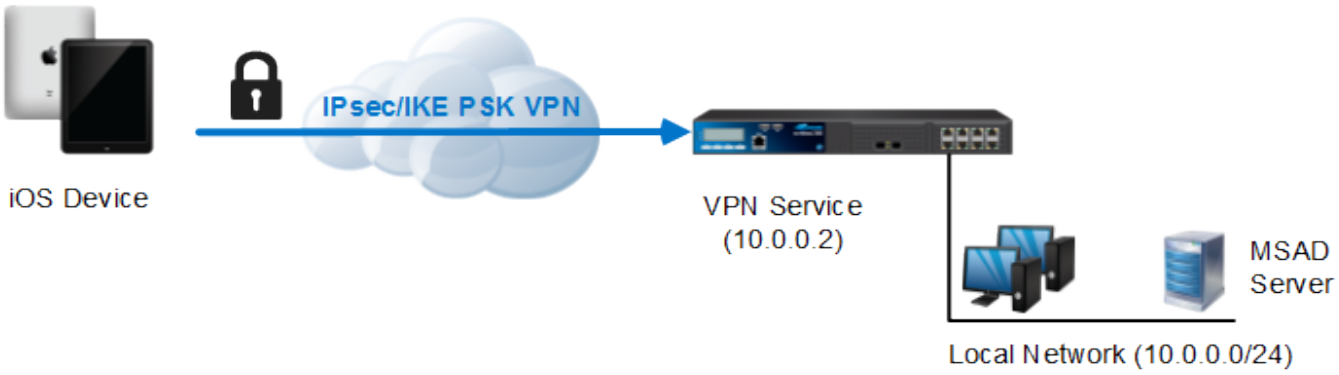
How to Configure a Client-to-Site IPsec VPN with PSK

https://campus.barracuda.com/doc/43847307/

To let users access a Client-to-Site IPsec VPN without having to install X.509 certificates on their client devices, you can create an IPsec Client-to-Site VPN group policy using a preshared key (PSK). For users with mobile devices that are not managed by a mobile device management platform (MDM), using a PSK is more convenient than having to install client certificates for authentication. To allow multiple concurrent Client-to-Site connections for a single user a premium remote connectivity license is required.

The connection is set up in two phases by the Internet Key Exchange (IKE). In phase I, the PSK is used to create a secure channel. Phase II uses this channel to negotiate the security associations for the IPsec service.



In this article:

Supported VPN Clients

Currently, only Apple iOS and Android devices are supported for IPsec VPNs with PSK.

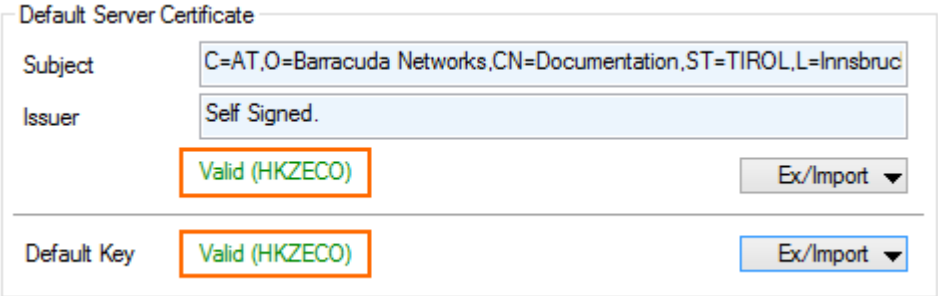
- For instructions on how to configure your Apple iOS device to use the IPsec PSK VPN, see How to Configure Apple iOS Devices for Client-to-Site IPsec VPNs with PSK.
- For instructions on how to configure Android device to use the IPsec PSK VPN, see How to Configure Android Devices for Client-to-Site IPsec VPNs with PSK.

