

StarWind iSCSI SAN Software: IP Security policy configuration



www.starwindsoftware.com

Copyright © StarWind Software 2008-2009. All rights reserved.



COPYRIGHT

Copyright © StarWind Software 2008-2009. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent of StarWind Software.

TRADEMARKS

"StarWind", "StarWind Software" and the StarWind and the StarWind Software logos are trademarks of StarWind Software which may be registered in some jurisdictions. All other trademarks are owned by their respective owners.

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 iSCSI Storage	5
Server-Side Configuration, Creating New Ip Security	
Policy	13
Client-Side Configuration, Creatng New Ip Security	
Policy	37
Connecting to the Target Using MS iSCSI Initiator	58
Conclusion	63



Guide

Introduction

This document will help you to configure the IP security policy on Windows 2003 Server for achieving secure connection between Target and Initiator sides. The diagram below illustrates the reference configuration used throughout this document.





Configuring iSCSI Storage

Launch the **StarWind** console selecting **Start -> All Programs -> StarWind Software -> 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 mouse button and select **Start Management** menu item from the pop-up menu.

From the **StarWind Servers** tree please select the server you want to connect to. Press **Connect** button to continue. You will be prompted to enter the login and password. Default ones are: **root**, **starwind**. You can always change them later.

After you have successfully connected to the **StarWind** service press the **Add Target** button to continue.

In the wizard that appears please specify **target name**. Under this **target name**, the device will be declared to the iSCSI initiators connecting to the **StarWind** over an IP network.

nmon target par Specify target alia:	rameters s and target name.
Target Alias:	
filestore 1	
Target Name:	
ign.2008-08.com.	starwindsoftware:wishmaster-filestore1





Select Image File device.

Add Targ	get Wizard
Devi S	ce type elect device type.
۲	Image File device
	Allows to create a virtual hard disk that uses a disk file as its storage medium. The file is a RAW set of all sectors that the virtual hard drive contains.
0	RAM disk device
	Allows to create extremely fast virtual disk that completely resides in random-access memory.
	< <u>B</u> ack <u>N</u> ext > Cancel Help



Select **Create new virtual disk** to create a new hard disk image or **Mount existing virtual disk** to mount an existing image that you've prepared before.

Add Targ	et Wizard
Devic Se	elect device creation method.
0	Mount existing virtual disk Choose existing virtual disk and export it as iSCSI target. Create new virtual disk Create new virtual hard disk and export it as iSCSI target. Create new virtual disk based on Snapshot and CDP one Choose existing Snapshot and CDP virtual disk to create new Image File virtual disk based on it and export it as iSCSI target.
	< <u>B</u> ack <u>Next</u> > Cancel Help



If you have decided to create a new virtual disk, specify the location and the name of the virtual disj you wish to be created. The virtual disk size is specified in megabytes. Refer to the online help for details regarding additional parameters (Fill with zeroes, Compressed and Encrypted).

Add Target Wizard	
Virtual disk parameters Specify virtual disk parameters.	≈
New virtual disk location and name:	
My Computer\C\filestore1.img	•
Size in MBs: 1024	
 Compressed Encrypted User account that will have access to this image 	
Name:	
Password:	
Fill with zeroes	
< <u>B</u> ack <u>Next</u> >	Cancel Help



An Image File device can have additional parameters. Refer to the online help for details regarding the additional parameters (Asynchronous mode, Allow multiple connections (clustering), Read-Only mode and Advanced options).

Add Target Wizard	X
Image File device parameters Specify Image File device parameters.	\approx
Select virtual disk you want to make accessible via iSCSI:	
My Computer\C\filestore1.img	•
Asynchronous mode	
Read-Only mode	
Allow multiple concurrent iSCSI connections (clustering)	
Advanced options	
File system buffering	
Header size in sectors: 0	
< <u>B</u> ack <u>Next</u> Cancel	Help



Check if all of the device parameters are correct. Press the **Back** button if any changes are required.

Add Target Wizard		×
	Add Target Wizard	
	The following device will be added: ImageFile1	
	You specified the following settings: File : My Computer\C\filestore 1.img Asynchronous : Yes Readonly : No Clustering : No	*
		-
	Click Next to add new device.	
	< <u>B</u> ack Next > Cancel Help	,



The information about the recently created device is displayed on the last wizard page (see image below).



Press the **Finish** button to close the wizard.



