO VMs Console

The **VMs** console displays status information about the virtual machines (VMs) that are resident on the appliance. From this console, you can modify a VM's settings, select to use the Auto-Export feature, manage folders, and manage servers and nodes.

The following three tabs are located on the VMs console

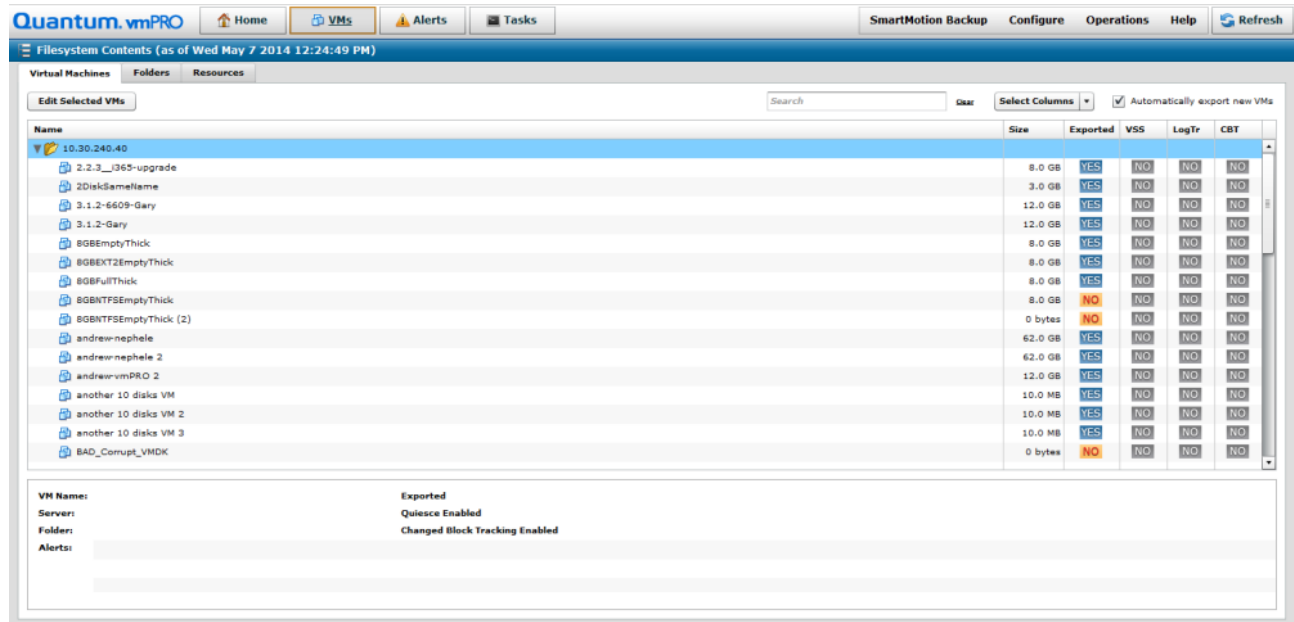
Virtual Machines Tab

Use this tab to view and manage VMs.

Navigate the Virtual Machines tab in the VMs console

1. On the vmPRO appliance GUI, click the **VMs** button to display the **VMs** console.
2. Click the **Virtual Machines** tab, as needed.

Figure 89: VMs Console – Virtual Machines Tab



3. Review the following information in the grid columns:

Note: You can select the columns to display from the **Select Columns** drop-down list, as well as search for a specific VM by entering its name in the **Search** field. Click **Clear** to clear any search criteria.

Column	Description
Name	The name of each VM being managed by the vmPRO appliance. The VMs are organized in folders. Click the arrow next to a folder to view the list of VMs within the folder.
Server	The server on which the VM is located.
Datstore	The datstore housing the VM's data.

Column	Description
Node	The IP address of the vmPRO appliance managing the VM.
Size	The maximum allocated capacity for the VM's virtual disks.
Exported	Whether the VM has been added to the vmPRO appliance's /export directory. If the VM has been exported and a SmartMotion™ backup policy is configured for the VM's folder, then the VM will be backed up to the defined storage target.
VSS	Whether the VSS operation is set to run during a SmartMotion backup of the VM. See Quantum VSS Writer . This option is only available for Windows-based VMs.
LogTr	Whether log truncation has been enabled for the VM. See Using Log Truncation for VSS Backups .
CBT	Whether Changed Block Tracking has been enabled for the VM. See vSphere Changed Block Tracking Support .

- Click on a VM to view summary information in the following fields at the bottom of the console:

Field	Description
VM Name	The name assigned to the VM.
Server	The server on which the VM is located.
Folder	The folder in which the VM is located.
Alerts	Whether alerts exist for the VM.
Exported	Whether the VM is backed up.
Quiesce Enabled	Whether quiesce has been enabled for the VM. See Preparing a Windows System for VSS Backups .
Change Block Tracking Enabled	Whether Change Block Tracking has been enabled for the VM. See vSphere Changed Block Tracking Support .

- Select one or more VMs and click **Edit Selected VMs** at the upper left of the grid to display the **Configure Virtual Machine** dialog box.

Use the dialog box to modify the selected VMs' configuration settings. See [Modifying VM Settings from the vmPRO Appliance](#).

6. Select the **Automatically export new VMs** check box located at the upper right of the grid to enable the Auto-Export feature. See [vmPRO Auto-Export Feature](#).

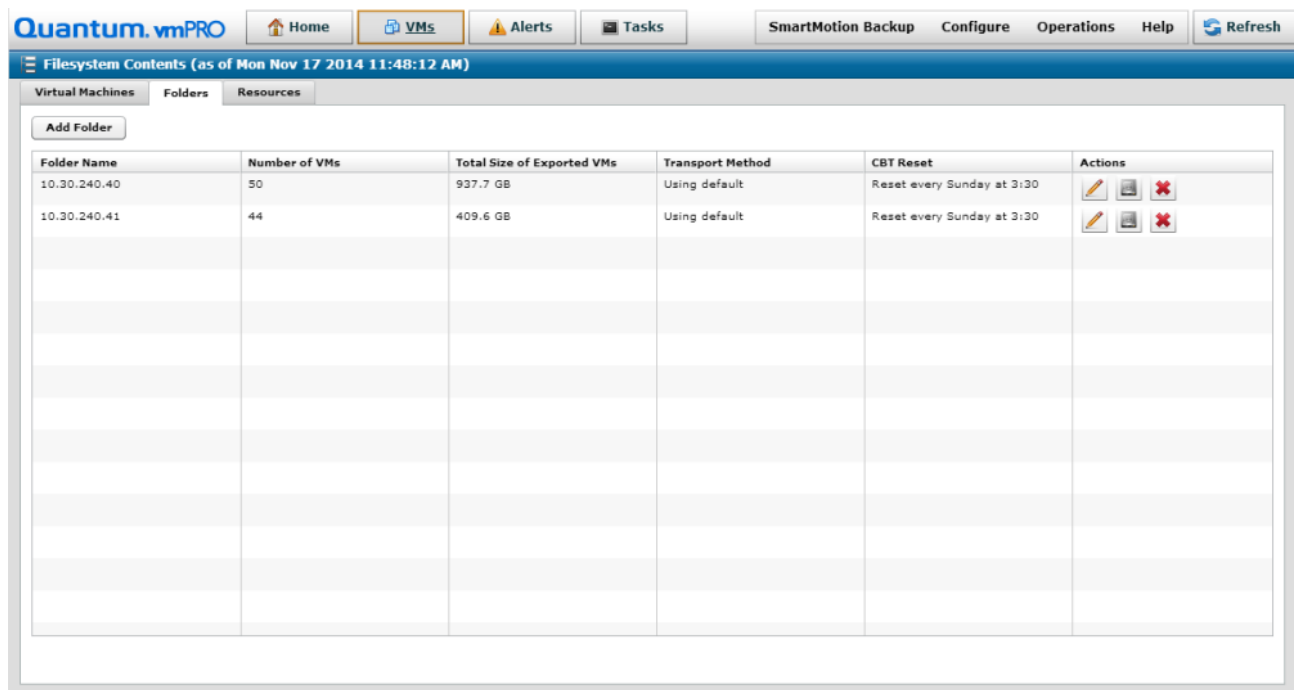
Folders Tab

Use this tab to view and manage folders.

Navigate the Folders tab in the VMs console




1. On the vmPRO appliance GUI, click the **VMs** button to display the **VMs** console.
2. Click the **Folders** tab, as needed.

Figure 90: VMs Console – Folders Tab



3. Review the following information in the grid columns:

Column	Description
Folder Name	The name of the folder.
Number of VMs	The number of VMs within the folder.
Total Size of Exported VMs	The total size of exported data for the VMs within the folder.

Column	Description
Transport Method	The method used to access the data of the VMs within the folder during SmartMotion backups: global default , HotAdd with fall back to NBD , or NBD only . See Configuring vmPRO Folders .
CBT Reset	The day and time on which the change block tracking schedule is reset for the VMs within the folder. See Configuring CBT on a vmPRO Appliance .
Actions	The following action icons:  Click to edit the folder. The Configure Folder dialog box displays. See Configuring vmPRO Folders .  Click to back up the folder. The Run SmartMotion Backup dialog box displays. See vmPRO SmartMotion Backup .  Click to delete the folder.

4. Click **Add Folder** to display the **Configure Folder** dialog box. Use this box to configure a new folder. See [Configuring vmPRO Folders](#).

Resources Tab

Use this tab to view and manage both servers configured for the vmPRO appliance, as well as [nodes](#)¹ assigned to the appliance if it is a group master. See [Managing vmPRO Groups](#).

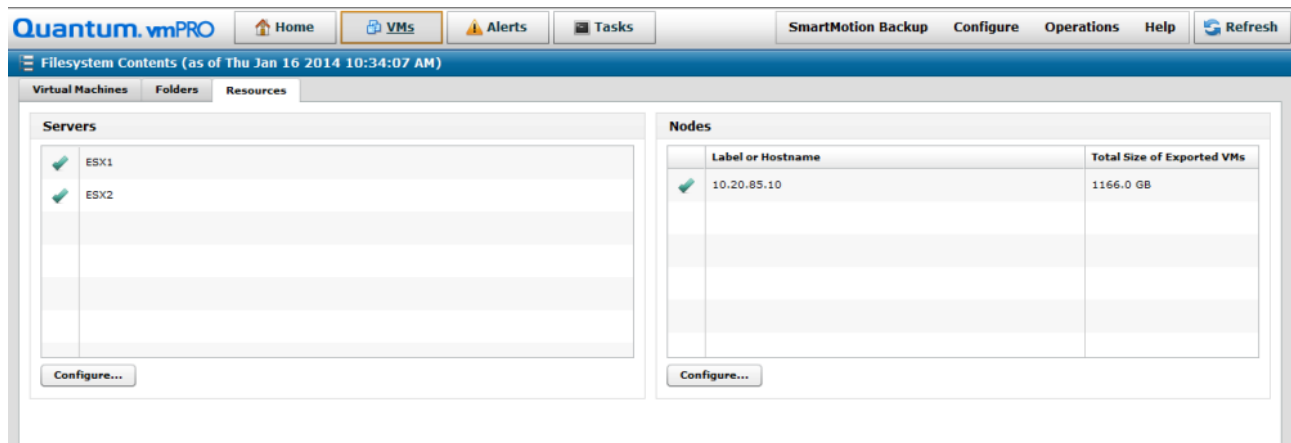
Navigate the Resources tab on the VMs Console

1. On the vmPRO appliance GUI, click the **VMs** button to display the **VMs** console.

¹Nodes are subordinate vmPRO appliances in a group configuration.

2. Click the **Resources** tab, as needed.

Figure 91: VMs Console – Resources Tab



3. In the **Servers** pane, review the list of servers configured for the vmPRO appliance.
4. In the **Servers** pane, click **Configure** to display the **Configure Server List** dialog box.

Use this dialog box to add ESX servers, edit servers, or delete servers. See [Managing Servers and Nodes from the VMs Console](#).

Note: You must add vCenter servers using the **Quantum vmPRO Configuration Wizard**. See [Configuring a vCenter Server for a vmPRO Appliance](#).

5. In the **Nodes** pane, review the following information for all nodes assigned to the master appliance:

Column	Description
Label or Hostname	The label or IP address assigned to the node.
Total Size of Exported VMs	The total size of the VM disks that have been exported to the node's /export directory and are available for SmartMotion backup.

6. In the **Nodes** pane, click **Configure** to display the **Configure Node List** dialog box.

Use this dialog box to edit a node's label, email a notification regarding a node, or delete a node. See [Managing Servers and Nodes from the VMs Console](#).

vmPRO Auto-Export Feature

The vmPRO Auto-Export feature automatically enables SmartView™ and SmartMotion capabilities for any new virtual machine (VM) discovered in the vCenter inventory. By default, when you deploy a new appliance, the Auto-Export feature is enabled.

Auto-Export Tips

Review the following tips before using Auto-Export:

Unattended Backups

The Auto-Export feature is convenient for unattended backups of remote, isolated, or fully automated vSphere environments. In addition, this feature assists with scheduled backups for systems where VMs are frequently moving between servers. When Auto-Export is enabled, the vmPRO appliance recognizes when VMware moves VMs.

Capacity Threshold Alerts

Keep in Mind that *automatic* does not mean set-and-forget. Each VM that is backed up consumes space on the target storage device. As the population of VMs grows, so do the storage requirements. To monitor storage requirements, set the threshold at which you want to receive alerts regarding your capacity. See [Adding Licenses to a vmPRO Appliance](#).

Large Environments

Use Auto-Export with caution, especially when enabling the feature in large environments. Excessive additions of VMs during a backup may overburden the storage target, causing the backup to run longer than anticipated. Account for any new VMs that may be automatically exported, typically due to a vMotion/DRS operation that relocates VMs onto a vSphere host that is being managed by the vmPRO appliance. Plan for available capacity in your backup target.

Modifying VM Settings from the vmPRO Appliance

You can modify virtual machine (VM) configuration settings from the **Virtual Machines** tab on the **VMs** console. You can modify a single VM's configuration settings, or select multiple VMs for which to modify these settings.

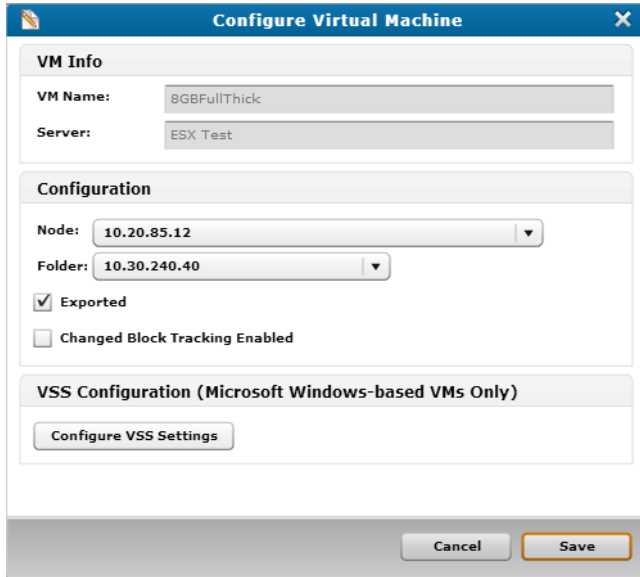
Modify VM configuration settings

1. On the vmPRO appliance GUI, click the **VMs** button to display the **VMs** console.
2. Click the **Virtual Machines** tab, as needed.
3. Select one VM, or multiple VMs, for which to modify configuration settings.
4. Click **Edit Selected VMs** to display the **Configure Virtual Machine** dialog box.

For a single VM

The VM's name and server display in the **VM Name** and **Server** fields, respectively.

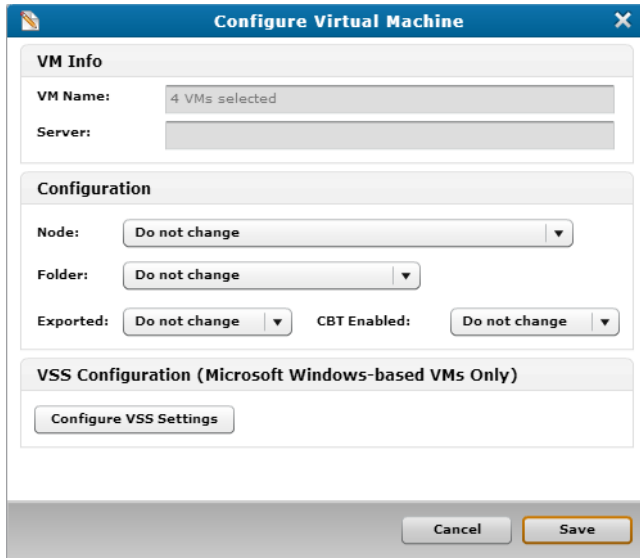
Figure 92: Configure Virtual Machine Dialog Box – Single VM



For multiple VMs

The number of selected VMs displays in the **VM Name** field. The **Server** field is unpopulated.

Figure 93: Configure Virtual Machine Dialog Box – Multiple VMs



5. Modify the following settings, as needed:

Field	Option
Node	From the drop-down list, select a different node to assign to the VM or VMs.
Folder	From the drop-down list, select a different folder to assign to the VM or VMs.
Exported	<ul style="list-style-type: none">• For a single VM, select the check box to tag the VM for SmartMotion backup.• For multiple VMs, select Yes or No from the drop-down list to indicate whether the VMs should be tagged for SmartMotion backup.
Change Block Tracking/CBT Enabled	<ul style="list-style-type: none">• For a single VM, select the check box to enable Changed Block Tracking (CBT) for the VM.• For multiple VMs, select Yes or No from the drop-down list to enable CBT for the VMs. See vSphere Changed Block Tracking Support .

6. To configure VSS settings for the VM(s), click **Configure VSS Settings** to display the **Configure VSS Login** dialog box. See [Quantum VSS Writer](#).

Note: You can configure VSS settings for Microsoft Windows-based VMs only.

7. Click **Save** to save updates and exit the dialog box.

Managing Servers and Nodes from the VMs Console

You can manage your vmPRO appliance's servers and nodes from the **Resources** tab on the **VMs** console.

Servers

From the **Resources** tab, you can add ESX servers, edit servers, or delete servers.

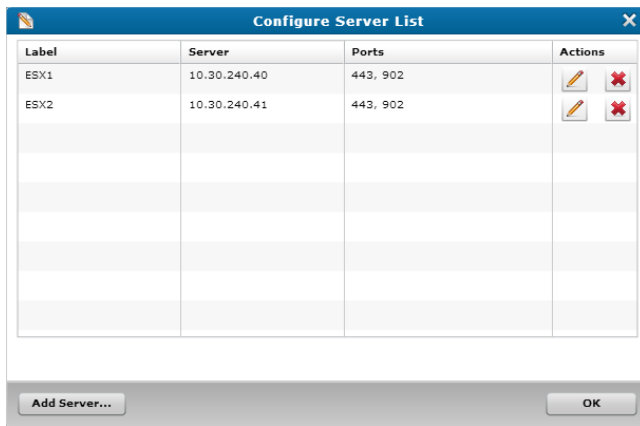
Note: You must add vCenter servers using the **Quantum vmPRO Configuration Wizard**. See [Configuring a vCenter Server for a vmPRO Appliance](#).

Manage servers

1. On the vmPRO appliance GUI, click the **VMs** button to display the **VMs** console.
2. Click the **Resources** tab, as needed.

3. In the **Servers** pane, click **Configure** to display the **Configure Server List** dialog box.

Figure 94: Configure Server List Dialog Box



The dialog box displays the following information for each server:

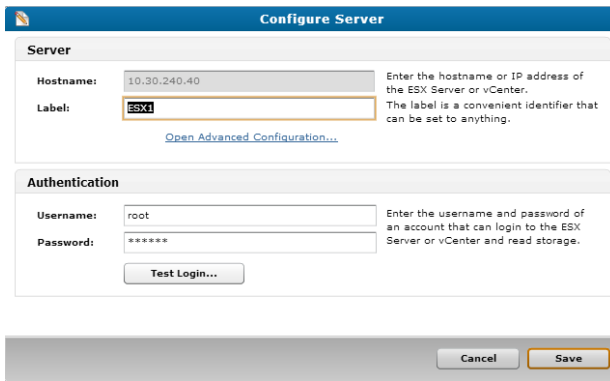
Column	Description
Label	The label assigned to the server.
Server	The server's IP address.
Ports	The server's ports.

4. Perform the following actions, as needed:

Edit a server

- a. In the **Actions** column, click to display the **Configure Server** dialog box.

Figure 95: Configure Server Dialog Box – Edit Server Mode

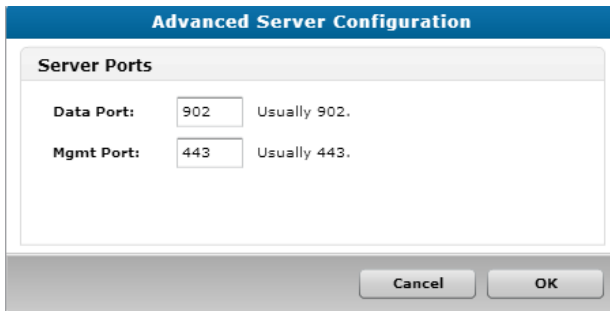


- b. In **Server** area's **Label** field, edit the label assigned to the server, as needed.

i Note: When you are editing a server, the **Hostname** field is view-only.


- c. In the **Server** area, click the **Open Advanced Configuration** link to display the **Advanced Server Configuration** dialog box.

Figure 96: Advanced Server Configuration Dialog Box



- d. In the **Data Port** and **Mgmt Port** fields, edit the server ports, as needed, and click **OK** to return to the **Configure Server** dialog box.
- e. In the **Authentication** area's **Username** and **Password** fields , edit the login credentials needed to access server read storage, as needed.
- f. In the **Authentication** area, click **Test Login** to verify that the login credentials work.
- g. Click **Save** to save updates and exit the dialog box.

Delete a server

- a. In the **Actions** column, click  to remove the server from the vmPRO appliance.
- b. At the prompt, confirm the deletion.

Add an ESX server

- a. Click **Add Server** to display the **Configure Server** dialog box.

Figure 97: Configure Server Dialog Box – Add Server Mode

The screenshot shows a dialog box titled "Configure Server". It is divided into two sections. The top section, "Server", contains two text input fields: "Hostname" (with a red border) and "Label". To the right of these fields are instructions: "Enter the hostname or IP address of the ESX Server or vCenter." and "The label is a convenient identifier that can be set to anything." Below the "Label" field is a blue link that says "Open Advanced Configuration...". The bottom section, "Authentication", contains two text input fields: "Username" (with "root" entered) and "Password". To the right of these fields are instructions: "Enter the username and password of an account that can login to the ESX Server or vCenter and read storage." Below the "Password" field is a button labeled "Test Login...". At the bottom of the dialog box are two buttons: "Cancel" and "Save".

- b. In the **Server** area's **Hostname** field, enter the host name or IP address to assign to the server.
- c. In the **Server** area's **Label** field, enter a label to assign to the server, as needed.
- d. In the **Server** area, click the **Open Advanced Configuration** link to display the **Advanced Server Configuration** dialog box.

Figure 98: Advanced Server Configuration Dialog Box

The screenshot shows a dialog box titled "Advanced Server Configuration". It has a section titled "Server Ports" which contains two text input fields: "Data Port" (with "902" entered) and "Mgmt Port" (with "443" entered). To the right of the "Data Port" field is the text "Usually 902." and to the right of the "Mgmt Port" field is the text "Usually 443.". At the bottom of the dialog box are two buttons: "Cancel" and "OK".

- e. In the **Data Port** and **Mgmt Port** fields, edit the server ports, as needed, and click **OK** to return to the **Configure Server** dialog box.
 - f. In the Authentication area's **Username** and **Password** fields, enter the login credentials needed to access server read storage.
 - g. In the **Authentication** area, click **Test Login** to verify that the login credentials work.
 - h. Click **Save** to save updates and exit the dialog box.
5. Click **OK** to save updates and exit the dialog box.

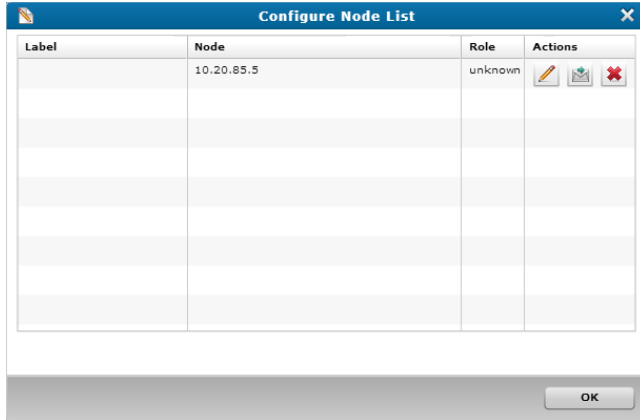
Nodes

From the **Resources** tab you can edit a node's label, email a notification regarding a node, or delete a node.

To manage nodes from the Resources tab

1. On the vmPRO appliance GUI, click the **VMs** button to display the **VMs** console.
2. Click the **Resources** tab, as needed.
3. In the **Nodes** pane, click **Configure** to display the **Configure Node List** dialog box.

Figure 99: Configure Node List Dialog Box



The dialog box displays the following information for each node:

Column	Description
Label	The label assigned to the node. A label allows you to easily identify nodes. You can enter any alphanumeric combination for a node label. If the node does not have a label, this field will be blank.
Node	The IP address assigned to the node.
Role	The role assigned to the node if the node is part of a group.

4. Perform the following actions, as needed:

Assign a label to a node


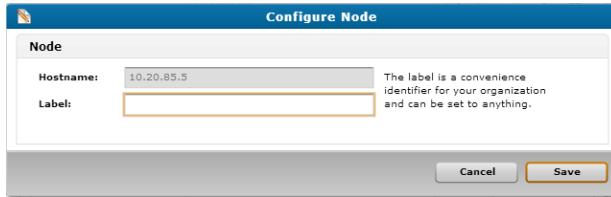

- a. In the **Actions** column, click  to display the **Configure Node** dialog box.

Figure 100: Configure Node Dialog Box




- b. In the **Label** field, enter a label to assign to the node.
- c. Click **Save** to save the node's label and return to the **Configure Node List** dialog box.

Email a notification

- In the **Actions** column, click .
- The node emails a report regarding its status, using the email settings configured on the **Configure Email** dialog box. See [Configuring Email for a vmPRO Appliance](#).

