SOPHOS

Cybersecurity made simple.

Sophos UTM

Remote access through Sophos Connect

Product version: 9.706

Contents

1 Introduction

This guide helps you configure step by step remote access to the UTM using Sophos Connect. Sophos Connect is VPN software that runs on Microsoft Windows 10 and macOS 10.12 and later. It establishes highly secure, encrypted VPN tunnels for off-site employees.

First, you configure the UTM to allow remote access. Then, you enable the User Portal of the UTM for the remote access users.

The User Portal offers the Sophos Connect client software, the configuration files, the necessary keys, and a configuration guide to the remote access user. You must provide users with their login data for the User Portal.

2 Configuring UTM

You configure UTM through WebAdmin from your administration PC. For information on how to use WebAdmin, see the UTM administration guide.

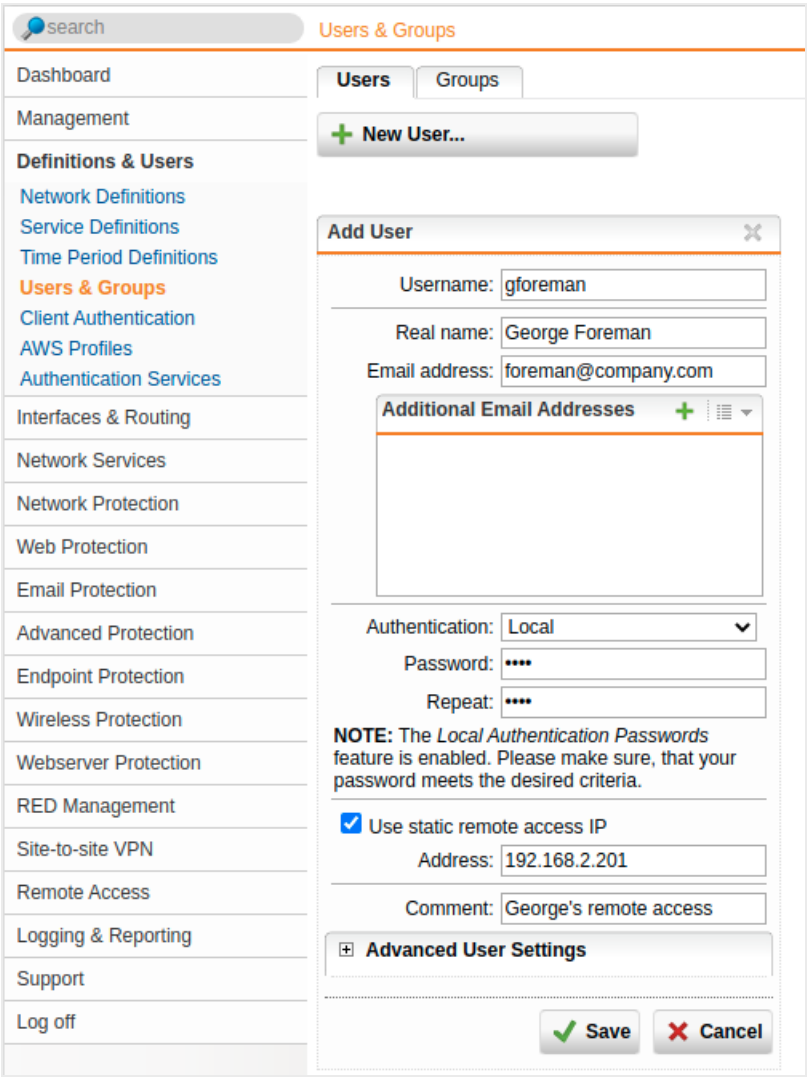
2.1 Defining a User Account

Create a user account that should be able to access the User Portal and use the VPN connection.

If you want to use an existing account, adopt the required settings from the user configured in the next steps.

1. Open the **Definitions & Users > Users & Groups > Users** page.
2. Click the **New User** button.

   The **Create New User** dialog shows.



3. Make the following settings:

   Username: Enter a username. Example: `gforeman`. The remote user needs this username later to log in to the User Portal.

   Real name: Enter the full name of the remote user. Example: `George Foreman`).

   Email address: Enter the e-mail address of the user. This creates an X.509 certificate for this user, using the e-mail address as the certificate's VPN ID. You can view the certificate under **Remote Access > Certificate Management > Certificates**.

   Authentication: For **Local** authentication, enter a password for the remote user.

   - **Password**: Enter the password for the user. You must provide it to the user for them to be able to log in to the User Portal.
   - **Repeat**: Confirm the password.

   Use static remote access IP (optional): You can assign the remote access user a static IP address. This IP address must not originate from the **IP address pool** used in the remote access settings. When the connection is being established, the IP address is automatically assigned to the host.

   Comment (optional): You can enter a description or additional information on the user.

4. Click **Save**.

Cross Reference: Find more information about user accounts in the UTM administration guide under **Definitions & Users**.

2.2 Configuring IPsec Settings

How to create a new IPsec connection, configure basic settings, and access control.

1. Go to **Remote Access > IPsec > Connections**.
2. Click **New IPsec Remote Access Rule**.

   The **Add IPsec Remote Access Rule** dialog box opens.

3. Make the following settings:

   Name: Enter a descriptive name for this connection.

   Interface: Select the network interface to use as the local endpoint of the IPsec tunnel.

   Local networks: Select the local networks that endpoint computers should be able to reach.

   Note: If you want that the IPsec-connected users can access the internet, select **Any** in the **Local Networks** box. Additionally, you must define appropriate masquerading or NAT rules later to allow this network traffic.

