GlobalProtect Configuration for Apple iOS Devices

Tech Note

Revision A

CONTENTS

Overview

In its original design, IKE only addressed authentication of two devices through a pre-shared symmetric key or a private/public key, in which the public key needed to be exchanged between the two devices to establish a secure tunnel.

Extended Authentication (XAUTH) describes a method of authenticating users as part of the IKE handshake between an IPSec client and gateway after the initial key exchange in phase 1. This concept is supported in a variety of IPSec VPN clients, such as the built in VPN client of Apple iOS devices like the iPhone and iPad.

In this tech note, we describe the steps needed to configure an existing GlobalProtect gateway to enable Apple iOS devices to establish VPN connectivity using the built-in iOS IPSec client. There are three methods for authentication that will be discussed: self-signed certificate, certificate issued by a root Certificate Authority (CA), and pre-shared secret.

Prerequisites

- GlobalProtect Gateway

  Support for XAUTH is introduced in PAN-OS 4.1 as a feature of GlobalProtect Gateway and doesn't require any specific license to be activated.

- Apple iOS

  Supported Apple iOS device running iOS 4.3 or iOS 5.0.

GlobalProtect Gateway Setup

This section describes how to setup the GlobalProtect Gateway and Apple iOS with certificate based authentication for IKE phase 1 and user based authentication (XAUTH) thereafter.

The benefit of such a setup is that you could either use certificates created in the PAN-OS management UI to reliably identify corporate devices, but also use certificates issued by an external certificate authority to authenticate individual devices in the enterprise prior to authenticating the user.

Certificate Creation

In order to setup certificate-based IKE phase 1 authentication, you need to create three certificates either in the PAN-OS management UI or in an external certificate authority.

- Root Certificate Authority

  Every Public Key Infrastructure requires a central source of its trust, which in an X.509 world is usually referred to as the Root Certificate Authority.

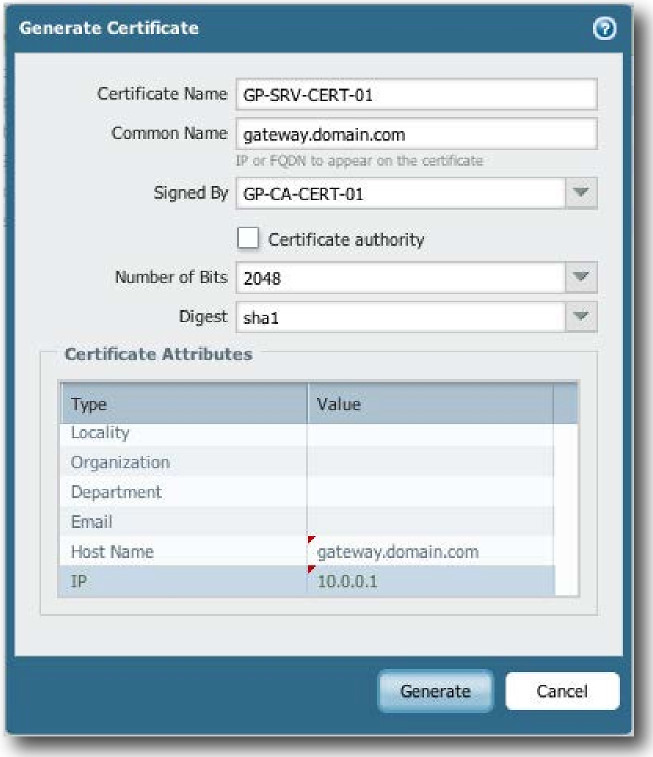
  Like every product leveraging certificate based authentication, GlobalProtect requires the existence of a Root Certificate, which can be either created within PAN-OS or from an external certificate authority (CA). If an external certificate authority is used, the root certificate needs to be imported into PAN-OS.

1. To create a certificate locally, navigate to the *Certificate* page on the *Device* tab and select *Generate*.
2. Enter a unique name for the certificate.
3. Leave the *Signed By* field empty and select the *Certificate authority* checkbox underneath.
4. Click Generate.

