

CHAP is a Challenge Handshake Authentication Protocol used in iSCSI Target/Initiator to authenticate connection. This authentication can be used in the discovery and Target connections. Discovery authentication is a global security for connection to the iSCSI server. Target authentication gives security only for specific iSCSI Target.

Open-E software supports CHAP authentication in the Target and Initiator.

To create CHAP user you need to use function "Configuration->iSCSI Target Manager->CHAP users (from left panel)->Create new CHAP user" entering his name and secret (it is a password but in this case called a secret). The CHAP secret need to have 12-16 characters and can't contain spaces and few special characters (' " `). The CHAP user name can't contain characters like : ~ ! @ # \$ ^ & () + [] { } * ; : ' " . , % | < > ? / \ = `.

The screenshot displays the Open-E DSS (Data Storage Server) web interface. The top navigation bar includes a 'logout' button, the 'DSS' logo, the title 'DATA STORAGE SERVER', and the 'open-e' logo. Below this, a secondary navigation bar contains tabs for 'SETUP', 'CONFIGURATION' (which is active), 'MAINTENANCE', 'STATUS', and 'HELP'. Under the 'CONFIGURATION' tab, there are sub-tabs: 'volume manager', 'NAS settings', 'NAS resources', 'iSCSI target manager' (which is active), and 'FC target manager'. The left sidebar shows a tree view with 'Targets' (containing 'big' and 'target0') and 'CHAP users' (which is highlighted). The main content area is titled 'Create new CHAP user' and contains three input fields: 'User name:', 'Secret:', and 'Confirm secret:'. A 'create' button is located at the bottom right of the form. At the bottom left of the interface, there is a 'status:' indicator with a red exclamation mark.

Selecting user from CHAP users (from left panel) will allow you to change the user secret or remove him.

The screenshot displays the DSS (Data Storage Server) web interface. The top navigation bar includes a 'logout' button and the title 'DSS DATA STORAGE SERVER' with the 'open-e' logo. Below this, a secondary navigation bar contains tabs for 'SETUP', 'CONFIGURATION' (which is active), 'MAINTENANCE', 'STATUS', and 'HELP'. A third navigation bar shows sub-tabs: 'volume manager', 'NAS settings', 'NAS resources', 'iSCSI target manager' (which is active), and 'FC target manager'.

The main content area is divided into two panels. The left panel, titled 'Targets', shows a tree view with 'big' and 'target0'. Below it, the 'CHAP users' panel shows a list with '1. chap2' and '2. testchap', where 'testchap' is selected. The right panel displays the configuration for the selected 'testchap' user. It includes a header 'CHAP user: testchap', an 'Edit CHAP user' section with input fields for 'New secret:' and 'Confirm secret:', and an 'apply' button. Below that is a 'Remove CHAP user' section with a 'delete' button.

At the bottom left, a 'status:' indicator shows a red exclamation mark.

The global CHAP user used for authenticate discovery can be set in Configuration->iSCSI Target Manager->CHAP user Target access. You need to enable the "Enable CHAP user access authentication" and move CHAP users from available CHAP users list to grand access list. Please note that if no user is on the grand list then no one will be able to connect to the iSCSI server from iSCSI Initiator.

The screenshot displays the DSS (Data Storage Server) web interface. The top navigation bar includes a 'logout' button and the title 'DSS DATA STORAGE SERVER' with the 'open-e' logo. Below this, a secondary navigation bar contains tabs for 'SETUP', 'CONFIGURATION' (highlighted), 'MAINTENANCE', 'STATUS', and 'HELP'. Under the 'CONFIGURATION' tab, there are sub-tabs for 'volume manager', 'NAS settings', 'NAS resources', 'iSCSI target manager' (highlighted), and 'FC target manager'.

