

# StarWind Virtual SAN: Feature Configuration Guide for Set Up Challenge-Handshake Authentication Protocol (CHAP)

2024

TECHNICAL PAPERS



## Trademarks

“StarWind”, “StarWind Software” and the StarWind and the StarWind Software logos are registered trademarks of StarWind Software. “StarWind LSFS” is a trademark 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 on the [Technical Papers](#) webpage or in [StarWind Forum](#). If you need further assistance, please [contact us](#) .

## About StarWind

StarWind is a pioneer in virtualization and a company that participated in the development of this technology from its earliest days. Now the company is among the leading vendors of software and hardware hyper-converged solutions. The company’s core product is the years-proven StarWind Virtual SAN, which allows SMB and ROBO to benefit from cost-efficient hyperconverged IT infrastructure. Having earned a reputation of reliability, StarWind created a hardware product line and is actively tapping into hyperconverged and storage appliances market. In 2016, Gartner named StarWind “Cool Vendor for Compute Platforms” following the success and popularity of StarWind HyperConverged Appliance. StarWind partners with world-known companies: Microsoft, VMware, Veeam, Intel, Dell, Mellanox, Citrix, Western Digital, etc.

## Copyright ©2009-2018 StarWind Software Inc.

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.

## Annotation

### Relevant Products

StarWind Virtual SAN (VSAN)

### Purpose

This document outlines the implementation and configuration of the Challenge-Handshake Authentication Protocol (CHAP) authentication within StarWind Virtual SAN targets.

### Audience

This document is intended for IT professionals, system administrators, and network administrators who are responsible for configuring and managing storage solutions within StarWind Virtual SAN.

### Expected Result

The expected result is the successful configuration of CHAP settings in StarWind Virtual SAN. Users should be able to implement CHAP for initiator authentication, ensuring secure access to their storage targets. The document also provides guidance on setting global and individual permissions.

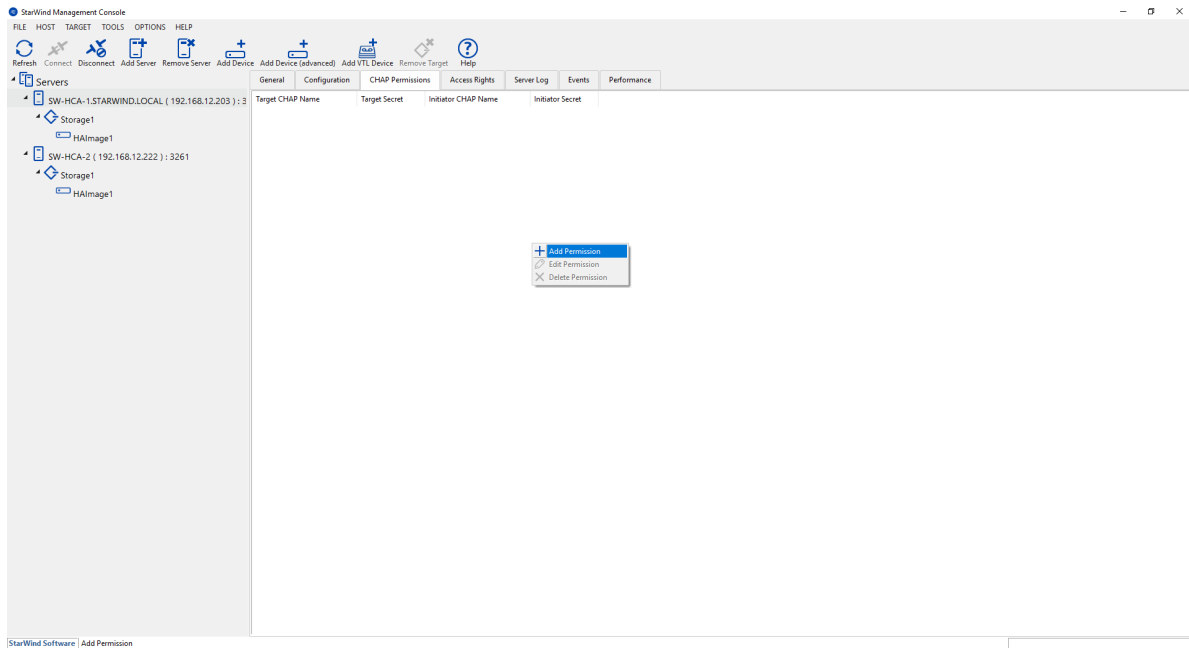
## Configuring Chap Settings In Starwind Management Console

StarWind enables global and individual access CHAP restrictions to targets. Challenge-Handshake Authentication Protocol (CHAP) authenticates a user or network host to an authenticating entity. CHAP provides protection against replay attacks by the peer through the use of an incrementally changing identifier and a variable challenge value. CHAP requires that both client and server know the plain text of the secret, although it is never sent over the network.

NOTE: More information about CHAP can be found [here](#).

### Setting global permissions

1. Select one of the hosts in the StarWind Management Console tree.
2. Click the CHAP Permissions tab. Right-click the main tab area and select Add Permission from the shortcut menu.



3. In New Permission Item, specify the required settings:

- Target CHAP name: is a name used by CHAP for initiator authentication.
- Target secret: is a secret that is used by CHAP for initiator authentication.
- Initiator CHAP name: is a name for the CHAP mutual authentication.
- Initiator secret: is a secret for the CHAP mutual authentication.

**New Permission Item** [X]

CHAP Authentication Options

Target CHAP Name: Target1

Target Secret: ●●●●●●●●

Confirm Secret: ●●●●●●●●

Mutual CHAP Authentication

Initiator CHAP Name: [Empty]

Initiator Secret: [Empty]

Confirm Secret: [Empty]

OK Cancel

Click OK.

