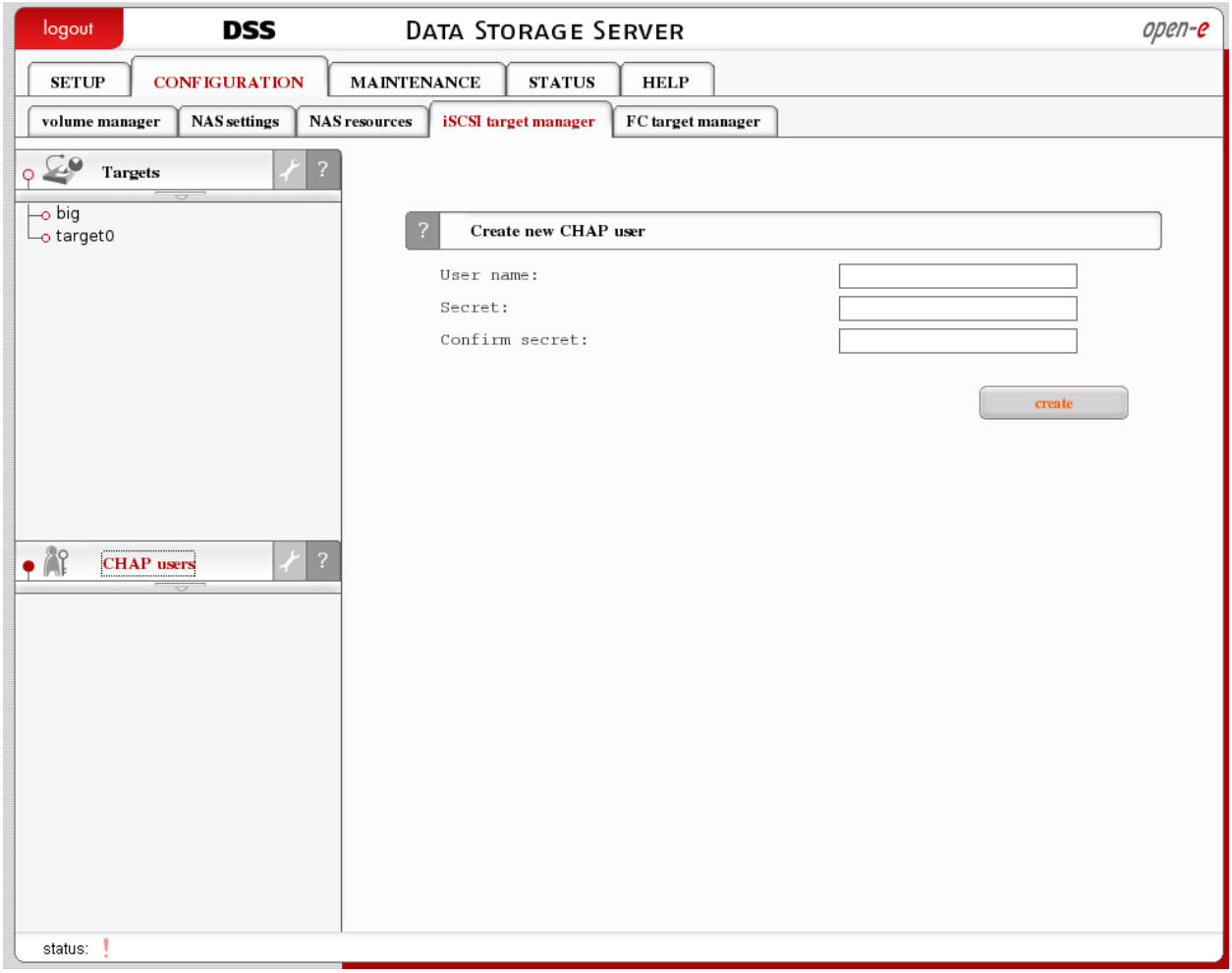
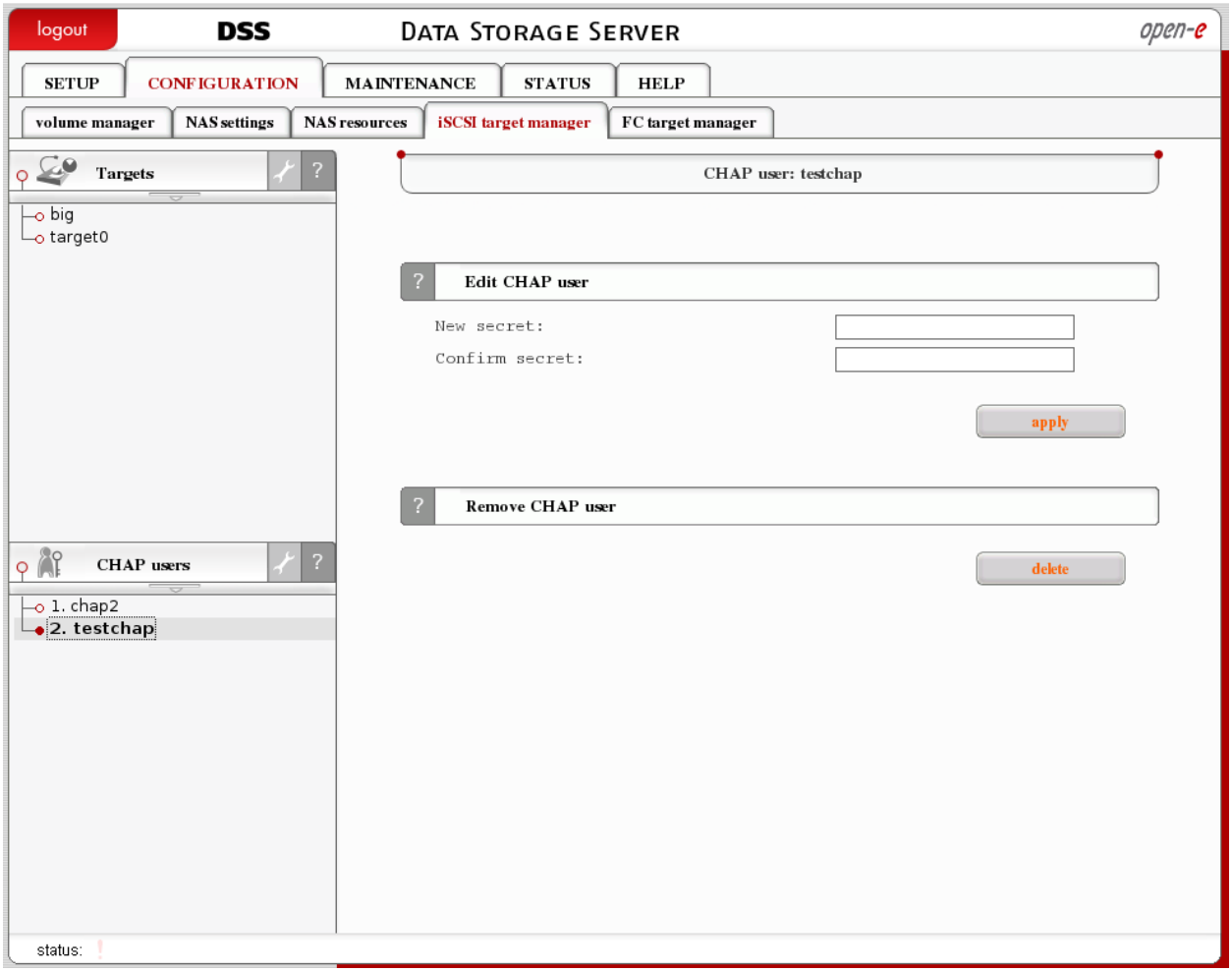
CHAP is a Challenge Handshake Authentication Protocol used in iSCSI Target/Initiator to authenticate connection. This authentication can be used in the discovery and Target connections. Discovery authentication is a global security for connection to the iSCSI server. Target authentication