# How to Get and Configure the Barracuda DC Agent

https://campus.barracuda.com/doc/26576057/

**For the Barracuda Web Security Gateway Only**: The Barracuda DC Agent 7.1.x and higher does not support Windows Server 2003. If you are running Windows Server 2003, please contact Barracuda Networks Technical Support. Otherwise, download the Barracuda DC Agent from the **USERS/GROUPS > Authentication** page of the Barracuda Web Security Gateway web interface as described below.

For Windows Server 2022:

- You must set the correct logon events per where Windows Server 2022 stores the settings "Audit Logon Event" and "Audit Account Logon Event".
- The Barracuda DC Agent service could fail to install with `error 1920` (Service Barracuda DC Agent failed to start). Verify that you have sufficient privileges to start system services. In this case, increasing the Windows Service Startup Time can avoid this error.

The following settings must be configured in the Domain Controller Policy:

- Computer Configuration -> Windows Settings -> Sec. Settings -> Local Policies ->sec. Options-> Audit: Force Audit policy sub - Enabled
- Computer Configuration -> Windows Settings -> Sec. Settings -> Advanced Audit Policy Config:
- Logon/Logoff Policy Setting
- Audit Logoff Success
- Audit Logon Success

The Barracuda DC Agent version 7.1.x replaces all previous versions published. Barracuda Networks recommends using the latest version of the Barracuda DC Agent. If you are not using the Barracuda Web Security Gateway, download the latest version by logging into the Barracuda Download Portal with your Barracuda Cloud Control (BCC) credentials. If you don't have a BCC account, create one here.

For iOS users: Due to the way Apple devices authenticate users with Windows Active Directory, the Barracuda DC Agent is unable to pick up Mac user logins to Windows Active Directory. The Barracuda DC Agent can, however, capture user logins from wireless devices such as iPads or iMacs if the user is authenticating via WAP against a RADIUS server.

## System Requirements

Before configuring the Barracuda DC Agent, make sure that your system meets the following requirements:

- Local Installation – Microsoft Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019, or 2022. Windows Server Core is not supported for local installation and monitoring. The DC Agent can, however, communicate with a domain controller that is running Windows Server Core. In this case, you could install the DC Agent on a server running Microsoft Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019, or 2022 and configure it to remotely monitor a domain controller that is running on a Windows Server Core machine.
- Remote Installation – Microsoft Windows 2008 and higher. Also note that, for the remote installation of DC Agent, you MUST be a domain member to query the server.

For remote monitoring of domain controllers, the Barracuda DC Agent **Active Directory Profile** must be provided with a domain controller user with administrative privileges.

## Get and Install the Barracuda DC Agent Version 7.x

You can install the Barracuda DC Agent directly on the domain controller or on a dedicated Windows PC within your network environment. To monitor wireless device logins using Windows Network Policy Server (NPS) log events, see Using the Barracuda DC Agent With Microsoft Network Policy Server.

**For the Barracuda Web Security Gateway:**

1. Log into the web interface as *admin*
2. Download the Barracuda DC Agent from the **USERS > Authentication** page using the **Barracuda DC Agent (Download/Install)** link at the bottom of the screen.
3. To launch the installation file (DCAgent.exe), right-click it and select **Run as administrator**.
4. Follow the instructions in the wizard. When going through the steps in the installation wizard, all settings normally should be left at default. The required settings to configure should be:
    - Your domain information
    - The IP address of the allowed Barracuda Web Security Gateway
5. Confirm that **Logon Events** are monitored by your domain controller:
    1. Open **Domain Controller Security Policy** (**Start > Programs > Administrative Tools**).
    2. Click **Local Policies**.
    3. For **Audit account logon events** and **Audit logon events**, verify that the **Policy Settings** column displays **Success**.