- Gateway Certificate

  The certificate for the gateway can be created on PAN-OS or imported from an external certificate authority. This section only covers how to create a certificate locally with a CA certificate on the device

  1. To **create a certificate locally**, navigate to the *Certificate* page on the *Device* tab and select *Generate*.
  2. Enter a unique name for the certificate in the configuration.
  3. Enter the gateway's **DNS hostname** as the **Common Name** (CN).
  4. Enter the gateway's **IP address** in IP address field. Use the device's internal and assigned IP address if your device resides behind a NAT device.
  5. Select the certificate authority created in the "Root Certificate Authority"section in the *Signed By* drop-down to issue this certificate.
  6. Click Generate.



Generate Certificate

Certificate Name: GP-SRV-CERT-01

Common Name: gateway.domain.com

IP or FQDN to appear on the certificate

Signed By: GP-CA-CERT-01

□ Certificate authority

Number of Bits: 2048

Digest: sha1

Certificate Attributes

Type	Value
Locality	
Organization	
Department	
Email	
Host Name	gateway.domain.com
IP	10.0.0.1

- Identity Certificate

  In the case of certificate based authentication, the client and the gateway go through a mutual authentication. Therefore the iOS device requires a certificate from a certificate authority trusted by the gateway. This certificate can either be issued by an external certificate authority or from PAN-OS. This section describes the creation of a client certificate (referred to as an Identity Certificate in iOS) in PAN-OS and the process to export this certificate.

1. To **create a certificate locally**, navigate to the *Certificate* page on the *Device* tab and select *Generate*.
2. Enter a unique name for the certificate in the configuration.
3. Enter any name in the **Common Name** (CN).
4. Select the certificate authority to issue this certificate.
5. Click Generate.

- Certificate Profile

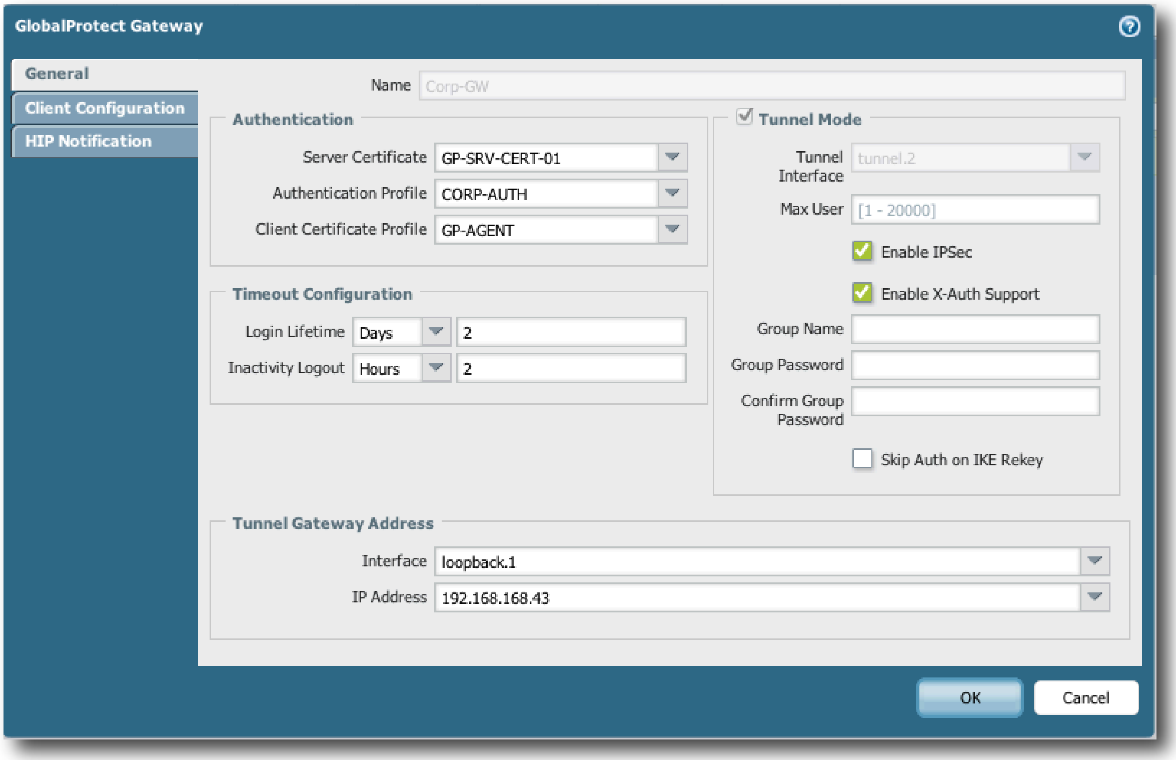
  In order to validate the client certificate, a Client Certificate Profile needs to be created which includes the CA certificate used to create the Identity Certificate. Please refer to the corresponding section on creating Client Certificate Profiles in the Palo Alto Networks Administrator's Guide.