gives security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

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

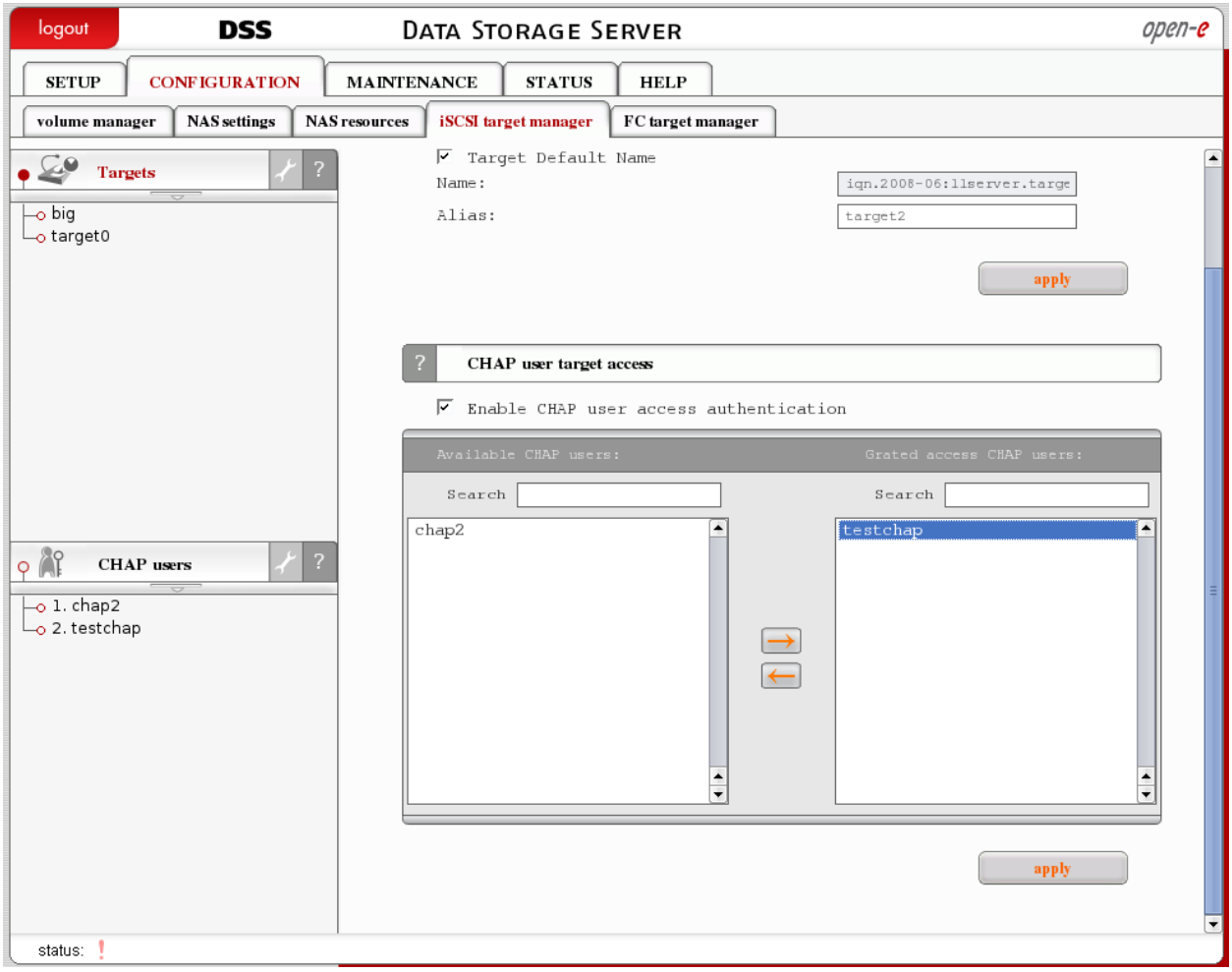
To create CHAP user you need to use function "Configuration->iSCSI Target Manager->CHAP users (from left panel)->Create new CHAP user" entering his name and secret (it is a password but in this