How to Set Up the Barracuda Terminal Server Agent

https://campus.barracuda.com/doc/39823430/

The TS Agent assigns each user on a Microsoft Terminal Server a port range and distributes the user/port information to a configurable list of CloudGen and X-Series Firewalls. Install and configure the Barracuda TS Agent on your Microsoft Terminal Servers, and Citrix Desktop running on Microsoft Terminal Servers. Then configure your CloudGen Firewall to get user information from the Barracuda TS Agent.

By default, connections with the Barracuda TS Agent are SSL encrypted. To authenticate the remote TS Agent on the terminal server, use SSL client certificates. If no SSL certificates are configured, all incoming SSL connections are accepted.

System Requirements

- Windows Server 2008 R2 (x64)
  Before installing the Barracuda Terminal Server Agent on Windows Server 2008 R2, the following updates must be applied: KB2533623 and KB3033929
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
  The Barracuda TS Agent does not work on Windows Server 2008.
- Active Directory server (can be installed on the same machine or a different one)
  The administrative user must have read permission to the Active Directory **`memberOf`** attribute.
- Barracuda CloudGen Firewall or Barracuda NextGen Firewall X-Series version 6.6 or higher.

Step 1. Download the Barracuda TS Agent

Download the Barracuda TS Agent from your Barracuda Cloud Control Account.

1. Log into the Barracuda Download Portal.
2. In the search bar, enter "**Barracuda Terminal Server Agent**" and then click **Search**.
3. Download the latest Barracuda TS Agent version that is compatible with your system.