Server-Side Configuration, Creating New Ip Security Policy

Launch the Local Security Settings management console selecting Start -> Control Panel -> Administrative tools -> Local Security Policy. Local Security Settings management console appears. Switch to the IP Security Policies on Local Computer tree item.

http://www.commenter.com/actions/actio				
Eile Action <u>V</u> iew <u>H</u> elp				
	<u>≤</u> <u>→</u>			
← ← € Image: Constraint of the second	Name A Server (Request Sec Client (Respond Only) Secure Server (Requi	Description For all IP traffic, always req Communicate normally (uns For all IP traffic, always req Greate IP Security Pol Manage IP filter lists a All Tasks Refresh Export List View Arrange Icons Ling up Icons	Policy Assigned No No No	Last Modified Tii 5/5/2009 4:20: 5/5/2009 4:20: 5/5/2009 4:20:
	<	<u>H</u> eib		

Click the right mouse button and select **Create IP Security Policy** option.



IP Security Policy Wizard appears.





Specify the **Name** of the new **IP Security Policy** and optionally provide a brief description of it.

curity Policy Wizard	
P Security Policy Name Name this IP Security policy and provide a brief description	
Na <u>m</u> e:	
SWS IP Security Policy	
Description:	
	A
	Y
< <u>B</u> ack <u>Next</u> >	Lancel



Uncheck the Activate the default response rule option.

P Security Policy Wizard		? ×
Requests for Secure Communication Specify how this policy responds to requests	s for secure communication.	Ē
The default response rule responds to remot other rule applies. To communicate securely secure communication.	e computers that request security, w , the computer must respond to requ	hen no ests for
Activate the default <u>r</u> esponse rule.		
	< <u>B</u> ack <u>N</u> ext>	Cancel



Set the Edit properties option.

IP Security Policy Wizard	? ×
	Completing the IP Security Policy Wizard
	You have successfully completed specifying the properties for your new IP Security policy.
	To edit your IP Security policy now, select the Edit properties check box, and then click Finish.
	Edit properties
	To close this wizard, click Finish.
	< <u>B</u> ack Finish Cancel

Press the Finish button.



On the **SWS IP Security Policy Properties** window that appears uncheck the **Use Add Wizard** option.

IP Security Policy Properties		
Constant		
Security it	ales for communicating with (orner computers
' Security rules: IP Filter List	Filter Action	Authentication
□ <dynamic></dynamic>	Default Response	Kerberos <1
•		Þ
A <u>d</u> d	Edit <u>R</u> emove	Use Add <u>W</u> izard
		OK Cance

Press the **Add** button on the Rules tab.



New Rules Properties window appears.

New Rule Properties
Authentication Methods Tunnel Setting Connection Type IP Filter List Filter Action
The selected IP filter list specifies which network traffic will be affected by this rule.
IP Filter Lists:
Name Description
All ICMP Traffic Matches all ICMP packets betw All IP Traffic Matches all IP packets from this
Add Edit <u>R</u> emove
OK Cancel <u>Apply</u>

Press the Add button on the IP Filter List tab.



IP Filter List window appears. Uncheck the **Use Add Wizard** option.

📑 IP Filte	r List			? X
	An IP filter list is composed addresses and protocol	sed of multiple filters. In s can be combined into	this way, multiple sub one IP filter.	nets, IP
<u>N</u> ame:				
StarWin	ıd			
<u>D</u> escript	ion:			<u>A</u> dd
			<u> </u>	<u>E</u> dit
			v	<u>R</u> emove
IP Filter <u>s</u>	;		Πι	Jse Add <u>W</u> izard
Mirrore	d Description	Protocol	Source Port	Destination
1				Þ
			ОК	Cancel

Specify the **Name** of IP Filter and optionally a brief description and press **Add** button.



Filter Properties window appears.

IP Filter Properties
Addresses Protocol Description
Source address:
Any IP Address
Destination address:
My IP Address
Mirrored. Match packets with the exact opposite source and destination addresses.

Specify **Source address** and **Destination address**. To delimit allow connections more strictly in the **Source address** field you can specify IP address of the separate host or subnet.



Switch to the **Protocol** tab.

IP Filter Properties
Addresses Protocol Description
Select a protocol type: TCP
Set the IP protocol port:
 Erom any port
C From this port:
◯ <u>T</u> o any port
 To this port:
3261
Cancel

Specify protocol (**TCP** in our case) and port number (**3261**) and press **OK**. This filter is for **StarWind** management console connections.