case called a secret). The CHAP secret need to have 12-16 characters and can't contain spaces and few special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



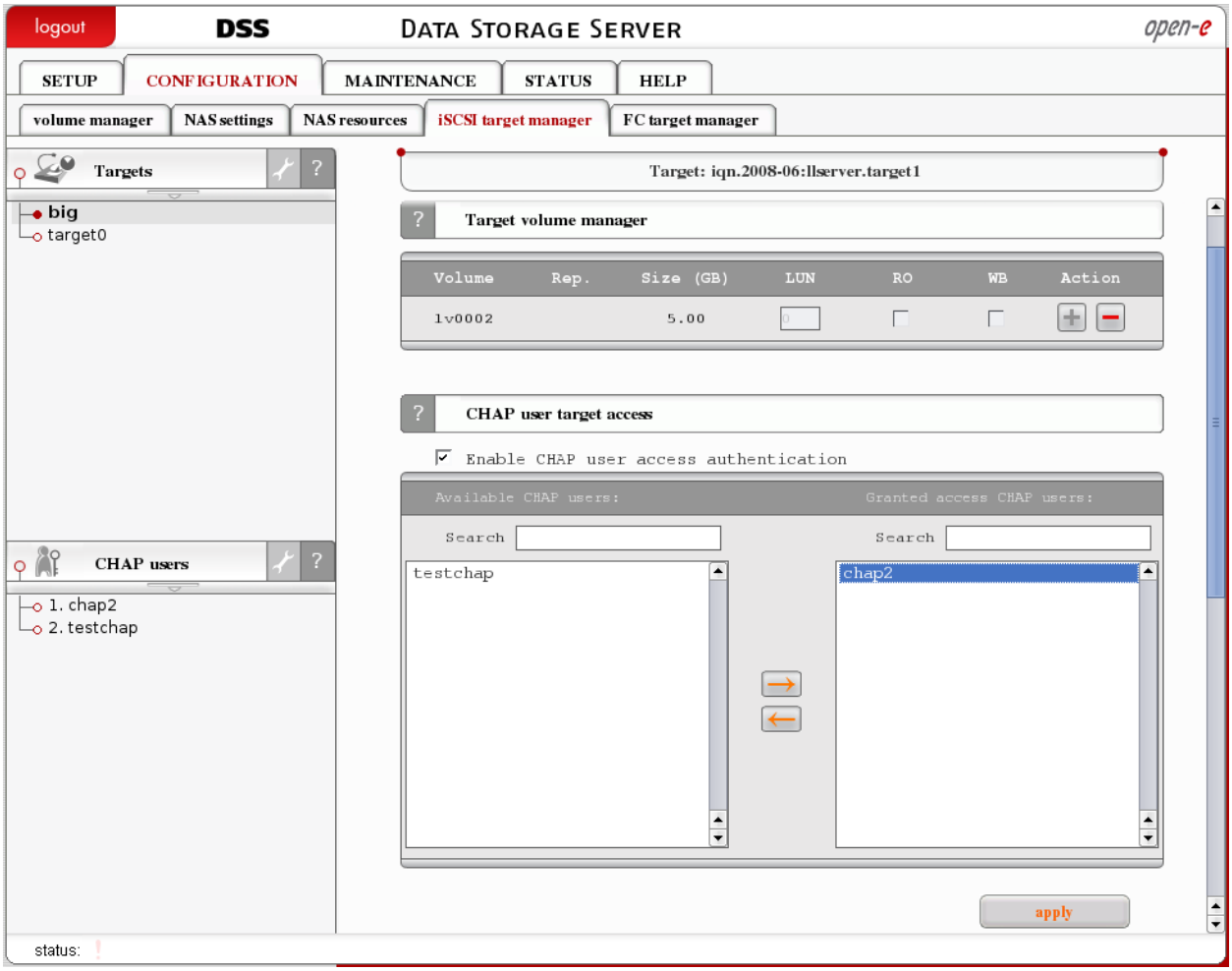
Selecting user from CHAP users (from left panel) will allow you to change the user secret or remove him.



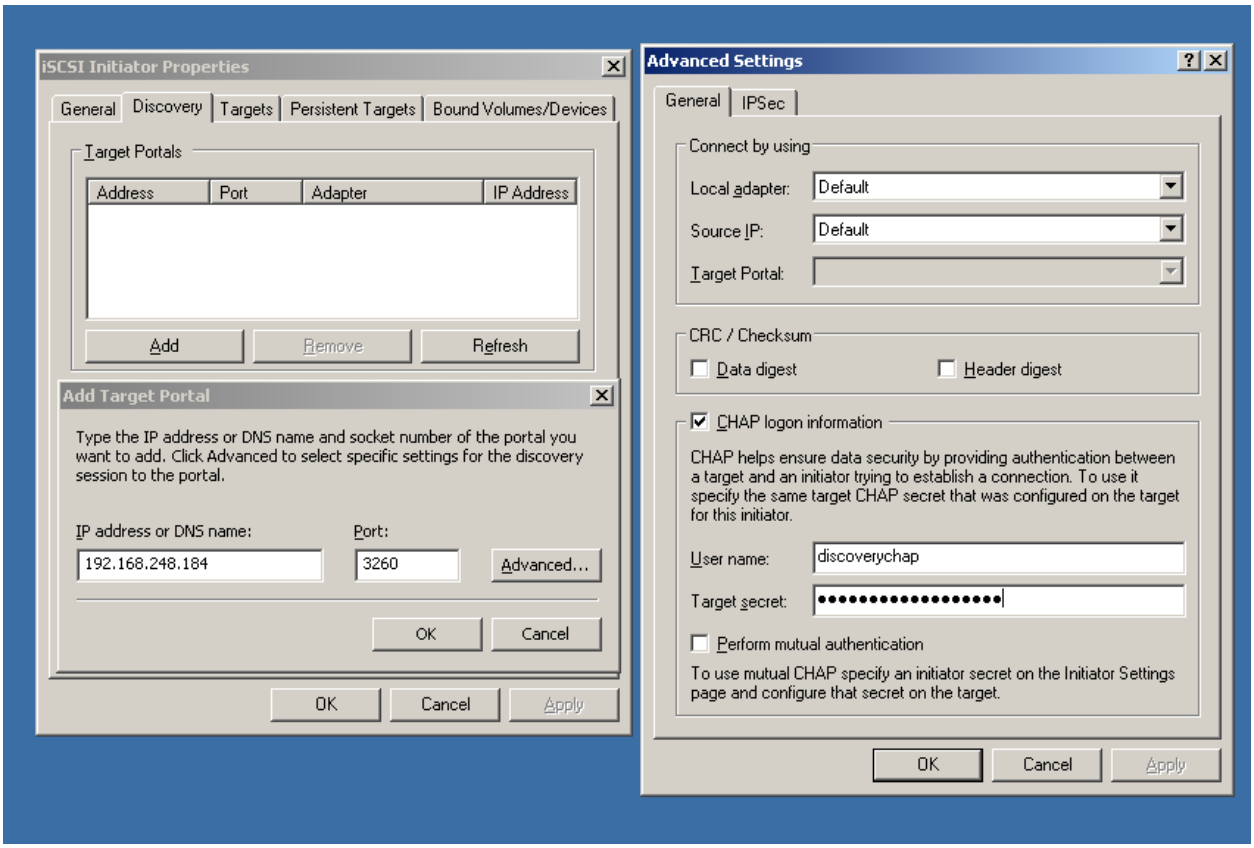