4. Check the new CHAP Permission tab.

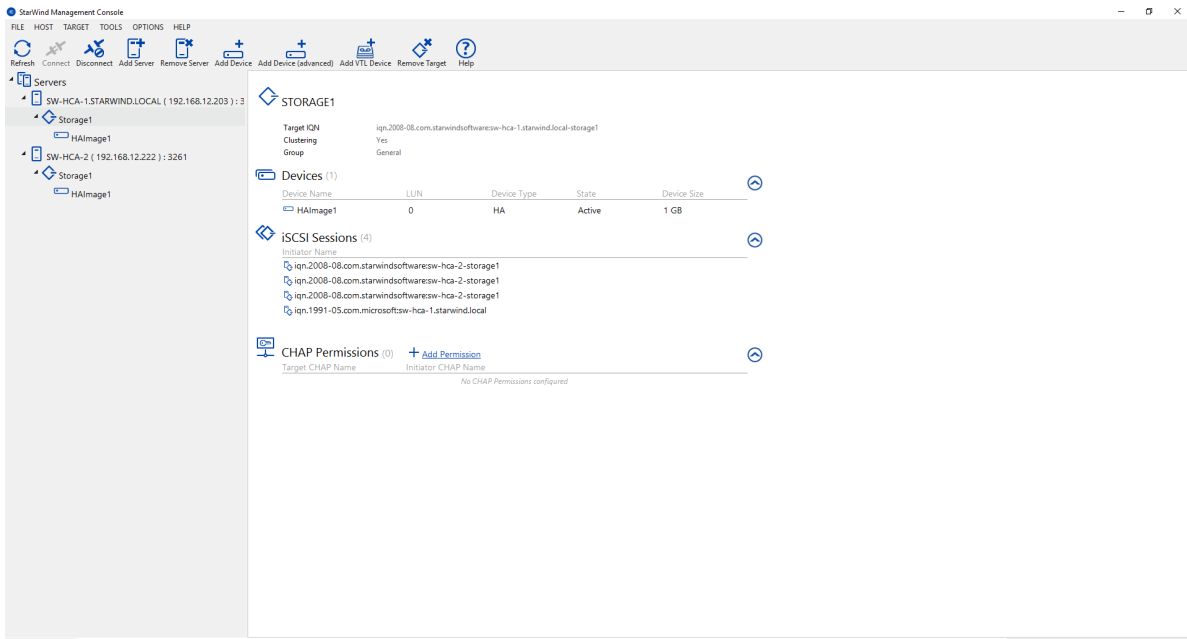
General	Configuration	CHAP Permissions	Access Rights	Server Log	Events
Target CHAP Name	Target Secret	Initiator CHAP Name	Initiator Secret		
Target1	*****				

NOTE: Repeat this step to add as many permissions as needed. Now all clients need to provide CHAP settings to access any target on this server.

NOTE: If the partner authentication settings are not changed, StarWind will not be able to synchronize HA devices to the partner node after the service restart.

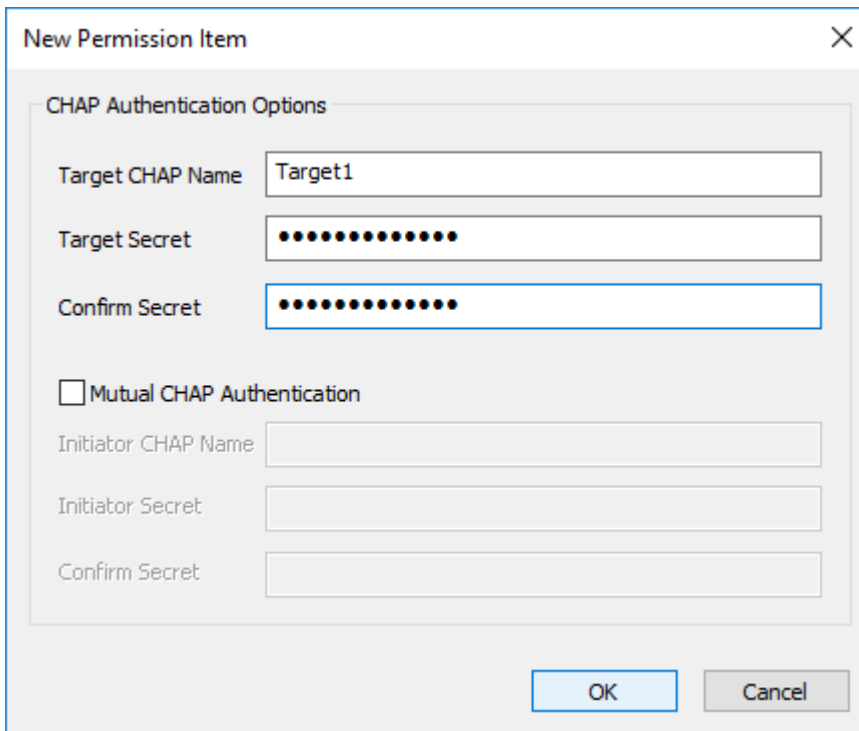
## Setting individual target permissions

1. Select the required target in the StarWind Management Console tree.
2. Click Add Permission in the CHAP Permissions area.



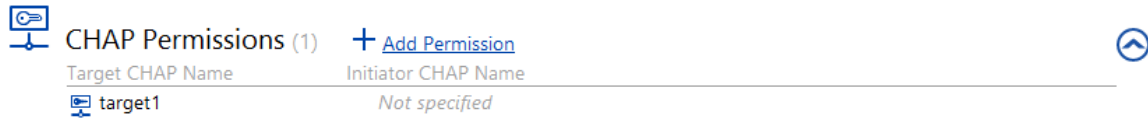
3. In the New Permission Item window, specify the required settings:

- Target CHAP name: is a name used by CHAP for initiator authentication.
- Target secret: is a secret that is used by CHAP for initiator authentication.
- Initiator CHAP name: is a name for the CHAP mutual authentication.
- Initiator secret: is a secret for the CHAP mutual authentication.