Delete a node

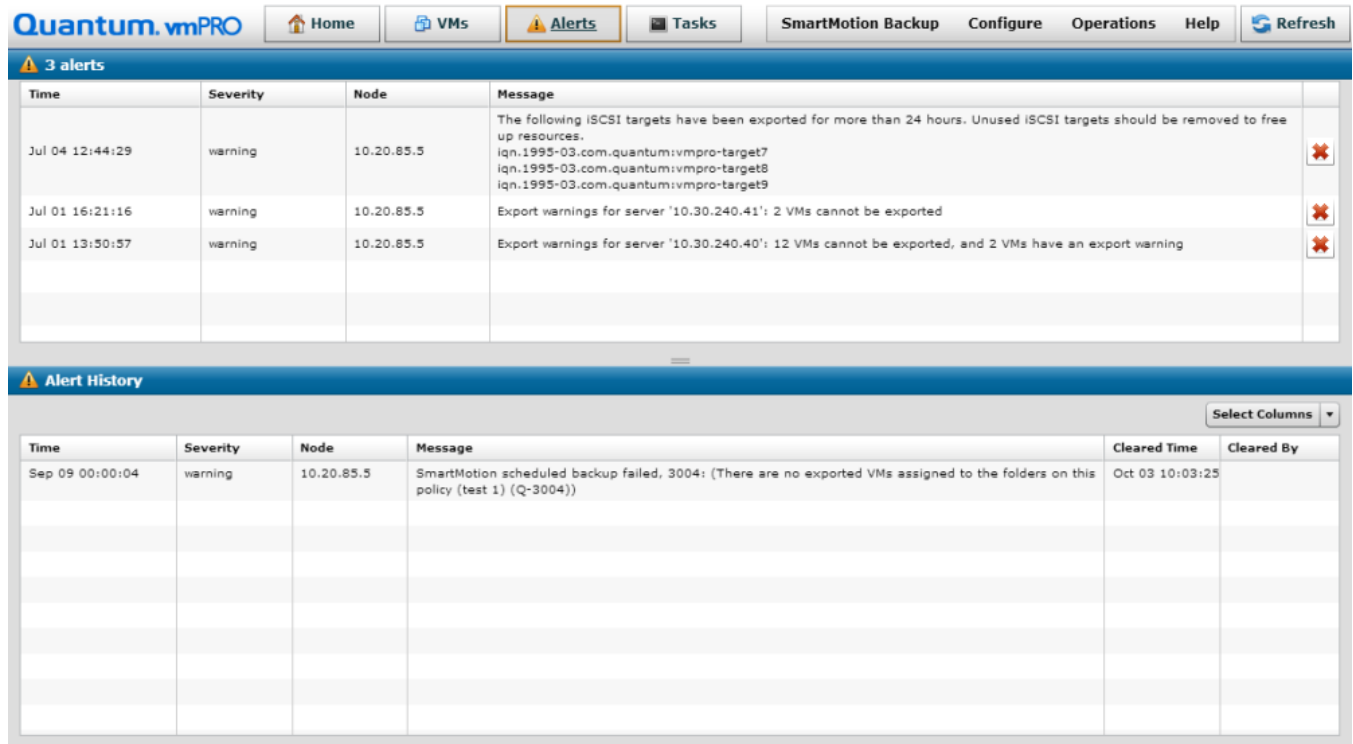
- a. In the **Actions** column, click .
 - b. At the prompt, confirm the deletion.
5. Click **OK** to save updates and exit the dialog box.

Navigating the vmPRO Alerts Console

Use the **Alerts** console on the vmPRO GUI to review and manage a list of current alerts.

After you have addressed an alert, you can delete it from the list of current alerts. Doing so moves the alert to an **Alert History** list, which you can use to determine when the alert was addressed, and by whom the alert was addressed.

Figure 101: Alerts Console



Navigate the vmPRO Alerts console

1. On the vmPRO appliance GUI, click the **Alerts** button to display the **Alerts** console.

The top pane displays the number of current alerts, and a list of each individual current alert, as follows:

Column	Description
Time	The date and time at which the alert was issued.
Severity	The severity of the alert, such as warning .
Node	The IP address for the node on which the alert occurred.
Message	A message indicating the reason for the alert.

2. When you have addressed an alert, click  to delete it from this pane and move it to the **Alert History** pane.

3. In the **Alert History** pane, review the following information:

Column	Description
Time	The date and time at which the alert was issued.
Severity	The severity of the alert, such as warning .
Node	The IP address for the node on which the alert occurred.
Message	A message indicating the reason for the alert.
Cleared Time	The date and time at which the alert was deleted from the current alert list.
Cleared By	The ID of the user who deleted the alert.

i Note: From the **Select Columns** drop-down list, you can select which columns display on the **Alert History** pane.

Navigating the vmPRO Tasks Console

Use the vmPRO **Tasks** console to manage SmartMotion™ Backup and Recovery tasks, as well as to view history for these tasks.

The following three tabs are located on the **Tasks** console.

Backup Tab

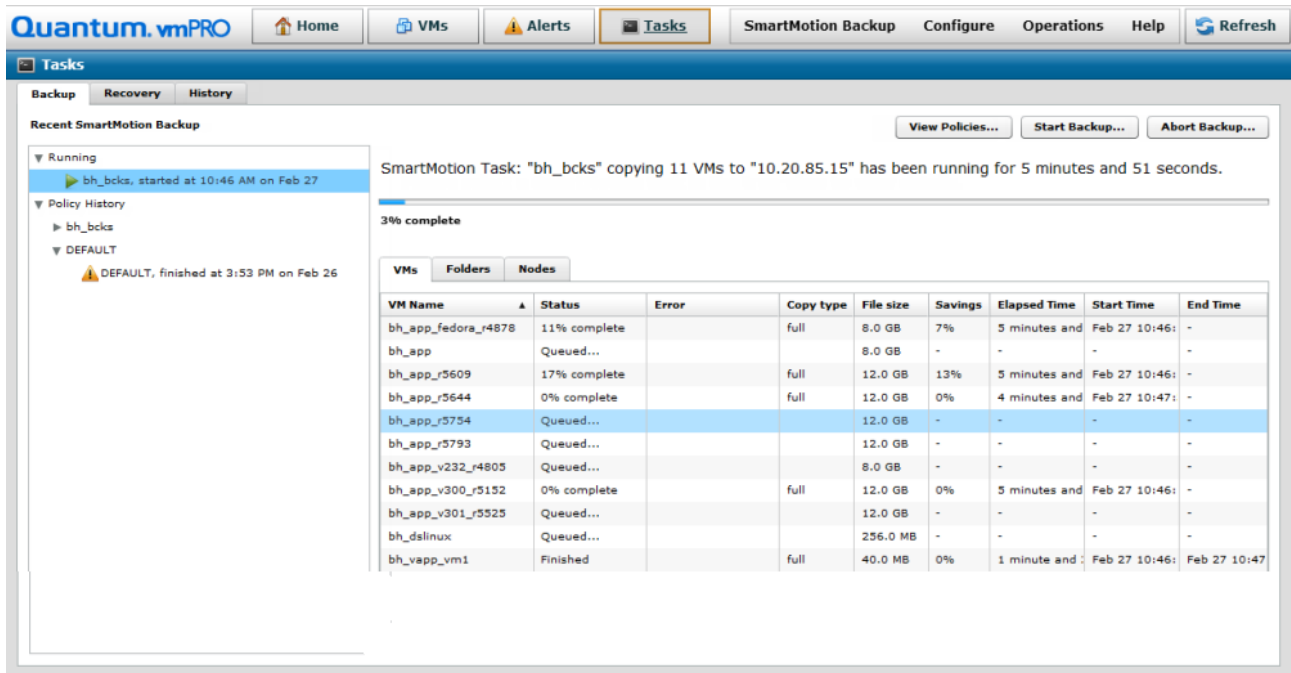
Use the **Tasks Console – Backup** tab to view and manage SmartMotion Backup tasks and policies.

Navigate the Backup tab on the Tasks console

1. On the vmPRO appliance GUI, click the **Tasks** button to display the **Tasks** console.

2. Click the **Backup** tab, as needed.

Figure 102: Tasks Console – Backup Tab



3. In the left pane, review a list of SmartMotion Backup tasks in the following drop-down lists:
 - **Running** – Currently running backup policy tasks.
 - **Policy History** – Completed backup policy tasks, sorted by folders.
4. Select a task for which to display the following details:

Note: Select the **VMs**, **Folders**, **Nodes**, or **Errors** tab, as needed. The **Errors** tab displays only when errors exist.

Tab	Column	Description
VMs	VM Name	The name of the backed-up virtual machine (VM).
	Status	The status of the backup task for the associated VM, such as Finished .
	Error	The number of errors that occurred for the backup task, if any.
	Copy type	The type of backup task for the associated VM, such as partial or full . For more information regarding partial or full backups, see vSphere Changed Block Tracking Support .
	File size	The amount of data that was backed up for the associated VM.
	Savings	The percentage of saved disk space for the associated VM and backup task.
	Elapsed Time	The amount of time that the backup task took for the associated VM.
	Start Time	The time at which the backup task began for the associated VM.
	End Time	The time at which the backup task ended for the associated VM.
Folders	Folder	The folder for which the backup task was run.
	Num VMs	The number of VMs within the folder that were included in the backup task.
	Status	The status of the backup task for the associated folder, such as Finished .
	Num Errors	The number of errors that occurred for the backup task, if any.

Tab	Column	Description
Nodes	Node	The node on which the backup task was run.
	Num VMs	The number of VMs on the node that were included in the backup task.
	Status	The status of the backup task on the associated node, such as Finished .
Error	VM Name	The name of the VM for which the backup error occurred.
	Error Message	The reason for the error.

5. Click the following buttons, as needed:

Button	Function
View Policies	Displays the Available Backup Policies dialog box. Use this dialog box to create a new policy, set a default policy, edit an existing policy, or delete a policy. See Creating SmartMotion Backup Policies .
Start Backup	Displays the Run SmartMotion Backup dialog box. Use this dialog box to start a SmartMotion Backup. See vmPRO SmartMotion Backup .
Abort Backup	Use to stop a selected SmartMotion Backup.

Recovery Tab

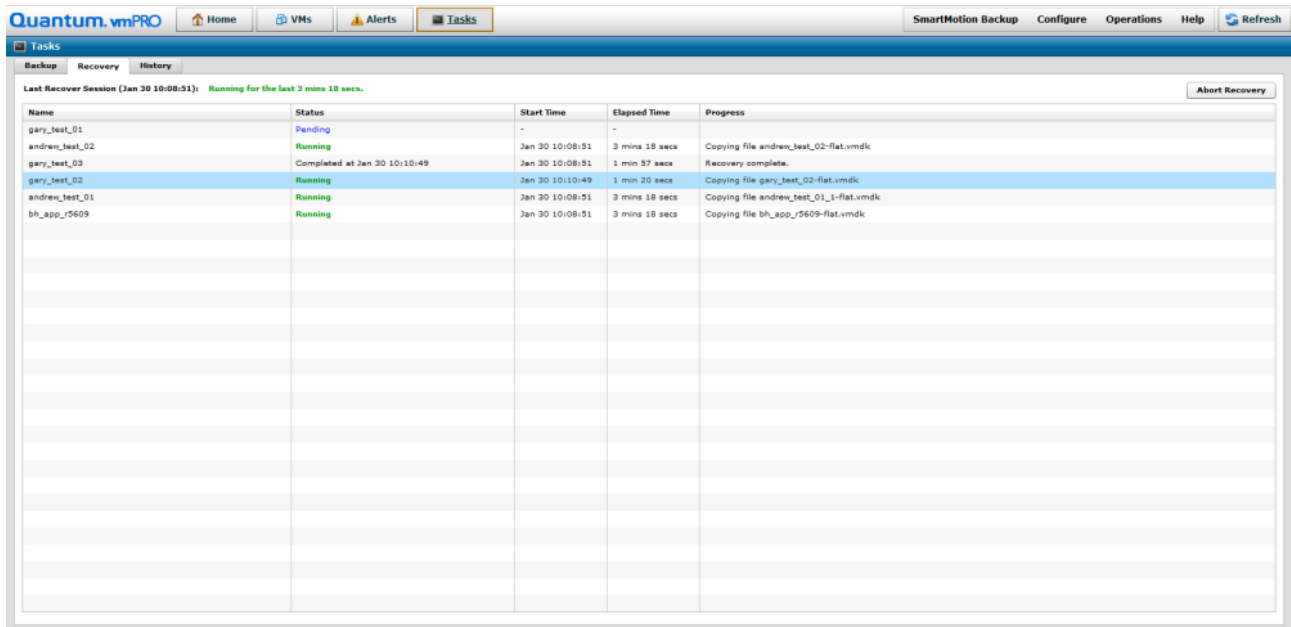
Use the **Tasks Console – Recovery** tab to manage SmartMotion Recovery tasks.

Navigate the Recovery tab on the Tasks console

1. On the vmPRO appliance GUI, click the **Tasks** button to display the **Tasks** console.

2. Click the **Recovery** tab, as needed.

Figure 103: Tasks Console – Recovery Tab



3. Review the following information for each VM that was included in the most recent SmartMotion Recovery:

Column	Description
Name	The name of the VM recovered during the recovery task.
Status	The status of the VM's recovery progress, such as Finished .
Start Time	The time at which the recovery task began on the associated VM.
Elapsed Time	The amount of time that the recovery task took for the associated VM.
Progress	The current progress of the recovery task for the associated VM.

Note: Click **Recover VMs** to start a SmartMotion Recovery task. See [vmPRO Data Recovery](#).

History Tab

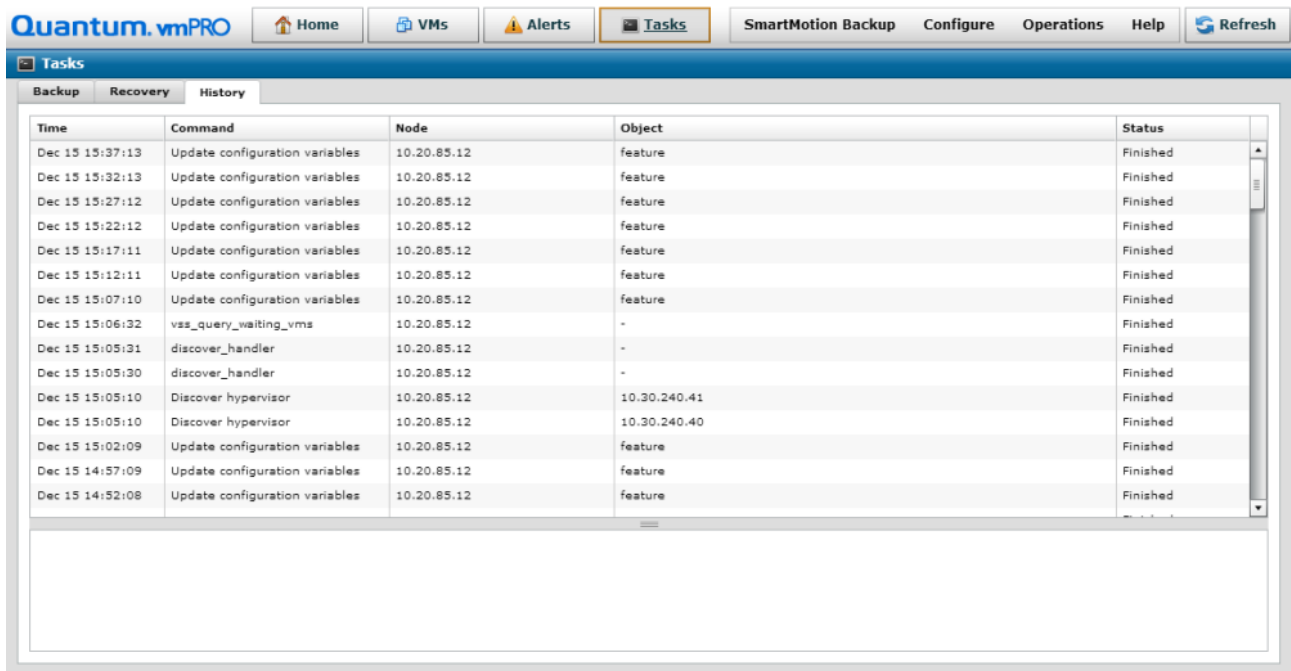
Use the **Tasks Console – History** tab to view a detailed list of tasks.

Navigate the History tab on the Tasks console

1. On the vmPRO appliance GUI, click the **Tasks** button to display the **Tasks** console.

2. Click the **History** tab, as needed.

Figure 104: Tasks Console – History Tab



3. Review the following information associated with each task:

Column	Description
Time	The date and time on which the task began.
Command	The description of the task, such as Discover hypervisor .
Node	The node on which the task occurred.
Object	The object on which the task was performed.
Status	The status of the task.



Chapter 4: vmPRO SmartMotion™ Backup

This chapter contains the following topics and sections:

vmPRO SmartMotion Backup	138
Manually Activating a SmartMotion Backup	141
vmPRO SmartMotion Backup Policies	142
Retention Schedules for SmartMotion Backups	143
Creating SmartMotion Backup Policies	146
Modifying SmartMotion Backup Policies	155

vmPRO SmartMotion Backup

The vmPRO SmartMotion™ Backup feature provides backup services for your vmPRO appliance by initiating a scheduled push of specified virtual machine disk (VMDK) files to any specified Network Attached Storage (NAS) target. The target can be resident on a plain NAS device or on a deduplication system, such as a Quantum DXi system.

Most SmartMotion backups run based on a schedule you set. In addition, you can manually activate a SmartMotion backup, as needed.

Prerequisites

Before you can use the SmartMotion Backup feature, you must first do the following:

Configure Servers and Discover VMs

Configure servers for your vmPRO appliance. The vmPRO appliance can then auto-discover all virtual machines (VMs) within the servers and display them on the VMs console. From the VMs console, you can select the VMs to export. SmartMotion can then back up data on the exported VMs to the NAS target.

VSAN

VMware's Virtual SAN (VSAN) is a cluster-wide resource that exists as datastores on a cluster of ESX servers. The vmPRO appliance manages VSAN through a vCenter server, which in turn manages the ESX servers housing the VSAN datastores. vmPRO supports backing up virtual machines (VMs) from VSAN datastores to NAS targets, as well as recovering VMs from the NAS targets back to VSAN datastores. In addition, you can use your vmPRO appliance to back up VMs from one type of datastore (VSAN or non-VSAN), and then recover the VMs to the other type of datastore.

Example

A VM backed up from a VSAN datastore can be recovered to a non-VSAN datastore.

In environments using VMware's Virtual SAN (VSAN) configuration, you must set up your vmPRO appliance to manage the configuration through a vCenter server, as opposed to managing individual ESX servers.

For information about configuring servers and discovering VMs, see [vmPRO Servers](#).

Set Up Folders and Groups

Set up folders within your vmPRO appliance to organize VMs for different backup needs, such as backing up VMs by type or location. In addition, you can use folders in conjunction with the Group Management feature to facilitate multiple backup policies on a single vmPRO appliance.

For more information about creating folders and groups for your vmPRO appliance, see [vmPRO Folders](#) and [vmPRO Group Configuration](#).

Configure Changed Block Tracking

Configure vSphere's Changed Block Tracking (CBT) feature to enable SmartMotion backups to complete faster.

CBT identifies the VMDK blocks that have changed since the last backup. SmartMotion uses this information to back up only the changed data on VMDKs, reducing network I/O and backup times.

For more information about configuring CBT, see [vSphere Changed Block Tracking Support](#).

Configure the Quantum VSS Writer

Configure the Quantum Volume Shadow Copy Service (VSS) Writer to perform VSS backups for Windows-based VMs on an Active Directory (AD) Domain Controller.

The VSS Writer prepares Windows for a VMware snapshot to back up the VM's data. It then automates a non-authoritative restore of the Windows AD Domain Controller when the VM is restored.

For more information about configuring the Quantum VSS Writer, see [Quantum VSS Writer](#).

Select VMs for Export

After your servers are configured and discovered, select the VMs to export.

- For ESX servers, you can select to export individual VMs or entire folders organizing the VMs.
- For vCenter servers, you can select individual VMs, entire folders organizing the VMs, or the entire vCenter server.

i Note: We do not recommend exporting entire vCenter servers because this type of export can exponentially increase backup times.

For more information about selecting VMs for export, see [Modifying VM Settings from the vmPRO Appliance](#) and [Configuring a vCenter Server for a vmPRO Appliance](#).

Set Up Storage

Set up NAS targets to which to back up data, such as a Quantum DXi appliance. This data is stored in the NAS device as a VM disk image. However, users cannot directly access this stored data. Instead, the vmPRO appliance communicates to the device over a CIFS or NFS protocol, both to store backed-up VM disk images and to recover the stored VM disk images. The vmPRO appliance presents the stored data to authorized users and machines in the **/export** and **/recover** directories as CIFS or NFS shares.

For more information about setting up NAS targets, see [Configuring NAS Targets for SmartMotion Backups](#).

Create Backup Policies

Create backup policies to direct SmartMotion backups. When you create a backup policy, you can specify the folders to be backed up, assign the NAS target for the backed-up data, set a schedule for the backup, and define a retention schedule for the backed-up data.

For more information about creating backup policies, see [vmPRO SmartMotion Backup Policies](#).

Additional Notes

Before using SmartMotion Backup, review the following information:

DXi V-Series Appliances

DXi V-Series appliances (such as DXi V1000 or DXi V4000) should not be backed up by a vmPRO

appliance. When a DXi V-Series appliance is managed by a vmPRO appliance, disable the DXi V-Series appliance from being exported. If you want to back up your DXi V-Series appliance, replicate it to another DXi appliance.

NAS Targets

If your NAS target is powered down or in a disconnected state, the vmPRO GUI times out. If you see messages or behavior to this effect, check the status of your NAS target. Proceed with a backup when the NAS target is behaving correctly.

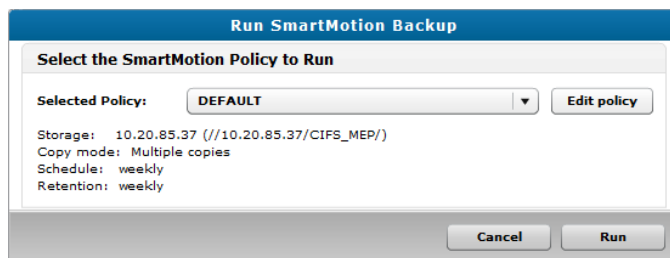
Additional Backup and Recovery Solutions

Quantum vmPRO can support your current backup and recovery solutions. For more information about using Quantum vmPRO with your current backup and recover solutions, see the product-specific technical notes on the Quantum Support site, and the online support article, [Using Quantum vmPRO with your backup solution](#).

Manually Activating a SmartMotion Backup

If you need to manually activate a SmartMotion™ backup, use the **Run SmartMotion Backup** dialog box. After initiating the backup, you can view the backup's progress and details from the **Backup** tab on the **Task** console. From this tab, you can also stop a SmartMotion backup. See [Navigating the vmPRO Tasks Console](#).

Figure 105: Run SmartMotion Backup Dialog Box



Manually activate a SmartMotion backup

1. From the **SmartMotion Backup** menu, select **Backup** to display the **Run SmartMotion Backup** dialog box.

2. In the **Selected Policy** field, select the appropriate backup policy to run.

Click **Edit policy** to display the **Configure SmartMotion Backup Policy** dialog box. Use this dialog box to edit the backup policy, as needed. See [Creating SmartMotion Backup Policies](#).

3. Click **Run** to run the SmartMotion backup.

4. From the **Task** console's **Backup** tab, view the progress of the SmartMotion backup. See [Navigating the vmPRO Tasks Console](#).

vmPRO SmartMotion Backup Policies

Create backup policies to direct SmartMotion™ Backups. You can create a single backup policy or multiple backup policies for a vmPRO appliance. Creating multiple backup policies allows for multiple backup and retention schedules, as well as the use of multiple storage targets.

After creating backup policies, you can define a default policy to use as a sample for creating future policies.

Considerations

Consider the following before creating backup policies:

Folders to Back Up

When your vmPRO appliance discovers a server, it creates a folder for that server and its associated virtual machines (VMs). You can configure additional folders to organize VMs based on backup needs, such as by geographic location.

Assign backup policies to folders and their associated VMs. Keep in mind that VMs can belong to only one folder at a time, but folders can have multiple backup policies assigned to them. A VM can be backed up multiple times with different backup policies.

Storage Targets

Select the storage target to which SmartMotion will back up the selected VMs. If needed, you can configure new storage targets or edit existing storage targets.

Backup policies are controlled by the vmPRO appliance for which they were created, regardless of storage targets.

Example

If vmPRO A and vmPRO B send data to the same storage target, the data exported by vmPRO A is backed up and retained based on backup policies configured for vmPRO A. This data is not affected by vmPRO B's backup and retention policies. The same applies for vmPRO B, where its backed-up

data is sent and retained by backup policies configured for vmPRO B, and not those configured for vmPRO A.

Backup and Retention Schedules

Each vmPRO appliance can have multiple backup policies, and each policy has its own schedule. However, a specific policy can run only once per day. In addition, in a group configuration, only two backup policies can run simultaneously for the master appliance and any of its nodes.

Retention schedules define both the amount of backed-up data to store and the amount of time for which to store the data on a Network Attached Storage (NAS) target. For information about setting retention schedules, see [Retention Schedules for SmartMotion Backups](#).

Configuration File Backup

Within a backup policy, you can select to back up an encrypted copy of the vmPRO appliance's current configuration file. This file contains all configuration data needed to restore the vmPRO appliance.

When SmartMotion backs up a vmPRO appliance's configuration file, it sends the file to the base directory of the NAS target. This base directory follows the hierarchy convention of **<Storage Sub-folder>\<YYY_MM>\<YYY_MM_DD_HHMMSS>**.

To restore the configuration file, use the Quantum vmPRO Configuration Save and Import feature. Access this feature, as well as the configuration file, from the vmPRO GUI to which you are restoring the vmPRO appliance's configuration. For more information about the Quantum vmPRO Configuration Save and Import feature, see [vmPRO GUI Menus](#).

Retention Schedules for SmartMotion Backups

Retention schedules define both the amount of backed-up data to store, and the amount of time for which to store the data on a Network Attached Storage (NAS) target. You can define retention schedules when you configure SmartMotion™ backup policies.