The global CHAP user used for authenticate discovery can be set in Configuration->iSCSI Target Manager->CHAP user Target access. You need to enable the "Enable CHAP user access authentication" and move CHAP users from available CHAP users list to grand access list. Please note that if no user is on the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



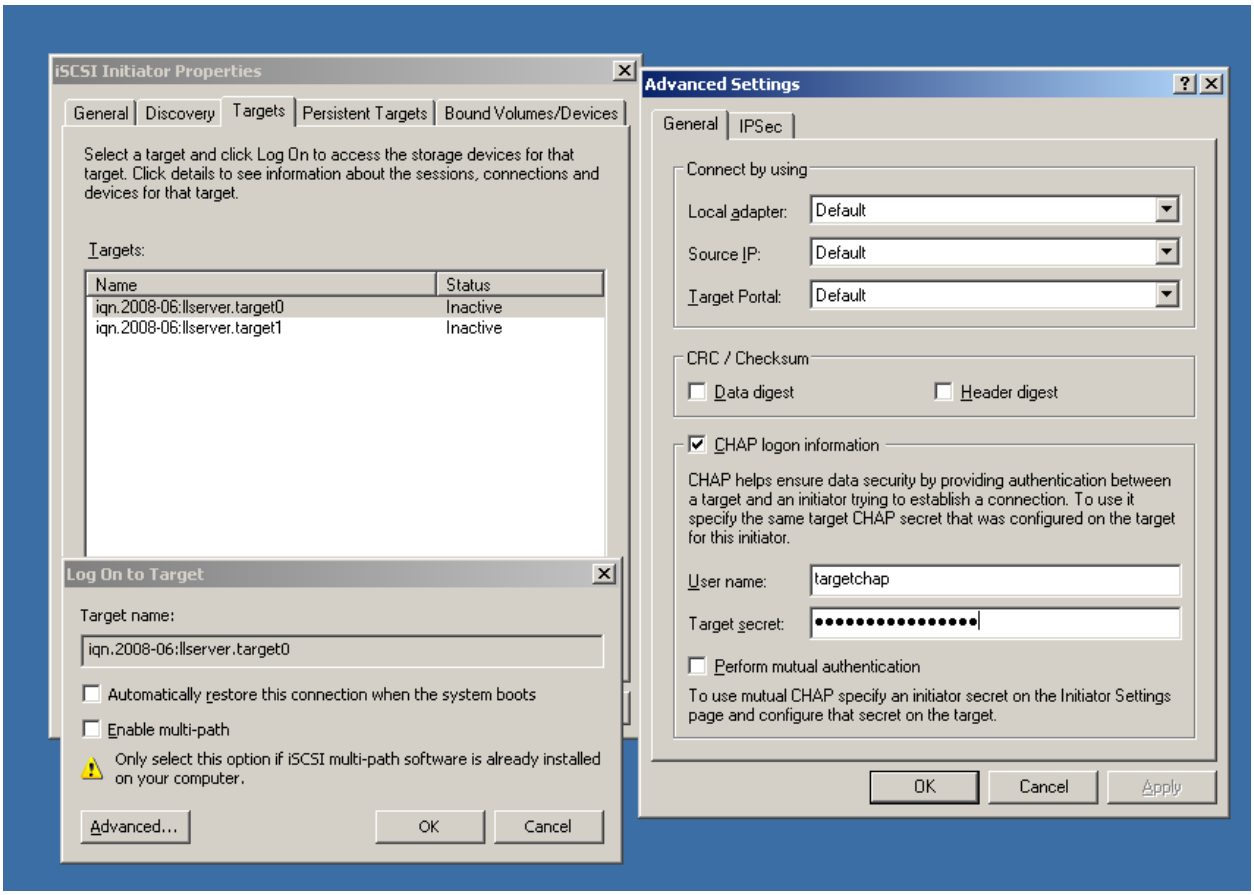
The Target CHAP user can be set in Configuration->iSCSI Target Manager->Targets-> <your target alias> ->CHAP user target access. You need to enable the "Enable CHAP user access authentication" and move CHAP users from available CHAP users list to grand access list. Please note that if no user is on the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



