StarWind iSCSI SAN Software: Challenge-Handshake Authentication Protocol (CHAP) for Authentication of Users

www.starwindsoftware.com

COPYRIGHT

TRADEMARKS

CHANGES

The material in this document is for information only and is subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, StarWind Software assumes no liability resulting from errors or omissions in this document, or from the use of the information contained herein. StarWind Software reserves the right to make changes in the product design without reservation and without notification to its users.

TECHNICAL SUPPORT AND SERVICES

If you have questions about installing or using this software, check this and other documents first - you will find answers to most of your questions here or there. If you need further assistance, please contact us.

Table of Contents

Introduction.. 4
Configuring Chap Settings on Server.. 5
Connecting the Target that Use Chap Authentication
(MS iSCSI initiator).. 8
Connecting the Target that Use Chap Authentication
(StarPort)... 15

Guide

Introduction

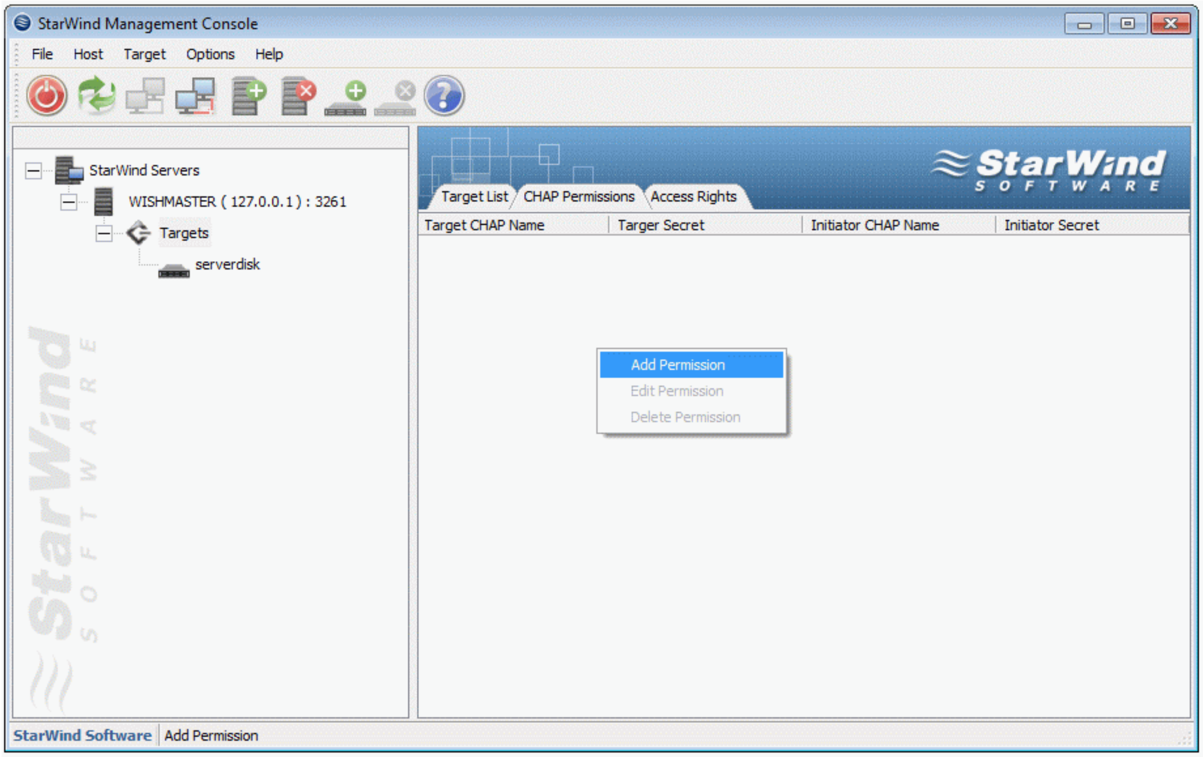
StarWind supports the **Challenge-Handshake Authentication Protocol (CHAP)** for authentication of users. Challenge Handshake Authentication Protocol is a type of authentication in which the authentication agent (typically a network server) sends the client program a random value that is used only once and an ID value. Both the sender and peer share a predefined secret. The peer concatenates the random value (or nonce), the ID and the secret and calculates a one-way hash using MD5. The hash value is sent to the authenticator, which in turn builds that same string on its side, calculates the MD5 sum itself and compares the result with the value received from the peer. If the values match, the peer is authenticated. By transmitting only the hash, the secret can't be reverse-engineered. The ID value is increased with each CHAP dialogue to protect against replay attacks.

You can limit access to all server targets at once or set permissions for each targets separately. If you want limit access to certain targets only and remain other targets shared for all, you need to set permissions for those targets only. Otherwise you may limit access for all targets by setting permissions for connection.

Also you can use one-side authentication or mutual authentication.