The main content area is divided into two sections. The left section, titled 'Targets', shows a tree view with 'big' and 'target0'. The right section, titled 'CHAP user target access', contains the following elements:

- A checkbox labeled 'Target Default Name' which is checked. Below it are input fields for 'Name:' (containing 'iqn.2008-06:11server.targe') and 'Alias:' (containing 'target2'). An 'apply' button is located to the right.
- A section titled 'CHAP user target access' with a checkbox labeled 'Enable CHAP user access authentication' which is checked.
- A table with two columns: 'Available CHAP users:' and 'Grated access CHAP users:'. Each column has a search input field. The 'Available CHAP users:' list contains 'chap2'. The 'Grated access CHAP users:' list contains 'testchap'. Between the two lists are two arrows (one pointing right, one pointing left) for moving users between the lists. An 'apply' button is located at the bottom right of this section.

At the bottom left of the interface, there is a 'status:' indicator with a red exclamation mark.

The Target CHAP user can be set in Configuration->iSCSI Target Manager->Targets-><your target alias> ->CHAP user target access. You need to enable the "Enable CHAP user access authentication" and move CHAP users from available CHAP users list to grand access list. Please note that if no user is on the grand list then no one will be able to connect to the iSCSI involved Target from iSCSI Initiator.

The screenshot shows the DSS (Data Storage Server) web interface. The top navigation bar includes 'logout', 'DSS', 'DATA STORAGE SERVER', and 'open-e'. Below this is a secondary navigation bar with tabs: 'SETUP', 'CONFIGURATION' (selected), 'MAINTENANCE', 'STATUS', and 'HELP'. Under 'CONFIGURATION', there are sub-tabs: 'volume manager', 'NAS settings', 'NAS resources', 'iSCSI target manager' (selected), and 'FC target manager'.

The left sidebar shows a tree view with 'Targets' and 'CHAP users'. Under 'Targets', there is a folder 'big' containing 'target0'. Under 'CHAP users', there are two entries: '1. chap2' and '2. testchap'.

The main content area is titled 'Target: iqn.2008-06:llserver.target1'. It contains a 'Target volume manager' section with a table of volumes:

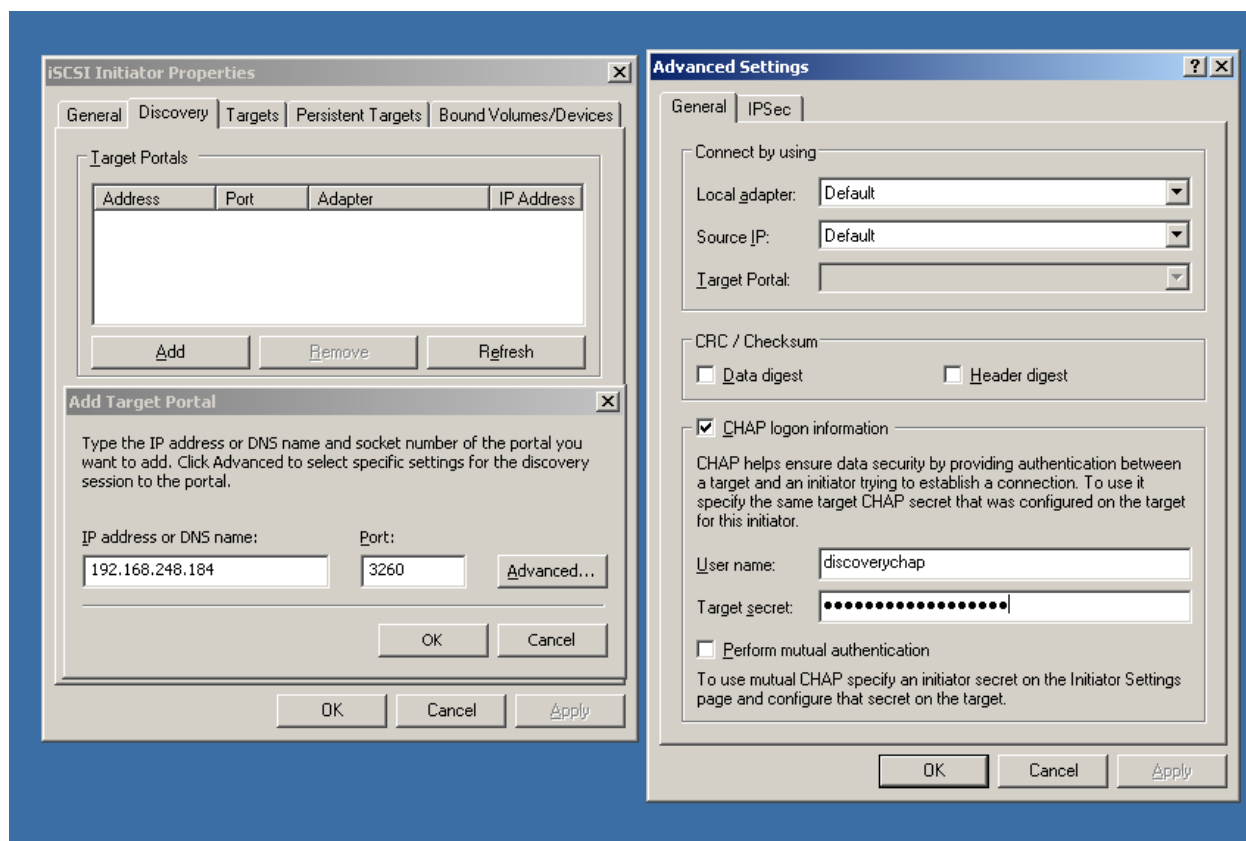
Volume	Rep.	Size (GB)	LUN	RO	WB	Action
1v0002		5.00	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="+"/> <input type="button" value="-"/>