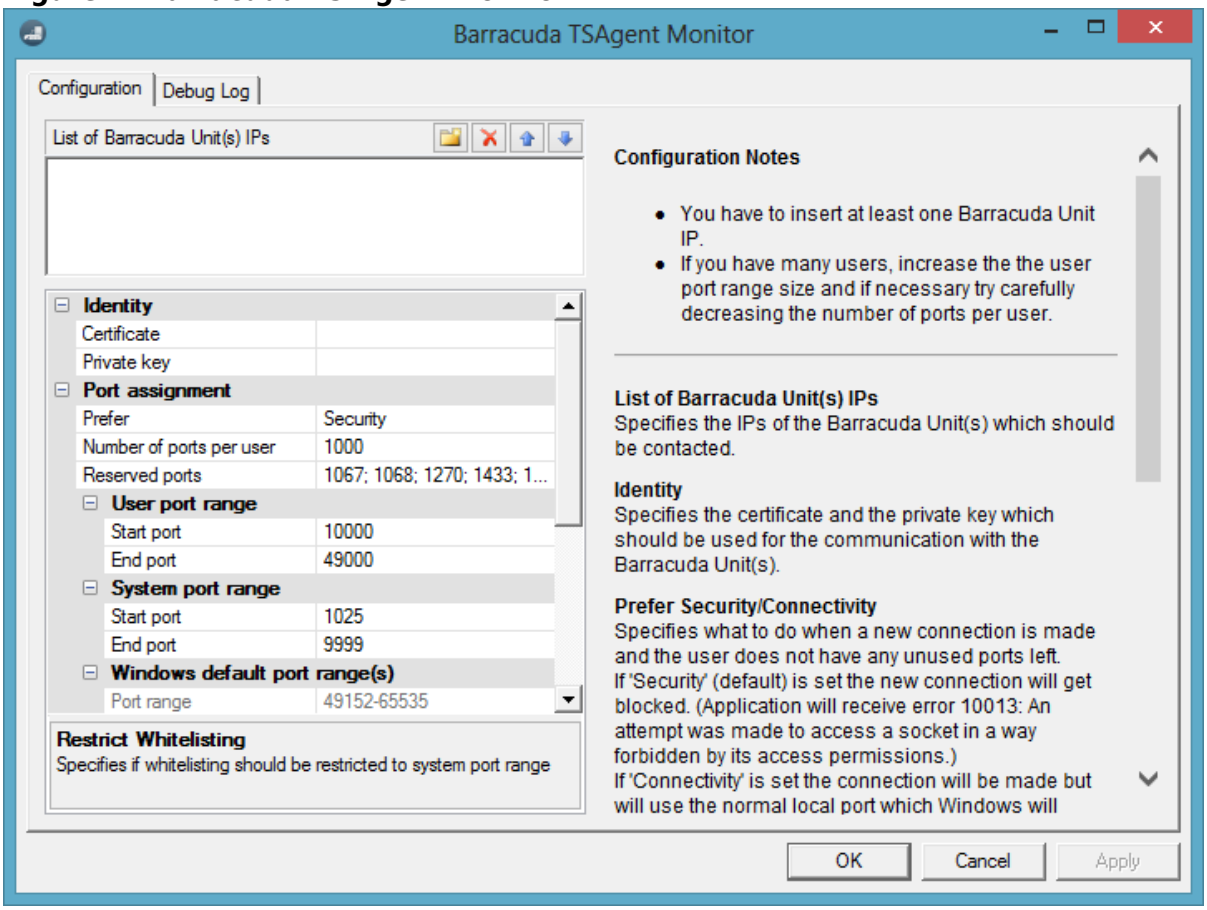
Step 2. Install the Barracuda TS Agent

Install and configure the Barracuda TS Agent on your Microsoft Terminal Server. Specify the IP

addresses of the firewalls that the TS Agent must communicate with.

1. Start the **setup.exe** file (or the **Terminal Server Agent.msi** package if you need an MSI installation package).
2. Complete the installation wizard.
3. After the setup finishes, reboot your server.
4. Launch **TS Agent Monitor** from the Windows start menu. The configuration interface of the Terminal Server Agent opens.

Figure 1. Barracuda TS Agent Monitor



5. In the **List of Barracuda Unit(s) IPs** section, click the folder icon and enter the management IP addresses of the firewalls that the Barracuda TS Agent must communicate with.
6. If required, change the default configuration settings. For more information on these settings, see **Configuration Options**.
7. Click **OK** or **Apply**.
8. After the TS Agent is installed, restart the server. You must restart the server to get the full functionality of the TS Agent and its security features.

Step 3. Configure Barracuda TS Agent Authentication

To use the TS Agent for authentication, configure the settings on your firewall. For instructions,

see How to Configure TS Agent Authentication.

Configuration Options

In the TS Agent interface, you can change the settings under the **Configuration** tab for your specific requirements. If your changes require a system restart, you are notified by a warning message in the interface. Any unsaved changes are highlighted in bold text.

Configuration Section	Description
List of Barracuda Unit(s) IPs	The management IP addresses of the firewalls that must receive user information from the Barracuda TS Agent. If the agent cannot establish a connection, it retries until it is successful. If you configured a non-default port, you can add it using the `IP:port` syntax.
Identity	The certificate and private key for communicating with the firewalls. With this certificate, firewalls can verify the identify of the Barracuda TS Agent.

