

## Kerberos Authentication Management

<https://campus.barracuda.com/doc/6553618/>

Select **Kerberos** as the authentication mechanism. The Kerberos Authentication Management screen appears, and displays a list of Kerberos authentication mechanisms.

Do one of the following:

- To edit a Kerberos mechanism, click the **Server Realm** name.
- To add an NTLM mechanism, click **Add Kerberos Authentication Mechanism**.

The Add/Update Kerberos Authentication Mechanisms screen appears.

Enter or edit the following fields:

- **Server Realm** - Your Windows administrative domain name.
- **KDC** - FQDN (fully qualified domain) of the KDC (Key Distribution Center) server for the above realm. This is typically the FQDN of your domain controller.
- **Username** - Windows Username of a user with privileges to join this machine to the Active Directory. Do not include the domain name in the **Username** entry. For example, if the **Username** is *administrator*, simply enter **administrator**.
- **Password** - Password for the user in the **Username** field, specified above.
- **Advanced Options > Short Domain Name** - Short domain name if different from the realm name.

Be sure to **Submit** then **Save Changes**. When prompted to sync the Barracuda Web Security Service Connector, click **Sync**.

© Barracuda Networks Inc., 2019 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.