Apple Inc.

Apple IOS 11 VPN Client on iPhone and iPad Guidance Documentation

June 2018

Version 1.3

Contents

Revision History

Version	Date	Description
1.3	June 2018	Updated based for Assurance Continuity

1 Introduction

1.1 Target of Evaluation

The TOE is the Apple iOS VPN Client which runs on iPad and iPhone devices. The IPsec VPN allows users the ability to have confidentiality, integrity, and protection of data in transit regardless of the transport mechanism (cellular or WiFi).

Note: The TOE is the VPN Client software only. The Apple iOS operating system (version 11) has been separately validated (VID10851).

Device Name	Model	Processor	WiFi	Bluetooth
iPhone 5s	A1453 A1457 A1518 A1528 A1530 A1533	A7	802.11/a/b/g/n/ac 802.11/a/b/g/n/ac 802.11/a/b/g/n/ac 802.11/a/b/g/n/ac 802.11/a/b/g/n/ac 802.11/a/b/g/n/ac	4.0 4.0 4.0 4.0 4.0 4.0
iPhone 6 Plus/ iPhone 6	A1522, A1524, A1593/ A1549, A1586, A1589	A8	802.11/a/b/g/n/ac 802.11/a/b/g/n/ac 802.11/a/b/g/n/ac	4.0 4.0 4.0
iPhone 6S Plus/ iPhone 6S	A1634, A1687, A1690, A1699/ A1633, A1688, A1691, A1700	A9	802.11/a/b/g/n/ac 802.11/a/b/g/n/ac	4.2 4.2
iPhone 7 Plus/ iPhone 7	A1661, A1784, A1785, A1786/ A1660, A1778, A1779, A1780	A10	802.11/a/b/g/n/ac 802.11/a/b/g/n/ac	4.2 4.2
iPhone SE	A1662 A1723 A1724	A9	802.11/a/b/g/n/ac	4.2
iPhone 8 Plus/ iPhone 8	A1864, A1897, A1898, A1899/ A1863, A1905, A1906, A1907	A11	802.11/a/b/g/n/ac 802.11/a/b/g/n/ac	5.0
iPhone X	A1901 A1902 A1865	A11	802.11/a/b/g/n/ac 802.11/a/b/g/n/ac	5.0
iPad mini 3	A1599 A1600 A1601	A7	802.11a/b/g/n 802.11a/b/g/n 802.11a/b/g/n	4.0 4.0 4.0
iPad mini 4	A1538 A1550	A8	802.11a/b/g/n 802.11a/b/g/n	4.2 4.2
iPad Air 2	A1566 A1567	A8X	802.11a/b/g/n/ac 802.11a/b/g/n/ac	4.2 4.2
iPad Pro 12.9”	A1670 A1671	A8X	802.11a/b/g/n/ac 802.11a/b/g/n/ac	4.2 4.2
iPad Pro 9.7”	A1673 A1674 A1675	A9X	802.11a/b/g/n/ac 802.11a/b/g/n/ac	4.2 4.2 4.2
iPad 9.7”	A1893	A10	802.11/a/b/g/n/ac	4.2

Device Name	Model	Processor	WiFi	Bluetooth
	A1954		802.11/a/b/g/n/ac	4.2

Table 1 TOE Platforms

This guide describes how to configure the TOE in the evaluated configuration, which is an Always-On IPSec VPN utilizing IKEv2 in order to provide a remote user persistent, secure access to enterprise resources from a remote location, either over WiFi or cellular network, be it GSM or CDMA.

1.2 Cryptographic Support

All cryptographic functions, including random number generation, in the TOE are provided by two cryptographic modules in the TOE platform: The Apple iOS CoreCrypto Kernel Module v8 and Apple iOS CoreCrypto Module v8. See the TOE platform ST (VID10851) for details regarding the available algorithm validation certificates (CAVP).

The TOE Platform performs various required POST tests, including Known Answer Tests, to verify cryptographic functions.

1.3 Glossary

Term	Definition
CA	Certificate Authority
CAVP	Cryptographic Algorithm Verification Program
CDMA	Code Division Multiple Access
DH	Diffie-Hellman
GSM	Global System for Mobile communications
IKE	Internet Key Exchange
MDM	Mobile Device Management
MDPP	Mobile Device Protection Profile
PKI	Public Key Infrastructure
POST	Power-On Self- Test
SA	Security Association
SPD	Security Policy Database
TOE	Target of Evaluation
VPN	Virtual Private Network
VPNPP	VPN Protection Profile

Table 2 Glossary

2 Operational Environment

2.1 Overview

In its evaluated configuration, the TOE is designed to support users in an enterprise setting by providing always-on connectivity via IPSec VPN tunnel in order to provide secure, reliable access to enterprise assets while on the go. To that end, certain elements of IT Infrastructure are utilized

2.2 IT Infrastructure

The following elements of IT Infrastructure are assumed to be present:

1. A VPN Gateway to service connections from the TOE
2. Mobile Device Management (MDM) system
    a. In order to operate in the evaluated configuration, the device must be "supervised" and enrolled in some MDM platform, capable of configuring and publishing the necessary Configuration Profile payload to the device
3. A PKI system
    a. If the TOE will be utilizing x509 certificates for authenticating to the VPN connection, then an enterprise PKI system will need to be in place with the following features:
        i. A CA trusted by both the VPN gateway and the TOE Platform
        ii. An OCSP responder or published CRL to service revocation checking requests.

2.3 Other Assumptions

In order to use the TOE in the evaluated configuration, the TOE Platform (i.e., the iPhone or iPad) must also be configured to meet the requirements of the Mobile Device Protection Profile (MDPP) as set forth in the Security Target and guidance documentation for the Apple iOS 11 software, operating on one of the hardware platforms listed in Table 1.