**For the NextGen Firewall F-Series:**

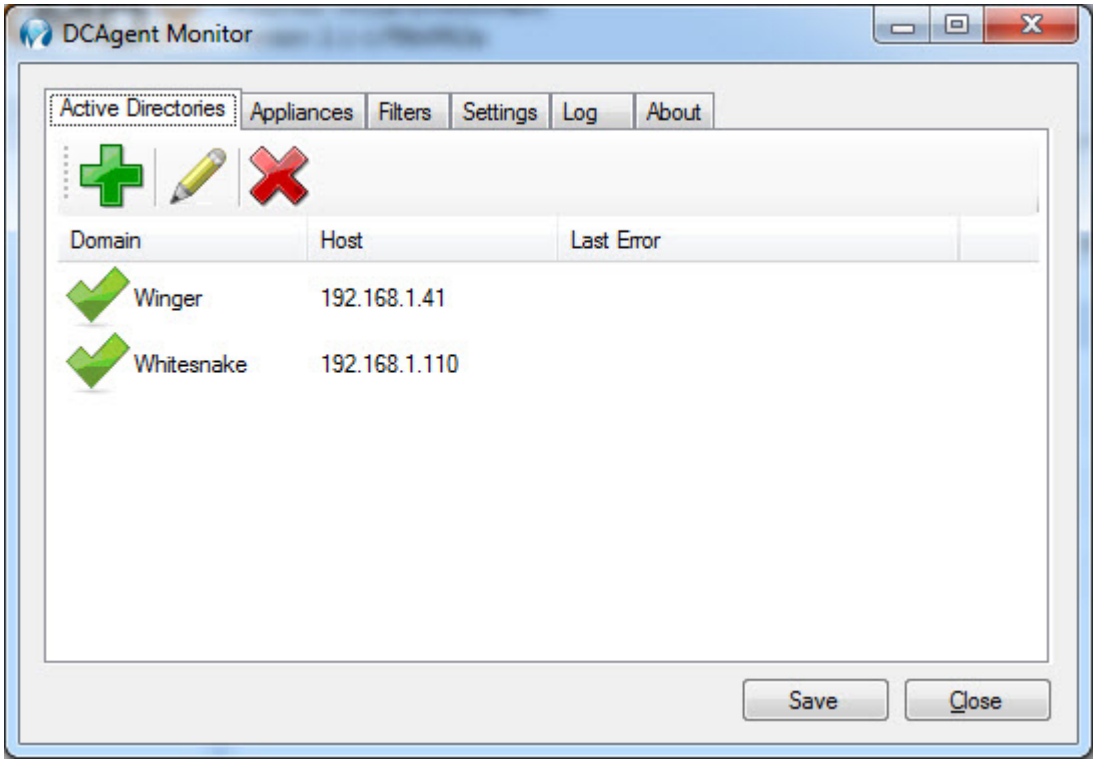
1. Get the Barracuda DC Agent from your Barracuda Cloud Control Account.
2. While logged into your account, go to the **Support > Downloads** page.
3. From the **Product** list, select **Barracuda NG Firewall**.
4. Select **Fulltext**, enter **Barracuda DC Agent**, and then click **Search**.
5. Download the latest Barracuda DC Agent version that is compatible with your system.
6. To launch the installation file (DCAgent.exe), right-click it and select **Run as administrator**.
7. Confirm that **Logon Events** are monitored by your domain controller:
    1. Open **Domain Controller Security Policy** (**Start > Programs > Administrative Tools**).
    2. Click **Local Policies**.
    3. For **Audit account logon events** and **Audit logon events**, verify that the **Policy Settings** column displays **Success**.