Before You Begin

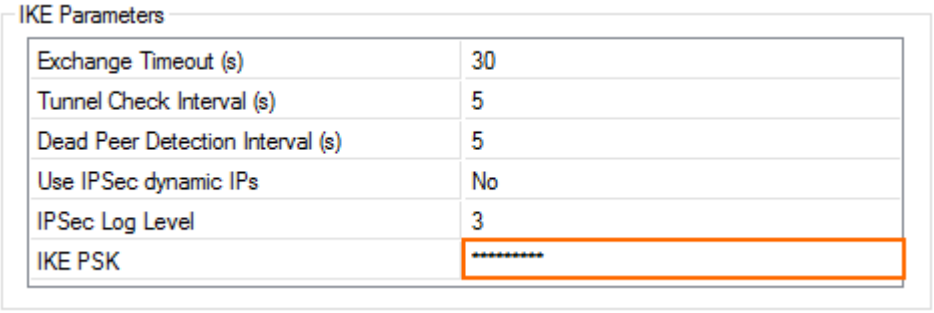
- Verify that the VPN service has been properly configured and that the **server** and **default certificates** are installed. The certificate must use DNS:*FQDN (e.g., DNS:vpn.mydomain.com*) as the **SubAltName** for iOS and Android devices to be able to connect. The FQDN must resolve to the IP address the VPN service is listening on. For more information, see How to Set Up VPN Certificates.
- Configure an external or local authentication service. For more information, see Authentication.
- Identify the subnet and gateway address for the VPN service in your network (e.g., `192.168.6.0/24` *and* `192.168.6.254`).
- Identify the IP address on which the VPN service will listen (e.g., `10.0.0.2`).

Step 1. Configure the Client Network and Gateway and PSK Key

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. Verify that the default server certificate and key are valid.
    1. Right-click the **Settings** table and select **Edit Server Settings**.
    2. Verify that the **Default Server Certificate** and **Default Key** are both valid (green). If the **Default Server Certificate** and **Default Key** are not valid, seeHow to Set Up VPN Certificates.

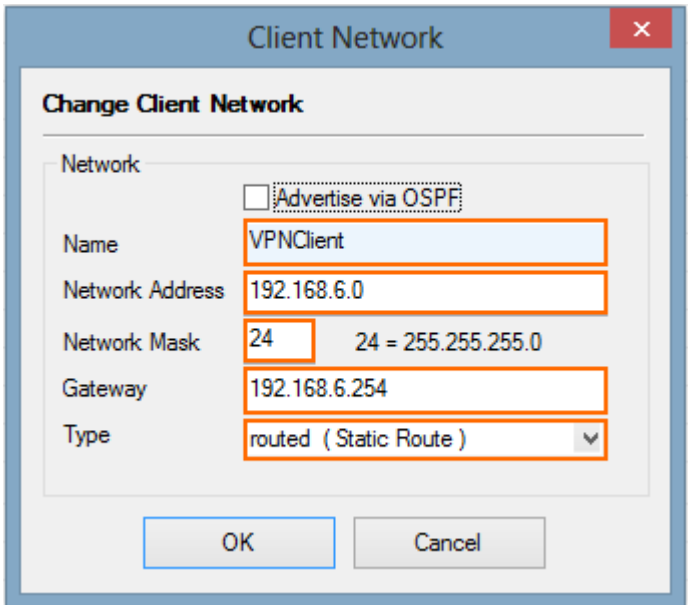


4. In the **Server Settings** window, click on the **Advanced** tab.
5. In the **IKE Parameter** section, enter the **IKE PSK** key. E.g., `pre$haredKey`



6. Configure the client network.
    1. Click the **Client Networks** tab.
    2. Right-click the table and select **New Client Network**. The **Client Network** window opens.
    3. In the **Client Network** window, configure the following settings:

- **Name** – Enter a descriptive name for the network.
- **Network Address** – Enter the base network address for the VPN clients. E.g., `192.168.6.0`
- **Network Mask** – Enter the subnet mask for the VPN client network. E.g., 24
- **Gateway** – Enter the gateway network address. E.g., 192.168.6.254
- **Type** – Select **routed (Static Route)**. VPN Clients are assigned an address via DHCP (fixed or dynamic) in a separate network reserved for the VPN. A static route on the Barracuda NG Firewall leads to the local network.