Retention schedules apply only when multiple copies of a virtual machine (VM) are backed up. Single copies of backed-up VMs are stored indefinitely.

Important Concepts

Review the following before defining new retention schedules for currently running backup policies.

Daily Retention Schedules

If you define a new daily retention schedule for a backup policy, all data backed up through this policy –

both before and after the retention schedule is defined – is deleted at the defined daily interval. If you do not want to delete data backed up prior to defining the retention schedule, define a weekly or monthly retention schedule instead. Weekly and monthly schedules only apply to backups completed after the change to the policy's retention schedule.

Weekly and Monthly Retention Schedules

Weekly and monthly retention schedules only affect backups that occur after the schedule is defined for the policy. Data backed up before a policy's weekly or monthly retention schedule is defined remains in the NAS target.

Multiple Retention Schedules

You can set SmartMotion backup and retention schedules to run daily, weekly, monthly, annually, or on any combination of those intervals.

When setting multiple schedules, keep the following in mind:

- Backups occur for the shortest interval of time defined.
- All retention schedules are followed.

Example

You schedule a backup policy to run both daily and weekly. The actual backups occur every day because that is the shorter of the two defined intervals.

The daily schedule's retention is set for 8 days, and the weekly schedule's retention is set for 5 weeks with Sunday being the day on which to retain backup data. The vmPRO appliance backs up data every day, and it deletes data every 8 days, excluding data backed up on the last 5 Sundays. This data is retained for 5 Sundays due to the weekly retention schedule.

Figure 106: Retention Schedule Example

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
BU	BU	BU	BU	BU	BU	BU
BU/Delete	BU	BU	BU	BU	BU	BU
BU	BU/Delete	BU	BU	BU	BU	BU
BU	BU	BU/Delete	BU	BU	BU	BU
BU	BU	BU	BU/Delete	BU	BU	BU
BU	BU	BU	BU	BU/Delete	BU	BU

BU = Daily Backups
 BU = Deleted Backups
 Delete = Day on which 8 previous backups are deleted, with the exception of the first 5 Sundays

i Note: When you run a manual backup, it is treated like a daily backup for retention purposes. For example, if you run a manual backup on a day when there is not a backup policy scheduled, the backup is saved as a daily backup and the daily retention schedule is applied to it.

NAS Targets and Retention Schedules

When setting a retention schedule, consider the type of NAS target to which you are backing up data:

Deduplicating NAS Targets

DXi systems and deduplicating NAS targets generally achieve a 10:1 to 20:1 reduction in aggregate backup volume, enabling greater retention periods than with comparably sized non-deduplicating storage devices. Full and Differential/Changed Block Tracking (CBT) backups impact storage usage by approximately the same amount as deduplication for the NAS target.

Non-Deduplicating Storage Targets

Non-deduplicating NAS targets consume disk space more rapidly than their comparably sized deduplicating counterparts. Full and Differential/CBT backups impact these storage targets differently. CBT backups generally reduce a backup by 15%-30%, depending on your environment.

Regardless of the type of NAS target, the biggest factor to consider in setting a retention schedule is the rate at which the VMs generate unique data blocks. VMs generating more unique data blocks use more storage. Until you can observe the capacity growth rate, we recommend setting a short retention schedule, retaining data for only 7 to 14 days.

Creating SmartMotion Backup Policies

Create backup policies to direct SmartMotion™ backups. You can create either a single backup policy or multiple backup policies for a vmPRO appliance. Creating multiple backup policies allows for multiple backup and retention schedules, as well as the use of multiple storage targets.

Before creating backup policies for your vmPRO appliance, we recommend reviewing the considerations outlined in [vmPRO SmartMotion Backup Policies](#) and [Retention Schedules for SmartMotion Backups](#).

Access the Configure SmartMotion Backup Policy dialog box

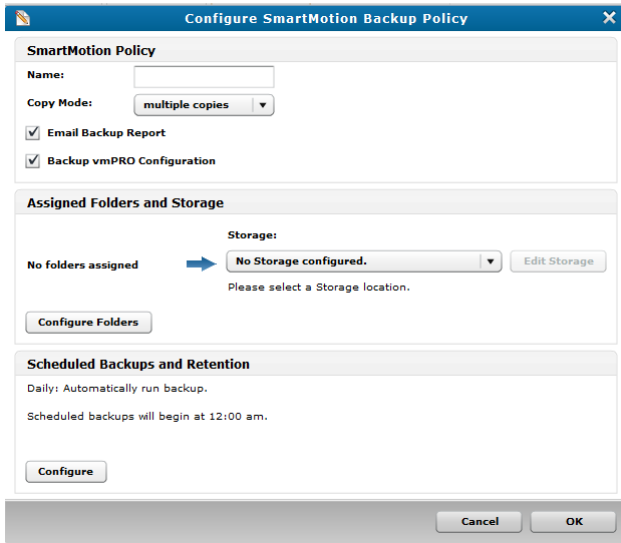
- Do one of the following:
 - a. From the **Tasks** tab, click **View Policies** to display the **Available Backup Policies** dialog box.
 - b. Click **Create a new policy** to display the **Configure SmartMotion Backup Policy** dialog box.
- Or**
- a. From the **SmartMotion Backup** menu, select **Backup Policies** to display the **Available Backup Policies** dialog box.
- b. Click **Create a new policy** to display the **Configure SmartMotion Backup Policy** dialog box.

Figure 107: Available Backup Policies Dialog Box

Name	Storage	Schedule	Start Time	Retention	Actions
*DEFAULT	<Not Configured>	Not scheduled		Not configured	
MEP_1	10.20.85.9 (10.20.85)	Not scheduled		Not configured	

Buttons:

Figure 108: Configure SmartMotion Backup Policy Dialog Box



Create a backup policy

1. Display the **Configure SmartMotion Backup Policy** dialog box.
2. In the **SmartMotion Policy** pane, do the following:

Field/Check Box	Action
Name	Enter a name to assign to the backup policy for easy identification.
Copy Mode	Select one of the following options for the drop-down list: <ul style="list-style-type: none"> • multiple copies – Save multiple copies of a virtual machine (VM). Retention schedules are applied to the multiple VM copies. See Retention Schedules for SmartMotion Backups. • one copy – Save just one copy of a VM. Retention schedules do not apply to this option because only one backup copy exists.
Email Backup Report	Select this check box to email a Backup Report to the recipients identified on the Reports & Alerts dialog box or Report & Alert Configuration page. See Configuring Reports, Alerts, and Autosupport for a vmPRO Appliance .
Backup vmPRO Configuration	Select this check box to back up a copy of the vmPRO appliance's configuration file. See vmPRO SmartMotion Backup Policies .

- In the **Assigned Folders and Storage** pane, do the following:

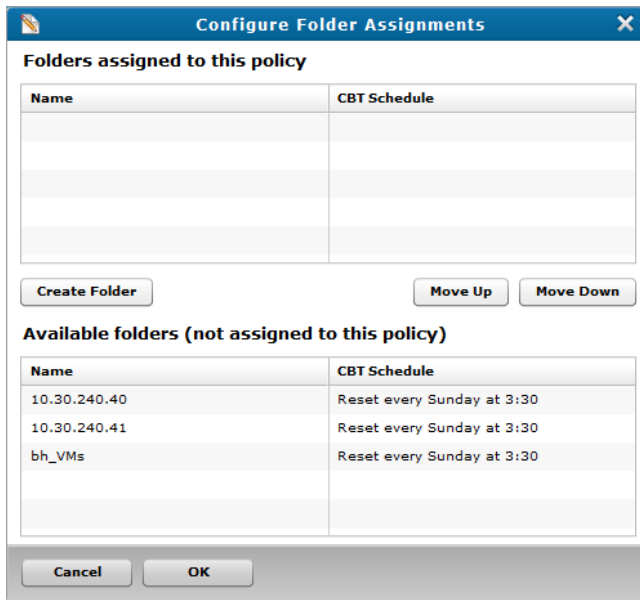
Field/Button	Action
Storage	Select one of the following options from the drop-down list: <ul style="list-style-type: none"> A storage target in which to store backed-up data. If needed, click Edit Storage to edit the storage target's settings. Create new Storage to create a new storage target to which to back up data. See Configuring NAS Targets for SmartMotion Backups .
Configure Folders	Click the button to display the Configure Folder Assignments dialog box. Use this dialog box to assign the backup policy to folders. See below.

- In the **Scheduled Backups and Retention** pane, click **Configure** to display the **Configure Backup Schedules and Retention** dialog box. Use this dialog box to set backup and retention schedules. See below.
- Click **OK** to save the policy and exit the dialog box.

Assign a backup policy to folders

- Display the **Configure Folder Assignments** dialog box.

Figure 109: Configure Folder Assignments Dialog Box



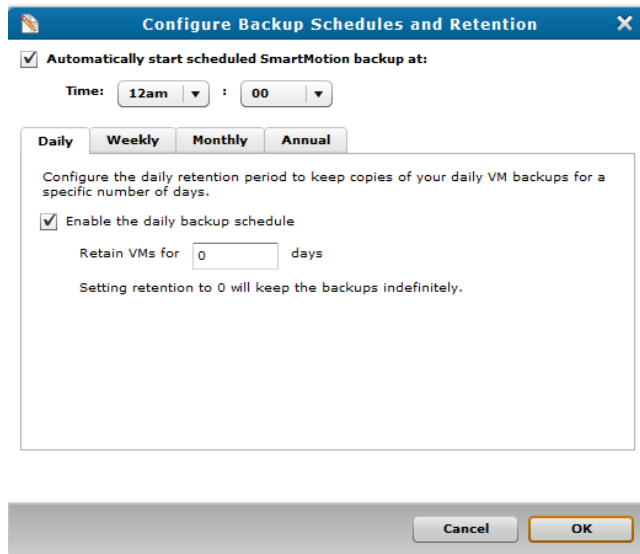
- In the **Available folders (not assigned to this policy)** list, select a folder to which to assign the backup policy.
- Click **Move Up** to move the folder to the **Folders assigned to this policy** list.

4. Do the following, as needed:
 - To remove a folder from the **Folders assigned to this policy** list, select the folder and click **Move Down**. The folder is moved to the **Available folders (not assigned to this policy)** list.
 - To create a new folder, click **Create Folder** to display the **Configure Folder** dialog box. Use this dialog box to create new folders to which to assign the backup policy. See [Configuring vmPRO Folders](#).
5. Click **OK** to save folder assignments and return to the **Configure SmartMotion Backup Policy** dialog box.

Set backup and retention schedules

1. Display the **Configure Backup Schedules and Retention** dialog box.

Figure 110: Configure Backup Schedules and Retention Dialog Box



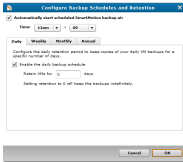
2. Set the time at which to automatically run the SmartMotion backup by doing the following:
 - a. Select the **Automatically start scheduled SmartMotion backup at** check box.
 - b. In the **Time** field's drop-down lists, select the hour and minute values at which to begin the backup.

3. Do the following to define your backup and retention schedule intervals.

Time Interval	Steps
---------------	-------

Daily

Figure 111: Daily Tab



- a. Select the **Daily** tab to run backups and retain data on a daily basis.
- b. Select the **Enable the daily backup schedule** check box to activate your backup and retention schedule.
- c. In the **Retain VMs for X days** field, enter the number of days for which to retain backed-up data. After the indicated number of days passes, the backed-up data is deleted from the storage target.

Example

In the **Retain VMs for X days** field, you enter **10**. The backup runs daily at the indicated time, retaining all stored data in the storage target for 10 days. After 10 days, the backed-up data is deleted from the storage target. The backup and retention schedule continues on this 10-day interval.

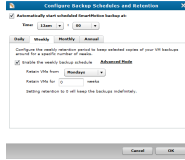
Caution: If you define a new daily retention schedule for a backup policy, all data backed up through this policy – both before and after the retention schedule is defined – is deleted at the interval you have defined. If you do not want to delete data backed up prior to defining the retention schedule, define a weekly or monthly retention schedule instead. Weekly and monthly schedules apply only to backups completed after the change to the policy's retention schedule.

Time Interval

Steps

Weekly – Basic Mode

Figure 112: Weekly Tab – Basic Mode



- Select the **Weekly** tab to run backups and retain data on a weekly basis.
- Select the **Enable the weekly backup schedule** check box to activate your backup and retention schedule.
- In the **Retain VMs from** field, select the day of the week on which both to run your backup and to delete retained files.
- In the **Retain VMs for X weeks** field, enter the number of weeks for which to retain backed-up data. After the indicated number of weeks, the backed-up data is deleted from the storage target.

Example

- In the **Retain VMs from** field, you select **Monday**.
- In the **Retain VM for X weeks** field, you enter **6**.

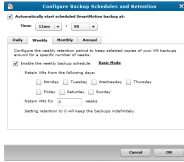
The backup runs every week on Monday at the indicated time, retaining all stored data for 6 weeks. After 6 weeks, the backed-up data is deleted from the storage target. The backup and retention schedule continues on this 6-week interval.

- i Note:** Weekly retention schedules only affect backups that occur after the schedule is defined for the policy. Data backed up before a policy's weekly retention schedule is defined remains in the NAS target.

Time Interval	Steps
---------------	-------

Weekly – Advanced Mode

Figure 113: Weekly Tab – Advanced Mode



- Select the **Weekly** tab to run backups and retain data on a weekly basis.
- Select the **Enable the weekly backup schedule** check box to activate your backup and retention schedule.
- Click the **Advanced Mode** link to display the **Advanced Mode** view.
- In the **Retain VMs from the following days** field, select each day of the week on which both to run the backup and for which to retain stored data.
- In the **Retain VMs for X weeks** field, enter the number of weeks for which to retain backed-up data. After the indicated number of weeks, the backed-up data is deleted from the storage target.

Example

- In the **Retain VMs from the following days** field, you select **Monday** and **Friday**.
- In the **Retain VMs for X weeks** field, you enter **6**.

The backup runs every week on both Mondays and Fridays, retaining all stored data for 6 weeks. After 6 Mondays, the backed-up data is deleted from the storage target, with the exception of the last 6 Friday backups. After 6 Fridays, the backed-up data is deleted from the storage target, with the exception of the last Monday backup.

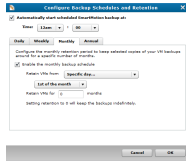
i Note: Weekly retention schedules only affect backups that occur after the schedule is defined for the policy. Data backed up before a policy's weekly retention schedule is defined remains in the NAS target.

Time Interval

Steps

Monthly

Figure 114: Monthly Tab



- a. Select the **Monthly** tab to run backups and retain data on a monthly basis.
- b. Select the **Enable the monthly backup schedule** check box to activate your backup and retention schedule.
- c. In the **Retain VMs from** field, select one of the following:
 - **Specific day** – Use to define a specific day of the month on which to run backups and begin the retention period. In the subsequent drop-down list, select the specific day of the month.
 - **The first backup of the month** – Use to begin the retention period on the first backup of the month.
 - **The last backup of the month** – Use to begin the retention period on the last backup of the month.
- d. In the **Retain VMs for X months** field, enter the number of months for which to retain backed-up data. After the indicated number of months, the backed-up data is deleted from the storage target.



Caution: A monthly backup is scheduled only if you select the **Specific day** option. Use **The first backup of the month** and **last backup of the month** options to define retention policies only, and then schedule backups to run daily or weekly.

Example

- You select **The last backup of the month**.
- In the **Retain VMs for X months** field, you enter **3**.
- You schedule backups to run weekly on Fridays.

The backup runs every week on Fridays, retaining all stored data for 3 months. After 3 months of backups, the backed-up data is deleted from the storage target, with the exception of the last Friday backup of the month. The backup and retention schedules continue, backing up data every Friday and deleting stored data every 3 months before the last Friday of the month.



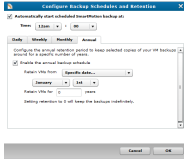
Note: Monthly retention schedules only affect backups that occur after the schedule is defined for the policy. Data backed up before a policy's monthly retention schedule is defined remains in the NAS target.

Time Interval

Steps

Annually

Figure 115: Annual Tab



- Select the **Annual** tab to run backups and retain data on an annual basis.
- Select the **Enable the annual backup schedule** check box to activate your backup and retention schedule.
- In the **Retain VMs from** field, select one of the following:
 - Specific date** – Use to define a specific date on which to run backups and begin the retention period. In the subsequent drop-down lists, select the specific month and day.
 - The first backup of the year** – Use to begin the retention period on the first backup of the year.
 - The last backup of the year** – Use to begin the retention period on the last backup of the year.
 - Caution:** An annual backup is scheduled only if you select the **Specific date** option. Use **The first backup of the year** and **last backup of the year** options to define retention policies only, and then schedule backups to run daily or weekly.
- In the **Retain VMs for X years** field, enter the number of years for which to retain backed-up data. After the indicated number of years, the backed-up data is deleted from the storage target.

Example

- You select **The last backup of the year**.
- In the **Retain VMs for X years** field, you enter **1**.
- You schedule backups to run weekly on Fridays.

The backup runs every week on Fridays, retaining all stored data for 1 year. After 1 year of backups, the backed-up data is deleted from the storage target, with the exception of the last Friday backup of the year. The backup and retention schedules continue, backing up data every Friday and deleting stored data every year before the last Friday of the year.

Note: Setting any retention period to zero will keep backed-up data indefinitely.

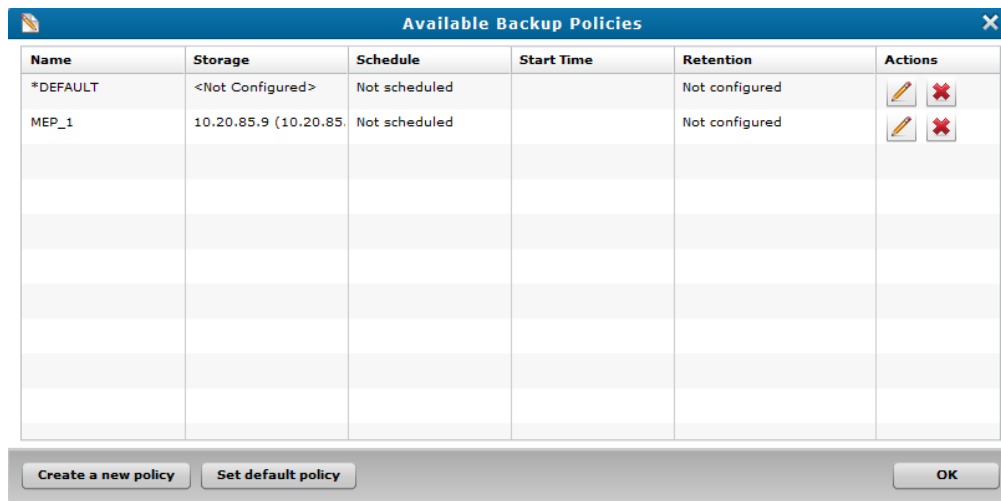
- Click **OK** to save your backup and retention schedules and return to the **Configure SmartMotion Backup Policy** dialog box.

Modifying SmartMotion Backup Policies

Use the **Available Backup Policies** dialog box to modify an existing SmartMotion™ backup policy by doing any of the following:

- Designate a backup policy as the default backup policy.
- Edit a backup policy's configuration settings.
- Delete a backup policy from the vmPRO appliance.

Figure 116: Available Backup Policies Dialog Box



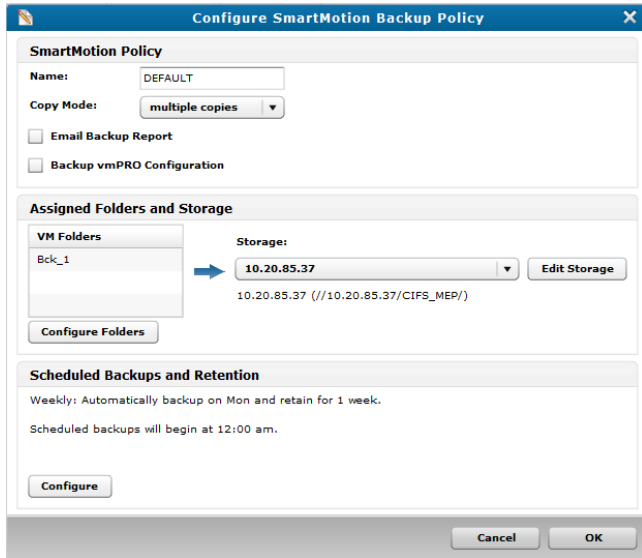
Designate a Default Backup Policy

1. From the **SmartMotion Backup** menu, select **Backup Policies** to display the **Available Backup Policies** dialog box.
2. Select the policy to set as your default backup policy, and click **Set default policy**.
The vmPRO appliance assigns the default status to the policy, and places an asterisk (*) next to it in the **Name** column.
3. Click **OK** to save settings and exit the dialog box.

Edit a backup policy's configuration settings

1. From the **SmartMotion Backup** menu, select **Backup Policies** to display the **Available Backup Policies** dialog box.
2. Select the policy to edit, and click to display the **Configure SmartMotion Backup Policy** dialog box in edit mode.


Figure 117: Configure SmartMotion Backup Policy – Edit Mode



Note: The **Configure SmartMotion Backup Policy** dialog box in edit mode includes a table displaying the VM folder assignments for the existing backup policy. Otherwise, the dialog box and steps taken to edit the policy are the same as when creating a backup policy.

3. Edit the policy's configuration settings, as needed. See [Creating SmartMotion Backup Policies](#).

Delete a backup policy from the vmPRO appliance

1. From the **SmartMotion Backup** menu, select **Backup Policies** to display the **Available Backup Policies** dialog box.
2. Select the policy to delete from the vmPRO appliance, and click  to display the **Confirm delete** popup box.
3. Click **Yes** to confirm the deletion and remove the policy from the vmPRO appliance.



Chapter 5: vmPRO Data Recovery

This chapter contains the following topics and sections:

vmPRO Data Recovery	157
Recovering Virtual Machines	159
Recovering VMs Backed Up with a Third-Party Application	169
Manually Registering a Recovered VM	172
Preparing for Exchange Recovery	174
Recovering Mailboxes on an Exchange Server	180
Manually Cleaning Up the Exchange Server	188
iSCSI Export and Recovery	193
Recovering VM Disks Using iSCSI	195
Individual File Recovery	201
Recovering Individual Files	202

vmPRO Data Recovery

Use the vmPRO **Recover Virtual Machines Wizard** to recover data.

When you recover data, the vmPRO appliance places the data in target datastores. We recommend that before recovering data, you verify that the target datastores have enough available space for the recovered data. The vmPRO appliance does not warn you if there is not enough space on a target datastore before executing a batch operation. Define the target datastores to which to recover data in the wizard.

The wizard supports the following data recovery options.

Virtual Machine (VM) Recovery

Use this feature to recover VMs to an ESX or vCenter server. When you recover VMs, you can select to have the vmPRO appliance automatically register the VMs with the server, or you can manually register the VMs with the server. By registering VMs with the server, you are adding them as new VMs to the server's inventory.

You can recover VMs backed up with SmartMotion™, and VMs backed up by a third-party application. The only difference between the two recovery processes is how the vmPRO appliance accesses the VMs to recover.

Topics

[Recovering Virtual Machines](#)

[Recovering VMs Backed Up with a Third-Party Application](#)

[Manually Registering a Recovered VM](#)

Exchange Recovery

Use this feature to recover mailboxes on an Exchange server. The vmPRO appliance exports and mounts backup disk images of an Exchange server virtual machine (VM) to a target iSCSI disk. The iSCSI target then pushes the disk images to a mailbox on a target Exchange server, where you can access the recovered mailbox.

Before using the Exchange Recovery feature, you need to set up both your vmPRO appliance and your system. After the vmPRO appliance completes the Exchange Recovery process, it initiates an automatic Exchange server cleanup. You can manually perform this process, if needed.

Topics

[Preparing For Exchange Recovery](#)

[Recovering Mailboxes on an Exchange Server](#)

[Manually Cleaning Up the Exchange Server](#)

iSCSI Export and Recovery

Use this feature to recover your backed-up data as disk images from a Windows-based virtual machine (VM) or physical machine.

With the iSCSI Export and Recovery feature, your vmPRO appliance works with the Windows iSCSI Initiator to capture the VM's file system as a disk image. On the same Windows system from which the iSCSI Initiator is running, you can mount the VM disk image (VMDK) to access the files within the VM.

Topics

[iSCSI Export and Recovery](#)

[Recovering VM Disks Using iSCSI](#)

Recovering Individual Files

Using the vmPRO SmartView feature, you can recover individual files within exported virtual machines (VMs). This process is separate from the VM recovery process. You can access and recover individual files within the exported VMs by mounting CIFS shares to your local system.

You can recover individual files from a mounted CIFS share only. This feature does not support NFS shares. You can access the share from either Windows or Unix/Linux systems.

Topics

[Individual File Recovery](#)

[Recovering Individual Files](#)

VSAN

vmPRO supports backing up virtual machines (VMs) from VSAN datastores to Network Attached Storage (NAS) targets, as well as recovering VMs from the NAS targets back to VSAN datastores. In addition, you can use your vmPRO appliance to back up VMs from one type of datastore (VSAN or non-VSAN), and then recover VMs to the other type of datastore.

Example

A VM backed up from a VSAN datastore can be recovered to a non-VSAN datastore.

Note: In environments using VMware's Virtual SAN (VSAN) configuration, you must set up your vmPRO appliance to manage the configuration through a vCenter server, rather than managing individual ESX servers. See [vmPRO Servers](#).

Recovering Virtual Machines

Use the vmPRO **Recover Virtual Machines Wizard** to recover virtual machines (VMs).

Considerations

Selecting VMs to Recover

From the wizard, you can easily select to recover VMs backed up with SmartMotion™. To recover VMs backed up with a third-party application, you need to create a staging area from which the vmPRO appliance can access the VM. See [Recovering VMs Backed Up with a Third-Party Application](#).

Recovering One or Multiple VMs

You can recover either one or multiple VMs at a time. Whichever option you choose, you need to define the backup date from which to recover the data, and a configuration to use in restoring the VMs and associated disks and files.