## Configure the Barracuda DC Agent

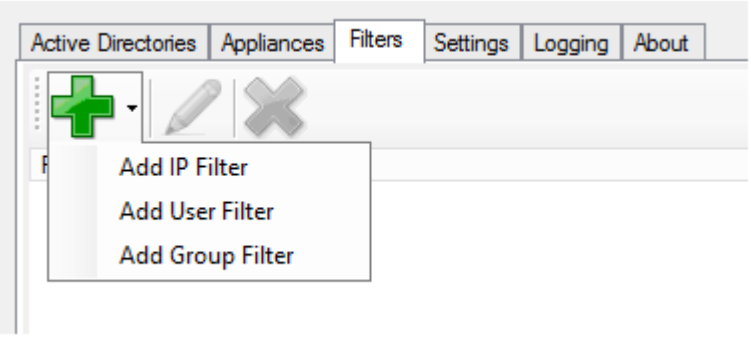
After the Barracuda DC Agent is installed and running correctly, launch the application and complete the following steps. Note: Your entries in the DC Agent interface will NOT be saved until you click the **Save** button.

1. Define location and login credentials for your Active Directory. Click the **Active Directories** tab and click the green **+** sign to add a domain.
    1. Select **Local** if you installed the DC Agent on the Domain Controller; select **Remote** if you installed on another machine on the network.
    2. If you selected **Remote**, enter the Fully Qualified Domain Name (FQDN) in the **Host** field.
    3. Enter a name for referring to the domain, e.g. 'Finance', 'Salesnet', etc.
    4. The **Username** should be associated with permissions to run WMI queries on the domain controller. Enter that user's **Password** and click **OK**.

        For remote monitoring of domain controllers, the Barracuda DC Agent **Active Directory Profile** must be provided with a domain controller user with administrative privileges.
        **Integration with External Systems and Services - Security Considerations:** Barracuda Networks products integrate with other systems and services in your environment, like your LDAP, FTP/FTPS, or, in this case, domain controller. Barracuda Networks 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.
    5. Click **Test** to verify connectivity with the domain controller.




2. Add the *internal* **IP Address** and a **Description** for each Barracuda Networks appliance (Barracuda Web Security Gateway, NG Firewall, etc. – hardware or virtual) with which you want to use the DC Agent.
3. On the **Filters** tab, specify any **IP Address, User,** or **Group** for which you don't want the DC Agent to capture and send login information to your Barracuda Networks products. These are exceptions and associated login events will be ignored by the DC Agent. Here are the formats you can use to specify IP address exemptions:
   Single IP address (Example: 192.168.0.1)
   IP Range/CIDR notation (Example: 192.168.0.0/24)
   IP Range/Subnet mask (Example: 192.168.0.0/255.255.255.0)




   User and Group (CN) formats are the same as in the Barracuda Web Security Gateway web interface, and they do support leading and trailing wildcards (e.g. “*name” or “name*” , but not “na*me”). For example: `CN=Jane Smith`

**Important: For the Barracuda Web Security Gateway**

If you install the **Barracuda DC Agent** software on your domain controller(s) for use with