New rule appears in the list.

📑 IP Filte	r List			? ×
	An IP filter list is compos addresses and protocol	ed of multiple filters. In s can be combined into	this way, multiple sub one IP filter.	onets, IP
<u>N</u> ame:				
StarWin	d			
	on:			<u>A</u> dd
			<u>^</u>	<u>E</u> dit
			-	<u>R</u> emove
IP Filters:	:			Jse Add <u>W</u> izard
Mirrore Yes	d Description	Protocol TCP	Source Port ANY	Destination 3261
•				Þ
			OK	Cancel

Click the **Add** button again.



Filter Properties window appears.

IP Filter Properties	? ×
Addresses Protocol Description	
Source address:	
Any IP Address	
Destination address:	
My IP Address	
Mirrored. Match packets with the exact opposite source and addresses	destination
	Cancel

Specify Source address and Destination address.



Switch to the **Protocol** tab.

IP Filter Properties
Addresses Protocol Description
Select a protocol type: TCP
Set the IP protocol port:
Erom any port
C From this port:
◯ <u>T</u> o any port
 To this port:
3260
Cancel

Specify protocol (**TCP** in our case) and port number (**3260**) and press **OK**. This filter is for **StarWind** service connections (iSCSI traffic itself).



One more new rule appears in the list.

📑 IP Filte	r List			? ×
	An IP filter list is compos addresses and protocol	ed of multiple filters. In s can be combined into	this way, multiple subr one IP filter.	nets, IP
<u>N</u> ame:				
StarWin	d			
, <u>D</u> escripti	on:			<u>A</u> dd
			<u> </u>	<u>E</u> dit
			•	<u>R</u> emove
IP Filters:			🗖 U	se Add <u>W</u> izard
Mirrore	d Description	Protocol	Source Port	Destination
Yes		TCP	ANY	3261
Yes		TCP	ANY	3260
•				Þ
			OK	Cancel



We return to the **IP Filter List** tab again.

New Rule Properties
Authentication Methods Tunnel Setting Connection Type IP Filter List Filter Action
The selected IP filter list specifies which network traffic will be affected by this rule.
IP Filter <u>L</u> ists:
Name Description
O All ICMP Traffic Matches all ICMP packets betw
O All IP Traffic Matches all IP packets from this
Add <u>E</u> dit <u>R</u> emove
Close Cancel Apply

Select newly created filter **StarWind** from the list and switch to the **Filter Action** tab.



On the Filter Action tab select Require Security option from the list.

New Rule Properties	<u>? ×</u>
Authentication Methods Tu IP Filter List	nnel Setting Connection Type Filter Action
The selected filter action for secure network traft	n specifies whether this rule negotiates ic, and how it will secure the traffic.
Eilter Actions:	
Name	Description
O Permit	Permit unsecured IP packets to
O Request Security (Optional)	Accepts unsecured communicat
Require Security	Accepts unsecured communicat
A <u>d</u> d	<u>R</u> emove □ Use Add <u>W</u> izard
	se Cancel Applu



Require Security Properties window appears. Select **Negotiate security**, specify **Security method preference** order and set **Accept unsecured communication**, but always respond using IPSec option.

Require Secu	rity Properties			? ×
Security Met	nods General			
C Per <u>m</u> it C Block • Negotia Security me	te security:	rder:		
Туре	AH Integrity	ESP Confidential	ES	A <u>d</u> d
Custom Custom	<none> <none> <none></none></none></none>	3DES 3DES DES	SH ME SH	<u>E</u> dit
Custom	<none></none>	DES	ME	<u>R</u> emove
				Move <u>up</u>
•			►	Move d <u>o</u> wn
I A <u>c</u> cept I Allo <u>w</u> u I Use set	unsecured commun nsecured commun ision <u>k</u> ey perfect fr	unication, but always ication with non-IPSe orward secrecy (PFS)	respond (c-aware	using IPSec computers
	[OK (Cancel	Apply



Switch to the **Connection Type** tab.

w Rule Properties			?
IP Filter List	. 1	Filter Actio	n
Authentication Methods	Tunnel Set	ting Conn	ection Type
This rule only a	applies to networl pe.	< traffic over conn	ections of
• All network connections			
C Local area network (LAN	1)		
C <u>R</u> emote access			
	Close	Cancel	Apply

Select All network connections.