Below this is the 'CHAP user target access' section. It has a checkbox 'Enable CHAP user access authentication' which is checked. Below the checkbox are two lists of CHAP users:

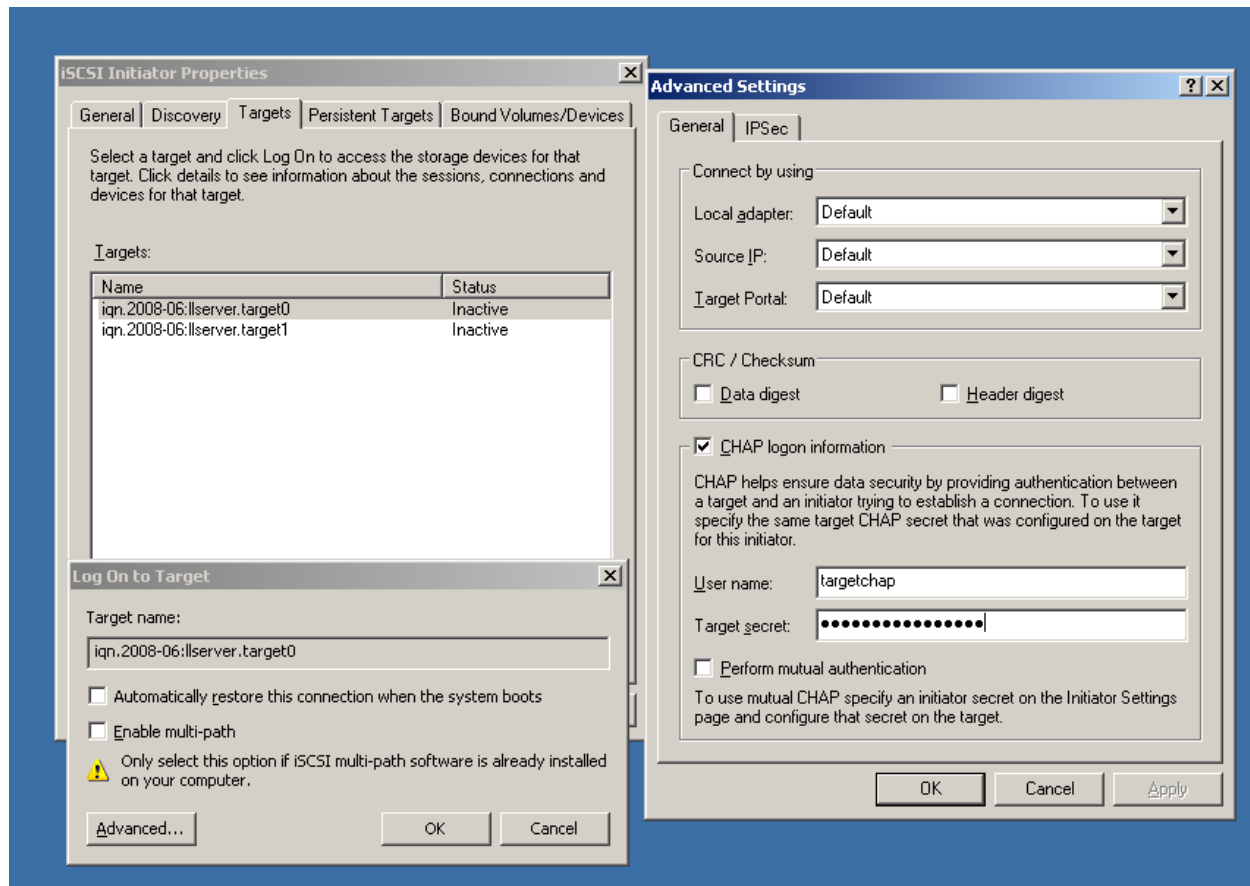
- Available CHAP users: testchap
- Granted access CHAP users: chap2

