How to Configure MS-CHAP Authentication

Use the Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAP V2) to authenticate VPN clients over L2TP/PPTP (mutual authentication between peers) or to authenticate HTTP Proxy users. The firewall must join the domain before using MS-CHAP authentication.

Connecting to Read-only Domain Controllers

In addition to the adding the hostname for the Barracuda NextGen Firewall F-Series, you must verify that the password for the user account used in the **Helper Scheme** is cached on the read-only domain controller.

Before You Begin

- Enable SMBv1 on the Windows Domain Controller.

Step 1. Configure MS-CHAP Authentication

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Authentication Service**.
2. In the left menu, select **MS-CHAP Authentication**.
3. From the **Configuration Mode** menu on the left, select **Switch to Advanced View**.
4. Click **Lock**.
5. Enable MS CHAP as external directory service.
6. Choose the NTLM protocol version supported by your authentication service.

   When changing the protocol version, a restart of the authentication daemon (phibs) is necessary. Restart the service in **CONTROL > Server > Service Status > box**.
7. In the **Domain Realm** field, enter the name of the Windows domain that is queried by the authenticator.
8. If the NetBIOS domain name differs from the MS Active Directory domain name, specify the **NetBIOS Domain Name**.

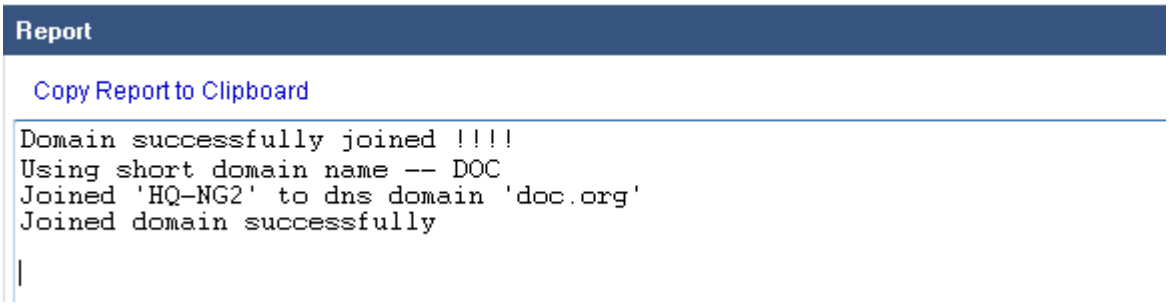
   The NetBIOS domain name is important for user group synchronization. It is required for NTLM authentication and URL Filter configuration when user group filters apply. For more information, see How to Configure URL Filtering in the HTTP Proxy.
9. Enter the MS Active Directory **Workgroup Name** if the workgroup name is different from the MS Active Directory domain name (**Domain Realm**).
10. In the **Domain Controller** field, enter the IP address of the domain controller.

    If you also configured the MSAD authentication scheme with the **Use MSAD-groups with NTLM** setting enabled, the Barracuda NextGen Firewall F-Series must be able to resolve the DNS name of the domain controller. (This also applies for the WINS Server IP address.)
11. In the **WINS Server** field, enter the IP address of the domain's Windows Internet Name Service (WINS) server.

12. If group information is queried from a different authentication scheme, select the scheme from the **User Info Helper Scheme** list. For example, select **MSAD** if MS-CHAP is used for identity verification but group information must be queried from MSAD.
13. Click **Send Changes** and **Activate**.

Step 2. Add the Barracuda NextGen Firewall F-Series to a Windows Domain

1. Go to **CONTROL > Box**.
2. In the left menu, expand **Domain Control** and click **Register at Domain**.



Verify that the Barracuda NextGen Firewall F-Series is joined to the domain by clicking **Show Registration Status** in **CONTROL > Box > Domain Control**.

Figures