Switch to the **Tunnel Setting** tab.

New Rule Properties	<u>? ×</u>
IP Filter List Authentication Methods Tunnel Setting	Filter Action
The tunnel endpoint is the tunneling c IP traffic destination, as specified by th list. It takes two rules to describe an IF	omputer closest to the ne associated IP filter "Sec tunnel.
 This rule does not specify an IPSec tunnel. The tunnel endpoint is specified by this IP addres 0 . 0 . 0 . 0 	955:
Close	ancel <u>Apply</u>

Select This rule does not specify an IPSec tunnel.



Switch to the Authentication Methods tab.

Filter Action Connection Type trust is established ication methods are ting security with anothe
Connection Type v trust is established ication methods are ting security with anothe
) trust is established ication methods are ting security with anothe
bbA
<u> </u>
<u>R</u> emove
Move <u>u</u> p
Move d <u>o</u> wn



Edit Authentication Method Properties window appears. Select Use this string (preshared key) option and type in the preshared key in the field.

dit Authent	ication Metho	od Properti	es		? ×
Authenticatio	on Method				
2	The authenti between the	ication metho computers.	d specifie:	s how trust	t is established
C Active	Directory <u>d</u> efau	lt (Kerberos V	'5 protocol)	
O Use ag	gertificate from t	this certificatio	on authorit	y (CA):	
					Browse
E)	clude the CA n	ame from the	certificate	e request	
	hable certificate	to account r	napping		
🖲 Use thi	s <u>s</u> tring (preshai	red key):			
1231	23				A
					and the second sec
					7
					T



We return to the **Authentication Methods** tab.

IP Filter List		Filter Action
Authentication Metho	ds Tunnel Setting	Connection Type
Authentic between offered ar computer	ation methods specify how computers. These authent nd accepted when negotia	rust is established ication methods are ting security with anothe
uthentication <u>m</u> ethod Method	preference order:	Add
Preshared Key	123123	
		<u> </u>
		<u>R</u> emove
		Move <u>up</u>
		Move d <u>o</u> wr

Press the **Close** button to continue.



Select **StarWind** from the list of available IP Security rules.

5 IP Security Policy	y Properties		1
ules General			
Security ru	les for communicating with o	other computers	
P Security rules:	Filter Action	Authentication	Tu
✓ StarWind	Require Security	Preshared Key	No
<			Þ
A <u>d</u> d	Edit <u>R</u> emove	Use Add <u>W</u>	izaro
		OK Ca	ance

Press the **Close** button.



Assign recently created policy by pressing right mouse button and selecting **Assign** option.

http://www.communicatives.com				
Eile <u>A</u> ction <u>V</u> iew <u>H</u> elp				
	🖹 <u> </u> 🗴			
Security Settings Control Control Con	Name A Server (Request Sec Client (Respond Only) Secure Server (Requi SWS IP Security Policy	Description For all IP traffic, always req Communicate normally (uns For all IP traffic, always req All Tasks ▶ Delete Rename Properties <u>H</u> elp	Policy Assigned No No No No	Last Modified Tii 5/5/2009 4:20: 5/5/2009 4:20: 5/5/2009 3:44: 5/7/2009 3:44:
Assigns this policy (attempts to make it active)	•			Þ



Client-Side Configuration, Creatng New Ip Security Policy

Launch the Local Security Settings management console selecting Start -> Control Panel -> Administrative tools -> Local Security Policy. Local Security Settings management console appears. Switch to the IP Security Policies on Local Computer.

http://www.commons.com/actions				
Eile Action View Help				
	<u>_</u>			
Security Settings	Name A	Description	Policy Assigned	Last Modified Ti
H Account Policies	Server (Request Sec	For all IP traffic, always req	No	5/5/2009 4:20:4
Public Key Policies	Secure Server (Requi	Communicate normally (uns For all IP traffic, always req	No	5/5/2009 4:20:4
🗉 💼 Software Restriction Policies	E Secare Server (Redain	r or airtir trainte, aways req	140	3/3/2007 1.20.
IP Security Policies on Local Computer				
		<u>C</u> reate IP Security Poli	icy	
		Manage IP filter lists a	nd filter actions	
		All Tas <u>k</u> s		•
		Refresh		
		Export List		
		⊻iew		•
		Arrange <u>I</u> cons		•
	•			F
Creates an IP Security policy.	, <u> </u>			

Click the right mouse button and select **Create IP Security Policy** option.