GlobalProtect Gateway Configuration

The following section describes the necessary steps to enable XAUTH required to support Apple iOS devices on an existing GlobalProtect gateway configuration.

Note: If there is no existing GlobalProtect configuration, please refer to the corresponding section in the Palo Alto Networks Administrator's Guide on how to configure a GlobalProtect Gateway.

1. In the *Server Certificate* drop-down, select the **gateway certificate** created in the **"Gateway Certificate"** section of this document.
2. In the *Client Certificate Profile* drop-down, select the **certificate profile** which includes the CA certificate used to issue the client certificate in the **"Client Certificate"** section.
3. Enable "Tunnel Mode" and select "Enable IPSec".
4. Enable **"Enable X-Auth Support"** to enable Extended Authentication.
5. Leave the **"Group Name"** and **"Group Password"** fields empty to enable certificate authentication in IKE phase 1.
6. Click OK and commit the configuration changes.



Name: Corp-GW

Authentication

Server Certificate: GP-SRV-CERT-01

Authentication Profile: CORP-AUTH

Client Certificate Profile: GP-AGENT

Timeout Configuration

Login Lifetime: Days 2

Inactivity Logout: Hours 2

☑ **Tunnel Mode**

Tunnel Interface: tunnel.2

Max User: [1 - 20000]

☑ Enable IPSec

☑ Enable X-Auth Support

Group Name:

Group Password:

Confirm Group Password:

☐ Skip Auth on IKE Rekey

Tunnel Gateway Address

Interface: loopback.1

IP Address: 192.168.168.43

Apple iOS setup

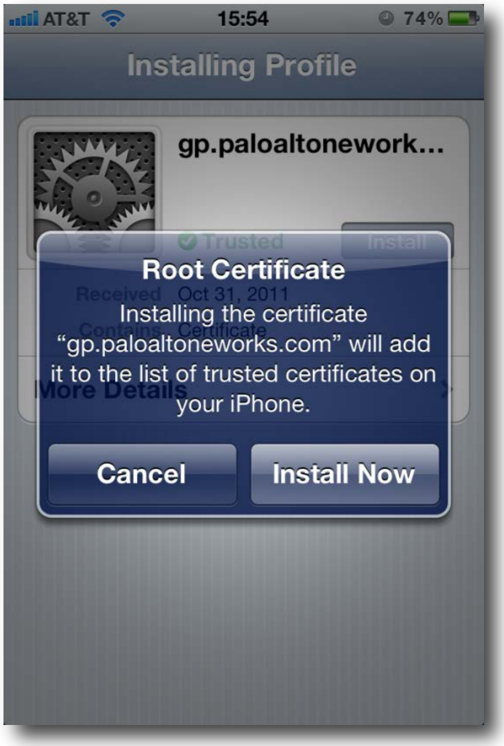
As with the previous section, this section focuses on integrating Apple iOS devices into GlobalProtect Gateway using certificate based authentication in IKE phase 1.

Exporting and Importing Certificates

As the first step, the certificates created in the “Root Certificate Authority” and “Identity Certificate” section need to be exported from PAN-OS and imported into the iOS device.

- Exporting the Root Certificate Authority
    1. In the PAN-OS management UI, navigate to the certificate section in the device configuration tab.
    2. Select the Root CA certificate created in the “Root Certificate Authority” section of this document.
    3. Click *Export* and select “Base64 Encoded Certificate (PEM)” as the file format.
    4. Uncheck the “Export private key” checkbox and click OK.

- Importing the Root Certificate into iOS
    1. Create a new email and attach the Root Certificate exported in the section above.
    2. Send the email to the iOS user.
    3. On the device, open the new email and tap on the root certificate attached.
    4. Select install in the certificate information.
    5. Select *Install Now* when prompted in the dialog and enter your device password.



