

Configure_CHAP

The `vserver iscsi security create` command configures CHAP (Challenge Handshake Authentication Protocol) security settings for an iSCSI initiator on a NetApp ONTAP SVM (Vserver). It establishes authentication credentials so that the storage system can verify and securely accept iSCSI sessions from specific hosts. [\[1\]](#), [\[2\]](#), [\[3\]](#)

Syntax and Parameters

The core syntax for defining a security policy for a specific initiator is: [\[1\]](#)

```
vserver iscsi security create -vserver [vserver_name] -initiator  
[initiator_ign] -auth-type CHAP -user-name [inbound_username]  
-outbound-user-name [outbound_username] -vserver: The name of the  
Storage Virtual Machine (SVM) hosting the iSCSI target.
```

- **-initiator:** The IQN (iSCSI Qualified Name) of the client host machine you are securing.
- **-auth-type:** Defines the authentication method. You will typically set this to `CHAP`.
- **-user-name:** The inbound CHAP username (used for one-way authentication). When creating this, the system will prompt you to securely enter the corresponding password.
- **-outbound-user-name:** (Optional) Used if you want to configure mutual (two-way) CHAP authentication. You must also provide an outbound password when prompted. Note that you cannot use the same password for both inbound and outbound settings.

Best Practices & Important Notes

- **Default Settings:** If you do not assign a user-defined policy, the system will fall back on whatever default authentication method you defined using the `vserver iscsi security default` command.
- **Configuration Details:** For comprehensive command options and troubleshooting scenarios involving many initiators simultaneously, you can consult the [NetApp CLI Reference](#) or review [NetApp Define Authentication Method Guidelines](#).