Click OK.

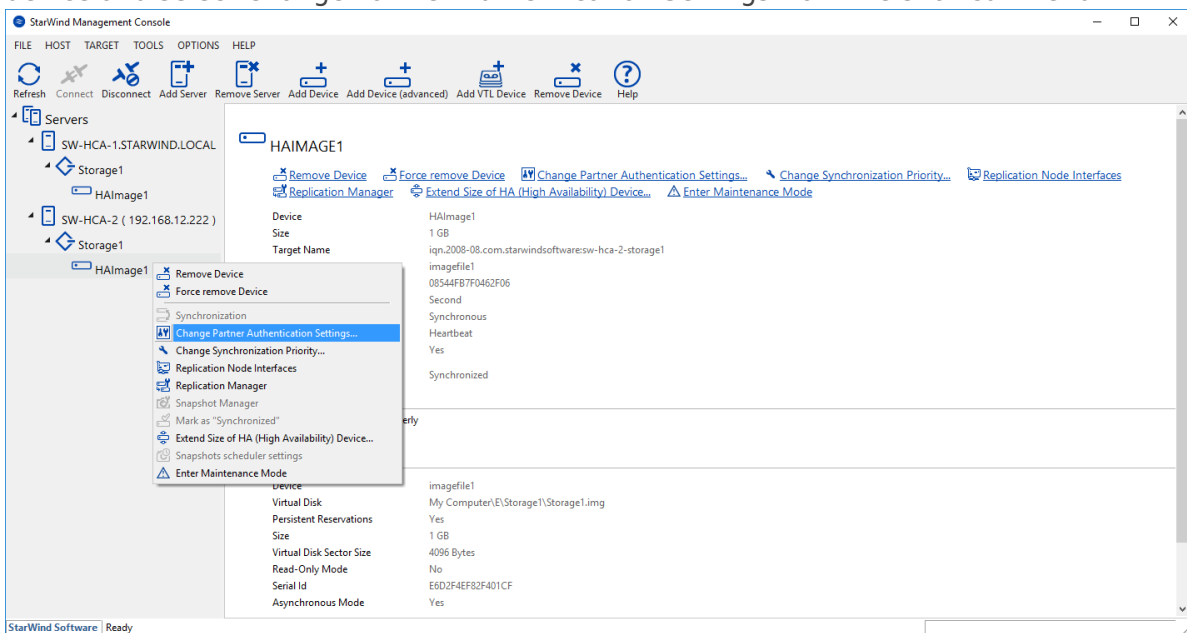
NOTE: Repeat this step to add as many permissions as needed. Now all clients need to provide CHAP settings to access target on this server.



NOTE: If the partner authentication settings are not changed, StarWind will not be able to synchronize HA devices to the partner node after the service restart.

## Setting permissions for HA target

1. Open StarWind Management Console.
2. Choose partner device. Click Change Partner Authentication Settings or right-click the device and select Change Partner Authentication Settings from the shortcut menu.



3. Select CHAP in Authentication Type.

Partner Authentication Settings

### Authentication Parameters

Partner

Authentication Type

Local Name

Local Secret

Peer Name

Peer Secret

4. In

dicating Local Name and Local Secret. Click OK.