IP Security Policy Wizard appears.





Specify the **Name** of the **new IP Security policy** and optionally provide a brief description.

Security Policy Wizard	?
IP Security Policy Name Name this IP Security policy and provide a brief description	Ē
Na <u>m</u> e:	
SWS IP Security Policy	
Description:	
	<u> </u>
	7
Z Back	



Uncheck the Activate the default response rule option.

IP Security Policy Wizard
Requests for Secure Communication Specify how this policy responds to requests for secure communication.
The default response rule responds to remote computers that request security, when no other rule applies. To communicate securely, the computer must respond to requests for secure communication.
C Activate the default response rule.
< <u>B</u> ack <u>Next></u> Cancel



Set the **Edit properties** option.

IP Security Policy Wizard	? ×
	Completing the IP Security Policy Wizard
	You have successfully completed specifying the properties for your new IP Security policy.
	To edit your IP Security policy now, select the Edit properties check box, and then click Finish.
	Edit properties
	To close this wizard, click Finish.
	< <u>B</u> ack Finish Cancel

Press the Finish button.



On the **SWS IP Security Policy Properties** window that appears uncheck the **Use Add Wizard** option.

IP Security Policy	y Properties	1
ules General		
Security ru	ules for communicating with c	other computers
	-	
P Security rules:		
IP Filter List	Filter Action	Authentication Tu
Comparise	Default Response	Kerberos <n< td=""></n<>
•		Þ
A <u>d</u> d	Edit <u>R</u> emove	Use Add Wizard
		OK Cance

Press the **Add** button on the Rules tab.



New Rules Properties window appears.

New Rule Properties
Authentication Methods Tunnel Setting Connection Type IP Filter List Filter Action
The selected IP filter list specifies which network traffic will be affected by this rule.
IP Filter Lists:
Name Description
All ICMP Traffic Matches all ICMP packets betw All IP Traffic Matches all IP packets from this
Add Edit <u>R</u> emove
OK Cancel <u>Apply</u>

Press the Add button on the IP Filter List tab.



IP Filter List window appears. Uncheck the **Use Add Wizard** option.

📑 IP Filte	r List			? X
	An IP filter list is compos addresses and protocol	sed of multiple filters. In s can be combined into	this way, multiple subr one IP filter.	nets, IP
<u>N</u> ame:				
MS iSC	SI Initiator			
Descripti	ion:			<u>A</u> dd
			<u>_</u>	<u>E</u> dit
			•	<u>R</u> emove
IP Filter <u>s</u>	;		🗖 U	se Add <u>W</u> izard
Mirrore	d Description	Protocol	Source Port	Destination
•				Þ
			ОК	Cancel

Specify the **Name** of **IP Filter** and optionally a brief description and press **Add** button.



IP Filter Properties window appears.

IP Filter Properties
Addresses Protocol Description
Source address:
My IP Address
Destination address:
A specific IP Address
IP add <u>r</u> ess: 192 . 168 . 1 . 10
Subnet mask: 255 . 255 . 255 . 255
Mirrored. Match packets with the exact opposite source and destination addresses.
OK Cancel

Specify **Source address** and **Destination address**. **Destination address** is the IP address of the **StarWind** server you wish to connect to.



Switch to the **Protocol** tab.

IP Filter Properties
Addresses Protocol Description
Select a protocol type: TCP
Set the IP protocol port:
Erom any port
C From this port:
◯ <u>T</u> o any port
 To this port:
3260
Cancel

Specify protocol (**TCP** in our case) and port number (**3260**) and press **OK**. This filter is for **StarWind** service connections (iSCSI traffic itself).



New rule appears in the list.

IP Filter	List			? X
	An IP filter list is compos addresses and protocol	sed of multiple filters. In t s can be combined into	this way, multiple subn one IP filter.	ets, IP
<u>N</u> ame:				
MS iSCS	l Initiator			
Descriptio	on:			<u>A</u> dd
				<u>E</u> dit
			~	<u>R</u> emove
IP Filter <u>s</u> :			🗖 U:	se Add <u>W</u> izard
Mirrored	Description	Protocol	Source Port	Destination
Yes		TCP	ANY	3260
•				Þ
			ОК	Cancel

Press the **OK** button.



We return to the IP Filter List tab again.