Viewing Recovery Status

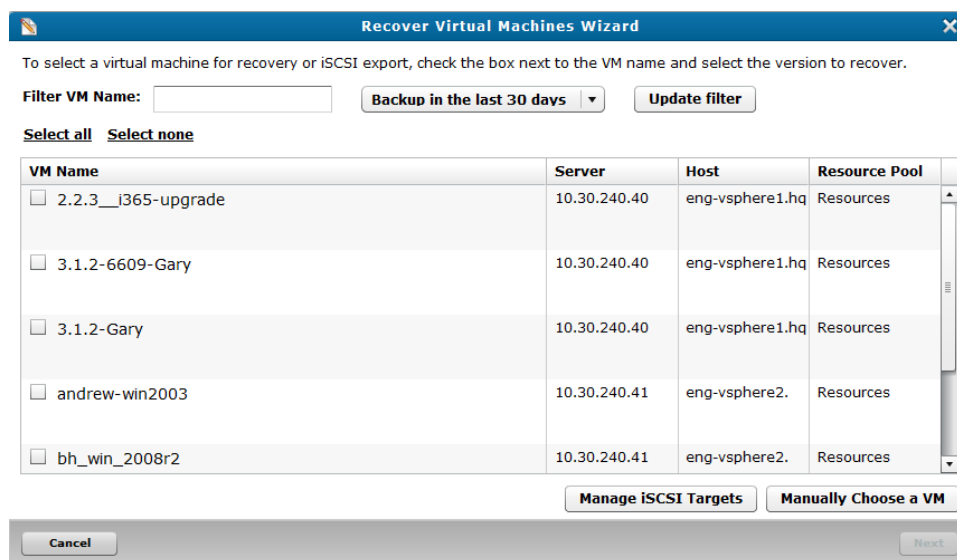
Both during and after the recovery process, you can use the **Tasks** console to view the progress of the recovery. See [Navigating the vmPRO Tasks Console](#).

Note: If you are recovering a VM with both Active Directory (AD) and VSS enabled, the VSS restore process reboots the VM twice. These reboots can take several minutes. During this time, we recommend that you do not attempt to use the VM.

Recover VMs backed up with SmartMotion

1. From the **SmartMotion Backup** menu, select **Recover** to display the **Recover Virtual Machines Wizard**.

Figure 118: Recover Virtual Machines Wizard



2. As needed, filter the list of VMs from which to select by doing the following:
 - In the **Filter VM Name** field, enter the name of the VM to recover.
 - In the **Backup in the last xx days** drop-down list, select to display VMs that have been backed up in the last 30 or 60 days, or select to display all backup history.
 - Click **Update filter** to update the list of VMs based on the filter criteria.
3. Select the VMs to recover by doing one of the following:
 - Click **Select All** to recover all displayed VMs.
 - Select the check box next to each VM to recover.

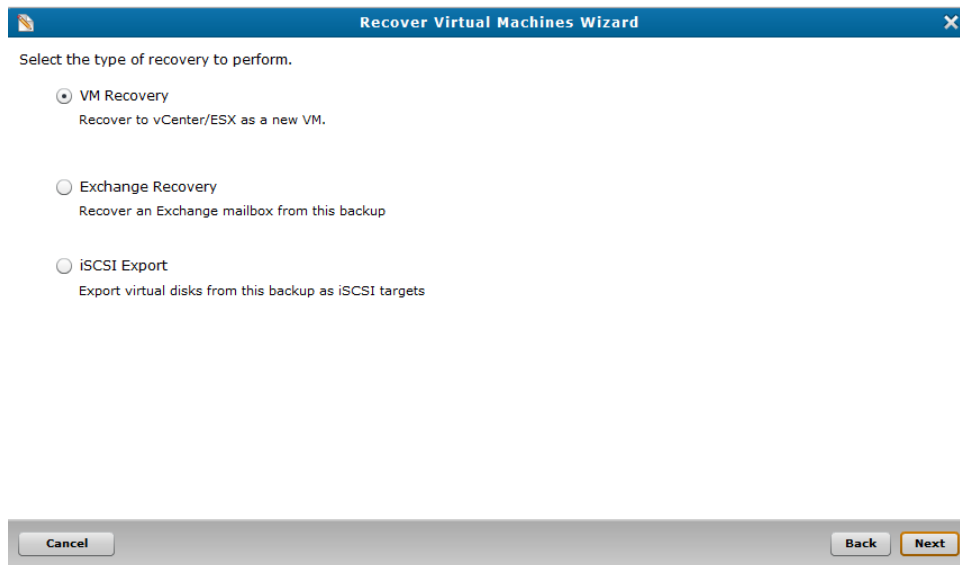
i Note: Click **Select none** to clear all current selections.

4. In the **Recover from** drop-down list for each selected VM, select the date and time of the backup from which to recover data.

i Note: If you are performing a recovery using iSCSI, click **Manage iSCSI Targets** to display the **iSCSI Targets** dialog box. Use this dialog box to view your current iSCSI targets, as well as to remove iSCSI targets you no longer need. See [Manually Cleaning Up the Exchange Server](#).

5. Click **Next** to display the **Select the type of recovery to perform** page.

Figure 119: Select the type of recovery to perform Page



6. Select **VM Recovery** to recover the selected VMs as new VMs on the appropriate vCenter or ESX server.
7. Click **Next**.

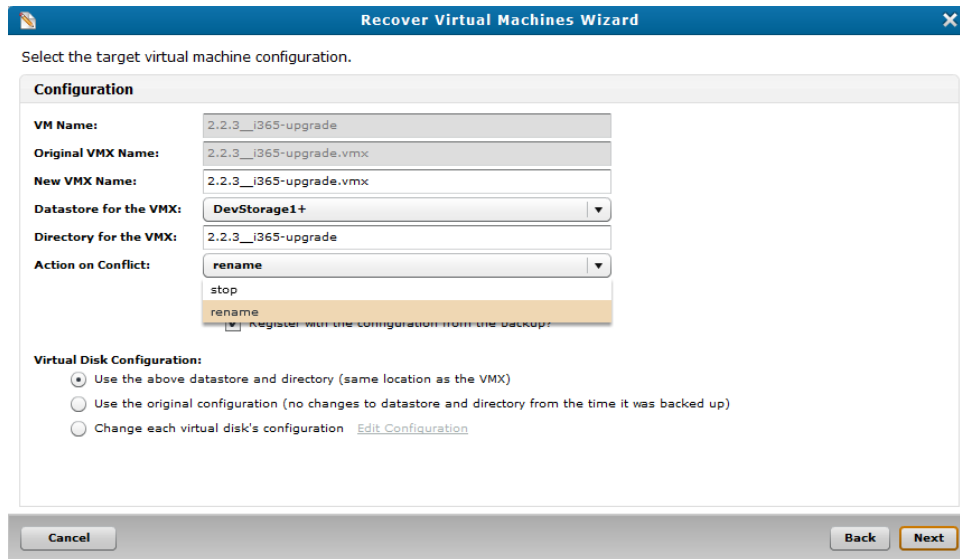
- Depending on whether you are recovering a single VM or multiple VMs, use one of the following tasks to complete VM recovery.

Recover a single VM

- On the **Select the type of recovery to perform** page, select **VM Recovery** to display the **Select a target virtual machine configuration** page.

The page displays the name of the VM selected for recovery, as well as the original name of the VM's configuration file.

Figure 120: Select a target virtual machine configuration Page



- Populate the following fields and check boxes, as needed:

Field/Check Box	Description
New VMX Name	The name of the VM's configuration file. Enter a new name for the configuration file, or keep the original name for the file.
Datastore for the VMX	The datastore to which to recover the VM's configuration file. Select a target datastore from the drop-down list.
Directory for the VMX	The directory in which to place the VM's configuration file. Enter a new directory, or keep the original directory structure for the file.

Field/Check Box	Description
Action on Conflict	<p>Select one of the following options if a VM name or directory name conflict occurs during the VM recovery:</p> <ul style="list-style-type: none"> • stop – The vmPRO appliance stops the recovery process. You will need to rename either the original VM/directory or the VM/directory being recovered, and then restart the recovery process. • rename – The vmPRO appliance continues the recovery process, and registers the recovered VM with a new name, using the following convention: <VM_name> (1). If <VM_name> (1) exists, the appliance uses the next sequential number, such as <VM_name> (2). The vmPRO appliance uses this same convention in renaming a duplicate directory.
Add the VM to vSphere/ESX inventory after restore	<p>Select to automatically add the VM to the vSphere or ESX server's inventory.</p> <p>If the VM is not originally from a vCenter or ESX server, or if you want to manually register the VM with a different server, clear this check box.</p>
Register with the configuration from the backup	<p>If you selected to automatically add the VM to the server's inventory, select if you want to register the VM to the same location from which it was backed up.</p> <p>If the VM is not originally from a vCenter or ESX server, or if you want to manually register the VM with a different server, clear this check box.</p>

3. In the **Virtual Disk Configuration** field, select one of the following options:

Virtual Disk Configuration	Description
Use the above datastore and directory	Recovers the VM with the configuration defined in the fields above.
Use the original configuration	Recovers the VM with its original configuration.

Virtual Disk Configuration	Description
<p>Change each virtual disk's configuration</p>	<p>Customize each disk's configuration on the VM.</p> <ol style="list-style-type: none"> Click the Edit Configuration link to display the Virtual Disk Configuration dialog box. In the Virtual Disk Number drop-down list, select the disk number for which to configure settings. In the Target Disk Name field, edit the name assigned to the disk, as needed. In the Target Datastore drop-down list, select the datastore to which to recover the disk. In the Target Directory field, enter the directory in which to place the disk. In the Disk Provisioning drop-down list, select the provision type to assign to the disk, either thick or thin. Click Save to save updates and return to the previous page.

4. Click **Next** to display the **Verify the configuration of the VM to be restored** page.

Figure 121: Verify the configuration of the VM to be restored Page

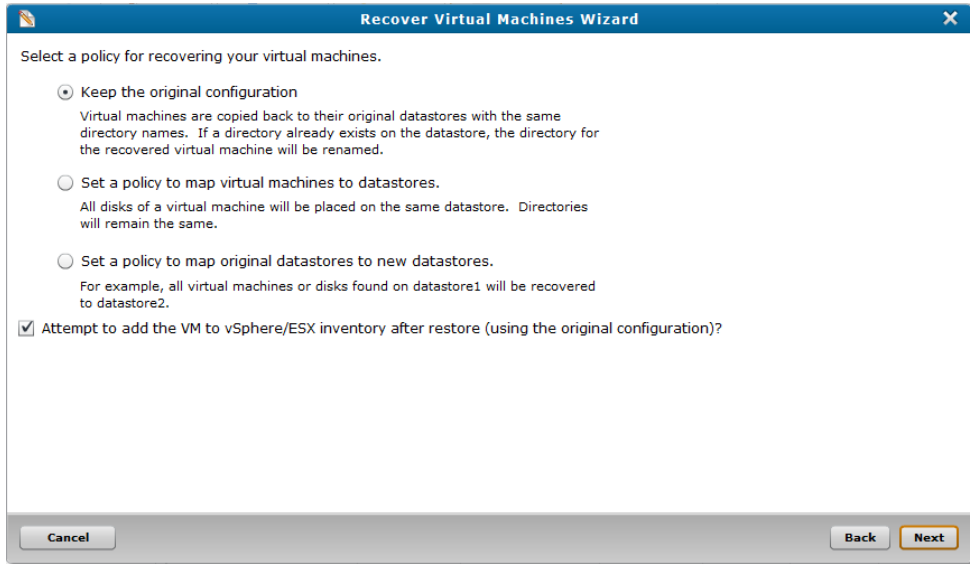


5. Review the recovery settings, and click **Start** to begin the recovery.

Recover multiple VMs

1. On the **Select the type of recovery to perform** page, select **VM Recovery** to display the **Select a policy for recovering your virtual machines** page.

Figure 122: Select a policy for recovering your virtual machines Page



2. Select one of the following recovery policy options:

Recovery Policy Option	Description
Keep the original configuration	The vmPRO appliance recovers the VMs to their original datastores, following the original directory structure. If the original directory still exists on the datastore, the vmPRO appliance renames the directory in which the recovered VMs are placed. Example <ul style="list-style-type: none">You want to recover all VMs to their original Datastore A, using the original directory_xyz.The vmPRO appliance recovers the VMs to Datastore A, but directory_xyz is still intact on the datastore.The vmPRO appliance creates directory_xyz_1 on Datastore A, and places the recovered VMs in this renamed directory.

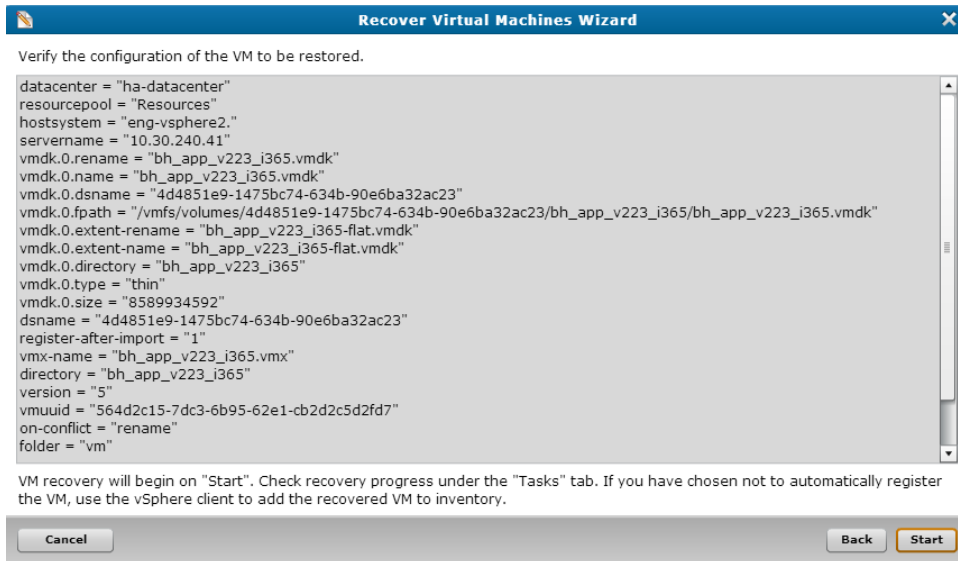
Recovery Policy Option	Description
Set a policy to map virtual machines to datastores	<p>The vmPRO appliance recovers the VMs to datastores that you define on the Configure policy mappings page. This page displays when you click Next. See below.</p> <p>The vmPRO appliance uses the recovered VMs' original directory structure.</p> <div data-bbox="678 472 1458 802"><p>Example</p><ul style="list-style-type: none">• You define Datastore B as the recovery target for VMs 1, 2, and 3.• VMs 1, 2, and 3 originally resided on Datastore A in directory_xyz.• The vmPRO appliance recovers VMs 1, 2, and 3 to Datastore B, creating directory_xyz for the recovered VMs.</div>
Set a policy to map original datastores to new datastores	<p>The vmPRO appliance recovers all VMs, files, and disks from one datastore to another datastore that you define on the Configure policy mappings page. This page displays when you click Next. See below.</p> <div data-bbox="678 997 1458 1276"><p>Example</p><ul style="list-style-type: none">• You define a policy to recover all VMs, files, and disks originally on Datastore A to Datastore B.• The vmPRO appliance uses this recovery policy and recovers VMs, files, and disks originally on Datastore A to Datastore B.</div>

3. Select the **Attempt to add the VMs to vSphere/ESX inventory after restore (using the original configuration)?** check box to register the recovered VMs to the appropriate server's inventory.

i Note: If you select this option, we recommend removing the original VMs from the server before restoring them. The vmPRO appliance does not rename the restored VMs, which could cause identification issues if you have both the original and restored VMs with the same name on the server.

4. Click **Next** to display the **Verify the configuration of the VM to be restored** page.

Figure 123: Verify the configuration of the VM to be restoredPage



5. Review the recovery settings, and click **Start** to begin the recovery.

Configure policy mappings

1. On the **Select a policy for recovering your virtual machines** page, select either **Set a policy to map virtual machines to datastores** or **Set a policy to map original datastores to new datastores**.

2. Click **Next** to display the **Configure** policy mappings page.

Figure 124: Configure policy mappings Page – Set a policy to map virtual machines to datastores Option

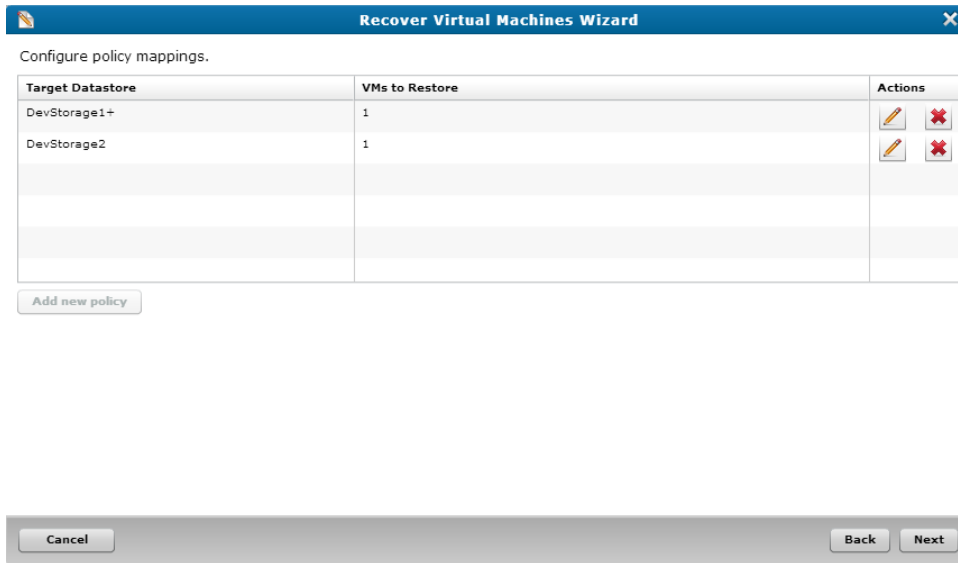
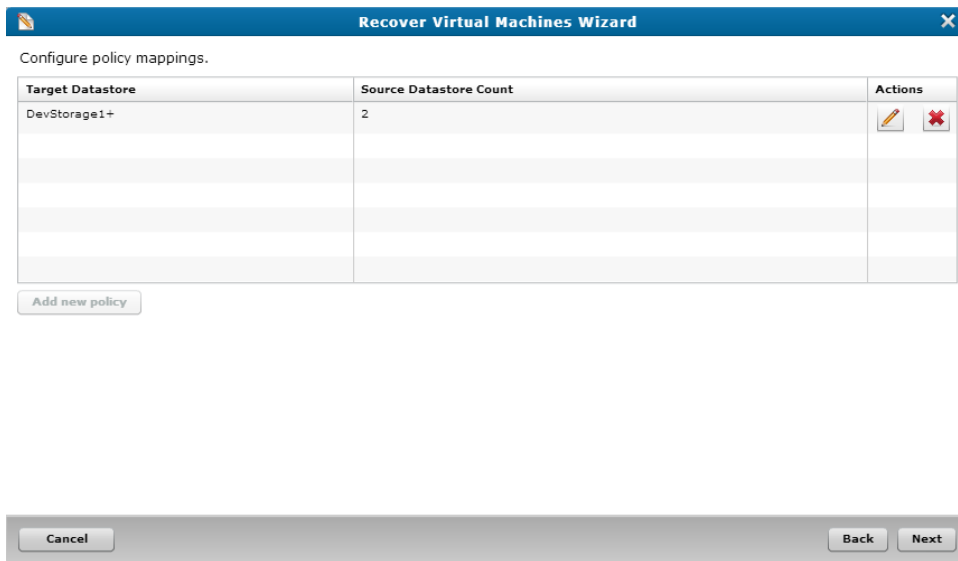


Figure 125: Configure policy mappings Page – Set a policy to map original datastores to new datastores Option



3. Depending on which option you selected, do the following to configure your restore policy:

Set a policy to map virtual machines to datastores

- a. Click **Add new policy** to display the **Configure Target Datastore** dialog box.
- b. In the **Target Datastore** drop-down list, select the datastore to which to recover the VMs.

- c. In the **VMs to recover to the target datastore** list, select each VM to recover to the selected datastore.
- d. Click **Save** to save updates and return to the **Configure policy mappings** dialog box with your new mappings displayed.
- e. Click **Next** to display the **Confirm your recovery configuration** page.
- f. Review the recovery settings, and click **Start** to begin the recovery.

Set a policy to map original datastores to new datastores

- a. Click **Add new policy** to display the **Configure Target Datastore** dialog box.
- b. In the **Target Datastore** drop-down list, select the datastore to which to recover the VMs.
- c. In the **Datastores to map to the target datastore** list, select each datastore to recover to the selected datastore.
- d. Click **Save** to save updates and return to the **Configure policy mappings** dialog box with your new mappings displayed.
- e. Click **Next** to display the **Confirm your recovery configuration** page.
- f. Review the recovery settings, and click **Start** to begin the recovery.

Recovering VMs Backed Up with a Third-Party Application

You can use the vmPRO **Recover Virtual Machines Wizard** to recover virtual machines (VMs) backed up with a third-party application.

-
- i Note:** If you are recovering a VM with both Active Directory (AD) and VSS enabled, the VSS restore process reboots the VM twice. These reboots can take several minutes. During this time, we recommend that you do not attempt to use the VM. See [Quantum VSS Writer](#)

Considerations

- Before using the wizard, restore the VM using your third-party application.
- Create a staging area from which the vmPRO appliance can access the VM.
- After recovering a VM backed up with a third-party application, manually delete the files from your staging area.

Create a staging area from which the vmPRO appliance can access the VM

1. Create the staging area in which to place the VM by doing one of the following:

If the vmPRO appliance can access the location to which you restored the VM

Use the restore location as your staging area.

If the vmPRO appliance cannot access the location to which you restored the VM

Create a staging area on a host other than your vmPRO appliance. You can create a staging area on any Network Attached Storage (NAS) device that is accessible to both the third-party application and the vmPRO appliance.

2. Ensure that the directory in which the VM is located is in the staging area, along with the following files:

Note: The VM's directory should have the same name as the VM.

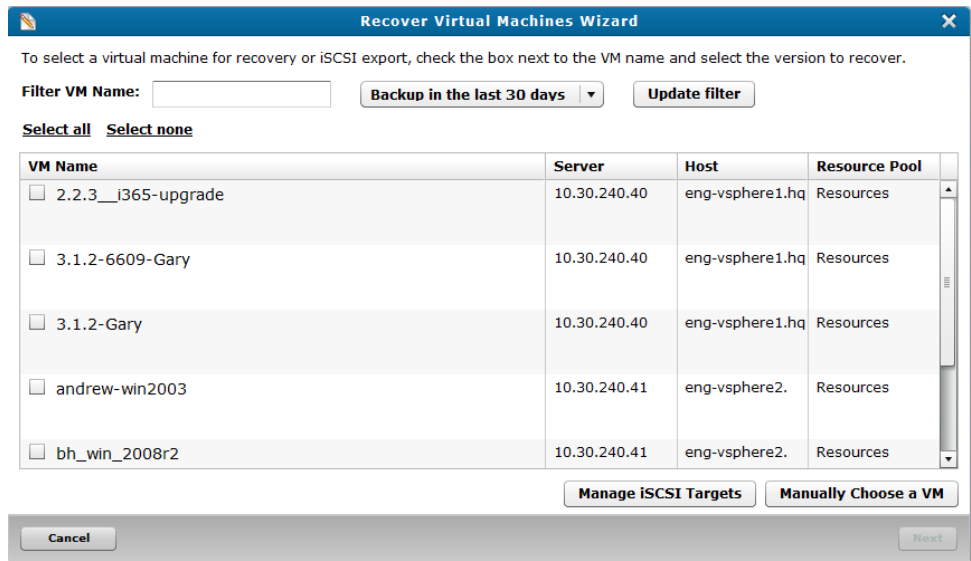
File	Description
<VM name>-flat.vmdk	The full base disk image.
<VM name>-pancvt.vmdk	If you use Changed Block Tracking (CBT), the file containing the changed blocks since the last full disk image was written. You should have the latest of these files for each flat file. See vSphere Changed Block Tracking Support .
<VM name>-.vmx	The VM's configuration file.

3. Add the staging area to the vmPRO appliance as additional storage to allow the **Recover Virtual Machines Wizard** to access the staging area. See [Configuring NAS Targets for SmartMotion Backups](#).

Recover a VM backed up with a third-party application

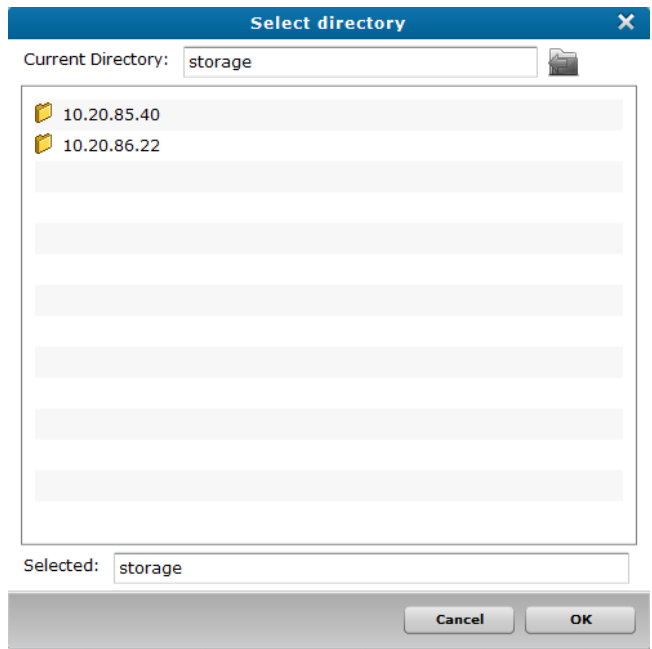
1. From the **SmartMotion Backup** menu, select **Recover** to display the **Recover Virtual Machines Wizard**.

Figure 126: Recover Virtual Machines Wizard



2. Click **Manually Choose a VM** to display the **Select directory** dialog box.

Figure 127: Select directory Dialog Box



3. Double-click the appropriate storage location, and then the appropriate folder, until the list of VMs displays.
4. Select the VM(s) to recover, and click **OK** to return to the **Recover Virtual Machines Wizard**.

5. To complete the recovery process, proceed with [step 5](#) from the [Recover VMs Backed Up with SmartMotion](#) task in the [Recovering Virtual Machines](#) topic.