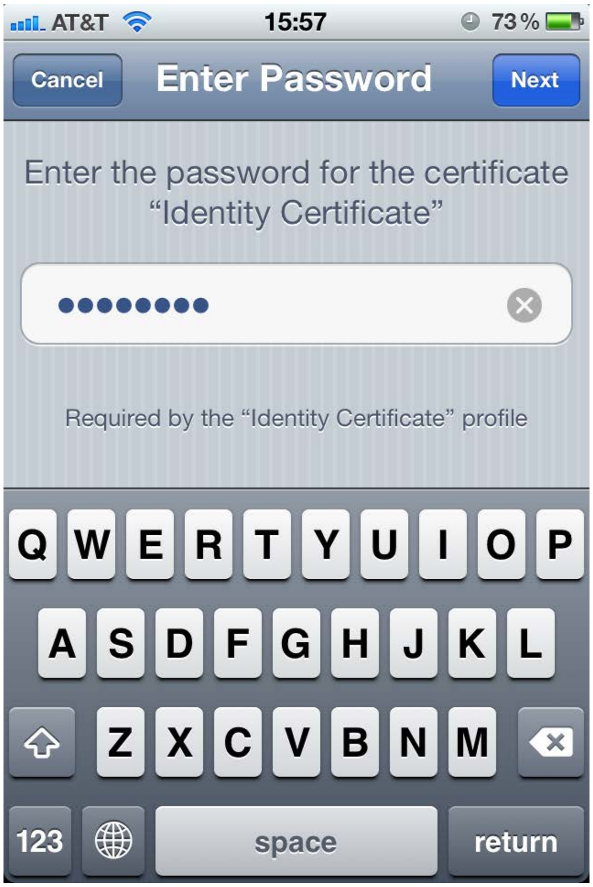
Installing the certificate "gp.paloaltoneworks.com" will add it to the list of trusted certificates on your iPhone.

- Exporting the Identity Certificate

  1. In the PAN-OS management UI navigate to the certificate section in the device configuration tab.
  2. Select the Identity Certificate created in the "Identity Certificate" section of this document.
  3. Click *Export* and select "Encrypted Private Key and Certificate (PKCS12)" as the file format.
  4. Enter an export password and click OK.

- Importing the Identity Certificate into iOS

  1. Compose a new email and attach the Identity Certificate exported in the section above.
  2. Send the email to the iOS user.
  3. On the device, open the new email and tap on the identity certificate attached.
  4. Select install in the certificate information.
  5. Select *Install Now* when prompted in the dialog and enter your device password.
  6. Enter the export password you specified in the previous section and click "Next"



Enter the password for the certificate "Identity Certificate"

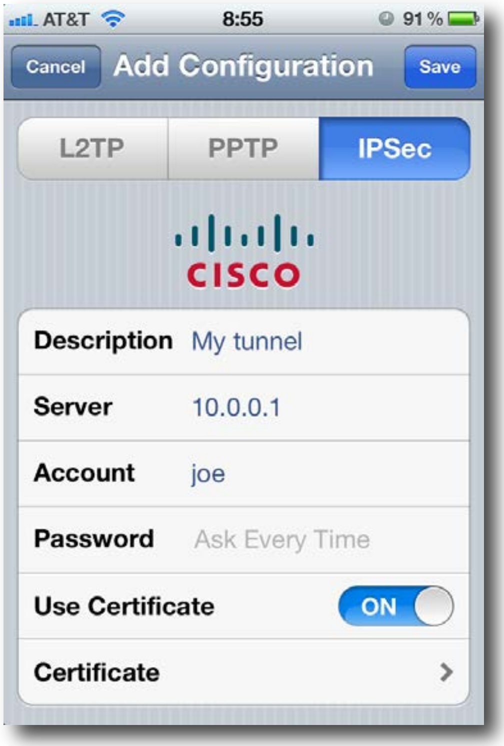
●●●●●●●●●

Required by the "Identity Certificate" profile

Creating a VPN Profile

To create a VPN profile in iOS, open the settings dialog and navigate to the "General > Network > VPN" section and perform the following:

1. Select IPSec as the type.
2. Define a descriptive name for this connection.
3. Enter the address of the GlobalProtect Gateway.
4. Enter the username and password for this iOS device user.
5. Enable the "Use Certificate" option.
6. Select the Identity Certificate in the certificate selection.
7. Click "Save"



Description My tunnel

Server 10.0.0.1

Account joe

Password Ask Every Time

Use Certificate ON

Certificate

Your VPN profile is now configured and you can enable the VPN connection through the iOS device *Settings*.