Virtual IP pool: By default, the UTM assigns addresses from the private IP space 10.242.4.x/24. This network is called the **VPN Pool (IPsec)**. To use a different network, create a different network here, or change the definition of **VPN Pool (IPsec)** under **Definitions & Users > Network Definitions**.

Policy: Select a predefined policy (in this example: AES-256) or go to **IPsec > Policies** tab to define your own policy.

Authentication type: IPsec remote access supports the following authentication types:

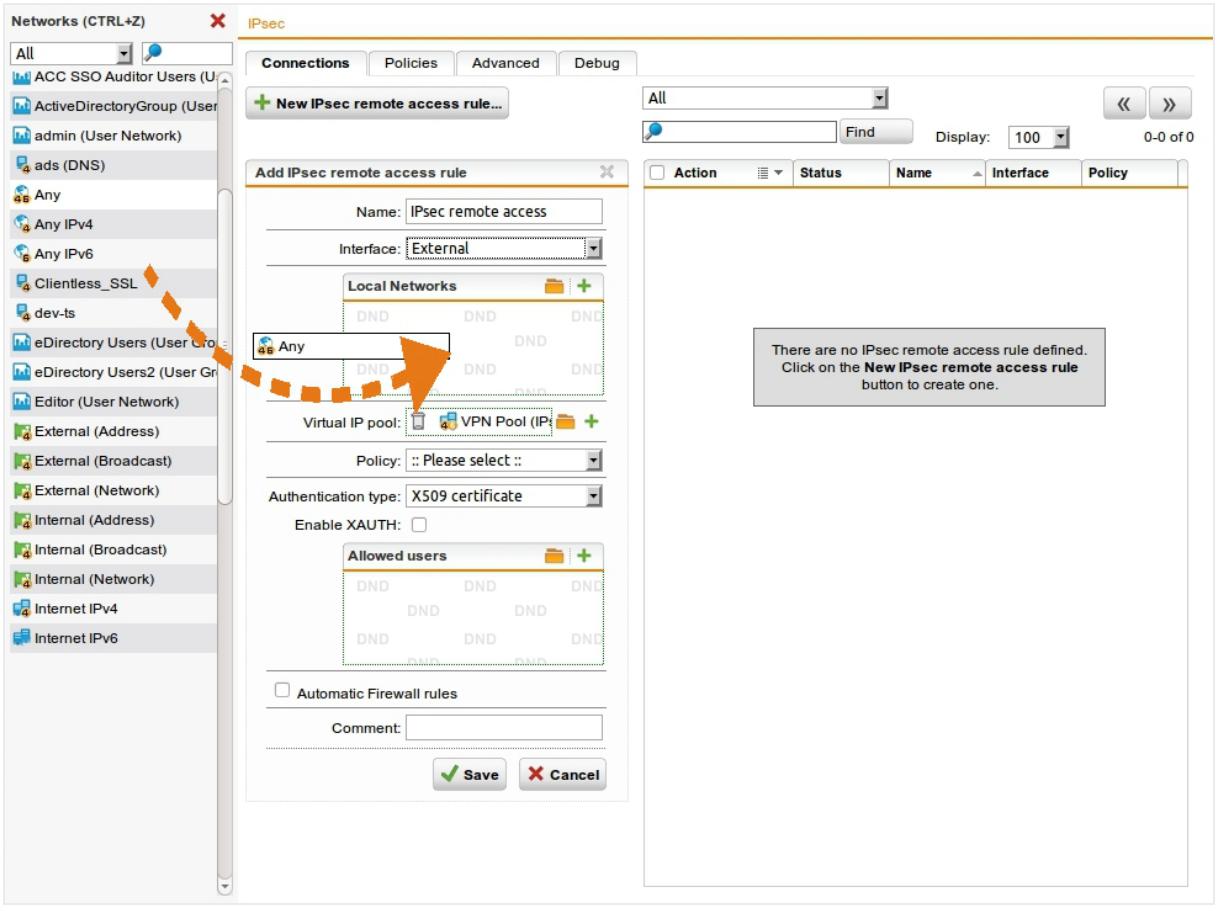
- **CA DN match**: The authentication is based on the Distinguished Name (DN).
  - **Authority**: Select the certificate authority **VPN Signing CA** for the VPN users.
  - **DN mask**: To use a Distinguished Name as an ID, you need information from the X.509 index. Possible indications are Country (C), State (ST), Local (L), Organization (O), Unit (OU), Common Name (CN), and E-Mail Address (E).
  - **Enable XAUTH** (optional): Turn on to use extended authentication of users against configured backends.
  - **Preshared key**
    - **Preshared key**: Enter the shared secret. This is a secure phrase or password used to encrypt the traffic using the encryption algorithm for IPsec.
    - **Confirm**: Confirm the shared secret.

      Security Note: Use a secure password. Ensure that this password does not fall into the hands of unauthorized third parties. With this password, an attacker can build a connection to the internal network. We recommend changing this password at regular intervals.

    Enable XAUTH (optional): Turn on to use extended authentication of users against configured backends. Turn on for users to be able to retrieve their access information from the User Portal and add the users to the **Allowed users** box.
- **X.509 certificate**
  - **Enable XAUTH** (optional): Turn on to use extended authentication of users against configured backends.
  - **Allowed users**: Select the users who had been created automatically and who should use the IPsec connection.
  - **Automatic firewall rules**: Select to automatically create firewall rules for the tunnel traffic. These rules exist only for the lifetime of the tunnel. If you don't select this option, you must define the firewall rules manually (see below).

