
How to Enable LDAP Domain User Authentication

<https://campus.barracuda.com/doc/6160472/>

If your network uses a Lightweight Directory Access Protocol (LDAP) or Active Directory authentication (AD) server, your LDAP domain users can use the LDAP or AD authentication service to be authenticated in the Barracuda Web Security Gateway system. The Barracuda Web Security Gateway can also enable you to look up users by organizational units you have defined on your LDAP server when creating exceptions to block/accept policy.

Integration with External Systems and Services - Security Considerations

The Barracuda Web Security Gateway integrates with other systems and services in your environment, like your LDAP, NTLM or Kerberos servers. Barracuda recommends creating separate service accounts for these integration points, rather than personal accounts, and then using the principle of least privilege. This integration strategy is part of an overall security policy. For more information, see [Security for Integrating with Other Systems - Best Practices](#).

To enable LDAP user authentication, from the **USERS/GROUPS > Authentication** page, in the LDAP tab, provide information about connecting to the LDAP server, binding to the LDAP server, encryption type and LDAP attributes. Click the **Help** button on the page for detailed steps.

To configure proxy authentication through LDAP for remote users such as students with Chromebooks, and other off-network users, see [How to Configure Proxy Authentication](#).

LDAPS Authentication

This section applies to firmware version 15.0.0.x and higher.

If you are using port 636 for LDAPS, you must export an LDAPS certificate from your Windows Server to upload the Barracuda Web Security Gateway, which uses the certificate to verify the identity of the server. The certificate must be in .pem format. Pre-requisites for using the certificate include:

1. AD Certificate Services Installed on your Windows Server 2008 or 2012 (you most likely need IIS services to be installed as well).
2. AD Domain Services must be configured.
3. Set up your AD to listen for LDAPS.

To export a root certificate from your Windows Server, see [How to Export a Root Certificate From Windows Server 2008 or 2012](#). For more information about LDAPS, see [LDAP Versus LDAPS](#).

How to Upload Your Certificate to the Barracuda Web Security Gateway

Make sure your certificate is in .pem format. Log into the Barracuda Web Security Gateway as *admin*.
For models 410 and higher:

1. Go to **ADVANCED > SSL Inspection**.
2. Scroll to the bottom of the page and use the **Upload SSL Certificate** feature to upload the recently exported file.

For models 210 and 310, contact [Barracuda Support](#) and provide the certificate in .pem format.

Advanced LDAP Configuration

These settings should only be configured by advanced users, and are set on the **USERS/GROUPS > Configuration** page. Contact [Barracuda Technical Support](#) with questions.

- **LDAP Server Timeout** – When an LDAP server is slow in responding to search requests, increase this timeout value. Default is 30 seconds.
- **LDAP Full Sync** – Use this setting to specify how many times the Barracuda Web Security Gateway does a full sync of users and groups against your authentication service in a day time frame. Default setting is *Twice*. If this setting is *Disabled*, then the Barracuda Web Security Gateway does not sync users and groups against your authentication service.
- **Require API Access for User Auth** – Setting to *Yes* means that, when authenticating users with the Barracuda Web Security Gateway's third-party authorization API, the request must come from an IP address within the **Allowed API IP/Range** and include the **API Password**, both as defined on the **BASIC > Administration** page.

© Barracuda Networks Inc., 2021 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.