Manually Registering a Recovered VM

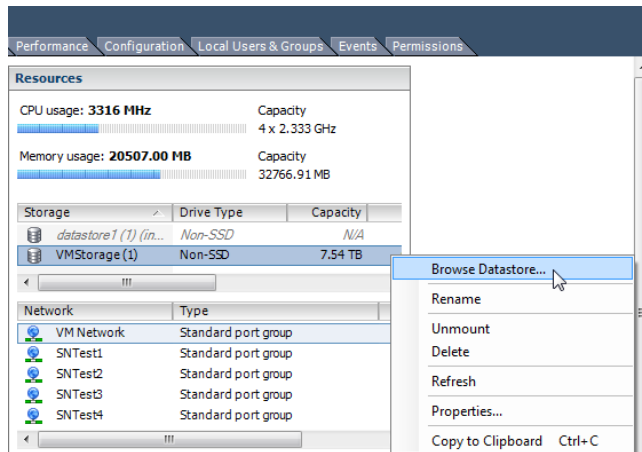
You must manually register a recovered virtual machine (VM) if you did not select to automatically add it to a server's inventory during recovery.

When the VM is registered with a server, it is added to the server's inventory and automatically discovered by the vmPRO appliance. In addition, the VM is automatically exported if you have **Automatically export new VMs enabled** on the VMs Console. See [Navigating the vmPRO VMs Console](#).

Manually register a recovered VM using the vSphere Client

1. Using a vSphere Client, log in to the ESX or vCenter server where the VM resides.
2. In the left pane, select the server to which to add the VM.
3. Click the **Summary** tab to display the server's general and resource information.
4. In the **Resources** pane, right-click the storage location of the recovered VM and select **Browse Datastore** to display the **Datastore Browser** dialog box.

Figure 128: Resources Pane – Storage Location

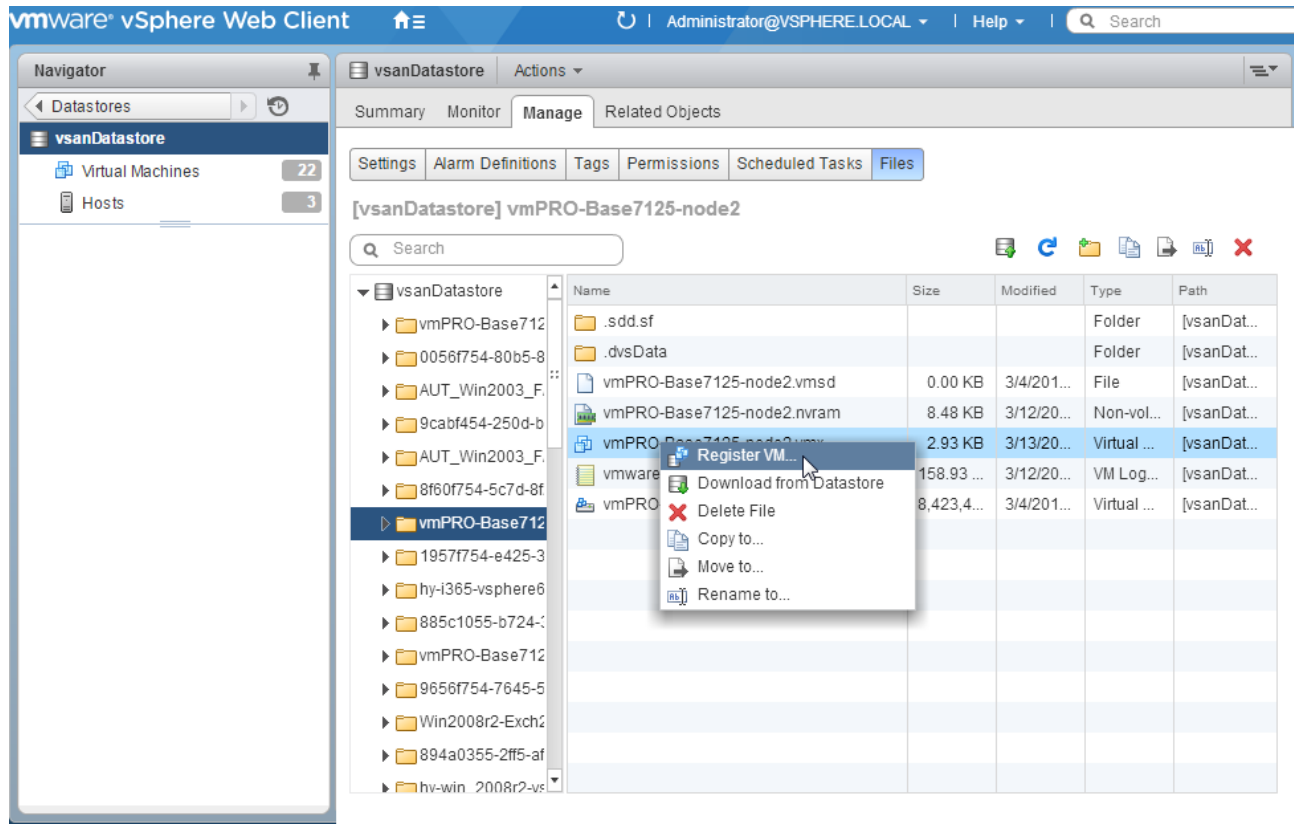


5. Locate and open the VM directory that was created during the recovery process.
6. Right-click the **.vmx** file, and select **Add to Inventory** to display the **Add to Inventory** wizard.
7. In the **Name** field, edit the name of the VM, as needed, and click **Next** to display the **Resource Pool** page.
8. In the **Resource Pool** pane, select the location in which to place the VM.
9. Click **Next** to display the **Ready to Complete** page, and click **Finish** to add the VM to the server's inventory.

Manually register a recovered VM using the vSphere Web Client

1. Open a vSphere Web Client.
2. From **vCenter Inventory Lists**, select **Datastores** to display a list of datastores.
3. Select the datastore to which to add the VM.
4. Locate and open the VM directory that was created during the recovery process.

Figure 129: Datastore Files List



5. Right-click the **.vmx** file, and select **Register VM** to display the **Register Virtual Machine** wizard.
6. In the **Name** field, edit the name of the VM, as needed.
7. In the **Select inventory location** list, select the folder in which to place the registered VM.
8. Click **Next** to display the **Host/Cluster** page.
9. In the displayed list, select the host or cluster on which to run the VM.
10. Click **Next** to display the **Resource Pool** page.
11. In the displayed list, select the resource pool in which to run the VM.

12. Click **Next** to display the **Ready to Complete** page, and click **Finish** to add the VM to the server's inventory.

Preparing for Exchange Recovery

Before using the vmPRO Exchange Recovery feature, make sure that the following prerequisites are met.

Prerequisites

Ensure that the following prerequisites are met before using Exchange Recovery:

Exchange Management Shell

You must have a working Exchange Management Shell to successfully recover mailboxes on an Exchange server.

Microsoft Exchange

You must have one of the following versions of Microsoft Exchange for mailbox recovery:

- Windows 2008R2/Exchange 2010
- Windows 2008R2/Exchange 2013
- Windows 2012R2/Exchange 2013

For systems that use Microsoft Exchange servers running Windows 2008R2 and Exchange 2010, the Windows Management Framework 3.0 must be installed.

Target iSCSI Disk

The vmPRO Exchange Recovery feature exports and mounts backup disk images of an Exchange server virtual machine (VM) to a target iSCSI disk.

Mapping eth0 to the iSCSI IP Address

The vmPRO appliance accesses the target iSCSI disk using the eth0 network path, which VMware tools automatically map to the iSCSI IP address. Ensure that eth0 is mapped to the iSCSI IP address. You will specify the iSCSI target in the wizard.

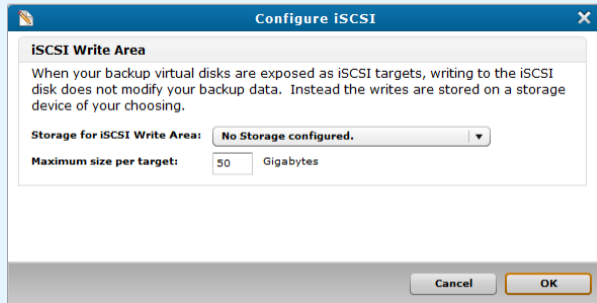
iSCSI Write Area Settings

In addition, the iSCSI target stores the recovered disk images of the Exchange server VM in its write area. This write area is separate from the area that the iSCSI target uses to store backed-up disk images. You must configure each iSCSI target's write area by specifying the amount of space to reserve for the recovered disk images.

Configure an iSCSI target's write area settings

1. From the **Configure** menu, select **iSCSI** to display the **Configure iSCSI** dialog box.

Figure 130: Configure iSCSI Dialog Box



2. In the **Storage for iSCSI Write Area** drop-down list, select the target iSCSI to which to recover Exchange server disk images, or select **Create new Storage** to configure an iSCSI storage target. See [Configuring NAS Targets for SmartMotion Backups](#).
3. In the **Maximum size per target** field, enter the amount of space to reserve for the recovered disk images in gigabytes.
4. Click **OK** to save changes and exit the dialog box.

Target Exchange Server

The iSCSI target pushes the recovered mailboxes to a mailbox on a target Exchange server. Make sure that the target mailbox has enough available space for the recovered mailbox. Otherwise, the Exchange Recover will fail.

You will specify the target Exchange server from the wizard.

Quantum VSS Agent

The vmPRO Exchange Recovery feature performs best when the Quantum VSS agent performs the backup of mailboxes on an Exchange server. To enable the Quantum VSS Agent, see [Quantum VSS Writer](#).

Note: You must use version 1.3 or higher of the Quantum VSS agent.

Adding the Exchange Server to the Organization Management Domain Group

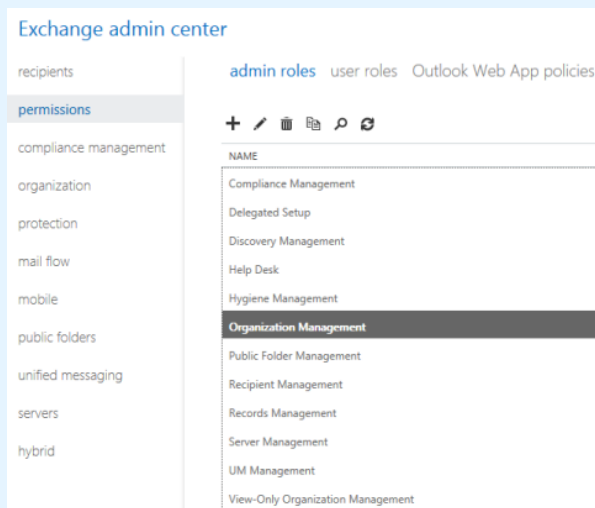
When using the Quantum VSS agent to perform the backup of mailboxes on an Exchange server, add the Exchange server to the Organization Management domain group within Microsoft Exchange. Adding the Exchange server to the domain group enables the Quantum VSS agent to capture the mailbox database information during a backup. Then during the recovery of an Exchange server's mailboxes, the vmPRO can access the mailbox database information located on the backed-up Exchange server.

If you do not add the Exchange server to the domain group, you must manually locate the mailbox databases to recover by browsing to the Exchange server's database .edb file and corresponding transaction log directory.

Add an Exchange server to the Organization Management domain group for Microsoft Exchange 2013

1. In a local browser, enter **https://<Exchange Server IP Address>/ecp/default.aspx** to access the **Exchange admin center** page for Microsoft Exchange 2013.
2. Select the **Permissions** tab, and then select the **admin roles** tab.

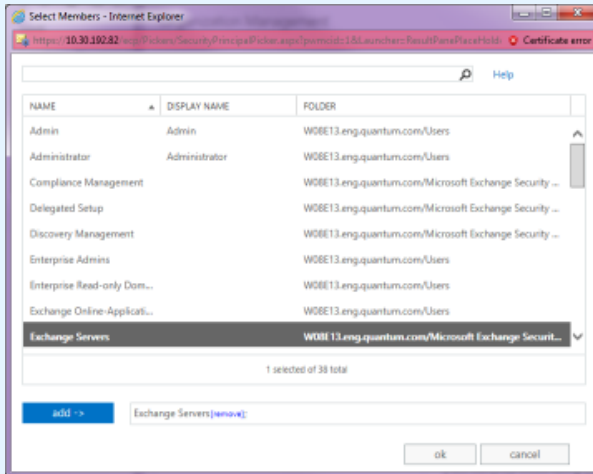
Figure 131: Exchange admin center – admin roles Tab



3. Double-click **Organization Management** to display the **Role Group** window.

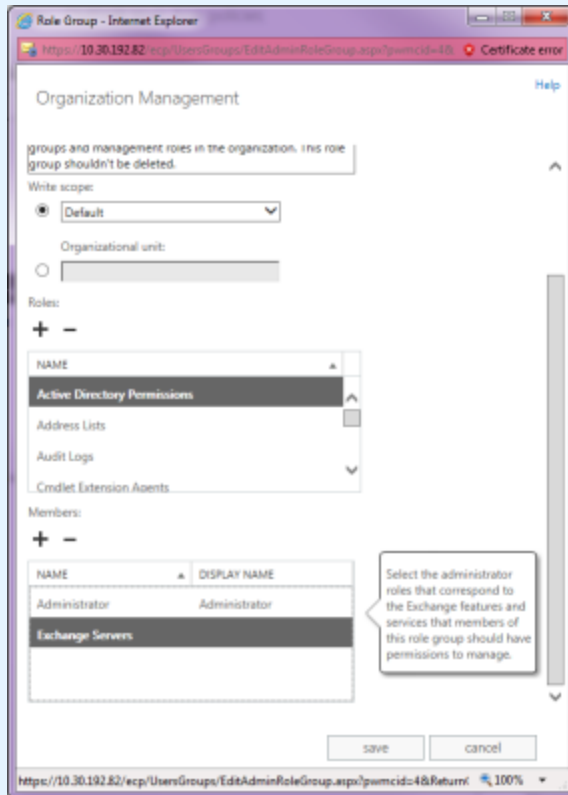
4. In the **Members** list, click the plus icon to display the **Select Members** window.

Figure 132: Select Members Window



5. In the displayed list, select **Exchange Servers** and click **add** to add the name to the Organization Management domain group.
6. Click **ok** to return to the **Role Group** window, with **Exchange Servers** displayed in the **Members** list.

Figure 133: Role Group Window – Members List



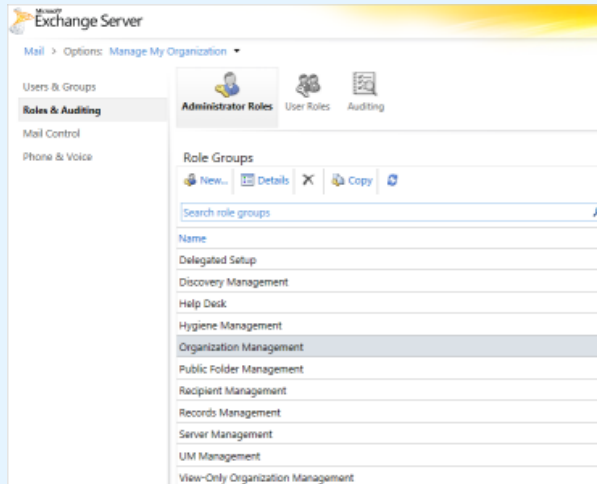
7. Click **Save** to save changes and exit the window.

Add an Exchange server to the Organization Management domain group for Microsoft Exchange 2010:

1. In a local browser, enter **https://<Exchange Server IP Address>/ecp** to access the **Exchange Server** page for Microsoft Exchange 2010.

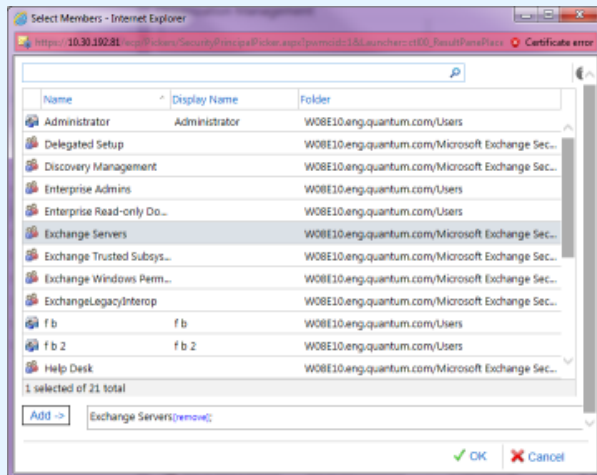
2. Select the **Roles and Auditing** tab, and then select the **Administrator Roles** tab.

Figure 134: Exchange Server – Administrator Roles Tab



3. Double-click **Organization Management** to display the **Role Group** window.
4. In the **Members** list, click the plus icon to display the **Select Members** window.

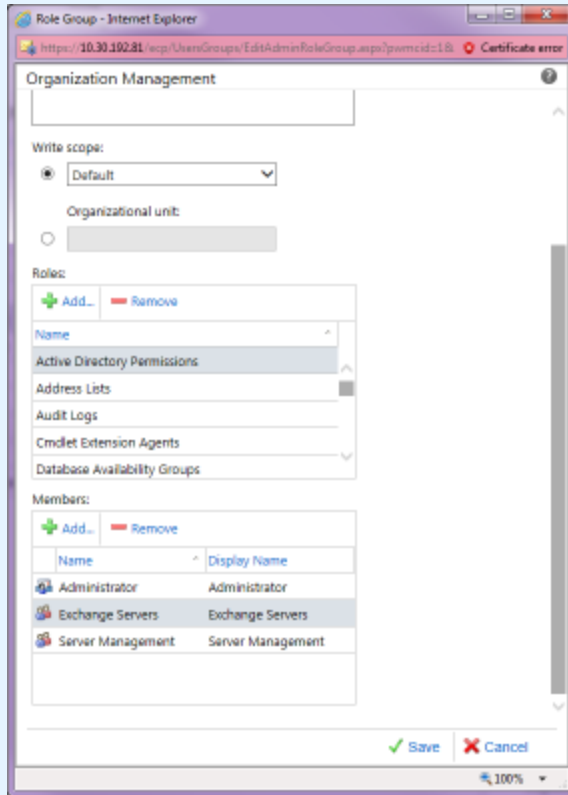
Figure 135: Select Members Window



5. In the displayed list, select **Exchange Servers** and click **Add** to add the name to the **Organization Management** domain group.

6. Click **OK** to return to the **Role Group** window, with **Exchange Servers** displayed in the **Members** list.

Figure 136: Role Group Window – Members List



7. Click **Save** to save changes and exit the window.

Recovering Mailboxes on an Exchange Server

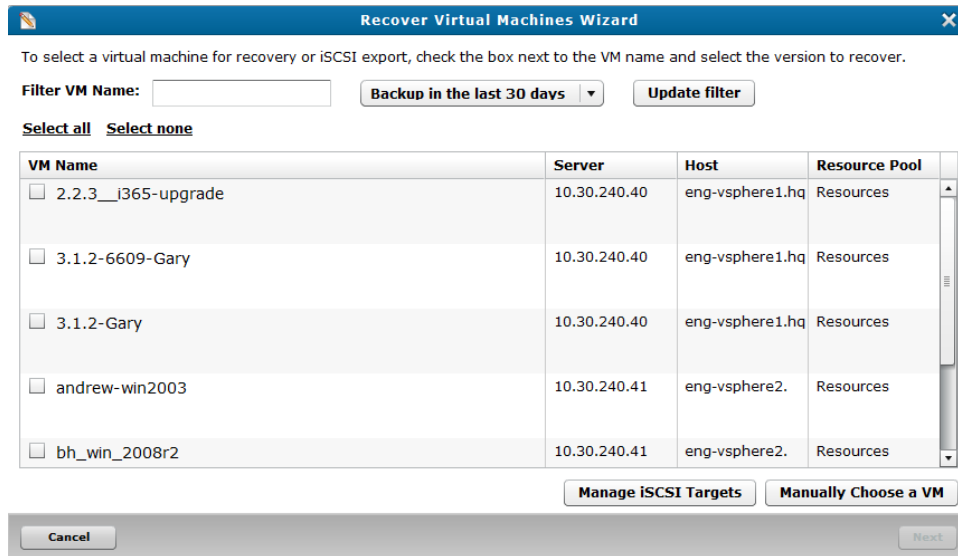
Use the **Exchange Recovery Wizard** to recover mailboxes on an Exchange server. You can view the status of a mailbox recovery on the **Tasks** console. See [Navigating the vmPRO Tasks Console](#).

Use the following tasks to recover a mailbox on an Exchange server. After the vmPRO appliance completes the recovery process, it initiates an automatic Exchange server cleanup process. See [Manually Cleaning Up the Exchange Server](#).

Access the Exchange Recovery Wizard

1. From the **SmartMotion Backup** menu, select **Recover** to display the **Recover Virtual Machines Wizard**.

Figure 137: Recover Virtual Machines Wizard



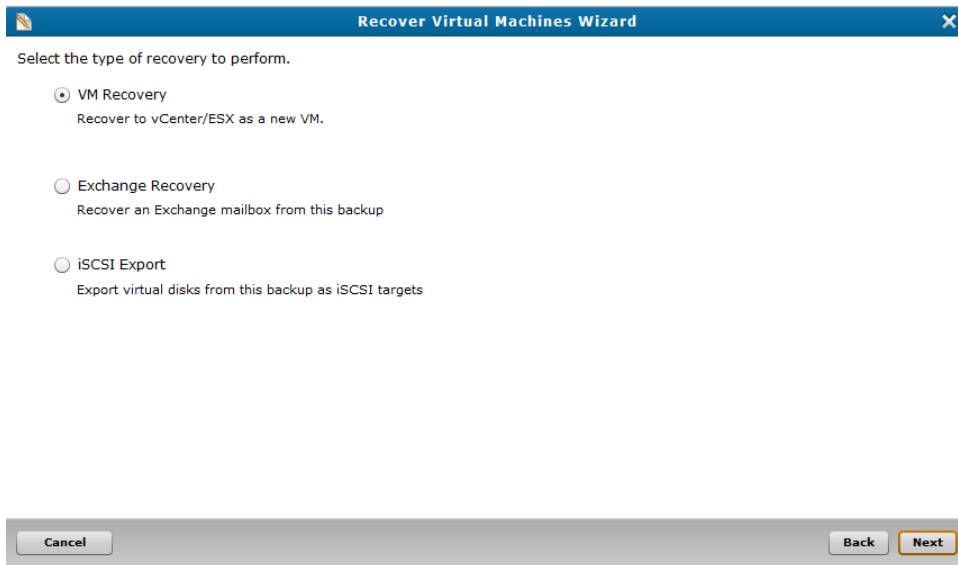
2. As needed, filter the list of VMs from which to select by doing the following:
 - In the **Filter VM Name** field, enter the name of the VM to recover.
 - In the **Backup in the last xx days** drop-down list, select to display VMs that have been backed up in the last 30 or 60 days, or select to display all backup history.
 - Click **Update filter** to update the list of VMs based on the filter criteria.
3. Select the VMs to recover by doing one of the following:
 - Click **Select All** to recover all displayed VMs.
 - Select the check box next to each VM to recover.
4. In the **Recover from** drop-down list for each selected VM, select the date and time of the backup from which to recover data.

Note: Click **Select none** to clear all current selections.

Note: If you are performing a recovery using iSCSI, click **Manage iSCSI Targets** to display the **iSCSI Targets** dialog box. Use this dialog box to view your current iSCSI targets, as well as to remove iSCSI targets you no longer need. See [Manually Cleaning Up the Exchange Server](#).

5. Click **Next** to display the **Select the type of recovery to perform** page.

Figure 138: Select the type of recovery to perform Page



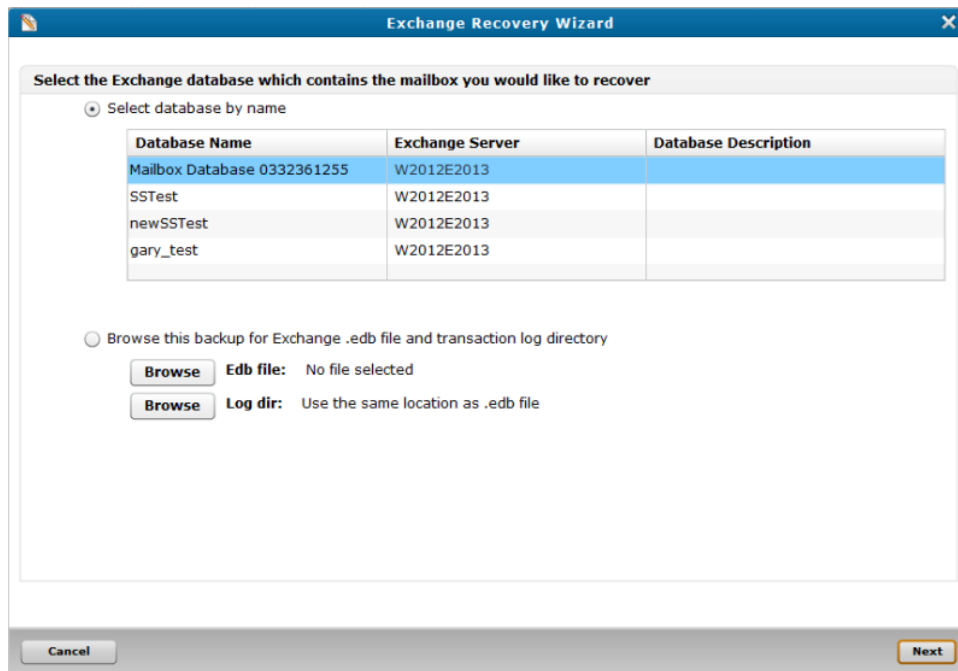
6. Select **Exchange Recovery** to recover mailboxes on an exchange server, and click **Next** to display the **Exchange Recovery Wizard**.