Comment (optional): Add a description or other information about the IPsec connection.

4. Click **Save**.



5. Enable the IPsec rule.

   You can enable the rule now or later after completing the whole UTM configuration.

   Click the toggle switch in front of the rule to activate the rule.

   The switch turns green. The IPsec remote access rule is active now.

Cross Reference: For more information about remote access go to **Remote Access** in the UTM administration guide.

2.3 Configuring Advanced IPsec Settings

1. Go to **Remote Access > IPsec > Advanced**.
2. In the **Local X.509 Certificate** section, select a certificate.

   By default, the **Local X509 Cert** is used for IPsec connections to authenticate the server.
3. Click **Apply**.
4. In the **Dead Peer Detection (DPD)** section, turn on DPD.

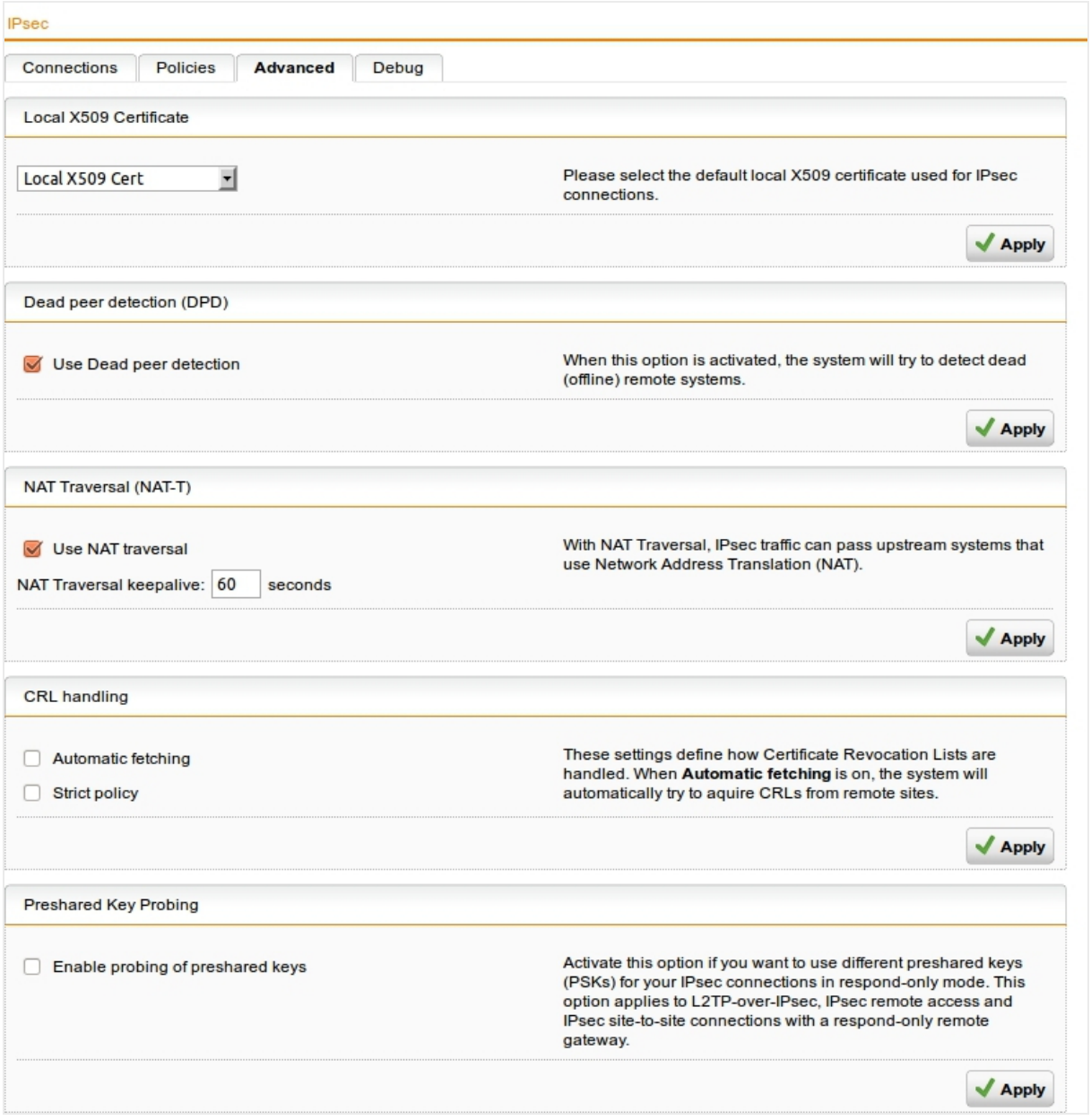
DPD is enabled by default. It is used to automatically determine whether a remote IPsec peer can still be reached. Usually, it is safe to always enable this option. The IPsec peers automatically determine whether the remote side supports DPD and fall back to normal mode if not.

5. Click **Apply**.
6. In the **NAT Traversal (NAT-T)** section, enable NAT-T.

   NAT-T is enabled by default with a keepalive of 60 seconds. It allows IPsec traffic to pass upstream systems that use Network Address Translation (NAT). You can change the keepalive interval for NAT traversal in the field **NAT traversal keepalive**.
7. Click **Apply**.
8. Configure **CRL Handling** (optional).

