

## How to Configure Barracuda DC Agent Authentication

<https://campus.barracuda.com/doc/43224453/>

The Barracuda DC Agent enables the Barracuda NextGen Firewall X-Series to transparently track user login activity in your Windows domains. When installed on a domain controller that runs either Windows Server 2003 with Service Pack 2 (SP2) or Windows Server 2008 or above, the Barracuda DC Agent monitors the user authentication logs. Configure the X-Series Firewall to query the Barracuda DC Agent so that it can learn which IP address is used by a network user.

### Before you Begin

Download and install the Barracuda DC Agent on your domain controller or dedicated Windows PC. The DC Agent can be downloaded directly from your X-Series Firewall:

Do not install the Barracuda DC Agent on Windows Server domain controllers that are configured to use NTLM.

1. Go to the **USERS > External Authentication** page.
2. Click the **DC Agent** tab.
3. Click **Download DC Agent**.
4. Install the DC Agent. For more information, see [How to Get and Configure the Barracuda DC Agent](#).

When configuring the Barracuda DC Agent, add the IP address(es) of your X-Series Firewall and configure local audit policies to generate an account login event whenever a user authenticates via the domain controller.

### Configure DC Agent Authentication

Configure the X-Series Firewall to communicate with the Barracuda DC Agent and specify the domain controllers where the Barracuda DC Agent is installed.

1. Go to the **USERS > External Authentication** page.
2. Click the **DC Agent** tab.
3. Set **Enable Single Sign-On** to **Yes**.
4. In the **Domain Controller IP** field, enter the IP address of the domain controller running the DC Agent. The X-Series Firewall polls the DC Agent to obtain the list of users authenticated against this domain controller.

5. Enter the **DC Agent Listening Port**. Default: 5049.
6. In the **Synchronization Interval** field, specify the time interval in seconds at which the X-Series Firewall should poll the DC Agent for the list of authenticated users. The recommended value is 15 seconds.
7. Click **Add**.
8. Enter the username in the **Exempt User Name** field to exclude specific domain users. You can use Perl-compatible regular expression (PCRE) pattern-matching notation, such as `\w` for any alphanumeric character or `\W` for any non-alphanumeric character.
9. Click **Add**.

© Barracuda Networks Inc., 2024 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.