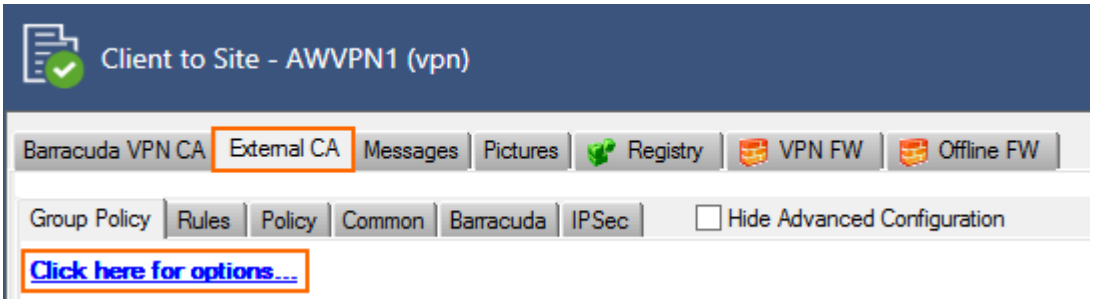


7. Click **OK**.
8. Click **Send Changes** and **Activate**.

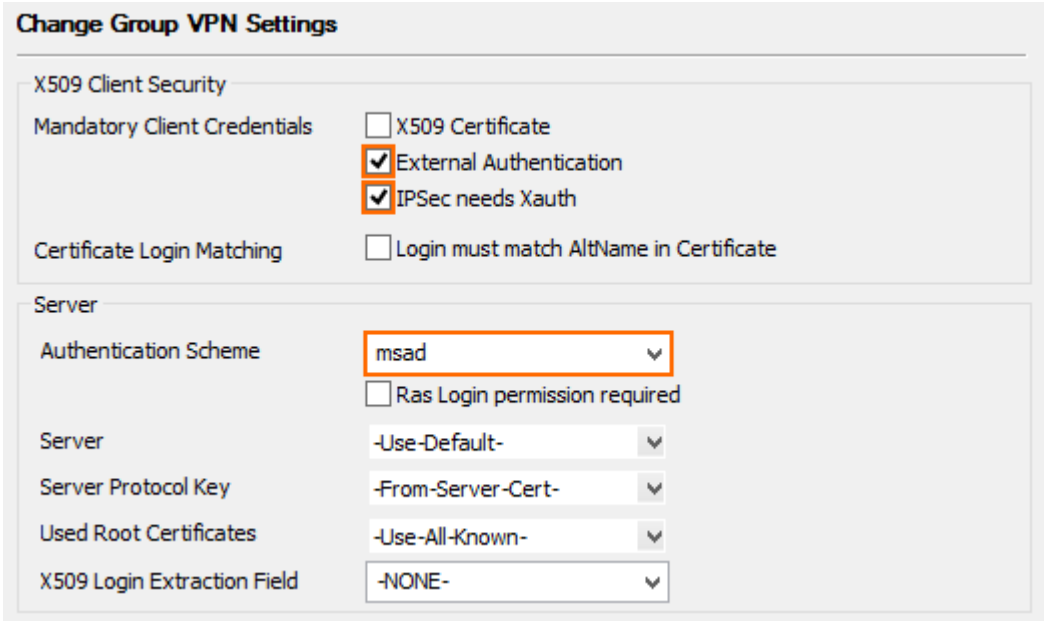
Step 2. Configure VPN Group Match Settings

Configure the global authentication settings for VPN tunnels using an external X.509 certificate and group configurations.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > Client to Site**.
2. Click **Lock**.
3. Click the **External CA** tab.
4. Click the **Click here for options** link. The **Group VPN Settings** window opens.