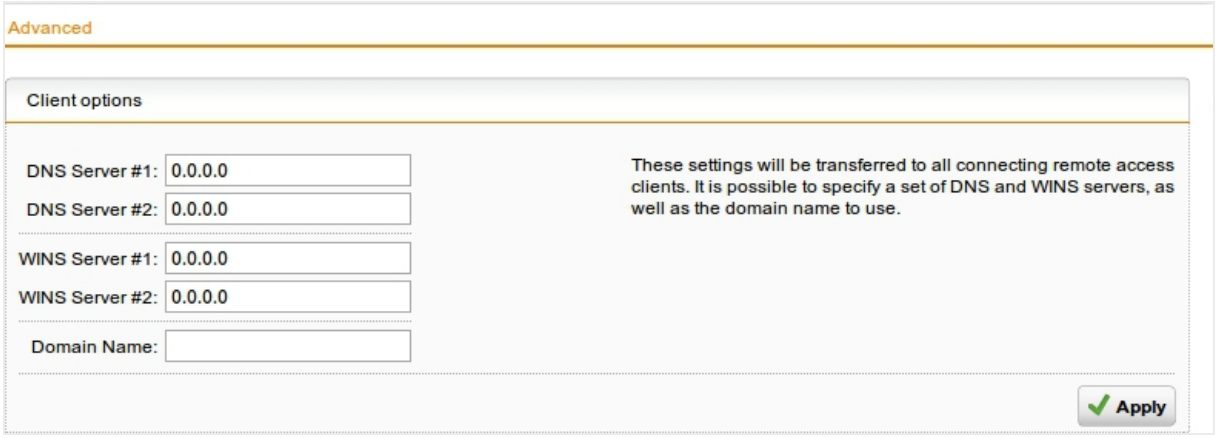
   There might be situations, in which the provider of a certificate attempts to revoke the confirmation awarded with still valid certificates, for example if it has become known that the receiver of the certificate fraudulently obtained it by using wrong data (name, etc.) or because an attacker has got hold of the private key, which is part of the certified public key. For this purpose, so-called Certificate Revocation Lists or CRLs are used. They normally contain the serial numbers of those certificates of a certifying instance that have been held invalid before their expiration.

   - **Automatic fetching**:Automatically requests the CRL through the URL defined in the partner certificate via HTTP, Anonymous FTP, or LDAP Version 3. On request, the CRL can be downloaded, saved, and updated, once the validity period has expired.
   - **Strict policy**: Using the option, any partner certificate without a corresponding CRL is rejected.
9. Click **Apply**.



10. Open the **Remote Access > Advanced** page.

    You can define name servers (DNS and WINS) and the name service domain that must be assigned to hosts during the connection establishment.



11. Click **Apply**.

2.4 Creating Firewall and Masquerading Rules

2.4.1 Defining a Firewall Rule

Only for authentication based on X.509 certificate, you do not need define this firewall rule if you have enabled the **Automatic firewall rule** function during the configuration of IPsec.

1. Open the **Network Protection > Firewall > Rules** page.
2. Click **New Rule**.

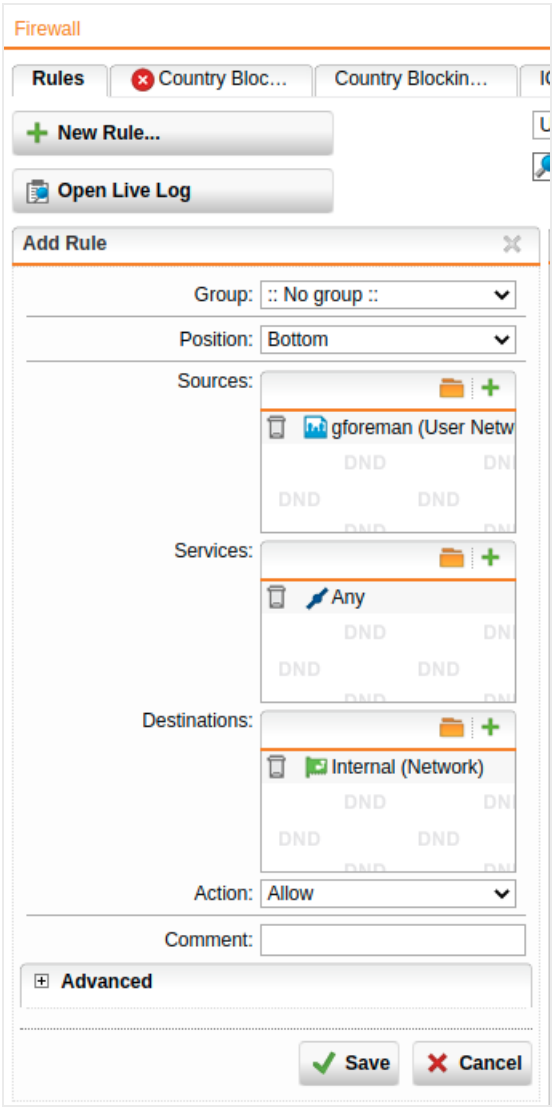
   The **Add Rule** dialog shows.
3. Make the following settings:

   Sources: Add the remote user network (in this example: **gforeman**).

   Services: Add the allowed services.

   Destinations: Add the allowed networks. Example: **Internal (Network)**. If remote users should be able to access internet you must select the appropriate network definition. Example: **Internet** or **Any**.

   Action: Select **Allow**.