There are search bars for both lists and two arrows (right and left) between them to move users. At the bottom right of the main content area is an 'apply' button. At the bottom left, there is a 'status:' label with a red exclamation mark icon.

To use CHAP for iSCSI discovery authentication in MS Windows iSCSI initiator you need to push "Advanced" button in "Add target portal" windows while connecting to the iSCSI Target Portal. Then in "Advanced settings" enable CHAP authentication and enter CHAP user name and Target secret according to CHAP user that was assigned to access the discovery.



Using of Target access CHAP is very similar in MS Windows iSCSI Initiator. In the "Log On to Target" window you need to push "Advanced" button and in the "Advanced Settings" window enable "CHAP logon information". After that you need to enter valid CHAP user name and Target secret from user that have access to selected target.



Additional security for iSCSI connection in Open-E Servers is the IPsec. This function gives a encrypted data transfer between iSCSI Initiator and iSCSI Target. Open-E iSCSI Servers support IPsec only in iSCSI Target.

The IPSEC can be enabled in "Setup->network->IPSEC" function on our web GUI. You need to enter one IP to with the secure network connection tunnel will be available and the password with will be needed to bind the encrypted transfer connection from the host side.

The screenshot shows the Open-E DSS (Data Storage Server) web interface. The top navigation bar includes a 'logout' button and tabs for 'SETUP', 'CONFIGURATION', 'MAINTENANCE', 'STATUS', and 'HELP'. Below this, a secondary navigation bar has tabs for 'network', 'administrator', 'H/W RAID', 'S/W RAID', 'Fibre Channel', 'iSCSI Initiator', 'hardware', and 'GUI'. The 'network' tab is active, and within it, the 'Interfaces' sub-tab is selected. On the left, a tree view shows 'eth0' and 'eth1'. The main content area is divided into three sections: 1. Network configuration for 'eth0' with fields for MAC (02:72:77:09:B0:E3), DHCP (disabled), Static (selected), Address IP, Netmask, Broadcast, and Gateway. A 'create' button is at the bottom right. 2. 'HTTP proxy' section with a checkbox 'Use HTTP proxy' and an 'apply' button. 3. 'IPSEC' section with a checked checkbox 'Use IPSEC', an 'IP' field (192.168.248.234), a 'Password' field (masked with asterisks), and an 'apply' button. A 'status:' indicator with a red exclamation mark is at the bottom left.

logout **DSS** DATA STORAGE SERVER *open-e*

SETUP CONFIGURATION MAINTENANCE STATUS HELP

network administrator H/W RAID S/W RAID Fibre Channel iSCSI Initiator hardware GUI

Interfaces ?