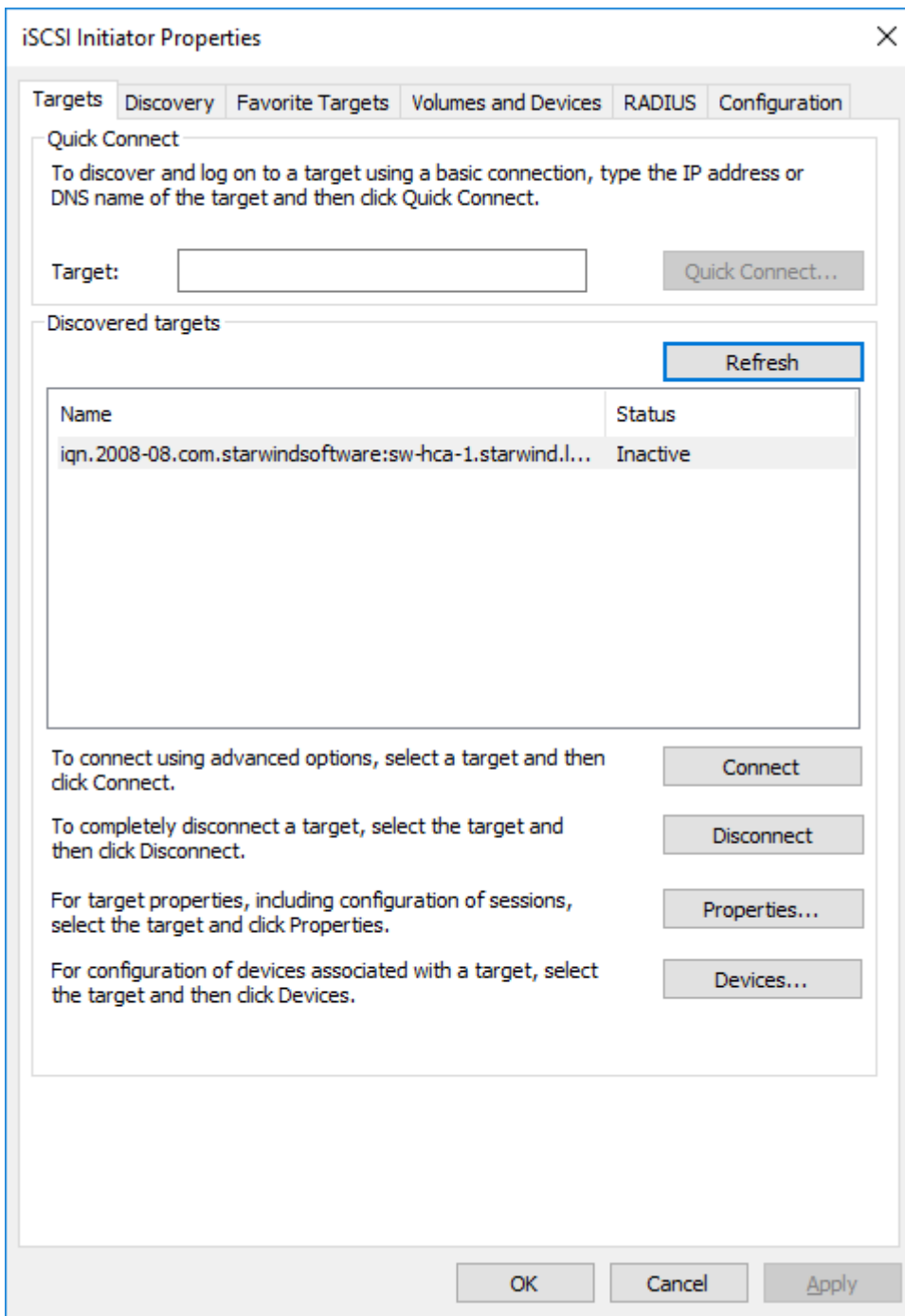
## Selecting The Hypervisor

Please select the required option:

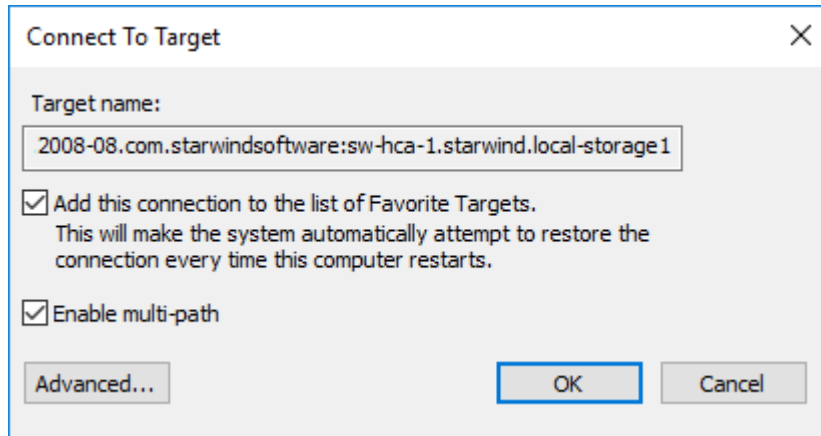
## Configuring Chap Settings On Hyper-V

Setting target permissions

1. Open iSCSI Initiator.
2. Select Target in the Discovered targets area. Click Connect.

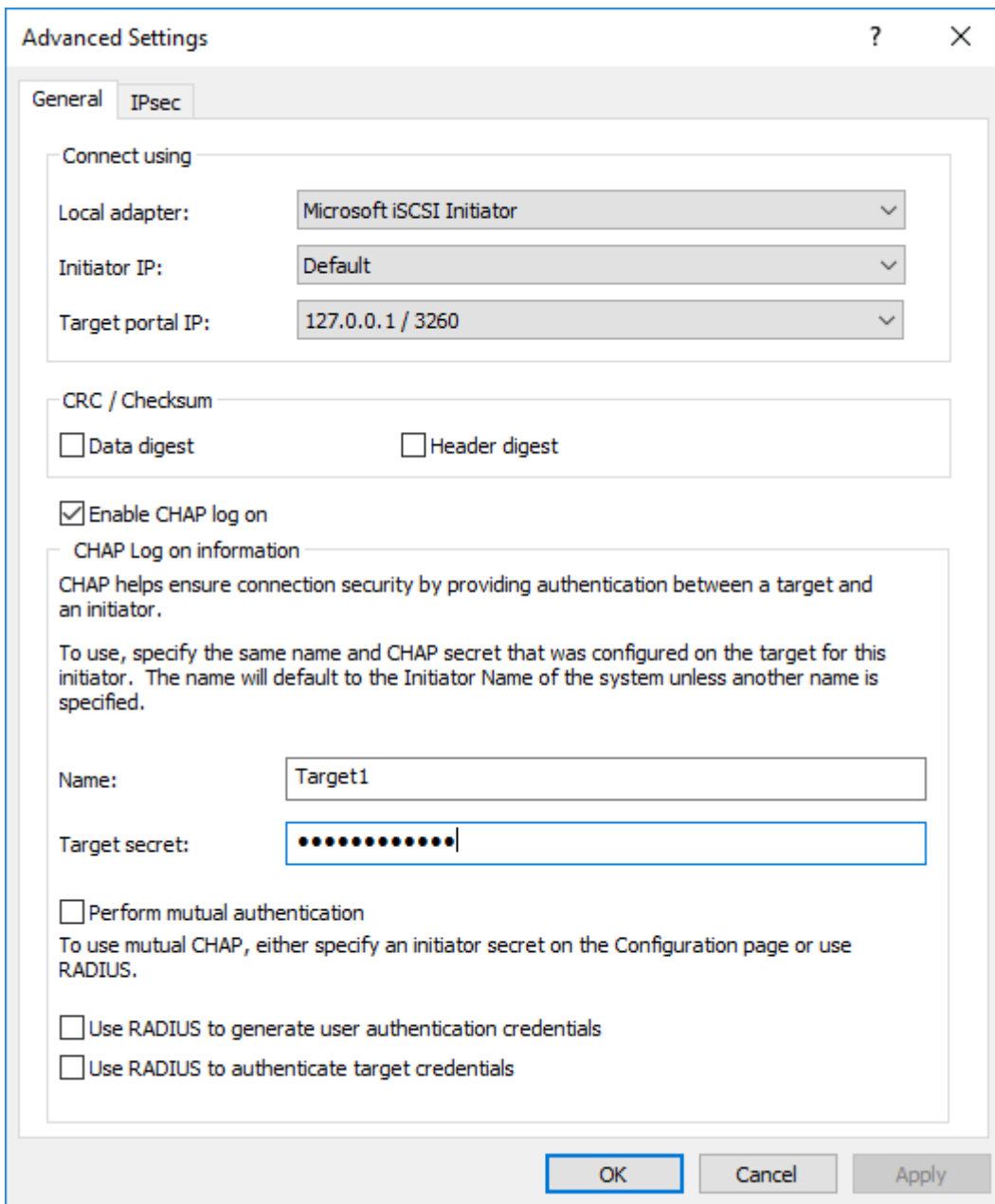


3. Click Advance



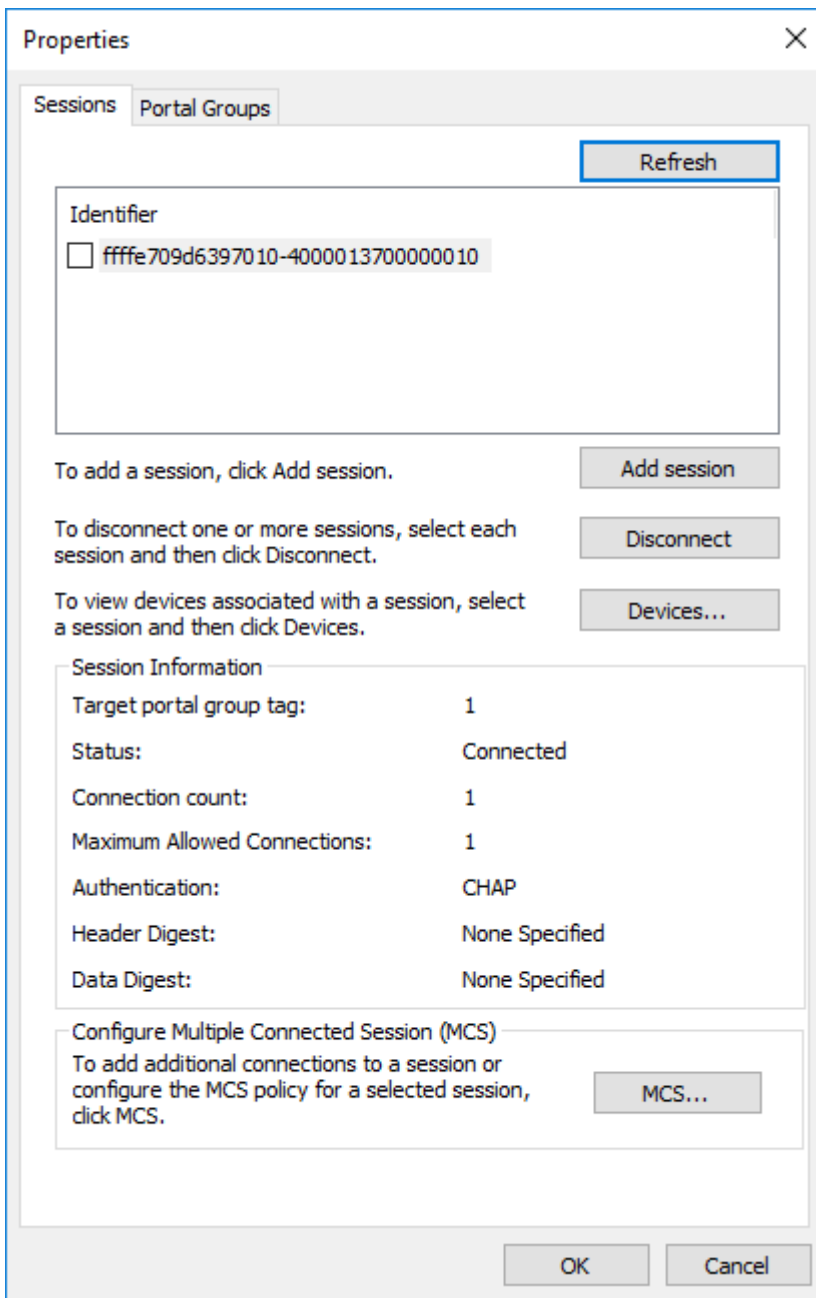
d... 4. To enable CHAP, select the Enable CHAP log on checkbox.