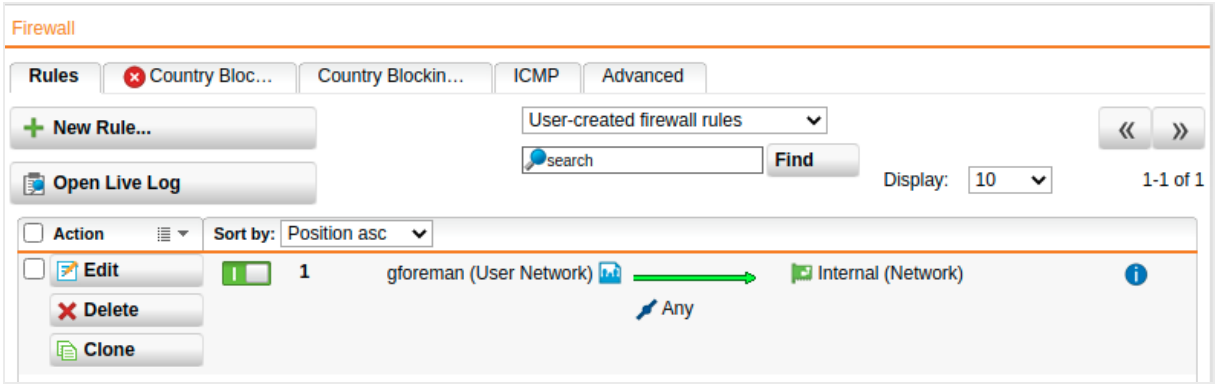


4. Click **Save**.

   The firewall rule shows in the list and is turned off (switch is gray).

5. Click the switch to turn on the rule.

   The switch turns green.



The UTM evaluates active rules from the top down until it finds a match. Once it finds a match, it doesn't evaluate subsequent rules. So, position the specific rules above the less specific rules.

Security Note: Don't place a rule such as **Any – Any – Any – Allow** at the top, since this matches all traffic, and the following rules are never evaluated.

Cross Reference: Find more information about firewall rules in the UTM administration guide under **Network Protection**.

2.4.2 Create a Masquerading Rule

Note: This is an optional step depending on your environment.

Masquerading is used to mask the IP addresses of one network with the IP addresses of a second network, in this example: **gforeman** with **External**. Thus, remote users who only have private IP addresses can, for example, surf on the internet with a public IP address. Depending on your system configuration, masquerading can also be necessary for other connection types.

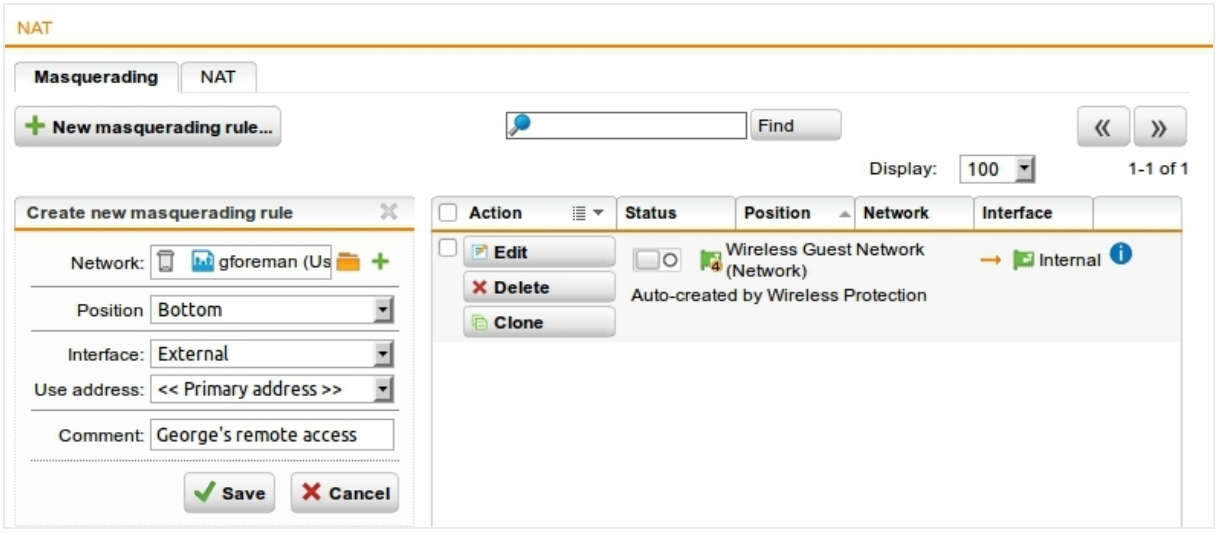
1. Go to **Network Protection > NAT > Masquerading**.
2. Click **New Masquerading Rule**.

   The **Add Masquerading Rule** dialog shows.
3. Make the following settings:

   Network: Select the network of the remote endpoint (in this example: **gforeman**).

   Interface: Select the interface that should be used to mask the clients (in this example: **External**).

   Use address: If the selected interface has more than one IP address, you can define which IP address should be used for masquerading. Default: **Primary address**.



4. Click **Save**.

   The masquerading rule shows at the end of the list and is turned off (switch shows gray).

5. Click the switch to turn on the rule.

   The switch turns green.

Cross Reference: Find more information about masquerading rules in the UTM administration guide under **Network Services**.

6. Optionally, activate the proxies:

   If the remote employees should access URL services via the remote access you may configure the required proxies on the UTM – this would be the DNS and HTTP proxy for example.

   Cross Reference: Find more information about proxies in the UTM administration guide.

Depending on the security policy of your organization and the requirements of your network, you might have to make additional settings.

After configuring the VPN server (headquarter), remote users must configure their devices.