Set up for the Exchange recovery

1. Access the **Exchange Recovery Wizard**.
2. Do one of the following, depending on whether you use the Quantum VSS agent to perform backups of your Exchange server:

If the Quantum VSS agent is enabled

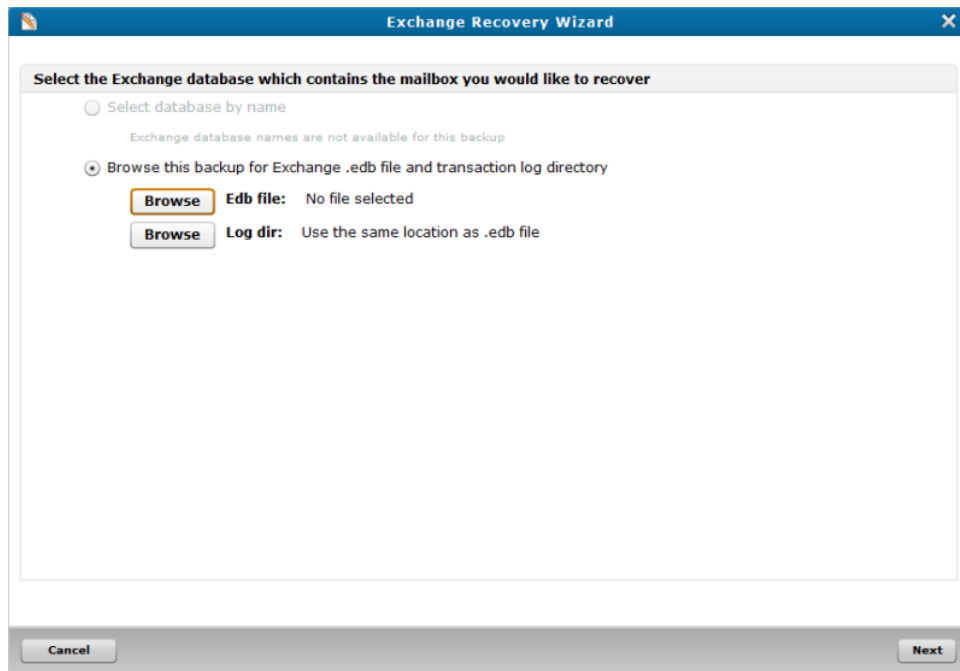
Figure 139: Select database by name



- Select the **Select database by name** check box, as needed.
- Select the Exchange database that contains the mailbox to recover.
- Click **Next** to display the **vCenter/ESX server information** page.

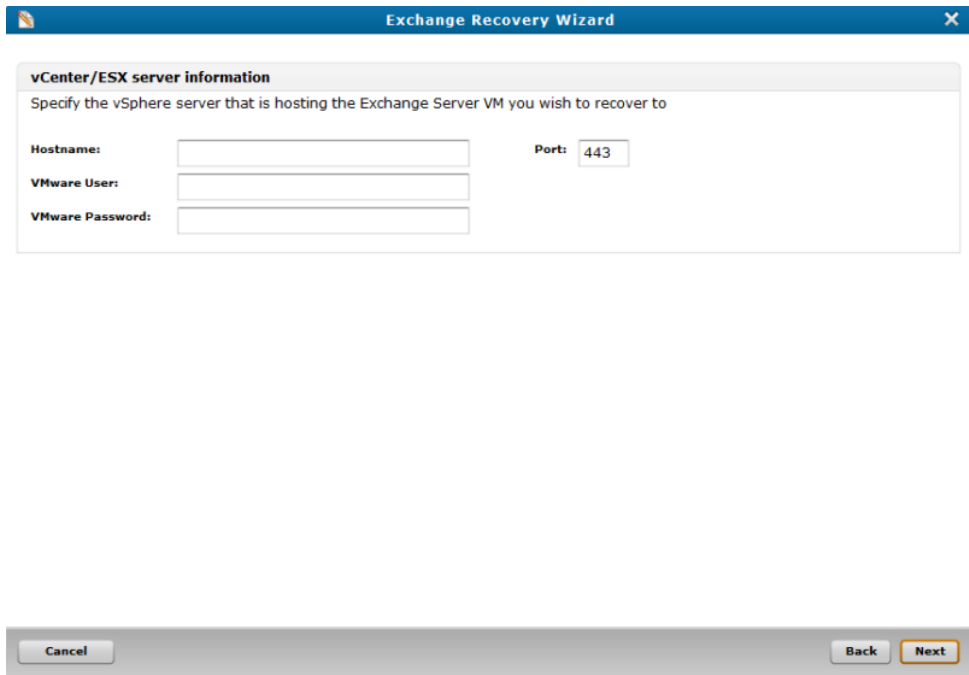
If the Quantum VSS agent is not enabled

Figure 140: Browse this backup for the Exchange .edb file and transaction log directory



- a. Click **Browse Edb. file** to display the **Select .edb file** dialog box.
- b. Navigate to the **.edb** file for the mailbox to recover, select it, and click **OK** to return to the **Exchange Recovery Wizard**.
- c. Click **Browse Log dir** to display the **Select log directory** dialog box.
- d. Navigate to the log directory for the mailbox to recover, select it, and click **OK** to return to the **Exchange Recovery Wizard**.
- e. Click **Next** to display the **vCenter/ESX server information** page.

Figure 141: vCenter/ESX server information Page



3. In the following fields, enter the credentials for the vSphere server that is hosting the Exchange server VM to recover:

Field	Description
Hostname	The vSphere server's host name.
VMware User	The user name needed to access the vSphere server.
VMware Password	The password needed to access the vSphere server.

4. Click **Next** to display the **Target Exchange Server** page.

Figure 142: Target Exchange Server Page

Exchange Recovery Wizard

Target Exchange Server

Specify the Exchange Server which will be the target of the mailbox recovery.
A temporary recovery database will be created on this server.

VM Name:

IP address:

Windows Username:

Windows Password:

Cancel Back Next

5. In the following fields, enter the credentials for the target Exchange server VM:

Field	Description
VM Name	The name of the target Exchange server VM.
IP address	The IP address of the target Exchange server.
Windows Username	The Windows user name needed to access the target Exchange server.
Windows Password	The Windows password needed to access the target Exchange server.

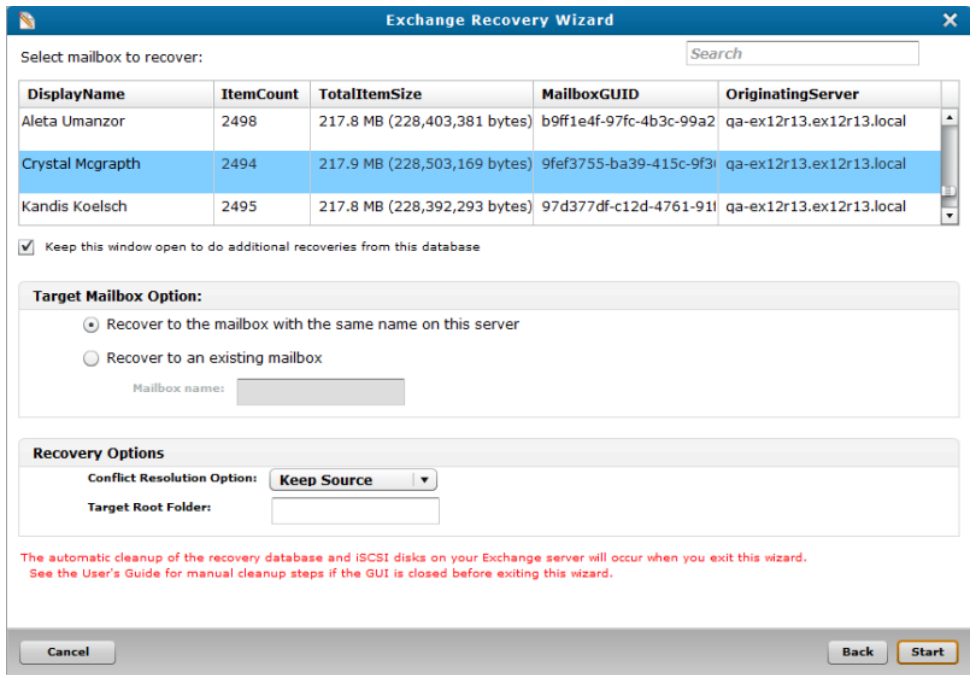
Note: Because Exchange Recovery requires administrator access to the target Exchange server VM, you must provide Windows credentials with administrator privileges.

6. Click **Next** to activate the recovery database setup. When the setup has completed, the **Select mailbox to recover** page displays.

Recover mailboxes on an Exchange server

1. Display the **Select mailbox to recover** page.

Figure 143: Select mailbox to recover Page



2. In the mailbox list, select the mailbox to recover.

Note: You can recover only one mailbox at a time.

3. Select the **Keep this window open to do additional recoveries from this database** check box to return to this page after the selected mailbox is recovered.

4. In the **Target Mailbox Option** area, select one of the following:

Option	Description
Recover to the mailbox with the same name on this server	Places the recovered mailbox in the target mailbox with the same name.
Recover to an existing mailbox	Places the recovered mailbox in the target mailbox specified in the Mailbox name field. In the Mailbox name field, enter the target mailbox's name.

5. In the **Recovery Options** area, indicate the following recovery options, as needed:

Option	Description
Conflict Resolution Option	<p>Specifies the action for the Mailbox Replication Service (MRS) to take if multiple matching messages exist in the target mailbox.</p> <p>From the drop-down list, select one of the following:</p> <ul style="list-style-type: none">• Keep Source – Keeps the source message and deletes all other matching messages.• Keep Latest – Keeps the latest message and deletes all other matching messages.• Keep All – Keeps all matching messages.
Target Root Folder	<p>Specifies the top-level folder in which to restore data. Enter a target root folder, as appropriate.</p> <p>If you do not enter a target root folder, the vmPRO appliance restores data to the top of the folder structure in the target mailbox. In doing so, the appliance merges content under existing folders, and creates new folders when they do not already exist in the target mailbox.</p>

6. Click **Start** to recover the mailbox. After the mailbox is recovered, one of the following happens:

If you did not select the Keep this window open to do additional recoveries from this database option:

The vmPRO appliance automatically activates the Exchange server cleanup process and closes the wizard.

If you selected the Keep this window open to do additional recoveries from this database option:

The **Mailbox Successfully Recovered** dialog box displays.

- Click **OK** to return to the **Select mailbox to recover** page.
- Continue restoring mailboxes, as needed.
- Before starting the last mailbox recovery, clear the **Keep this window open to do additional recoveries from this database** check box. The vmPRO appliance recovers the last mailbox, and automatically activates the Exchange server cleanup process and closes the wizard.

i Note: If you abort a mailbox recovery, you will see mailboxes continue to be moved to the target mailbox for a period of time due to a time delay between the abort command and the Exchange server's suspension of the recovery.

Manually Cleaning Up the Exchange Server

During the recovery of an Exchange server, the vmPRO appliance configures iSCSI disks and a recovery database on your Exchange server. The appliance automatically cleans up this configuration when the

recovery process is complete, or when you exit the **Exchange Recovery Wizard** by using the **back**, **cancel**, or **X** buttons.

If you close the vmPRO GUI without exiting the **Exchange Recovery Wizard**, or if the browser crashes when a recovery is running, the vmPRO appliance does not automatically clean up the configuration changes made to your Exchange server. If this occurs, you must do a manual cleanup of your Exchange server.

Removing the Recovery Database

Use your Exchange Management Shell to dismount and remove the recovery database from your Exchange server.

Remove the recovery database from the Exchange server

1. Open your Exchange Management Shell.
2. At the prompt, enter `Get-MailboxDatabase | Select-Object Name` to display the **vmPRO-Recovery** database name.

Figure 144: Obtain the Recovery Database Name

```
[PS] C:\>Get-MailboxDatabase | Select-Object Name
Name
-----
Mailbox Database 0013042993
test_database
diff_part_same_disk
vmPRO-Recovery-ign.1995-03.com.quantum:vmpro-target1
```

3. At the prompt, enter `Dismount-Database <database name>` to display a confirmation prompt.
4. Enter **Y** to confirm the dismount.

Figure 145: Dismount the Recovery Database

```
[PS] C:\>Dismount-Database vmPRO-Recovery-ign.1995-03.com.quantum:vmpro-target1
Confirm
Are you sure you want to perform this action?
Dismounting database "vmPRO-Recovery-ign.1995-03.com.quantum:vmpro-target1". This may result in reduced availability for mailboxes in the database.
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (default is "Y"):
[PS] C:\>
```

5. At the next prompt, enter `Remove-MailboxDatabase-identity <database name>` to display a confirmation prompt.
6. Enter **Y** to confirm the removal.

Figure 146: Remove the Recovery Database

```
[PS] C:\>Remove-MailboxDatabase-identity vmPRO-Recovery-ign.1995-03.com.quantum:vmpro-target1
Confirm
Are you sure you want to perform this action?
Removing mailbox database "vmPRO-Recovery-ign.1995-03.com.quantum:vmpro-target1".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (default is "Y"):
WARNING: The specified database has been removed. You must remove the database file located in C:\Program
Files\QuantumExcReco\3eeb746f-7867-42ce-b7f3-ed94c2a013a5\vmpro_exc_recovery-target1-1\edb_location\diff_part_same_disk.edb from your computer manually if it exists. Specified database:
vmPRO-Recovery-ign.1995-03.com.quantum:vmpro-target1
[PS] C:\>
```

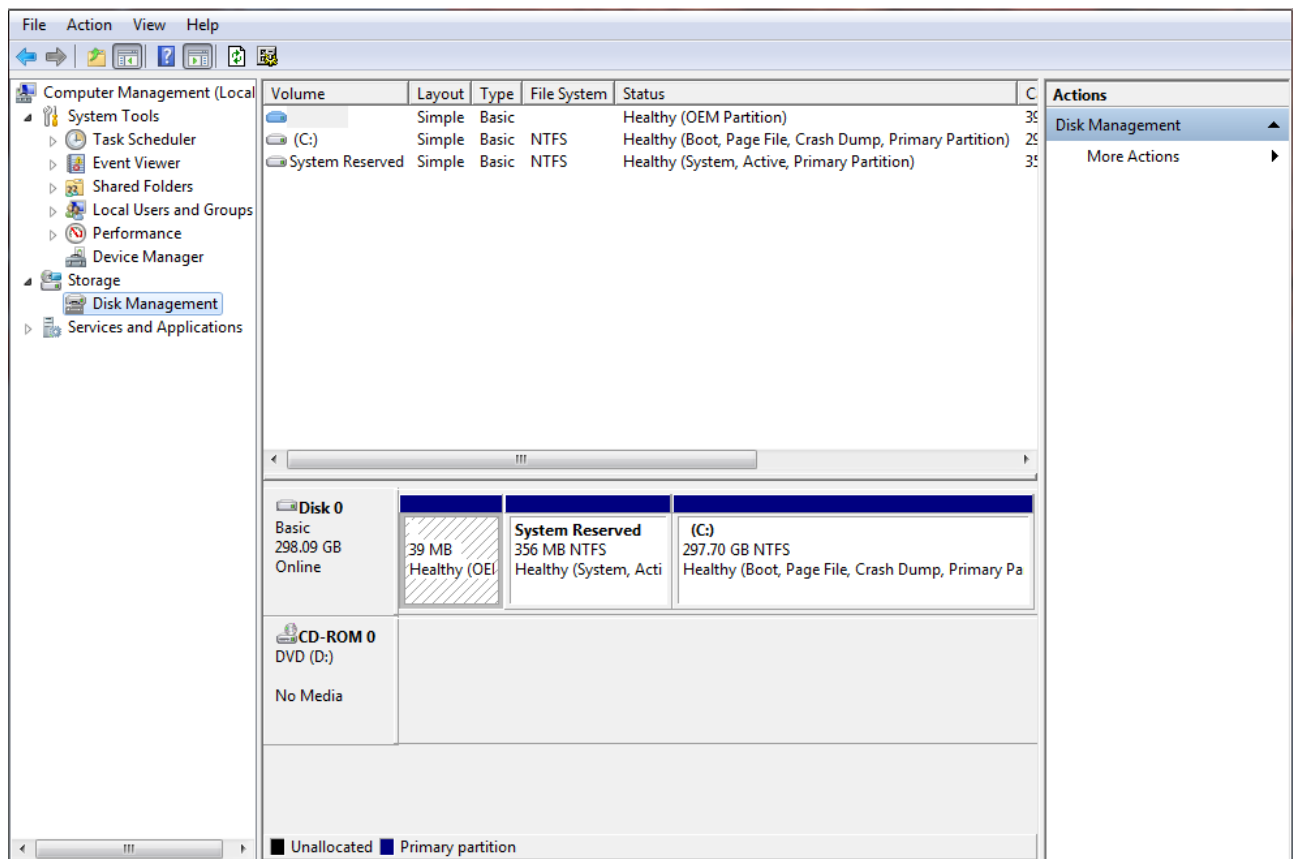
Dismount Volumes from Your Local System

The vmPRO appliance adds one or more disks to your system. It adds more than one disk when the Exchange database and transaction logs are on different disks. When the Exchange database and transaction logs are on the same disk, but in different partitions, the vmPRO appliance mounts two volumes on that disk. You need to dismount each volume on each disk that the vmPRO appliance added.

Remove vmPRO mounted volumes

1. From the **Computer Management** window, select **Storage > Disk Management** to display the system's mounted volumes and disk information in the center pane.

Figure 147: Computer Management – Disk Management Pane



2. Right-click the appropriate volumes on each disk mounted by the vmPRO appliance, and then select **Change Drive Letter and Paths** to display the **Change Drive Letter and Paths for New Volume** dialog box.

Note: Volumes mounted by the vmPRO appliance display **QuantumExcRecv** in the dialog box.

3. Click **Remove** to dismount the volume.
4. Right-click each volume that you dismounted, and select **Offline** to take the volumes offline.

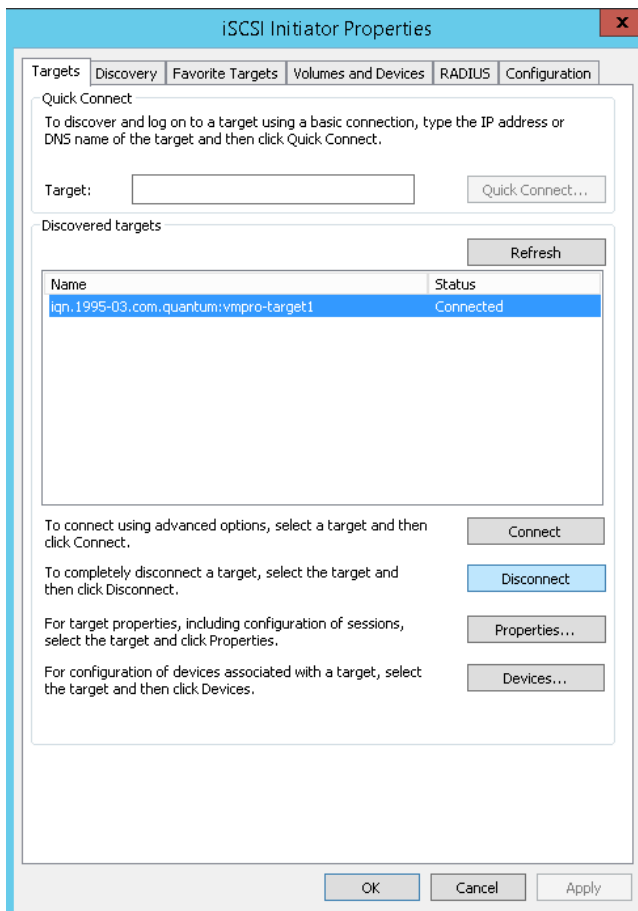
Remove the vmPRO Target

Make sure to both disconnect the vmPRO target and remove the vmPRO target portal from the iSCSI Initiator before the removing the iSCSI target.

Remove the vmPRO target from your iSCSI Initiator

1. Open the **iSCSI Initiator Properties** dialog box.
2. Click the **Targets** tab, as needed, and select the vmPRO target.

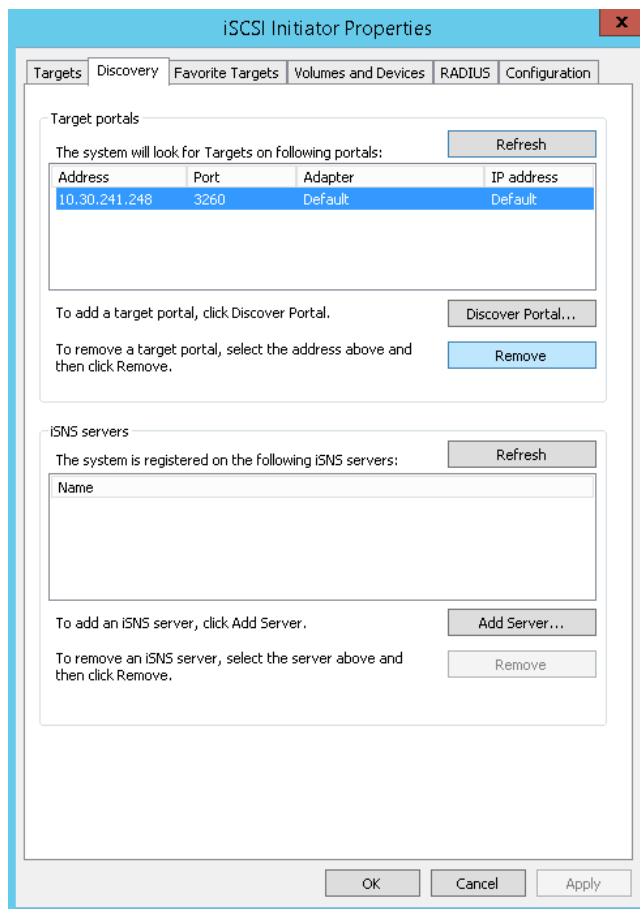
Figure 148: iSCSI Initiator Properties Dialog Box – TargetsTab



3. Click **Disconnect** to disconnect the vmPRO target from the iSCSI Initiator.

4. Click the **Discovery** tab, and select the vmPRO target portal.

Figure 149: iSCSI Initiator Properties Dialog Box – Discovery Tab



5. Click **Remove** to remove the vmPRO target portal from the iSCSI Initiator.

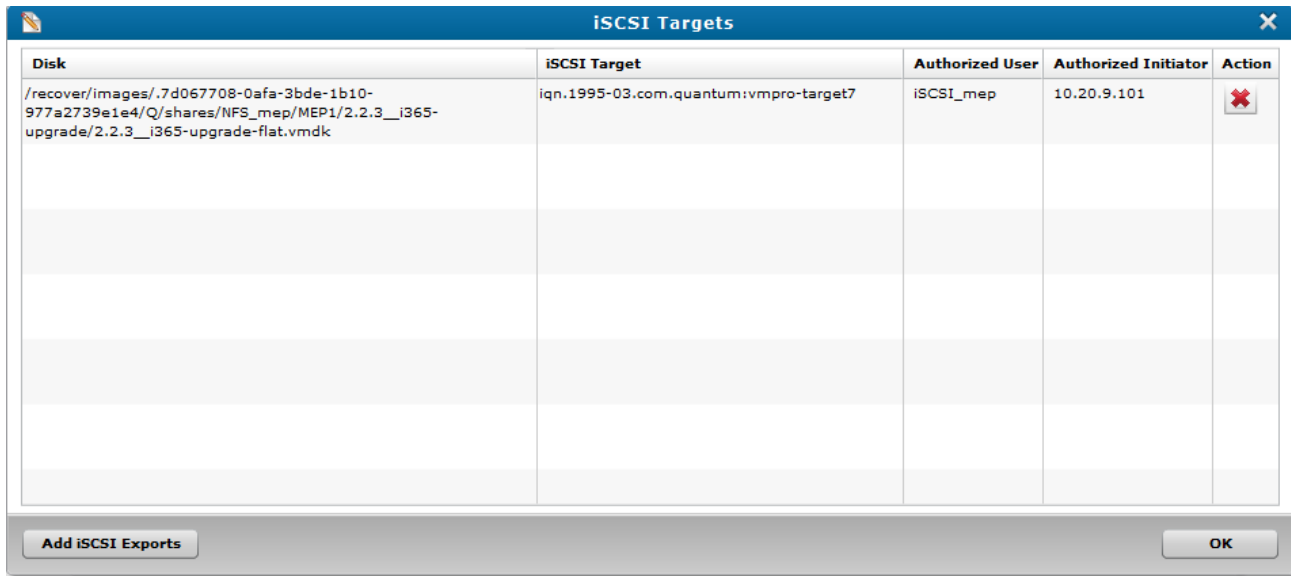
Remove the iSCSI Target

As your final clean up step, you need to access your vmPRO GUI to remove the iSCSI target from your vmPRO appliance.

Remove the iSCSI target from your vmPRO appliance:

1. Display the vmPRO GUI.
2. From the **SmartMotion Backup** menu, select **iSCSI Targets** to display the **iSCSI Targets** dialog box.

Figure 150: iSCSI Targets Dialog Box



3. For each iSCSI target to remove, click to delete it from the vmPRO appliance.
4. Click **OK** to exit the dialog box.

iSCSI Export and Recovery

Use the vmPRO appliance's iSCSI Export and Recovery feature to recover your backed-up data as disk images from a Windows-based virtual machine (VM) or physical machine.

The iSCSI Export and Recovery feature differs from VM recovery as follows:

- When you recover a backed-up VM, you are recovering an entire file system from the Network Attached Storage (NAS) target. The VM's file system is added to the datastore's (target server's) inventory as a new VM, which users can then access.
- With the iSCSI Export and Recovery feature, your vmPRO appliance works with the Windows iSCSI Initiator to capture the VM's file system as a disk image. On the same Windows system from which the iSCSI Initiator is running, you can mount the VM disk image (VMDK) to access the files within the VM.

For more information about recovering entire VM file systems, see [Recovering Virtual Machines](#).

Prerequisites

Before using the iSCSI Export and Recovery feature, make sure your system meets the following prerequisites:

Windows iSCSI Initiator Installation

The Windows iSCSI Initiator must be installed on your Windows system, typically in the **Administrative Tools** folder. If you need to download the iSCSI Initiator, you can do so from <http://www.microsoft.com/en-us/download/details.aspx?id=18986>.

iSCSI User Configuration

For authentication and security purposes, the Windows iSCSI Initiator requires a unique user.

Using the **Configure User** dialog box, create a user for the iSCSI Initiator. You must assign the iSCSI user a 12- to-16-character password. See [Configuring Users for a vmPRO Appliance](#).

iSCSI Write Area Settings

The iSCSI Initiator adds each exported disk image as a file to the iSCSI target's write area storage. You must configure the iSCSI write area settings for these files. See the "Target iSCSI Disk" section of [Preparing For Exchange Recovery](#).

iSCSI Configuration Notes

Keep the following in mind when using the iSCSI Initiator to recover VM file systems:

iSCSI IP Address

The VMDK is exported to a specific IP address for the iSCSI Initiator. Other iSCSI Initiators cannot discover the vmPRO appliance or its exported VMDKs.

