How to Configure Public Key Authentication

https://campus.barracuda.com/doc/39814729/

The public key authentication module is a very secure authentication mechanism, combining a client certificate and a passphrase with the possibility to store the authentication keys on an external storage device. No external services or appliances are needed. All keys are generated and managed by the Barracuda SSL VPN. You can configure the module as either a primary or secondary authentication mechanism. You must generate a private and public key which is then uploaded to the Barracuda SSL VPN and stored on the user's USB key device or home directory. You can choose to also let users generate their own initial public keys.

When users authenticate with a public key, the following steps are followed:

1. The Barracuda SSL VPN generates a random ticket (certificate).
2. The user selects the private key and enters the corresponding passphrase.
3. The ticket is signed with the user's private key and sent to the Barracuda SSL VPN.
4. The Barracuda SSL VPN verifies if the signed ticket is valid with its public key.
5. If the check is successful, the user is logged in.

Step 1. Configure the authentication scheme

To use public key authentication, add the **Authentication Key** module to an authentication scheme. If you want users to generate their own initial public keys, they must provide their passwords before they can generate the new keys.

Step 2. Configure key authentication settings

Specify if passphrases must conform to the SSL VPN security policy and if users can also generate keys.

1. Go to the **Manage System > ACCESS CONTROL > Security Settings** page.
2. Configure the settings in the **Key Authentication** section.
3. Click **Save Changes**.

Step 3. Generate keys

As an administrator, you can either generate keys for users or you can let users generate the keys

themselves.

Generate a key for a user

To generate a key for a user:

1. Go the **Manage System > ACCESS CONTROL > Accounts** page.
2. For the user that you want to generate the key for, click **More** and select **Generate Authentication Key**.
3. Enter the **Passphrase**. You can require the passphrase to conform to the password security policy.
4. Click **Generate**.
5. Download the zip file.
6. Click **Close**.
7. Distribute the key stored in the zip file to the individual user. For greater security, Barracuda Networks recommends that you use a USB key.

Make the user generate a key

To make a user generate a key, reset their authentication key.

1. Go to the **Manage System > ACCESS CONTROL > Accounts** page.
2. For the user who must create the authentication key, click **More** and select **Reset Authentication Key**.

During the next login, the user must enter their password and a new passphrase. The Barracuda SSL VPN then generates a zip file containing the authentication key, which the user can download.