3 Configuring the Remote Client

For users to be able to access the UTM through Sophos Connect, they must configure their client device. For that, they must access the UTM User Portal with a browser from their remote client. There, they can download the Sophos Connect client and view installation instructions. Sophos Connect can be installed on Windows and macOS.

3.1 Getting the Software and Certificates

The UTM User Portal is available to all remote access users. They can download guides and tools for the configuration of their endpoint computer. They should receive the following user credentials for the User Portal from their system administrator: IP address, username, and password.

For authentication with an X.509 certificate, the User Portal offers the Sophos Connect client software, configuration files, and necessary keys.

Users must follow these steps:

1. Open a browser and enter the address of the User Portal.

   Example: `https://218.93.117.220`.

   A security note may show.

2. (Optional) Accept the security note.

   Depending on the browser, click **I Understand the Risks > Add Exception > Confirm Security Exception** (Mozilla Firefox), or **Proceed Anyway** (Google Chrome).

3. Log in to the User Portal using your credentials.

   Username: The username you received from your administrator.

   Password: The password you received from your administrator.

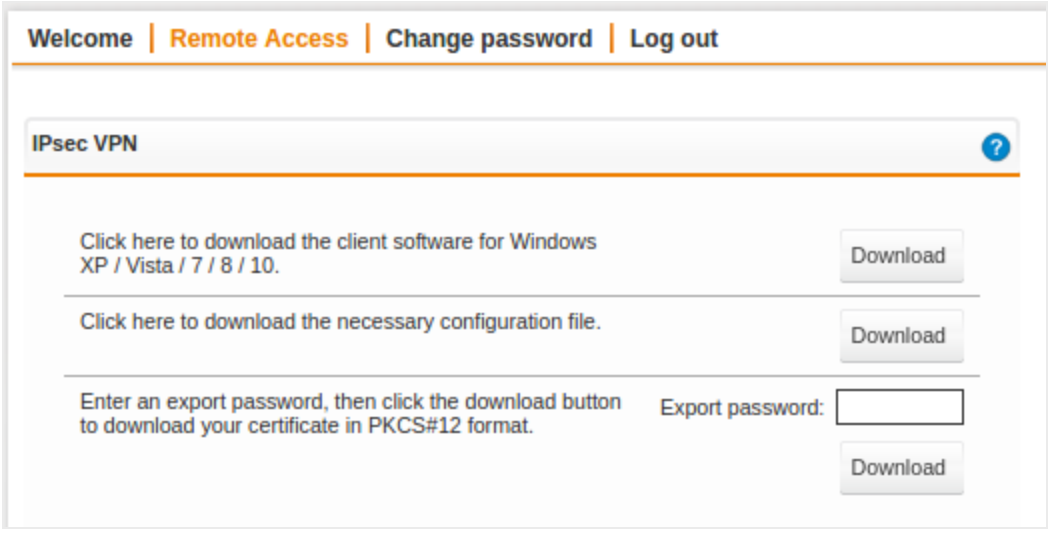
   Click **Login**.

4. Go to **Remote Access**.

   This page can contain multiple sections, depending on the remote access connection types (IPsec, SSL, L2TP, PPTP, iOS devices) your administrator enabled for you.

   Most sections have a help icon that links to the respective configuration guide.

   The **IPsec VPN** section contains the former, NCP-based executable endpoint computer software, configuration file, and certificate (if selected) for the remote access client.

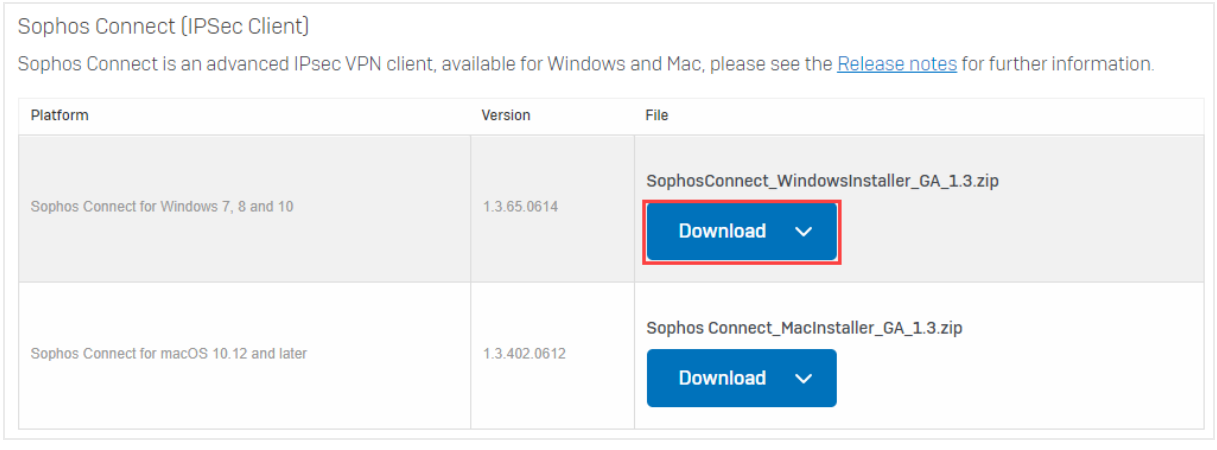


5. In the **Export password** field, enter a password to secure the PKCS#12 container before downloading the certificate. Note that you will need the security password of the certificate later on.
6. Start the download processes by clicking the respective **Download** button. Download all files and store them in a location of your choice. You will need those files later on when installing and configuring the Sophos client.
7. Click **Log out** to close the User Portal session.

The rest of the configuration takes place in the Sophos Connect client.