Edit Rule Properties	<u>? ×</u>
Authentication Methods Tu IP Filter List	nnel Setting Connection Type
The selected IP filter lis	st specifies which network traffic will be
IP Filter <u>L</u> ists:	
Name	Description
O AILICMP Traffic	Matches allICMPpackets betwe
O All IP Traffic	Matches all IP packets from this
A <u>d</u> d <u>E</u> dit	<u>R</u> emove
Clo	se Cancel <u>Apply</u>

Select newly created filter **MS iSCSI Initiator** from the list and switch to the **Filter Action** tab.



On the Filter Action tab select Require Security option from the list.

New Rule Properties	<u>? ×</u>
Authentication Methods Tur IP Filter List	nnel Setting Connection Type Filter Action
The selected filter actio for secure network traffi	n specifies whether this rule negotiates c, and how it will secure the traffic.
Eilter Actions:	
Name	Description
O Permit	Permit unsecured IP packets to
O Request Security (Optional)	Accepts unsecured communicat
Require Security	Accepts unsecured communicat
A <u>d</u> d	Bemove
Clo:	se Cancel Apply



Require Security Properties window appears. Select **Negotiate security**, specify **Security method preference** order and set **Accept unsecured communication**, but always respond using IPSec option.

Require Secu	rity Properties			? ×
Security Met	hods General			
C Per <u>m</u> it C Block C Negotia Security me	ite security.	order:		
Туре	AH Integrity	ESP Confidential	ES	A <u>d</u> d
Custom Custom	<none> <none> <none></none></none></none>	3DES 3DES DES	SH ME SH	<u>E</u> dit
Custom	<none></none>	DES	ME	<u>R</u> emove
				Move <u>up</u>
•			►	Move d <u>o</u> wn
I A <u>c</u> cept ☐ Allo <u>w</u> u ☐ Use se:	unsecured comm nsecured commur ssion <u>k</u> ey perfect f	unication, but always i nication with non-IPSe orward secrecy (PFS)	respond (c-aware	using IPSec computers
	[ОК	Cancel	Apply



Switch to the **Connection Type** tab.

v Rule Properties	?
IP Filter List	Filter Action Connection Type
This rule only applies to network the selected type.	traffic over connections of
All network connections	
C Local area network (LAN)	
<u>Remote access</u>	
	e 1 + 1
Llose	Lancel Apply

Select All network connections.



Switch to the **Tunnel Setting** tab.

New Rule Properties	<u>? ×</u>
IP Filter List Authentication Methods Tunnel Setting	Filter Action
The tunnel endpoint is the tunneling c IP traffic destination, as specified by th list. It takes two rules to describe an IF	omputer closest to the ne associated IP filter "Sec tunnel.
 This rule does not specify an IPSec tunnel. The tunnel endpoint is specified by this IP addres 0 . 0 . 0 . 0 	955:
Close	ancel <u>Apply</u>

Select This rule does not specify an IPSec tunnel.



Switch to the Authentication Methods tab.

Authentication Methods Tunnel Setting C Authentication methods specify how trust is a between computers. These authentication m offered and accepted when negotiating secu- computer. Authentication method preference order: Method Details Kerberos	Action Connection Typ established hethods are urity with anothe
Authentication methods specify how trust is a between computers. These authentication m offered and accepted when negotiating secu computer.	established nethods are urity with anothe
Authentication <u>m</u> ethod preference order: Method Details Kerberos	
Kerberos	Add
	Edit
	Bemove
	Move <u>up</u>
	Move d <u>o</u> wr



Edit Authentication Method Properties window appears. Select Use this string (preshared key) option and type in the preshared key in the field (the same one as in StarWind IPSec policy).

Edit Authentio	ation Method Properties	<u>? ×</u>
Authentication	n Method	
	The authentication method specifies how trust is between the computers.	established
C Active D C Use a <u>c</u>	Directory <u>d</u> efault (Kerberos V5 protocol) ertificate from this certification authority (CA):	
		Browse
Ego	clude the CA name from the certificate request	
L⊥ <u>En</u>	able certificate to account mapping string (preshared key);	
12312	23	*
	OK	Cancel



We return to the **Authentication Methods** tab.