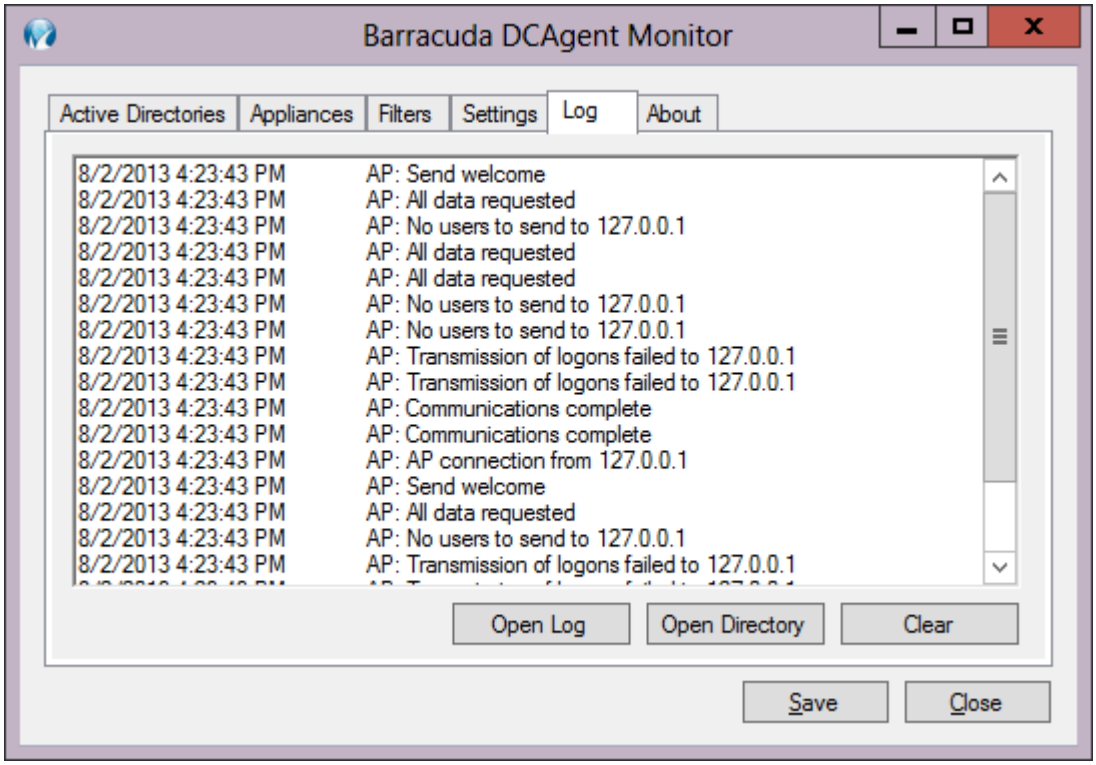
clients authenticating via LDAP, (see About the Barracuda DC Agent) and you later add users to your Barracuda Web Security Gateway in Citrix or other terminal environments who will be authenticating with either Kerberos or NTLM, make sure to do the following:

1. Run the **Barracuda DC Agent** monitor and click on the **Filters** tab.
2. Specify the IP addresses of the terminal servers where users will authenticate via Kerberos or NTLM. These are IP addresses for which the DC Agent should not capture and send login information to your Barracuda Web Security Gateway.

4. On the **Settings** tab, configure the following:
   - **Appliance Listening Port** – If required, you can change the TCP listening port. Make sure that you also specify the same port on all configured Barracuda Networks products. Default is port 5049.
   - **Debug Log Level**:
     - **Errors Only** = log errors only
     - **Info** = informational
     - **Debug** = verbose (most information logged)
   - **Group Options** (Barracuda Next Firewalls only) – select which option best fits your logging requirements. If group information is required for authenticated users, select one of these group name types.
   - **Cache groups for:** Amount of time, in minutes, to allow the DC Agent to rely on cached login information. Since users will most likely log in once/workday, the default time is 480 minutes, or 8 hours. The shorter this time is, the more often the DC Agent will retrieve login event information from the domain controller and pass it to the Barracuda Networks product, which requires more processing overhead.

## DC Agent Logging

Typically you'll only need the Log upon first install of the DC Agent to make sure everything is working as expected. Note that, if you were previously running another version of the DC Agent, that data logged while the old agent was running will no longer show in the user interface log window. That data is still, however, in the database and will appear in reports as usual. To monitor wireless device logins using Windows Network Policy Server (NPS) log events, see Using the Barracuda DC Agent with Microsoft Network Policy Server.




## Configure your Barracuda Networks Product

To ensure that your Barracuda Web Security Gateway or NextGen Firewall can communicate with the Barracuda DC Agent, you must configure the product as well.

- For the Barracuda Web Security Gateway, see the online help on the **USERS > Authentication** page in the web interface.
- For the Barracuda NG Firewall, see How to Configure the MSAD DC Client.

## How to Uninstall the Barracuda DC Agent

1. Verify that the Barracuda DC agent service is not running.
2. Use the **Add/Remove Programs** or **Programs and Features** tool in the Windows Control Panel to uninstall the Barracuda DC Agent.

.

## Figures

1. ActiveDirectories.jpg
2. Filters tab.png
3. Log WIndow 2013.png