3.2 Download and Install Sophos Connect Client

1. Go to the UTM Support Downloads website.
2. Scroll down to the **Sophos Connect (IPsec Client)** section and download the client appropriate for your operating system.

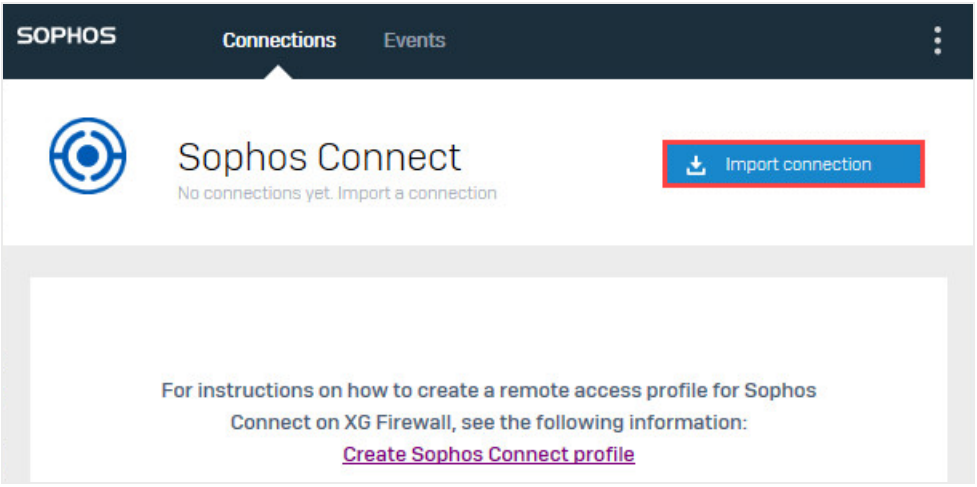


3. Send the .ini or the .scx file to the users.
4. On their computer, users must install SophosConnect.msi that they downloaded before.

5. They must start Sophos Connect.

   Note: Sophos Connect runs in the system tray.

6. Users must click **Import Connection** and select the .ini or the .scx file.

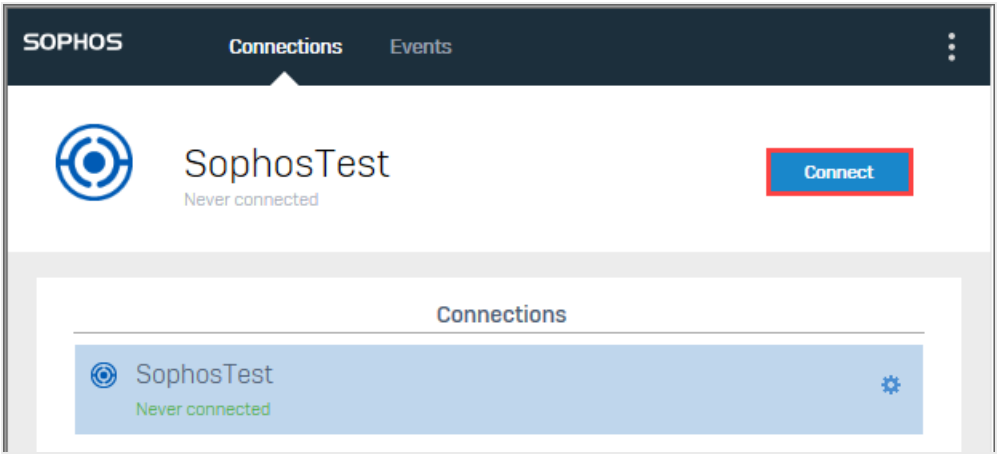


   If an X.509 certificate is required for authentication, users see an additional step **Import certificate credentials**. They must do the following:

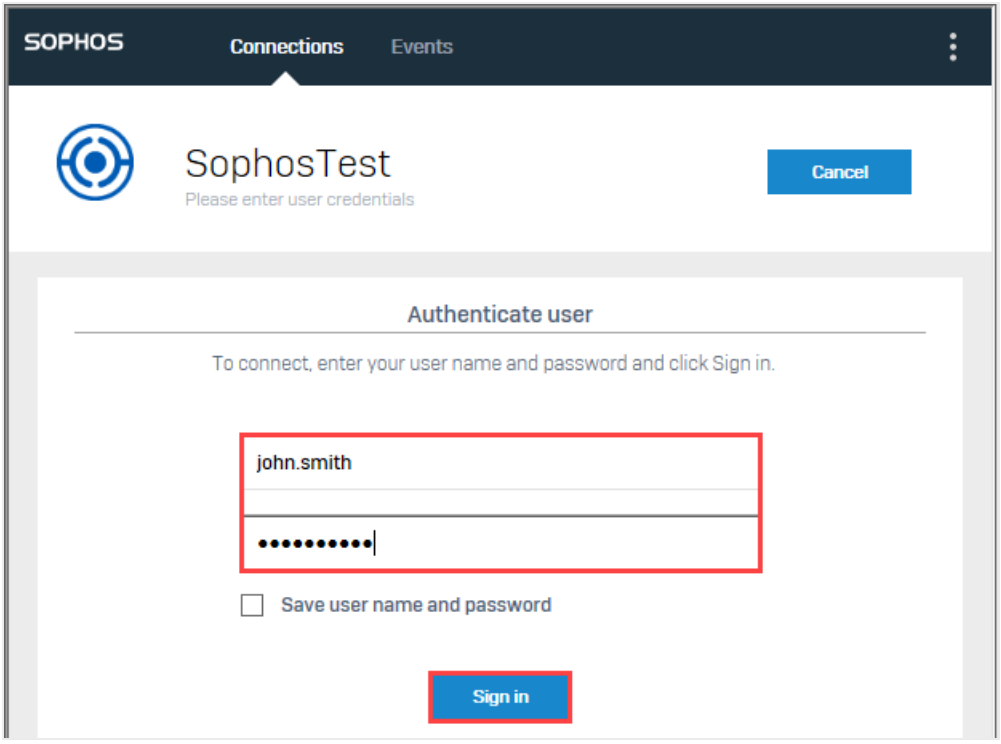
   a. Enter the export password for the PKCS#12 certificate.

   b. Click **Import PKCS#12 file**, browse to the location where they stored the certificate and select it.

