

## How to Configure SSH

<https://campus.barracuda.com/doc/43847104/>

Each Barracuda NG Firewall system is routinely equipped with an SSH daemon listening on TCP port 22 on all administrative IP addresses (the primary box IP address and all other IP addresses that administrative services bind to). You should only open an SSH connection to the Barracuda NG Firewall when you are performing software updates or special maintenance tasks. Otherwise, perform all routine administrative tasks in Barracuda NG Admin.

You can use an external SSH client to open an SSH connection to the Barracuda NG Firewall. You can also use the terminal integrated in Barracuda NG Admin; direct access to the Barracuda NG Firewall is provided via SSH version 2. To access the SSH terminal, click the **SSH** tab.

### In this article:

You can enable event notifications for SSH, as well as view the SSH log for information such as system access and remote command execution. In the **Select Log File** list on the **Logs** page, you can find the `sshd` log file in the **Box** directory.

## Use an External SSH Client

If you prefer to use your own SSH client, configure NG Admin with the path to the executable:

1. Click on the **OPTIONS** tab in the top left corner.
2. Select **Settings**.
3. Expand the **Client Settings** section.
4. In the **External SSH Client** enter the command for for external SSH client. use **%ip** and **%user** to dynamically insert the IP address and user name. E.g., `C:\putty.exe %user@%ip`

## Configure SSH

1. Go to **CONFIGURATION > Full Configuration > Box > Advanced Configuration > SSH**.
2. Click **Lock**.
3. To configure the general settings for SSH, click **Basic Setup** from the **Configuration** menu in the left navigation pane.  
**Basic Setup Settings**

On the **Basic Setup** page for SSH, you can configure the following settings in the **General Settings** section:

Setting	Description
<b>Event on SSH</b>	<p>Specifies if event notifications should be triggered when the system succeeds or fails to start up or shut down (Events Daemon Startup Failed/Succeeded [2070/2071] and Daemon Shutdown Failed/Succeeded [2072/2073]). You can select any of the following options:</p> <ul style="list-style-type: none"> <li>◦ <i>Startup Failure</i></li> <li>◦ <i>Startup/Shutdown Failure</i></li> <li>◦ <i>Startup/Shutdown Failure + Startup Success</i></li> <li>◦ <i>Startup/Shutdown Failure + Startup/Shutdown Success</i></li> </ul> <p>You are not notified when SSHd is killed manually or just dies unexpectedly. These settings only pertain to SSHd behavior during controlled start or stop sequences.</p>
<b>Allow TCP Forwarding</b>	<p>Specifies if TCP is enabled or disabled. This setting is only available in <b>Advanced View</b> mode.</p> <p>Disabling TCP forwarding does not improve security. You must also deny shell access to users because forwarders can be installed with the <i>ssh</i> command.</p>
<b>Login Timeout</b>	<p>The maximum length of time in seconds that a user has to successfully log in before the server disconnects. The minimum time limit is <i>10</i> seconds. The default length of time is <i>90</i> seconds.</p>
<b>Permit Root Login</b>	<p>Permits or prohibits SSH logins for the root user.</p> <p>If you prohibit SSH logins for the root user, the following configuration entities will not work: <b>Box Exec</b> tab and <b>Software Update</b> tab.</p>
<b>Check User Home</b>	<p>Specifies whether sshd should check file modes and ownership of the user's files and home directory before accepting login. This is normally desirable because novices sometimes accidentally leave their directories or files writable. The default is yes. This setting is only available in <b>Advanced View</b> mode.</p>
<b>Send Keepalives</b>	<p>Specifies if the server should send keepalive messages. Default: yes.</p> <ul style="list-style-type: none"> <li>◦ To avoid hanging sessions, enable keepalive messages to monitor the connection. The server notices if the network goes down or the client host reboots. However, this may cause some inconveniences because connections are disconnected even when the route is temporarily down.</li> <li>◦ If keepalive messages are disabled, sessions may hang indefinitely on the server, leaving "ghost" users and consuming server resources.</li> </ul>
<b>Supported Protocols</b>	<p>Specifies which SSH versions are supported by sshd. You can enable support for only version 2, or you can enable support for both versions 2 and 1 (with version 2 being the preferred choice).</p> <p>Barracuda Networks recommends that you only enable support for SSH version 2 because version 1 is vulnerable to man-in-the-middle attacks. By default, the Barracuda Networks client tries to use version 2.</p> <p>This setting is only available in <b>Advanced View</b> mode.</p>

- To configure settings that are specific to each SSH version, click **Advanced Setup** from the **Configuration** menu in the left navigation pane.