IP Filter List		Filter Action
Authentication Metho	ds Tunnel Setting	Connection Type
Authentic between offered ar computer	ation methods specify how t computers. These authentic nd accepted when negotiatir	rust is established ation methods are ng security with anothe
uthentication <u>m</u> ethod Method	preference order:	Add
Preshared Key	123123	
		<u>E</u> dit
		<u>R</u> emove
		Move <u>up</u>
		Move d <u>o</u> wr

Press the **Close** button to continue.



Select MS iSCSI Initiator from the list of available IP Security rules.

/S IP Security Policy	Properties		?
Rules General			
Security rule	es for communicating with o	ther computers	
IP Security rules:			
IP Filter List	Filter Action	Authentication	Tu
MS iSCSI Initiator	Require Security	Preshared Key	Ne
•			Þ
<u>Add</u>	Edit <u>R</u> emove		(izard
	OK	Cancel 🔬	pply

Press the **OK** button.



Assign recently created policy by pressing right mouse button and selecting **Assign** option.

🚡 Local Security Settings				
<u>Eile Action View H</u> elp				
	🖹 <u> </u> 🗴			
Security Settings	Name A Server (Request Sec Client (Respond Only) Secure Server (Requi SWS IP Security Policy	Description For all IP traffic, always req For all IP traffic, always req For all IP traffic, always req All Tasks ▶ Delete Rename Properties Help	Policy Assigned No No No	Last Modified Tii 5/5/2009 4:20: 5/5/2009 4:20: 5/5/2009 4:20: 5/7/2009 3:44:
Assigns this colicy (attempts to projectly active)	•			F



Connecting to the Target Using MS iSCSI Initiator

Launch the **MS iSCSI Initiator** by selecting **Start -> All Programs -> Microsoft iSCSI Initiator -> Microsoft iSCSI Initiator**. Switch to the **Discovery** tab. Here you can specify the computer with the **StarWind** installed or **iSNS** server.

iSCSI Initi	ator Prope	rties				×
General	Discovery	Targets P	ersistent Targe	ets Bound	Volumes/Devic	es
_ <u>⊺</u> arge	et Portals —					
Add	lress	Port	Adapter		IP Address	
	Add		<u>R</u> emove	R	<u>e</u> fresh	
 ∣SNS	Servers —					
Nar	ne					
	A <u>d</u> d		Remove	R	e <u>f</u> resh	
			ОК	Cancel	Apply	

Press the **Add** button to continue.



In the appearing dialog type in the **IP address** of the computer with **StarWind** installed and port of that machine

Add Target Portal		×
Type the IP address or DNS name a want to add. Click Advanced to sele session to the portal.	nd socket number o ct specific settings f	f the portal you for the discovery
IP address or DNS name: 192.168.1.10	<u>P</u> ort: 3260	<u>A</u> dvanced
	OK	Cancel



Switch to the Targets tab.

iSCSI Initiator Properties	×
General Discovery Targets Persistent Targets Bou	und Volumes/Devices
Select a target and click Log On to access the storage target. Click details to see information about the session: devices for that target.	devices for that s, connections and
Targets:	
Name	Status
▼	▶ R <u>e</u> fresh
OK Cano	el <u>Apply</u>

Select the device you have recently shared and press Log On to continue.



Log On to Target dialog appears.

Log On to Target	×
Target name:	
ign.2008-08.com.starwindsoftware:wishmaster-filestore1	1
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.	Ч
Advanced OK Cancel	

Check any additional parameters of the target you wish to connect. For example **Automatically restore this connection when the system boots** checkbox.

Press the **OK** button to logon to the **StarWind**.



The information about the connection status is displayed on the **Targets** tab (see the image below). If the logon is successful the new iSCSI device will appear in the system after a few seconds.

SI Initiator Propert	ies	
ieneral Discovery 1	argets Persistent Targets Boun	d Volumes/Devices
Select a target and cliv target. Click details to devices for that target.	ck Log On to access the storage de see information about the sessions,	vices for that connections and
Targets:		Status
ign. 2008-08. com. sta	rwindsoftware:wishmaster-filestore1	Connected
	Details	► R <u>e</u> fresh

Press the **OK** button to exit initiator management console.

Conclusion



Contacts

Support:	www.starwindsoftware.com/support	
Support Forum:	www.starwindsoftware.com/forums	
Sales E-mail:	sales@starwindsoftware.com	
US Headquarters		
Phone:	617-449-7717	
Fax:	617-505-5845	
EMEA:	1-888-532-2203	

StarWind Software Inc.

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