Apple iPhone Configuration Utility

To simplify configuration of the iOS VPN client and push out a configuration to all of your users, you can use the iPhone Configuration Utility from Apple. This section describes how to create a configuration for iOS devices and distribute it.

Obtaining the Utility

The utility and documentation can be accessed at http://www.apple.com/support/iphone/enterprise/.

Creating a Configuration Profile

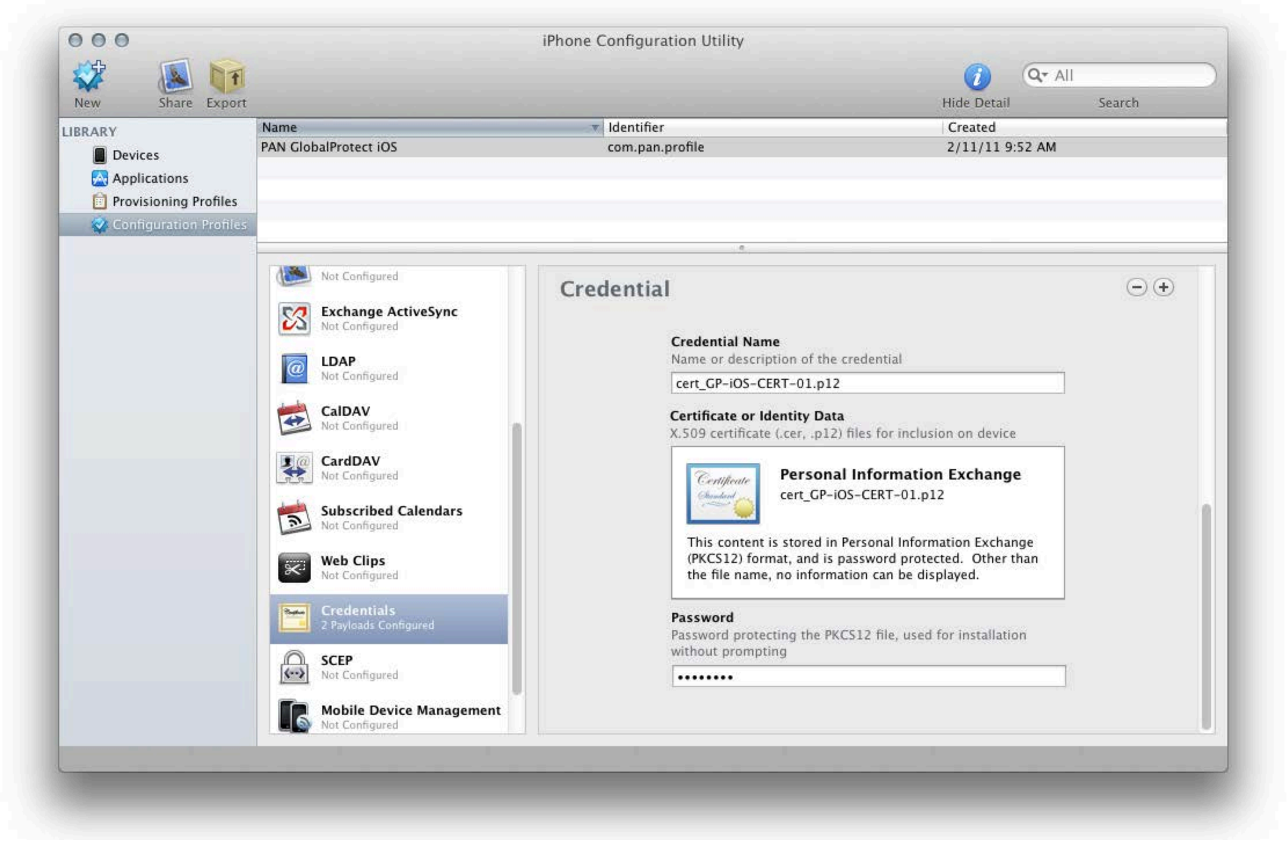
First, after opening the iPhone Configuration Utility, you need to create a new configuration profile for your iOS users.