Additionally, the VPN gateway device in your enterprise's operation environment must support the necessary settings in the VPN Protection Profile.

3 Configuration of the TOE

3.1 Device credential generation

In the evaluated configuration, the TOE supports only the use of X.509v3 certificates for authentication.

3.1.1 Certificate Generation

The enterprise CA will need to generate the X.509v3 certificates to be used for client authentication to the VPN connection, following the guidance from your PKI vendor. Device certificates and keys will need to be bundled as either a PCKS1 or PKCS12 file in order to be imported into the TOE platform.

In the evaluated configuration, the TOE may support RSA certificates with a 2048-bit key, or ECDSA certificates with either a 256- or 384-bit curve length.

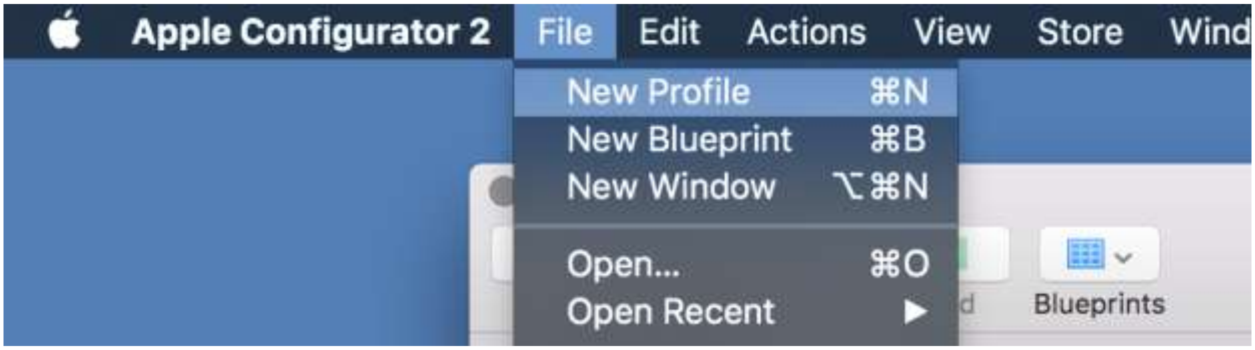
3.2 Configuration Profile

The configuration of the TOE must be done through an MDM platform or similar tool capable of creating configuration profiles, publishing them to the device, and otherwise managing the device. In order to support always-on VPN and, thus, to be operating in the evaluated configuration, the device must be "supervised." Unsupervised devices and BYOD devices cannot be configured to operate in the evaluated configuration.

This guide will assume that the TOE platform is already set up as a supervised device and enrolled in the MDM. Configuration Profile creation will be illustrated by the use of Apple Configurator.

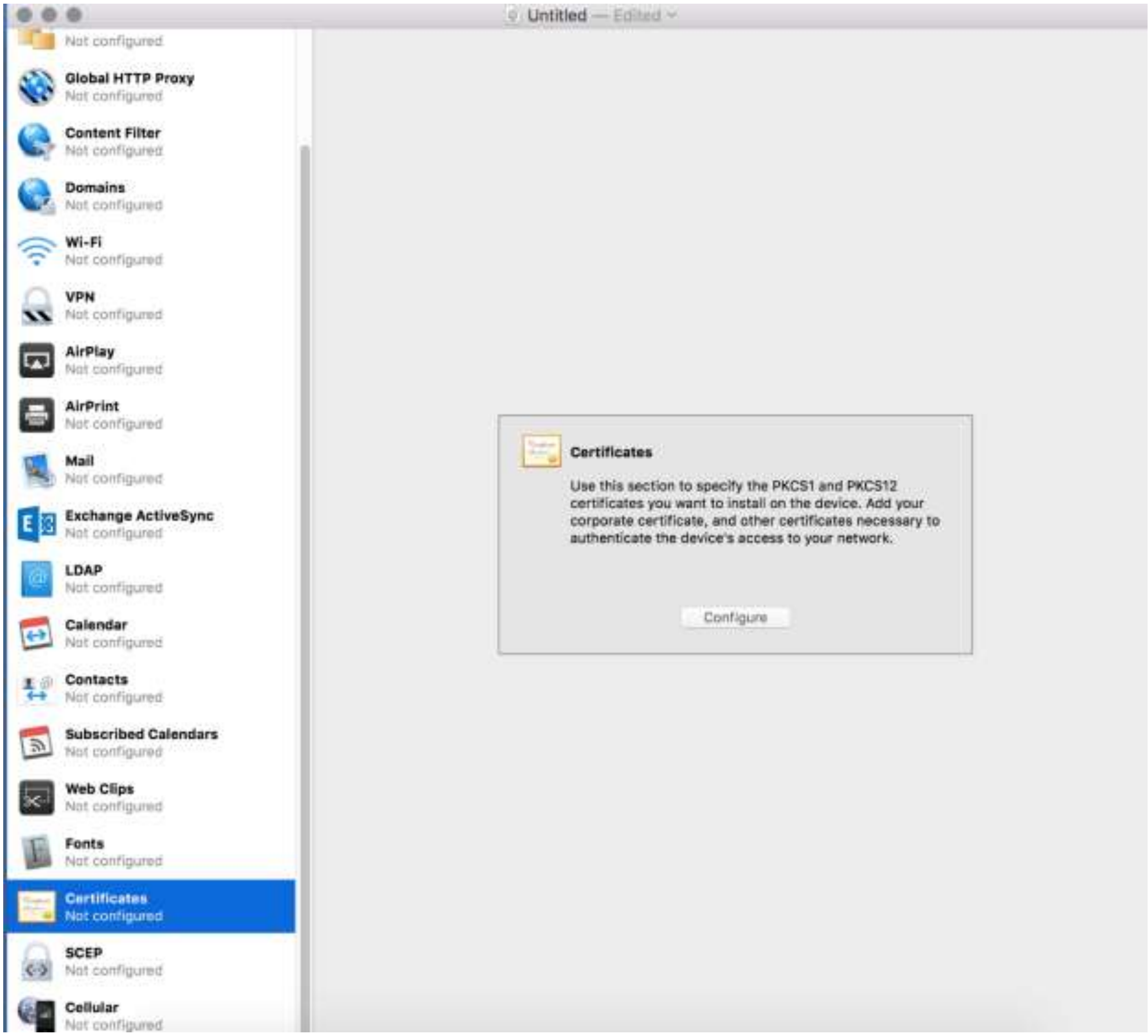
3.2.1 Creating a new configuration profile