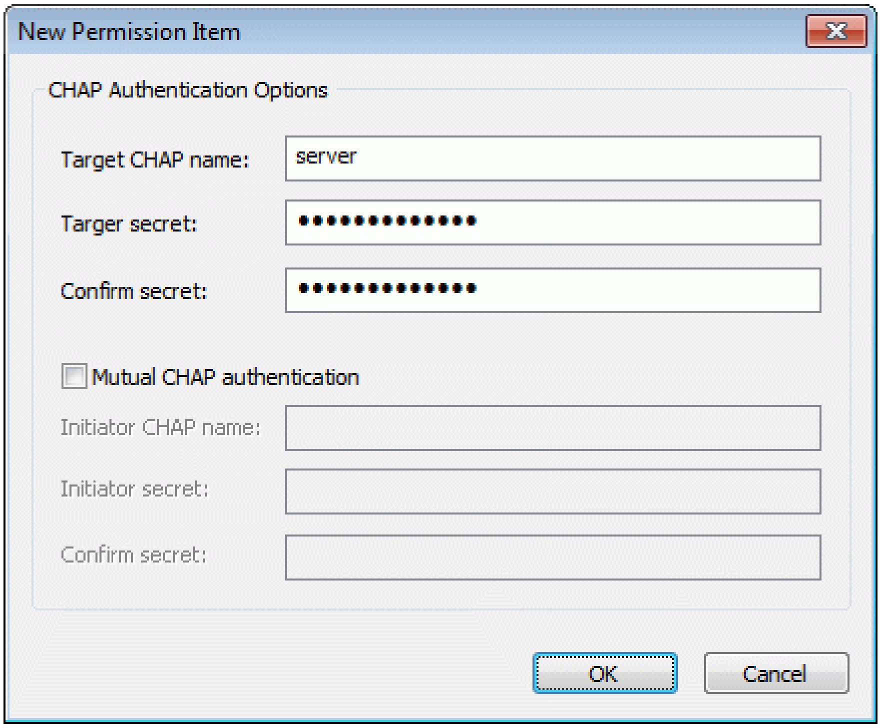
Configuring Chap Settings on Server

Launch the **StarWind** console selecting **Start -> All Programs -> StarWind Software -> StarWind -> StarWind**. After the console is launched its icon appears in the system tray. Double click the icon with the left mouse button or single click it with the right and select **Start Management** pup-up menu item.
From the **StarWind Servers** tree please select the server you want to connect to. Press the right mouse button over the desired host and select the **Connect** popup menu item. You will be prompted to enter the login and password. Default ones are: root, starwind. You can always change them later.
To set global target permissions (which are applied to all targets) connected to the **StarWind Service**, click the **Targets** tree node then click CHAP Permissions tab.



Select **Add Permission** pop-up menu item to continue.

New Permission dialog appears. Specify **Target CHAP name** and **Target secret** only if you want use one-side authentication. If you want use mutual authentication specify also **Initiator CHAP name** and **Initiator CHAP secret**.



New Permission Item

CHAP Authentication Options

Target CHAP name: server

Targer secret: ••••••••••••••

Confirm secret: ••••••••••••••

□ Mutual CHAP authentication

Initiator CHAP name:

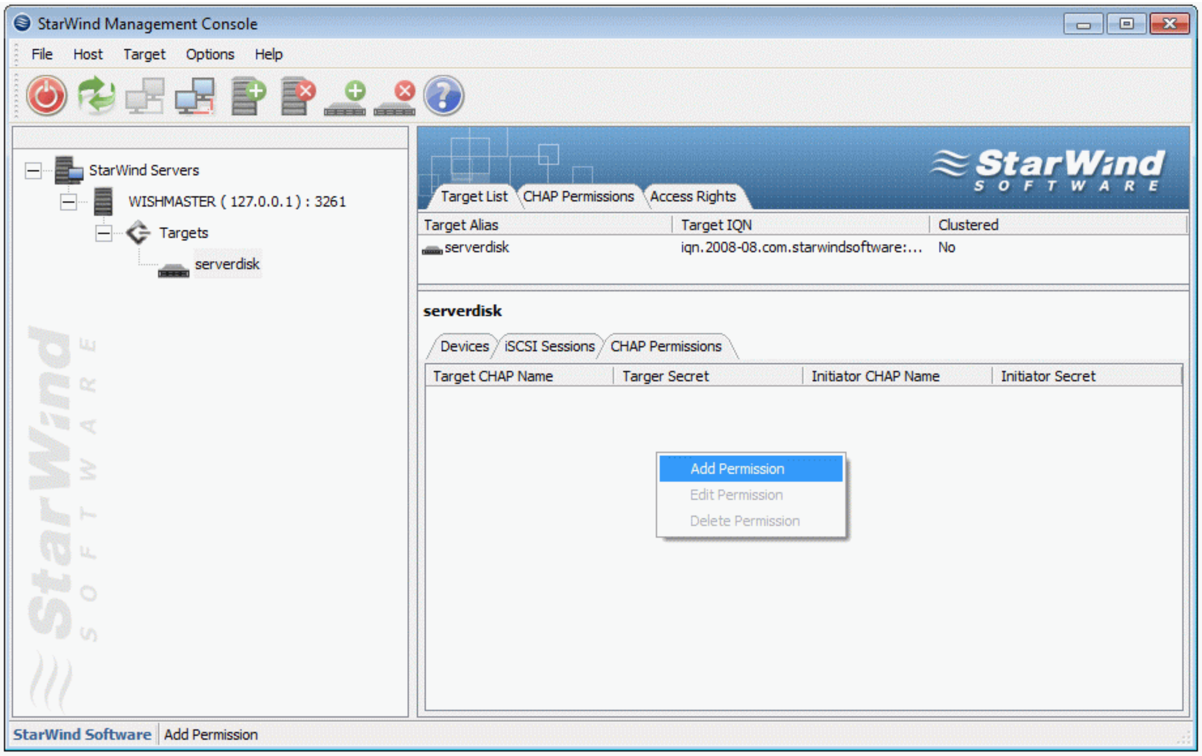
Initiator secret:

Confirm secret:

Press the **OK** button.

You can repeat this step to add permissions as many as you need. Now all clients need to provide CHAP settings to access any target on this server.

To set CHAP settings for certain target not for all targets at once (individual CHAP permissions) you need click on the target then click CHAP Permissions tab of the target.



