How to Enable NTLM Domain User Authentication

https://campus.barracuda.com/doc/6160449/

If your network uses an NT LAN Manager (NTLM) authentication server, your NTLM domain users transparently become authenticated in the Barracuda Web Security Gateway using their Microsoft Windows credentials. This single sign-on (SSO) method of access control is provided by transparent proxy authentication against the your NTLM server. Note that you can configure NTLM authentication in conjunction with LDAP as well as running the Barracuda DC Agent on your domain controller(s).

NTLM is not supported for multiple domains on one Barracuda Web Security Gateway.

To enable transparent proxy authentication against your NTLM server, you must join the Barracuda Web Security Gateway to the NTLM domain as an authorized host. The process of joining the domain also synchronizes NTLM group information from your domain controller to the Barracuda Web Security Gateway. For details on how to set up NTLM and configuration, see the **USERS/GROUPS > Authentication** page **NTLM** tab in the Barracuda Web Security Gateway web interface.

For details on integrating with your existing user authentication server, see How to Integrate the Barracuda Web Security Gateway With a User Authentication Service.

Windows Support for NTLM authentication

Windows Server 2000 and Windows 2003 with Active Directory (in mixed mode) run the NTLM authentication protocol by default. In a native mode Active Directory domain, Windows Server 2003 runs the Kerberos authentication protocol.

Starting with Windows Vista, and also with Windows Server 2008 and Windows 7, both LM and NTLM are de-activated by default. Microsoft specifies Kerberos as the preferred authentication protocol for Windows 2003 and Windows Server 2008 Active Directory domains. Kerberos is typically used when a client belongs to a Windows Server domain, or if a trust relationship with a Windows Server Domain is established in some other way. For more on Kerberos, see How to Configure Kerberos Authentication. However, NTLM can still be used in the following situations:

- The client is authenticating to a server using an IP address
- The client is authenticating to a server that belongs to a different Active Directory forest, or doesn't belong to a domain at all
- No Active Directory domain exists

For detailed descriptions of these scenarios, click the **Help** button on the **USERS/GROUPS > Authentication** page.

Requirements for using an NTLM Authentication Server

Before you integrate with an NTLM authentication server, verify the following requirements:

- The Barracuda Web Security Gateway must be deployed as a forward proxy.
- Kerberos authentication is not already configured.
- Web browsers must be configured to use the Barracuda Web Security Gateway as the HTTP proxy.

For detailed descriptions of these requirements, click **Help** on the **USERS/GROUPS > Authentication** page.

If you have installed the **Barracuda DC Agent** software on your domain controller(s) for use with clients authenticating via LDAP, (see About the Barracuda DC Agent) make sure to do the following when adding users in terminal environments who will be authenticating with either Kerberos or NTLM:

1. Run the **Barracuda DC Agent** monitor and click on the **Filters** tab.
2. Specify any IP addresses for which the Barracuda DC Agent **should not** capture and send login information (for LDAP logins) to your Barracuda Web Security Gateway. This includes Citrix or other terminal servers used when implementing Kerberos or NTLM authentication mechanisms, while you also have PCs using LDAP and utilize a Barracuda DC Agent. These IP addresses are exceptions and associated login events (for LDAP logins) will be ignored by the Barracuda DC Agent.

Limitations when using an NTLM Authentication Server

The following limitations apply when using an NTLM authentication server with the Barracuda Web Security Gateway:

- No login override of blocked pages for NTLM domain users who encounter a block message.
- No logout option for NTLM domain users who proceed to a blocked web page.
- NTLM domain users are not listed in the Account View page.
- NTLM realm is not listed for users listed in the syslog output.

For detailed descriptions of these restrictions, click **Help** on the **USERS/GROUPS > Authentication** page.

If an Active Directory Group object does not have any members (i.e. the group is empty), the group will not display in the **Lookup** field on any page in the Barracuda Web Security Gateway web interface where you can select an authentication mechanism. Conversely, when using LDAP, empty Active Directory groups are displayed if they exist.