Port Assignment	The ports that are assigned to users and how to handle connections when ports are not available. You can configure these settings: • **Prefer** – The action that is taken if there are no available ports for a new connection (e.g., if more users are connected than user port ranges available). You can select one of the following options: ◦ **Security** (default) – The connection is blocked, and the application receives error `10013: An attempt was made to access a socket in a way forbidden by its access permissions` ◦ **Connectivity** – The connection is assigned a local port by Windows. This means there is no user tracking for the connection. With this option, ensure that the port ranges do not overlap with the ranges that are displayed in the Windows default port range(s) field. • **Number of ports per user** – (Requires a system restart) The number of ports from the user port range that can be assigned for each user. For a Terminal Server that lets users browse the web, 1000 ports are recommended. If more than 39 users can possibly connect at the same time to the Terminal Server, increase the user port range. If you cannot increase the user port range, decrease the number of ports per user. If a user uses up all ports in their range, a log message is generated. Applications such as web browsers can open multiple connections in a short time frame. If you do not allocate enough ports for users, the application will not function properly for users who exceed the limit. • **Reserved Ports** – The TCP and UDP ports (IPv4 and IPv6) that must never be automatically assigned to a user. If you have an application that uses a specific listening port in one of the port ranges, add the port to this exclusion list. You can also add port ranges (e.g., `1050-1099`). The **Add Windows Server default port requirements** option adds the ports mentioned in the Microsoft Knowledge Base article 832017 (http://support.microsoft.com/kb/832017) to the list. By default, all ports specified in this article are included in the list so that they cannot be assigned by the Barracuda TS Agent. Changes to these settings require a system restart.
User Port Range (Requires a system restart)	The port range from which users are assigned their own ranges, excluding any reserved reserved ports. The number of these ranges is the number of users possible on the server. The range must have at least 100 ports, be large enough to hold at least 5 users, and not overlap with the system port range. If you set **Prefer** to **Connectivity**, ensure that the user port range does not overlap with the port range displayed in the **Windows Default Port Range(s)** section.
System Port Range (Requires a system restart)	The port range for the Microsoft Windows built-in 'System' user. The range must be at least 100 ports and not overlap with the user port range. If you set **Prefer** to **Connectivity**, ensure that the system port range does not overlap with the port range displayed in the **Windows Default Port Range(s)** section. Configuring a range that is too small can have severe effects on the whole server. For instance, the default configuration of the Microsoft DNS service requires 2500 ports from this range.

Windows Default Port Range(s)	(Read-only) Displays the ephemeral port ranges that are normally used by Windows if the Barracuda TS Agent does not change them. If you set **Prefer** to **Connectivity** , ensure that other port ranges do not overlap with the Windows default port range because the Barracuda TS Agent lets the OS assign a port number from the Windows default port range when there are no user or system ports available.
Advanced	This section offers the option to configure MSAD Domain Controller credentials. Only one Active Directory server can be queried. Defining multiple servers will result in queries to fail. • **Use domain usernames** – Select if reported usernames should be prefixed with the domain name. E.g., MYUSER is displayed as MYDOMAIN\MYUSER. • **Active Directory Server** – Enter the MSAD Domain Controller to be used for user group lookup. • **AD User** – Enter the username for the MSAD group lookup. • **AD Password** – Enter the password for the MSAD group lookup. • **Send Group Information** – Enable user group information to be sent. • **Query Nested Groups** – Collect nested group information. Enabling this setting can have impacts on the performance. • **Cache AD** – Enable caching of usernames and group information received from the Active Directory server. • **AD Cache Timeout** – Time in seconds after which cached information is considered invalid. • **Whitelisted Programs** – Enter the path to programs that should be allowed to bind connections to a specific port. For example: `\Device\Harddisk\Volume2\Windows\System32\example.exe` • **Restrict Whitelisting** – Select if whitelisting should be restricted to the system port range.

View Debug Log Files

Debug log files written by the Barracuda TS Agent are displayed under the **Debug Log** tab. For more information on the log messages, see Barracuda Terminal Server Agent Debug Log Messages.

Uninstalling the Barracuda TS Agent

To uninstall the Barracuda TS Agent using the InstallShield wizard:

1. Start the **setup.exe** file.
2. In the InstallShield wizard, click **Next**, and select **Remove** on the **Program Mainenance** page.

3. Complete the wizard to uninstall the Barracuda TS Agent.

To uninstall the Barracuda TS Agent from the Windows Control Panel:

1. Go to **Programs and Features**.
2. In the Uninstall or change a program list, right-click **Terminal Server Agent** and select **Uninstall**.
3. Complete the wizard to uninstall the Barracuda TS Agent.

Figures