Target Alias	Target IQN	Clustered
serverdisk	iqn.2008-08.com.starwindsoftware:...	No

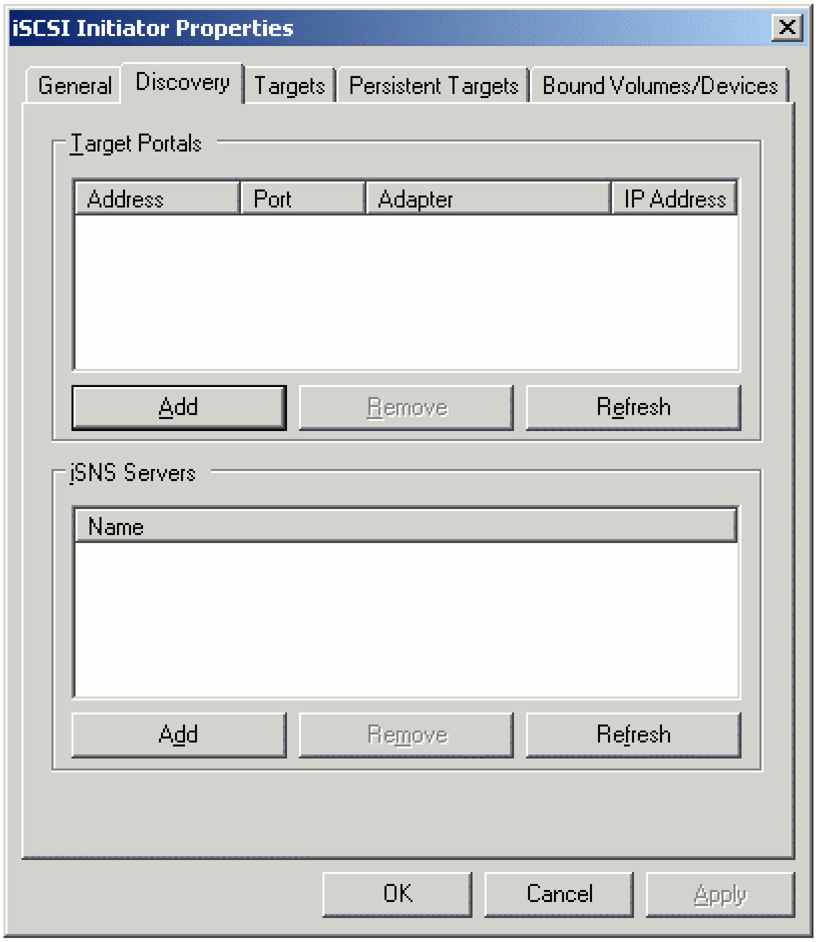
serverdisk

Target CHAP Name	Targer Secret	Initiator CHAP Name	Initiator Secret

The other steps would be the same.

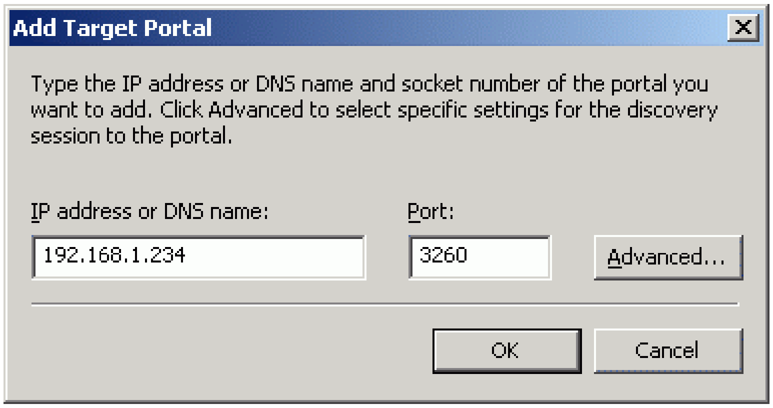
Connecting the Target that Use Chap Authentication (MS iSCSI initiator)

Launch the Microsoft iSCSI Software Initiator application **Start->All Programs->Microsoft iSCSI Initiator-> Microsoft iSCSI Initiator**. Select the **Discovery** Tab. In the **Target Portals** group, click the **Add** button.



Press the **Add** button.

In the **Add Target Portal** dialog enter **IP address or DNS name** of the **StarWind** target server.



Add Target Portal

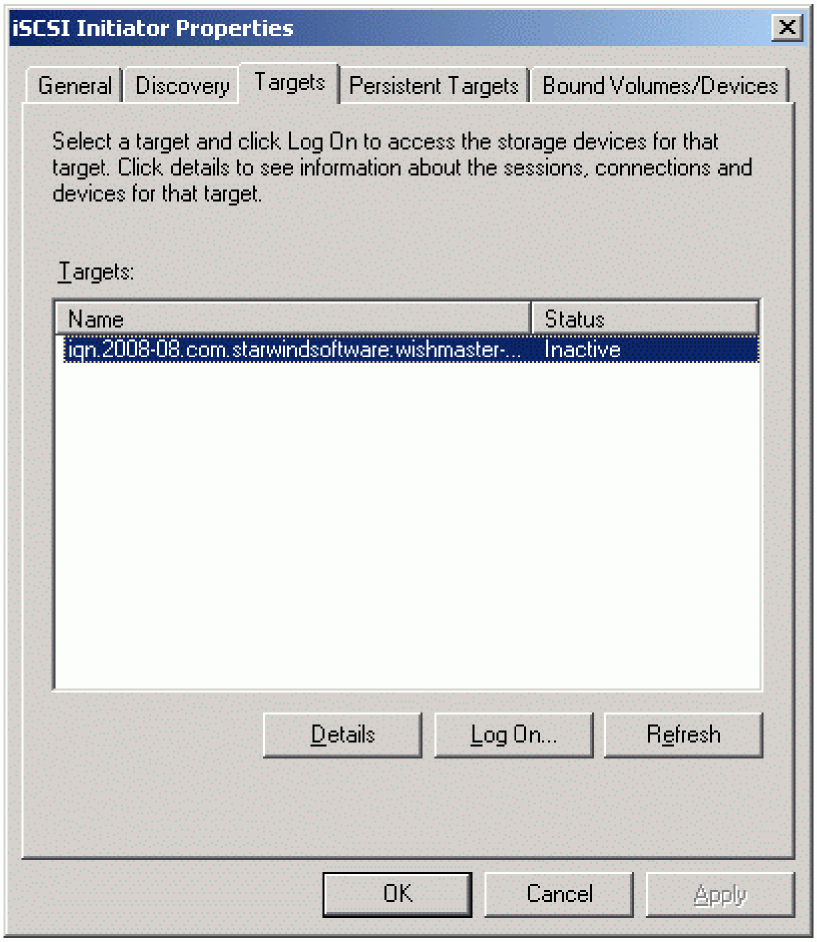
Type the IP address or DNS name and socket number of the portal you want to add. Click Advanced to select specific settings for the discovery session to the portal.