#### SSH Version 2 Options

For SSH version 2, you can configure the following settings in the **Protocol Version 2 Options** section:

Setting	Description
<b>Allow Compression</b>	Specifies if compression should be enabled or disabled for SSH clients.
<b>Force Key Authentication</b>	Specifies if key usage is mandatory or optional for SSH clients. If key usage is mandatory for external SSH clients and you want to automate user logins, the private key of the client certificate on the Windows system must be generated in a UNIX compatible format. For instructions on how to generate the required key, see the following <a href="#">Handling Forced Key Authentication</a> section. This setting is only available in <b>Advanced View</b> mode.
<b>Secure FTP Support</b>	Specifies if sshd implements the sftp subsystem. Secure FTP may be viewed as a more comfortable alternative to the <i>humble scp</i> command when trying to transfer bulk data to or from the box. This setting is only available in <b>Advanced View</b> mode.

### SSH Version 1 Options

For SSH version 1, you can configure the following settings in the **Protocol Version 1 Options** section:

Setting	Description
<b>Server Key Length (Bits)</b>	Defines the number of bits in the ephemeral protocol version 1 server key. The minimum value is 512, and the default is 768.
<b>Key Regeneration Period</b>	Specifies the interval in seconds that the ephemeral server key is automatically regenerated after being used. Regenerating the key prevents the decryption of captured sessions if the keys are stolen. The key is only stored in memory. If you do not want the key to be regenerated, enter 0. The Barracuda Networks default is 900 (seconds).

5. Click **Send Changes** and **Activate**.

## Handling Forced Key Authentication

For various administrative purposes (such as collecting statistics with external tools), it may be desired to randomly connect to a system with an external SSH client, thereby omitting user interaction. Using the Microsoft Management Console (MMC), you can export a private key in encrypted PFX file format from the Certificate Store. However, this file is not usable by the Barracuda NG Firewall. You must convert the PFX file to an unencrypted private key in PEM format.

### 1. Create an Administrative Login

1. Go to **CONFIGURATION > Full Configuration > Box > Administrators**.
2. Click **+** to add a new administrative account.
3. Enter a name for the account and click **OK**.

4. In the **Administrator Authentication** section of the **Administrators** window, set **Authentication Level** to **Key**.
5. Import the public RSA key that has been issued for this user from the Microsoft Certificate Management Store.

## 2. Export the Private Key from the Certificate Management Store

1. On the Windows client, open the Certificate Management Store. At the DOS prompt, enter:  
`C:\windows\system32\certmgr.msc`
2. Browse to **Personal > Certificates**.
3. Right-click the certificate and select **All Tasks > Export**.
4. In the **Certificate Export Wizard**, select **Yes** to export the private key.
5. In the **PKCS #12** tab, clear the **Enable strong protection** check box.
6. Enter a password.
7. Specify a file name. For example, *private\_key.pfx*.

## 3. Copy the PKCS12 (.pfx) file to a UNIX Client Supporting OpenSSL

Copy the PFX file to a UNIX client that supports OpenSSL, such as the Barracuda NG Firewall.

## 4. Convert the RSA Key from PKCS12 Format to PEM Format (encrypted)

On the UNIX client, browse to the RSA key. At the command line, enter:

```
# openssl pkcs12 -in private_key.pfx  
-nocerts -out priv.key
```

where *priv.key* specifies the file name after conversion.

## 5. Extract the Private Key and Generate an OpenSSH SSH-2 Private Key (unencrypted)

At the command line, enter:

```
# openssl rsa -in priv.key > ~/.ssh/  
id_rsa_my_priv_key
```

where *id\_rsa\_my\_priv\_key* specifies the file name after decryption, and *~/.ssh/* is an arbitrarily chosen path on the UNIX client.

## 6. Log into the Barracuda NG Firewall

At the command line, enter:

```
# ssh -i ~/.ssh/id_rsa_my_priv_key
```

---

`-lloginname dest-ip`

where *loginname* specifies the name of the administrative account as defined in **Step 1**, and *dest-ip* specifies the Barracuda NG Firewall's login IP address.

Depending on the client that the key was converted on, you may need to change the file permissions of the private key file. If the gateway refuses to use the key, change the file permissions of the key by entering:

```
chmod 600 ~/.ssh/id_rsa_my_priv_key
```

You can use the transformed private key with third-party remote SSH clients. For example, you can use it with SSH agents or import it into PuTTYGen for conversion into the file format for PuTTY (.ppk).

© 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.