Once the device is enrolled and the necessary certificates or PSKs have been generated, the next step is to create a new configuration profile:



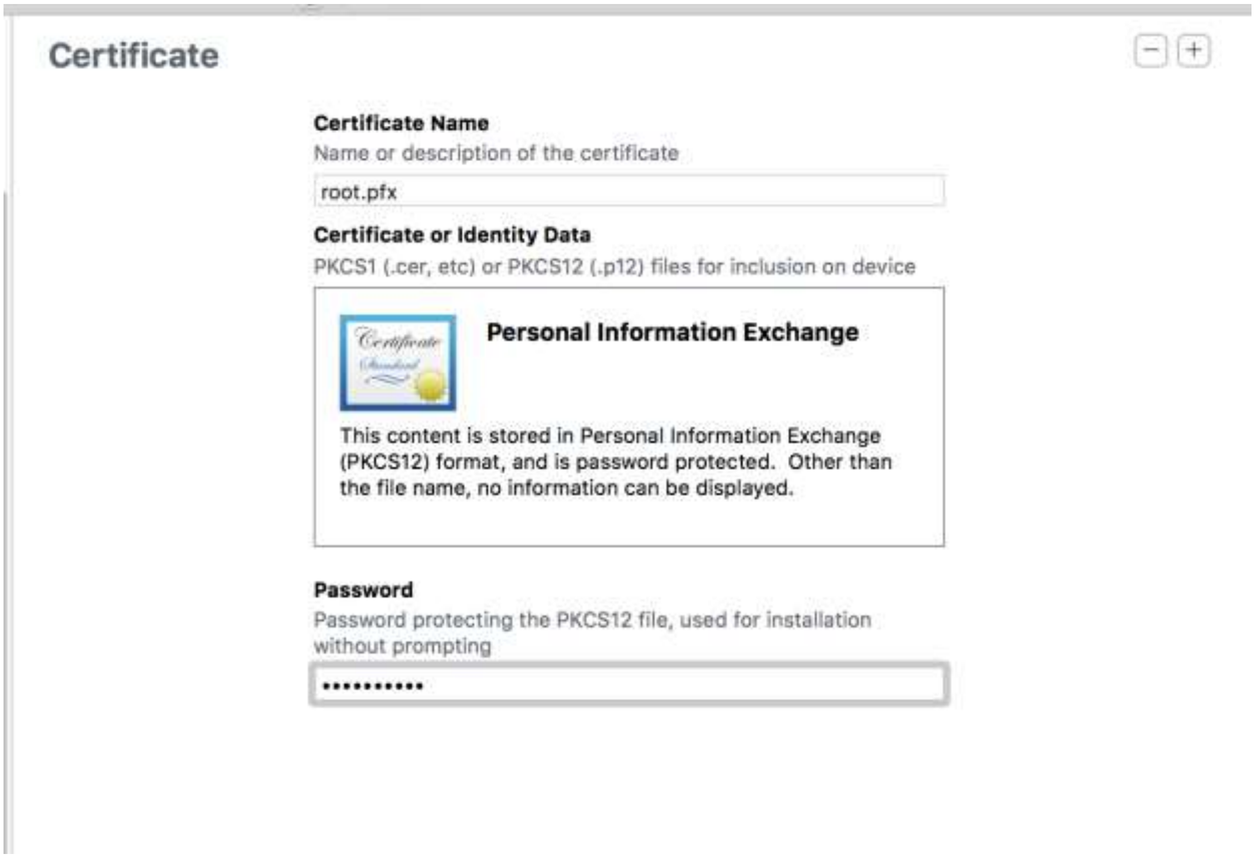
3.2.2 Add Certificate Payloads

If the TOE will be authenticating to the VPN with the use of X.509v3 client certificates, then the device certificate, as well as the enterprise CA certificate used to sign both the device certificate as well as the VPN gateway certificate will need to be added and trusted:



Certificates

Use this section to specify the PKCS1 and PKCS12 certificates you want to install on the device. Add your corporate certificate, and other certificates necessary to authenticate the device's access to your network.