- eth0
- eth1

MAC: 02:72:77:09:B0:E3

☐ DHCP

☒ Static

Address IP:

Netmask:

Broadcast:

Gateway:

create

? HTTP proxy

☐ Use HTTP proxy

apply

? IPSEC

☒ Use IPSEC

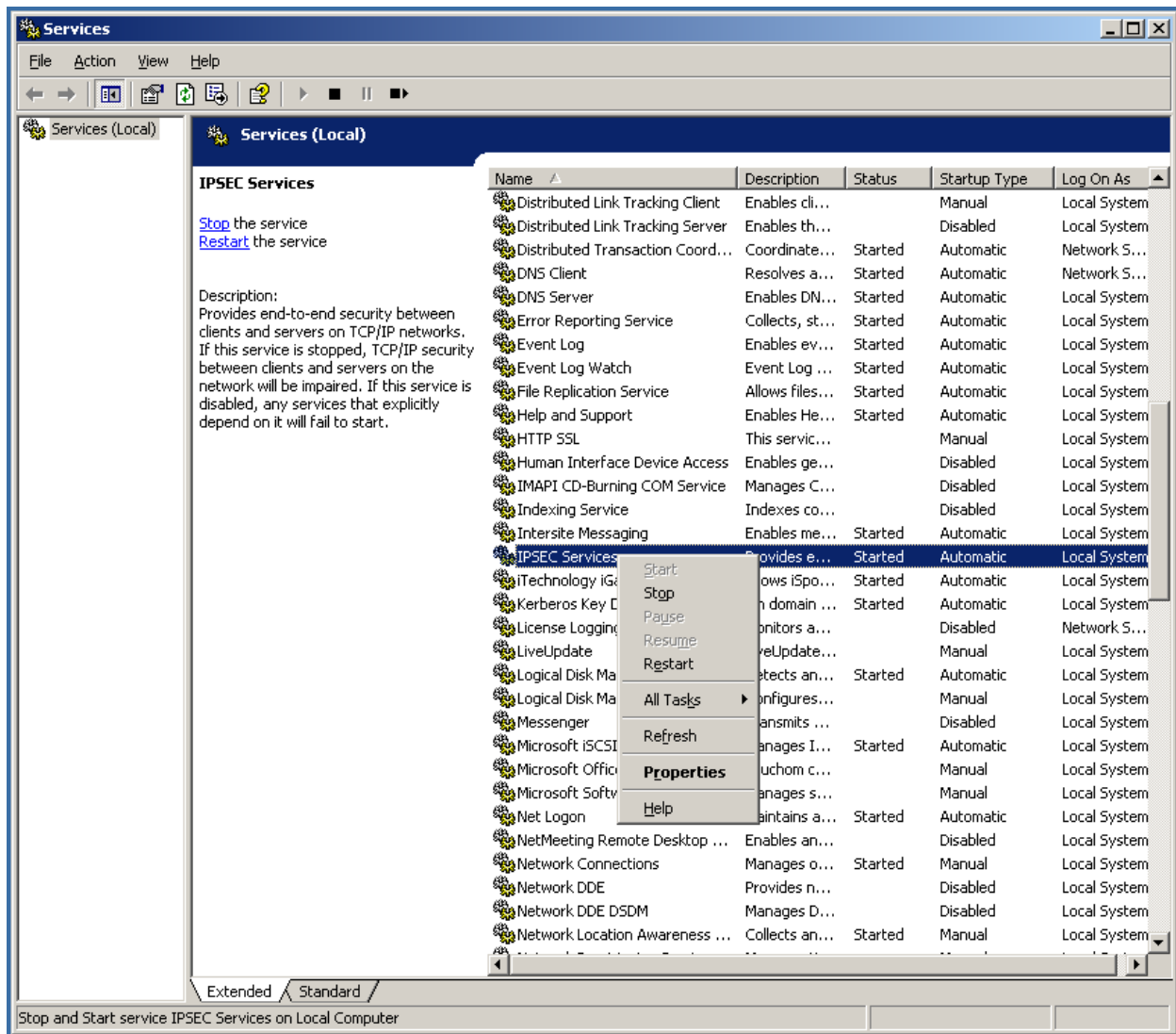
IP: 192.168.248.234

Password:

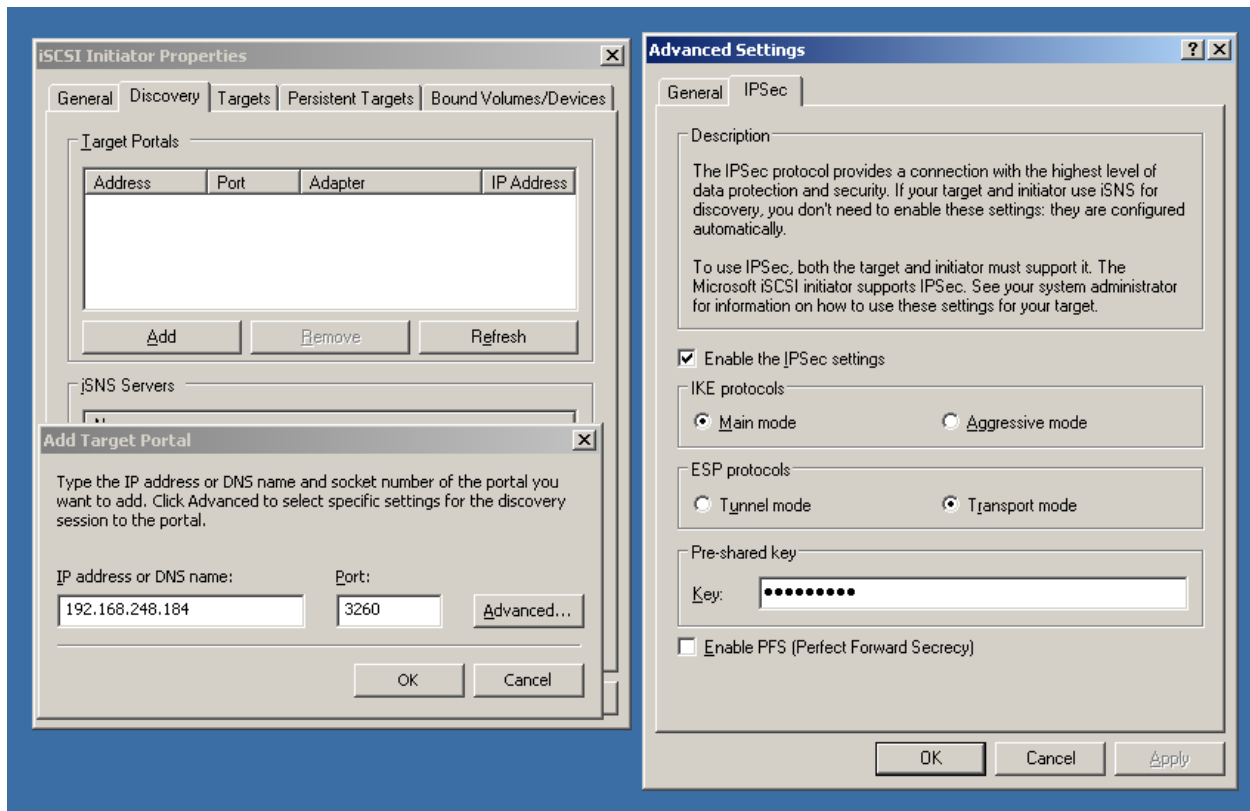
apply

status: !

To use IPsec on Windows iSCSI initiator side you need to restart IPsec services and iSCSI initiator service to properly connect into the iSCSI Target over IPsec.



After restarting services you need to configure it in "Add Target Portal" window by pushing "Advanced" button and in choosing IPSec tab in "Advanced Settings" window. On this windows you need to enable IPSec settings choose "Transport mode" in "ESP protocol".



If while connecting to the iSCSI Target you will get message that "no tunnel mode found" - that means you need to remove the target from the list, restart the IPSec services and try again with connection.