IP address or DNS name: 192.168.1.234

Port: 3260

Press the **OK** button to continue.

Click on the **Targets** tab. Select the IQN of the target just added.



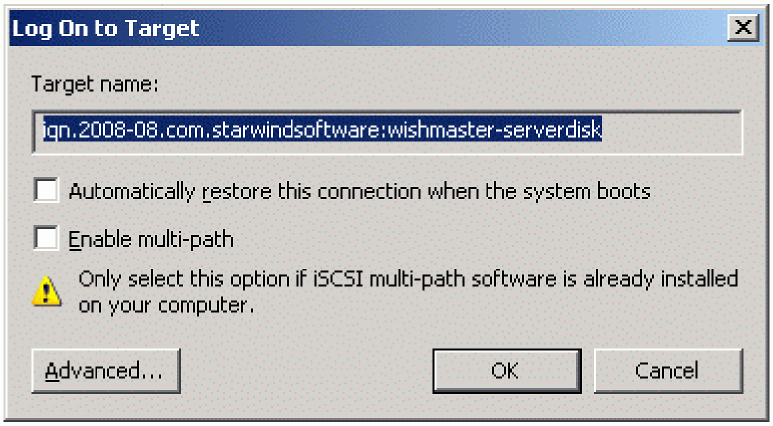
Select a target and click Log On to access the storage devices for that target. Click details to see information about the sessions, connections and devices for that target.

Targets:

Name	Status
iqn.2008-08.com.starwindsoftware:wishmaster-...	Inactive

Press the **Log On...** button.

The **Log On to Target** dialog now appears.



Target name:

iqn.2008-08.com.starwindsoftware:wishmaster-serverdisk

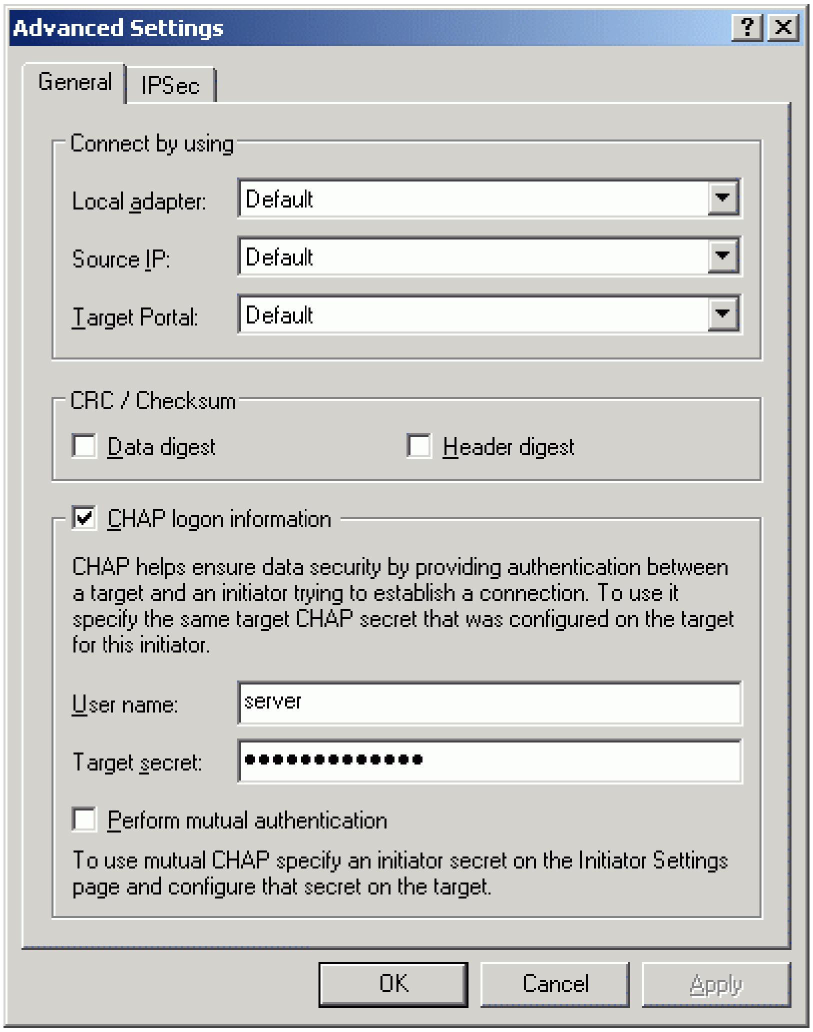
□ Automatically restore this connection when the system boots

□ Enable multi-path

Only select this option if iSCSI multi-path software is already installed on your computer.

Press the **Advanced** button to continue.

Advanced Settings dialog appears. Enter only **Local name** and **Local secret** from StarWind CHAP settings into User name and Target secret fields.



Connect by using

Local adapter: Default

Source IP: Default

Target Portal: Default

CRC / Checksum

□ Data digest □ Header digest

☑ CHAP logon information

CHAP helps ensure data security by providing authentication between a target and an initiator trying to establish a connection. To use it specify the same target CHAP secret that was configured on the target for this initiator.