Certificate

Certificate Name

Name or description of the certificate

root.pfx

Certificate or Identity Data

PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device

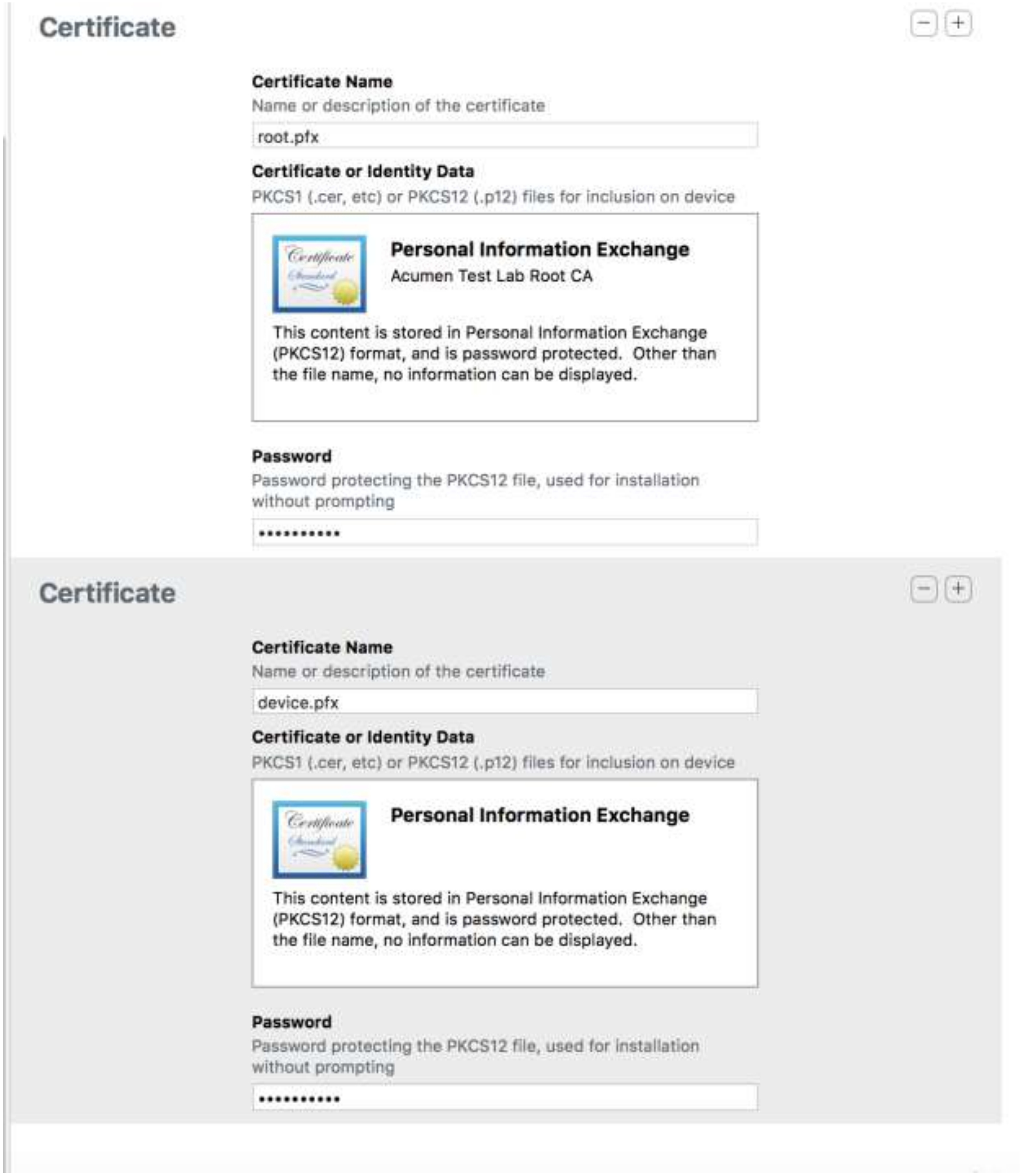
Personal Information Exchange

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

••••••••••



Certificate

Certificate Name
Name or description of the certificate
root.pfx

Certificate or Identity Data
PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device

Personal Information Exchange
Acumen Test Lab Root CA

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
•••••••••••

Certificate

Certificate Name
Name or description of the certificate
device.pfx

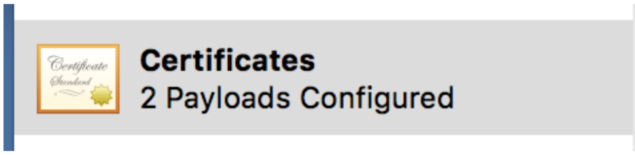
Certificate or Identity Data
PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device

Personal Information Exchange

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
•••••••••••

Apple Configurator should report that 2 payloads are configured for this section:

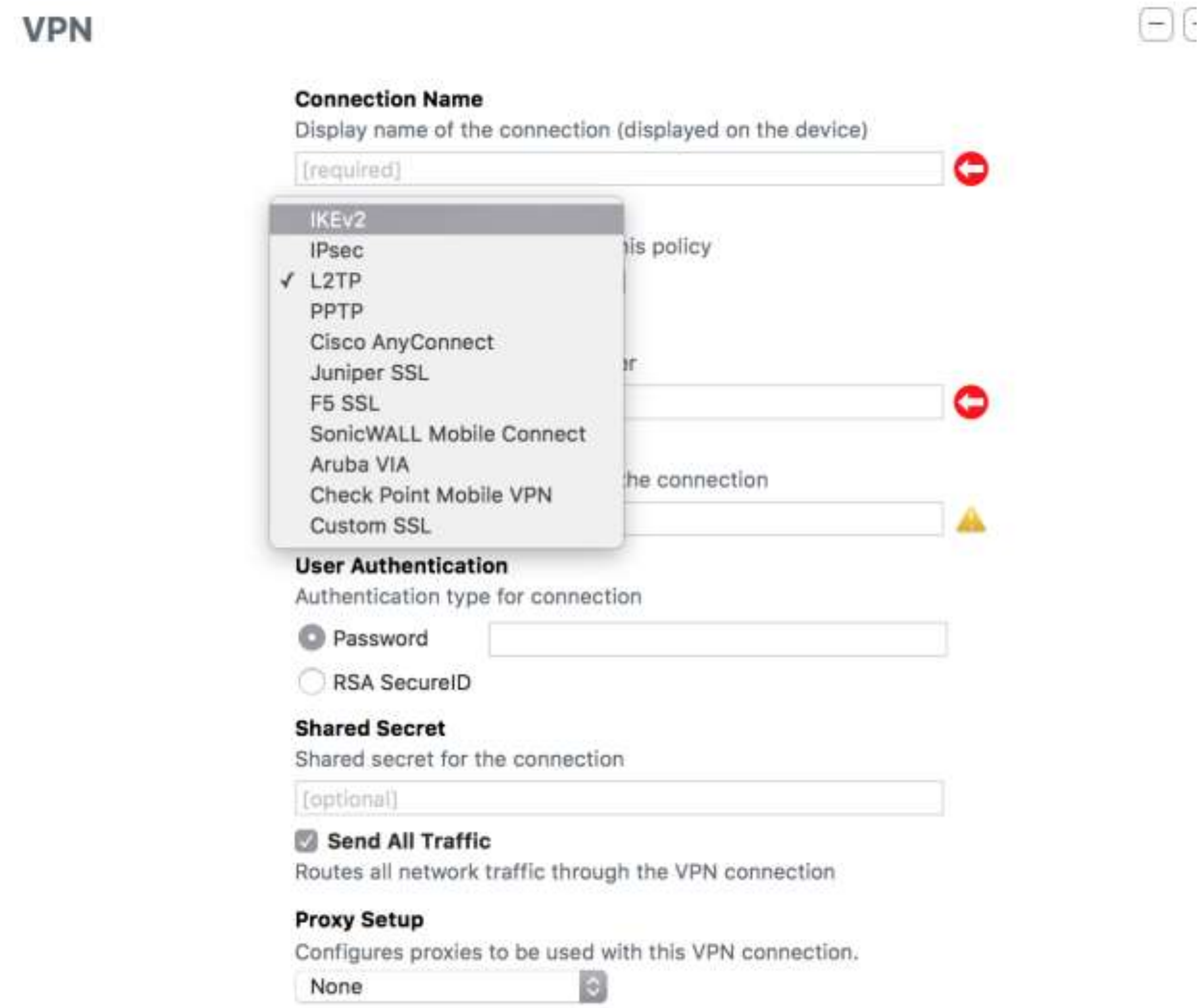


Certificates
2 Payloads Configured

3.2.3 VPN Settings

3.2.3.1 Connection Type

In the evaluated configuration, the TOE supports IPSec with IKEv2 only. Apple Configurator will have L2TP selected by default, so the IKEv2 connection type will need to be selected in order to proceed:



VPN

Connection Name
Display name of the connection (displayed on the device)
[required]

User Authentication
Authentication type for connection
● Password
○ RSA SecureID

Shared Secret
Shared secret for the connection
[optional]

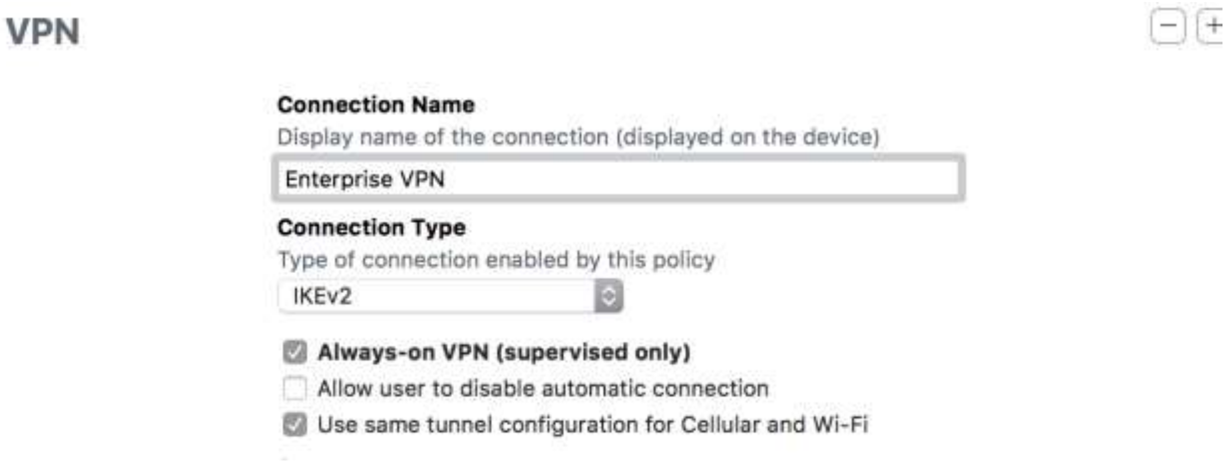
☑ **Send All Traffic**
Routes all network traffic through the VPN connection

Proxy Setup
Configures proxies to be used with this VPN connection.
None

All of the configurable options will then change to allow us to set up the TOE in the evaluated configuration.