- Importing the Credentials

  As the next step, you need to import the Root Certificate and Identity Certificate created in the previous sections.

  1. In the iPhone Configuration Utility, select "Credentials" and click "configure"
  2. Click the "add" icon and select the Root Certificate file you exported earlier and click ok.
  3. Click the "add" icon and select the Identity Certificate file (PKCS12) you exported earlier and then click ok.

4. Enter the export password you defined earlier in the password field below the Identity Certificate display.



Name	Identifier	Created
PAN GlobalProtect iOS	com.pan.profile	2/11/11 9:52 AM

Credential

Credential Name
Name or description of the credential
cert_GP-iOS-CERT-01.p12

Certificate or Identity Data
X.509 certificate (.cer, .p12) files for inclusion on device

Personal Information Exchange
cert_GP-iOS-CERT-01.p12

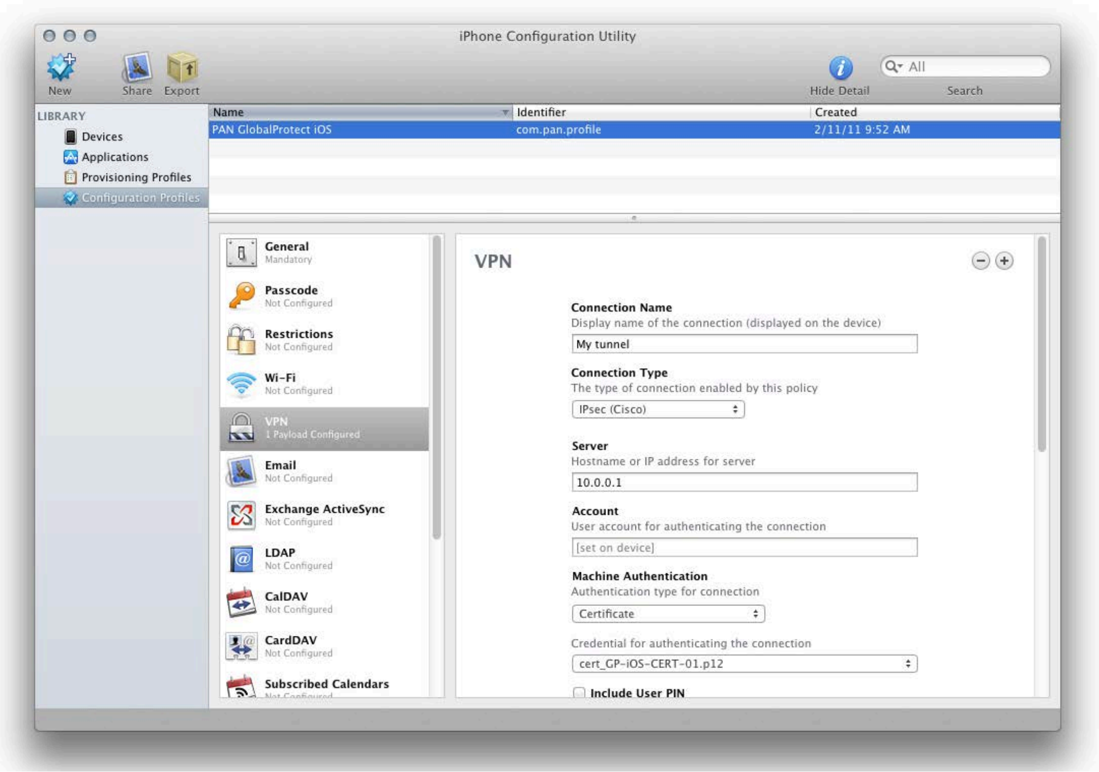
This content is stored in Personal Information Exchange (PKCS12) format, and is password protected. Other than the file name, no information can be displayed.

Password
Password protecting the PKCS12 file, used for installation without prompting
••••••••

- Creating a VPN profile

Next you need to create the profile for the IPSec client connection.

1. In the iPhone Configuration Utility, select “VPN” and click “Configure”.
2. Define a meaningful connection name.
3. For the connection type, choose “IPSec”.
4. Leave the “Account Name” empty unless you want to pre-populate a user name for this configuration.
5. Select “Certificate” under “Machine Authentication” and choose the Identity Certificate imported in the previous section.
6. Select “Share” in the toolbar to start the distribution of the profile.