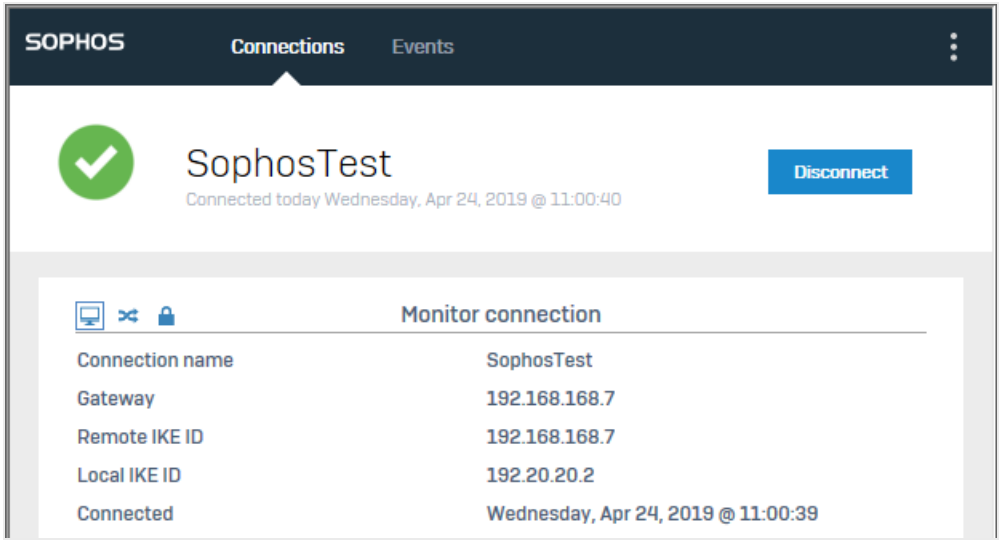
7. Users must click **Connect** to turn on the connection.



8. They must enter their credentials and click **Sign in**.



The connection is being established:

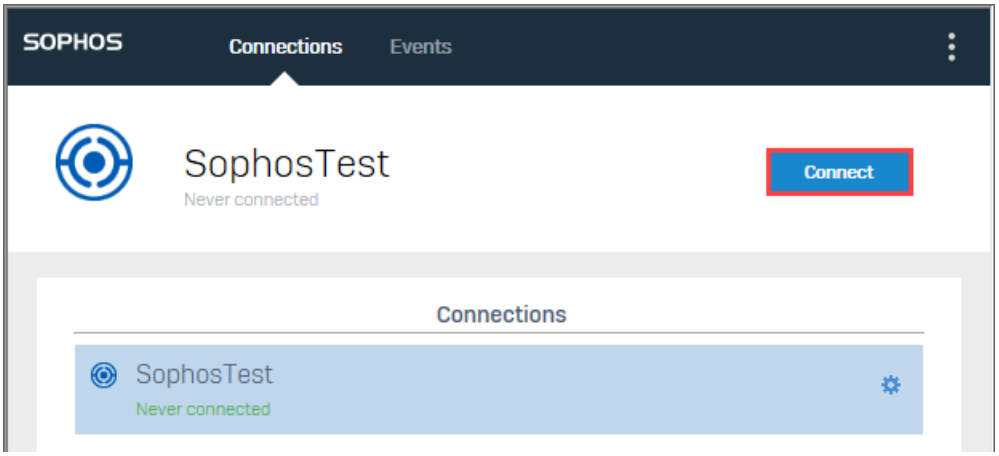


3.3 Install and Configure Sophos Connect

1. Send the .ini or the .scx file to the users.
2. On each user's computer, install SophosConnect.msi that you've downloaded earlier.
3. Run Sophos Connect.

   Note: This will stay in the system tray of the workstation.

4. Click Import Connection and select the .ini or the .scx file.
5. Click Connect to turn on the connection.



3.4 Security Note on Backup Images

Each installation of the Sophos Connect client generates a unique GUID on a clean installation. The GUID is saved in a file called scvpn.uid and lives in the installation folder. This GUID will carry over on upgrade.

If you want to create a backup image (Ghost image) of endpoint computers that includes the Sophos Connect client, you should remove the scvpn.uid file beforehand. Follow the steps below depending on the operation system. You can also include them in a script.

3.4.1 On Windows

1. Open the command line and run the following commands:

```
net stop scvpn
del c:\Program Files (x86)\sophos\connect\scvpn.guid
```

3.4.2 On macOS

1. Open the command line and run the following commands:

```
net stop scvpn
sudo rm /Library/Sophos Connect/scvpn.uid
```

3.5 Related Information

Sophos Connect: Command-line interface (CLI) guide: KBA 000038531

Open source software attributions

Third-party license information

Copyright notice

http://www.sophos.com

Limited Warranty

No guarantee is given for the correctness of the information contained in this document.