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.

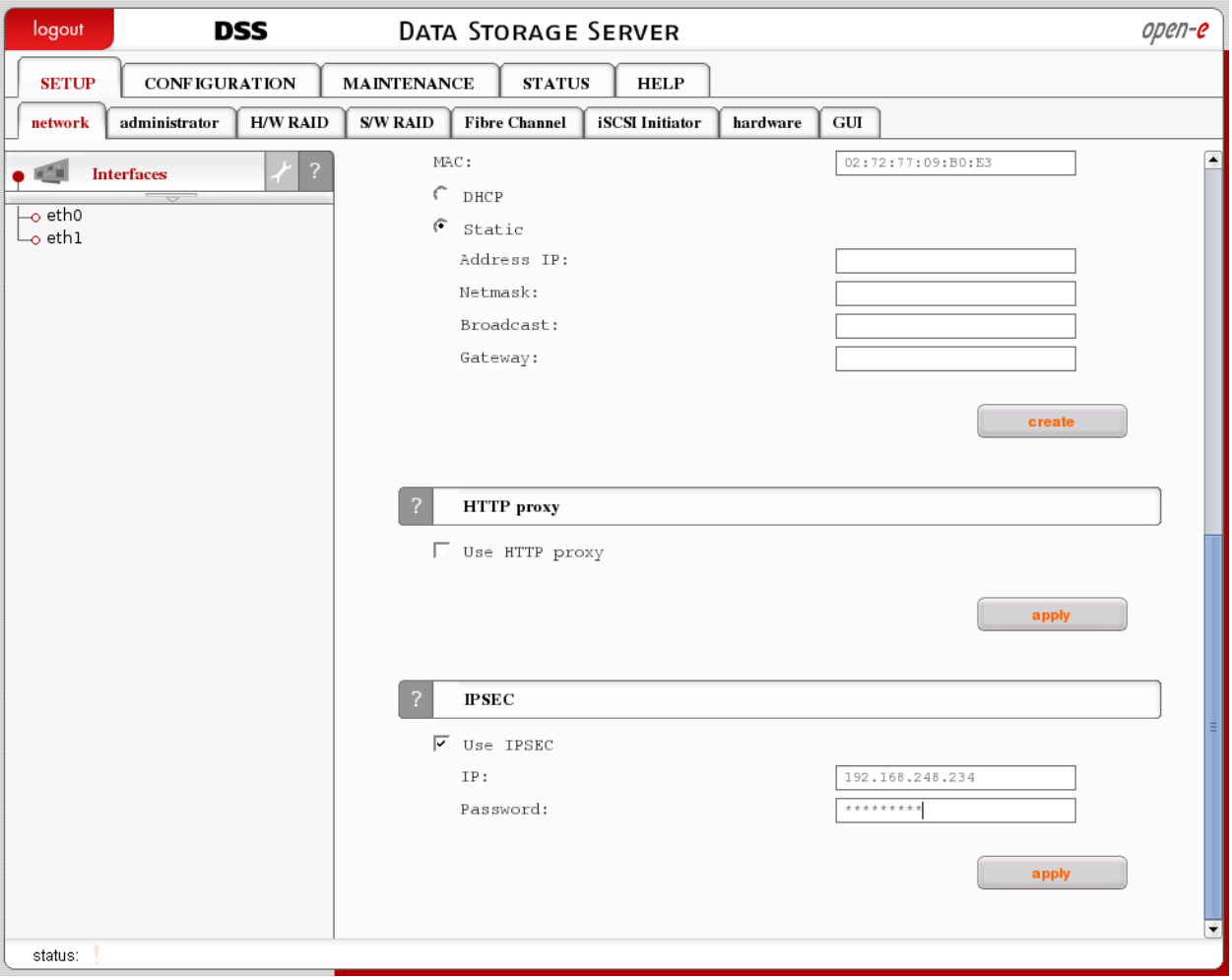


Using of Target access CHAP is very similar in MS Windows iSCSI Initiator. In the "Log On to Target" window you need to push "Advanced" button and in the "Advanced Settings" window enable "CHAP logon information". After that you need to enter valid