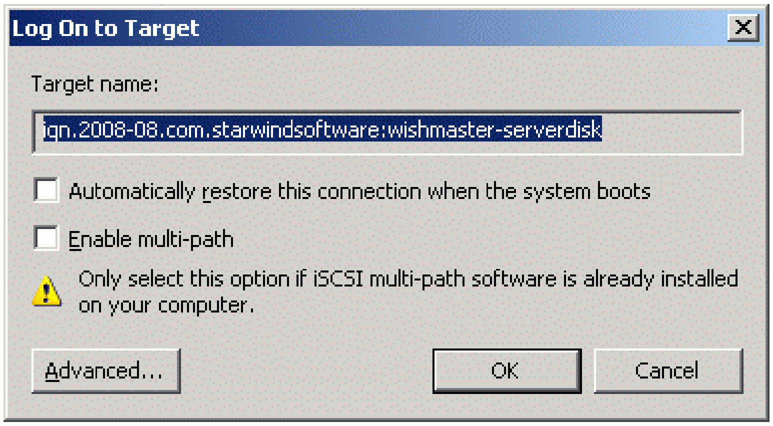
User name: server

Target secret: ••••••••••••••

□ Perform mutual authentication

To use mutual CHAP specify an initiator secret on the Initiator Settings page and configure that secret on the target.

Press the **OK** button to continue.



Log On to Target

Target name:

iqn.2008-08.com.starwindsoftware:wishmaster-serverdisk

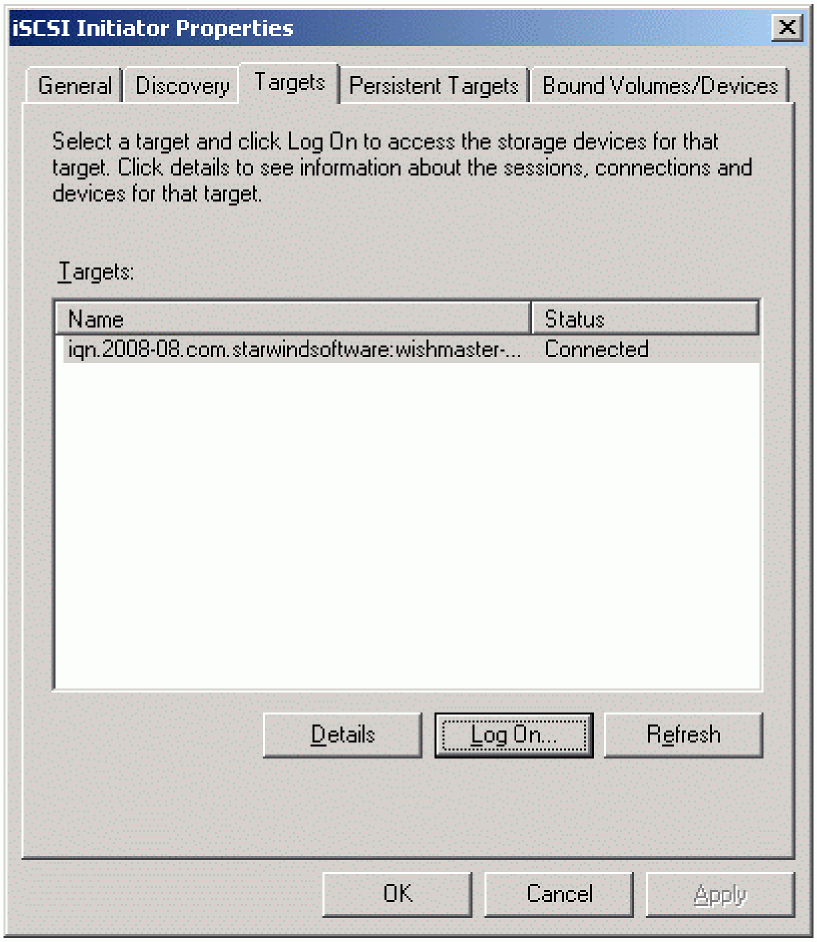
□ Automatically restore this connection when the system boots

□ Enable multi-path

Only select this option if iSCSI multi-path software is already installed on your computer.

Press the **OK** button to continue.

If successful, the initiator is now logged on to **StarWind**.



Select a target and click Log On to access the storage devices for that target. Click details to see information about the sessions, connections and devices for that target.

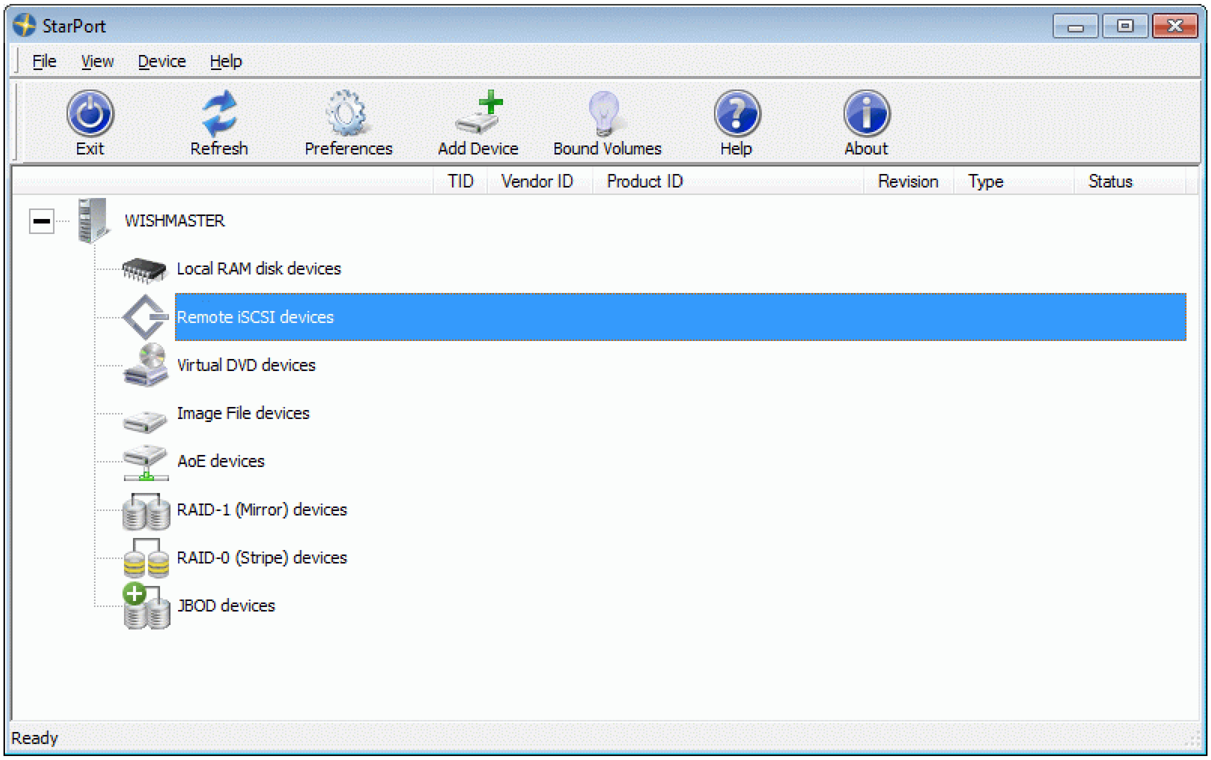
Targets:

Name	Status
iqn.2008-08.com.starwindsoftware:wishmaster-...	Connected

Press the **OK** button to exit the application.

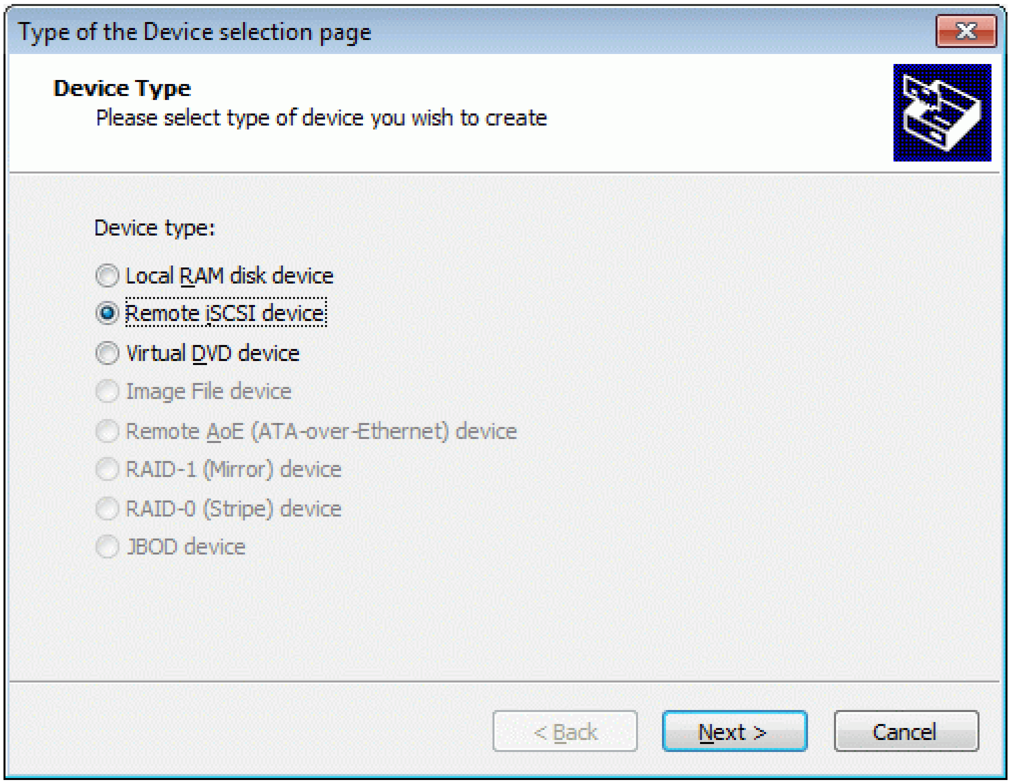
Connecting the Target that Use Chap Authentication (StarPort)

Launch the **StarPort** console selecting **Start -> All Programs -> StarWind Software -> StarPort -> StarPort**. After the console is launched its icon appears in the system tray. Double click the icon with the left mouse button or single click it with the right and select Start Management menu item from the pop-up menu.



Select the **Add Device…** menu item to continue.

New device installation wizard will appears. On this step of Wizard please select **Remote iSCSI device**.