3.2.3.2 Always-on VPN

To operate in the evaluated configuration, Always-on VPN must be selected (note: Always-on VPN only supports IPsec Tunnel mode):



VPN

Connection Name
Display name of the connection (displayed on the device)
Enterprise VPN

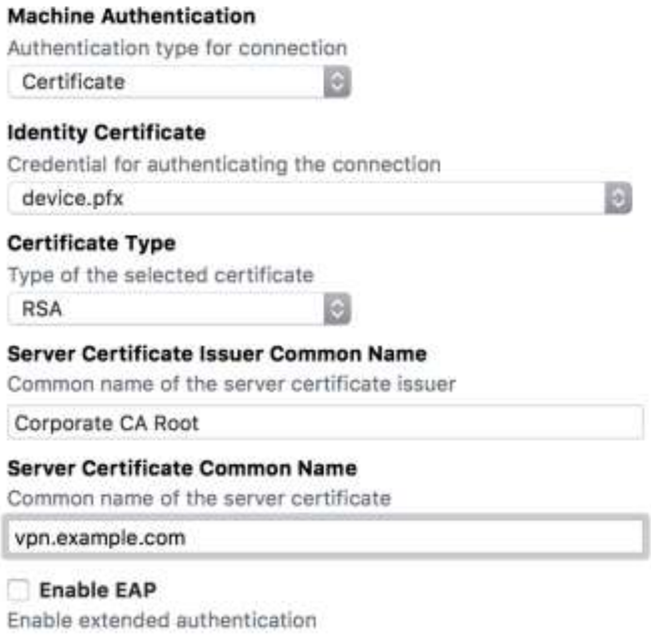
Connection Type
Type of connection enabled by this policy
IKEv2

☑ **Always-on VPN (supervised only)**
□ Allow user to disable automatic connection
☑ Use same tunnel configuration for Cellular and Wi-Fi

The user should not be permitted to disable the automatic connection. Whether or not to use the same tunnel configuration for both Cellular and Wi-Fi depends on the operating environment the TOE will be configured to connect to. For illustration purposes, the option will be selected.

3.2.3.3 Machine Authentication

For machine authentication, there are two options: “Certificate” and “Shared Secret” (PSK). To operate the TOE in the evaluated configuration, “Certificate” must be selected. The certificate type must be selected to match that of the certificate payload provided, and be one of the supported certificate types (RSA or ECDSA) previously listed in section 3.1.1.



Machine Authentication
Authentication type for connection
Certificate

Identity Certificate
Credential for authenticating the connection
device.pfx

Certificate Type
Type of the selected certificate
RSA

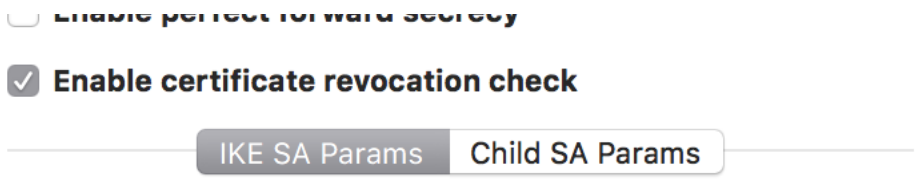
Server Certificate Issuer Common Name
Common name of the server certificate issuer
Corporate CA Root

Server Certificate Common Name
Common name of the server certificate
vpn.example.com

□ **Enable EAP**
Enable extended authentication

The Server Certificate Issuer Common Name and Server Certificate Common Name must match whatever is in the CN of your corporate CA certificate, as well as the certificate for your VPN gateway. The values will not auto-populate and must be manually entered by the administrator.

Additionally, when using certificates, revocation checking must be enabled:



□ Enable perfect forward secrecy

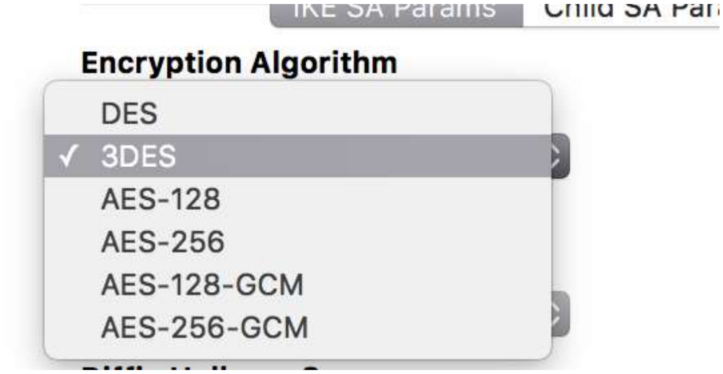
☑ Enable certificate revocation check

3.2.3.4 *IKE SA Parameters*

In order to operate in the evaluated configuration, the IKE (Phase 1) SA parameters must meet the requirements in the VPNPP, as stated in the TOE Security Target. The allowed/disallowed options are discussed in the sections below.

3.2.3.4.1 Encryption Algorithm

To operate in the evaluated configuration, one of the AES ciphers must be selected. Both 128 and 256 bit are supported in both CBC and GCM modes. However, neither DES nor 3DES may be used, although 3DES will be the default in the Apple Configurator Drop Down:



Encryption Algorithm

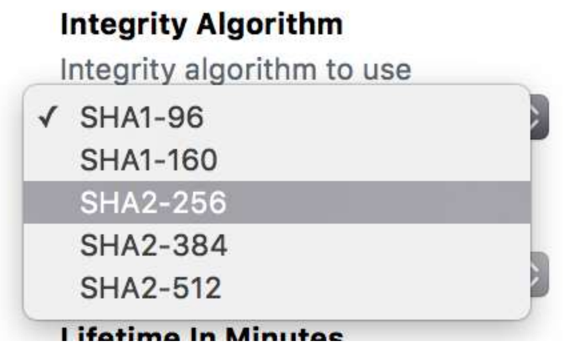
DES
✓ 3DES
AES-128
AES-256
AES-128-GCM
AES-256-GCM

AES-128 and AES-256 are the CBC modes of operation.

Whether to use GCM or CBC, as well as the bit length, depends on what support was implemented in the VPN gateway and the selection on the TOE will need to reflect the settings on the VPN gateway.

3.2.3.4.2 Integrity Algorithm

With the exception of SHA1-96, any of the supported integrity algorithms may be used in the evaluated configuration. Please note that SHA1-160 is not supported in the TOE with AES-CBC ciphers, only AES-GCM ciphers.