5. In the **Group VPN Settings** window, configure the following settings:
   1. In the **X509 Client Security** section, select the **External Authentication** checkbox.
   2. In the **Server** section, select your previously configured authentication service from the **Authentication Scheme** list. For more information, see Authentication.



6. Click **OK**.
7. Click **Send Changes** and **Activate**.

Step 3. Create a VPN Group Policy

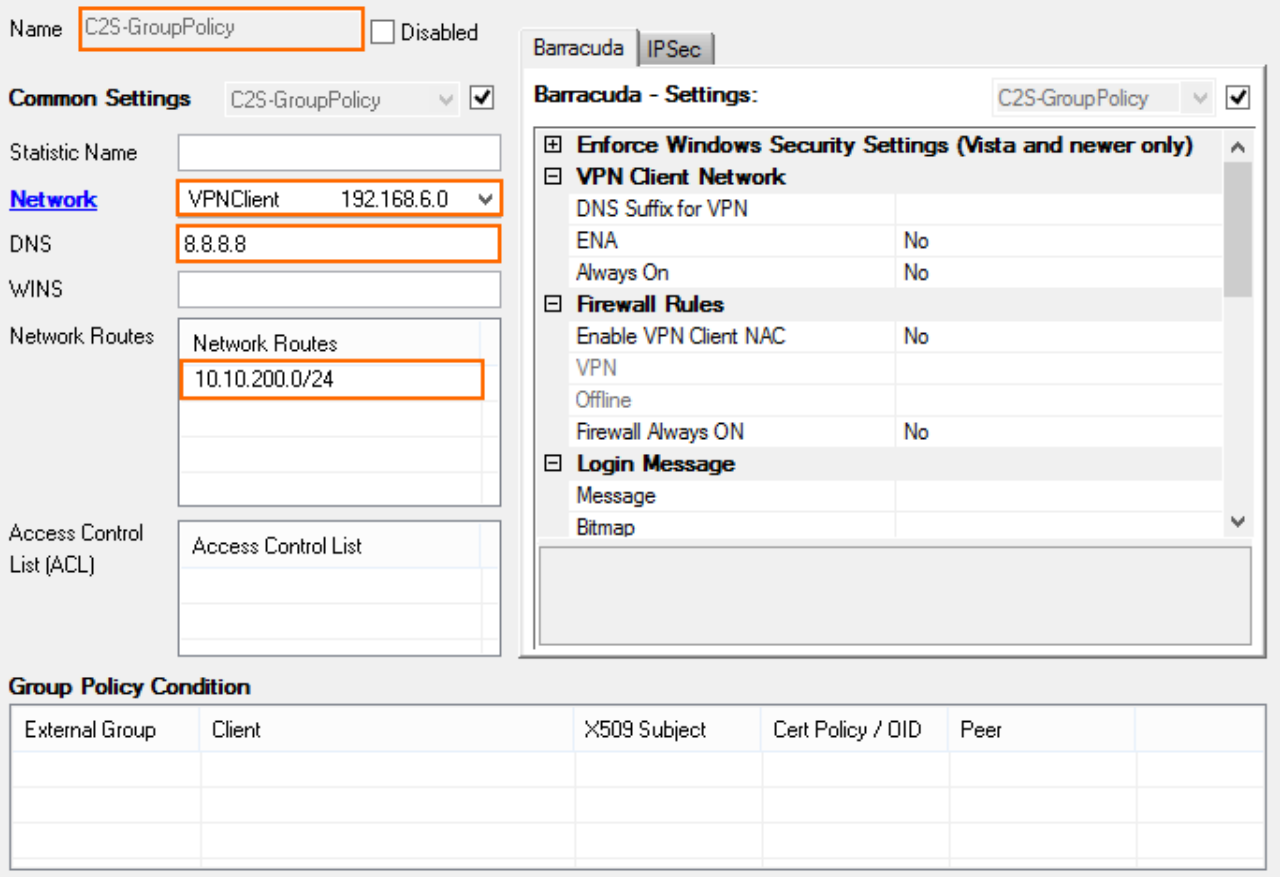
The **VPN Group Policy** specifies the network IPsec settings. You can create group patterns to require users to meet certain criteria, as provided by the group membership of the external authentication server (e.g., `CN=vpnusers*`). You can also define conditions to be met by the certificate (e.g., `O(Organization)` must be the company name).

