# How to Configure SCEP Settings

https://campus.barracuda.com/doc/46208975/

SCEP (Simple Certificate Enrollment Protocol) supports the secure issuing of certificates to network devices in a scalable manner, using existing technology whenever possible. After configuring SCEP on the Barracuda NextGen Firewall F-Series, you can configure TINA and IPsec VPN tunnels to use SCEP with X.509 certificates.

The SCEP protocol supports the following operations:

- CA and RA public key distribution
- Certificate enrollment
- Certificate query
- CRL query

For more information about the SCEP protocol, see http://tools.ietf.org/html/draft-nourse-scep-17.

**In this article:**



When sending SCEP requests to a DNS hostname instead of a server IP address, verify that the DNS resolver of the gateway has been configured and is able to resolve it.

Connect the SCEP server to the Barracuda NextGen Firewall F-Series and configure the settings for your certificate requests.

#### Step 1. Configure SCEP Server Settings

1. Go to **CONFIGURATION > Configuration Tree > Box > Administrative Settings**.
2. In the left menu, expand **Configuration Mode** and click **Switch to Advanced**.
3. In the left menu, click **SCEP**.
4. Click **Lock**.
5. **Enable SCEP**.
6. Next to **SCEP Settings**, click **Set/Edit**. The **SCEP Settings** window opens.

7. In the **SCEP Server IP or Hostname** field, enter the IP address or hostname of the SCEP server where the SCEP requests will be sent to.
8. In the **SCEP URL path** field, enter the complete URL path of the SCEP server destination.
9. To configure **HTTP Authentication** for the SCEP server, click **Set** or **Edit**. The **SCEP HTTP Server Authentication** windows opens.
10. Specify the **Authentication Type**. You can select:
    - **None** – Only a password is used.
        - Enter a **Password**.
    - **Basic-Authentication –** No external authentication, only username and password.
        - Enter **Username** and **Password**.
    - **NTLM-Authentication** – NTLM authentication is used.
        1. Enter **Username** and **Password**.
        2. Set the **Domain** where the user is located.
11. Click **OK**.

#### Step 2. Configure X509 Request Settings

1. Specify the **Common Name** (CN) of the certificate (default: $BOXNAME). This value will be replaced with the real hostname of the box when the request is created.
2. In the **Alternative Name** field, specify the alternative name of the certificate (default: IP:$BOXIP). This value will be replaced with the real IP address of the box when the request is created.
3. Add any applicable information to the certificate request fields.

   The **X509 Key Usage** table defines specific key usage. Leave blank for general purpose key usage. Key pairs may be intended for particular purposes, such as encryption only, or signing only. The usage of any associated certificate can be restricted by adding key usage and extended key usage attributes to the PKCS#10.
4. Specify the **SCEP Password Policy**. You can select:
    - **No-Password** – No challenge password will be included in the certificate request.
    - **Password-from-Configuration –** The challenge password is statically configured on the Barracuda NextGen Control Center and will be included in the certificate request.
        - Enter the static challenge **SCEP Password**.
    - **Enter-Password-at-Box –** The challenge password will be prompted at the box when the certificate request is created.
    - **Get-Password-From-Website –** The challenge password is fetched from a website (typically the CA itself).
        1. In the **SCEP Password URL Path** field, enter the search path required when requesting the password from the CA website.
        2. In the **SCEP Password Search Pattern** field, enter the text to search for when requesting the password from the CA website.
5. Click **OK**.

#### Step 3. Configure Connection Details

Use the systems HTTP proxy settings or configure an explicit proxy connection.

1. From the **Proxy Settings** list, select whether to use the system settings or define explicit settings.

2. When using an explicit proxy, click **Set/Edit**. The **SCEP HTTP Proxy Settings** window opens.
    1. Enter the **Proxy IP Address** of the proxy server.
    2. In the **Proxy Port Number** field, enter the TCP port number on which the proxy server listens for requests (default: 3128).
    3. Select the **Proxy Authentication Type** used at the proxy server and fill in the credentials required for authentication.
3. Click **OK**.
4. Import the SCEP HTTPS client key and certificate.

#### Step 4. Configure Encoding Parameters

Specify the format in which the transaction ID field should be sent to the SCEP server and specify encryption settings.

1. From the **Transaction ID Encoding** list, specify the format for the transaction ID field:
    - **Binary** – The transaction ID field is sent in a binary format.
    - **Text** – The transaction ID field is sent in base64 encoded text format.

    Some SCEP servers support both binary and text format for the transaction ID. When experiencing problems with the binary format, switching to text format might help.
2. From the **PKCS7 Cipher** list, select the encoding cipher for use when communicating with the CA, accordingly to the CA settings.
3. From the **PKCS7 Hash** list, select the hashing method for use when communicating with the CA, accordingly to the CA settings.
4. Enable **PKCS7 Replay Protection** to protect your system from replay attacks.
5. From the **Select Encryption Certificate** list, select the certificate encryption method.
6. Click **Send Changes** and **Activate**.

SCEP is now configured. Unless the SCEP password policy was set to **Enter-Password-at-Box**, no further intervention is required for successful operation. However, Barracuda NextGen Admin offers options to interact with the SCEP subsystem in order to display SCEP status, re-initiate pending requests, force SCEP update or retry and set the SCEP password.

The SCEP status and control menus are available on the **CONTROL > Box** page under the **SCEP Control** menu, when connected to the Barracuda NextGen Firewall F-Series unit. The files held by the SCEP subsystem are stored in the `/opt/phion/certs/scep-*` directory on the box.

## Configure VPN Tunnels with SCEP

Configure your TINA and IPsec VPN tunnels to use SCEP with X.509 certificates. Import the root certificate and configure your VPN tunnel to accept SCEP as an identification type. For general information about configuring VPN tunnels with the GTI editor, see How to Create a VPN Tunnel with the VPN GTI Editor.

#### Step 1. Import the Certificate

1. Open to the **VPN GTI Editor** page for your range or cluster.
2. Click **Lock**.
3. Click the **Root Certificates** tab.
4. Right-click the table and select **Import PEM from File**.
5. Import the root certificate used by the CA for signing the SCEP certificates.

To specify the SCEP authentication method at the GTI level, GTI group level, or individually per tunnel, select the **Just like any other VPN tunnel setting** authentication method.

#### Step 2. Configure the VPN Tunnel

To configure your VPN tunnel to accept SCEP as an identification type:

1. Click the **TINA** or **IPSec** tab.
2. From the **Accept Identification Type** list, select **Box SCEP Certificate (CA signed)**.
3. Click **OK**.
4. Click **Send Changes** and **Activate**.