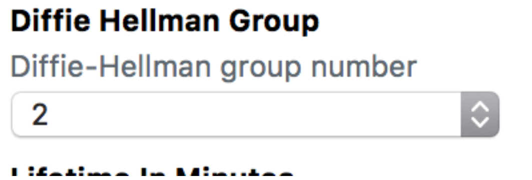


Integrity Algorithm

Integrity algorithm to use

3.2.3.4.3 Diffie Hellman Group

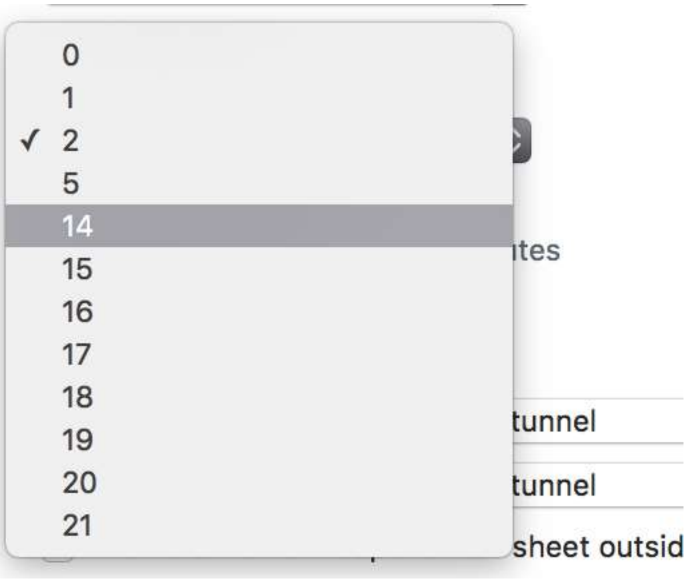
The only DH groups supported by the TOE in the evaluated configuration include the following, Group 1, Group 2, Group 5, Group 14, Group 15, Group 16, Group 17, Group 18, Group 19, and Group 20. In order to operate in the evaluated configuration, one of these must be selected. Again, it must match what the VPN Gateway expects.



Diffie Hellman Group

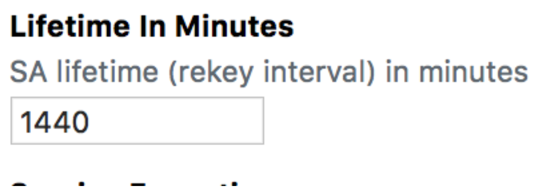
Diffie-Hellman group number

2



3.2.3.4.4 SA Lifetime

SA Lifetimes are configurable based on time. The default for the IKE SA is 1440 minutes, or 24 hours. The SA rekey will actually happen at 75% of the time interval. The 24 time limit is that used in the evaluated configuration.



Lifetime In Minutes

SA lifetime (rekey interval) in minutes

1440

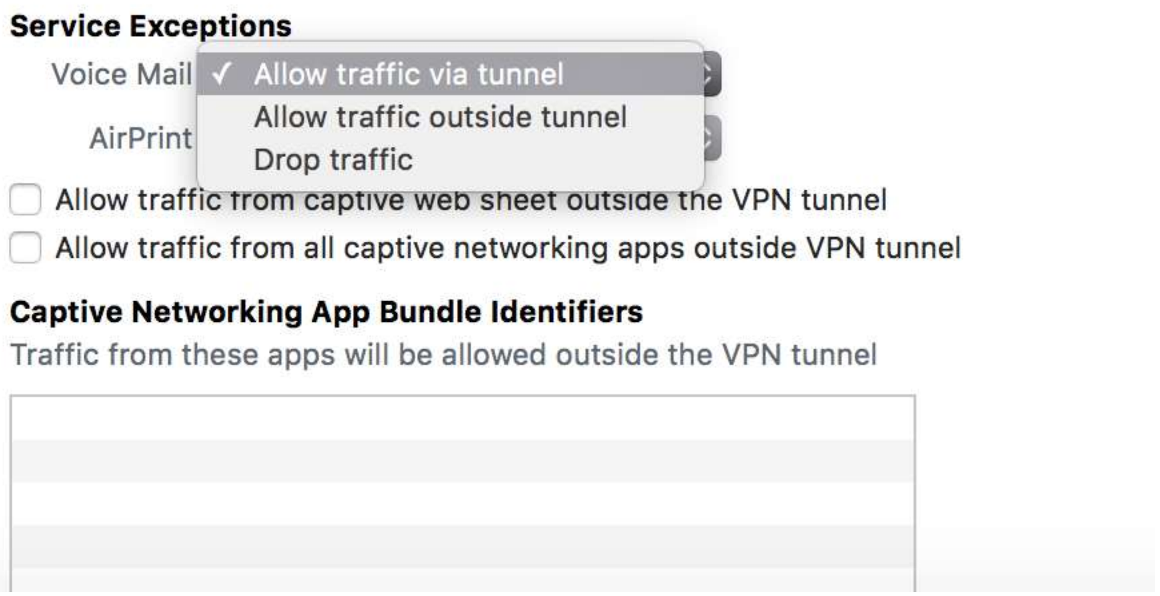
3.2.3.5 Child SA Parameters

All Child (Phase 2) SA parameters may be configured the same as the IKE SA parameters, with the exception that the lifetime of the SA should be set to 8 hours (480 minutes). Please note that the Child SA rekey will actually happen at 75% of the selected time.

3.2.3.6 Service Exemptions and Security Policy Database

The TOE provides support for making changes to the Security Policy Database (SPD) through the use of Service Exemptions and Captive Networking App Bundle Identifiers.

The two main services which can be configured are Voice Mail and AirPrint. Both of these support the required actions of DISCARD, BYPASS or PROTECT.