Target vmPRO Appliances

- Target vmPRO appliances on the iSCSI Initiator consume system resources. We recommend that you remove unused targets from your iSCSI Initiator.
- The iSCSI Initiator keeps track of how long a target is active, and it generates a warning when the target has been exposed for more than 24 hours.

Note: You cannot delete a target vmPRO appliance when it is connected to the iSCSI Initiator.

iSCSI User

You cannot edit or delete the iSCSI user or password created on your vmPRO appliance when the following occurs:

- The vmPRO appliance is connected to the iSCSI Initiator.
- The iSCSI user is connected to the target iSCSI disk through the iSCSI Initiator.

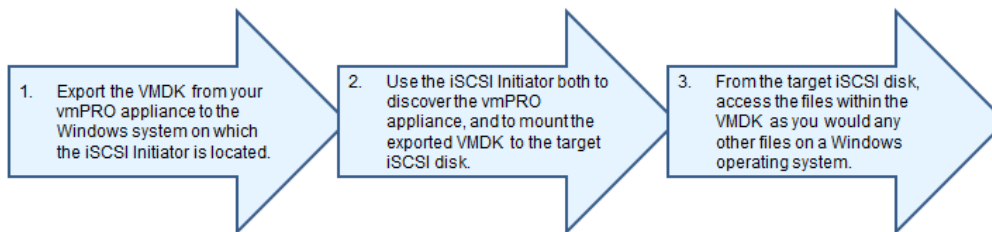
Reboots

When a vmPRO appliance is rebooted, its connection to the iSCSI Initiator is lost, along with all previously written data. In addition, previously exported VMDKs are no longer available. After a reboot, you must perform a new iSCSI export and recovery.

Recovering VM Disks Using iSCSI

Use the following workflow to recover virtual machine disk images (VMDKs) using iSCSI:

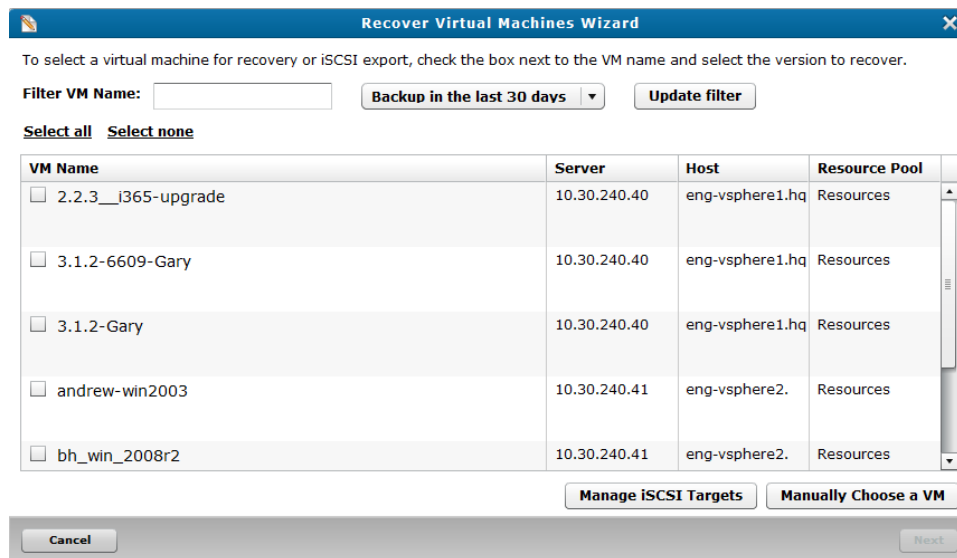
Figure 151: iSCSI Recovery Workflow



Export VMDKs to an iSCSI target

1. From the **SmartMotion Backup** menu, select **Recover** to display the **Recover Virtual Machines Wizard**.

Figure 152: Recover Virtual Machines Wizard



2. As needed, filter the list of VMs from which to select by doing the following:
 - In the **Filter VM Name** field, enter the name of the VM to recover.
 - In the **Backup in the last xx days** drop-down list, select to display VMs that have been backed up in

the last 30 or 60 days, or select to display all backup history.

- Click **Update filter** to update the list of VMs based on the filter criteria.
3. Select the VMs to recover by doing one of the following:
 - Click **Select All** to recover all displayed VMs.
 - Select the check box next to each VM to recover.

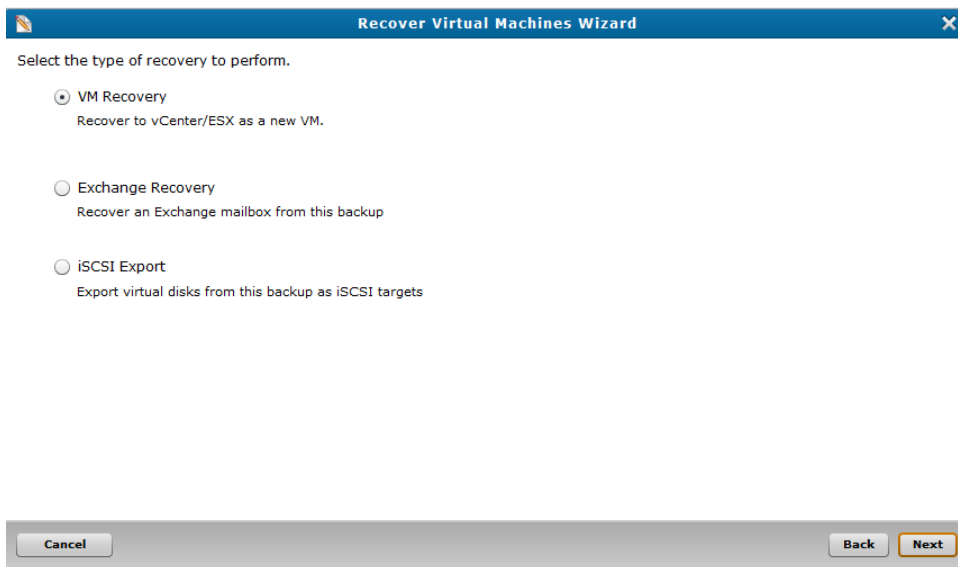
i Note: Click **Select none** to clear all current selections.

4. In the **Recover from** drop-down list for each selected VM, select the date and time of the backup from which to recover data.

i Note: If you are performing a recovery using iSCSI, click **Manage iSCSI Targets** to display the **iSCSI Targets** dialog box. Use this dialog box to view your current iSCSI targets, as well as to remove iSCSI targets you no longer need. See [Manually Cleaning Up the Exchange Server](#).

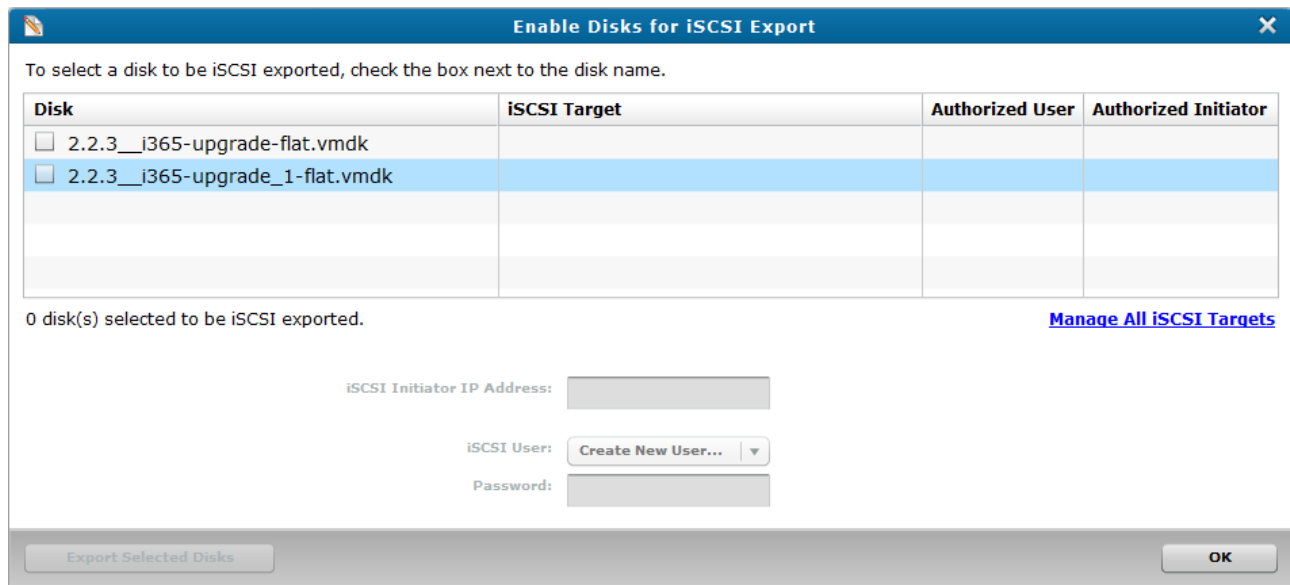
5. Click **Next** to display the **Select the type of recovery to perform** page.

Figure 153: Select the type of recovery to perform Page



6. Select **iSCSI Export** and click **Next** to display the **Enable Disks for iSCSI Export** dialog box.

Figure 154: Enable Disks for iSCSI Export Dialog Box



7. Select the check box next to each VMDK to export to the iSCSI target.

Note: Click **Manage All iSCSI Targets** to display the **iSCSI Targets** dialog box. Use this dialog box to view your current iSCSI targets, as well as to remove iSCSI targets you no longer need. See the **Remove the iSCSI Target** task in [Manually Cleaning Up the Exchange Server](#).

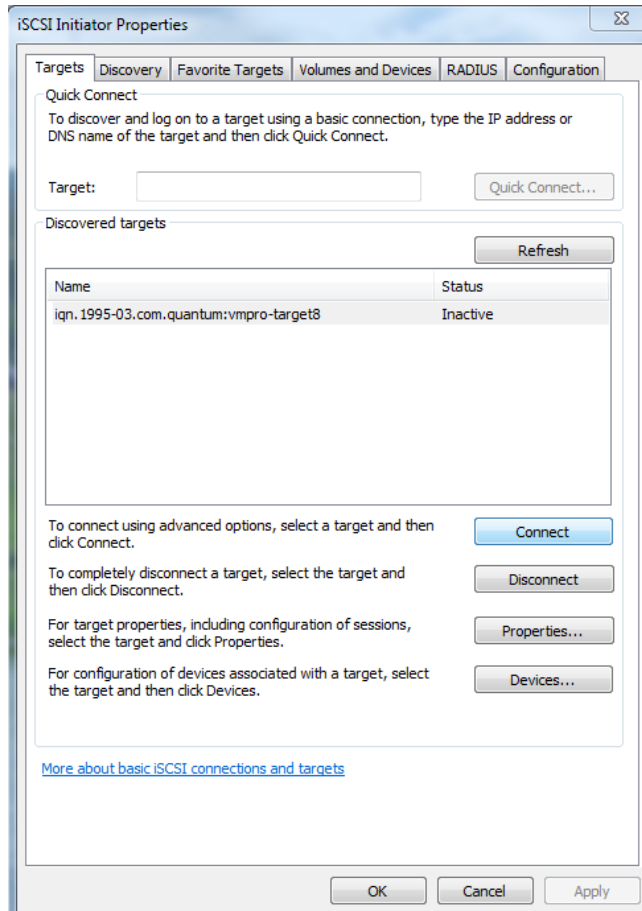
8. In the **iSCSI Initiator IP Address** field, enter the address of the computer on which the iSCSI Initiator is running.
9. In the **iSCSI User** drop-down list, select one of the following:
 - The user created for the iSCSI Initiator.
 - **Create New User** to display the **Configure User** dialog box. Use this dialog box to create a user for the iSCSI Initiator. See [Configuring Users for a vmPRO Appliance](#).
10. In the **Password** field, enter the 12- to-16-character password assigned to the iSCSI user.
11. Click **Export Selected Disks** to export the selected VMDKs to the iSCSI target.
12. Click **OK** to exit the wizard.

Recover disk images from the iSCSI Initiator

1. Open your iSCSI Initiator.
2. Discover the vmPRO:
 - a. Click the **Discovery** tab to display the **Discovery** page.
 - b. Click **Discover Portal** to display the **Discover Target Portal** dialog box.

- c. In the **IP address or DNS name** field, enter the IP address of your vmPRO appliance.
 - d. Click **OK** to save changes and exit the dialog box.
3. Click the **Targets** tab of the iSCSI Initiator to display the vmPRO appliance in the **Discovered targets** field.

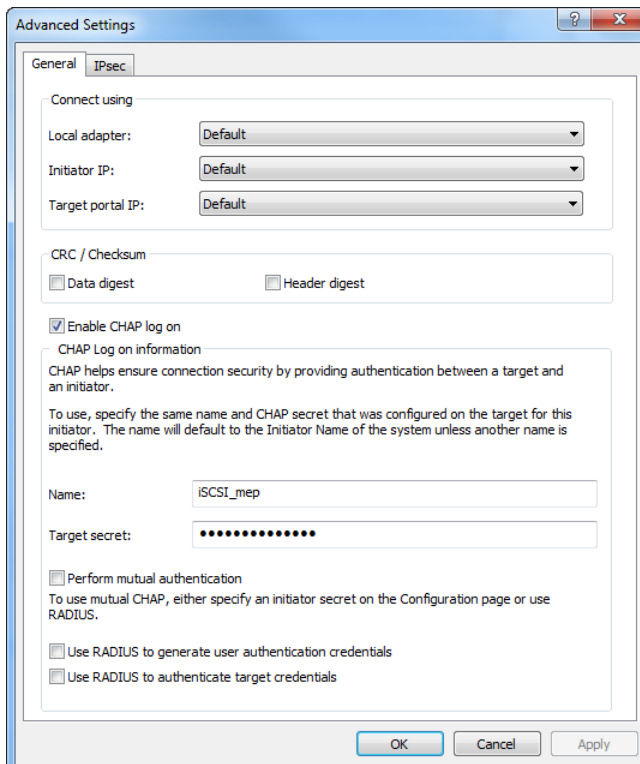
Figure 155: Targets Page



4. Select the vmPRO appliance, and click **Connect** to display the **Connect To Target** dialog box.

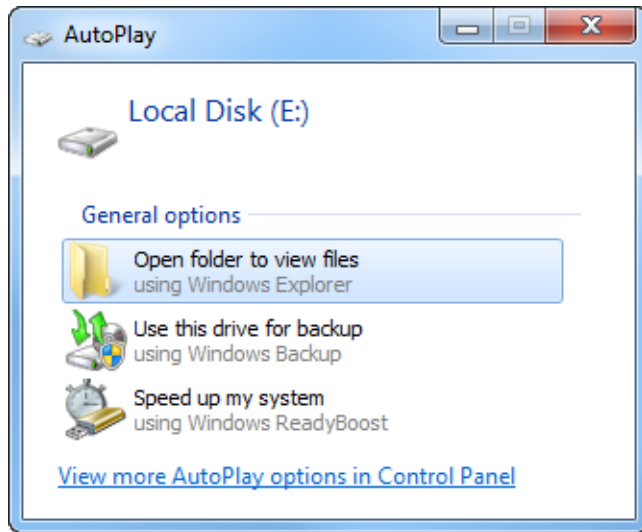
5. Click **Advanced** to display the **Advanced Settings** dialog box.

Figure 156: Advanced Settings Dialog Box



6. Connect to the iSCSI target from the vmPRO appliance:
 - a. Select the **Enable CHAP log on** check box to encrypt the password needed to access the target.
 - b. In the **Name** field, enter the user name created for the vmPRO iSCSI user. See the "Prerequisites" section of [About iSCSI Export and Recovery](#).
 - c. In the **Target secret** field, enter the password assigned to the vmPRO iSCSI user.
 - d. Click **OK** to save changes and exit the dialog box.
7. In the **Connect To Target** dialog box, click **OK** to display an **AutoPlay** dialog box, which you can use to access your mounted VMDK.

Figure 157: AutoPlay Dialog Box for iSCSI Target



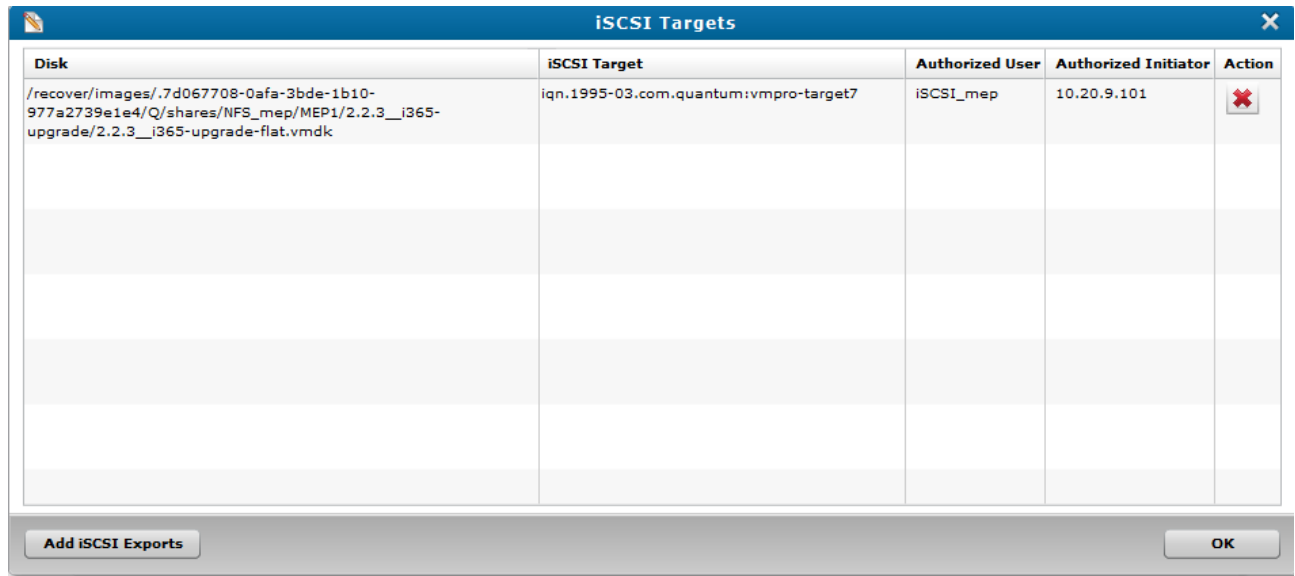
8. Open your mounted VMDK to access its files.

⚠ Caution: Do not close the iSCSI Initiator after connecting to the target vmPRO appliance. If you close the iSCSI Initiator, the **AutoPlay** dialog box will not display, and you will be unable to access the files on the VMDKs without repeating the discovery and connection process.

Abort an iSCSI export

1. Display the **iSCSI Targets** dialog box by doing one of the following:
 - From the **SmartMotion Backup** menu, select **iSCSI Targets**.
 - From the **Recover Virtual Machines Wizard**, click **Manage iSCSI Targets**.

Figure 158: iSCSI Targets Dialog Box



2. Select the VMDK being exported to an iSCSI target.
3. Click to abort the export.
4. Click **OK** to save updates and exit the dialog box.

Individual File Recovery

Using the vmPRO SmartView feature, you can recover individual files within exported virtual machines (VMs) by mounting CIFS shares to your local system.

Note: You cannot recover individual files from NFS shares.

Note: This process is separate from the VM recovery process. If you use a third-party application to back up data, you must use that application to recover the entire VM. See [Recovering VMs Backed Up with a Third-Party Application](#).

Prerequisite

Before you can access the mounted CIFS share, you must configure the **Mount options** setting on the vmPRO appliance to point directly to the location of the SmartMotion backups. This setting provides file-level access to the backups at the `\\<vmPRO-Host_IP>\recover\files` directory on the CIFS share. For instructions on how to configure the **Mount options** setting, see [Configuring NAS Targets for](#)

[SmartMotion Backups.](#)

Supported File Systems and Dynamic Disks

The vmPRO SmartView feature supports only a limited number of types of file systems, dynamic disks, and partitions. Review the following table to view a list of supported and unsupported file systems, dynamic disks, and partitions.

Supported File Systems, Dynamic Disks, and Partitions	Unsupported File Systems, Dynamic Disks, and Partitions
Extended file systems (ext) 2, 3, and 4	Windows dynamic disks that span multiple drives
File Allocation Table (FAT) file systems	Windows dynamic disks that are striped
New Technology File Systems (NTFS)	Windows dynamic disks that use RAID
Supported file systems that are embedded in logical volume manager (LVM) 2 volumes that do not span multiple virtual disks	Windows 2008 dynamic disk file level access
Disks with Master Boot Record (MBR) partitions	Dynamic volumes that span multiple disks
Disks with GUID Partition Table (GPT) partitions	Volumes that span multiple virtual disks
Windows 2003 simple dynamic disks with a single partition	Solaris Unix file systems (UFS)
i Note: If there are multiple partitions on a Windows 2003 dynamic disk, you can only access files on the first partition.	File systems on raw (un-partitioned) disks
	Physical/logical LVM partitions that have been created on raw (un-partitioned) disks
	Disk partition tables that are converted from GPT to MBR.

Recovering Individual Files

Recover individual files within an exported virtual machine's disk by mounting the CIFS share on your local system.

You can recover individual files from a mounted CIFS share only. This feature does not support NFS shares. You can access the share from either a Windows or Unix/Linux operating system (OS).

- From a Windows OS, mount the CIFS share, and then navigate to the files in the CIFS share using Windows Explorer.

- From a Unix/Linux OS, mount the CIFS share, and then navigate to the files in the CIFS share using the change directory (**cd**) command from your vmPRO appliance's console command line interface (CLI).

Recover individual files from a Windows system

1. Mount the CIFS **recover** share. For mounting a CIFS share on a Windows system, see [Configuring a CIFS Protocol for a vmPRO Appliance](#).
2. Open Windows Explorer.
3. In the **UNC Path** field, enter **\\<vmPRO-Host_IP_Address>\recover\files** to access the **recover\files** directory in the mounted CIFS share.
4. Navigate to the individual files to recover by using the following path:

storage-target (such as **DXi Storage**)

smartmotion_backups

yyyy-mm (month of backup)

yyyy-mm-dd-tttt (date and time of backup)

server folder (such as the IP address for an ESX server)

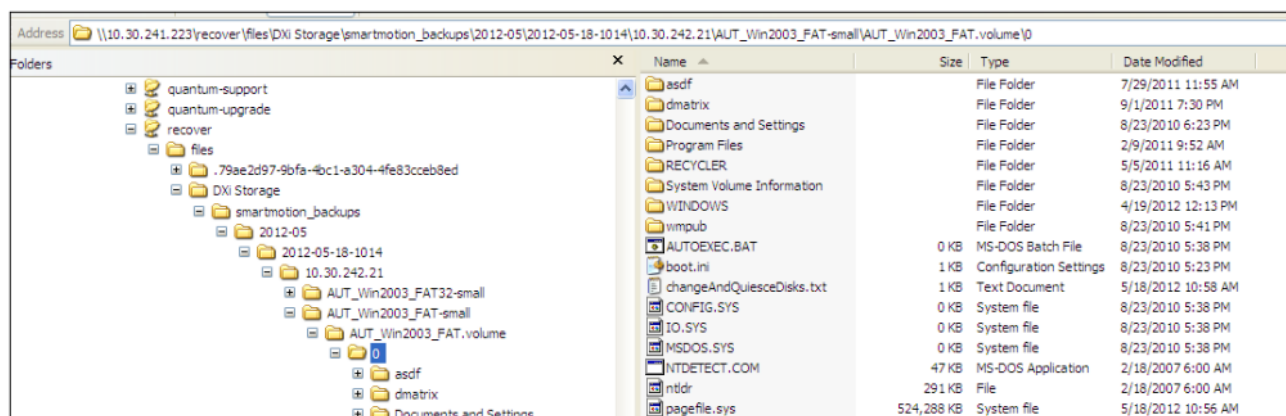
VM directory (identified by a file system, such as **FAT-small**)

disk name (identified by **.volume**)

partition number (identified by a number, such as **0, 1, 2, ...**)

files and directories

Figure 159: recover\files Directory Hierarchy



Recover an individual file from a Unix/Linux system

1. Log on to your vmPRO appliance's console command line interface (CLI).

2. At the command line, enter the mount command to mount the CIFS `\recover` share. For mounting a CIFS share on a Linux system, see [Configuring a CIFS Protocol for a vmPRO Appliance](#).
3. At the command line, enter `cd <vmPRO-Host_IP_Address>/recover/files` to locate the `/recover/files` directory.

The `/recover/files` directory contains directories for each configured NAS target. Each NAS target directory then contains the data exported from your vmPRO appliance. See the directory structure in the preceding task.

4. At each successive command line, enter the appropriate `cd` command to drill down to and automatically mount the correct partition directory.

i Note: You can use the `cd` command to mount more than one partition. There could be a short delay during the automatic mount process of multiple partitions.

5. Access and recover the individual files from the mounted partitions.



Appendix 1: vmPRO CLI Guide

This appendix contains the following topics and sections:

vmPRO CLI Guide	206
Accessing the vSphere Client Console for vmPRO	207
vmPRO Console Commands – autosupport	211
vmPRO Console Commands – cbt	212
vmPRO Console Commands – config	212
vmPRO Console Commands – filesys	213
vmPRO Console Commands – group	214
vmPRO Console Commands – help	215
vmPRO Console Commands – import	215
vmPRO Console Commands – log	216
vmPRO Console Commands – nagios	217
vmPRO Console Commands – net	217
vmPRO Console Commands – ntp	219
vmPRO Console Commands – nw	220
vmPRO Console Commands – smartmotion	221
vmPRO Console Commands – snmp	222

vmPRO Console Commands – ssh	222
vmPRO Console Commands – system	223
vmPRO Console Commands – tsm	225
vmPRO Console Commands – vss	225
External Monitoring Support for a vmPRO Appliance	226

vmPRO CLI Guide

You configure most settings for your vmPRO appliance using the vmPRO GUI or the VMware vSphere Client **Console Configuration Wizard**. You can also perform a limited number of functions from the vmPRO appliance's VMware vSphere Client console command line interface (CLI).

Examples

- If your vmPRO appliance does not have Internet access, you can perform an offline upgrade using the console command line.
- If you use NTP servers to control your vmPRO appliance's internal clock, you can configure NTP time servers from the console command line.