5. Indicate Name and Target secret. Click OK.

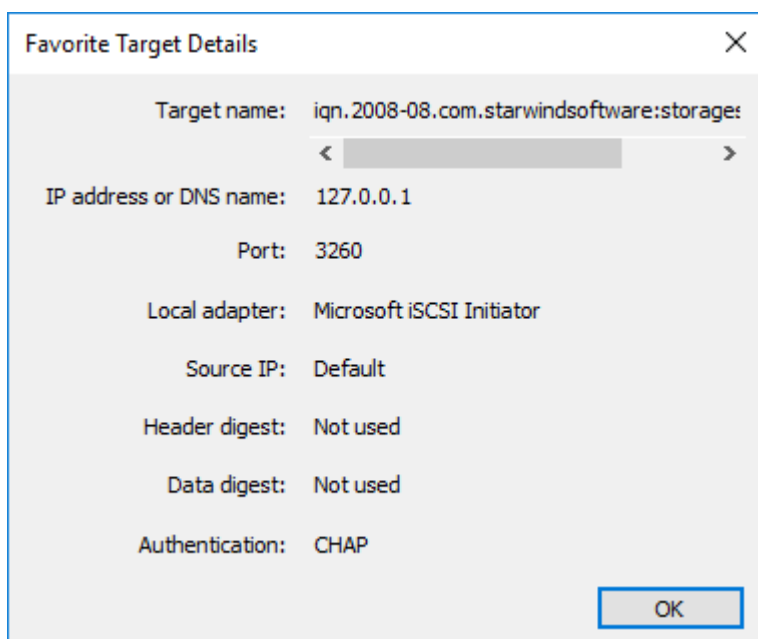


6. Open P

roperties... in the iSCSI Initiator and check Authentication of the connected session.



7. Check Favorite Target

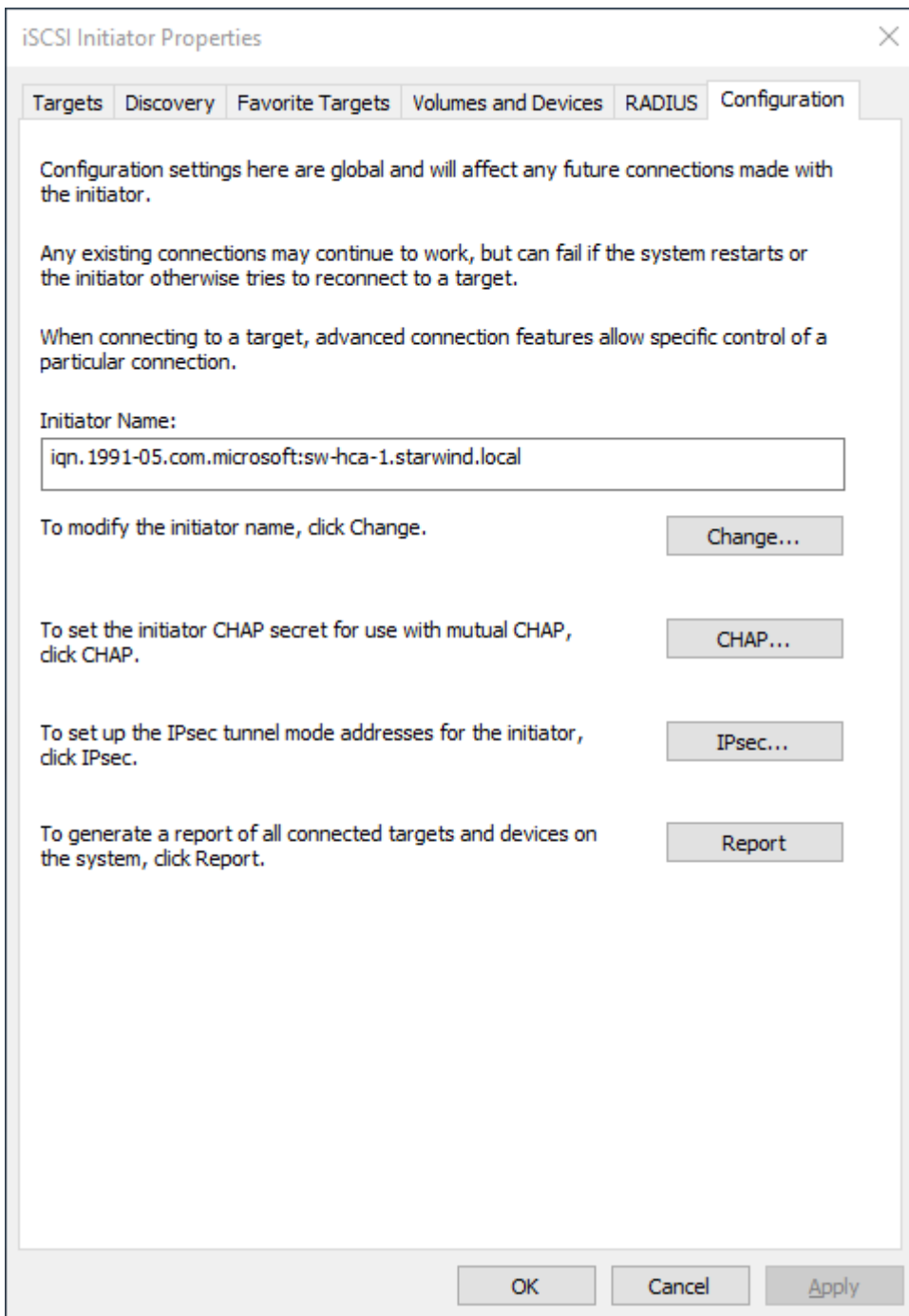


Details.

NOTE: Target will not be reconnected after the service restart in case it does not have CHAP Authentication.

## Changing CHAP initiator configuration

1. Open iSCSI initiator and click Configuration.



NOTE: Click Change... to modify the initiator name. Click CHAP... to set the initiator CHAP secret.

## Configuring Chap Settings On Esxi

1. Click Add dynamic target in Dynamic Targets. Click Edit Settings.

2. Uncheck Inherit from parent.

3. Write Name and Secret in the corresponding fields. Click Save.

4. Click the Save configuration button.

NOTE: Target will not be reconnected after the service restart if it does not have CHAP



Authentication.