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > Client to Site**.
2. Click **Lock**.
3. Click on the **External CA** tab and then click the **Group Policy** tab.
4. Right-click the table and select **New Group Policy**. The **Edit Group Policy** window opens.
5. Enter a name for the **Group Policy**. For example, `IPsecPSKGroupPolicyName`.

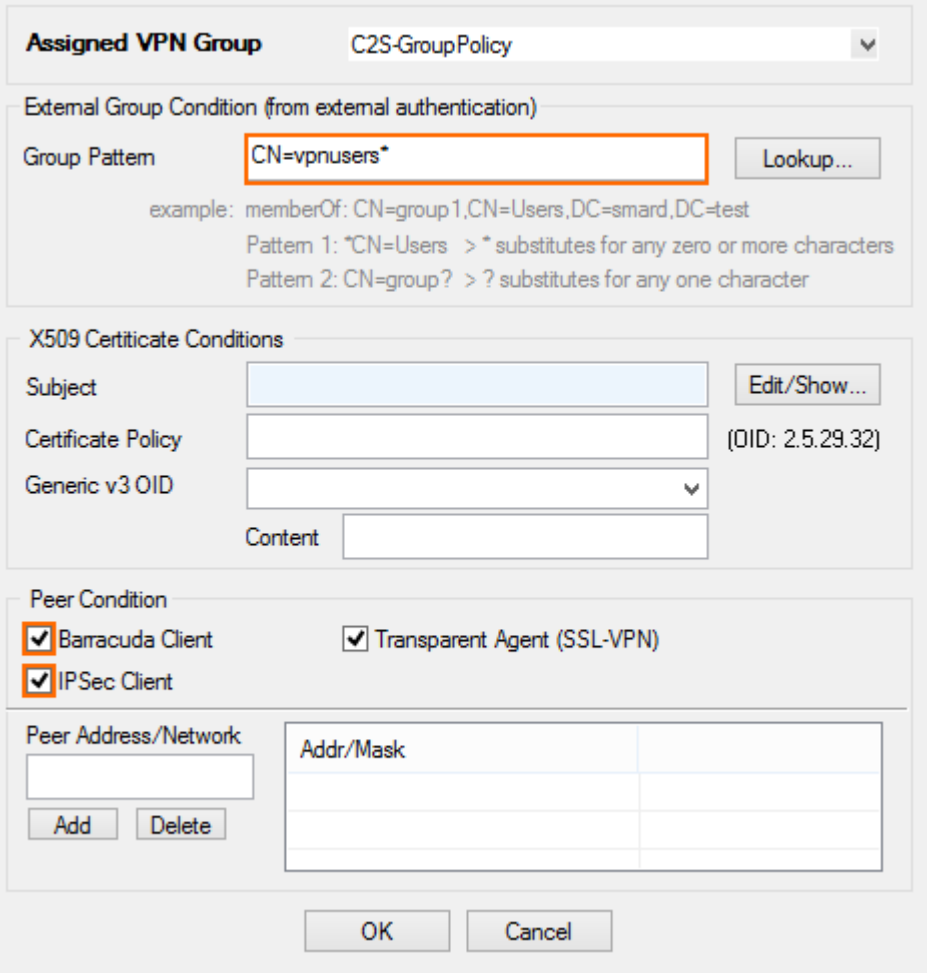
The name of the group policy is used to associate VPN clients with the correct group policy. Depending on the VPN client, it can be referred to as **group name** or **IPsec identifier**. For more information, see How to Configure Android Devices for Client-to-Site IPsec VPNs with PSK or How to Configure Apple iOS Devices for Client-to-Site IPsec VPNs with PSK.