Name	Identifier	Created
PAN GlobalProtect iOS	com.pan.profile	2/11/11 9:52 AM

VPN

Connection Name
Display name of the connection (displayed on the device)
My tunnel

Connection Type
The type of connection enabled by this policy
IPsec (Cisco)

Server
Hostname or IP address for server
10.0.0.1

Account
User account for authenticating the connection
[set on device]

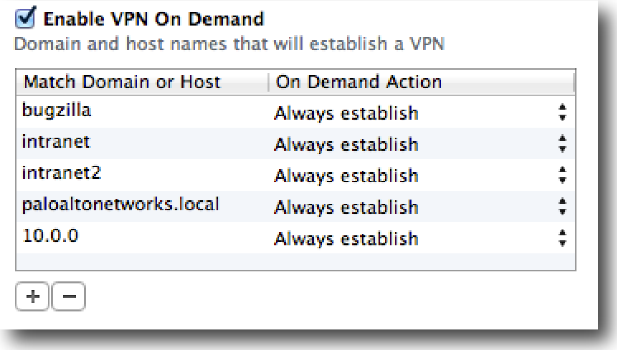
Machine Authentication
Authentication type for connection
Certificate

Credential for authenticating the connection
cert_GP-iOS-CERT-01.p12

□ **Include User PIN**

Optional Automatic Connection Configuration

If you want the iOS VPN to automatically bring up a VPN connection when accessing internal resources, you can use the *Enable VPN On Demand* settings. This is only available when using the Certificate authentication type. In the VPN On Demand section, add strings that match internal hostnames or IP addresses. When iOS attempts a connection to anything containing a string in the list that is set to *Always establish* it will initiate the VPN first.



☑ **Enable VPN On Demand**
Domain and host names that will establish a VPN

Match Domain or Host	On Demand Action
bugzilla	Always establish
intranet	Always establish
intranet2	Always establish
paloaltonetworks.local	Always establish
10.0.0	Always establish

Distributing the Configuration Profile

The easiest way to distribute the configuration profile to a group of users is via email. After you select “Share” in the iPhone Configuration Utility, you can select to send the profile via email.

1. Send the email to the target user or users.
2. On the iOS device, open the email and tap on the attached configuration profile.
3. Select “Install” in the configuration verification dialog and “Install now” in the following pop-up dialog.

Your VPN profile is now configured and you can enable the VPN connection through the iOS device *Settings*.

Pre-Shared Secret Authentication

As an alternative to certificate based authentication in IKE phase 1, you can configure a pre-shared secret based authentication method.

Configuring a Pre-Shared Secret on the GlobalProtect Gateway

1. Navigate to the GlobalProtect Gateway configuration.
2. Enable “Tunnel Mode” and select “Enable IPSec”.
3. Enable “Enable X-Auth Support”.
4. Enter a group name in the tunnel configuration section of the GlobalProtect Gateway General configuration.
5. Enter and confirm the group secret below the group name field.
6. Click Ok and commit the configuration.

Configuring a Pre-Shared Secret on the iOS Device

1. Open your settings application.
2. Navigate to the “General > Network > VPN” section and create a new VPN configuration profile.
3. Select IPSec as the type.
4. Define a descriptive name for this connection.
5. Enter the address of the GlobalProtect Gateway.
6. Enter the username and password for this iOS device user.
7. Enter the group name configured before in the "Group Name" field.
8. Enter the group password in the "Secret" field.
9. Save the configuration and enable your VPN connection.

Configuring a Pre-Shared Secret in the Apple iPhone Configuration Utility

If you configure a pre-shared secret through the iPhone Configuration Utility, you don't need to go through any of the certificate import steps previously outlined. Just perform the following steps to create your VPN configuration profile:

1. In the iPhone Configuration Utility, select “VPN” and click “Configure”.
2. Define a meaningful connection name.
3. For the connection type chose “IPSec”.
4. Leave the “Account Name” empty unless you want to pre-populate a user name for this configuration.
5. Select "Shared Secret / Group Name" in the "Machine Authentication" drop down menu.
6. Enter the group name configured previously in the "Group Name" field.
7. Enter the group password in the "Secret" field.
8. Select “Share” in the toolbar to start the distribution of the profile.