For instructions on accessing the console command line, see [Accessing the vSphere Client Console for vmPRO](#).

Supported Console Commands

- [autosupport](#)
- [cbt](#)
- [config](#)
- [filesys](#)
- [group](#)
- [help](#)
- [import](#)
- [log](#)
- [nagios](#)
- [net](#)

- [ntp](#)
- [nw](#)
- [smartmotion](#)
- [snmp](#)
- [ssh](#)
- [system](#)
- [tsm](#)
- [vss](#)

i Note: All network commands reflect the network related to the vmPRO appliance.

Accessing the vSphere Client Console for vmPRO

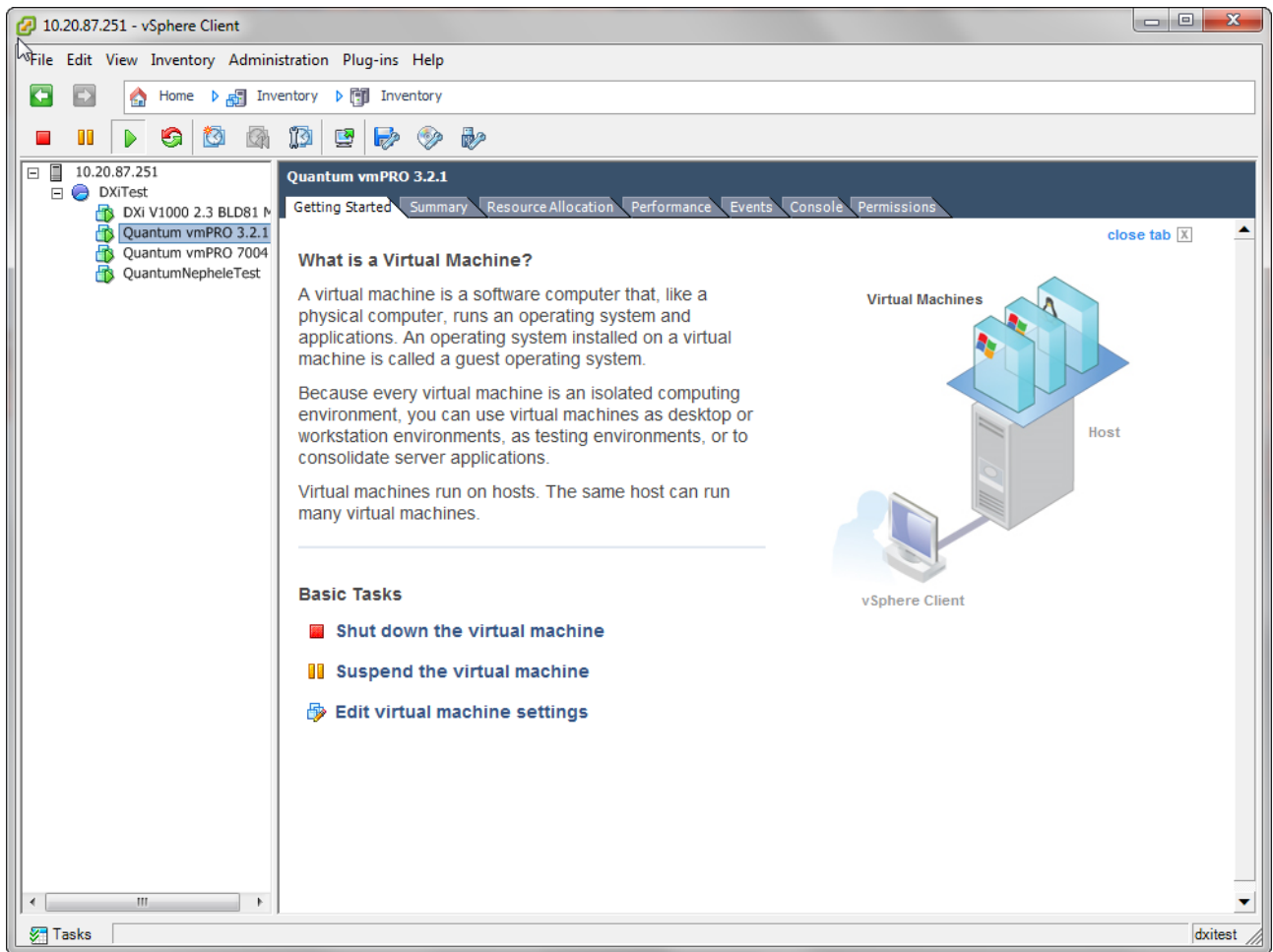
Use the VMware vSphere Client or Web Client console to use the command line interface (CLI) for your vmPRO appliance.

Launch the vSphere Client console for vmPRO

1. Log in to your VMware vSphere Client.

2. In the vSphere Client's left pane, select your vmPRO appliance.

Figure 160: vSphere Client – Left Pane



3. In the vSphere Client's right pane, select the **Console** tab to display the appliance's console. The console displays the Quantum vmPRO version number and IP address for the appliance.

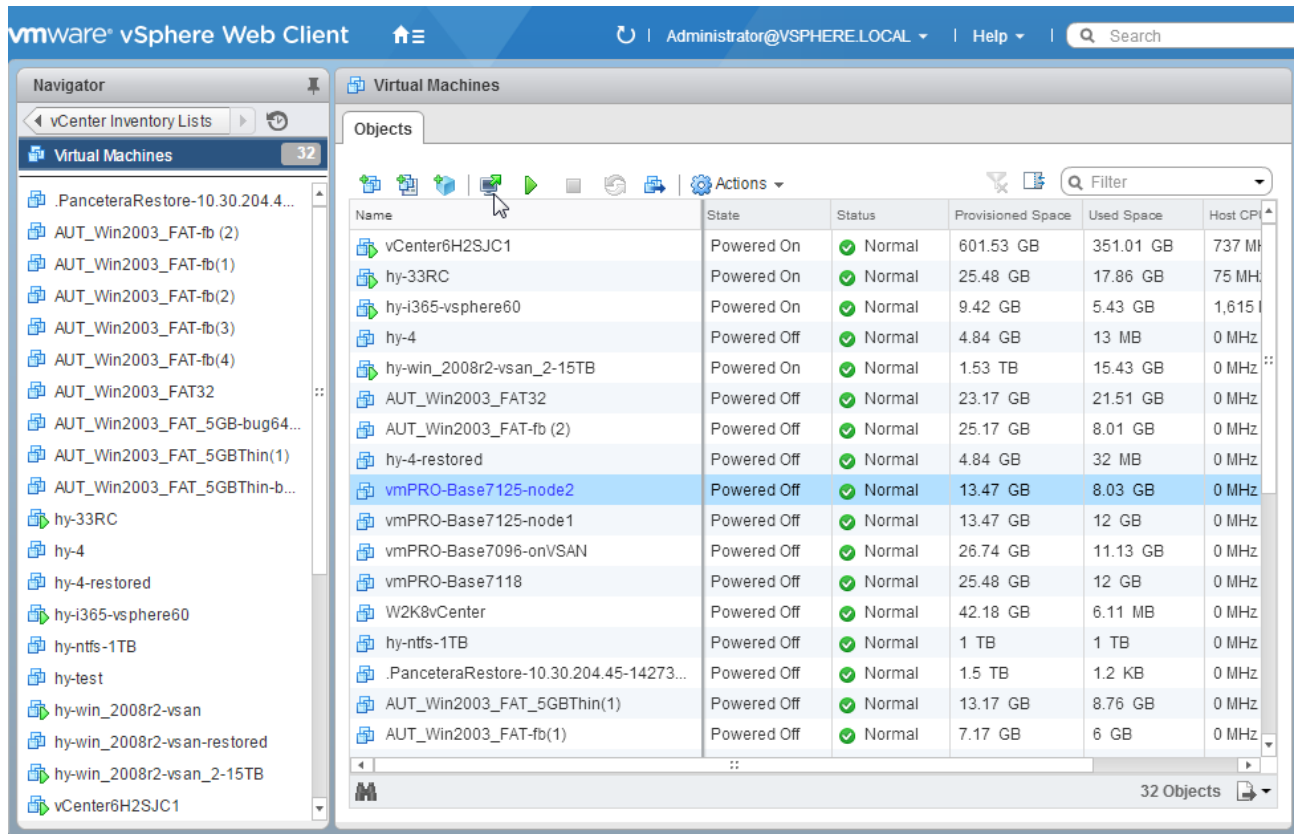
Figure 161: vSphere Client – Console Tab



Launch the vSphere Web Client console for vmPRO

1. Log in to your VMware vSphere Web Client.
2. From **vCenter Inventory Lists**, select **Virtual Machines** to display the list of virtual machines (VMs) within the vCenter.

Figure 162: vSphere Web Client – Virtual Machines Grid



3. From the grid, select the vmPRO appliance.
4. Click  to launch the appliance's console. The console displays the Quantum vmPRO version number and IP address for the appliance (see the **vSphere Client – Console Tab** figure above.)

Log in to the vmPRO appliance's console

1. Click inside the **Console** screen and enter **1** to display the CLI.
2. At the **localhost login** prompt, enter the user name for the vmPRO appliance.
3. At the **Password** prompt, enter the password for the vmPRO appliance.

Additional Navigation Functions

Use the following functions to navigate the vmPRO appliance's client console.

Function	Description
<ctrl + alt>	Use to free the cursor from the console.
Arrow Keys	Use to navigate to different options.
Enter	Use to access the setting on which the cursor is placed. After changing the setting, press <Enter> again to save the setting.
Spacebar	Use to activate an input area.
X or *	Either of these characters inside the brackets indicates the option is selected, such as [X] or [*] .
exit	Use to exit the command line.

vmPRO Console Commands – autosupport

Use the **autosupport** commands to gather log files, and to send the compiled packages to the provided email address.

i Note: Before using this command, you must set up SMTP mail in the vmPRO appliance GUI. See [Configuring Email for a vmPRO Appliance](#).

autosupport commands

autosupport send logs [<email-address>]

Use to email support packages to the email address given in the command.

autosupport upload logs [nocreate]

Use to upload support packages to the Quantum Support site. The **nocreate** flag tells the system not to create a support package, since it has already been created.

autosupport upload report

Use to upload reports the Quantum Support site.

autosupport set daily-upload-packages on|off

Use to activate or deactivate automatic uploading of support bundles when core files are generated.

i Note: Using this command does not change settings configured for reports and alerts in the vmPRO appliance GUI. See [Configuring Reports, Alerts, and Autosupport for a vmPRO Appliance](#)

vmPRO Console Commands – cbt

Use the Changed Block Tracking (**cbt**) command to reset the base disk's last modified time to the current time. See [vSphere Changed Block Tracking Support](#).

cbt command

cbt reset [all] | [<hypervisor> <vm name> | folder <folder>]

Use to reset the base disk's last modified time to the current time. With this command, you can reset all virtual machines (VMs) on the vmPRO appliance, or specify an individual VM within a specific folder.

vmPRO Console Commands – config

Use the **config** command to configure your appliance's system date and time, as well as to create a new HTTPS SSL certificate for your appliance.

i Note: You will configure most settings for your vmPRO appliance using the vmPRO GUI or the VMware vSphere Client Console Configuration Wizard. See [vmPRO Setup and Configuration](#).

config commands

config set date MM/DD/YYYY HH:MM[:SS]

Use to set the system date and time.

config set time zone <timezone>

Use to set the system time zone.

vmPRO uses standard time zone names, such as US/Pacific, Asia/Tokyo, and Europe/Paris. You can view a complete list of time zones on the Quantum Support site. See

<http://www.quantum.com/serviceandsupport/index.aspx>.

config create https-certificate

Use to create a new HTTP SSL certificate for your vmPRO appliance.

i Note: If you have the vmPRO appliance GUI open, refresh the browser for the new certificate to take effect.

vmPRO Console Commands – fileys

Use the **fileys** commands to list file systems within the defined parameters.

fileys commands

fileys find <search-term> | vmx | vmdk

Use to list known files and directories.

- **<search term>** – Use this argument to limit listings by the term entered. The **<search-term>** argument can be the whole file or directory name, or part of the file or directory name.
- **vmx** – Use this command argument to list every **.vmx** file.
- **vmdk** – Use this command argument to list every **.vmdk** file.

Example

```
fileys find quantum
/export/192.168.1.110/quantum-4/
/export/192.168.1.110/quantum-4/quantum-4.vmx
/export/192.168.1.110/quantum-4/quantum-4.vmdk
/export/192.168.1.110/quantum-4/quantum-4-flat.vmdk
```

filesystems list [<export-path>]

Without a specified command argument, use to list everything mounted under the Quantum vmPRO **/export** directory. With an **<export-path>** argument, use to list only what is mounted in that path.

Example

```
filesystems list /export/192.168.201.10
```

vmPRO Console Commands – group

Use the **group** commands to configure vmPRO groups for your network. See [vmPRO Group Configuration](#).

group commands

group status

Use to view the vmPRO appliance's current group membership.

group create master

Use to make the current vmPRO appliance the master appliance for the group.

group join <master>

Use to add the current vmPRO appliance to the group with the master identified in the **<master>** argument.

group leave

Use to remove the current vmPRO appliance from its current group.

If the appliance is the group's master, you cannot remove it until all other appliances have been removed from the group.

group update master <master>

Use to update the group master's new IP address/host name for the current vmPRO appliance.

Run this command only after **net set hostname** is run on the group master.

vmPRO Console Commands – help

Use the **help** command to list a summary of top-level commands. Enter a command argument to list all command options for the argument.

help commands

help

Use to list a summary of available top-level commands.

help <command argument>

Use to list all command options for the defined **<command argument>**.

Example

```
quantum:bsmith> help ssh
showing commands that start with 'ssh':
  ssh disable
  ssh enable
  ssh status
```

i **Note:** To list all of an argument's options, you can also enter the **<command argument>** without using the **help** command. For example, you can enter **ssh** to receive the same response as you do when you enter **help ssh**.

vmPRO Console Commands – import

Use the **import** commands during a single-step recovery from the **/import** directory.

import commands

import mkdir <directory-name>

Use to create a directory under the **/import** directory.

import rmdir <directory-name>

Use to remove the directory from the **/import** directory.

import edit <cfg-file>

Use to edit the **cfg** file found in the **/import** directory, such as **/import/my_directory/vmname.cfg**.

import show errors <directory-name>

Use to list all error files (**.err**) in the **/import** directory, as well as all errors within the **.err** files.

import list

Use to list all files and directories within the **/import** directory.

vmPRO Console Commands – log

Use the **log** commands to access vmPRO logs.

log commands

log list

Use to list all Quantum vmPRO logs.

log search <phrase>

Use to search all log files for a character string.

The system handles strings as plain text, meaning that it does not use regular expressions or pattern matching. If the string contains one or more spaces, enclose the string in quotes. Use **Ctrl-C** to exit the command.

log view <log-file>

Use to display the contents of the named log. Use the **log list** command to find log names. Use **Ctrl-C** to exit the command.

log watch <log-file>

Use to display the most recent entries of the named log, and to update the display any time a new message is added to the log. Use **Ctrl-C** to exit the command.

vmPRO Console Commands – nagios

Use the **nagios** commands to enable and disable the Nagios plugin for your vmPRO appliance, as well as to check the status of the Nagios application. For more information about using the Nagios plugin with your vmPRO appliance, see [External Monitoring Support for a vmPRO Appliance](#).

nagios commands

nagios disable

Use to disable the Nagios plugin on your vmPRO appliance.

nagios enable

Use to enable the Nagios plugin on your vmPRO appliance.

nagios status

Use to check the status of the Nagios plugin.

vmPRO Console Commands – net

Use **net** commands to access and monitor network settings, edit network hosts, and initiate or stop a **tcpdump**.

net commands

net hosts add <IP_address> <host-list>

Use to add one or more hosts to your network.

net hosts del <IP_address>

Use to delete a host from your network.

net hosts reset

Use to delete all hosts from your network.

net hosts show

Use to display all hosts for your network.

net nslookup <hostname | IP_address>

Use to check for DNS-to-IP or IP-to-DNS mapping. Use this command for debugging network problems.

net ping <hostname>

Use to confirm a connection between the vmPRO appliance and a host.

net reset

Use to reset network service.

net set hostname <hostname | IP_address>

Use to set a host name or IP address for the vmPRO appliance.

net show config [all]

Use to display the current network driver settings for the Quantum vmPRO Ethernet interface.

net show dhcp

Use to display Dynamic Host Configuration Protocol (DHCP) details.

net show hostname

Use to display the current host name used by the vmPRO appliance.

net show routes

Use to display all entries in the IP routing table.

net show status

Use to display network statistics, including live connections.

net tcpdump start [<tcpdump argument> ...]

Use to begin a **tcpdump** that writes output to a file similar to **tcpdump.2010-09-20.09-54.log**.

Any valid arguments for the **tcpdump** command can be used.

Example

```
net tcpdump start -c 100 executes tcdump -c 100
```

You can run only one **tcpdump** at a time.

net tcpdump stop

Use to stop a running **tcpdump**, and print the file to which the data was being written.

Output files for **tcpdump** commands cannot exceed 8 MB. If a single **tcpdump** file reaches 8 MB in size, the system automatically stops running the command. Older **tcpdump** log files are deleted to make room for new ones.

vmPRO Console Commands – ntp

Use **ntp** commands to configure and monitor the list of Network Time Protocol (NTP) servers that your vmPRO appliance can use to control its internal clock. In addition, use **ntp** commands to activate and deactivate NTP service for your vmPRO appliance, as well as to sync the appliance with its NTP server.

ntp commands

ntp add <server>

Use to add a time server to the list of available NTP servers.

ntp del <server>

Use to delete a time server from the list of available NTP servers.

ntp disable

Use to deactivate the NTP service for your vmPRO appliance.

ntp enable

Use to activate the NTP service for your vmPRO appliance.

ntp reset

Use to read through the list of time servers, and to identify changes to the list of servers.

ntp show

Use to display the list of time servers available to your vmPRO appliance.

ntp sync

Use to synchronize your vmPRO appliance with its assigned NTP server.

vmPRO Console Commands – nw

Use NetWorker (**nw**) commands to access your NetWorker agent.

nw commands

nw install

Use to run the Tivoli Storage Manager (TSM) install script provided by pancetera-integ-networker RPM. You must install this script before using NetWorker.

nw uninstall

Use to uninstall the NetWorker agent.

nw edit servers file

Use to edit the NetWorker server file.

nw set nsrports <number of ports>

Use to set the range of NetWorker's nsrports. The port range begins at 7937.

nw show nsrports

Use to show NetWorker port settings.

nw enable

Use to start the NetWorker agent.

nw disable

Use to stop the NetWorker agent.

nw restart

Use to restart the NetWorker agent.

nw status

Use to show service NetWorker status and network statistics (**netstat -nlp | grep nsrexecd**).

nw save <save arguments>

Use to save files, directories, or entire file systems to the NetWorker server.

nw mminfo <mminfo arguments>

Use to report information about NetWorker media and save sets. The **mminfo** command can produce several different reports, depending on the specified flags.

nw recover <recover arguments>

Use to browse the saved file index and recover selected files from the NetWorker system.

vmPRO Console Commands – smartmotion

Use **smartmotion** commands to control SmartMotion backups from your command console.

smartmotion commands

smartmotion abort [<policy name>]

Use to abort the identified SmartMotion backup.

smartmotion backup [<policy name>]

Use to start the identified SmartMotion backup.

smartmotion set [policy <policy name>] [schedule {never | daily <hr>:<mn>}] [email {enabled | disabled}]

Use to set parameters for a SmartMotion backup policy.

smartmotion show policy [<policy name>]

Use to show the identified SmartMotion backup policy.

smartmotion status [<policy name>]

Use to show the status of the identified SmartMotion backup.

smartmotion sync

Use to start a SmartMotion backup of the default policy.

vmPRO Console Commands – snmp

Use Simple Network Management Protocol (**snmp**) commands to configure SNMP for your vmPRO appliance.

snmp commands

snmp disable

Use to disable SNMP for your vmPRO appliance.

snmp enable

Use to enable SNMP for your vmPRO appliance.

snmp reset rocommunity

Use to reset the read-only community string to **public**.

snmp set rocommunity <community string>

Use to set the read-only community string to the named argument.

snmp status

Use to show whether SNMP is enabled, and to print the current read-only community string.

vmPRO Console Commands – ssh

Use Secure Shell (**ssh**) commands to enable or disable SSH service for vmPRO appliance's network.

ssh commands

ssh disable

Use to disable the SSH service for your vmPRO appliance's network. Attempted logins through SSH fail.

ssh enable

Use to enable the SSH service for your vmPRO appliance's network. By enabling the SSH service, you are allowing SSH logins to your vmPRO appliance.

ssh status

Use to display whether the SSH service is enabled and running, along with the process ID number and all active SSH sessions.

vmPRO Console Commands – system

Use **system** commands to reboot, restart, shut down, or upgrade your vmPRO appliance. You can also use the **system** commands to access system information.

system commands

system reboot

Use to reboot the vmPRO appliance.

system restart services [all]

Use to restart all services for the vmPRO appliance.

system status [all]

Use to view service statuses for the vmPRO appliance.

system show date

Use to display the current system day of the week, date, and time for the time zone.

system show license

Use to display the vmPRO appliance's licenses and associated information.

Example

```
quantum: vmPR5152> system show license
SmartView License Information:
  Expires: in 66 days
  Licensed sockets: 20
```

system show uptime

Use to display the amount of time that has passed since the vmPRO appliance's last reboot.

system show version [detail | all]

Use to display the version numbers of the Quantum components.

The **all** option lists version numbers for all open source packages used by Quantum vmPRO. Updates to the open source packages are included in standard Quantum vmPRO updates.

system shutdown

Use to shut down the vmPRO appliance.

system stackdump controller

Use to create a stack trace of the controller process.

system upgrade [local]

Use to check for Quantum vmPRO updates. If updates are available, the command automatically downloads and installs the updates, which are typically 2 MB.

The automatic system upgrade process uses port 443 and opens updates.quantum.com. If your system uses a firewall, you may need to change your port settings, as appropriate. The process uses signed, private key/public key encryption to verify and authenticate the updates.

The process does not update an open GUI. To see updates in a GUI, close the browser and start a new instance of the vmPRO appliance GUI.

Use the **local** argument to manually perform a system upgrade. Before performing a manual upgrade, you need to manually copy the upgrade files to the upgrade directory. After copying the files to the upgrade directory, you can run the **system upgrade local** command to manually upgrade your vmPRO. See [Installing vmPRO Software Updates Offline](#).

vmPRO Console Commands – tsm

Use the Tivoli Storage Manager (**tsm**) commands to install and control the TSM client service from your vmPRO appliance's console.

tsm commands

tsm install

Use to run the TSM install script provided by the Quantum RPM. You must install this script before using TSM.

tsm edit dsmsys

Use to edit the TSM **dsm.sys** file.

tsm edit dsmopt

Use to edit the TSM **dsm.opt** file.

tsm dsmc <dsmc arguments>

Use to run the **dsmc** command to back up and restore data from TSM.

tsm enable

Use to enable the installed TSM client service.

tsm disable

Use to disable the installed TSM client service.

tsm status

Use to view the status of the installed TSM client service.

tsm restart

Use to restart the installed TSM client service.

vmPRO Console Commands – vss

Use the Volume Shadow Copy Service (**vss**) commands to list virtual machines (VMs) being backed up with VSS, as well as to control log truncation for VMs with completed VSS backups.

vss commands

vss query

Use to list all virtual machines (VMs) waiting for the VSS backup to complete.

vss backup complete [query | all | <vm uuid>]

Use to perform log truncation on VMs with a completed backup.

Use the **query** argument to list VMs that are waiting for log truncation.

Specific VM

To run log truncation for a specific VM from the returned list, enter the list number of the VM.

All VM s

To run log truncation on all listed VMs, use the **all** argument.

VM UUID

To run log truncation for a VM using its universally unique identifier (uuid), use the **<vm uuid>** argument.

vss backup fail [query | all | <vm uuid>]

Use to remove VMs with a completed backup from the log truncation waiting list.

Use the **query** argument to list VMs that are waiting for log truncation.

Specific VM

To remove a specific VM from the log truncation waiting list, enter the list number of the VM.

All VMs

To remove all listed VMs from the log truncation waiting list, use the **all** argument.

VM UUID

To remove a VM from the log truncation waiting list using the VM's universally unique identifier (uuid), use the **<vm uuid>** argument.

External Monitoring Support for a vmPRO Appliance

You can use external monitoring applications for the devices in your vmPRO environment to catch issues that require administrative attention. Quantum vmPRO supports the following external monitoring applications.

Simple Network Management Protocol (SNMP)

You can use SNMP version 2c for external read-only monitoring of your vmPRO environment. SNMP allows access to any object in a system's branch of a tree within your vmPRO environment. Configure SNMP from your vmPRO appliance's **Client** console. For a list of vmPRO-supported SNMP commands, see [vmPRO Console Commands – snmp](#).

In addition, Quantum vmPRO supports the Management Information Base (MIB) II as the information repository for SNMP.

System Statistics MIBs

MIB	Description
.1.3.6.1.4.1.2021.4	Memory
.1.3.6.1.4.1.2021.9	Disks (<i>/</i> , <i>/var</i> , and <i>/var/cores</i> only)
.1.3.6.1.4.1.2021.10	Load
.1.3.6.1.4.1.2021.11	CPU
.1.3.6.1.2.1.1	System information, such as uptime.
.1.3.6.1.2.1.2.0.0.0.2	Interfaces (eth0 only)
.1.3.6.1.2.1.4	Networking

Nagios

For UNIX/Linux systems, you can use Nagios for external monitoring of certain aspects of your vmPRO appliance in addition to SNMP. Use the Nagios remote plugin executor (NRPE) add-on to plug Nagios into your vmPRO appliance.

Use your vmPRO appliance's **Client** console to enable and disable the Nagios plugin for your vmPRO appliance. In addition, you can check the status of the Nagios application from this console. See [vmPRO Console Commands – nagios](#).

Execute monitoring commands from the external Nagios application. Use the following **check_nrpe** plugin with arguments to specify the host address and command:

```
check_nrpe -H <Quantum vmPRO appliance address> -c <command>
```


Supported Commands

Command	Description
<code>check_disk</code>	Check the disk space on the appliance file system.
<code>check_load</code>	Check the system load average over the last 1, 5, or 15 minutes.
<code>check_snmp</code>	Check the status of SNMP on the appliance.