CHAP user name and Target secret from user that have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

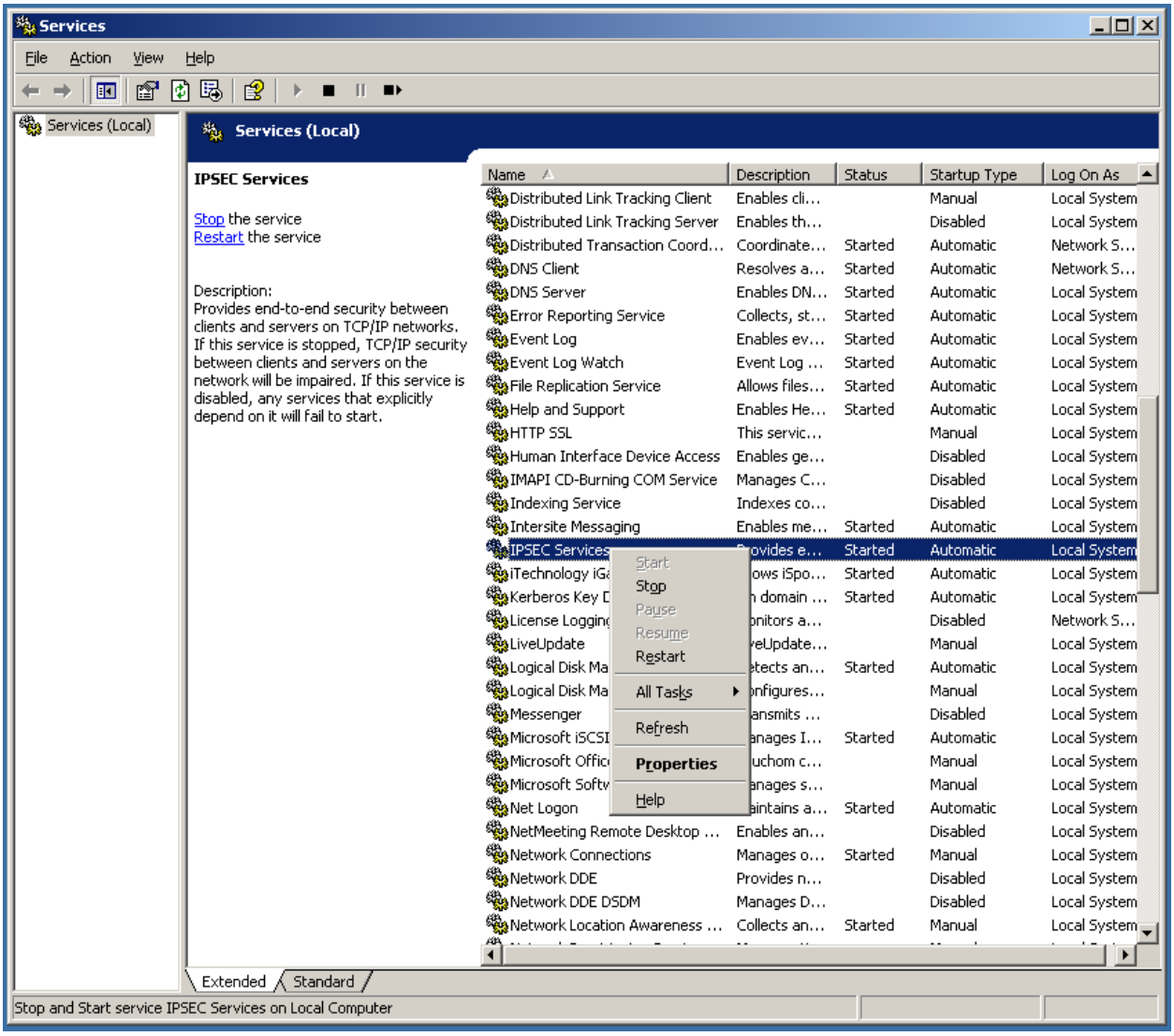


Additional security for iSCSI connection in Open-E Servers is the IPSec. This function gives a encrypted data transfer between iSCSI Initiator and iSCSI Target. Open-E iSCSI Servers support IPSec only in iSCSI Target.