## Configuring Chap Settings On Xen

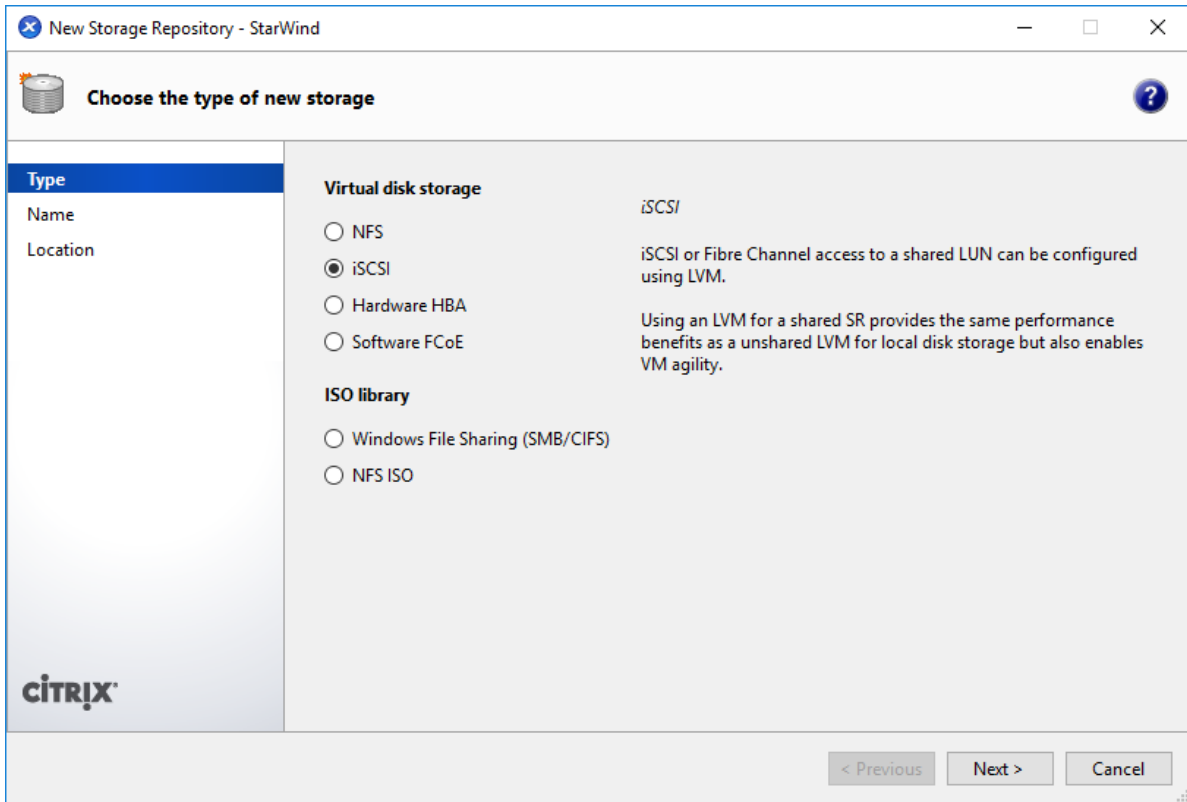
1. Open XenCenter and click on the Server tab. Then select Storage tab and click New SR...

The screenshot shows the 'Storage Repositories' tab in XenCenter. At the top, there are navigation tabs: General, Memory, Storage (selected), Networking, NICs, Console, Performance, Users, and Search. Below the tabs is a header 'Storage Repositories' and a sub-header 'Storage'. A table lists the following storage repositories:

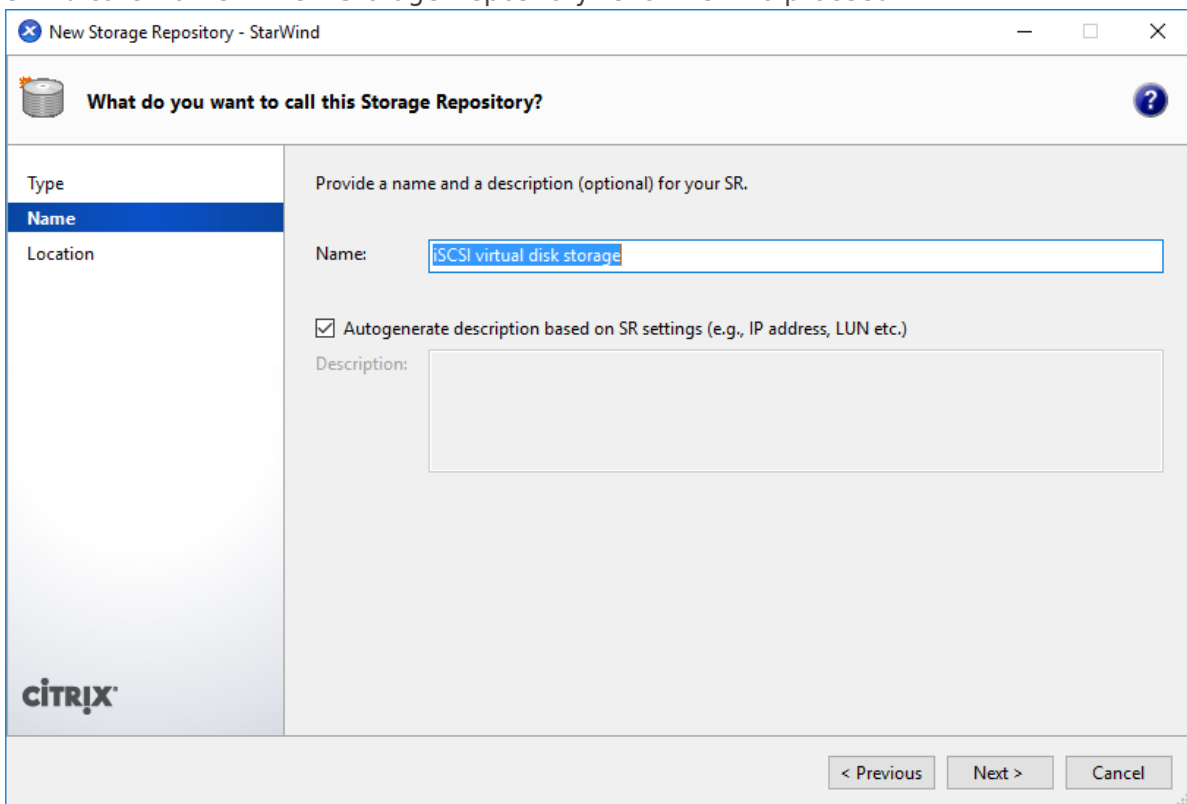
Name	Description	Type	Shared	Usage	Size	Virtual allocation
Local storage on sw-sed...	Local storage on s...	LVM	No	83% (32.1 GB used)	38.5 GB	32 GB
SR1	iSCSI SR [172.16.10...	LVM over iS...	Yes	0% (4 MB used)	1012 MB	0 B
DVD drives on sw-sed-b...	Physical DVD drive...	udev	No	100% (652 MB used)	652 MB	652 MB
SR2		LVM over iS...	Yes	0% (4 MB used)	1012 MB	0 B
Removable storage on s...	Physical removabl...	udev	No	0% (0 B used)	0 B	0 B