6. From the **Network** list, select the VPN client network.
7. In the **Network Routes** table, enter the network that must be reachable through the VPN connection. For example, `10.10.200.0/24`.

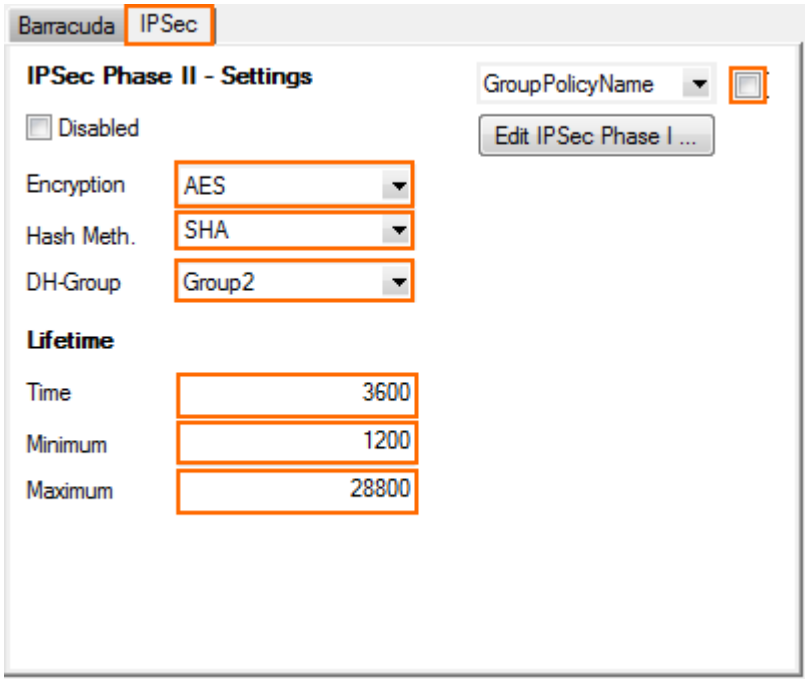
   To route all traffic through the Client-to-Site VPN tunnel, add a `0.0.0.0/0` network route.



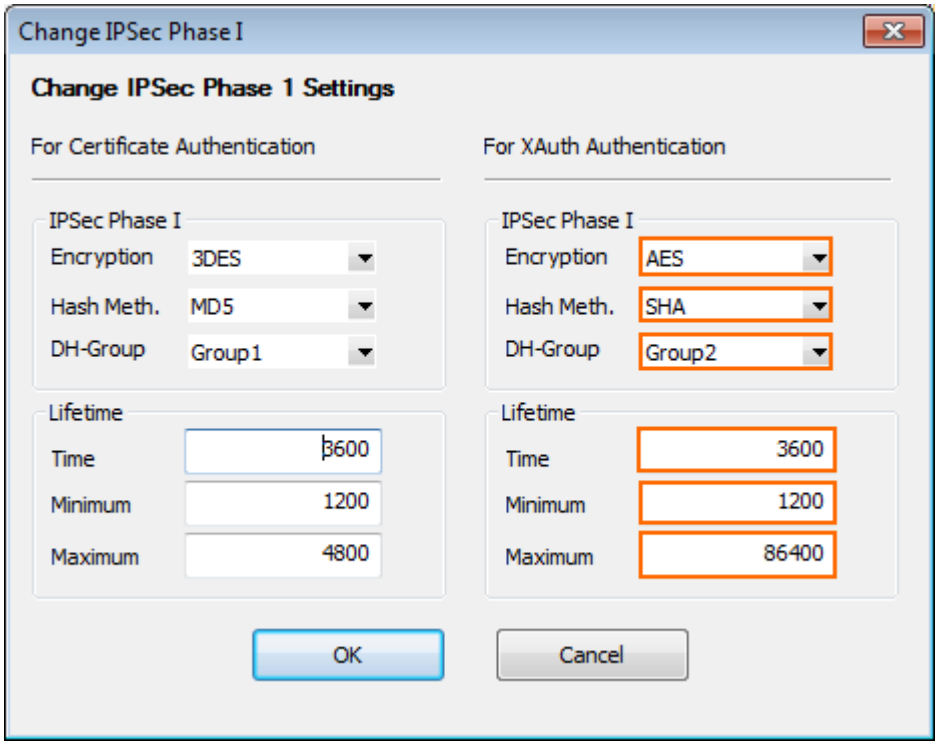
8. Configure the group policy.
   1. Right-click the **Group Policy Condition** table and select **New Rule**. The **Group Policy Condition** window opens.
   2. In the **Group Pattern** field, define the groups that will be assigned the policy. E.g.: `CN=vpnusers*`
   3. In the **Peer Condition** section, verify that **IPsec Client** checkbox is selected.
   4. To use this Group Policy for SSL-VPN VPN Template Resources, and CudaLaunch, enable **Barracuda Client**.
   5. Click **OK**.