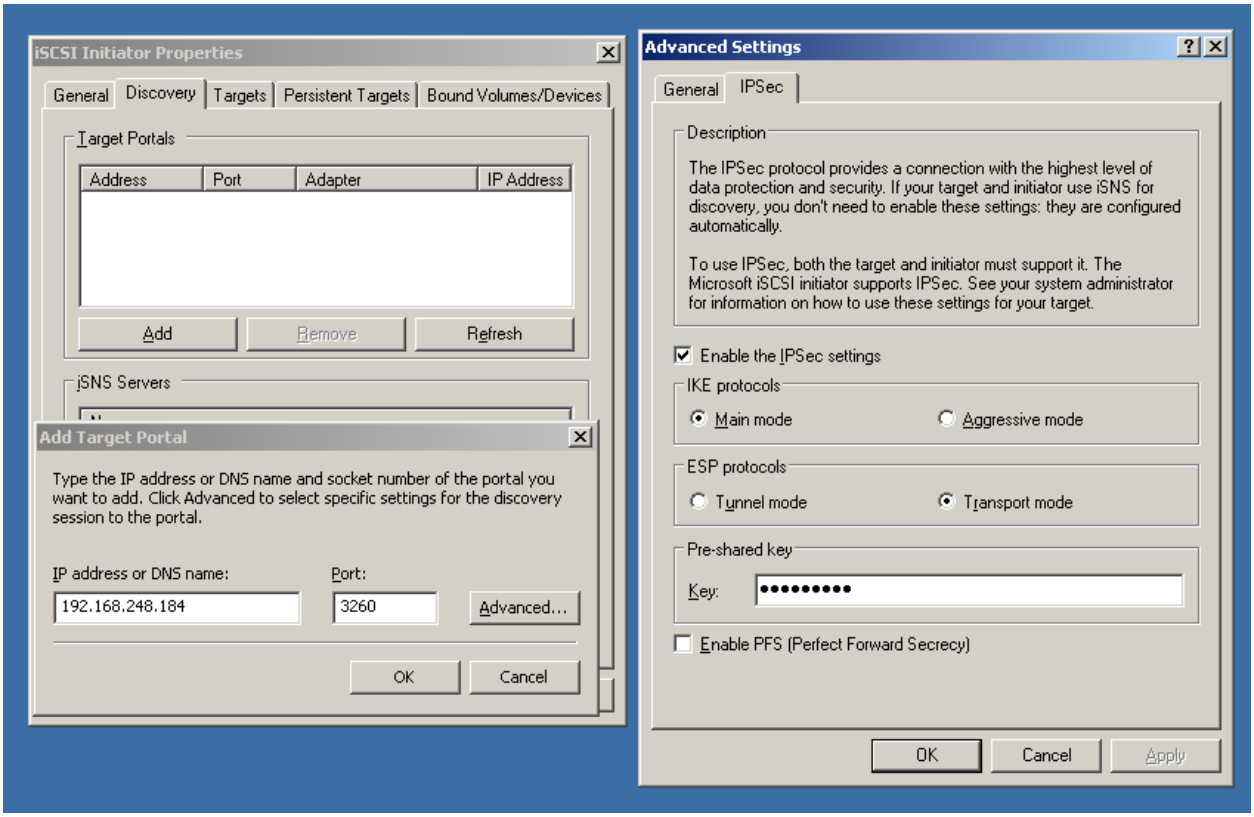
The IPSEC can be enabled in "Setup->network->IPSEC" function on our weg GUI. You need to enter one IP to with the secure network connection tunnel will be available and the password with will be needed to bind the encrypted transfer connection from the host side.



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 tunel mode found" - that means you need to remove the target from the list, restart the IPSec services and try again with connection.