Type of the Device selection page

Device Type

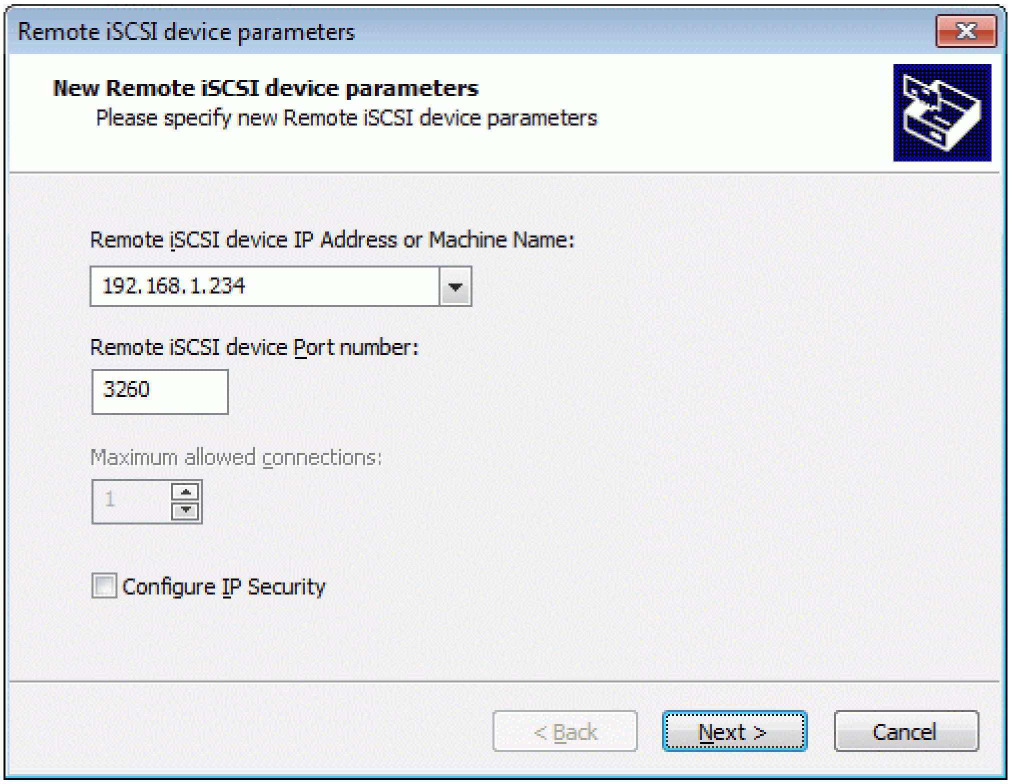
Please select type of device you wish to create

Device type:

- ○ Local RAM disk device
- ● Remote iSCSI device
- ○ Virtual DVD device
- ○ Image File device
- ○ Remote AoE (ATA-over-Ethernet) device
- ○ RAID-1 (Mirror) device
- ○ RAID-0 (Stripe) device
- ○ JBOD device

Press the **Next** button to continue.

Type in the **IP address** of the computer with **StarWind** installed and port of that machine.


Remote iSCSI device parameters

New Remote iSCSI device parameters

Please specify new Remote iSCSI device parameters

Remote iSCSI device IP Address or Machine Name: 192.168.1.234

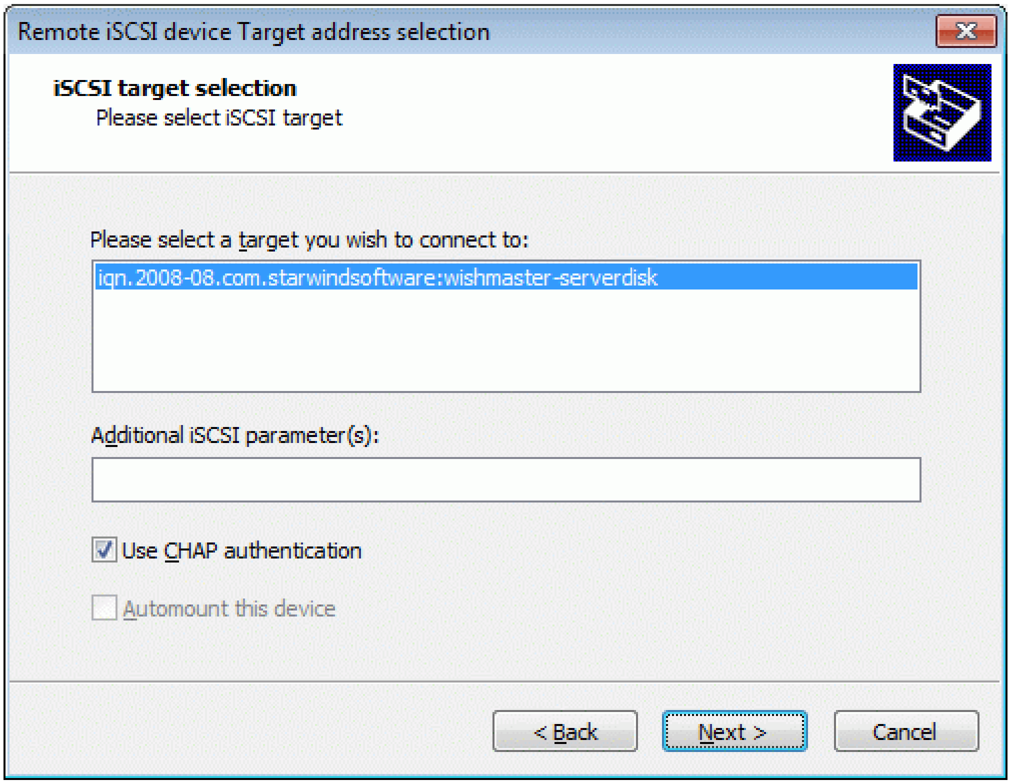
Remote iSCSI device Port number: 3260

Maximum allowed connections: 1

☐ Configure IP Security

Press the **Next** button to continue.

On this step select target from list and check **“Use CHAP authentication”** option.



Remote iSCSI device Target address selection

iSCSI target selection

Please select iSCSI target

Please select a target you wish to connect to:

iqn.2008-08.com.starwindsoftware:wishmaster-serverdisk

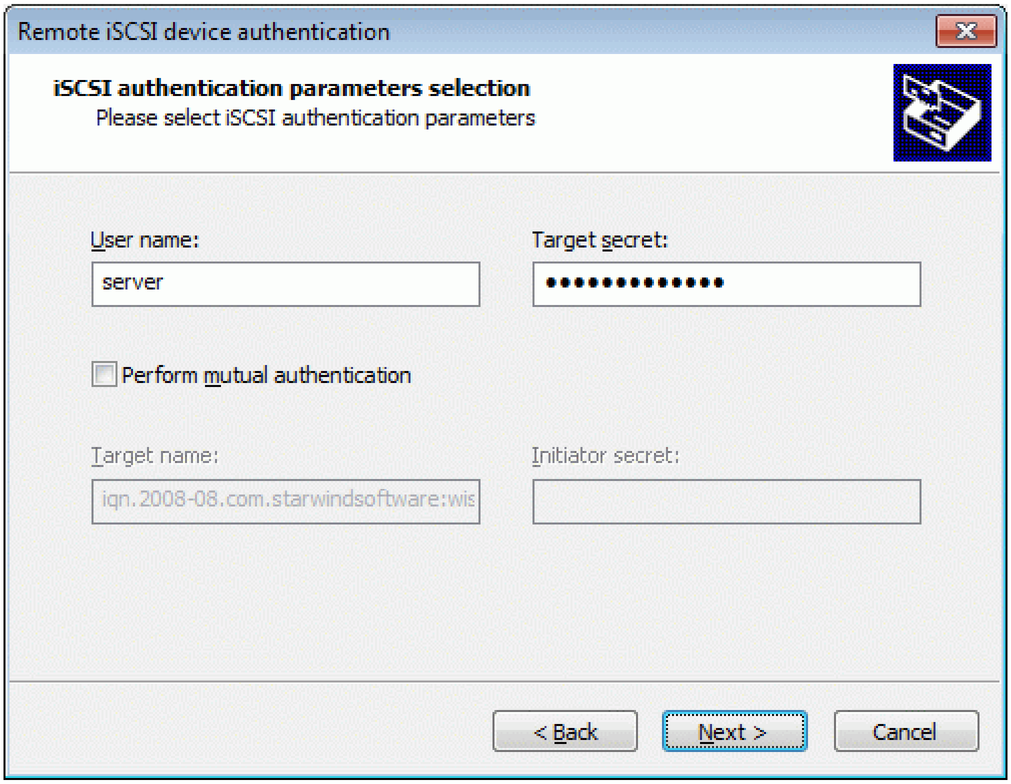
Additional iSCSI parameter(s):

☑ Use CHAP authentication

□ Automount this device

Press the **Next** button to continue.

Provide only **Local name** and **Local secret** from StarWind CHAP settings into first two fields if you want use one-side authentication. If you want use mutual authentication check **Perform mutual authentication** and provide **Peer name** and **Peer secret** into other two fields.



Remote iSCSI device authentication

iSCSI authentication parameters selection

Please select iSCSI authentication parameters

User name: server

Target secret: ••••••••••••••

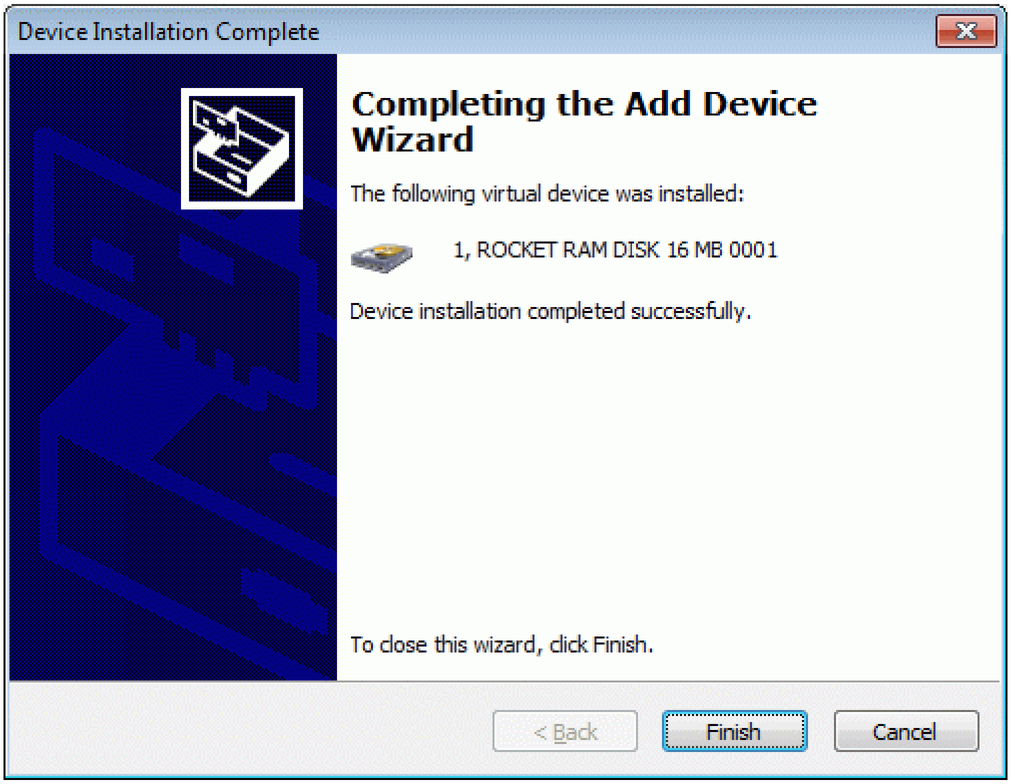
□ Perform mutual authentication

Target name: iqn.2008-08.com.starwindsoftware:wis

Initiator secret:

Press the **Next** button to continue.

The information about the recently connected device is displayed on the last wizard page (see image below). If all names and secrets were provided without errors, target would be connected.



Device Installation Complete

Completing the Add Device Wizard

The following virtual device was installed:

1, ROCKET RAM DISK 16 MB 0001

Device installation completed successfully.

To close this wizard, click Finish.

Press the **Finish** button to exit the wizard. After these steps the device will be accessible from client computer.

Contacts

Support:	www.starwindsoftware.com/support
Support Forum:	www.starwindsoftware.com/forums
Sales E-mail:	sales@starwindsoftware.com

US Headquarters

Direct phone number:	1-617-449-7717
Fax:	1-617-507-5845

EMEA, APAC

Direct phone numbers:	+44-0-2071936727
	+44-0-2071936350
Voice Mail:	1-866-790-2646

StarWind Software Inc.
40 Mall Rd., Burlington
MA 01803, USA
www.starwindsoftware.com