9. Configure the encryption and hashing settings:
    1. Click the **IPSec** tab.
    2. Clear the checkbox in the top-right corner.
    3. From the **IPsec Phase II - Settings** list, select the entry that includes **(Create New)** in its name. For example, if you choose *Group Policy* as a name, the entry name is *Group Policy (Create new)* .
    4. Set the following encryption algorithm settings for Phase II:
        - **Encryption** – Select **AES.**
        - **Hash Meth.** – Select **SHA**.
        - **DH-Group** – Select **Group2**.
        - **Time** – Enter `3600`.
        - **Minimum** – Enter `1200`.
        - **Maximum** – Enter `28800`.



5. Click **Edit IPsec Phase I** and select the encryption algorithm in the **For XAuth Authentication** section:
   - **Encryption** – Select **AES.**
   - **Hash Meth.** – Select **SHA**.
   - **DH-Group** – Select **Group2**.
   - **Time** – Enter `3600`.
   - **Minimum** – Enter `1200`.
   - **Maximum** – Enter `86400`.



6. Click **OK** .

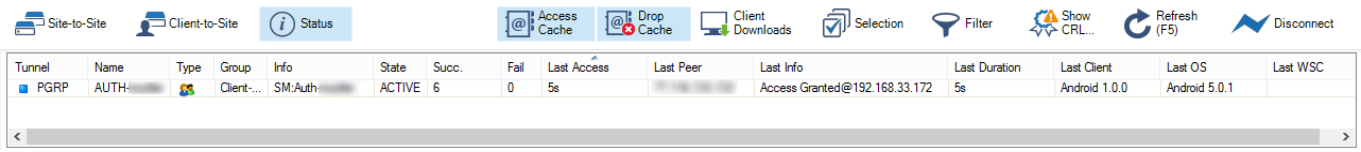
10. Click **OK**.
11. Click **Send Changes** and **Activate**.

Step 4. Add Access Rules

Add two access rules to connect your Client-to-Site VPN to your network. For instructions, see How to Configure an Access Rule for a Client-to-Site VPN.

Monitoring VPN Connections

On the **VPN > Client-to-Site** page, you can monitor VPN connections.



The page lists all available Client-to-Site VPN tunnels. In the **Tunnel** column, the color of the square indicates the status of the VPN:

- **Blue –** The client is currently connected.
- **Green –** The VPN tunnel is available but not in use.
- **Grey –** The VPN tunnel is disabled. To enable the tunnel, right-click it and select **Enable Tunnel**.

For more information about the **VPN > Client-to-Site** page, see VPN Tab.

Troubleshooting

To troubleshoot VPN connections, see the `/yourVirtualServer/VPN/VPN` and `/yourVirtualServer/VPN/ike` log files. For more information, see LOGS Tab.

Figures

1. Client2SiteIPsecXAUTHPSKVPN.png
2. PSK01.png
3. PSK02.png
4. PSK03.png
5. PSK04.png
6. PSK05.png
7. PSK06.png
8. PSK07.png
9. C2S_00.png
10. C2S_01.png
11. C2S_status_connected.png