At the bottom of the table, there are three buttons: 'New SR...', 'Reclaim freed space', and 'Properties'.

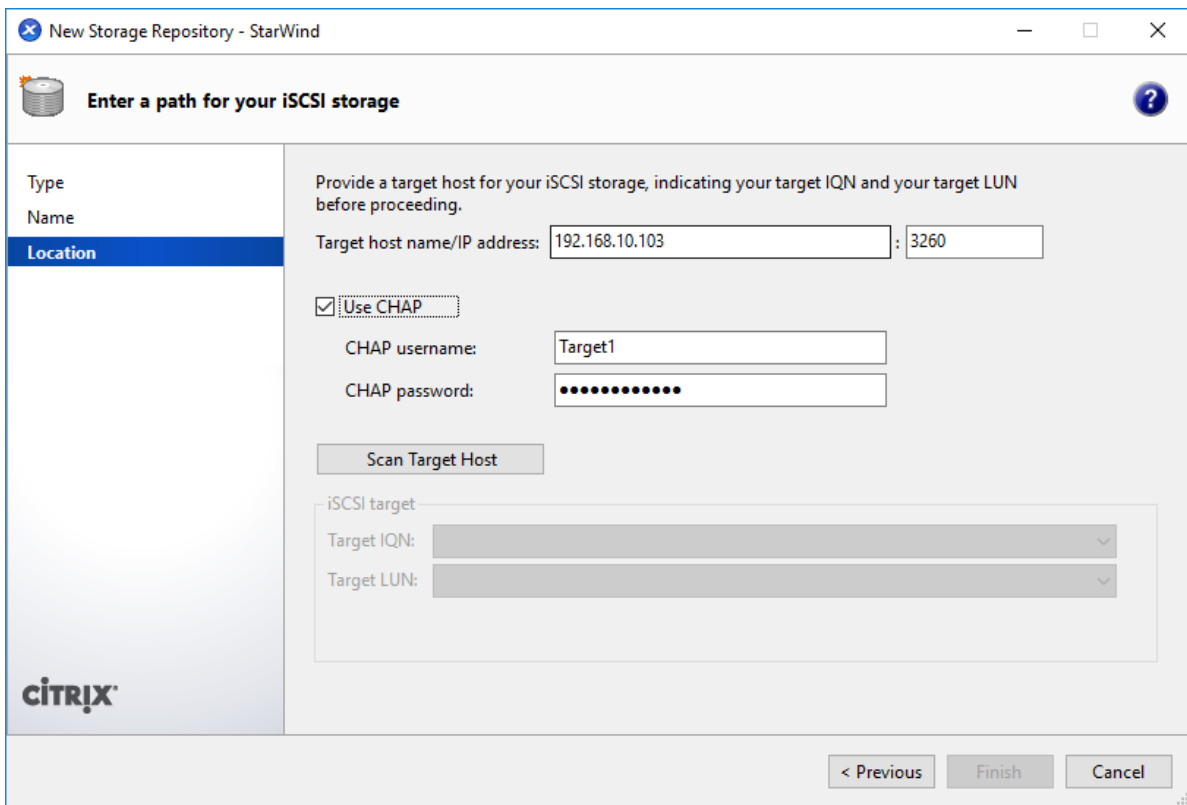
2. Select iSCSI as Virtual disk storage and click Next.



3. Indicate Name in New Storage Repository. Click Next to proceed.










4. Indicate Target host name/IP address and check Use CHAP. Type username and password. Click Finish.



## Conclusion

By implementing CHAP, users can enhance the security of their storage solution by authenticating users or network hosts and protecting against replay attacks. The document covers both global and individual access CHAP restrictions, ensuring that users have the flexibility to configure authentication settings as needed.

## Contacts

US Headquarters	EMEA and APAC
 +1 617 829 44 95	 +44 2037 691 857 (United Kingdom)
 +1 617 507 58 45	 +49 800 100 68 26 (Germany)
 +1 866 790 26 46	 +34 629 03 07 17 (Spain and Portugal)
	 +33 788 60 30 06 (France)

Customer Support Portal: <https://www.starwind.com/support>

Support Forum: <https://www.starwind.com/forums>

Sales: [sales@starwind.com](mailto:sales@starwind.com)

General Information: [info@starwind.com](mailto:info@starwind.com)



StarWind Software, Inc. 100 Cummings Center Suite 224-C Beverly MA 01915, USA  
[www.starwind.com](http://www.starwind.com) ©2024, StarWind Software Inc. All rights reserved.