Service Exceptions

Voice Mail ✓ Allow traffic via tunnel

AirPrint

□ Allow traffic from captive web sheet outside the VPN tunnel

□ Allow traffic from all captive networking apps outside VPN tunnel

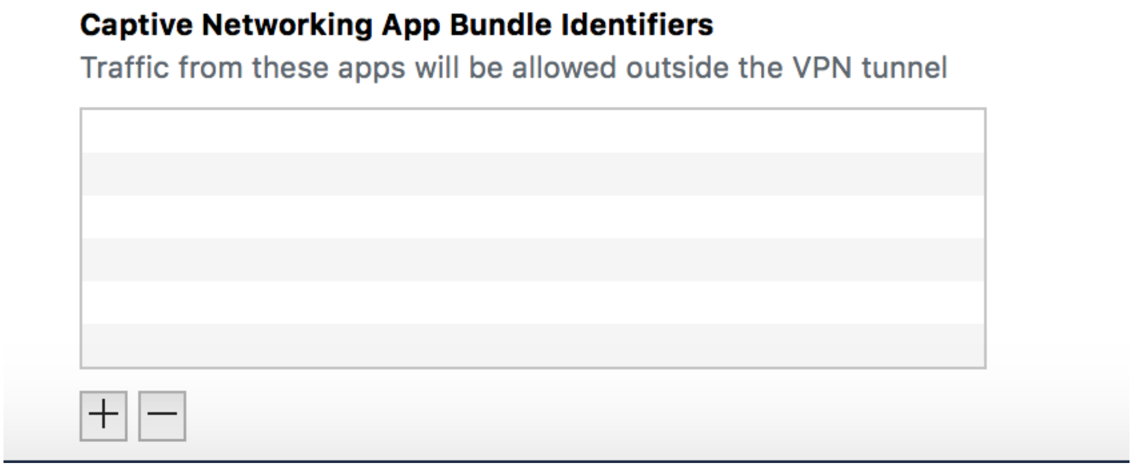
Captive Networking App Bundle Identifiers

Traffic from these apps will be allowed outside the VPN tunnel

In order to set a service to match a PROTECT rule in the SPD, select “Allow traffic via tunnel.” “Drop Traffic” will cause that traffic to match a DISCARD rule. “Allow traffic outside tunnel” will create a BYPASS rule for that service.

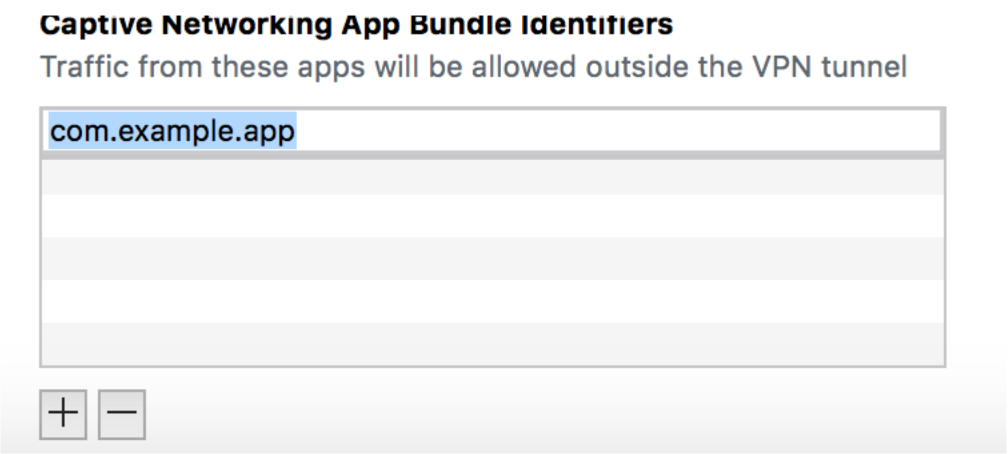
Please note that depending on the carrier, sending visual voice mail traffic through the VPN may result in the traffic being rejected by the carrier network. Consult with your carrier before selecting this option.

Additionally, captive web sheets and captive networking apps may have BYPASS rules created for them:



Captive Networking App Bundle Identifiers

Traffic from these apps will be allowed outside the VPN tunnel



Captive Networking App Bundle Identifiers

Traffic from these apps will be allowed outside the VPN tunnel

com.example.app

3.2.4 Publish Configuration Profile

Once the configuration profile has been created, it must be published to the TOE platform via your MDM following the instructions from your MDM vendor.

3.3 TOE Operation

3.3.1 Usage

Once the Configuration Profile is published to the TOE Platform and enabled, the VPN connection should become active. The status bar of the iOS display should show an icon indicating that a VPN connection has been established and data should be all flowing through the IPSec tunnel.

Functionality can be verified by accessing an enterprise asset, such as an intranet page, which does not have a public-facing presence, as well as by checking the status of the connection in the Device Settings application on the TOE Platform itself.

These configurations can be used to connect to any gateway IKE/IPSec device. This includes any CA used to verify certificate validity.

In the event that the connection between the TOE and the remote gateway is broken (For instance, due to loss of Wi-Fi or LTE signal, downtime on the gateway, or some other interruption), the TOE will repeatedly attempt to retry establishing a connection. No network traffic which does not otherwise have an exception will be allowed to leave the device until the connection is re-established.

3.3.2 Updating the TOE

Updating the TOE is done by updating the iOS software on the TOE Platform itself, as the TOE is the native client built into the Apple iOS software.

Verification of update packages are conducted by the TOE platform, using digital signatures to verify authenticity and integrity

4 External References

- Configuration Profile Reference, Apple Inc., 2015
  - https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/iPhoneConfigurationProfileRef.pdf